Advanced Science and Technology Letters

The ASTL series is committed to the publication of proceedings of Advanced Science and Technology. Its objectives is to publish original research in various areas of Science and Technology. This will provide good chances for academic and industry professionals to discuss recent progress in areas of Science and Technology.

Research papers were strictly peer-reviewed by program committees to make sure that the papers accepted were high quality and relevant to the current and future issues and trends in Science and Technology. The scope of ASTL includes the entire area of science and technology from the current and future trends. The language of publication is English. The Authors have to sign the SERSC ASTL copyright transfer form.

Information Security and Assurance

Proceedings
International Conference, ISA 2012
Shanghai China, April 2012

ISSN 2287-1233

ASTL
Proceedings

The 6th International Conference on Information Security and Assurance

ISA 2012

April 28-30, 2012

Howard Johnson Hongqiao Airport Hotel Shanghai,
Shanghai, China.
Foreword

Information Security and Assurance are areas that attracted many academic and industry professionals to research and develop. The goal of this conference is to bring together the researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of Information Security and Assurance.

We would like to express our gratitude to all of the authors of submitted papers and to all attendees, for their contributions and participation. We believe in the need for continuing this undertaking in the future.

We acknowledge the great effort of all the Chairs and the members of Editorial Committee of the above-listed event. Special thanks go to SERSC (Science & Engineering Research Support Society) for supporting this conference.

We are grateful in particular to the following speaker who kindly accepted our invitation and, in this way, helped to meet the objectives of the conference: Prof. Prof. Bharat Bhargava, Purdue University; Prof. Chin-Chen Chang, Feng Chia University; Prof. Sabah Mohammed, Lakehead University, Canada, and Prof. Jinan Fiaidhi, Lakehead University, Canada.

April 2012

Chairs of ISA 2012
Preface

We would like to welcome you to the Regular Papers proceedings of The 6th International Conference on Information Security and Assurance (ISA 2012) which was held on April 28-30, 2012, at Howard Johnson Hongqiao Airport Hotel Shanghai, Shanghai, China.

ISA 2012 is focused on various aspects of advances Information Security and Assurance. It provided a chance for academic and industry professionals to discuss recent progress in the related areas. We expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. We would like to acknowledge the great effort of all the Chairs and members of the Editorial Committee.

We would like to express our gratitude to all of the authors of submitted papers and to all attendees, for their contributions and participation. We believe in the need for continuing this undertaking in the future.

Last but not the least, we give special thanks to Leian Bartolome, graduate student of KAIST, Korea who contributed to the editing process of this volume with great passion.

April 2012

Jemal Abawajy  
Muhammad Khurram Khan  
Ronnie D. Caytiles  
Yvette E. Gelogo
Organization

General Chair
J. H. Abawajy, Deakin University, Australia

Program Chair
Muhammad Khurram Khan, King Saud University, KSA

Publicity Chair
Tao Gong, Donghua University, China and Purdue University, USA

Editorial Committee
Jin Wang, Nanjing University of Information Science & Technology, China
Hsi-Ya Chang (Jerry), National Center for High Performance Computing, Taiwan
Aboul Ella Hassanien, Cairo University, Egypt
Adrian Stoica, NASA JPL, USA
Carlos Ramos, GECAD and ISEP, Portugal
Muhammad Khurram Khan, King Saud University, Kingdom of Saudi Arabia
Dominik Slezak, Warsaw University & Infobright, Poland
Filip Orsag, BUT, Faculty of Information Technology, Czech Republic
Gongzhu Hu, Central Michigan University, U.S.A
Hideo KURODA, FPT University, Vietnam
J. H. Abawajy, Deakin University, Australia
Javier Garcia-Villalba, Universidad Complutense of Madrid, Spain
Kirk P. Arnett, Mississippi State University, U.S.A
Martin Drahansky, BUT, Faculty of Information Technology, Czech Republic
Muhammad Khurram Khan, King Saud University, KSA
Sabah Mohammed, Lakehead University, Canada
Samir Kumar Bandyopadhyay, University of Calcutta, Kolkata, India
Sankar Kumar Pal, Indian Statistical Institute, India
Tadashi Dohi, Hiroshima University, Japan
Tao Gong, Donghua University, China
Tatsuya Akutsu, Kyoto University, Japan
Wai-chi Fang, National Chiao Tung University, Taiwan
Wenbin Jiang, Huazhong University of Science & Technology, China
Hsi-Ya Chang (Jerry), National Center for High Performance Computing, Taiwan
# Table of Contents

A KTAP Framework for Investigating Cellular Self-Repair Mechanism under IR perturbations ................................................................. 1  
Qi jinpeng, Ding Yongsheng, Gong Tao, and Lin ying

Cryptanalysis of A Robust and Efficient Smart Card Based Remote Login Mechanism for Multi-Server Architecture .......................................... 4  
Chun-Ta Li, Chi-Yao Weng, and Chun-I Fan

An XML based Single Sign-On Scheme for Multimedia Device Control in the Ubiquitous Home Network ..................................................... 7  
Dongkyoo Shin and Dongil Shin

Breaking H^2-MAC using Birthday Paradox ........................................... 10  
Fanbao Liu, Tao Xie, and Changxiang Shen

Gabor Based Optimized Discriminant Locality Preserving Projection for Biometric Recognition ................................................................. 13  
Xi Chen and Jiashu Zhang

A Quantum Mechanical Meet-in-the-middle Attack Against NTRU ............... 16  
Zhijian Xiong, Jinshuang Wang, Yanbo Wang, Tao Zhang,  
and Liang Chen

The Effect of Chunk-Based Jitter Management Algorithm on IP Packet Size .... 19  
Ikram Ud Din, Noor ul Amin, and Arif Iqbal

On Security of A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment ........................................... 22  
Cheng-Chi Lee, Yan-Ming Lai, and Chun-Ta Li

Attack on Fully Homomorphic Encryption over Principal Ideal Lattice ........ 26  
Gu Chun-sheng and Gu Ji-xing

Combing Multi-Independent Algorithms for Human Face Recognition ........ 29  
Wenkai Xu and Eung-Joo Lee
Robustness of Regional Internet to both Random and Targeted Attacks ............. 32
Ye Xu and Zhuo Wang

Access Control and Security in Cloud Computing Systems ................................. 35
Xixu Fu, Kaijun Wu, and Xizhang Gong

A Design of Electronic Payment Authentication Method based on NFC Smartphone ............................................................................................. 38
Seolhwa Han, Okkyung Choi, Kangseok Kim, Hongjin Yeh, and Taesik Shon

Comments on Chang-Lee's Anonymous E-Voting Scheme ................................. 41
Chun-Ta Li and Min-Shiang Hwang

The Cluster Modeling with Zone-Based Multi-hop Communication in Wireless Sensor Networks ............................................................................... 44
Choon-Sung Nam, Kyung-Soo Jang, Gyoo-Seok Choi, and Dong-Ryeol Shin

An Light-weight Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks ........................................................................... 47
Jianhong Zhang, Cui Yuanbo, and Chen Zhipeng

Parallel Reduction Algorithm of Multiple-Precision over Finite Field GF(2n) .... 50
Yongnan Li, Limin Xiao, Aihua Liang, Zhenzhong Zhang, Li Ruan

Web Services Based on OPC Unified Architecture .............................................. 53
Jianping Qiu, Lichao Chen, and Yingjun Zhang

Secure Business Transaction based on ebXML APPLYING Web Service Security ............................................................................................ 56
Dongkyoo Shin and Dongil Shin

Transparent Visitor Centric Web Metering Using Identity Management Systems ........................................................................ 59
Fahad Alarifi

DEVS-based Modeling, Simulation, Scheduling of Bottleneck Process in Semiconductor Manufacturing .......................................................... 62
Youngshin Han, JinMyoung Kim, and Chilgee Lee
A Distribution Model for Issuing Mechanism of Wrapper-based Digital Publication .......................................................... 65
   Wei-Chen Wu, Horng-Twu Liaw, Jiann-Fu Lin, Li-Lin Hsiao,
   and Chih-Ta Yen

Security Evaluation of Mobile Device Management Agents .................. 68
   Keunwoo Rhee, Hawon Kim, and Hac Yun Na

Improved Password-Authenticated Key Agreement Using Smart Cards .... 71
   Kai Chain, Wen-Chung Kuo, Jiin-Chiou Cheng, and Jar-Ferr Yang

An Off-Line Dictionary Attack on Abdalla and Pointcheval's 3-Party Key Exchange Protocol ......................................................... 74
   Junghyun Nam, Jinsoo Kim, Juryon Paik, and Dongho Won

Gesture Recognition based on 2D and 3D Feature by using Kinect Device .... 77
   Wenkai Xu and Eung-Joo Lee

   Yi Wang and Zhoujun Li

A New Method for Key Sharing in Wireless Mesh Networks .................. 83
   Peng Xiao, Jingsha He, and Yingfang Fu

The Design of a Novel Signature Scheme Based on the SIS Problem ......... 86
   Yanqing Yao, Zhoujun Li, and Hua Guo

Interleaving and Collusion Attacks on a Dynamic Group Key Agreement Scheme for Low-Power Mobile Devices ........................................... 89
   Junghyun Nam, Juryon Paik, Jeeyeon Kim, Youngsook Lee,
   Woongryul Jeon, and Dongho Won

Designing Secure SMS Scheme on Android OS .................................... 92
   Jongseok Choi and Howon Kim

An Improved Quantum-behaved Particle Swarm Optimization Algorithm Based on Culture ............................................................... 95
   Gao X. Z, Wu Ying, Huang Xianlin, and Kai Zenger
Study on Analysis Method for SELinux Security Policy ................................. 98
Gaoshou Zhai and Tong Wu

An Alert Correlation Analysis Oriented Incremental Mining Algorithm
of Closed Sequential Patterns with Gap Constraints ................................. 101
He Hui, Wang Dong, Zhang Weizhe, and Zhang Hongli

Invariant Image Watermarking Using Harris Feature Extraction
and Zernike Moments ................................................................. 104
XIAO-CHEN YUAN and CHI-MAN PUN

Cryptanalysis of a two-factor user authentication scheme over
Insecure channels ........................................................................ 107
Jin Qiuyan, Kwangwoo Lee, and Dongho Won

Time-Space Trust in Networks ....................................................... 110
Shunan Ma, Jingsha He, and Yuqiang Zhang

Secure Password by Using Two Factor Authentication in Cloud Computing....113
Ali Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, and Deqing Zou

Testing an Anomaly Detection Scheme ........................................ 116
Jinlong Piao and Seong Baeg Kim

Multi-resolution Image Authentication Watermarking Based
on Progressive Image Transmission .................................................. 119
Piyu Tsai, Yu-Chen Hu, Hsiu-Lien Yeh, and Wei-Kuan Shih

An Introduction to Privacy Critical Location-Sharing Services ............. 122
FEI XU, JINGSHA HE, JING XU, and YUQIANG ZHANG

Sybil Attacks VS Identity Clone Attacks in Online Social Networks ..........125
Lei Jin, Xuelian Long, Hassan Takabi, and James B.D. Joshi

A Resilient Privacy Ensuring Protocol for Smart Metering in Smart Grid.......128
Waleed Akram Baig, Faraz Idris, Ki-Hyung Kim, and Seung Yoo

A User Oriented Negative Access Control Model in Cloud Computing .......131
Xiaohui Li, Jingsha He, and Ting Zhang
Encryption Extensions Model based on Hidden Attribute Certificate .......... 134
    LI Yu, ZHAO Yong, GONG Bei

An Encrypted Verification Method for Effective Black Hole Attack in Mobile Ad Hoc Networks ......................................................... 137
    Firoz Ahmed, Seok Hoon Yoon, and Hoon Oh

A Model-driven Approach to Secure Development Lifecycle ............... 140
    Zhendong Ma, Christian Wagner, Arndt Bonitz, Thomas Bleier,
    Robert Woitsch, and Markus Nichterl

Analysis of Human Identification based on Soft Biometrics in Video Surveillance System .......................................................... 143
    Min-Gu Kim, Hae-Min Moon, and Sung Bum Pan

A Semantic Rule-based Detection Scheme against Flooding Attacks on Application Layer ................................................................. 146
    Chu-Hsing Lin, Chen-Yu Lee, Shin-Pin Lai, and Wei-Shen Lai

A Cloud-aided RSA Signature Scheme for Digital Forensics Applications ...... 149
    Chu-Hsing Lin, Chen-Yu Lee, and Tang-Wei Wu

A Ticket based Authentication Scheme for Group Communication .......... 152
    Soobok Shin, Hongjin Yeh, and Kangseok Kim

MalSig: Collaborative Malware Clustering and Signature Generation using Rendezvous-based Sharing .............................................. 156
    Xiaofeng Wang, and Jinshu Su

Surviving under large scale CXPST-like Attack ..................................... 159
    Hongjun Liu, Xiaofeng Hu, Dan Zhao, and Xicheng Lu

Action Based Access Control Model for Multi-level Security (MLS) ............... 162
    Mang Su, Fenghua Li, Guozhen Shi, and Li Li

A Defeasible Description Logic Based Semantic Security Policy Conflict Analysis Approach ............................................................ 165
    Luokai Hu
A Faster Cryptographic Time-Memory Tradeoff .......................................................... 168
   Jung Woo Kim, Jungjoo Seo, Jin Hong, and Kunsoo Park

Output Control of Three Phase AC Power Source System with SCR Rectifier
and Linear Power Amplifier .................................................................................. 172
   Jeong-Chay Jeon, Hun Oh and In Ho Ryu

Design and Implementation of Class B Power Amplifier for 5kW AC
Power Source .................................................................................................... 175
   Jeong-Chay Jeon, Hyoung-Keun Park and Hyun Seob Cho

Development and Test of Simultaneous Power Analysis System for
Three-Phase and Four-Wire Power System ..................................................... 178
   Hun Oh, In Ho Ryu and Jeong-Chay Jeon

Robust IPSec Key Recovery Solution for IKEv2 under Mobile
and Wireless Environment ............................................................................... 181
   Yunjung Lee, Jungwon Cho, Keun-Wang Lee

Bus bar formation process was designed by multi-layer metal deposition ....... 184
   Younghun Lee, and Soobon Koo

Protection Profile for Mobile Device Management System .............................. 187
   Keunwoo Rhee, Woongryul Jeon, and Dongho Won

Text Hiding Scheme Using Big-5 Code ........................................................... 190
   Jun-Chou Chuang, Chun-Chi Lo, Yu-Chen Hu, and Piyu-Yu Tsai

Infrared Face Temperature Normalization in Fourier Domain ....................... 193
   Xie Zhihua and Zeng Jie

A Reversible Data Hiding Scheme Using Segmentation Strategy
and Histogram Adjustment ........................................................................... 197
   Yung-Chen Chou, Chun-Yi Huang, and Yu-Chen Hu

Experiments of DDoS detect using Triangle Expectation with MapReduce .... 200
   Jin-Hyun Yoon, Ho-Seok Kang, and Sung-Ryul Kim

Improving Clonal Selection Algorithm in Security Optimization ............. 203
   Tao Gong, Long Li, Changsheng Guo, and Xiaolei Gong
Research on Immunizing Embedded Linux Core Against Viruses and Software Faults ................................................................. 206
   Tao Gong and Changxing Du

Secure Gauge Control System Based on ARM and Fuzzy PI Controller ........ 209
   Tao Gong and Lei Qi

Effect Analysis of Electric Vehicle Charging to Smart Grid with Anti-Islanding Method .................................................................... 212
   Bum-Sik Shin, Kyung-Jung Lee, Sunny Ro, Young-Hun Ki and Hyun-Sik Ahn

A Modular Transform Method of Crypto Algorithm for Optimized FPGA Synthesis ........................................................................ 215
   Dongsoo Kim, Hae-Wook Choi
Abstract. To illustrate the different kinetics of cellular self-repair mechanism under external perturbations from outer environment, a mathematical model of DNA damage repair process is proposed by using the Kinetic Theory of Active Particles (KTAP) framework. The profile of cellular self-repair process is represented by two sub-populations, each of which is made up of the active particles with different discrete states. The dynamic kinetics of DNA damage generation, repair mRNA transcription, Repair Protein (RP) translation, DSBC synthesis are investigated by the particle interactions between the molecular pairs within DNA and RP sub-systems.

Keywords: Cellular self-repair, IR, DNA damage, Kinetic Theory, Modeling.

1 Introduction

Generally, a biological system consists of from a few copies to millions of different components with specific interactions. Especially, as a unit of a bio-system, a cell also consists of a large number of active molecules, such as, DNA, mRNA, protein etc. Also, a biological phenomenon can be dealt as the evolution of the dynamics of several interacting modules. Especially, in response to acute perturbations from outer environment, a cell can trigger its internal self-defense mechanism by complicated interactions between these “active particles”.

By KTAP approach, the description of bio-system essentially means defining the microscopic state of the interacting molecules and their distribution function over the active state. To further investigate cellular self-repair mechanisms under acute perturbation from outer environment, a mathematical framework is proposed by using KTAP approach at single cell level. In this framework, DNA damage and Repair Protein (RP) are dealt as two sub-systems, the dynamic processes of Double Strand Breaks (DSBs) and RP generating, DSBC-protein complexes (DSBCs) synthesizing are represented by the particle interactions between the active molecular pairs with different discrete states.
2 Method

Fig 1 is the profile of cellular self-repair mechanisms, it is composed of two populations, DNA damage and repair enzyme, each of which is composed of active particles with different microscopic active states. As acute IR is applied into a cell, DNA is broken down stochastically, and the resulting DSB occur. As a result of the particle interactions between the molecular pairs of repair gene and DSB, repair mRNA transcription is prompted, and RP translation is accelerated due to the particle interactions between repair mRNA and DSB.

Suppose RP is available around damage sites, DSBC can be synthesized after DSB combining with RP. With the cellular self-repair mechanism, most of the DSBs can be correctly fixed, and the correct repair part of DSBCs (rDSBCs) can further transfer the damage signal into downstream gene and their regulation pathways. Whereas, a little part of DSB cannot be repaired correctly, both of disrepair part of DSBCs (mDSBCs) and intact DSBs will be accumulated as a part of cellular toxins, which can seriously weaken cellular viability and self-defense capability, even lead to abnormal and cancerous finally.

3 Result

3.1 DSBs generation induced by IR

The profile of DSBs generation induced by continuous IR is shown in Fig 2. As external function of acute IR, \( g_i^{(p)} \), is applied into a cell, DNA is stochastically broken into two pieces of DSBs, each of which is dealt as a new DNA.
3.2 Repair mRNA transcription and RP translation

As shown in Fig 3, the dynamic processes of repair mRNA transcription and RP translation are prompted by particle interactions between molecular pairs of DSB and repair gene, as well as DSB and repair mRNA, respectively.

![Fig 3. Repair mRNA and RP generation process with particle interactions between the molecular pairs of DSB and repair gene, as well as DSB and repair mRNA, respectively.](image)

3.3 DSBCs synthesis kinetics

The profile of DSBC synthesis process is shown in Fig 4, in which the particle interactions between the molecular pairs of DSB and RP trigger the binding of RP into the nascent DNA ends, and then synthesize into DSBC, whereas, some DSBC being unstable state might be reversibly broken into DSB and RP again.

![Fig 4. The profile of DSBC synthesis and dis-synthesis kinetics](image)

3 Conclusion

By using the KTAP framework, a mathematical model of cellular self-repair mechanism is proposed under IR perturbations. The kinetics of DSB generation, repair mRNA transcription, RP translation, DSBC synthesis are represented by particle interactions between molecular pairs with different discrete microscopic states in the DNA and RP sub-systems. Our model is flexible and suitable for illustrate the complex interactions between molecular particles within different sub-systems, and provide a mathematical framework to investigate the dynamic kinetics of cellular self-repair mechanisms in response to IR perturbations from outsiders.
Cryptanalysis of A Robust and Efficient Smart Card Based Remote Login Mechanism for Multi-Server Architecture

Chun-Ta Li 1  Chi-Yao Weng 2,○ Chun-I Fan 2

1 Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.)
Email: th0040@mail.tut.edu.tw
2 Department of Computer Science and Engineering, National Sun Yat-sen University
70 Lienhai Road, Kaohsiung City 80424, TAIWAN (R.O.C.)
○ Corresponding author: cyweng@mail.cse.nsysu.edu.tw

Abstract. Recently, Chang and Cheng proposed a robust mechanism for smart card based remote logins in a multi-server architecture, where two kinds of participants, each login user shares a human-memorable password and adopts a smart card with a trusted registration center and each service provider shares a secret key with a trusted registration center, can construct a common session key and achieve mutual authentication between login user, service provider and trusted registration center. They claimed that their mechanism can withstand various known attacks. However, based on the security analyzes conducted by us, we find their mechanism is vulnerable against smart card lost problems, leak-of-verifier attack, and session key disclosure attack.

Keywords: Information security; Key agreement; Multi-server architecture; Password; Smart card.

1 Introduction

The more network communication technologies and application services are being developed, the more people can receive desired services through personal mobile devices anywhere and anytime. In order to frustrate illegal users’ attempts of getting the serviceable resources maintained in remote servers, two-factor (password and smart card) user authentication is the widely accepted and most adopted method in client-server architecture. However, in traditional remote login mechanisms for a multi-server architecture, a user needs to register with different service providers and remember the various identities and passwords for ensuring higher security. Therefore, single registration is the most important feature in a multi-server architecture and any user can take desired services from various network servers without repeating registration to each service provider. Password authentication with smart card is one of the mechanisms that were widely used to authenticate the validity of participants between a login user, the service providers and a trusted registration center.
In 2011, Chang and Cheng developed a more robust and efficient smart card based remote login mechanism [1] in which only lightweight one-way hash function and exclusive OR operation are required during multi-server authentication processes. Unfortunately, based on the security analyses conducted by us, Chang-Cheng’s login mechanism is still vulnerable against the smart card lost problems, leak-of-verifier attack, and session key disclosure attack. In this paper, we will demonstrate a series of steps to show how the above-mentioned attacks can be invoked on their mechanism in the presence of a malicious adversary.

2 Review of Chang-Cheng’s Mechanism

Chang-Cheng’s mechanism contains four phases: registration, login, authentication and key agreement, and password modification phase. Their’s mechanism consists of one trusted registration center (RC), service providers (SP$_j$) and login users (U$_i$). To shorten the length of this paper, we omit the review and notations explanation. Please refer to [1].

3 Attacks on Chang-Cheng’s Mechanism

Although Chang and Cheng claimed that their mechanism can resist many types of attacks and satisfy all the essential requirements for multi-server architecture authentication. However, the actual situation is not the case and the cryptanalysis of Chang-Cheng’s mechanism has been made in this section. The detailed cryptanalysis is presented as follows.

3.1 Smart Card Lost Problems

In this attack, we assume that U$_i$’s smart card is stolen by an adversary U$_a$ and the secret information ($TID_i$, $h(\cdot)$, $TPW_i$, $\sigma_i$) which is stored in the smart card can be extracted by monitoring its power consumption [2].

Off-line password guessing attack: As we know, the content of the smart card is ($TID_i = T_i||id_i, h(\cdot), TPW_i = h(pw_i), \sigma_i = H(TID_i||k) \oplus pw_i$). With this information, U$_a$ can select a guessable password $pw'_i$ and compute $h(pw'_i)$. If $h(pw'_i)$ is equal to $TPW_i$, it indicates the correct guess of U$_i$’s low-entropy password and Chang-Cheng’s mechanism cannot withstand off-line password guessing attack.

Impersonation attack: Once the adversary U$_a$ got the secret information ($TID_i$, $h(\cdot)$, $TPW_i$, $\sigma_i$) and correctly derived U$_i$’s password $pw'_i$, he/se can make a valid login request with ease. For example, U$_a$ computes $\alpha = h(\sigma_i \oplus pw'_i \oplus N_A \oplus SID_j)$ and makes a valid login message to impersonate U$_i$ by sending $\{TID_i, \alpha, N_A\}$ to the service provider SP$_j$, where $N_A$ is a nonce chosen by U$_a$. 
3.2 Leak-of-Verifier Attack

In Chang-Cheng’s mechanism, we found that their mechanism may suffer from leak-of-verifier attack and any legitimate user $U_i$ who possesses the smart card can easily derive service provider $SP_j$’s secret $h(H(SID_j||k))$ by performing the following steps:

**Step 1:** In Step 7 of authentication and key agreement phase, $U_i$ receives the response message $\{ \alpha', N_R, \gamma_U \}$ from $SP_j$.

**Step 2:** Then, $U_i$ computes $u = \gamma_U \oplus h(\sigma_i \oplus pw_i^*) = h(H(SID_j||k))||ran$ and removes $ran$ from $h(H(SID_j||k))||ran$. Finally, $U_i$ derives $SP_j$’s secret $h(H(SID_j||k))$.

3.3 Session Key Disclosure Attack

In case of $SP_j$’s secret $h(H(SID_j||k))$ is successfully derived by $U_a$, $U_a$ can use it to derive the previous and subsequent session keys which are constructed by other users and $SP_j$. We assume that some victim user $U_i$’s login message $\{TID_i, \alpha, N_U \}$, $SP_j$’s authentication message $\{TID_i, \alpha, N_U, SID_j, \beta, N_S \}$ and $RC$’s response message $\{\beta', N_R, \alpha', \gamma_S, \gamma_U \}$ are collected by $U_a$. Then, the session key disclosure attack can be launched by performing the following steps:

**Step 1:** $U_a$ eavesdrops above-mentioned messages and obtains three nonces $N_U$, $N_S$, and $N_R$ from $U_i$, $SP_j$, and $RC$, respectively.

**Step 2:** $U_a$ uses $SP_j$’s secret $h(H(SID_j||k))$ to derive $s$ by computing $s = \gamma_S \oplus h(H(SID_j||k)) = ran||h(H(TID_i||k))$.

**Step 3:** $U_a$ derives the session keys of past and future sessions by computing $SK = h((h(H(SID_j||k))||s) \oplus N_U \oplus N_S \oplus N_R)$.

4 Conclusions

In this paper, we showed that Chang and Cheng’s two-factor based multi-server authentication protocol is insecure. By adopting power analysis attacks, we found their protocol may suffer from leak-of-verifier attack and any legitimate user who possesses the smart card can easily obtain service provider’s secret and further launch a session key disclosure attack.

References


An XML based Single Sign-On Scheme for Multimedia Device Control in the Ubiquitous Home Network

Dongkyoo Shin* and Dongil Shin

Department of Computer Engineering, Sejong University
98 Gunja-Dong, Gwangjin-Gu, Seoul 143-747, Korea
{shindk, dshin}@sejong.ac.kr

Abstract. A single sign-on scheme is proposed to obtain user authentication and control a remote device through a mobile terminal in a home network running the OSGi (Open Service Gateway Initiative) service platform based on SAML (Security Assertion Markup Language). Single sign-on profile is defined to overcome the handicap of the low computing and memory capability of the mobile terminal and automated user authentication is applied to control a remote multimedia device in a home network based on the OSGi.

Keywords: single sign-on, SAML, home network, OSGi, device control

1 Introduction

In the OSGi service platform, every service bundle in the gateway operator requires user authentication. The main security problem with a home network environment based-on the OSGi service platform is that the security infrastructure is distributed and these architectures usually require that key security features be built into all parts of the system. In addition, a user must memorize usernames and passwords for each service. SSO (Single Sign-On) is a good alternative to solve these problems. SSO is a security feature that allows a user to log into the many different services offered by the distributed systems while only needing to provide authentication once, or at least always in the same way [1].

2 Background

Release 4 of the OSGi service platform defines a "User Admin Service" but only offers authentication for each service unit [2]. SSO can be implemented by exchanging and reusing a user's authentication information, including the fact that the user has previously been authenticated by a specific method among different security

*Corresponding author.
This research is supported by Seoul R&BD Program (SS110008).
domains. We specified the information in a uniform and unified way based on SAML.

In order to apply the SSO scheme to the home network, the services extended from core services provided by the OSGi framework should be developed and deployed onto the OSGi framework [3]. Figure 1 shows core services provided by the OSGi framework and extended services which we constructed.

![Fig. 1. OSGi framework and extended services](image)

SAML is an XML-based standard framework designed to offer single sign-on for both automatic and manual interactions between systems. SAML defines the request-response protocol by which systems accept or reject subjects based on assertions [4]. An assertion includes the statements generated by the SAML authority, conveying them and verifying that they are true. SAML defines three types of assertions: Authentication Assertion, Attribute Assertion, Authorization Assertion.

### 3. Single Sign-On architecture for mobile and home network service environment

![Fig. 2. Proposed Single Sign-On Scheme](image)
The concept of the proposed Single Sign-On architecture is shown in Figure 2, in which the OSGi delivers certain services offered by service providers to the end user regardless of the system environments. In our implementation, a mobile user gains access to services being managed by a gateway operator with the SAML-based information related to his own authentication in order to control a remote camera and projector. A mobile user keys in his username and password to a mobile device in order to access the Camera Control Service in the gateway operator of the Wide Area Network. This user credential information is transferred to the SSO Service through the gateway operator, which connects the mobile device and Wide Area Network.

The user authentication procedure for the architecture is presented in the form of a sequence diagram in Figure 3, where each box in the diagram denotes an entity involved in this process. Figure 3 explains the messages between entities applying a user's single sign-on among services, in which there are mutual trust relationships.

![Fig. 3. Sequence Diagram of the Proposed Single Sign-on Architecture](image)

References

3. OSGi Alliance Std., OSGi Service Platform Release 4.3, OSGi Alliance, (2011)
Breaking $H^2$-MAC using Birthday Paradox

Fanbao Liu$^{1,2}$, Tao Xie$^1$ and Changxiang Shen$^2$

$^1$ School of Computer, National University of Defense Technology, Changsha, 410073, Hunan, P. R. China
$^2$ School of Computer, Beijing University of Technology, 100124, Beijing, P. R. China
liufanbao@gmail.com

Abstract. We propose an efficient method to break $H^2$-MAC, by using a generalized birthday attack to recover the equivalent key, under the assumption that the underlying hash function is secure (collision resistance).

Keywords: $H^2$-MAC, Equivalent Key Recovery, Birthday Paradox.

1 Introduction

In ISC 2009, Yasuda proposed $H^2$-MAC [5], a variant of HMAC, which aims to remedy the drawback of HMAC and keep its advantages and security at the same time. $H^2$-MAC is defined by removing the outer key of HMAC, which is shown as follows,

$$H^2\text{-MAC}(K)(M) = H(H(K||pad||M))$$

where $K$ is an $n$-bit key, and $pad \in \{0, 1\}^{m-n}$ is a fixed constant.

$H^2$-MAC is proven to be a secure PRF (pseudorandom function) under the assumption that the underlying compression function is a PRF-AX [5].

In ISA 2011, Wang [3] proposed an equivalent key recovery attack to $H^2$-MAC instantiated with the broken MD5 [2, 4], with complexity about $2^{97}$ on-line MAC queries.

We break $H^2$-MAC by recovering its equivalent key through a generalized birthday attack with two groups. First, we get a lot of MAC values of $H^2$-MAC using different messages in group $G_1$, through on-line queries. Second, we directly compute many values of $H(H(C||pad||m))^1$, called $H^2$, in group $G_2$ through off-line, where $Cs$ and $ms$ can be both randomly generated. If the on-line queries in $G_1$ is $2^{n/2}$ and the off-line computations in $G_2$ is also $2^{n/2}$, then, there is a pair $(m, m')$ that the inner hashing part of $H^2$-MAC and $H^2$ equate with great probability [1]. Therefore, the equivalent key of $H^2$-MAC can be recovered by computing the corresponding value of $H^2$.

$^1$ The secret key of $H^2$-MAC is replaced with a constant, for example, the IV of the underlying hash function.
2 Notations

Let $H$ be a concrete hash function mapping $\{0,1\}^* \rightarrow \{0,1\}^n$. Let $IV$ be the initial chaining variable of $H$. Let $K$ denote a secret key with $n$ bits. $x||y$ denotes the concatenation of two bit strings $x$ and $y$. $|G|$ denotes the number of elements of the set $G$. $pad(M)$ denotes the padding bits of $M$ in Merkle-Damgård style. $H^2$ means that the secret key to $H^2$-MAC is replaced with a constant $C$ or a known parameter to everybody, hence, $H^2$ can be also viewed as the double application of the underlying hash function $H$.

3 Breaking $H^2$-MAC Using Birthday Paradox

We call $I_K = H(K||pad||M)$ the inner hashing of $H^2$-MAC, $Oh = H(I_K)$ the outer hashing of $H^2$-MAC, respectively.

We apply the generalized birthday attack with two groups [1] to $H^2$-MAC and then recover its equivalent key $K_e = H(K||pad||M_0)$.

We use 1-block messages $M_i$s to generate the corresponding $H^2$-MAC values, and use 1-block messages $M_j'$s to generate the corresponding $H^2$ values, where $1 \leq i, j \leq 2^{n/2}$. The overall strategy of equivalent key recovery attack to $H^2$-MAC is shown as follows.

1. Generate a group one $G_1$ with $r = |G_1| = 2^{n/2}$ elements, by computing the corresponding values of $H(H(c||M_j'))$ for $r$ different $c$s and $M_j'$s, which can be randomly generated. Specifically, $c$ can be a pre-chosen constant.
2. Generate a group two $G_2$ with $s = |G_2| = 2^{n/2}$ elements, by querying the corresponding values to $H^2$-MAC oracle with the secret key $K$ for $s$ different $M_i$s, where $M_i$s are randomly generated.
3. There is a pair $(M_i, M_j')$ that not only satisfies $H^2$-MAC$_K(M_i) = H^2(M_j')$, but also satisfies $H(K||pad||M_i) = H(c||M_j')$ (an inner collision between $H^2$ and $H^2$-MAC happens), with great probability [1].
4. Since $H(K||pad||M_i) = H(c||M_j')$, and we know the value of $c$ and $M_j'$, we can compute the value of $K_e = H(K||pad||M_i) = H(c||M_j')$.
5. Let $pad_0$ and $pad_1$ be the padding bits of $K||pad||M_i$ and $K||pad||M_i||pad_0||x$, respectively, for arbitrary message $x$. Hence, we can generate the result of $H(K||pad||M_i||pad_0||x)$ by computing $y = h(K_e, x||pad_1)$, then we compute $H(y)$ further, and we get the very value of $H^2$-MAC($K||pad||M_i||pad_0||x$), eventually.

**Complexity analysis.** The elements of group $G_1$ computed by $H^2$ need $2^{n/2}$ off-line $H^2$ computations. The elements of group $G_2$ queried through $H^2$-MAC need $2^{n/2}$ on-line $H^2$-MAC queries. The probability of that at least one inner collision happens is 0.632 [1]. We can store the values of these elements of both groups in hash tables. The above algorithm will require $O(2^{n/2})$ time and space to complete.
4 Conclusion

We can recover the equivalent key in about $2^{n/2}$ on-line queries to $H^2$-MAC and $2^{n/2}$ off-line $H^2$ computations. Our attack shows that the security of $H^2$-MAC is totally dependent on the CR of the underlying hash function, which claims that the security of $H^2$-MAC is totally broken.

Acknowledgement. We thank the anonymous reviewers for their valuable comments. This work was partially supported by the program “Core Electronic Devices, High-end General Purpose Chips and Basic Software Products” in China (No. 2010ZX01037-001-001), and supported by the 973 program of China under contract 2007CB311202, and by National Science Foundation of China through the 61070228 project.

References


Gabor Based Optimized Discriminant Locality Preserving Projection for Feature Extraction and Recognition

Xi Chen\(^1\), Jiashu Zhang\(^2\)

\(^1\) the School of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China (E-mail: xcbiometrics@126.com)
\(^2\) Si-Chuan province Key Lab of Signal and Information Processing at Southwest Jiaotong University, Chengdu, 610031, China. (E-mail: jszhang@home.swjtu.edu.cn)

Abstract: This paper proposed a Gabor based optimized discriminant locality preserving projections (ODLPP) algorithm which can directly optimize discriminant locality preserving criterion on high-dimensional Gabor feature space via simultaneous diagonalization, without any dimensionality reduction preprocessing. Experimental results conducted on the VALID face database indicate the effectiveness of the proposed algorithm.

Keywords: Optimized Discriminant Locality Preserving Projection; Gabor Feature; Face Recognition.

1 Introduction

Discriminant locality preserving projection (DLPP) [1] encodes discriminant information into the objective of locality preserving projection and can obtain better classification performance than LPP. However, DLPP suffers from “small sample problem”. To conquer such weakness of DLPP, we proposed the optimized discriminant locality preserving (ODLPP) algorithm. The proposed ODLPP directly implemented the objective of DLPP in high-dimensional space without matrix inverse, which utmostly obtain the optimal discriminant vectors for DLPP without larger computation burden. In this paper, ODLPP was used to reduce the dimensionality of high-dimensional Gabor feature vector.

The rest of this paper is organized as follows: Section 2 introduces our algorithm in detail. Experimental results are given in Section 3. Section 4 highlights the conclusions.

2 Optimized Discriminant Locality Preserving Projection in Gabor Feature Space

Given a set of training Gabor feature set \( T = \{x_1, \ldots, x_N\} \), where \( x_i \) denotes an \( n \)-
dimensional Gabor feature column vector and \( N \) is the number of samples. Each Gabor feature vector \( x_i \) belongs to one of the \( C \) classes \( \{ X_1, X_2, \ldots X_C \} \), where \( X_i = \{ x_i^1, x_i^2, \ldots x_i^N \} \), \( (i = 1, 2, \ldots, C) \). DLPP tries to maximize an objective function as follows \([1]\):

\[
J(A) = \frac{A^T F H F^T A}{A^T X L X^T A}
\]

where \( L \) and \( H \) are within-class Laplacian matrices and between-class Laplacian matrices, respectively. \( X = [x_1, x_2, \ldots, x_N] \). As the dimension of sample is always larger than the number of sample, \( X L X^T \) is always singular and is nonreversible, ODLPP simultaneously diagonalize \( X L X^T \) and \( F H F^T \) to obtain the projection subspace without matrix inverse. Four steps were included in our proposed ODLPP which are presented as follows \([2]\):

**Step 1.** Diagonalization of \( F H F^T \). To find a matrix \( V \in R^{n \times n} \) such that \( V^T (F H F^T) V = \Delta \), where \( V^T V = I \) and \( \Delta \) is a diagonal matrix whose elements are ordered in decreasing order. Matrix \( V \) is formed by the eigenvectors of \( F H F^T \). Suppose the rank of \( F H F^T \) is \( P \), there should exist \( P \) nonzero eigenvalues. Let \( Y \) be the \( P \) first columns of \( V \), then we can write \( Y^T (F H F^T) Y = \text{Diag}_H > 0 \), where \( \text{Diag}_H \) corresponds to the main \( P \times P \) submatrix of matrix \( \Delta \) and it is a positive definite diagonal matrix, without zero elements on its diagonal.

**Step 2.** Let \( Z \) be defined as \( Y \text{Diag}_H^{1/2} \) with \( Z \in R^{n \times P} \). Clearly,

\[
(Y \text{Diag}_H^{1/2})^T (F H F^T) (Y \text{Diag}_H^{1/2}) = I_P
\]

then \( Z^T (F H F^T) Z = I_P \). Matrix \( Z \) diagonalizes \( F H F^T \) and reduces its dimension from \( n \times n \) to \( P \times P \).

**Step 3.** Diagonalization of \( Z^T (X L X^T) Z \). To find a matrix \( U \in R^{P \times P} \) such that \( U^T Z^T (X L X^T) Z U = \text{Diag}_L \) with \( U^T U = I \). Again it is possible to find \( \text{Diag}_L \in R^{P \times P} \) and \( U \) through an eigenvalue eigenvector analysis of matrix \( Z^T (X L X^T) Z \).

**Step 4.** Let \( A \) be defined as \( A = U^T Z^T \), with \( A \in R^{P \times n} \). It’s clear that matrix \( A \) can simultaneously diagonalize \( F H F^T \) and \( X L X^T \). \( A \) corresponds to the matrix formed by the eigenvectors associated with the \( P \) nonzero eigenvalues of \( (X L X^T)^{-1} (F H F^T) \). \( A \) is also the solution of our proposed ODLPP.

### 3 Experimental Evaluation

In this section, we experimentally evaluate results and discussions on the proposed scheme for Gabor based face recognition on the VALID face database. Images of three persons are shown in Fig.1. We randomly choose the training samples and
record the minimal error rate. We repeat the procedure 10 times and record the mean minimal error recognition rate and standard deviation on table 1. Experimental results on these databases show mean minimal error recognition rate of Gabor based ODLPP is lowest than the others with different number of training samples.

| Table 1. Mean Minimal Error Recognition Rate (%) and Standard Deviation on the Finger Vein And Valid Database
<table>
<thead>
<tr>
<th>#class</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gabor-LPP</td>
<td>20.5±1.2</td>
<td>27.4±2.5</td>
<td>18.2±3.4</td>
<td>15.8±2.2</td>
</tr>
<tr>
<td>Gabor-ODLPP</td>
<td>18.3±1.7</td>
<td>17.3±2.2</td>
<td>14.6±2.3</td>
<td>12.5±1.9</td>
</tr>
<tr>
<td>Gabor-GLPP</td>
<td>17.4±2.3</td>
<td>15.7±2.1</td>
<td>11.2±2.0</td>
<td>12.5±2.1</td>
</tr>
<tr>
<td>Gabor-OLPP</td>
<td>16.7±1.8</td>
<td>14.5±2.1</td>
<td>12.7±1.9</td>
<td>11.4±2.1</td>
</tr>
<tr>
<td>Gabor-OLP</td>
<td>11.2±1.7</td>
<td>10.3±2.1</td>
<td>7.4±2.4</td>
<td>6.8±2.3</td>
</tr>
</tbody>
</table>

Fig. 1 the preprocessed sample images of three subjects from VALID face database

4 Conclusion

In this paper, ODLPP directly optimizes discriminant locality preserving criterion on the Gabor feature space via simultaneous diagonalization without any dimensionality reduction preprocessing. Experiments show superior performance of our proposed technique on feature extraction and classification.

Acknowledgments. This paper is supported by the Doctor's Launching Project of Kunming University of Science and Technology.

References

A Quantum Mechanical Meet-in-the-middle Attack Against NTRU

Zhijian Xiong¹, Jinshuang Wang¹, Yanbo Wang², Tao Zhang¹, Liang Chen²

¹ Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China
² Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China
küperain@sina.com

Abstract. We proposed a quantum mechanical meet-in-the-middle attack method against NTRU. Our method managed to combine the advantages of Meet-in-the-middle attack and the Grover quantum searching algorithm. Our evaluation reveals that the time complexity dropped dramatically comparing with classical meet-in-the-middle attacks. Our method also decreases time complexity comparing with Wang’s attacking algorithm dramatically. Main variants of NTRU were also studied.

Keywords: NTRU, meet-in-the-middle attack, Grover search, quantum attack

1 Introduction


Based on the above observations, we proposed a quantum mechanical meet-in-the-middle attack against NTRU accordingly, which is better than the above methods according to our evaluation.

2 A Quantum MITM Attack Against NTRU

Meet-in-the-middle attack is the most effective method against NTRU at present, though the time complexity is still very large. Wang’s method can be seen as a quantum brute-force search, which reduced the time complexity from $O(C_N^{d_p})$ to
It is attractive to combine the quantum computation with meet-in-the-middle attack, we managed to provide such a method.

2.1 Algorithm Describe

Without loss of generality, we assumed: (1) private key \( f \in B(d) \); (2) \( N \) and \( d \) are even; (3) The bin which contains polynomial \( f_1 \) will be labeled as \( \text{label}_{f_1} \), and \( \text{bin}(f_1) = \{\text{label}_{f_1}\} \); (4) \( \text{bin}(f_2) = \{\text{label}_{f_2}\} \);

The basic idea of quantum meet-in-the-middle attack against NTRU is:

1. Compute all \( \{\text{label}_{f_1}, f_1\} \) and arranged as a table \( L \) indexed by \( \text{label}_{f_1} \);
2. Search \( f_2 \) with the Grover search algorithm, with \( \text{label}_{f_1} \in \text{bin}(f_2) \), and \((f_1 + f_2)^* h(\text{mod} \; q) \in \{0,1\}^N \);
3. Search \( f_1 \) correspond to \( \text{label}_{f_1} \) in \( L \);
4. Verifies \( f_1 + f_2 \) with other conditions.

The detail of searching \( f_2 \) based on Grover algorithm is:

1. Compute the maximum label value \( C_{dN/2+1}^{d/2} \), let \( n = \log_2 C_{dN/2+1}^{d/2} \).
2. Initialize the quantum system with \( |0\rangle^\otimes n \otimes |0\rangle \). Apply Hadamard transform \( H^{\otimes n} \) to the first register to produce the equally-weighted superposition state \( |s\rangle \).

\[
|s\rangle = H^{\otimes n} |0\rangle^\otimes n = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}-1} |x\rangle
\]

(3) Oracle details: \( F_{f_2} : B(d_2 / 2) \rightarrow \{0,1\} \), where:

\[
F_{f_2} = \begin{cases} 
1, \exists \text{label}_{f_1} \in \text{bin}(f_2), (f_1 + f_2)^* h(\text{mod} \; q) \in \{0,1\}^N. \\
0, \text{others}
\end{cases}
\]

(4) Apply Grover algorithm \( \frac{\pi}{4} 2^{n/2} \) times. There are two operations performed in Grover iteration:

1. Apply the Oracle;
2. Apply the unitary operator \( I_\phi = 2|\phi\rangle\langle\phi| - I \) on the superposition state \( |s\rangle \), note \( \phi = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}-1} |x\rangle \).

(5) Measure the first register, and return \( f_2 \).

2.2 Algorithm Evaluation

Oracle is a simple judging function, therefore the time complexity of Grover quantum searching algorithm only depends on the iterative times. The time complexity of
NTRU quantum meet-in-the-middle attack is \( O(\sqrt[4]{C_{N/2+1}^{d/2}}) \). The table \( L \) needs to be saved, which is similar to meet-in-the-middle attack, so the space complexity is \( O\left(\frac{C_{N/2}^{d/2}}{N}\right) \). A detailed comparison was given in Table 1.

Table 1. Time and space complexity comparison for different NTRU attacks

<table>
<thead>
<tr>
<th></th>
<th>Brute-force</th>
<th>MITM Attack</th>
<th>Wang’s attack</th>
<th>Quantum MITM attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time complexity</strong></td>
<td>( O(C_N^d) )</td>
<td>( O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}) )</td>
<td>( O(\sqrt[4]{C_{N/2+1}^{d/2}}) )</td>
<td>( O(\sqrt[4]{C_{N/2+1}^{d/2}}) )</td>
</tr>
<tr>
<td><strong>Space complexity</strong></td>
<td>( O(1) )</td>
<td>( O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}) )</td>
<td>( O(1) )</td>
<td>( O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}) )</td>
</tr>
</tbody>
</table>

3 Conclusions

Quantum computation strongly influenced cryptography. Combining Meet-in-the-middle attack and the Grover quantum searching algorithm, this paper proposed a quantum meet-in-the-middle attack method against NTRU. Our evaluation reveals that our time complexity \( O(\sqrt[4]{C_{N/2+1}^{d/2}}) \) dropped dramatically comparing with classical meet-in-the-middle attacks’ \( O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}) \), with the same space complexity. Our method also improves time complexity comparing with Wang’s attacking algorithm dramatically, with the cost of space complexity.

References

The Effect of Chunk-Based Jitter Management Algorithm on IP Packet Size

Ikram Ud Din, Noor ul Amin, Arif Iqbal,

Department of Information Technology, Hazara University, Mansehra, Pakistan
Ikramuddin205@yahoo.com, namin@hu.edu.pk, arifiqbalumar@yahoo.com

Abstract. In this paper, the end-to-end delay and variation in delay (jitter) in the network have been examined using OPNET Modeler 14.0. We have analyzed performance of the network in case of receiving and sending video and voice packets. The Chunk-based Jitter Management (CJM) algorithm is applied on the buffer at the receiver side which divides the incoming packets into same size chunks. It was found that if the packet size is constant (576 bytes) then the end-to-end delay and jitter is high, but if we reduce the packet size from 576 to 256 bytes, the performance is significantly improved. The performance metrics used in this work are: jitter and end-to-end delay. The simulation results show that both stable video and voice quality and transmission efficiency is achieved.

Keywords: IP Packet CJM, Jitter, Delay, Buffer.

1 Introduction

The Internet provides many services. The people retrieve and exchange information through it. Voice over Internet Protocol (VoIP) is the most widely used and popular service. Real time applications such as video conferencing and VoIP are the recent applications used widely. VoIP allows the users to communicate freely at low cost with each other. This feature becomes popularity of the VoIP. A variety of network impairments such as end-to-end delay, jitter, and packet loss drastically degrade network quality. This work focuses on end-to-end delay and jitter, which are the critical problems to be addressed. The required quality of service (QoS) of promising real time applications cannot be satisfied by the existing Internet service. Composition of several building blocks makes VoIP application. The voice signals are periodically sampled by the encoder at sender side, and then the voice packets are decoded at the destination end. Before playout of these packets, they are stored in the buffer for a while [1]. In playout buffer, the voice or video packets are enforced to be decoded at the same interval at which they were encoded at the source end. If the packets arrive after its expected time, then the buffer may reorder or even drop them [2], [3].
2 Materials and Methods

In Fig. 1, we have established a network between two cities of Pakistan (i.e., Karachi and Lahore). The network has two servers i.e., video and VoIP, and two clients which are: video and VoIP clients. The distribution of the clients and servers are at two different sites, i.e., the clients are located at site Karachi (in this case) and the servers at the other site (say Lahore).

Using OPNET Modeler 14.0, the two networks were tested in this study, which were sending and/or receiving both voice and video packets of different sizes, i.e., 576 and 256 bytes. The scenario was simulated for 10 minutes. The networks were named as Packet_Size_576_Bytes and Packet_Size_256_Bytes.

3 Conclusion

In this paper, we tested a network with a scalable and fast algorithm using OPNET Modeler 14.0. In particular, we proposed a Chunk-based Jitter Management (CJM) algorithm to minimize the problem of delay and jitter in the transmission of real time applications. We proved the efficiency of our algorithm via extensive simulations. The proposed algorithm improves the performance of IP networks in the transmission of real time data. In the future, we will study how to extend the framework for Wireless networks.
References


On Security of A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment

Cheng-Chi Lee¹,² Yan-Ming Lai¹ Chun-Ta Li³,*

¹Department of Library and Information Science, Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City, Taipei County 24205, Taiwan, R.O.C.
e-mail: ccllee@mail.fju.edu.tw

²Department of Photonics and Communication Engineering, Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C.
e-mail: ccllee@asia.edu.tw

³Department of Information Management, Tainan University of Technology
529 Jhong Jheng Road, Tainan 710, Taiwan, ROC
*e-mail: th0040@mail.tut.edu.tw

Abstract. Recently, user authentication scheme is becoming an important issue in the public Internet environment. There are so many information exchanges on the network every day, and there will be more in the future. There are also a lot of services being provided while network is developing, such as webmail, online bank, and cloud computing. When a user wants to use the network services, he/she must log on to a server and the server needs to authenticate the user. Therefore, user must remember his/her identity and password for each different server. As a result, the user has to memorize more and more passwords as he/she registers at a different server in order to access more services. In 2011, Lee et al. proposed a scheme for this issue. They claimed their scheme can remedy the weaknesses of prior schemes and is thus more effective. However, we find Lee et al.’s scheme still fails to achieve the anonymity and has the security weakness of a smart card clone.

Keywords: Anonymous, authentication, dynamic ID, multi-server, key agreement.

1 Introduction

Today, network services are a popular issue, because increasingly more services are being provided. When we want to access information or ask something from the server, first we need to log on to the server. Therefore, we need an authentication scheme for network servers to authenticate the legitimate users. However, the Internet now is a public environment, anyone can intercept messages of communication between users and servers from the Internet. In order to protect users' secrets, schemes related to maintaining the security of user authentication is becoming more and more important nowadays.

In 2004, Das et al. proposed a dynamic ID-based scheme to solve user tracking problems [1]. However, in 2005, Liao et al. pointed out that Das et al.’s scheme cannot protect against guessing attacks and achieve mutual authentication [4]. In 2009,
Liao and Wang proposed a new authentication scheme with anonymity for a multi-server [5]. Their scheme only uses one way hash functions to improve efficiency. But Hsiang and Shih pointed out Liao and Wang’s scheme cannot withstand insider attacks, masquerade attacks, server spoofing attacks, and registration center spoofing attacks in the same year [2]. To overcome the weaknesses of Liao and Wang’s scheme, Hsiang and Shih proposed their scheme. Nevertheless, in 2011, Lee et al. found Hsiang and Shih's scheme still could not overcome masquerade attacks, and server spoofing attacks [3]. In addition, they proposed an improved scheme to solve the weaknesses of Hsiang and Shih’s scheme. Lee et al.’s scheme let registration center share a secret value with a legal server to compute the legal user's secret value. In their paper, they claimed their scheme is practicable in the future. However, we find Lee et al.’s still scheme fails to achieve the anonymity and has security weakness of a smart card clone.

2 Review of Lee et al.'s scheme

In this section, we will review the Lee et al.’s scheme. Three roles participate in this scheme: the registration center (RC), the remote server (S), and the User (U). The RC chooses a master key $x$ and secret value $y$ to compute $h(x||y)$ and $h(y)$. After that, RC shares $h(y)$ to registered server (S). User (U) registers at RC and login S, which registers at the same RC, to access resources. The scheme is divided into four phases: registration phase, login phase, verification phase, and password change phase. To shorten the length of this paper, we omit the review. Please refer to [3].

3 Cryptanalysis of Lee et al.'s scheme

In this section, we will show the weaknesses of Lee et al.’s scheme that fails to achieve the necessary anonymity, and the situation is a high-risk when the information of the smart card is disclosed. In addition, their mechanism for changing a password is not really friendly. We will assume that the communication between $U$ and $S$ is eavesdropped on by an adversary $Z$, and explain how the adversary $Z$ can attack Lee et al.’s scheme.

3.1 Fails to achieve the anonymity

When a legal user $U_i$ wants to access roaming services from server $S_j$, he/she must send $\{CID_i, P_{ij}, Q_i, N_i\}$ to $S_j$. If the adversary $Z$ is another legal user who registers at the same RC with $U_i$, $Z$ can derive a unique value of $U_i$ and trace $U_i$ by the value at this moment. Because $Z$ registered at the same RC with $U_i$, he/she also has the value $h(y)$. After intercepting $\{CID_i, P_{ij}, Q_i, N_i\}$, $Z$ can compute

$$T_i = P_{ij} \oplus h(h(y)||N_i)||SID_j)$$
$$A_i = h(T_i||h(y)||N_i)$$
$$h(b \oplus PW_i) = CID_i \oplus h(T_i||A_i||N_i)$$
Because the unique value $h(b \oplus PW_i)$ of $U_i$ doesn’t change frequently, $Z$ can trace $U_i$ by this unique value. For this reason, we can know that Lee et al.’s scheme fails to achieve the really anonymity.

### 3.2 Smart card clone

In Lee et al.’s scheme, the security is based on the secure value $B_i$. In both user authentication or session key establishment, $B_i$ always plays an important role. However, this important value is not stored securely in the smart card. If the adversary $Z$ is another legal user who registers at the same $RC$ with $U_i$ and if he/she temporarily possesses the smart card of $U_i$, $Z$ can easily obtain $B_i$ and uses it to attack the system, such as by re-establishing the session key $SK$, which is established by $B_i$, $N_i$, $N_j$, $A_i$, and $SID_j$ to decrypt those cipher-text. Because $\{N_i, N_j, SID_j\}$ can be intercepted from the public network environment, and as $A_i$ can be derived as section 3.1 mentioned, $Z$ can implement a man-in-the-middle attack and masquerade an attack as follows.

### 3.3 Man-in-the-middle attack

If $Z$ obtains $B_i$, $Z$ can execute a man-in-the-middle attack with processes as follows.

- **Step ZV1:** $Z$ intercepts $\{CID_i, P_{ij}, Q_i, N_i\}$ and computes $\{T_i, A_i, h(b \oplus PW_i)\}.
  
  \[
  T_i = P_{ij} \oplus h(h(y)||N_i||SID_j)
  \]
  
  \[
  A_i = h(T_i||h(y)||N_i)
  \]

  \[
  h(b \oplus PW_i) = CID_i \oplus h(T_i||A_i||N_i)
  \]

- **Step ZV2:** After $Z$ obtains $\{T_i, A_i, h(b \oplus PW_i)\}$, $Z$ chooses a random number $N_{zi}$ and computes $\{CID_{zi}, P_{zi}, Q_{zi}, N_{zi}\}$.
  
  \[
  A_{zi} = h(T_i||h(y)||N_{zi})
  \]
  
  \[
  CID_{zi} = h(b \oplus PW_i) \oplus h(T_i||A_{zi}||N_{zi})
  \]
  
  \[
  P_{zi} = T_i \oplus h(h(y)||N_{zi}||SID_j)
  \]
  
  \[
  Q_{zi} = h(B_i||A_{zi}||N_{zi})
  \]

  And then, $Z$ sends $\{CID_{zi}, P_{zi}, Q_{zi}, N_{zi}\}$ to $S_j$.

- **Step ZV3:** After $S_j$ returns $\{M'_{ij}, N_j\}$, $Z$ also intercepts the data and computes both $M''_{zi} = h(B_i||N_{zi}||A_{zi}||SID_j)$ and the session key $SK_{zi} = h(B_i||N_{zi}||A_{zi}||SID_j)$.

- **Step ZV4:** $Z$ randomly chooses a number $N_{zj}$ and intercepts the data and computes both $M''_{zj} = h(B_j||N_{zj}||A_j||SID_j)$ and the session key $SK_{zj} = h(B_j||N_{zj}||A_j||SID_j)$. Finally, $Z$ sends $M''_{zj}$ to $S_j$ and sends $M''_{zj}$ to $U_i$ individually.

Because $Z$ has the secret value $B_j$, he/she can establish session $\{SK_{zj}, SK_{zi}\}$ with $S_j$ and $U_i$ individually, and then $Z$ can eavesdrop or alter the communication between $U_i$ and $S_j$. 

- 24 -
4 Conclusion

In this article, we found that the Lee et al.'s secure dynamic ID based remote user authentication scheme is vulnerable to some security weaknesses for multi-server environment. Their scheme fails to achieve the anonymity and has the security weakness of a smart card clone. In the future, these security weaknesses should be considered for multi-server environment.

Acknowledgments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 100-2221-E-030-015 and NSC 100-2221-E-165-002.

Reference

Attack on Fully Homomorphic Encryption over Principal Ideal Lattice

Gu Chun-sheng\textsuperscript{1,2} Gu Ji-xing\textsuperscript{3}

\textsuperscript{1} School of Computer Engineering, Jiangsu Teachers University of Technology, China Changzhou 213001
\textsuperscript{2} School of Computer Science and Technology, University of Science and Technology of China, China Hefei 230027
\textsuperscript{3} Institute of Image Communication & Information Processing, Shanghai Jiaotong University, China Shanghai 200240

guchunsheng@gmail.com

Abstract. For the fully homomorphic encryption schemes in [3, 6], this paper presents attacks to solve an equivalent secret key and directly recover plaintext from ciphertext for lattice dimensions \(n=2048\) by using lattice reduction algorithm. Suppose the average-case behavior of LLL in [8] is true, then their schemes are also not secure for \(n=8192\).

Keywords: Fully Homomorphic Encryption, Cryptanalysis, Principal Ideal Lattice, Lattice Reduction

1 Introduction

Rivest, Adleman and Dertouzos [1] first presented the concept of homomorphic encryption, which has many applications in cryptography. But until 2009, Gentry [2] constructed the first fully homomorphic encryptions based on ideal lattice, all previous schemes are insecure. After the scheme of [2], Smart and Vercauteren [3] presented an optimizing FHE with smaller ciphertext and key by using principal ideal lattice. Dijk, Gentry, Halevi, and Vaikuntanathan [4] proposed a simple fully homomorphic encryption scheme over the integers, whose security depends on the hardness of solving approximate GCD over the integers. Stehle and Steinfield [5] improved Gentry's fully homomorphic scheme and obtained to a faster fully homomorphic scheme. Similar to [3], Gentry and Halevi [6] implemented Gentry’s scheme by applying principal ideal lattice. The security of FHE’s in [3, 6] depends on the hardness assumption of finding small principal ideal lattice, given its HNF form or two elements form. This paper will present two lattice attacks for FHE’s in [3, 6].

By using block lattice reduction algorithm [7], we solve an equivalent secret key for \(n=2048\) of FHE’s in [3, 6]. Suppose the average case behavior of LLL [8], then the ratio \(\frac{\mu}{\lambda(L)}\) is about \((1.02)^{\ast}\), i.e. \(\mu \lesssim (1.02)^{\ast} \lambda(L) \ll 2^{380} \lambda(L)\) for \(n=8192\), where 380 is the bit-size of the coefficients in the generator polynomial of [6]. So, our first result shows the FHE’s in [3, 6] are not secure for \(n=8192\).
2 Preliminaries

Let $n$ be security parameter, $[n]=\{0,1,...,n\}$ . Let $R$ be a ring of integer polynomials modulo $f_n(x)$, i.e., $R=\mathbb{Z}[x]/f(x)$, where $f_n(x)$ is an irreducible polynomial of degree $n$ over the integers. Let $R_p$ denote the polynomial ring $\mathbb{Z}_p[x]/f(x)$ over modulo $p$. For $\forall u \in R$, we denote by $\|u\|$ the infinity norm of $u$, $u=[u_0,...,u_{n-1}]$ the coefficient vector of $u$, $\bar{u}$ the polynomial of $u$’s coefficients modulo 2.

Theorem 2.1 (Theorem 2.6 [10]) Every block $2k$-reduced basis $b_1,...,b_m$ of lattice $L$ satisfies $\|h\| \leq \sqrt{\frac{n^4}{\lambda_k}} \lambda(L)$, where $\lambda_k$ is another lattice constant using in Schnorr’s algorithm analysis.

Theorem 2.2 (Theorem 2.3 [7]) For all $k \geq 2$, Schnorr’s constant $\lambda_k$ satisfies: $k/12 \leq \lambda_k \leq (1+k/2)^{2n+4/k}$. Asymptotically it satisfies $\lambda_k \leq 0.1 \times k^{2n+4/k}$. In particular, $\lambda_k \geq k^{1/4}$ for all $k \leq 100$.

Theorem 2.3 ([8]). Suppose the average case behavior of LLL is true, then the first vector $b_1$ of LLL is satisfied to $\|b_1\|/\lambda(L) \approx (1.02)^n$ on the average for lattice $L$.

3 Attack on Smart-Vercauteren’s FHE

Theorem 3.1. Given a principal ideal $\pi$ in either two element $(p,\alpha)$ or HNF representation, there is a polynomial time algorithm which finds $w(x)=\delta(x)\times v(x)$ over $\mathbb{Z}_p$ such that $\|\delta(x)\| \leq \sqrt{n}(4/3)^{3n-4/2} \beta_k^{\text{poly}(4)}$.

Proof. Since $\alpha$ is a root of $f_n(x)=x^n+1$ over modulo $p$, so $x^n+1=(x-\alpha)g(x) \mod p$. It is easy to verify $g(x)=(x^3)(x)\mod p$. Assume $g(x)=x^n+g_{n-2}x^{n-2}+\cdots+g_0$. One constructs the following lattice $M$.

\[
M = \begin{pmatrix}
g_0 & g_1 & \cdots & g_{n-2} & 1 \\
-1 & g_0 & \cdots & g_{n-3} & g_{n-2} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
-g_1 & -g_2 & \cdots & -1 & g_0 \\
p & 0 & \cdots & 0 & 0 \\
0 & p & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & p
\end{pmatrix}.
\]

To reduce lattice $M$, one calls the lattice reduction algorithm in [7,10]. By Theorem 2.1, 2.2, one gets $w(x)=\delta(x)\times v(x)$ such that $\|\delta(x)\| \leq \sqrt{n}(4/3)^{3n-4/2} \beta_k^{\text{poly}(4)}$. Recall that $w(x) \in R$ since $u(x)\times v(x) = p \mod f_n(x)$.

When $n=2048$, $k=16$ and $\eta=298$, $\sqrt{(4/3)^{3n-4/2} \beta_k^{\text{poly}(4)}} < 2^{n+12}$. Hence, if $\|w(x)\times C(x)\| < p/2$, then one can correctly recover the bit in a ciphertext.
4 Attack on Gentry-Halevi’s FHE

By the decryption algorithm in [6], a ciphertext vector is \( \hat{c} = (c,0,...,0) \). Hence, \([\hat{c} \times \text{Rot}(v)]_p = [(\hat{c} v_0, v_1,..., v_{n-1})_p = ([c v_0]_p, [c v_1]_p, ..., [c v_{n-1}]_p)_p \). On the other hand, we have \([\hat{c} \times \text{Rot}(v)]_p = [\hat{a} \times \text{Rot}(v)]_p = \hat{a} \times \text{Rot}(v) / p \), where \([\cdot]\) is fractional part, and \( \hat{a} = 2\hat{r} + b\hat{v} \) with small vectors \( \hat{r} \) and \( \hat{v} = (1,0,...,0) \). So, \([\hat{c} \times \text{Rot}(v)]_p = \hat{a} \times \text{Rot}(v) = 2\hat{r} \times \text{Rot}(v) + b\hat{v} \). That is, \(([c v_0]_p, [c v_1]_p, ..., [c v_{n-1}]_p)_p = b\hat{v} \mod 2 \) for any decryptable ciphertext \( c \).

We apply the same method in Section 3, which finds a small multiple \( w(x) = \delta(x) \times \nu(x) \) of the secret key \( \nu(x) \). When all the entries of \( \hat{a} \times \text{Rot}(w(x)) \) are less than \( p / 2 \), we may recover the message bit in a ciphertext \( c \) as follows: \( b = 1 \) if \(([c w_0]_p, [c w_1]_p, ..., [c w_{n-1}]_p)_p = \hat{w} \mod 2 \), otherwise \( b = 0 \). Thus, we finds \( w(x) = \delta(x) \times \nu(x) \) over \( \square(x) \) with \( \|\delta(x)\| \leq \sqrt{\frac{\log(4/3)}{\eta^{1/3-\epsilon}}} \beta_h^{n2L-1} \) by Theorem 3.1.

When \( n = 2048, k = 16 \) and \( \eta = 380 \), we can recover the message bit in a ciphertext by the above method. Furthermore, we can also recover the message bit in a ciphertext for \( n = 8196, \eta = 380 \) by Theorem 2.3.

Reference

Combining Multi-Independent Algorithms for Human Face Recognition

Wenkai Xu, Eung Joo Lee
Department of Information & Communications Engineering, Tongmyong University, Busan, Korea
xwk6298@hotmail.com, ejlee@tu.ac.kr

Abstract. During the past 30 years, many different face-recognition techniques have been proposed, motivated by the increased number of real-world applications requiring the recognition of human faces. In this paper, a combination methodology of Discrete Cosine Transform (DCT) and an improved D-LDA and Neural Networks was proposed. After calculating the eigenvectors and a new Fisher’s criterion using improved D-LDA algorithm we proposed, the projection vectors are calculated for the training set and then used to train the neural networks for human identity. The experimental results on ORL face database show that this combined method has well performance.

Keywords: Face recognition, DCT, D-LDA, BPNNs

1 Introduction

In the past decades, many different face-recognition techniques have been proposed, motivated by the increased number of real-world applications requiring the recognition of human faces. PCA algorithm is known as Eigen face method; In PCA method the images are projected onto the facial value so called eigenspace [1] and [2]. PCA approach reduces the dimension of the data by means of basic data compression method [3] and reveals the most effective low dimensional structure of facial patterns [4]. LFA method of recognition is based on the analysis the face in terms of local features e.g. eye, nose etc. by what is referred LFA kernels. Recognition by Neural Network [5] and [6] are based on learning of the faces in an “Example Set” by the machine in the “Training Phase” and carrying out recognition in the “Generalization Phase”. Support Vector Machines (SVM) technique is in fact one of the binary classification methods. The support vectors consist of a small subset of training data extracted by the algorithm given in [7]. Face recognition based on template matching represents a face in terms of a template consisting of several enclosing masks the projecting features e.g. the mouth, the eyes and the nose [8]. In [9], a face detection method based on half face-template is discussed.
2 Improved D-LDA algorithm for feature extraction in DCT domain

DCT own fast Fourier Transform algorithm (FFT), as great speed advantage than K-L transform. Based on the theory above, we implement the original face image with DCT before the extraction of face feature. As figure 1(b) show us, we only reserve the part of DCT coefficient on the top-left corner to reduce dimensions, it can concentrate the energy and overcome the shortcomings of missing useful information in \( \mathbb{S}_W \) null space indirectly when wiping off \( \mathbb{S}_B \) null space using LDA at next step.

There is a problem in D-LDA algorithm: its optimization criteria are not directly related to the classification accuracy, as well as traditional LDA algorithm. Because the edge class plays a leading role which decomposes to the characteristic, it leads to dimension reduction matrix emphases the class excessively which has been classed well, thereby to make the others classes overlapped. To this problem, we redefine the within-class scatter matrix and the between-class scatter matrix of the sample.

3 Face recognition based on neural networks

In this paper, we construct integrated BP neural networks to identify face. The core of integrated networks design is dividing K categories into 2-category problems. This construction can swift one complex problems into several easy questions and the modules in integrated networks are mutual parallel connection and each is in charge of one mode identify. According to this idea, we design a kind of integrated sorter composed by several BP networks. Namely, we integrate K multi-input and single-output BP networks and one BP networks is one sub networks charging one mode class in K categories.

4 Conclusion

In this paper, a combination methodology of Discrete Cosine Transform (DCT) and an improved LDA and integrated BPNNs was proposed. The method based on DCT can compress the information of original signal efficiently; Furthermore, the improved D-LDA algorithm we proposed can withhold useful information and restrain the effect of edge class preferable through redefining the within-class scatter matrix and between-class scatter matrix, enhance the recognition rate by reducing dimension, and it can solve the small sample size problem without losing useful information. After that, the projection vectors are calculated for the training set and then used to train the neural networks for human identity.

We performed our experiments with the standard ORL face database. Experimentally, we find that the methodology we proposed which based on combination multi-algorithm provide better results than the corresponding individual algorithms.
Acknowledgement. This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the IT/SW NHN Program supervised by the NIPA (National IT Industry Promotion Agency)’’ (NIPA-2011-C1820-1102-0010).

Reference

Robustness of Regional Internet to both Random and Targeted Attacks

Ye Xu¹, Zhuo Wang¹

¹ College of Information Science and Engineering, Shenyang Ligong University, Shenyang China
{xuy.mail@gmail.com, zhuowang@163.com}

Abstract. To study the robustness of Internet to random and targeted attacks, we set up various simulation environments and found that Internet is to some extent having the performances of highly resistance to random attacks and great fragilities to intentional attacks. And in hybrid attack situations, we found that Internet is fragile no matter what ratio of intentional attacks over the random ones is.

Keywords: Internet; robustness; random attacks; targeted attacks.

1 Introduction

Recently, plenty of research interests are found in studies of the resilience of scale-free network to random attacks or to targeted attacks on the highest degree nodes. Studies to scale-free networks [1-3] have found its specific properties against attacks under both random and intentional conditions. Hybrid attacks, however, is not studied. On this ground, again, we start Internet robustness studies to hybrid attacks.

2 Robustness Evaluations to Attacks

We control attacks types by variable of attack degree $t$. $t=1$ means a complete random attack occurs. We control the network load by variable of network load ratio $w$. Network load ratio $w=0$ means the network is empty loaded[4-5]. We set $N$ as the number of the overall nodes in the target networks, and $N'$ is the node size of the largest connected graph after removing fractions $p$ nodes by hybrid attacks. Then we set $G=N/N'$ to evaluate the collapse level of the network.

2.1 Simulation of network under hybrid attacks

First experiment of hybrid attacks against the targeted networks is performed. In the experiments, we set $N=4000$, meaning that there are 4000 nodes in the networks.
We set \( t \) to \([0, 0.1, 0.2, \ldots, 1]\), representing hybrid attacks from completely intentional attacks (\( t=0 \)) to totally random attacks (\( t=1 \)). Besides, we set \( w \) to \([0, 0.1, 0.2, \ldots, 1]\), representing various workload of the networks. The reason to construct networks with different load under hybrid attacks is that we are trying to simulate the real world attacks on Internet, as well as to get profound explanations of the relationship between the network robustness and the load of the same networks. Some of the experiment results are as follows.

Fig. 1. Collapse of the networks with different network load under hybrid attacks. The attacks range from completely target attacks at \( t=0 \) to totally random attacks at \( t=1 \). The attacks with \( t \) not equals to 0 or 1 are those hybrid attacks.

From Fig. 1, we find that Internet shows highly robustness against completely random attacks and is rather fragile to intentional attacks. This is quite consistent to what was found in studies of scale-free networks. The reason is that both Internet and scale-free networks have obvious power-law distributions properties, i.e., some nodes in the networks have large quantity of connections to others whereas the most nodes have relatively very few links shown as having low degrees. The target attacks over the high degree node certainly will result in large extent collapse of whole networks.

What surprises us most, however, is that Internet is also quite fragile to hybrid attacks no matter what ratio of intentional attacks over the random ones (almost in the level of that of completely intentional attacks). Which means although there might be minor target attacks, the effect over the networks robustness is quite notable.
2.2 Evaluations of the network robustness under hybrid attacks

(1) Under Random Attacks
As what is found in Fig. 1(a)-(d), Internet is quite robust against random attacks. However, the robustness decreases along with the increment of network load ratio \( w \).
When \( w=0.3 \), as is shown in Fig. 1(a), according to the line with \( t=1 \), we find that only to randomly destroy nearly 37.5% percent of all \( N \) nodes, the networks would collapse to level of 50%. And when the destroyed nodes reach 75%, the networks is considered to be totally collapsed due to collapse level \( G \) reaches more than 90%. When it comes to a network with \( w=0.5 \) as is shown if Fig. 1(b), we find that only to destroy nearly 18% percent of all \( N \) nodes, the networks would collapse to level of 50%. And when the destroyed nodes reach 30%, the networks is considered to be totally collapsed and the collapse level \( G \) reaches more than 90%.

Although Internet is proved to be quite resistant to random attacks, it is obvious that the robustness of Internet would decrease sharply when network load ratio \( w \) is growing larger. Especially the networks under conditions when \( w>0.8 \), a minor random attacks would lead to a total collapse of the networks directly.

(2) Under Targeted Attacks
As what is found under random attacks in the above figures, it is obvious found that Internet robustness decrease sharply when network load ratio \( w \) grows larger, even under intentional attacks. Especially when \( w>0.8 \), a minor intentional or hybrid attacks would lead to a total collapse of the networks directly. The relationship between network load and robustness of networks is consistent to what we find in real world.

3 Conclusions
As is shown in the experiments, robustness of Internet is to some extent consistent to that of scale-free networks by the performances of highly resistance to random attacks and great fragilities to intentional attacks. The relationship between network load and robustness of networks is studied, and we find that networks with high loads would easily result in more damaged networks even under the same attacks.

References
Access Control and Security in Cloud Computing Systems

Xixu Fu, Kai jun Wu, Xi Zhang Gong

Institute of Information Technology, Shanghai Ocean University, Shanghai, China
xxfu@shou.edu.cn

Abstract. Security is an important issue in cloud architecture. Good access control can prevent computer systems from many security problems. This paper discussed how security problems can be prevented by access control in cloud systems. Advices on infrastructure were provided in this paper to enhance the security of cloud systems.

Keywords: Cloud System, Security, Virus, Access Control

1 Introduction

Security is a serious problem for any computer systems. Malwares exhaust system resource, steal important information and tamper important configurations. What’s more, virus can spread through the internet in amazing speed. Antivirus software systems tried to prevent systems from threatens of attacking and infection by recognizing the pattern of virus. However, a lot of resource had been used on preventing malicious software and fixing system vulnerabilities. As new virus emerges, more and more resource will be used on malware protection.

Nowadays, computers and servers become more and more powerful. Cloud computing architectures can make full use of powerful machines by creating virtual machines on them and rearrange the computing power for different applications [1]. In cloud systems, infrastructure, platform and software are regarded as services. All resource can be distributed for different applications. IaaS corresponds to hardware of traditional computer system. PaaS corresponds to the operation system layer of traditional computer system. SaaS corresponds to the software and applications of traditional computer system.

In cloud computing systems, malwares can be even more fatal [2]. Virus can spread easily in virtual machines than in real machines. Furthermore, manager of virtual machines can be the super user over many servers. The whole system will be in danger if administrator access gained by hackers [3]. On the other hand, antivirus software can cost more computing resource than that in traditional systems.
2 Virus and Security in Clouds

Traditional antivirus systems prevent computers from malware by recognition patterns of virus. Although effective antivirus software developed every year, many new viruses spread in computers every year. Table 1 shows the virus in computers every year stated by an antivirus corporation.

<table>
<thead>
<tr>
<th>Year</th>
<th>New Types of Virus</th>
<th>Infected Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>10375</td>
<td>18832094</td>
</tr>
<tr>
<td>2007</td>
<td>100017</td>
<td>34414776</td>
</tr>
<tr>
<td>2008</td>
<td>47743</td>
<td>27998478</td>
</tr>
<tr>
<td>2009</td>
<td>101586</td>
<td>14933761</td>
</tr>
<tr>
<td>2010</td>
<td>91994</td>
<td>11533661</td>
</tr>
<tr>
<td>2011</td>
<td>66686</td>
<td>3743721</td>
</tr>
</tbody>
</table>

Machine learning based method such as frequent pattern recognition [6] had been implemented for security. However, malware and hacking have not stop till now with these methods while the cost of antivirus software was rising steadily.

Cloud architecture break the physical isolation of servers, virus can be more infectious in such architectures. By traditional method, every virtual machine in the cloud should install antivirus software and update operating systems frequently. It is a big cost for light weighted virtual machines. Some works also advanced architecture to enhance the security of cloud computing systems [5], the availability and security can not be ensured with this system.

3 Advices on Security of Clouds

3.1 Target of Hackers

Although various malicious software and hacking methods have been developed, target of hackers remains the three as shown below.

- Stop or hamper normal applications.
- Get unwarranted information.
- Distort or destroy information in the system.

The first and the third target can seriously hamper the performance of a computer system. Access control can solve these problems in great exentent.

3.2 Write, Execute and Access Control

Control writing and executing priorities can prevent system from being hampered or distorted. Most operation systems control these priorities merely by an authority system. Once the authority system does not work, nothing can be warranted.
A good example for high availability is the computer lab system. Computers in the lab are protected by a recovery card or even boot from the network. Once they are infected, reboot can fully recover the computer.

Effective control of writing and executing authorization can solve most security problems and keep system high available.

3.3 Secure Platform as Service

Light weighted servers such as web servers need to be stable. Limited executions need to be run at these virtual machines. No special security software should be installed on such operations. Executions should run in the memory. Executions can not take place on data section.

Operation systems for core applications should implement more security components to stop malicious operations such as password stealing.

All operations should have features below.
- Read-only system core.
- Isolation of writing and executing section.
- As simple as needed.

4 Conclusion

This paper gave some advices to enhance the security of cloud systems by access control. The method was proved effective for cloud systems.

References

A Design of Electronic Payment Authentication Method based on NFC Smartphone

Seolhwa Han, Okkyung Choi*, Kangseok Kim, Hongjin Yeh, Taesik Shon

Dept. of Knowledge Information Security, Graduate School of Ajou University, Suwon, Korea
{hsh3440, okchoi, kangskim, hjyeh, tsshon}@ajou.ac.kr
*Author to whom correspondence should be addressed; E-Mail: okchoi@ajou.ac.kr

Abstract. Unlike the phones from the past, Smartphone holds greater performance like that of PC and it is also true that riskier security threat comes along. Also, with the rapid development of mobile NFC payment services, an importance of the mobile security is growing rapidly but currently, the security-related technology is a very secure manner. Therefore this paper aims to propose an electronic payment authentication method using vibration cues, which will be then utilized for design and implementation. The proposed method enables an efficient, secure mobile payment service by analyzing security issues likely to occur in payments using NFC Smartphone and by proposing payment protocols with an authentication method using vibration cues to resolve such issues.

Keywords: NFC(Near Field Communication), User Study, Mobile Phones, Vulnerability Analysis, Authentication, Shoulder Surfing Attack, Relay Attack, MITM Attack, Vibration Cue.

1 Introduction

NFC, short for Near Field Communication, literally means a short-range wireless interaction. It makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch[1].

It is important to provide a simple method for designing and implementing NFC payment systems that offer both reasonable security protection as well as ease of use for the user[2]. Therefore this paper aims to propose an electronic payment authentication method using vibration cues, which will be then utilized for design and implementation. Furthermore, the existing NFC payment system has some weakness of low efficiency and difficulty in the aspect of usability but those problems were solved in this study by developing a method that can be easily used in the Smartphone environment.
2 Proposed Method

The method proposed in this study, intended to cover such vulnerability, is possibly dedicated to preventing data forgery through the use of a biotouch vibration cue like a method for the lock on a safe, coding and storing the payment information in the DB registry to enable strengthening user authentication and getting prepared for personal information leakage.

![Fig. 1. Flow chart of proposed method.](image)

Fig. 1 shows the staged process of the overall flowchart for the proposed method.

1. User puts the NFC reader to contact the NFC payment writer for payment.
2. The NFC payment writer transfers payment information to the NFC reader.
3. The NFC reader upon receipt of payment information performs a vibration cue authentication which then enters a pin value in the completed pin setting in a vibration way. Security factors used here include: 1) pin management that prevents pin number from leaking through periodical renewal, re-coding process and continuous management of the first registered pin number, 2) an authentication that uses the vibration cue recognized by biotouch to prevent pin number from leaking due to SSA, and 3) the DB encryption that encodes significant personal information such as pin number and payment information using AES256 and SHA1, strengthens personal information by comparing hash values.
4. If the vibration cue authentication is successful, payment information is encoded and stored in the registry. If the vibration cue authentication fails over 3 times, the process is forcibly closed so no further payment process can develop. Making repayments is possible only by moving to the initial screen for pin number setting, going through the user authentication process and setting the pin number again.
5. Lastly, a success message is delivered to the NFC reader and the payment process is closed.
3 Conclusion

With the growing popularity of Smartphone, electronic payment services using Smartphone are rapidly gaining traction. Therefore, mobile NFC services market combining with communication and payment is growing rapidly and they are becoming an alternative computing approach to provide lots of convenient services to users. This paper proposed the mobile payment service using NFC based on vibration cues to prevent Reply attack, MITM attack and SSA that are likely to occur in NFC payment service. The proposed method can deter an attack from an outside attacker that can take place in payment process by applying security factors such as Authentication, PIN management and Access Control to banking security techniques. On top of this, while the existing method held disadvantages such as inefficiency and inconvenience in terms of usability, this method considered a matter of security and complemented it for a better use in smartphones.

Acknowledgments. This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA(Korea Internet Security Agency).

References

Comments on Chang-Lee’s Anonymous E-Voting Scheme

Chun-Ta Li 1  Min-Shiang Hwang 2,∗

1 Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan 710, TAIWAN (R.O.C.)
Email: th0040@mail.tut.edu.tw

2 Department of Computer Science and Information Engineering, Asia University
500 Lioufeng Road, Taichung 413, TAIWAN (R.O.C.)
∗ Corresponding author: mshwang@asia.edu.tw

Abstract. In recent years, several electronic voting (e-voting) schemes for communication networks have been proposed. In 2006, Chang and Lee presented an anonymous electronic voting scheme which can be applied in real-world elections. However, this paper shows that Chang-Lee’s e-voting scheme suffers from susceptibility to security attacks and, as a result, some essential security requirements of their e-voting scheme may be compromised.

Keywords: Anonymity; blind signature; e-voting; security; key exchange.

1 Introduction

In 1981, Chaum [3] proposed the first electronic election mechanism that enables people to electronically cast his/her ballot over insecure network. Recently, a lot of electronic voting (e-voting) schemes [1, 2, 5–8] are proposed and a secure e-voting scheme should satisfy the following requirements:

1. Anonymity of voter: No one can identify the relation between a ballot and the voter who cast it.
2. Fairness of vote: No one can learn any information about the progress of the election until the final voting results are published.
3. Convenience of vote: The voter does not need to have complicated knowledge or be able to perform special techniques and no additional voting equipment. In other words, it is voter-friendly.
4. Perceptibility of double voting (Uniqueness): Each legal voter cannot cast his/her ballot more than once and all double voting ballots will be detected and eliminated.
5. Correctness of vote: All valid ballots must be counted correctly and no one can remove, duplicate or alter a valid ballot.
6. Unforgeability of ballot: No one can fake or forge a ballot.
7. Verifiability of vote: For this requirement, each voter should be able to independently check that his/her legitimate ballot has been counted correctly.
In 2006, Chang and Lee [2] proposed an anonymous e-voting scheme. In order to satisfy the above requirements, in their scheme, they combine the techniques of Diffie-Hellman key exchange [4], blind signature and a proxy server in their e-voting scheme. This scheme not only provides an anonymous link from the voter to the voting authority but also enhances the performance such that it can be practically applied over the Internet. However, we find that Chang-Lee’s e-voting scheme is vulnerable to some security attacks and thus some essential requirements of e-voting cannot be achieved in their scheme.

2 Review of Chang-Lee E-Voting Scheme

In this section, we will review Chang-Lee’s e-voting scheme. Chang-Lee’s e-voting scheme consists of the following participants: Registration Center (RC), Certification Center (CC), Monitor Center (MC), Vote Counter (VC), Voter (Vi) and a Proxy Server (PS). Chang-Lee’s e-voting scheme is divided into three phases: initial phase, voting phase, and publishing phase. To shorten the length of this paper, we omit the review and notations explanation. Please refer to [2].

3 Security Problems of Chang-Lee’s E-Voting Scheme

In this section, we will look at the security problems of Chang-Lee’s e-voting scheme. These security problems are described as follows.

Attack 1 – RC compromise attack: Suppose that there is a traitor E in RC, E could replace the valid ballot \( M_i \) with another one, said \( M'_i \) in the voting phase and no one knows that \( V_i \)’s valid ballot has been replaced by another one. In the voting phase, E first generates a new ballot \( M'_i \) (with new \( m'_i, R'_1 \) and \( R'_2 \)) to replace the original \( M_i \) in Step 2 and the following steps are continued until Step 5. Next, in order to convince the MC and VC, in Step 6, before the messages are sent through a proxy server, E must alter the messages \( (h(SN.V_i), SG_i, B_i, R_1) \) and \( (h(SN.V_i), SG_i, B_i, R_2) \) sent by \( V_i \) with another \( (h(SN.V_i), SG_i, B_i, R'_1) \) and \( (h(SN.V_i), SG_i, B_i, R'_2) \), respectively. Thus, MC and VC will store \( R'_1 \) and \( R'_2 \) in their own databases, respectively. Finally, the requirement of correctness cannot be achieved in Chang-Lee’s scheme.

Attack 2 – RC compromise attack: In this attack, E could send the same serial number \( SN.V_i \) repeatedly to many legal voters in the voting phase. Thus, only one voter’s ballot will be counted correctly and other voters who used the same serial number would be cancelled because of duplications. Finally, the requirement of correctness is also not achieved in Chang-Lee’s scheme.

Attack 3 – RC compromise attack: Like above-mentioned attacks, E could send an invalid timestamp \( t'_i \) to many legal voters in voting phase. Next, in publishing phase and Step 2, these voter’s ballots will be ignored by MC and VC because \( t'_i \) will not pass the procedure of freshness checking. Again, the requirement of correctness will not be achieved in Chang-Lee’s scheme.
Attack 4 – Denial of vote attack: In the voting phase, before the messages are sent through the proxy server in Step 6, any adversary can intercept the messages \((h(SN_{Vi}), SG_i, B_i, R_1)\) and \((h(SN_{Vi}), SG_i, B_i, R_2)\) sent by \(Vi\) and thus \(Vi\) is unable to cast his/her ballot to MC and VC. Undoubtedly, it can be said that a denial of vote attack can occur in Chang-Lee’s scheme because it lacks mutual authentication between \(Vi\) and the proxy server. Similarly, this attack might occur in communications between the proxy server and MC/VC and, as a result, their scheme is unable to resist an adversary to remove a valid ballot from the final tally. Finally, the requirements of correctness and verifiability are not achieved in Chang-Lee’s scheme.

Attack 5 – Double voting attack: In the voting phase, any crafty voter can generate \(n\) fake serial numbers \((SN_{Vi_j}, j = 1, 2, \cdots, n)\) for double voting in Step 6. Before the crafty voter sends the messages for double voting, he/she only needs to change the message \(h(SN_{Vi_j})\) leaving the messages \((SG_i, B_i, R_2)\) and \((SG_i, B_i, R_2)\) unchanged. So, a crafty voter could transmit \(n\) ballots with \(n\) serial numbers. Moreover, because MC and VC only have to check that \(h(SN_{Vi_j})\) is stored in its database only once. Therefore, the requirements of perceptibility of double voting and unforgeability of ballot cannot be achieved in Chang-Lee’s scheme.

4 Conclusion

In this paper, we have shown that Chang-Lee’s e-voting scheme is vulnerable to some attacks and the essential requirements of general electronic voting cannot be achieved in their scheme.

References

The Cluster Modeling with Zone-Based Multi-hop Communication in Wireless Sensor Networks

Choon-Sung Nam¹, Kyung-Soo Jang², Gyoo-Seok Choi³ and Dong-Ryeol Shin¹

¹ School of Information and Communication, Sungkyunkwan University, Korea
² Kyung-In Wommen’s College, Korea
³ Department of Computer Science, Chungwoon University, Korea
namgun99@skku.edu, ksjang@kic.ac.kr, lionel@chungwoon.ac.kr, drshin@skku.edu

Abstract. A clustering technique is a communication method which can classify the area by nodes with same or similar sensing and prevent duplicated sensing data to reduce communication. To use a clustering technique, the environment to build clustering has to be considered, which means cluster heads counts can affect clustering formation. Thus, this paper proposes use of a clustering technique with zone-based multi-hop communication in WSNs.

Keywords: WSNs, clustering technique, zone-based communication, multi-hop manner.

1 Introduction

Wireless Sensor Networks (WSNs) are made of large number of tiny sensor nodes, which have the restricted resource and transmit environmental information using self-organized networks[1,2]. Although ad-hoc networks focus on mobility of nodes, WSNs focus on the most efficient use of the available energy resources like expanding network life time. To achieve this, many mechanisms and models have been proposed[3]. Among the many methods, a clustering technique is proposed for network life time, network scalability and load balancing with each node[4]. The communication method between a cluster head and member nodes can use multi-hop manner in clustering routing. WSNs have to use multi-hop manner through neighbor nodes as normal sensor networks cover huge area beyond the communication scope of nodes. When using multi-hop communication, energy consumption of sensor nodes occurs by transmission-bits and receive-bits[5,6]. Thus, this paper propose conditions of clustering formation by comparing of transmission-bits and receive-bits considering communication features of sensor node and calculating energy consumption of WSNs.
2 Cluster Modeling

In non-clustering, the amount of sensing data is dependent on distance, hop-counts, between a sink and nodes. On the other hand, in clustering, member nodes of a local cluster only are dependent on a cluster head. A cluster head collects, aggregates and analyzes sensing data and transmits the aggregated data to a sink node. To compare two cases, clustering and non-clustering, we set up the environment as shown in Figure 1.

![Cluster Modeling Diagram]

**Fig. 1.** Clustering vs non-clustering transmission methods

To calculate energy of non-clustering and clustering, we use the bit-hop metric [7]. The bit-hop metric uses $BT$, the total number of Bit Transmission in the network. $ET_{\text{bit}}$, the energy consumed for transmitting one bit of data, shows 1 J and $ER_{\text{bit}}$, the energy consumed for reception of one bit of data, is 0.5 J. These equations are as follows.

- For non-clustering: $\text{Energy} = BT \times ET_{\text{bit}}$
- For clustering: $\text{Energy} = BT \times ER_{\text{bit}}$
\[ E_t = BT \cdot E_{T\text{-bit}} \] \hspace{1cm} (1)

\[ E_r = BT \cdot E_{R\text{-bit}} \] \hspace{1cm} (2)

From (1) and (2), the total energy cost of the network (E) is as following:

\[ E = E_t + E_r = BT \cdot (E_{T\text{-bit}} + E_{R\text{-bit}}) \] \hspace{1cm} (3)

However, transmission BT and reception BT is different. It is shown in Figure 2. When nodes transmit sensing data to neighbor nodes, BT of transmission, BT(Transmit), is only one cell, but BT of reception, BT(Receive), is 8 cells. Thus, like equation (2) and (3), BT of transmission and reception cannot be equal. To revise this problem, we define new BT(Transmit) and BT(Receive). In Figure 2, we do not revise BT(Transmit) which is same to BT. However, we find out BT(Receive) is dependent on network size. To achieve this, new BT(Receive) equation is derived from appendix A of cluster vs non cluster[8].

5 Conclusion

The clustering technique of WSNs is communication method to improve network life time, network scalability and load balancing. However, if a clustering technique is applied without considering reception energy of nodes, clustering is not better than non-clustering. Thus, we proposed the extended energy modeling of clustering in WSNs. This modeling helps sensor network application using clustering.

References

6. ChoonSung Nam, YoungShin Han, DongRyeol Shin, Multi-hop Routing-based optimization of the number of cluster-heads in wireless sensor networks, Sensors, 2011, 11, 2875-2884.
An Light-weight Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks

Jianhong Zhang¹, Cui Yuanbo¹,², Chen Zhipeng¹,²

¹ College of Science, North China University of Technology, Beijing 100144, P.R.China,
² Institute of image process and pattern recognition, North China University of Technology, Beijing 100144 China

Abstract. Due to the characters of vehicular ad hoc networks, to protect the privacy of the vehicles, the message must be anonymously transmitted in VANETs. However, the existing technologies to realize anonymity, pseudonyms certificate and group-oriented signature, have complex key management and large computational cost. They don’t satisfy actual demand. To solve the above problem, we propose a novel privacy-preserving authentication protocols based on self-certified cryptography in this paper. And we show that the security of the scheme is related to the extended k + 1 exponent Problem (EP).

Keywords: vehicular ad hoc networks, self-certificate cryptography, the exponent problem.

1 Introduction

By combining the advance control, communication, navigation and processing systems available in modern vehicles with wireless ad-hoc networks, VANET is put forward to build intelligent applications for traffic congestions, vehicle density in roads, road repair work, etc. It is a special kind of mobile ad hoc networks consisting of entities including the vehicles, also known as onboard units (OBUs), and the roadside units (RSUs). In a vehicular ad hoc network, the OBUs and RSUs, equipped with on-board sensory, processing, and wireless communication modules, can form a self-organized networks. In VANET, each vehicle can not only communicate with each other, i.e., vehicle-to-vehicle (V-2-V) communication, but also communicate with roadside unit, i.e., vehicle-to-infrastructure (V-2-I) communication. Therefore, compared with the traditional pure infrastructure-based network, the hybrid of V-2-V and V-2-I communications is promising since it can not only overcome the disadvantages of infrastructure-based network, but also overcome the disadvantage of non-infrastructure -based network. As for the development of VANETs, it is expected to serve as a general platform for the development of any vehicle centered applications [2] in the near future.
In the recent years, several researches on VANETs have been investigated by academic or industries, such as IEEE P1609.2 working group. In these researches, most studies focused on the performance of medium access control (MAC) layer or the routing issues inherent in VANETs. Very recently, some works addressed the security issues and privacy issues. As a special mobile ad hoc networks, VANETs may suffer any malicious user’s behaviors, such as bogus information and replay attacks on the disseminated messages. Among various security threats, privacy preservation in VANETs is one of the new challenges to protect users’ private information including the driver’s name, license plate, driving model, and traveling route. Therefore, before deploying VANET for practical application, security and privacy issues must be addressed. Otherwise, the VANET might be confronted with many potential attacks.

Based on the above problems, to protect own privacy, a vehicle must transmit message in a privacy preserving manner. For example, a honest vehicle driver, which want to inform the authorities about other vehicles present at a scene of an accident may not directly transmit a message to the authorities for fear of reprisals from other vehicle drivers. In the other side, the authorities might not receive a unconditionally anonymous message that cannot be authenticated as it could be an attempt to mislead an investigation by providing fraudulent data. To achieve these functions, conditional privacy should be preserved. The user related information has to be protected from malicious access, while the authorities can reveal the sender if a dispute appears.

The most widely adopted privacy-preserving technique in VANET is divided into two types. one is based on pseudonyms certificate, during registration, each vehicle is supposed to pre-loaded a large number of pseudonyms certificates with pseudo identities in this type, and randomly chooses one of the available pseudonymous certificates for signing a message at one time. However, when a vehicle is revoked, all the pseudo identities would be added into a CRL. Thus, certificate management and revocation are troublesome; the other is based on group-oriented signature which is a combination of group signature(ring signature) and ID-based signature. Each vehicle is considered as a group member and can anonymously produce a message-signature. However, the length of group signature is much longer than one of ordinary signature and the computational cost of verifying group signature is high, and the revocation of member is the inherent problem in the group signature.

Self-certified public key cryptosystem was introduced by Girault[4]. In the self-certified public key system, certificate verification and management are not required and the key escrow problem can be eliminated. The idea is that certificate is replace by a witness and the public key is embedded in it. Anyone who holds a witness along with an attributive identity can recover the corresponding public key to verify signature. Thus, it leads in the reduction of communication, computation and storage amount.

**Our Contribution:** To overcome the above problems in the privacy-preserving, we propose a novel privacy-preserving authentication protocols to address the security and privacy based on self-certified signature in this paper. And we show
that our scheme can achieve conditional privacy preserving and is proven be secure in the random oracle.

2 Objectives

To avoid reinventing the wheel, refer to [2] for a full discussion of the attack and security requirements to the interested reader. In the following, we focus on anonymity and liability.

1. Anonymity: it includes vehicle’s identity anonymity and anonymous user authentication. vehicle’s identity anonymity denotes that given a safety message with a valid signature, identifying the actual signer is computationally hard for everyone but the trusted authority. Malicious nodes cannot obtain the private information of the vehicles from the safety message. Anonymous user authentication indicates that the process of attempting to verify that a user is authentic and legitimate but does not reveal the real identity of the user.

2. Liability: If a malicious vehicle with OBU produces a fraudulent message. Then the authority must be able to open the corresponding signature to trace the actual identity of the vehicle. Our design objective is to make that \( TA \) can open a group signature with the \( TA \)'s master key to compute the real identity of the sender.

The Extended \( k + 1 \) Exponent Problem (EP) Let \( G_1 \) and \( G_2 \) be two multiplicative cyclic groups of order \( q \), \( g_2 \) is a generator of group \( G_2 \). \( Z_q \) is a finite field, \( \psi \) is a computable isomorphism from group \( G_2 \) onto group \( G_1 \) such that \( \psi(g_2) = g_1 \). Given \( k + 1 \) values \((g_2, g_2^a, g_2^{a^2}, \ldots, g_2^{a^k})\) and a isomorphism map \( \psi \), where \( k \) is an integer and \( a \in Z_q \), its goal is to compute \( g_1^{a^{k+1}} \).

Acknowledgments.

This work was supported partly by Supported by Beijing Natural Science Foundation (No:4122024).

References

Parallel Reduction Algorithm of Multiple-Precision over Finite Field GF(2ⁿ)

Yongnan Li¹, Limin Xiao¹, Aihua Liang¹, Zhenzhong Zhang¹, Li Ruan¹

¹ School of Computer Science and Engineering, Beihang University,
Beijing, 100191, China
{liyongnan1984, liangah, zzzhang}@cse.buaa.edu.cn {xiaolm, ruanli}@buaa.edu.cn

Abstract. This paper presents a parallel reduction algorithm concerning multiple-precision integer over finite field GF(2ⁿ). The data dependency of the sequential reduction algorithm is analyzed to design the parallel algorithm. We take one time clock as the computation time unit to compute the time complexities of parallel algorithm and sequential algorithm. The speedup shows high efficiency of the proposed parallel algorithm.

Keywords: parallel algorithm; finite field GF(2ⁿ); reduction

1 Introduction

The finite field GF(2ⁿ) is one of the common used mathematical sets for constructing some cryptosystems including conic curves cryptosystem [1,2] and elliptic curves cryptosystem [3,4]. In recent years, the parallel algorithms of some fundamental operations over finite field GF(2ⁿ) have received considerable attention due to massive computation caused by the increased security demands. However, there is less deep study on fast parallel algorithms concerning multiple-precision integers over finite field GF(2ⁿ). Our previous works have designed several parallel algorithms about some basic operations of multiple-precision integers over two other mathematical sets [5-8]. This paper proposes an efficient parallel reduction algorithm of multiple-precision over finite field GF(2ⁿ) to accelerate the speed of this basic operation over finite field GF(2ⁿ).

2 Reduction Algorithm over GF(2ⁿ)

The following algorithm is the traditional algorithm for computing reduction over GF(2ⁿ).

Reduction over GF(2ⁿ)

Input: module \( f(Z) = Z^n + r(Z) \),
polynomial \( C(Z) = C_{2n-2}Z^{2n-2} + \cdots + C_1Z + C_0 \).
Output: \( C(Z) \mod f(Z) \).

1. for \( i \) from \( n - 2 \) to 0, repeat:
1.1 if $C_{i+n} = 1$, then

$$j \leftarrow |i/W|, \quad k \leftarrow i - Wj, \quad C\{j\} \leftarrow u_k(Z) \oplus C\{j\}.$$ 

2. return $(C[i-1], \ldots, C[1], C[0])$.

### 3 Parallel Reduction Algorithm over GF($2^n$)

This section discusses the proposed parallel reduction algorithm over finite field GF($2^n$). We take one time clock as the computation time unit to compute the time complexities of parallel algorithm and sequential algorithm.

The parameter $W$ represents the word length of the computer and the parameter $n$ denotes the degree of the modular polynomial $f(Z)$. The parameter $u_k(Z)$ means $Z^k r(Z)$ where $0 \leq k \leq W - 1$. We define $m = \lceil (2^n - 1)/W \rceil$, so the polynomial $C(Z)$ could be expressed as $(C[m], \ldots, C[1], C[0])$. The parameter $C\{j\}$ means $(C[m], \ldots, C[j + 1], C[j])$.

![Fig. 1. An example of incorporating the intermediate results](image)

In the first step, one comparison must be executed to decide whether or not to execute the two arithmetic operations and one logical operation. The average number for computing the other three operations in all rounds of the first step is $(n - 1)/2$ for the reason that the probability of $C_{i+n}$ equal to 1 is 0.5. In substep 1.1, operation $j \leftarrow |i/W|$ denotes computing the word length of $\{C(i+n), \ldots, C(n)\}$ and it could be calculated in one time clock. Operation $k \leftarrow i - Wj$ is used to get the number of the bits in the highest word of $\{C_iZ^i + \ldots + C_1Z^1 + C_0\}$, so the operation of multiplication and operation of deduction are not needed to be computed. Only one time clock is needed to obtain the result of this operation. Operation $C\{j\} \leftarrow u_k(Z) \oplus C\{j\}$ means executing XOR for every bit of $u_k(Z)$ and $C\{j\}$ from the lowest bit to the highest bit and it also needs one time clock. To sum up, the total runtime of the sequential procedure for computing reduction over GF($2^n$) is $5(n - 1)/2$.

For the parallel procedure, every round of the first step can be calculated simultaneously except the operation of $C\{j\} \leftarrow u_k(Z) \oplus C\{j\}$. To obtain the final value of $C(Z) \mod f(Z)$, the intermediate results of $u_k(Z)$ in substep 1.1 should be incorporated after the other operations finished. Obviously, the average number of the temporary result of $u_k(Z)$ is $(n - 1)/2$. As depicted in Fig.1, we use the merging principle.
to incorporate the intermediate results of $u_k(Z)$ and it will cost $\lceil \log_2((n-1)/2) \rceil$ time clocks. Then the total parallel runtime of reduction over $\text{GF}(2^n)$ is $\lceil \log_2((n-1)/2) \rceil + 2$.

Therefore, the speedup is

$$S = \frac{5(n-1)/2}{\lceil \log_2((n-1)/2) \rceil + 2}. \quad (1)$$

4 Conclusions

In this paper, we presented a fast parallel reduction algorithm of multiple-precision over finite field $\text{GF}(2^n)$. The parallel algorithm is designed by analyzing the data dependency of the sequential algorithm. Time complexities of the parallel algorithms and the sequential algorithms are discussed to show the high efficiency of the proposed algorithm. We only discussed the method for paralleling reduction operation over finite field $\text{GF}(2^n)$ in this paper. The future works may focus on parallelization of other basic operations over finite field $\text{GF}(2^n)$.

Acknowledgments. This study is sponsored by the National “Core electronic devices high-end general purpose chips and fundamental software” project under Grant No. 2010ZX01036-001-001, the Hi-tech Research and Development Program of China (863 Program) under Grant No. 2011AA01A205 and the National Natural Science Foundation of China under Grant No. 60973008.

References

Web Services Based on OPC Unified Architecture

Jian-ping CHOU, Li-chao CHEN, YingJun ZHANG, Lihu PAN

School of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan, Shanxi 030024, China
E-mail: choujianp@yahoo.com.cn

Abstract. Web Services require reliable communication over a wide area. While Internet can be used for this communications, for customers these Web Services must satisfy requirements for security, availability, reliability, and performance/scalability. Additionally, these web services must be readily integrated into existing communication networks at the communication end points. This paper considers the use of Web Services based OPC Unified Architecture.

Keywords: Demand Response, Web Services, OPC UA, Communication Network.

1 Introduction

In order for utilities to more effectively control equipment, we must be able to communicate reliably with load control systems and devices.

For customers, the architecture must support two-way PUSH and the PULL communications between a centralized utility server and distributed client load control systems and devices. When using PUSH, the server sends client load control systems XML documents asynchronously. When using PULL, the load control clients request XML documents from the server.

While it is easier and frequently necessary to employ a PULL model for communication, clients typically don’t know when events occur in the server. Clients can continuously poll the server, but as the number of clients increases, the latency of message delivery increases. A reliable standardized mechanism for clients to asynchronously receive an XML document is needed.

This paper describes how Web Services can be use to perform reliable asynchronous communication through which a client can receive demand response related XML documents. The proposed solution employs OPC UA Web Services. OPC UA does not define the content of the XML document, but only the means by which clients set up a reliable and secure two-way communication channel with servers.
2 Possible Solutions

The development of Web Services for Demand Response can be seen as consisting of two tasks. The first is the specification of message payloads and the second is the specification of how Web Service technology is used to transmit payloads. The specification of payloads is particular to Demand Response since the content of message payloads reflects the content of the communication. However, the specification of the way in which Web Service technology is used to reliably communicate information need not be specific to Demand Response. Instead, the reuse of generic technology may be employed as long as that technology meets the requirements of Demand Response Communication.

OPC UA is attractive for communication for several reasons:
- Older OPC technology based on Microsoft COM technology is widely used by control systems. It is straightforward to wrap existing OPC COM based interfaces.
- OPC UA is under consideration for communication within the operations and maintenance areas within electric utilities.

It is believed that OPC UA meets all requirements for Demand Response communication and will enable more rapid uptake. In particular, since OPC UA has been developed in cooperation with many of the large management/process automation/utility SCADA companies, OPC UA provides the most expedient way to reach consensus with regard to communication.

2.1 OPC UA Performance/Scalability

OPC UA services can be implemented over a variety of communication transport profiles. This means a single application wrapper can be used regardless of the technology used to transport data. Consequently, the technology used for a communications link can be optimized based on end point and communication channel sizing. For example, requirements for a high throughput link may not allow the use of XML data encoding, but instead may employ binary encoding of data on the network. However, switching binary encoding on the network does not mean the adapter needs to be rewritten.

2.4 OPC UA Reliability

It should be noted that the requirement for reliable communication for communications suggests that the Web Services should not follow the Representational State Transfer (REST) paradigm. Typically REST based services have the following characteristics:
- A pull-based interaction style: consuming components pull representations. However, for demand response, push is also needed.
- Stateless: each request from client to server must contain all the information necessary to understand the request, and cannot take advantage of any stored context.
on the server. Therefore, neither the client nor the server can positively know if all messages sent by the server have been received.

It should be noted that a REST based protocol may be suitable with residential customers for whom a lost message does not have as great a potential economic impact.

2.5 OPC UA Availability

The WS specifications by themselves do not enable the construction of interoperable highly available components.

2.6 OPC UA Securities

In the absence of OPC UA, WS Security provides a very large number of options. It is difficult to achieve interoperability without limiting the choices to those that are applicable to the utility metering and operations environment. OPC UA includes a set of mandatory encryption and authentication profiles based on WS standards.

3 Conclusions

Web Services could defined that implement the WS specifications to meet specific needs, however UA provides a pre engineered solution with support by major vendors. By reusing the generic OPC UA services, building/industrial/utility automation systems can limit the number of supported interfaces.

Acknowledgements

- Project (No. 2007BAK29B01) supported by Key Projects in the National Science & Technology Pillar Program
- Project (No. 20100322004) supported by Key Technologies R & D Program of Shanxi
- Project (No. 20110081033) supported by Bureau of International Cooperation of Shanxi
- Project (No. 20111025) supported by the Graduate Innovative Projects of Taiyuan University of Science and Technology
Secure Business Transaction based on ebXML
Applying Web Service Security

Dongkyoo Shin* and Dongil Shin

Department of Computer Engineering, Sejong University
98, Gunja-Dong, Gwangjin-Gu, Seoul 143-747, Korea
{shindk, dshin}@sejong.ac.kr
*Corresponding Author

Abstract. ebXML business transaction models are proposed which allow trading partners to securely exchange business transactions by employing Web service security standard technologies.

Keywords: electronic commerce, ebXML, Web service security, secure business transaction

1 Introduction

ebXML (Electronic Business using eXtensible Markup Language) is a modular suite of specifications for the XML-based global infrastructure for e-business transactions, and provides a standard method to exchange business messages, conduct trading relationships, communicate data in common terms and define and register business processes [1, 2]. The technical infrastructure of ebXML is composed of the following major elements: Messaging Service, Registry, Trading Partner Information (It consists of two specifications: CPP (Collaboration Protocol Profile) and CPA (Collaboration Protocol Agreement)), Business Process Specification Schema, Core Components.

There are well-known conventional security technologies that can be used by ebXML implementers to resolve the risks [2]: user-id and password, PKI (Public Key Infrastructure), SSL (Secure Socket Layer), S/MIME (Secure Multi-Purpose Internet Mail Extensions). Web Service security technologies emerging recently have extensibility and flexibility suitable for ebXML security implementation such as encryption, digital signature, access control and authentication. XML digital signatures [3] and SAML (Security Assertion Markup Language) [4] can be exploited to solve the unauthorized transactions and fraud problems in electronic business systems. XML digital signatures are used in ebXML to provide data integrity on messages, existing authentication and authorization schemes as well as non-repudiation between entities. SAML is recommended to provide identification, authentication and authorization and often used with XACML (eXtensible Access Control Markup Language) [5] to allow or deny access to an XML resource. XML Encryption [6] is recommended to solve the loss of confidentiality problem. Also XKMS (XML Key Management Specification) [7] is recommended for key...
management as a substitute for PKI.

2. Secure Business Transaction Models based on the ebXML

A high-level use case scenario for two trading partners is explained based on the ebXML technical architecture specification [1] as follows.

Company A will first review the contents of an ebXML Registry, especially the registered business processes that may be downloaded or viewed. Based on a review of the information available from an ebXML Registry, Company A can build or buy an ebXML implementation suitable for its anticipated ebXML transactions. The next step is for Company A to create and register a CPP with the registry. Company A might wish to contribute new business processes to the registry, or simply reference
available ones. The CPP will contain the information necessary for a potential partner to determine the business roles in which Company A is interested, and the type of protocols it is willing to engage in for these roles. Once Company A is registered, Company B can look at Company A's CPP to determine that it is compatible with Company B's CPP and requirements. At that point, Company B should be able to negotiate a CPA automatically with Company A, based on the conformance of the CPPs, plus agreement protocols, given as ebXML standards or recommendations. Finally, the two companies begin actual transactions.

Fig. 2. The second model: Exchange of Business Transactions

Based on the scenario, we propose two ebXML business transaction models ensuring the trust relationship within the real trading partners. The first model performs a user authentication and updates the CPP in the registries. The second model performs business transactions within the trading partners. These models will explain how each Web service security technology solves the risks for ebXML.

We showed how each Web service security technology meets the ebXML standard by constructing the experimentation software and validating messages between the trading partners.

References

Abstract. Web Metering is a method to find out content and services exposure to visitors. This paper proposes a visitor centric voucher scheme that uses an identity management systems solution to incorporate a Web Metering function. The proposed scheme runs transparently to the visitor and utilises security properties available in identity management systems. On a higher level, the scheme introduces the use of authentication protocols to provide Web Metering evidence.

1 Introduction

Web Metering is defined here as a method to measure the interactions done between the visitor and the Webserver over a specific period of time. Web Metering became a valuable measurement tool when “Online Advertising” services played an important role in the Internet. There is an enquirer party which is interested in measuring the interactions between the visitor and the Webserver. The Web Metering operation can be provided by an Audit Agency or a Service Provider.

A Web Metering scheme is defined as a transparent if it executes inside or behind another action or property in the web interaction so it does not require an explicit action from visitor. That is, the scheme does not require the visitor to change browser “structure” by installing hardware or software not needed during a “normal” interaction between visitor or Webserver. Also, the scheme does not require the visitor to change his behaviour (experience) to access the Webserver by executing an explicit human action (e.g. clicking on a specific button).

2 Previous Work

The majority of Web Metering schemes is based on Secret Sharing schemes and one of the early published schemes was by Naor and Pinkas [5]. The Webserver here needs to receive a specific number of shares from visitors to be able to compute a required result using a Secret Sharing scheme as evidence of the visits. Further research continued on Naor and Pinkas work, for example, Masucci work on Web Metering schemes [1, 2]. Using such schemes necessitates the visitors to securely receive or generate required shares. For visitors receiving shares from the Audit Agency, the visitor has to be authenticated to stop an adversary from receiving the shares and consequently inflating number of visits. This entity
authentication poses privacy and transparency concerns. For the case of the visitor generating the shares, the visitor has to be explicitly involved in the scheme which does not make it transparent.

Another visitor centric scheme is the use of hash chaining and digital signature for constructing non-repudiation evidences of visits as proposed by Harn and Lin in [4]. In such scheme, the visitor hashes the result of the hash chain with additional information and sends a signature of the hash to the Webserver. The scheme provides a Web Metering evidence using a signature by the visitor. To alleviate the visitor from producing a costly signature for each visit, a hash chain is proposed. That is, the Webserver uses received signature (which reveals visitor identity) and hash values as evidence for number of visits. This visitor signature is a privacy concern and its production does not run transparently nor efficiently.

3 Problem Description

Web Metering schemes are vital for measuring today’s Internet visits. However, many of voucher schemes lack visitor transparency and have integrity problems. Generally, the majority of Web Metering schemes approached the integrity issue without paying more attention to the transparency part. A transparency property is important in order for a scheme to be usable as there will be no actions required from the visitor side. In this paper, we propose a novel solution based on integrating Web Metering schemes with identity management systems. We show how to solve this problem by designing a Web Metering scheme which utilises existing vouchers to securely carry Web Metering evidence. On a higher level, this research also addresses the feasibility of hiding Web Metering feature behind another existing application. The result of this can be used to encourage the idea of “piggybacking” Web Metering function to other existing applications.

4 Proposed Web Metering Scheme

The proposed scheme depends on protocols that are already used between the visitor and the Service Provider and have padding capability to carry Web Metering evidence transparently to the visitor. Such “flexible” ticket-based protocols are authentication protocols described in ISO/IEC 10181-2 and ISO/IEC 9798 where tickets (or vouchers) can be redesigned to carry the evidence. In these authentication protocols, a third party authenticates the visitor and embeds the Web Metering evidence in a ticket which is sent to the Webserver. The addition of a Web Metering feature is possible here because ISO/IEC allows additional information to be carried in text fields in authentication protocols [3]. While studying many identity management systems, we observed background communications between Webserver and Identity Provider (IdP) can be used to carry Web Metering evidences for visits to Webserver. The IdP is regarded here as a Service Provider that provides visit evidence transparently to visitors.
The proposed scheme also utilises the ability to extend attribute statement in SAML messages [6]. This feature affects accuracy as well because granularity of metered data can be increased by the Webserver extending the requested attributes in the attribute statement. Also, there is a cryptographic binding of assertion and IdP through a digital signature and since IdP is a trusted entity, the signature will enhance the reliability of the metering process. There are two fields in an attribute statement which are produced by the IdP and sent to the visitor which finally gets forwarded to the visited Webserver. The first field is Metering Statement which represents a statement from the IdP, assuring that the Webserver has been visited at a specific time. The second is Statement Signature which is a signature on the Metering Statement using the IdP private key. The Metering Statement can be published by the Webserver to interested parties and the Statement Signature serves as an evidence.

We tested a simplified version of the scheme on a server with 1024 MB memory and 1.6GHz processor. This server was hosting both the Webserver and the IdP. The signature on the metering statement is produced using open source PKCS#1 (v2.1) RSA compliant library. Execution time from IdP side is around 40 seconds and generated evidence is 204 characters. The inefficiency of the proposed scheme centres around the on-fly digital signature from IdP side and the dynamic text (as time is included) that has to be signed. As a result, the efficiency can be improved by signing a smaller pointer message (e.g. a number) which can be used as a signed reference at the Webserver side.

5 Conclusion

Secure Web Metering schemes are needed to address today’s Internet challenges. In this paper, we proposed a Web Metering scheme by utilising an identity management system to transparently carry a Web Metering evidence. The scope of other interesting Web Metering functions that could benefit from the leverage of IdPs is more than the produced Statement Signature e.g. IdPs can be Audit Agencies that publish Web Metering results.

References

DEVS-based Modeling, Simulation, Scheduling of Bottleneck Process in Semiconductor Manufacturing

YoungShin Han, JinMyoung Kim, Chilgee Lee

School of Information and Communication Engineering, Sungkyunkwan University, Suwon 440-746, Republic of Korea
hanys@skku.edu

Abstract. In this paper shows DEVS modeling and simulation of a bottleneck system which is used in the semiconductor manufacturing. The model of the system consists of an EFForBottleNeck coupled model and a BottleNeckSystem coupled model. In this work we compare scheduling methods to increase the production of the wafer fabrication.

Keywords: DEVS, semiconductor manufacturing, BottleNeck, Scheduling

1 Introduction

The globalization of semi-conductor market is changing the market trend in vendor market and customer market as well as creating new business opportunities. This change in the market even affects its manufacturing process. It causes frequent unexpected disturbance (equipment failure, urgent actions etc.) in semi-conductor production line leading to the lower productivity. It is necessary to reduce the disturbance or factors causing adverse effects in order to enhance competitiveness.

A bottleneck facility (BF) is, as the name implies, a production facility that constrict the smooth flow of production on the production line. The facility can be identified by inspecting queue length, machine utilizations, or loading level. In wafer fabrication process, many devices are connected with BF and they require a setup time, workload and WIP (Working in Progress)[1]. Since BF selects the job from the devices by considering the factors, scheduling problem occurs.

2 Related Research

The DEVS conceptual framework is composed of real system, model, simulator and experimental frame. The DEVS basic model (M) is defined as:

\[ M = \langle X, S, Y, \delta_{\text{int}}, \delta_{\text{ext}}, \lambda, t\alpha \rangle \]

In the equation, X is a set of inputs events, S is a set of sequential states, and Y is a set of output events. \( \delta_{\text{int}} \) and \( \delta_{\text{ext}} \) is the internal and external transition function, respectively. \( t\alpha \) represents a time advance function. The function calculates the time for each state. For an arbitrary system, the system can be represented by one or more
basic model. The coupled model (CM) represents an interconnection between the models. CM is defined:

\[ CM = \left\{ X, Y, D, \{ M_i \}, \{ l_j \}, \{ Z_{i,j} \} \right\} \]

Where X and Y are sets of input and output events and D is an index set for the components of the coupled model [2].

3 System Modeling

Fig. 1 shows the simple structure of the bottleneck facility. In the figure, various devices can be joined to the BF. Each device has own unique pre-processing time, setup time and post-processing time. Generally, since the cost of the BF is very high, heterogeneous devices should be joined to the facility in order to process all jobs from the devices.

![Fig. 1 Processing step in the bottleneck facility](image)

After jobs are loaded into the job queue, BF selects the job from the queue by considering the various factors to increase a throughput, utilization and so on. Also WIP balancing is an important factor since intermediate products from an arbitrary device is buffered without dispatch then the fault rate of the products increase. In this paper, based on the workload that is proposed by Y.D. Kim [3], we compare the performance of FCFS, Same Setup and loop heuristic method.

4 Simulation Result

We simulated the models with a pre-specified desired accuracy and a significance level. The simulation executed 5 times for a statistic analysis. A warm-up period of this simulation results is 500 minutes, and the total simulation time is 5000 minutes.

<table>
<thead>
<tr>
<th>Table 1. FCFS(First-Come First-Serve) Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
</tr>
<tr>
<td>Throughput(avg)</td>
</tr>
<tr>
<td>Average Cycle Time(mean)</td>
</tr>
</tbody>
</table>
Table 2. Same Setup Rule

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput(avg)</td>
<td>1,831</td>
<td>1,778</td>
<td>1,731</td>
<td>1,734</td>
<td>1,731</td>
</tr>
<tr>
<td>Average Cycle Time(mean)</td>
<td>15,794</td>
<td>14,239</td>
<td>14,770</td>
<td>16,494</td>
<td>16,645</td>
</tr>
</tbody>
</table>

Table 3. Loop Heuristic ($\delta = 10$)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput(avg)</td>
<td>1,797</td>
<td>1,783</td>
<td>1,725</td>
<td>1,714</td>
<td>1,774</td>
</tr>
<tr>
<td>Average Cycle Time(mean)</td>
<td>18,474</td>
<td>16,454</td>
<td>17,238</td>
<td>16,320</td>
<td>15,576</td>
</tr>
</tbody>
</table>

5 Conclusion

In this paper, we compare scheduling methods to increase the production of the wafer fabrication. We model the process based on DEVS (Discrete Event System Specification) and estimate our method. According to the simulation results in this study, heuristic rule is superior to FCFS rule in terms of the average cycle time but it is agreed that the same setup rule is the best. FCFS takes longer than 10 times than other alternatives. This is because its setup is more complicated and time-consuming. Its setup time is much longer than processing time (about 3-5 times longer). Subsequently, there will be more WIP if the setup occurs more often and the average cycle time will become longer.

Acknowledgements. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2011-0379-000).

References

A Distribution Model for Issuing Mechanism of Wrapper-based Digital Publication

Wei-Chen Wu1 *, Horng-Twu Liaw2, Jiann-Fu Lin3, Li-Lin Hsiao2, and Chih-Ta Yen4

1 Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County, Taiwan, R.O.C.
wwu@hsc.edu.tw
2 Department of Information Management, Shih Hsin University, Taipei, Taiwan, R.O.C.
{htliaw,hsiao}@cc.shu.edu.tw
3 Department of Management Information System, Takming University of Science and Technology, Taipei, Taiwan, R.O.C.
alfu@takming.edu.tw
4 Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C.
yeng019@gmail.com

Abstract. With the advance in the electronic devices, digital publications become more and more popular in our life. However, the properties of digital contents make themselves be easily copied and transferred if there is not any proper protection for them. Hence, it is a critical issue for publication provider to effectively control and distribute their digital publications. Digital Rights Management is a mechanism, which might congregate various techniques to protect the rights of digital publication from copyrights violations. Moreover, Wrapper-based Digital Rights Management technique applies encapsulating digital contents by packaging content and monitoring by API-Hook to control and protect them, which provide a way to authenticate users by users’ machine serial number or smart card via network. Hence, users may use the digital contents without changing their digital content player. According to the definition of Digital Rights Management, this paper provides a digital publication issuing mechanism, which supports superdistribution for advertising digital publications effectively and improving development of digital contents.

Keywords: Digital rights management; API-hook; Wrapper; Superdistribution; Business model.

* Corresponding author: Computer Center, Hsin Sheng College of Medical Care and Management No. 418, Kaoping Village, Lungtan Township, Taoyuan County 32544, Taiwan, R.O.C. Tel:+88634117578 ext.260, Fax:+88634117600 email:wwu@hsc.edu.tw
1 Introduction

With the rapid development of the Internet and computers, more and more digital documents and digital products weed through the old to bring forth the new unceasingly. It is essential to protect digital contents, which will improve the intention of digital contents providers to create new products and protect the rights of legal customers.

Digital Rights Management (DRM) is a mechanism, which congregates hardware and software to ensure the rights of digital publication providers against illegal usage [1]. The DRM could track and manages the usage of digital contents, such as the legality of copy or distribution. However, some prevailing systems, such as Windows Media Rights Manager, iTunes, and Adobe Systems, only support their own digital content types. These systems do not provide interoperability, which limits the usage of digital contents with many restrictions.

The concept and architecture of Superdistribution is proposed by Mori [2,3] for building up a software service system in a P2P structure. Superdistribution could also be a business model, which distributes digital publications safely and effectively by combining some free methods [4,1].

There are some advantages would be obtained if DRM supports superdistribution, such as progressing distribution channels, reducing distribution costs, and forming strong partner networks. In this paper, we will propose a secure, fair and effectively distributing digital publications issuing mechanism for the systems lacking of business models and charging mechanisms to solve the problems of digital publications being transacted on the Internet. The rest of this paper is organized as follows. We propose a novel wrapper-based digital publication issuing mechanism in Section 2. Finally, a conclusion is presented in Section 3.

2 Our Mechanism

In our mechanism, we adopts Elliptic Curve Cryptography (ECC) [5], KryptoKnight authentication and key distribution system [6] to protect customers’ personal information, and add a trusted third party call certificate authority to issue licenses and to support fair judgment in transactions if necessary. The original business mode of DRM is still kept in our mechanism for easily adapting the rights of new customers. The major five roles of this mechanism are described as follows: Customer(C), Certificate Authority (CA), Digital Publication Provider(PP), Digital Publication Rights Issuing Management Platform(MP) and Bank(BK). Our mechanism contains the following seven phases.

1. Certificate Requesting and Registration Phase: This phase is an initial phase, all roles of this mechanism must register to CA and request certificates. After registration, PP assigns the basic grants for superdistribution and transfers the grants of digital publications to XrML format. Then, PP sends digital publications and XrML to MP through a secure channel.

2. Superdistribution Phase: The potential customer $C_N$ could receive a protected digital publication shared by original customer $C_O$ through email, instant message, or P2P. $C_N$ can use the publication with basic grants.
3. Publication Selecting and Authentication Phase: After the customer finishes registration and gets the certificate, the customer could get publications from the website of MP or by superdistribution. The Customer C sends request containing wanted publication identity and wanted grants to MP.

4. License Issuing Phase: After payment, the customer can request the license to enjoy the publication. C sends \textit{TradeOK}_C (a success message of \textit{X}'s transaction) to MP for requesting the license.

5. Tracking Phase: Regardless of online or offline patterns, DRM controller must record and trace the processes of how users enjoy publications for protecting the publications.

6. Customers’ License Transferring Phase: In order to handle various modes of transactions, we support license transferring services for flexible use of valid licenses.

7. Rights Transferring Phase: There are various business models in commercial circumstances. Considering the demands of providers, they may transfer their rights to others. For example, some enterprises may find business opportunities from some digital publications and then buy out them. Moreover, the transferred target must be the member of this mechanism.

3 Conclusion

In this paper, we proposed a secure, fair and effectively distributing digital publications issuing mechanism for the systems lacking of business models and charging mechanisms to solve the problems of digital publications being transacted on the Internet.

References

Security Evaluation of Mobile Device Management Agents

Keunwoo Rhee, Hawon Kim, and Hac Yun Na*

1 The Attached Institute of ETRI
909, Jeonmin-dong, Yuseong-gu, Daejeon, 305-390, Korea
{kwrhee, wonny, hyna}@ensec.re.kr

Abstract. In this paper, we propose the first criteria and methods to evaluate the Mobile Device Management agent. The proposed criteria and methods are practical since we illustrate the evaluation items and real world evaluation methods for Android devices.

Keywords: Mobile Device Management agent, Android devices, evaluation

1 Introduction

There are no criteria to evaluate functions of an MDM agent. Therefore, we propose criteria and methods to evaluate an MDM agent. The proposed criteria and methods have the following significances. (1) They are the first evaluation criteria for an MDM agent. (2) They may improve the security of an MDM agent. They can be extended to evaluate the security of other applications on mobile devices. (3) They are practical since we describe the real world evaluation methods for Android devices.

2 Security Requirements

In order to propose evaluation items, first we identify security requirements.

Table 1. Security Requirements

<table>
<thead>
<tr>
<th>Security Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1. The MDM agent should provide secure communication channel between the MDM agent and the server.</td>
</tr>
<tr>
<td>R2. The MDM agent should communicate with the authenticated MDM server.</td>
</tr>
<tr>
<td>R3. The MDM agent should cope with disconnecting.</td>
</tr>
<tr>
<td>R4. The MDM agent should authenticate a mobile device user before accessing the mobile device and its functionality.</td>
</tr>
<tr>
<td>R5. The MDM agent should prevent modification or removal of configurations and audit data</td>
</tr>
</tbody>
</table>

* Corresponding author.
Table 1. (Continued)

<table>
<thead>
<tr>
<th>Security Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>R6. The MDM agent should control hardware modules of mobile device.</td>
</tr>
<tr>
<td>R7. The MDM agent should protect confidential data.</td>
</tr>
<tr>
<td>R8. The MDM agent should enforce minimum condition of cryptographic mechanisms.</td>
</tr>
<tr>
<td>R9. The MDM agent should control installation, removal, execution and stop the applications.</td>
</tr>
<tr>
<td>R10. The MDM agent should detect and prevent modification of operating system.</td>
</tr>
</tbody>
</table>

3 Security Evaluation

3.1 Evaluation Items and Processes

Our proposed evaluation criteria contain 15 key evaluation items. Table 2 shows these evaluation items. In Table 2, ‘SR’ means security requirements.

<table>
<thead>
<tr>
<th>Evaluation Item</th>
<th>SR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item1. Encrypted communication between the MDM agent and the server.</td>
<td>R1</td>
</tr>
<tr>
<td>Item2. Management of server access profile.</td>
<td>R2</td>
</tr>
<tr>
<td>Item3. Periodical check of connectivity</td>
<td>R3</td>
</tr>
<tr>
<td>Item4. User authentication</td>
<td>R4, R8</td>
</tr>
<tr>
<td>Item5. Device lock before user authentication</td>
<td>R4</td>
</tr>
<tr>
<td>Item6. Integrity of configuration and audit data</td>
<td>R5</td>
</tr>
<tr>
<td>Item7. Hardware control</td>
<td>R6</td>
</tr>
<tr>
<td>Item8. Bypassing path</td>
<td>R6</td>
</tr>
<tr>
<td>Item9. Encryption of confidential data</td>
<td>R7</td>
</tr>
<tr>
<td>Item10. Remote locking or wiping</td>
<td>R7</td>
</tr>
<tr>
<td>Item11. Encryption key &amp; cryptographic data management</td>
<td>R7</td>
</tr>
<tr>
<td>Item12. Countermeasure of authentication failure</td>
<td>R8</td>
</tr>
<tr>
<td>Item13. MDM agent removal/stop restriction</td>
<td>R9</td>
</tr>
<tr>
<td>Item14. Application installation/removal/execution/stop restriction</td>
<td>R9</td>
</tr>
<tr>
<td>Item15. Detection of the OS modification</td>
<td>R10</td>
</tr>
</tbody>
</table>

3.2 Test Methods for Android Devices

In this subsection, we propose the tools and test methods for Android devices although there are many tools for various operating systems and devices.

**Sniffing and analyzing packets.** We can collect packets by mirroring or tapping. We can also capture outbound packets from the rooted device by ‘Shark for root [1]’.
Exploring and editing files. In order to access and modify the system directories and files, we can use ‘Root explorer [1]’, ‘Android Debug Bridge (ADB) [2]’, ‘Dalvik Debug Monitor Service (DDMS) [2]’ after rooting.

Executing commands. Using ADB, we can transfer files, install applications, uninstall applications, and so on. In particular, we can execute various shell commands on the rooted device.

Decompiling source codes. Generally, the source codes of application are not provided to the evaluator. Fortunately, we can easily decompile Android applications since the applications are developed based on Java programming language. Using ‘Dex2jar [3]’, we can convert an APK file to a JAR file.

Editing database. Android uses SQLite database to store data. We can use ‘Sqlite editor [1]’ to find `.db` files and edit them. If we modify the configuration of mobile device we can use restricted functions of mobile device.

Forensic analysis. Forensic tools are used to recover the deleted data. So, we can use forensic tools to check the device is correctly wiped.

Rooting and managing permission. In Android, the evaluator can get the root permission after rooting the device. By obtaining root permission, the evaluator can access system folders or files and execute commands which are restricted to a user. In order to use applications which need the root permission, we can use ‘Superuser [1]’ application.

4 Conclusion

In this paper, we proposed the first evaluation criteria for the MDM agent. The proposed evaluation items can be used for various platforms. In addition, they can be reused and extended to evaluate security of other applications on mobile devices. By evaluating an MDM agent according to the proposed practical criteria and methods, the security of the MDM agent will be improved. And improving security of the MDM agent will strengthen the security of the mobile devices.

References

Improved Password-Authenticated Key Agreement Using Smart Cards

Kai Chain¹, Wen-Chung Kuo², Chun-Pei Hsiang³, Jiin-Chiou Cheng³, Jar-Ferr Yang¹

¹ Institute of Computer and Communication Engineering, Department of Electrical Engineering, National Cheng Kung University, Taiwan, R.O.C.
chainkai@crypto.ee.ncku.edu.tw
jfyang@ee.ncku.edu.tw

² Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Taiwan, R.O.C.
simonkuo@yuntech.edu.tw

³ Department of Computer Science and Information Engineering, Southern Taiwan University, Taiwan, R.O.C.
{m99g0105, chiou}@webmail.stut.edu.tw

Abstract. Using smart cards for authentication has become a common trend. Although this system brings conveniences, it also increases the risk in the case of lost cards. In this paper, we analyze the lost smart card attack from Juang et al.’s scheme [4] that proposes password authenticated key agreement. In order to bolster the security of the entire system, we mitigated some of its weaknesses.

Keywords: key exchange, elliptic curve cryptosystem, smart card, authentication.

1 Introduction

In 2008, Juang et al. (for short JCL-scheme)[4], point out the major drawbacks are loss of anonymity for the user and high computation and communication cost in Fan et al.’s scheme. To improve upon these drawbacks, Juang et al. proposed a scheme that not only can provide identity protection but also keep lower communication and computation cost by using elliptic curve cryptosystems. They also proposed a solution for minimizing the risk of lost cards. The use of a fixed server key allows an offline attack to be mounted against the server key when an attacker possesses the user card. Therefore, we propose to improve JCL-scheme and mitigate the exposure of the entire system when a smart card is compromised.

2 Review and Analysis of the JCL-scheme

A review and analysis of the JCL-scheme is given in this section.
2.1 The JCL-scheme

The JCL-scheme consists of five phases: parameter generation, registration, pre-computation, log-in, and the password-changing phase. Due to space limitation, if the readers want to understand the JCL-scheme deeply, please refer to [4].

2.2 Security Analysis of the Juang et al. Scheme

The system may be compromised by extracting information from the smart card in order to falsify server authentication. Specifically, in the case of known ID_i and C_i (these messages are stored on the smart card), the attacker will attempt to solve \( V_i = h(ID_i, s, C_i) \). The attacker can seek out the secret server key \( s \) using offline attack. After the secret value \( s \) is known, the attacker can freely tamper with the internal value of \( b_i \), compromising the security of the entire system.

3 The Proposed Scheme

We improve on JCL-scheme and propose an enhanced password-authentication key agreement scheme in this paper. This scheme not only maintains all the benefits of the JCL-scheme but also can enhance the security of the server when the smart card contents are disclosed. Our proposed scheme also consists of the same four phases: parameter generation, registration, pre-computation and log-in.

(i). Parameter Generation Phase:

1. The server selects three numbers: a larger prime number \( P \) and \( a \in \mathbb{Z}_P \) and \( b \in \mathbb{Z}_P \) must satisfy \( 4a^3 + 27b^2 \pmod{P} \neq 0 \), and \( E_P : y^2 = x^3 + ax + b \).
2. The server generates a point \( G \) from order \( n \) and satisfies \( O \cdot G = n \).
3. The server selects \( x_s \) as the private key, and the public key is \( P_S = (x_s \cdot G) \).
4. The server publishes the parameters \( (P_S, P, E_P, G, n) \).

(ii). Registration Phase:

The user can use the smart card to send identification information for the server to authenticate.

Step 1 The smart card chooses \( b \) and calculates \( T_1 = h(PW_i || b^{-1}) \). Then the smart card sends \( \{ID_i, h(PW_i || b), T_1\} \) to the server.

Step 2 The server chooses \( S_2 \) and computes \( T_2 = T_1 \cdot S_2^{-1} \), \( V_i = h(ID_i, T_1, C_i) \) and \( b_i = E_i(h(PW_i || b)||T_2||ID_i||C_i||h(ID_i||C_i||h(PW_i||b))) \).

Step 3 The user receives \((ID_i, C_i, b_i, V_i)\) and then stores these parameters and \( b \) into the smart card.

(iii). Pre-computation Phase:

The smart card chooses a random number \( r \) and calculates \( e = (r \times G) \) and \( c = (r \times P_S) = r \times x \times G \). Then \( e, c \) is stored in card memory for use in the log-in phase.

(iv). Log-in Phase:

The user \( i \) wants to login to the server and must use his own smart card and password.

Step 1 After calculating \( E_{V_i}(e) \), the smart card sends \( E_{V_i}(e) \) and \( b_i \) to the server.

Step 2 The server obtains \((T_2||ID_i||C_i||h(PW_i||b)), T_1 = T_2 \times S_2 \) and \( V_i = h(ID_i, T_1, C_i) \).

Then, the server chooses \( u \) and computes \( c = (e \times x) = (r \times x \times G), M_S = h(c || u || V_i) \).
Step 3 The smart card calculates and checks $M_S$. If $M_S$ is true, the smart card calculates $M_U = h(h(PW_i||b))||T_1||c||u)$ and $S_k = h(V,c,u)$. 
Step 4 Obtain a session key $S_k = h(V,c,u)$ when $M_U$ is true.

4 Security Analysis and Comparison

The following table compares the properties of the proposed scheme and previous schemes. Where C1: low communication and computation cost; C2: users can choose the passwords; C3: no time-synchronization problem; C4: mutual authentication; C5: identity protection; C6: session key agreement; C7: preventing offline dictionary attack against the smart card information.

Table 1: Properties of the proposed scheme versus previous schemes

<table>
<thead>
<tr>
<th></th>
<th>Hwang &amp; Li scheme</th>
<th>Juang scheme</th>
<th>Fan et al. scheme</th>
<th>Sun scheme</th>
<th>Chien et al. scheme</th>
<th>Juang et al. scheme</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C2</td>
<td>X</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C3</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C5</td>
<td>X</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C6</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>C7</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

5 Conclusion

In our scheme, even if the attacker holds the user’s card, and mounts an offline attack to obtain the server key, it will not result in risk to the entire system. We use Juang et al.’s mechanism to revoke cards and ensure the privacy of the user. Possession of a smart card does not allow knowledge of the second secret key in the server, so the attacker cannot break the security of the system.

Acknowledgment: This work was supported by NSC 100-2221-E-224-016.

References

An Off-Line Dictionary Attack on Abdalla and Pointcheval’s 3-Party Key Exchange Protocol

Junghyun Nam1, Jinsoo Kim1, Juryon Paik2, and Dongho Won2**

1 Department of Computer Engineering, Konkuk University, Korea
{jhnam,jinsoo}@kku.ac.kr
2 Department of Computer Engineering, Sungkyunkwan University, Korea
wise96@ece.skku.ac.kr, dhwon@security.re.kr

Abstract. Protocols for authenticated key exchange are of fundamental importance in building a secure communication channel over a public insecure network. In this work, we are concerned with the security of Abdalla and Pointcheval’s protocol for password-authenticated key exchange in the three-party setting. We first show that Abdalla and Pointcheval’s protocol is vulnerable to an off-line dictionary attack whereby a malicious client can find out the passwords of other clients. We then present how to eliminate the security vulnerability of the protocol with no performance degradation.

Key words: Security, key exchange protocol, password, dictionary attack.

1 Introduction

In 2005, Abdalla and Pointcheval proposed a simple three-party PAKE protocol [1], which we denote by AP-3PAKE. The AP-3PAKE protocol is very efficient both in terms of computation and communication complexities, and requires no use of cryptographic keys like server’s public/private keys. Although the claimed proof of security for AP-3PAKE was found to be invalid [2], there have been so far no known dictionary attacks against the protocol. In this paper, we reveal the vulnerability of AP-3PAKE to an off-line dictionary attack. Due to the vulnerability, the AP-3PAKE protocol should not be deployed in its current form. This paper also presents how to make AP-3PAKE immune against the off-line dictionary attack.

2 The AP-3PAKE Protocol

This section revisits the AP-3PAKE protocol, Abdalla and Pointcheval’s three-party PAKE protocol [1]. The protocol participants consist of a single server S

* This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0018397).
** The corresponding author: Dongho Won (e-mail: dhwon@security.re.kr).
The followings are the public system parameters used in the A and two clients S.

\[ x \in \mathbb{Z}_q, X = g^x \]
\[ pw_{A,1} = G_1(A, B, pw_A) \]
\[ X^* = X \cdot pw_{A,1} \]
\[ y \in \mathbb{Z}_q, Y = g^y \]
\[ pw_{B,1} = G_1(A, B, pw_B) \]
\[ Y^* = Y \cdot pw_{B,1} \]

![Fig. 1. Abdalla and Pointcheval’s three-party PAKE protocol](image)

The clients A and B wish to establish a session key between them while the server S exists to provide the clients with authentication services. Let \( pw_A \) and \( pw_B \) be the passwords of A and B, respectively. Each client’s password is assumed to be shared with the authentication server S via a secure channel. The followings are the public system parameters used in the protocol.

- A finite cyclic group \( \mathbb{G} \) of prime order \( q \) and a random generator \( g \) of the group \( \mathbb{G} \).
- A hash function \( H \) modeled as a random oracle. The outputs of \( H \) are \( \ell \)-bit strings, where \( \ell \) is a security parameter representing the length of session keys.
- Two hash functions \( G_1 \) and \( G_2 \) modeled as random oracles. The outputs of \( G_1 \) and \( G_2 \) are the elements of the cyclic group \( \mathbb{G} \).
With the passwords and the parameters established, the AP-3PAKE protocol proceeds as shown in Fig. 1.

3 An Off-Line Dictionary Attack

The AP-3PAKE protocol seems to be secure against off-line dictionary attacks if we only consider honest clients who stick to the protocol specification. But in the 3-party setting, there may be malicious clients who deviate from the protocol. Indeed, the existence of insider attacks by malicious clients is one of the major differences between the 2-party and the 3-party settings. We here show that AP-3PAKE is not secure against an off-line dictionary attack in the presence of a malicious client.

Our attack exploits the fact that, once the session key $SK$ has been established, the clients $A$ and $B$ will exchange their subsequent messages that are generated using the key $SK$. Let $msg_{SK}$ be the first such message. Without loss of generality and for simplicity, we assume that it is the client $A$ who generates/sends $msg_{SK}$. Then, our off-line dictionary attack can be mounted by $B$ against $A$’s password. (We stress that our attack also works even when $msg_{SK}$ is generated/sent by $B$. In this case, the attack can be mounted by $A$ against $B$’s password.) Due to space limitation, the detailed description of the attack will be given in the full version of this paper.

4 Security Improvement

We finally present a simple countermeasure against the off-line dictionary attack described above. Our idea is to use a block cipher in encrypting $X$ and $Y$ as well as $X$ and $Y$. Consider a block cipher $E : \{0, 1\}^\kappa \times \mathcal{G} \rightarrow \mathcal{G}$. Each key $k \in \{0, 1\}^\kappa$ defines a permutation $E_k = E(k, \cdot)$ on $\mathcal{G}$. Let $D_k$ denote the inverse of $E_k$. Generation of keys for the cipher will make use of a hash function $G : \{0, 1\}^* \rightarrow \{0, 1\}^\kappa$. We will give the details of the improvement in the full version of this paper.

References

Gesture Recognition based on 2D and 3D Feature by using Kinect Device

Wenkai Xu, Eung Jo Lee

Department of Information & Communications Engineering, Tongmyong University, Busan, Korea
xwk6298@hotmail.com, ejlee@tu.ac.kr

Abstract. Human gesture recognition is a non-verbal part for interaction or movement that can be used to involves real world and virtual world. In this paper, we explain a study in human gesture recognition using RGB color information and depth information by Kinect camera from Microsoft Corporation. To achieve the goal, hand tracking and gesture recognition have no major dependencies of the work environment, lighting or users’ skin color, libraries of particular use for natural interaction and Kinect device, which serves to provide RGB images of the environment and the depth map of the scene were used. An improved Camshift tracking algorithm combined with depth information is used to tracking hand motion, and then an associative method of HMM and FNN is propose for gesture recognition step. The experimental results show out its good performance and it has higher stability and accuracy as well.

Keywords: Camshift, depth information, gesture recognition, Kinect

1 Introduction

Massive technology shift has played a dominant role in all disciplines of science and technology. The use of hand gesture is an active area of research in the vision community, mainly for the purpose of sign language recognition and Human-Computer Interaction (HCI). The history of interaction and interface design is a flow and step from complex interaction to simple interaction between human and computer [1]. The word natural interaction came from Natural User Interface (NUI) that use human body interaction and voice interaction, verbal and non-verbal communication, becoming a one of Human-Computer Interaction (HCI) area. It is an evolution from Graphical User Interface (GUI).

In this paper, An improved Camshift tracking algorithm combined with depth information is used to tracking hand motion by Kinect, and then an associative method of HMM and FNN is propose for gesture recognition step, which combines ability of HMM model for temporal data modeling with that of fuzzy neural network for fuzzy rule modeling and fuzzy inference.
2 Hand Tracking and Recognition

Because the Camshift algorithm is based on color images, tracking error will easily occur when there is similar color in background. Considering the object is usually separated from the surrounding environment in depth, and has fixed moving range, so threshold segmentation in depth map can accurately distinguish the player from the background. According to reference [2], we combined depth information with traditional Camshift tracking algorithm by using Kinect. Gesture Recognition Using Improved HMM Algorithm

Choosing suitable features to recognize the hand gesture path play significant role in the whole system. There are three basic features: location, orientation and velocity. The previous research [3, 4] showed that the orientation feature is the best in term of accuracy results. Therefore, we regard the orientation feature as the main feature during our research process. Based on the research above, a gesture path is spatiotemporal pattern which consists of centroid point. So, the orientation is determined by the change between two consecutive points from hand gesture path [5].

Fuzzy Neural Network has strong ability for fuzzy rule modeling and fuzzy inference due to its integration of fuzzy set theory and Neural Network together. Since traditional FNN cannot model temporal data and conventional HMM do not own ability for fuzzy inference, we integrate the two models together to represent complex gesture trajectory and perform inference by the integrated HMM-FNN model based on [6] [7] [8], which is shown in Fig.4, for the recognition of dynamic gesture.

HMM-FNN model includes five layers. Its first layer, second layer and HMM layer constitute the fuzzy preprocessing part, third layer and fourth layer constitute fuzzy inference part, fifth layer is the defuzzification part of HMM-FNN and produce distinct output. The following will introduce these five layers in detail.

3 Experimental results

In our experiments, the fuzzy rules, with a total number of characters, are obtained by data clustering combined with human experiences. The initial connecting weights are also set by people’s prior knowledge about dynamic gestures. For each dynamic gesture, we ask each of 5 testers to perform it 5 times, and then get 25 video sections. As a result, there are totally 125 samples for all 5 kinds of gestures, 100 of which are used for model training and the others are for testing. When the error of testing is below the threshold or training times reach its maximum, the model is considered well-trained.

4 Conclusion

In this paper, we propose an automatic system to recognize gestures in real-time. At first, an improved Camshift tracking algorithm combined with depth information is
used to tracking hand motion; Next, HMM-FNN model is proposed for gesture recognition, which combines ability of HMM model for temporal data modeling with that of fuzzy neural network for fuzzy rule modeling and fuzzy inference. The experimental results show out its good performance and it has higher stability and accuracy as well. In the future work, we will study about complex gesture recognition using Kinect for reflecting the methodology we proposed better and making more abundant controlling contents for NUI.

Acknowledgement. This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the IT/SW NHN Program supervised by the NIPA (National IT Industry Promotion Agency)” (NIPA-2011-C1820-1102-0010).

Reference

Learning System for SQL Injection Detection Using Syntax and Semantic Kernel in Support Vector Machine

Yi Wang¹, Zhoujun Li¹

¹ State Key Laboratory of Software Development Environment, Beihang University
100191 Beijing, China
{wangyi160@hotmail.com, lizj@buaa.edu.cn}

Abstract. Modern web application systems are generally consisted of database systems in order to process and store business information. These systems are highly interesting to hackers as they contain sensitive information and the diversity and amount of attacks severely undermine the effectiveness of classical signature-based detection. In this work we propose a novel approach for learning SQL statements and apply machine learning techniques, such as one class classification, in order to detect malicious behavior between the database and application. The approach incorporates the tree structure of SQL queries as well as input parameter and query value similarity as characteristic to distinguish malicious from benign queries. We develop the learning system integrated in PHP and demonstrate the usefulness of our approach on real-world application.

Keywords: sql injection, web security, machine learning, support vector machine, kernel tricks

1 Introduction

The majority of today’s web-based applications does employ the multi-layer infrastructure and rely heavily on database storage for information processing. A lot of attacks against web-applications are aimed at injecting commands into database systems in order to gain unprivileged and access to sensitive records stored in these systems. The approach of protecting web application is by introducing detection models on the network layer firewall systems.

Besides pattern based approaches, there exists a variety of research on employing anomaly based methods for detecting web-based intrusions or program analysis on source code of target web application[1,2,3,4,5,6,7,8]. The main contribution of our work is the use of both syntax and semantic based analysis, i.e. tree-vector-kernel based learning, which became popular within the field of natural language processing (NLP). Our approach incorporates the parse tree structure of SQL queries as well as input parameter and query value similarity characteristic to distinguish malicious from benign queries. By applying this kernel trick into the SVM(support vector machine) classifier, we can determine abnormal query accurately and efficiently.
2 Kernel function for SQL query

The kernels between corresponding pairs of trees and/or vectors in the input sequence are summed together.

\[ K_x(o_1, o_2) = \tau \times \sum_{i=1}^{\min(n,n')} k_x(T_i, T'_i) + \sum_{i=1}^{\min(n,n')} k_b(v_i, u_i) \]  

(1)

2.1 Tree kernel function

The main idea of tree kernels is to compute the number of the common sub-structures between two trees \( T_1 \) and \( T_2 \) without explicitly considering the whole fragment space. For this purpose, we need to define the tree kernel function in order to compute the similarity of two trees.

\[ K_f(T_1, T_2) = \sum_{n_1 \in N_{T_1}} \sum_{n_2 \in N_{T_2}} \Delta_k(n_1, n_2) \]  

(3)

where \( N_{T_1} \) and \( N_{T_2} \) are the sets of the \( T_1 \)'s and \( T_2 \)'s nodes, respectively. By adopting the concept of tree kernel from (ECAL 2006), we can define

\[ \Delta_k(n_1, n_2) = \begin{cases} 0 & \text{if } \prod(n_1) \neq \prod(n_2) \\ \lambda & \text{if } \text{height}(n_1) = \text{height}(n_2) = 1 \\ \lambda \prod_{j=1}^{\left| n_1 \right|} (\sigma + \Delta(c_{n_1}^j, c_{n_2}^j)) & \text{otherwise} \end{cases} \]  

(4)

where \( \lambda \) is the decay factor and \( \sigma \in [0,1] \) is the counting factor, \( |n| \) is the number of the children of node, for the last condition, \( |n_1| \neq |n_2| \).

2.2 Vector kernel function

The best-known character-based string similarity metric is Levenshtein distance(LD). In order to make measurement for similar strings bigger than different strings, we define:

\[ \Delta_b(u, v) = \frac{1}{\text{LD}(u, v)} \]  

(5)

By making input-query value pair \( P = \{ \Delta_b(u_1, v_1), \Delta_b(u_2, v_1), \ldots, \Delta_b(u_n, v_n) \} \), we can define vector kernel to calculate the similarity:

\[ K_b(P, P') = \sum_{i=1}^{\left| P \right|} \text{Gaussian}(P_i, P'_i) \]  

(6)

Where \( |P|=|P'| \) Gaussian(…) is the Gaussian radial basis function:

\[ \text{Gaussian}(x_i, x_j) = \exp(-\gamma \cdot \| x_i - x_j \| ^2), \gamma > 0 \]  

(7)
3 System design and evaluation

We present our prototype system SQL LEARN as a mysqlnd extension integrated in PHP interpreter. It functions as a SQL proxy with the ability of query learning and anomaly detection between PHP application and Mysql database. Several vulnerable PHP content management system applications are tested within this framework, the results show that our system can provide accurate and complete protection against SQL injection attacks.

Moreover, we compare the tree-vector kernel with tree and vector kernel alone to show that the combination kernel surpass any singleton kernel and obtain the best result. This reflect the fact that both syntax and application context play important role in the detection of malicious SQL injection.

4 Conclusion

We presented an approach using tree-vector-kernels in SVM for SQL statements to prevent SQL injection in web applications. The results confirm the benefit of incorporation of syntax information of query and semantic context from application in analyzing SQL queries. Compared to previous approaches, the combination gains more accuracy than using syntax or context analysis alone as it brings more information into classification.

References

A New Method for Key Sharing in Wireless Mesh Networks

Peng Xiao¹, Jingsha He², and Yingfang Fu³

¹ College of Computer Science and Technology, Beijing University of Technology
Beijing 100124, China
xp4523@emails.bjut.edu.cn

² School of Software Engineering, Beijing University of Technology
Beijing 100124, China
jhe@bjut.edu.cn

³ Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China
fuyingfang@bjut.edu.cn

Abstract. Combining the advantages of WLANs and ad hoc networks, wireless mesh networks (WMNs) are wireless access networks based on IP technologies and have become effective broadband access networks with high capacity, high speed and wide coverage. Security is a crucial and urgent problem in WMNs as in other types of networks and a simple and effective distributed key management is essential for the establishment of secure WMNs. In this paper, we present an effective distributed key management scheme based on several technologies, such as ad hoc network model, ECC, \((t, n)\) threshold cryptographic method, verifiable secret sharing and so on.

Keywords: Wireless mesh networks; distributed key management; cheater identification; ECC; cryptography

1 Introduction

Combining the advantages of WLANs and ad hoc networks, WMNs are wireless broadband access networks completely based on IP packet networks and have quickly become effective broadband access networks with high capacity, high speed and wide coverage. Security is a crucial and urgent problem in WMNs as in any other types of networks [1]. A simple and effective distributed key management is crucial for the establishment of secure WMNs.

2 Related Work

Hong et al. proposed an efficient key distribution scheme with self-healing property, which is optimal in terms of user memory storage and more efficient in terms of communication complexity [2]. IEEE P802.11s™/D1.01 provides efficient mesh security association (EMSA) [3] based on the IEEE 802.11i standard in which the
802.1x scheme and four handshakes are used to implement access authentication and key establishment. Fu et al. proposed a mutual authentication in WMNs [4] based on a \((t, n)\) cryptography method but without verifiable secret sharing. Duan et al. proposed an efficient location-based compromise-tolerant key management scheme for sensor networks based on sensor deployment and localization [5]. Dahshan et al. proposed an elliptic curve distributed key management scheme for mobile Ad Hoc networks based on ECDLP and \((t,n)\) threshold cryptography [6]. But they are all suitable for certain type of networks only and don’t support cheater identification for locating the malicious node. In relatively complex hybrid WMNs, they need to be improved to adapt to the networks.

3 Distributed Group Key Management

In this paper, we use traditional Lagrange interpolation to implement secret key sharing and elliptic curve cryptography (ECC) to generate authorized certificates.

3.1 Cheater Detection

In the initial stage of key establishment in our scheme, a public key piece \((d_0, SK_0)\) generated by the offline CA is broadcast to the whole network. When \(t\) key pieces are collected, a new matrix equation \(D' \cdot A' = S'\) is established,

\[
D' = \begin{bmatrix}
  d^{-1} & \cdots & d_1 & 1 \\
  d^{-1} & \cdots & d_2 & 1 \\
  \vdots & \vdots & \vdots & \vdots \\
  d^{-1} & \cdots & d_{t-1} & 1 \\
  d^{-1} & \cdots & d_0 & 1
\end{bmatrix},
\quad
A' = \begin{bmatrix}
  a_{t-1} \\
  a_{t-2} \\
  \vdots \\
  a_0
\end{bmatrix},
\quad
S' = \begin{bmatrix}
  SK_1 \\
  SK_2 \\
  \vdots \\
  SK_t
\end{bmatrix},
\quad
\text{and} \quad \overline{D}' = \begin{bmatrix}
  d^{-1} & \cdots & d_1 & 1 & SK_1 \\
  d^{-1} & \cdots & d_2 & 1 & SK_2 \\
  \vdots & \vdots & \vdots & \vdots & \vdots \\
  d^{-1} & \cdots & d_{t-1} & 1 & SK_t \\
  d^{-1} & \cdots & d_0 & 1 & SK_0
\end{bmatrix}
\]

At the moment, we can deduce that \(R(\overline{D}) = R(D) \leq t + 1\). So,

1. If \(R(\overline{D}) = R(D) < t\), there are more than one solutions for the equation. So, more key pieces need to be gathered to get the unique solution until \(R(\overline{D}) = R(D) = t\).

2. If \(R(\overline{D}) = R(D) = t\), there is a unique solution for the equation. So, a correct secret key \(SK\) will be reconstructed.

3. If \(R(\overline{D}) = R(D) = t + 1\), there is no feasible solution for the equation. So, there exists at least one incorrect key piece in the participants. Hence, a cheater is detected.

3.2 Cheater Identification

Once detected, the cheater must be identified. When a new participant is acquiring a key piece from an existing participant, the latter must deliver its own key piece along
with its digital signature to the former. So, after the new participant has collected $t$ key pieces and found a cheater in the network, as described in the last section, it will broadcast a request to arouse the offline CA. Then, it will deliver all the collected key pieces with its digital signature to the offline CA. The CA can verify which key pieces are incorrect through the pre-selected $(t-l)$-degree polynomial $f(x)$ and which participants are dishonest through their registered certificates.

4 Conclusions

We presented an effective distributed key management scheme for the establishment of a secure WMN in this paper, which is based on several technologies, such as ad hoc network model, ECC, $(t, n)$ threshold cryptographic, verifiable secret sharing. In the future, we will consider distributed key management in the handoff and roaming scenario in WMNs to further improve our protocol [7].

References

The Design of a Novel Signature Scheme Based on the SIS Problem

Yanqing Yao*, Zhoujun Li, and Hua Guo
State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China
School of Computer Science and Engineering, Beihang University, Beijing, China
yaoyanqing1984@sina.com, lizj@buaa.edu.cn, hguo@buaa.edu.cn

Abstract. Network coding signature schemes can be employed to prevent malicious modification of data in network transition. But existing network coding signature schemes are only suitable for linear network coding. To adapt to nonlinear network coding, in this paper we introduce the concept of nonlinear network coding signature scheme and its unforgeability, and propose a unforgeable nonlinear network coding scheme based on the hardness of the small integer solution (SIS) problem in lattice-based cryptography. The scheme in this paper can be used to provide cryptographic protection in nonlinear network coding.

Key words: nonlinear network coding signature scheme, the small integer solution problem, lattice-based cryptography

1 Introduction

Signature scheme is a basic cryptographic tool in network security. In contrast to traditional “store-and-forward” routing, network coding [1] is related to a general class of routing mechanisms where intermediate nodes modify data packets in transit. In a signature scheme, every file is bound with an identifier $id$ that is chosen by the sender when the first packet associated with the file is transmitted. The identifier provides a mechanism for honest nodes, and especially the receiver, to distinguish packets associated with different files [1]. Nowadays, network coding has been suggested for applications in wireless and/or ad-hoc networks. However, the signature schemes in previous literature are only suitable for linear network coding with homomorphic signature scheme [1,2] because of its strong verification requirement. Nowadays, nonlinear network coding has aroused scholars’ interest [4,5]. To provide cryptographic protection against pollution attacks,
we will propose the concepts of nonlinear network coding signature scheme and its unforgeability and present a secure nonlinear network coding scheme.

2 Preliminaries

In this section, we propose the concepts of nonlinear network coding signature scheme and its unforgeability. The scheme can be used to prevent adversary’s attacks such as corrupting an arbitrary number of nodes in the network, eavesdropping on all network traffic, and inserting or modifying an arbitrary number of packets.

Definition 1. A nonlinear network coding signature scheme for a message space \( \mathcal{M} \) is defined by a triple of probabilistic, polynomial time algorithms, \((\text{Gen}, \text{Sign}, \text{Verify})\) with the following functionality:

- **Gen**: On input a security parameter \( 1^n \) (in unary) and additional public parameters \( \text{params} \) that include the length of a vector to be signed, this algorithm outputs a public key \( \text{pk} \) and a secret key \( \text{sk} \).

- **Sign**\((sk, \mu, id)\): On input a secret key \( sk \), an identifier \( id \) that is an element of a randomly samplable set \( \mathcal{I} \), and a vector \( \mu \in \mathcal{M} \), this algorithm outputs a signature \( \sigma \).

- **Verify**\((pk, id, \mu, \sigma)\): On input verification key \( pk \), an identifier \( id \in \mathcal{I} \), a message \( \mu \), and a signature \( \sigma \), this algorithm outputs either 0 (reject) or 1 (accept).

We require that for each \((pk, sk)\) output by \( \text{Gen} \), the following holds: for all \( \mu \in \mathcal{M} \) and for all \( id \in \mathcal{I} \), if \( \sigma \leftarrow \text{Sign}(sk, \mu, id) \), then \( \text{Verify}(pk, id, \mu, \sigma) \) should accept with overwhelming probability.

3 The nonlinear network coding signature scheme

In this section, based on the signature scheme in [3], we construct a nonlinear network coding signature scheme. Compared to the signature scheme in [3], the identifiers are added. Accordingly, the prime \( q \) in [3] has been changed into \( 2q \) in the corresponding positions, and the verification items have been changed.

- a dimension \( m = O(n \log 2q) \) and a bound \( L = O(\sqrt{n \log 2q}) \).

- a (hashed) message length \( k \) inducing a ‘total dimension’ \( m' = m \cdot (k + 1) \).

- a Gaussian parameter \( s = L \cdot \omega(\sqrt{\log n}) \).

The nonlinear network coding signature scheme (NSIG) is defined as follows:

- **Gen**: generate \((A_0; S_0) \leftarrow \text{GenBasis}(1^n; 1^m; 2q)\), where \( A_0 \in \mathbb{Z}_{2q}^{n \times m} \) is negligibly close to uniform and \( S_0 \) is a basis of \( A^\perp_0 \) with \( ||S_0|| \leq L \). Let \( F : \{0, 1\}^n \rightarrow \mathbb{Z}_2^k \) be a one to one mapping. Then for each \((b, j) \in \{0, 1\} \times [k]\), choose uniformly random and independent \( A_{j(b)} \in \mathbb{Z}_{2q}^{n \times m} \). Output \( pk = (A_0, \{A_{j(b)}\}; F) \) and \( sk = (S_0; pk) \).

- **Sign**\((sk, \mu \in \{0, 1\}^k, id \in \{0, 1\}^n)\): Let \( A_{\mu} = A_0|A_{\mu(1)}| \cdots |A_{\mu(k)} \). Output \( \sigma \leftarrow D_{A_{\mu}, F(id); s} \), via \( \sigma \leftarrow \text{SampleD}(\text{ExtBasis}(S_0, A_{\mu}); q \cdot F(id); s) \).
In the rare event that $||\sigma|| > s \cdot \sqrt{m'}$, resample $\sigma$.

- **Verify** $(pk, id, \mu, \sigma)$: let $A_\mu$ be as above. Accept if $||\sigma|| \leq s \cdot \sqrt{m'}$, and $A_\mu \cdot \sigma \equiv q \cdot F(id) (mod 2q)$; else, reject.

**Correctness**: Denote the output of $\text{ExtBasis}(S_0, A_\mu)$ as $S$, we have $||\tilde{S}|| = ||\tilde{S}_0||$. Combining $s = \tilde{L} \cdot \omega(\sqrt{\log n})$ and $||\tilde{S}_0|| \leq \tilde{L}$, we have $s \geq ||\tilde{S}|| \cdot \omega(\sqrt{\log n})$.

Then from Lemma 2.4 of [3] we conclude that the vector $\sigma$ output by the $\text{Sign}$ algorithm satisfies $A_\mu \cdot \sigma \equiv q \cdot F(id) (mod 2q)$ and is drawn from a distribution statistically close to $A_\mu \cdot \sigma \equiv q \cdot F(id) (mod 2q)$.

By Lemma 2.4 of [3] we conclude that $||\sigma|| \leq s \cdot \sqrt{m'}$ with overwhelming probability.

Now we prove unforgeability of our nonlinear network coding signature scheme. Given an adversary that breaks the signature scheme for a message space $\{0, 1\}^k$ and an identity space $\{0, 1\}^n$, we construct an adversary that simulates the signature scheme and solves the $\text{SIS}_{q, \beta}$ problem.

**Theorem 1.** Let $\mathcal{N}$ be the nonlinear network coding signature scheme described above. Suppose that $\beta = s \cdot \sqrt{m'}$. Then $\mathcal{N}$ is unforgeable assuming that the $\text{SIS}_{q, \beta}$ problem is infeasible. In particular, let $A$ be a polynomial-time adversary and make at most $Q$ signature queries. Then there exists a probabilistic polynomial-time algorithm $B$ that solves the $\text{SIS}_{q, \beta}$ problem, such that

$$\text{Adv}_{\text{SIS}_{q, \beta}}(B) \geq \left[1 - \frac{1}{2} \left(\frac{Q}{2^k} + \frac{Q - 1}{2^k - 1}\right) \cdot \frac{1}{k \cdot Q - g_Q} \text{Adv}_{\text{NSIG}}(A) - \text{negl}(n)\right].$$

**Proof.** It can be proved by employing the Chinese remainder theorem and the technique proposed by David Cash et.al. in EUROCRYPT 2010.

**References**

Interleaving and Collusion Attacks on a Dynamic Group Key Agreement Scheme for Low-Power Mobile Devices

Junghyun Nam\textsuperscript{1}, Juryon Paik\textsuperscript{2}, Jeeyeon Kim\textsuperscript{2}, Youngsook Lee\textsuperscript{3}, Woongryul Jeon\textsuperscript{2}, and Dongho Won\textsuperscript{2}\textsuperscript{**}

\textsuperscript{1} Department of Computer Engineering, Konkuk University, Korea \texttt{jhnam@kku.ac.kr}
\textsuperscript{2} Department of Computer Engineering, Sungkyunkwan University, Korea \texttt{wise96@ece.sku.ac.kr, jeeyeonkim@paran.com,\{wrjeon,dhwon\}@security.re.kr}
\textsuperscript{3} Department of Cyber Investigation Police, Howon University, Korea \texttt{ysooklee@howon.ac.kr}

Abstract. This paper investigates the security of Bresson et al.’s dynamic group key agreement scheme for low-power mobile devices. Bresson et al.’s scheme consists of three protocols — the setup protocol, the join protocol, and the remove protocol — which are designed to minimize the cost of the rekeying operations associated with group updates. The protocols of the scheme were claimed to be provably secure against active adversaries. In this paper, we show that this claim is not necessarily true but in fact, none of the protocols are secure in the presence of an active adversary. We demonstrate this by mounting interleaving attacks on the setup and join protocols and mounting a collusion attack on the remove protocol.

Key words: Key agreement, dynamic group, wireless communication, interleaving attack, collusion attack.

1 Introduction

In this paper, we revisit the dynamic group key agreement scheme proposed by Bresson et al. [1]. This scheme is not only simple and efficient but also well suited for unbalanced networks consisting of devices with strict power consumption restrictions and wireless gateways with less stringent restrictions. The proposed scheme consists of three protocols: the setup protocol GKE.Setup, the remove protocol GKE.Remove, and the join protocol GKE.Join. The main GKE.Setup protocol allows a set of mobile devices (also called clients) and a wireless gateway (also called server) to agree on a common secret key called a session key. To meet

* This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0018397).

** The corresponding author: Dongho Won (e-mail: dhwon@security.re.kr).
the efficiency needs of clients, the protocol shifts most of computational burden to the gateway and provides mobile devices with the ability to perform public-key cryptography operations off-line. The other protocols of the scheme allow the server to efficiently handle dynamic membership changes of clients within a wireless domain.

Although Bresson et al.’s scheme was claimed to be secure under certain intractability assumptions, it turned out that none of the protocols of the scheme are secure in the presence of an active adversary. Due to space limitation, we here present only an interleaving attack against the GKE.Join protocol. Attacks against the GKE.Setup and GKE.Remove protocols will be given in the full version of this paper.

2 The GKE.Join Protocol

Let $G$ be a finite cyclic group of $\ell$-bit prime order $q$, where $\ell$ is a security parameter, and let $g$ be an arbitrary generator of $G$. The protocol uses three hash functions $H : \{0, 1\}^* \rightarrow \{0, 1\}^\ell$, $H_0 : \{0, 1\}^* \rightarrow \{0, 1\}^{\ell_0}$, and $H_1 : \{0, 1\}^{\ell_1} \times G \rightarrow \{0, 1\}^{\ell_0}$. Long-term keys are generated as follows:

1. The server $S$ chooses a random $x \in \mathbb{Z}_q^*$ and sets its private/public keys to be $(SK_S, PK_S) = (x, y)$ where $y = g^x$.
2. Each client $U_i \in C$ generates a pair $(SK_i, PK_i)$ of signing/verifying keys by running the key generation algorithm of a signature scheme.

Let $J$ be a set of new clients who want to join an existing client group $G_c$. Then, the client group $G_c$ is updated to be $G_c \cup J$ and the GKE.Join protocol is performed to provide $S$ and each client $U_i \in G_c$ with a new session key $sk$.

**Round 1.** Each new client $U_j \in J$ chooses a random $x_j \in \mathbb{Z}_q$, and precomputes $y_j = g^{x_j}$, $\alpha_j = y^x_j$ and a signature $\sigma_j$ of $y_j$ under the signing key $SK_j$. Each client $U_j \in J$ then sends $(y_j, \sigma_j)$ to the server $S$.

**Round 2.** The server $S$ verifies the incoming signatures. If they are all correct, $S$ increases the counter $c$, computes the common secret value $K = H_0(c \parallel \{\alpha_i \}_{i \in I_c})$, and sends to each client $U_i \in G_c$ the values $c$ and $K_i = K \oplus H_1(c \parallel \alpha_i)$.

**Key computation.** Each client $U_i \in G_c$ already holds the value $\alpha_i = y^{x_i}$ and the old counter value (set to zero for the new ones). So it first checks that the new counter is greater than the old one, and simply recovers the common secret value $K = K_i \oplus H_1(c \parallel \alpha_i)$ and the session key $sk = H(K \parallel G_c \parallel S)$.

3 An Interleaving Attack on GKE.Join

Let’s assume that a set of new clients, $J$, wants to join two existing sessions of the GKE.Setup protocol with the client groups $G_c$ ($A \in G_c$) and $G'_c$ ($A \notin G'_c$), respectively. Assume further that the clients in $J$ are permitted to join, and
thus two concurrent runs of the GKE.JJoin protocol are started with the new client groups $G_c = G_c \cup J$ and $G'_c = G'_c \cup J$, respectively. Then, an interleaving attack given below can be mounted against the clients in $J \subset G'_c$. Increasing the counter (in the second round of the GKE.JJoin protocol) does not play any role in preventing the following attack.

1. In the first round of the second run, the adversary intercepts all the messages $(y'_j, \sigma'_j)$ sent to $S$ by the clients in $J \subset G'_c$.
2. In the first round of the first run, the adversary $\mathcal{A}$ replaces the message $(y_j, \sigma_j)$ sent to $S$ by each client $U_j$ in $J \subset G_c$ with $(y'_j, \sigma'_j)$ obtained in the previous step of this scenario.
3. In the second round of the first run, the server $S$ operates as specified in the protocol since the received signatures are all valid; $S$ computes $\alpha_j = y'_j^x$ for each new client $U_j$ in $J \subset G_c$, increases the counter $c$, and computes the common secret value $K$. The server $S$ then sends to each client $U_i$ in $G_c$ the values $c$ and $K_i = K \oplus H_1(c||\alpha_i)$, and to the adversary $\mathcal{A}$ the values $c$ and $K_A = K \oplus H_1(c||\alpha_A)$. Now, the adversary $\mathcal{A}$ intercepts all the messages sent by $S$ to the other clients, while recovering the common secret value $K$ from $K_A$.
4. In the second round of the second run, the adversary $\mathcal{A}$ (pretending to be the server $S$) sends to each client $U_j$ in $J \subset G'_c$ the message $(c, K_j)$ intercepted in the second round of the first run. After receiving this message from $\mathcal{A}$, each client in $J \subset G'_c$ first checks that the newly received counter is greater than the old one; this verification will succeed since the server $S$ increased the counter in the second round of the first run. Then, each client in $J \subset G'_c$ recovers $K$ from $K_j$ and compute the session key as:

$$sk' = H(K||G'_c||S).$$

Consequently, all the clients in $J \subset G'_c$ share with the adversary the same key $sk'$. Hence, the adversary $\mathcal{A}$ can decrypt all the encrypted messages sent to $S$ from the clients in $J \subset G'_c$. But, the clients in $J \subset G'_c$ believe that they have established a session key with $S$ while in fact they have shared it with $\mathcal{A}$.

References

Designing Secure SMS Scheme on Android OS*

Jongseok Choi and Howon Kim**

Information Security and System LSI Laboratory,
Computer Engineering Department,
Pusan National University,
Busan, Korea
{jschoi85,howonkim}@pusan.ac.kr

Abstract. In this paper, we present secure SMS scheme based on pairing operations. The Android platform has been dealt as a topic of mobile security because of the Android is an open platform whose sources can be observed by anyone. The malicious code inserted in any application can perform to intercept and forward a SMS with hiding the action. In order to protect the SMS on the platform, the designed scheme provide confidentiality of a SMS. The designed protocol is based on the pairing-based cryptography which is a public key cryptosystem to certify entities without PKI because of that it is hard to construct a PKI framework for the android platform.

Keywords: Mobile Security, Android, SMS, Authentication

1 Introduction

Recently, there are many researches on mobile security[1–3] and Android platform[4–8]. However any schemes cannot fully satisfy the attack using malicious codes. In order to overcome the issues Brotherston et al. proposed a scheme using [9] that is vulnerable to the Man-in-The middle attack. After that Cerbo et al. [10] proposed the scheme detecting malicious codes by permissions. It still remains because of detection on malicious codes is difficult as a spy-ware because of the malicious software is getting advanced.

In this paper we designed a scheme that provides confidentiality and authentication. The designed scheme is based on pairing-based cryptography that makes the scheme use the public key cryptography without the PKI framework.

2 Designing Secure SMS

Our scheme is composed of Initialization and Communication phases.

---

* This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621 ).

** Corresponding author
**Initialization** This phase generates parameters needed to authenticate, encrypt or decrypt messages. Let $G_1$ be a additive group, $G_2$ be a multiplicative group, $\hat{e}$ be a bilinear map, $H_1 : \{0,1\}^* \rightarrow G_1$ be a transform map, $\Phi_i$ be a unique mobile identification of the device of the $i$-th user, $\sigma$ be a secret key of SMS gateways and $m$ be the number of devices registered. We assumed that $v$-th user is registered Where $P$ is a element of $G_1$.

**Step1** Generates and distributes a common public key.

$$\sigma P \prod_{k=0}^{m} \Phi_k$$  \hspace{1cm} (1)

**Step2** Generates a private key of $v$-th user .

$$\frac{P \prod_{k=0}^{m} \Phi_k}{\Phi_v}$$ \hspace{1cm} (2)

**Step3** A mobile device stores the common public key and the private key $K$.

$$(G_1, G_2, \hat{e}, H_1, P, CPK, K)$$ \hspace{1cm} (3)

**Communication** This phase is to send messages. Since the issues mentioned in previous section, our scheme stored the common public key that is used to encrypt messages instead of personal public keys of each of devices. Let $CPK$ be the common public key and $\alpha$ and $\beta$ be cellphone numbers of Alice and Bob, respectively. Where Alice want to send a message $M$ to Bob, our scheme performs following steps.

**Step1** Alice’s device encrypts the message by the common public key irrespective of who Alice want to send the message to.

$$C_1 = \hat{e}(H_1(\beta), \frac{CPK}{\Phi_\alpha}) \cdot M$$ \hspace{1cm} (4)

**Step2** Alice sends the encrypted message and Bob’s cellphone number to a SMS gateway.

**Step3** The SMS gateway transshapes and forwards the message received from Alice by using including cellphone number.

$$C_2 = \frac{C_1 \cdot \Phi_\alpha}{\sigma \Phi_\beta}$$ \hspace{1cm} (5)

**Step4** Upon receiving the message Bob decrypts it by his own private key $K_\beta$.

$$M = \frac{C_2}{\hat{e}(H_1(\beta), K_\beta)}$$ \hspace{1cm} (6)
3 Conclusion

Our scheme have three points. The first point is encryption. At the encryption progress a device encrypts a message by its own public key derived from the common public key. The next point is roles of SMS gateway. SMS gateways can know all the messages since all the keys are produced by mobile identifications stored in the server. They transform sender’s public key to a private key of receiver. The final point is decryption. At decryption steps the devices can easily decrypt it by using their own private key stored in the devices.

References

6. Adrienne Porter Felt, Helen J. Wang, Alexander Moshchuk, Steven Hanna and Erika Chin, Permission re-delegation: attacks and defenses, Proceedings of the 20th USENIX conference on Security, p.22-22(2011); August 08-12, San Francisco, CA
An Improved Quantum-behaved Particle Swarm Optimization Algorithm Based on Culture

Gao X. Z\textsuperscript{2}, Wu Ying\textsuperscript{1}, Huang Xianlin\textsuperscript{1} and Kai Zenger\textsuperscript{2},

\textsuperscript{1}Center for Control Theory and Guidance Technology, Harbin Institute of Technology, 150001 Harbin, China
\textsuperscript{2}Department of Automation and Systems Technology, Aalto University School of Electrical Engineering, 00076 Aalto, Finland
{ xiao-zhi.gao@aalto.fi, wying_hit@hotmail.com, xlinhuang@hit.edu.cn, kai.zenger@ aalto.fi, }

Abstract. An improved culture-based quantum-behaved particle swarm optimization algorithm (CQPSO) is proposed. The cultural framework is embedded in the QPSO, and the knowledge stored in the belief space can guide the evolution of the QPSO. 15 high-dimensional and multi-modal functions are employed to investigate the proposed algorithm. Numerical simulation results demonstrate that the CQPSO can indeed outperform the QPSO.

Keywords: Culture-based; Quantum-behaved; PSO; Knowledge.

1 Introduction

The Particle Swarm Optimization (PSO) is a population-based optimization method [1]. It might be stuck into local optima when dealing with multi-modal optimization problems. One of the novel hybridization for PSO is to apply the Quantum laws of mechanics to observe its behavior---Quantum-behaved PSO (QPSO), which has less parameters to control [2]. Cultural Algorithm (CA) proposed by Reynolds in 1995 is a powerful solution to demanding problems, due to its flexibility and efficiency [3].

In this paper, a novel cultural quantum-behaved Particle Swarm Optimization, CQPSO, is proposed to improve the convergence performance of the QPSO. The mutation operator and CA work together to increase the diversity of the swarm population, and enhance the global search capability of the QPSO.

2 Quantum-behaved Particle Swarm Optimization

Suppose there are \( N \) particles in the particle swarm, which are initialized randomly. Each particle can fly in the \( D \)-dimension search space according to its own velocity \( V_i = (v_{i1}, v_{i2}, \ldots, v_{id}) \). The particles are associated with their positions \( X_i = (x_{i1}, x_{i2}, \ldots, x_{id}) \) standing for the possible solutions to the problems under
consideration. In the QPSO, all the particles have the quantum behavior. The state of a particle in QPSO is stated by wave function $|\psi(x,t)|^2$ [4]. The particles move according to the following formulations:

$$\begin{align*}
X_{i+1}^t &= \begin{cases}
M_i^t + \text{belta} \cdot |X_{\text{mbest}}^t - X_i^t| \cdot \ln(1/u) & \text{if } k \geq 0.5 \\
M_i^t - \text{belta} \cdot |X_{\text{mbest}}^t - X_i^t| \cdot \ln(1/u) & \text{if } k < 0.5
\end{cases}.
\end{align*}$$

(1)

$$X_{\text{mbest}}^t = \frac{1}{N} \sum_{i=1}^{N} X_i^t,$$

$$M^t = \frac{c_1 \cdot x^t + c_2 \cdot P_{g^t}}{c_1 + c_2}.$$  

(2)

where belta is the contraction-expansion coefficient, $c_1$, $c_2$, $u$ and $k$ are uniformly random numbers.

3 Cultural Quantum-behaved Particle Swarm Optimization

As proposed by Reynolds, the CA is composed of population space, belief space and the communication protocol [3]. The belief space is the place, where cultural knowledge is formed and stored. In this paper, two typical kinds of knowledge are used: situational knowledge, normative knowledge.

The combination of cultural algorithm and PSO can not guide the iteration for the velocity in a proper way. The emergency of the quantum-behaved particle swarm optimization can solve this problem, because the position is the only iteration term in the QPSO. In this paper, four kinds of influence functions are utilized to decide the iteration for the QPSO to improve the performance of the QPSO.

For example, if the normative knowledge and situational knowledge are used to determine the size of the mutation change and direction of the mutation respectively, our CQPSO is named as CQPSO (NsSd).

4 Simulation Results

A total of 15 nonlinear functions with 30 dimension are used to investigate the optimization capability of our CQPSO. The optimization results are provided in Table 1. It can be figured that the performance of the CQPSO is much better than that of the QPSO for almost all the functions except for the Sal function and Schwefel function.
Table 1. Function optimization performance comparison

<table>
<thead>
<tr>
<th>Functions</th>
<th>PSO</th>
<th>CQPSO (NsSd)</th>
<th>CQPSO (NsNd)</th>
<th>CQPSO (Sd)</th>
<th>CQPSO (Ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ackley</td>
<td>1.2436</td>
<td>0.8856</td>
<td>0.2310</td>
<td>1.1877×10^-4</td>
<td>0.5860</td>
</tr>
<tr>
<td>CM</td>
<td>-0.3453</td>
<td>-1.3899</td>
<td>-2.0098</td>
<td>-2.0676</td>
<td>-1.3456</td>
</tr>
<tr>
<td>DeJongf4</td>
<td>0.0246</td>
<td>4.5454×10^-322</td>
<td>6.5711×10^-322</td>
<td>9.4242×10^-18</td>
<td>1.9994×10^-293</td>
</tr>
<tr>
<td>Expfun</td>
<td>1.2266</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>Griewank</td>
<td>0.0190</td>
<td>1.2212×10^-16</td>
<td>6.6613×10^-17</td>
<td>1.1102×10^-17</td>
<td>1.8874×10^-16</td>
</tr>
<tr>
<td>LM1</td>
<td>0.0962</td>
<td>1.5705×10^-32</td>
<td>1.5705×10^-32</td>
<td>1.5705×10^-32</td>
<td>1.5705×10^-32</td>
</tr>
<tr>
<td>LM2</td>
<td>1.6626</td>
<td>0.0099</td>
<td>0.0065</td>
<td>0.0011</td>
<td>0.0312</td>
</tr>
<tr>
<td>Neumaier</td>
<td>-133.3331</td>
<td>-4930</td>
<td>-4930</td>
<td>-4928.6</td>
<td>-4930</td>
</tr>
<tr>
<td>Rastrigin</td>
<td>57.2142</td>
<td>23.3815</td>
<td>22.6850</td>
<td>19.2635</td>
<td>23.8790</td>
</tr>
<tr>
<td>Rosenbrock</td>
<td>65.8476</td>
<td>1.1960</td>
<td>0.4036</td>
<td>28.3834</td>
<td>0.8098</td>
</tr>
<tr>
<td>Sal</td>
<td>0.2679</td>
<td>0.3199</td>
<td>0.3199</td>
<td>0.3199</td>
<td>0.3399</td>
</tr>
<tr>
<td>Schwefel</td>
<td>6462.2058</td>
<td>6791.9461</td>
<td>7.0318568</td>
<td>6312.3102</td>
<td>6514.5500</td>
</tr>
<tr>
<td>Sphere</td>
<td>0.1425</td>
<td>4.0166×10^-272</td>
<td>5.6356×10^-281</td>
<td>1.4878×10^-144</td>
<td>1.2513×10^-228</td>
</tr>
</tbody>
</table>

Acknowledgments. This work is supported by the Academy of Finland under Grants No. 135225 and No. 127299 and the NSFC under Grant No. 60874084.

References

Study on Analysis Method for SELinux Security Policy

Gaoshou Zhai, Tong Wu

School of Computer and Information Technology, Beijing Jiaotong University, No.3 Shang Yuan Cun, Hai Dian District, Beijing, China 100044
{gszhai, 09120572}@bjtu.edu.cn

Abstract. SELinux is implemented as a security application module of Linux and it enforces a policy based on robust mandatory access control. But its security policy configuration is a hard and complicated task, while errors and bugs are incidental in configuration. Therefore, it is rather significant to study automatic analysis method about SELinux security policy configuration. In this paper, SELinux security mechanism, policy description language and related methods for analysis of validity and integrity of security policy configuration are discussed. Then a prototype for automatic analysis of SELinux security policies is implemented using C language and a security policy configuration case as to an application system called Student-Teacher system is designed to be used to test the prototype. Results show that the prototype and corresponding methods can verify validity and integrity of policy configuration and are helpful to assist people to perform configuration work.

Keywords: Secure Operating Systems; Access Control; SELinux; Security Policy; Analysis Method

1 Introduction

Operating systems are the key foundation of security for information systems while mandatory access mechanism is a necessary part of secure operating systems [1-5].

SELinux is initially developed by National Security Agent of U.S. and it is currently implemented as a loadable security application module based on Linux Security Modules (LSM) [6]. SELinux can enforce a policy based on robust mandatory access control and can be used cooperated with discretionary access control inside Linux kernel to implement effective control whenever a subject request to access an object. But its security policy configuration is a hard and complicated task, while errors and bugs are incidental in configuration. Therefore, it is rather significant to study automatic analysis method about security policy configuration and to build an appropriate tool to assist users with the configurations [7].

2 Methodology

Nowadays, SELinux is implemented based on LSM and Flask architecture and it
supports three types of security models including Type Enhancement (TE), Role-Based Access Control (RBAC) and Multi-Level Security (MLS). In addition, two types of logic structural rules, i.e. constraints rules and conditional rules are provided in SELinux policy configuration language. A few demonstration polices (among which strict policy and targeted policy are rather widely used) have been provided by system developers so as to make users’ policy design more convenient and a new architecture as to so-called reference policy is established in order to improve modularization and maintainability [8].

Policy analysis in this paper is taken aim at validity and integrity, i.e. to make sure that the policy configuration has carried out expected access regulations and to verify that subjects inside Trusted Computing Base (TCB) are prohibited to read wrong information from non-trusted objects while sensible information inside TCB objects are protected from wrongly modified. Thereafter, a security analysis model is built up and all rules for TE and RBAC are rewritten as formal expressions while all subjects, objects and elements are marked as sets and mappings formally. Algorithms for analysis are designed based on such model. Comparing with SELAC model [9], scope of possible values for role can be reduced and thus a great many invalid security contexts are eliminated in our method.

3 Prototype and Results

A prototype is implemented using C language, which is made up of reference policy transformation module, security policy extract module, security policy analysis module and analysis result display module. In addition, a group of security policy modules are designed based on architecture of reference policy as to so-called student-teacher system and are used to test the prototype. Results show that the prototype and corresponding methods can verify validity and integrity of policy configuration and are helpful to assist people to perform configuration work. Some test results for verification of validity can be illustrated in Fig.1.

![Fig. 1. Test Result Example for Verification of Validity.](image-url)
4 Summary

In this paper, methods for automatic analysis of SELinux policies are discussed and a corresponding prototype is implemented. Meanwhile, a group of security policy modules as to so-called student-teacher system are designed based on the architecture of reference policy, which is used to test the prototype. Test results are satisfactory. Nevertheless, some simplified measures are adopted in this paper. For example, Boolean variables and a few special signs and macro blocks are ignored during the analysis. All these details ought to be full considered in the future research. In addition, both method and prototype for analysis must be improved farther for practicability.

Acknowledgments. The authors would like to give grateful thanks to the support of the Fundamental Research Funds for the Central Universities (No.2009JBM019).

References


An Alert Correlation Analysis Oriented Incremental Mining Algorithm of Closed Sequential Patterns with Gap Constraints

He Hui, Wang Dong, Zhang Weizhe, Zhang Hongli
School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China . 150001
hehui@hit.edu.cn

Abstract. This paper focuses on picking up alert information efficiently and timely, which is an important need. According to the characteristics of intrusion detection log, we put forward the method of using incremental mining algorithm of closed sequential patterns with gap constraints – cispan algorithm to analyze the growing log database, we also compare the performance of cispan algorithm, prefixspan algorithm and clospan algorithm in analyzing intrusion detection log, and proves that cispan algorithm has higher efficiency in analyzing alert log.

Keywords: alert analysis, sequential pattern, gap constraint, closed sequential pattern, incremental mining algorithm of closed sequential patterns.

1 Introduction

The well-known BT site - Mininova has suffered a large-scale botnet attack across three continents recently. How to effectively and timely pick up useful alert information from the large amount of alert log data is a complicated and meaningful work.

Many complicated intrusions have a fixed time sequences, such as when a hacker attacks, at first he often scans port, executes some specific codes to get special permission, carries out an attack [1] and so on, these acts will leave the same alert sequences in alert log. Picking up alert sequences above has an important guiding significance to analyze the true purpose of intruder. In order to accurately pick up the alert sequence, incremental mining algorithm of closed sequential patterns with gap constraints – cispan algorithm will be used in this paper to the analysis of alert log, it find high frequency of frequent sequential patterns, then analyzes the contract between the alert information.

In section 2, the related definitions and content of cispan algorithm are given, in section 3, the performance comparison of cispan algorithm, clospan algorithm and prefixspan algorithm are presented. Finally, our conclusions of this paper are summarized in section 4.
2 Cispan Algorithm with Gap Constraints

Yan [2], et al. used a new pruning method on the basis of prefixspan algorithm, he found two sequences \( s \) and \( s' \), if \( s \subseteq s' \) and \( I(D_s) = I(D_{s'}) \), then for any of item \( C \) in project set \( D_s' \), \( \text{support}(s \bowtie c) = \text{support}(s' \bowtie c) \). According to the above findings, he proposed two pruning methods – backward sub-pattern pruning method and backward super-pattern pruning method. When extending the sequence \( s' \), at first we determine whether there is a sequence \( s \) that has extended, which makes \((1) \ s' \subset s \) or \((2) \ s \subset s' \), if so, we can stop extending sequence \( s \). When condition meets \((1) \), we can directly stop extending \( s' \). When condition meets \((2) \), we don’t extend \( s' \), instead, we directly transplant the offspring of \( s \) to the offspring of \( s' \).

When combining with gap constraints, the paper [3] put forward a prefixspan algorithm with gap constraints, when extending an element, the author puts forward a method, which records all the positions that the element appears in each of sequence in the database, rather than records the first positions that the elements appears in each of sequence in the database, but each of sequence in the sequential patterns database can only increase support degree count of the element at most once.

Cispan algorithm is future improved on the basis of cisman algorithm to speed up the speed of mining incremental database. Cispan algorithm divides the incremental operation into two steps – remove and insert. When sequence \( s \) grows for \( s' \), cisman algorithm first removes sequence \( s \), then inserts sequence \( s' \). Let \( I \) be the inserted sequence, let \( R \) be the removed sequence, let \( U \) be the unchanged sequence. Let \( IS \) be the frequent sequence that appears in \( I \), let \( Li \) be the prefix case that contains all sequences in \( IS \). Let \( US \) be the frequent sequence that appears in \( U \), let \( Lo \) be the sequence that contains all sequences in \( US \).

Cispan algorithm [5] is divided into three steps:
1) For each frequent sequence that appears in \( I \), we call incclspan algorithm to mine \( Li \)
2) Modifying \( Lo \) of the original database. When a sequence appears in \( R \), reducing the count. When the count is less than the minimum support degree, removing corresponding node of this sequence, finally we get \( Lo' \)
3) Merging \( Lo' \) and \( Li \) recursively. During merging, recursively traversing each node in preorder. Since \( Li \) is the new inserted prefix case, when the structure of corresponding node of \( Lo' \) is not same as that of \( Li \), modifying the corresponding node of \( s \). Step 2 and step 3 detailed see the cispan algorithm [10] of Ding, Yuan, et al.

3 Experimental Results and Analysis

Experimental data is the testing sample - Lincoln Laboratory Scenario(DDos) 1.0 [4] which is provided by DARPA 2000, experimental platform environment is 4 cores inter(R) Xeon(TM), CPU frequency is 3.2 GHZ, memory is 4G, OS is Linux, kernel version is 2.6.9, compiler is GCC 3.2.3, programming language is c++.
We compare the spending time of prefixspan algorithm, clospan algorithm and cispan algorithm, and separately analyze the logs that their log number are 1681, 85930 and 688134. For each log we divide the log into four paragraphs to simulate incremental process, at first use program to analyze the first paragraph log, then use the second paragraph log as increment, make program continue to analyze the new generation of log database, and use the third and the fourth paragraphs of log as increment in turn with program analyzing. Each paragraph’s increment of three logs are 100, 5000 and 20000. The results are shown in figure 1, figure 2 and figure 3, in first processing time which three algorithms need is similar, in the later log growth, cispan algorithm only needs to analyze the new incremental log, which greatly accelerates the processing speed, however, clospan algorithm and prefixspan algorithm have to deal with the whole sequential patterns database again. All in above confirm that in analyzing the intrusion detection log, cispan algorithm based on increment is better than prefixspan algorithm and cloapan algorithm in efficiency.

4 Conclusions

This paper use the cispan algorithm with gap constraints to analyze snort log, analyze the growing log database, the performance is better than the primitive clospan algorithm and prefixspan algorithm, at the same time, real-time alert performance and vast log information compression are improved to a certain extent.

Acknowledgments. This work was supported by the National Natural Science Foundation of China (NSFC) under grant No. 61173145, the National High Technology Research and Development Program of China under Grant No. 2010AA012504 and No. 2011AA010705, and the National Basic Research Program of China under Grant No.G2011CB302605.

References

2. X. Yan, J. Han, and R. Afshar.CloSpan: MiningClosed Sequential Patterns in Large Databases.In SDM’03, San Francisco, CA, May 2003.
5. Ding Yuan, Kyuhyung Lee, Hong Cheng Gopal Krishna, Zhenmin Li, Xiao Ma, Yuanyuan Zhou and Jiawei Han .CISpan: Comprehensive Incremental Mining Algorithms of Closed Sequential Patterns for Multi-Versional Software Mining. In Proceedings of SDM'2008. pp.84–95.
Invariant Image Watermarking Using Harris Feature Extraction and Zernike Moments

Xiao-Chen Yuan, Chi-Man Pun

Department of Computer and Information Science
University of Macau, Macau SAR, China
(yb07417, cmpun)@umac.mo

Abstract. A robust and geometric invariant digital image watermarking scheme based on feature extraction and local Zernike transform is proposed in this paper. The Adaptive Harris Detector is proposed to extract feature patches for watermarking use. A local Zernike moments-based watermarking scheme is raised, where the watermarked patches can be obtained directly by inverse Zernike Transform. Each extracted circular patch is decomposed into a collection of binary patches and Zernike transform is applied to the appointed binary patches. Magnitudes of the local Zernike moments are calculated and modified to embed the watermarks. Inverse Zernike transform is applied to reconstruct the watermarked binary patch. Experimental results show that the proposed scheme is very robust against geometric distortion such as rotation, scaling, cropping, and affine transformation, and common signal processing.

Keywords: Geometric Invariant, Feature Extraction, Adaptive Harris Detector, Local Zernike Transform, Inverse Zernike Transform

1 Introduction

Digital watermarking is proposed as an effective solution to the problems of multimedia copyright protection and data authentication. Quite a number of geometric invariant algorithms have been proposed in the past years [1-4]. Moments and its invariant functions have also been extensively used for invariant feature extraction in a wide range of pattern recognition applications [5]. Of various types of moments, Zernike moments have been shown to be superior to the others in terms of their insensitivity to image noise, information content, and ability to provide faithful image representation. Therefore, they are employed for watermarking in many literatures for its special invariance properties against distortions.

A novel geometric invariant digital image watermarking scheme based on Harris feature extraction and Zernike moments is proposed in this paper. The Adaptive Harris Detector is proposed for more robust feature points extraction. Due to the cumulative computational errors of Zernike transform, it is difficult to reconstruct watermarked image/patch without visible quality degradation directly using its inverse transform. Therefore, the bit-plane decomposition based scheme is proposed.
Each extracted circular patch is decomposed into a collection of binary images and Zernike transform is applied to the selected binary patches.

The details of the scheme will be addressed in the following sections. Section 2 illustrates watermark embedding and extraction. Section 3 presents the experimental results. And section 4 draws the conclusions.

2 Watermark Embedding and Extraction Procedure

For watermarking embedding, firstly, the proposed Adaptive Harris Detector is applied to the host image to extract feature points. Each extracted patch is decomposed into $m$ binary circular patches. Some of the binary patches are appointed for watermark embedding. Each appointed binary circular patch is translated to its centroid, and scaled to a standard size; afterwards, Zernike transform is applied into the normalized binary patch to calculate its Zernike moments. The magnitudes are proved to be so robust against RST attacks that they are used as watermark embedder.

The watermark is generated with a predefined seed. Spread spectrum communication technique is used to embed the watermark, as shown in equation (1).

$$Y = X + \alpha \times W.$$  

Where $X$ denotes Zernike moments magnitudes, $\alpha$ is the predefined parameter to control the watermark embedding strength, and $W$ presents the random watermark sequence of Gaussian distribution. $Y$ is the watermarked data.

For watermark extraction, the inverse procedure of watermark embedding is operated. The linear correlation defined in equation (2) [6] is used to detect the existence of the watermark in the Zernike moments magnitudes. The watermark is detected when the linear correlation result is larger than a predefined threshold value.

$$C_{Linear} = \frac{1}{S} \sum w \cdot y.$$  

Where $C$ is the linear correlation, $S$ is size of the Zernike moments magnitudes for watermark detection, $y$ is the watermarked data, and $w$ is the watermark data sequence generated by using the same seed used in watermark embedding process.

3 Experimental Results

Many experiments are implemented to evaluate the proposed watermarking scheme. In the following experiments, the number of feature points $N$ is set to be 3. The radius $r$ of the extracted circular patches is set to be 40. For watermarking, each circular patch is decomposed into 8 binary patches. The order of Zernike transform is defined as 40. The watermark is generated randomly under Gaussian distribution and the watermark embedding strength $\alpha$ is set to be 10. PSNR (Peal Signal-to-Noise Ratio) is used to evaluate the distortion of the watermarked image. By experiments, the fifth bit plane of each selected patch is adaptable for watermarking, to ensure the
success of watermark extraction and to decrease distortion of the image. Table 1.
presents the comparison results of the proposed scheme and the existing schemes,
revealing that the proposed scheme performs well compared with the existing
methods.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Rotation</td>
<td>$1^\circ - 5^\circ$</td>
<td>$0^\circ - 360^\circ$</td>
<td>$0^\circ - 360^\circ$</td>
</tr>
<tr>
<td>Image Scaling</td>
<td>$-0.7 - 1.8$</td>
<td>$0.4 - 3$</td>
<td>$0.4 - 3$</td>
</tr>
<tr>
<td>Image Cropping</td>
<td>Up to 10%</td>
<td>Up to 40%</td>
<td>Up to 40%</td>
</tr>
<tr>
<td>Affine Transformation</td>
<td>Up to 5%</td>
<td></td>
<td>Up to 20%</td>
</tr>
<tr>
<td>JPEG compression</td>
<td>$40 - 100$</td>
<td>$10 - 100$</td>
<td>$10 - 100$</td>
</tr>
<tr>
<td>Median Filtering</td>
<td>$3 \times 3$</td>
<td>$8 \times 8$</td>
<td>$8 \times 8$</td>
</tr>
<tr>
<td>3$\times$3 Gaussian Filtering</td>
<td>Pass</td>
<td>$\leq 0.5$</td>
<td>$\leq 2$</td>
</tr>
</tbody>
</table>

In Table 1, the dash ‘–’ indicates that the simulation was not recorded in the literature.

4 Conclusion

In this paper, the digital image watermarking scheme based on Harris feature
extraction and Zernike transform is proposed. The Adaptive Harris Detector is
proposed for local region extraction. Bit-plane decomposition method is used to
decompose each patch into a collection of binary patches. Zernike transform is
applied to each appointed binary patches to calculate Zernike moments for
watermarking use. The proposed scheme is proved to survive geometric distortions
very well. It is very robust against image rotation, scaling, cropping, affine
transformation and common signal processing. The comparison results show the
proposed scheme outperforms the several representative feature extraction based
schemes in terms of robustness to various attacks.

References

2. S. Pereira, T. Pun, Robust template matching for affine resistant image watermarks. *Image
3. P. Bas, J. M. Chassery, B. Macq, Geometrically invariant watermarking using feature
   Mathematical Modeling and Analysis of the Watermarking Processes. *Image Processing,
Cryptanalysis of a two-factor user authentication scheme over insecure channels

Jin Qiuyan¹, Kwangwoo Lee¹, and Dongho Won¹,*

¹ Information Security Group,
School of Information and Communication Engineering, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746,
Suwon, Republic of Korea
{qyjin, kwlee, dhwon}@security.re.kr

Abstract. With the booming of network technology, secure service and privacy protection are concerned. Remote user authentication scheme is used to verify if the communication parties are trustable and legitimate. In 2009, Li, Lee and Wang proposed a two-factor user authentication scheme which provides mutual authentication and key agreement over insecure channels. However, in this paper, we find that Li-Lee-Wang’s scheme is vulnerable to some attacks.

Keywords: Cryptanalysis; Remote user authentication; Smart card; Network security; Mutual authentication.

1 Introduction

During the last couple of decades, a remote user authentication scheme has become necessary, which is used to verify if the communication parties are trustable and legitimate. Usually, a smart card used for user authentication is required. In 2005, Yoon et al. proposed a scheme [1], which does not provide mutual authentication. To overcome the drawback, Li, Lee and Wang proposed an enhancement of Yoon et al.’s scheme [2]. However, in this paper, we find that Li-Lee-Wang’s scheme is vulnerable to smart card stolen attack. The rest of the paper is organized as follows. In Section 2, we review Li-Lee-Wang’s scheme. In Section 3, we show a security analysis of Li-Lee-Wang’s scheme. Finally, we conclude this paper in Section 4.

2 Review of Li-Lee-Wang’s scheme

In this section, we briefly review the remote user authentication scheme proposed by

* Corresponding Author: Dongho Won (dhwon@security.re.kr)
* This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)(KCA-2012-12-912-06-003)
Table 1. Notations used in this paper.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U$</td>
<td>A user</td>
</tr>
<tr>
<td>$S$</td>
<td>A remote server</td>
</tr>
<tr>
<td>$ID, PW, SC$</td>
<td>$U$’s identity, password and smart card</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>The bitwise WOR operation</td>
</tr>
<tr>
<td>$</td>
<td></td>
</tr>
<tr>
<td>$x$</td>
<td>$S$’s secret key, which is kept secret and only known by $S$</td>
</tr>
<tr>
<td>$T_{TSA}$</td>
<td>A timestamp provides by a trust time stamping authority $TSA$</td>
</tr>
<tr>
<td>$N_C$</td>
<td>A nonce generated by $U$</td>
</tr>
<tr>
<td>$N_S$</td>
<td>A nonce generated by $S$</td>
</tr>
<tr>
<td>$SK$</td>
<td>The common session key established by $U$ and $S$</td>
</tr>
<tr>
<td>$H(.)$</td>
<td>A collision resistant one-way hashing function</td>
</tr>
</tbody>
</table>

2.1 Registration phase

In this phase, the user $U$ registers with the server $S$ by performing the following steps. Firstly, $U$ chooses his own identity $ID$ and password $PW$. Then $U$ sends $ID$ and $PW$ to $S$ through a secure channel. Receiving the registration request, $S$ computes $V_C = H(ID, T_{TSA}, x)$, $A_C = H(ID, T_{TSA}, x) \oplus PW$. Finally, $S$ sends the smart card $SC$ to $U$ with the parameters $\{ID, V_C, A_C, H(.)\}$ through a secure channel.

2.2 Login phase

If $U$ wants to login to $S$, firstly, he inserts his own $SC$ gained from $S$ into a card reader and enters his $ID$ and $PW$. $SC$ computes $B_C = A_C \oplus PW$, if $B_C \neq V_C$, $SC$ rejects the login request. Otherwise, $SC$ computes: $C_1 = B_C \oplus N_C$, $N_C$ is a nonce generated by $U$. Then $SC$ sends $\{ID, C_1\}$ to $S$.

2.3 Authentication phase

Upon receiving the login request, $S$ rejects $U$’s login request if the received $ID$ is invalid. Otherwise, $S$ computes $B_S = H(ID, T_{TSA}, x)$, $C_2 = C_1 \oplus B_S$, $C_3 = B_S \oplus N_S$, $SK = H(B_S \|| C_2 \|| N_S)$, $C_4 = H(C_1 \|| C_3 \|| SK)$, then $S$ sends $\{C_3, C_4\}$ to $U$ for unilateral authentication. $U$ computes $C_5 = C_3 \oplus B_C$ and $C_6 = H(C_1 \|| C_3 \|| H(B_C \|| N_C \|| C_5))$, where $H(B_C \|| N_C \|| C_S)$ is the common session
key. If \( C_6 = C_4 \), \( U \) believes that \( S \) is the real server and the user authentication is completed. Otherwise, \( U \) terminates the session. When the unilateral authentication is achieved, \( U \) computes \( C_7 = H(N_C \parallel C_s \parallel B_C) \), then sends \( C_7 \) to \( S \) for mutual authentication. \( S \) computes \( C_8 = H(C_2 \parallel N_S \parallel B_s) \). If \( C_8 = C_7 \), \( S \) believes \( U \) is the real user and the mutual authentication is completed. Otherwise, \( S \) terminates the session.

3 Smart card stolen attack on Li-Lee-Wang’s scheme

Case 1: The remote server \( S \) stored the information \( \{ID,V_C,A_C,H(\cdot)\} \) into \( U \)’s SC in the registration phase. If an adversary steals the SC and obtains the parameters \( A_C \) and \( V_C \), he can easily compute out the password of the real user \( U \) by computing \( A_C \oplus V_C = PW \).

Case 2: The real user and server transmit the login request ( \( m_1 = \{ID,C_1\} \) ) and authentication message ( \( m_2 = \{C_3,C_4\} \) ) via insecure channel. An attacker can intercept the transmitted messages and obtain \( V_C \) from the stolen smart card. With these values, the attacker can compute out \( SK \), which is used for secure communication, by computing \( B_S = H(ID,T_{TXA},x)=V_C \), \( N_C = C_1 \oplus V_C \), \( N_S = C_3 \oplus V_C \), \( SK = H(B_S \parallel C_2 \parallel N_S) = H(V_C \parallel N_C \parallel N_S) \).

4 Conclusion

In this paper, we have presented a cryptanalysis of Li-Lee-Wang’s scheme. We point out that their scheme is not secure against smart card stolen. Finally, our further research direction ought to propose a robust and practical remote user authentication scheme which can solve these problems.

References

Time-Space Trust in Networks

Shunan Ma, Jingsha He, and Yuqiang Zhang

1College of Computer Science and Technology
2School of Software Engineering
Beijing University of Technology, Beijing 100124, China
msn1679@126.com, jhe@bjut.edu.cn

Abstract. Trust is part of our daily life and thus can be used as a mechanism for providing security in computer networks. In this paper, we consider the time and space nature of trust, and propose the concept of time-space trust which includes two factors: time and place, and compute a value for trust.

Keywords: trust, security, time, space

1 Introduction

Trust is a part of our daily life and thus can be used as a tool to reduce the complexity of making access decisions, which can be accomplished by using trust to provide security [1]. In recent years, many researchers have applied trust to the dynamic environments. Trust models have been proposed to control anonymity, unpredictability and uncertainty [2-5]. The concept of trust is originally derived from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [6]. Blaze first introduced the notion of “trust management” and identified trust as a separate component of security services in networks [7]. In recent years, many researchers have also applied trust to solving network security problems in which measurement of trust relationship between entities in networks has become a key issue. However, the application of classic mathematics functions to compute trust values often leads to inaccuracy. The reason is that trust has the nature of subjectivity and fuzziness.

In this paper, we consider the time and space nature of trust, and propose the concept of time-space trust which includes two factors: time and place, and compute a value for trust.

2 Trust Computation

Trust is very subjective that reflects one body’s subjective expectation on another body’s future actions based on their previous exchanges. Trust exhibits three characteristics: dynamism, subjectivity and ambiguity. Every user has a particular
trust value towards others at a certain point of time or during a certain period of time. The trust value changes as a result of interactions with others.

Given each factor of trust, suppose every factor’s trust value is $T_0$, $T_1$, ..., $T_{n-1}$, respectively, and the weight of each factor is $W_i$. Trust value can be computed as:

$$T = \sum_{i=0}^{n-1} (W_i \times T_i).$$

For different application, factors of trust can be set specifically. In addition, trust computation consists of two parts: determine each factor’s trust evaluation method to get each factor’s trust value and each factor’s weight allocation.

To reflect dynamicity of trust in an open environment, we compute trust with two factors introduced above as follows:

$$T = \alpha_1 T_1 + \alpha_2 T_2$$

in which $\alpha_1 + \alpha_2 = 1$ (1)

In this paper, we can define the weights of time and space is 0.5.

According to an object’s property and a subject’s behavior history information, we can establish tables for the time and place of the trust evaluation rules. For example, the trust value of a subject who accesses a recreation resource during work hours is lower than that during spare time. For accessing educational resources, trust value of a subject whose IP address belongs to an educational network is higher than that to a non-educational network.

According to the property of each resource, time can be divided into $n$ periods. For each time period $[t_i,t_j]$, we formulate corresponding trust interval $[T_i,T_j]$, which means that when a subject accesses the resource at time $t$, if $t_i \leq t \leq t_j$, then randomly generate a trust value $T \in [T_i,T_j]$. To avoid denial of access to an object in high crime periods, we use the following method. For each time period $[t_i,t_j]$, when the number of accesses reaches a certain value, count the total access number $m$ and fraud number $k$ and the fraud probability in this period is $p=k/m$. Then, randomly generate a trust value $T_x$ at time $x$ where $T_x \in [T_i,T_j]$. The trust value of time factor is then

$$T = T_x \times (1 - p).$$

According to the time attribute of resources, trust evaluation table for the time factor is shown in Table 1.

**Table 1. Trust evaluation table for the time factor.**

<table>
<thead>
<tr>
<th>Time period</th>
<th>$[t_0,t_1)$</th>
<th>$[t_1,t_2)$</th>
<th>$[t_2,t_3)$</th>
<th>...</th>
<th>$[t_{n-1},t_n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust interval</td>
<td>$[T_0,T_1)$</td>
<td>$[T_1,T_2)$</td>
<td>$[T_2,T_3)$</td>
<td>...</td>
<td>$[T_{n-1},T_n)$</td>
</tr>
<tr>
<td>Fraud probability</td>
<td>$p_0$</td>
<td>$p_1$</td>
<td>$p_2$</td>
<td>...</td>
<td>$p_{n-1}$</td>
</tr>
</tbody>
</table>

We use IP addresses as the place factor. Subjects can be classified according to the property of an object. For example, subjects can be classified into subjects in the same
subnet, domain, important service segment and general service segment. We then formulate the trust evaluation intervals. For each network segment, when the length of access time reaches a certain number, we count the fraud probability in this network segment. For a given IP address, we can use Formula (2) to compute the trust value of the IP factor. Trust evaluation table for the IP factor is shown in Table 2.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Same subnet</th>
<th>Same segment</th>
<th>Important service</th>
<th>General service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust interval</td>
<td>[T₀, T₁)</td>
<td>[T₁, T₂)</td>
<td>[T₂, T₃)</td>
<td>...</td>
</tr>
<tr>
<td>Fraud probability</td>
<td>p₀</td>
<td>p₁</td>
<td>p₂</td>
<td>...</td>
</tr>
</tbody>
</table>

4 Conclusion

In this paper, we considered the time and space nature of trust, proposed the concept of time-space trust which includes two factors: time and place, and computed a value for trust.

References

Secure Password by Using Two Factor Authentication in Cloud Computing

Ali A. Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, and Deqing Zou

Services Computing Technology and System Lab
Cluster and Grid Computing Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
aliadel2005alamre@yahoo.co, hjin@hust.edu.cn

Abstract. Security threats are considered the main barrier that precluded potential users from reaping the compelling benefits of the cloud computing model. Unfortunately, traditional password authentication jeopardizes user privacy. Anonymous password authentication (APA) represents a promising method to maintain users privacy. However, the major handicap that faces the deployment of APA is the high computation cost and inherent shortcomings of conventional password schemes. In our proposed scheme, we present a new setting where users do not need to register their passwords to service provider. They are supplied with the necessary credential information from the data owner. Furthermore, for enabling the service provider to know the authorized users, data owner provides the service provider with some secret identity information that is derived from the pair (username/password) of each user. Our approach shows good results in terms of high scalability which make our scheme more suitable to the cloud environment, strong authentication that withstands different known attacks.

Keywords: cloud authentication; zero-knowledge proof; service provider; password authentication; privacy-preserving; asymmetric scalar-product-preserving encryption (ASPE)

1 Introduction

In this section, we present a new password authentication scheme and privacy-preservation for cloud environments. Our proposed scheme is involved with three components, data owner (DW), a user set, a server such as a service provider (SP). Our work consists of three stages: setup, registration, and authentication. Setup and registration stages are executed only once, and the authentication stage is executed whenever a user wishes to login. In the setup and registration stages, the user (Ui) registers her/his identity (username Un i and password Pw i ) into DW who saves Un i and Pw i , and then provides public system parameters (ZPK) to service provider and each user in secure channel. We can describe this step as follows.

DW sets up \( n = pq \), where \( p \) and \( q \) are two large primes. He selects \( (M_i, M_i^{-1}, g_i, k_i \in Z_n^*) \). DW uses a cryptographic hash function \( H(.) \), asymmetric scalar-product-preserving encryption \( E_T(.) \), symmetric key encryption \( Enc(.) \) and \( T \) transport function. DW
computes important information \((f_i, y_i, x_i, s_i)\), where \(x_i = H(Pw_i), y_i = g_i^{x_i \mod n}, f_i = g_i^{U_i, y_i}, s_i = Pw_i^T \cdot M_i \cdot M_i^{-1} Pw_i^T\). The public system parameters contain \(ZKP = (g_i, k_i, n, H(\cdot), Enc(\cdot)).\) Briefly, \(DW\) supplies \(U_i\) and \(SP\) by important information as follows. 1) \(DW \rightarrow U_i: ZKP, M_i, f_i, y_i, x_i;\) 2) \(DW \rightarrow SP: U_i, H(y_i, k_i), Pw_i, s_i, ZKP\)

\(U_i\) encrypts his important information \((ZKP, M_i, f_i, y_i, x_i)\) by using private key \(pk_i\), i.e., \(Enc_{pk_i}(ZKP, M_i, f_i, y_i, x_i)\), he computes his private key by composing between \(Pw_i\) and \(M_i\), private key is \(pk_i = Pw_i \| M_i\), where \(\|\) means concatenation function. Then, \(U_i\) saves his credential file to his preferred storage such as USB. After that, the user may use the authentication stage to login. 2FA authentication session is qualified as follows.

1. \(U_i\) uses decryption function \(Dec_{pk_i}(ZKP, M_i, f_i, y_i, x_i)\) to decrypt his credential file by \(pk_i\) and sends \((Un_i, (y_i, K_i))\) to \(SP\) as a first factor. When \(SP\) detects the identity of \(U_i\), it will provide \(U_i\) by \(\alpha \in Z_n^*\), which generates randomly for each login attempt of \(U_i\).
2. \(U_i\) computes \(E_{i1} = E_T(Pw_i^T, M_i) = Pw_i^T \cdot M_i\), generates a random \(r_{x_i} \in Z_n^*\), and then calculates \(t_i = g_i^{r_{x_i}}\).
3. \(U_i\) calculates \(E_{i2} = Enc_k_i(y_i), c_i = H(y_i, t_i, f_i, \alpha), z_{x_i} = x_i - c_i x_i\) and \(w_{x_i} = x_i - c_i x_i\). Finally, \(U_i\) submits \((E_{i1}, E_{i2}, c_i, z_{x_i}, w_{x_i})\) to \(SP\) as a login request (second factor).
4. Service Provider: Upon receiving the information in Step 3, \(SP\) performs the following steps:
   - \(SP\) computes \(s_i' = E_{i1} Pw_i = Pw_i^T \cdot M_i \cdot M_i^{-1} Pw_i\) to check whether \(s_i'\) equals the stored \(s_i\). If so, \(SP\) computes as follows.
     (a) \(y_i' = Dec_k_i(E_{i2}), t_i' = (y_i')^{c_i} g_i^{z_{x_i}}, \) and \(f_i' = (y_i')^{c_i} g_i^{U_i, y_i} g_i^{W_{x_i}}\).
     (b) \(c_i' = H(y_i', t_i', f_i', \alpha).\) The mathematical proofs (1, 2) demonstrate how \(SP\) obtains the secret parameters \((t_i', f_i')\) from \(U_i\).
   - If \(c_i'\) equals \(c_i\) that means \(U_i\) is an authorized user, \(SP\) computes \(E_i'' = Enc_{k_i}(t_i' + f_i')\) and then sends it to \(U_i\).
5. \(U_i\) will ensure the validity of \(SP\) by computing \(E_{i3} = Enc_{k_i}(t_i + f_i).\) After that, he checks whether \(E_i 3 = E_i''\) or not. If the result of the comparison is true, \(SP\) is a valid server otherwise it is an impersonator party.

\[
\text{Prof (1)}
\begin{align*}
t_i' &= (y_i')^{c_i} g_i^{z_{x_i}} \\
&= (g_i^{x_i})^{c_i} g_i^{(r_{x_i} - c_i x_i)} \\
&= g_i^{c_i x_i + r_{x_i} - c_i x_i} \\
&= g_i^{r_{x_i}} = t_i
\end{align*}
\]

\[
\text{Prof (2)}
\begin{align*}
f_i' &= (y_i')^{c_i} g_i^{w_{x_i}} \\
&= (g_i^{x_i})^{c_i} g_i^{x_i - x_i c_i} \\
&= g_i^{username_i} g_i^{x_i - x_i c_i} \\
&= f_i
\end{align*}
\]

## 2 Compared with Previous Works and Performance Investigation

We compare security properties of our proposed scheme with ones of four authentication schemes, including Das et al. [1], Chien et al. [2], and Pathan et al. [3]. Table 1
Table 1. Comparison of authentication schemes

<table>
<thead>
<tr>
<th></th>
<th>Our Scheme</th>
<th>Das et al. [8]</th>
<th>Chien et al. [9]</th>
<th>Pathan et al. [10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>C2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>C3</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>C4</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>C5</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

C1: Freely chosen password; C2: User anonymity; C3: Secure password change; C4: session key agreement; C5: Mutual authentication.

describes comparison of security properties. We conduct several experiments for gauging the efficiency and the effectiveness of our work. We test the effectiveness in terms of authentication accuracy. We have registered during our experiments 2000 users and suppose that each user needs maximum 2 seconds for logging the system. Unsurprisingly, the average time for the authentication stage of our work is equal to 0.0257 seconds for each user which indicates the high speed of our solution. We gain this average time from 100 runs of our proposed scheme.

3 Conclusion

This paper investigates the feasibility of adopting 2FA and anonymous password for user authentication in cloud computing environment. Security analysis explains that our proposed scheme can resist various possible attacks and gratify all the security requirements. The main comparison reinforces the good qualities of our work in contrast to the preceding anonymous password authentication schemes for cloud environment. Especially, our scheme can support the privacy preservation of password. Thus, our scheme proposes anonymity and security of the login users. In the performance appraisal, our presented scheme has been evidenced to achieve sturdy security with lower cost than its previous schemes. Our on-going research is to apply the current work to multi-cloud, hacker blocking.

References

Abstract. We propose and analyze a novel approach for security based on an execution behavior of an application program, which aims at detecting previously unknown anomaly execution patterns. Our scheme, which is a sort of hardware-based approach, uses the basic block information of an application program for the purpose of detecting and preventing unknown anomaly execution behaviors effectively.

Keywords: Security, Branch prediction, Basic block, Anomaly execution behavior

1 Introduction

In general, to attack a computer system, there should be executed at least malicious two operations. First, there should be an operation to inject an attacking code into a computer system. Second, it is required to hijack a program execution control. For example, stack smashing is a well-known approach to be used to attack a computer system. There has been several research related to stack smashing. The basic solution to prevent stack smashing is to prohibit a stack overflow that can occur from the execution code stored in data segments. However, some programs attempt to generate an executable code at run time using just-in-time compiler, which is required for executing instructions stored in a data segment.

There are hardware-based approaches to solve stack overflow attacks. [2] uses a secure cache called \textit{SCache Architecture}. [3] uses an LIFO small memory stack called \textit{SRAS (Secure Return Address Stack)}. Also, there is a compiler-based approach [4]. This approach is based on a combination of static and dynamic monitoring and proposes models using context-free grammar and automata. However, these approaches do not provide a solution to detect any unknown anomaly execution behaviors except stack smashing.

2 The Structure for Basic Block Information

Our scheme uses the basic block of an application program, which is a sequence of
instructions with one entry point and one exit point within it. Our scheme aims at detecting anomaly execution behaviors using the basic block information of an executable program. It maintains the pairs of the starting and ending address of each basic block in a table called EBCI (Execution Boundary Check Information), as shown in Table 1.

<table>
<thead>
<tr>
<th>Starting Addr.</th>
<th>Offset or Ending Addr.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. The structure of EBCI

There are two steps to enable the operation of our scheme as shown in Fig. 1. As the first step, it is necessary to construct EBCI from an application program using a basic block analyzer. The next step is to detect anomaly execution behaviors by checking EBCI using an execution behavior checker during execution.

3 Experimental Results

3.1 Experimental method

We made an experiment using SimpleScalar simulator and developed an analysis tool to obtain basic block information. We used ‘objdump’ program to get the instruction trace information of the program. We used two benchmarks: SPEC200 benchmarks and Mibench v1.3. We verified our approach by inserting the address of an anomaly execution behavior into a normal execution trace. The analysis tool developed collected the information such as the number of instruction per basic block, the basic block’s starting address, the basic block’s ending address, the distribution of the basic block size, which is the number of instruction within a basic block.
3.2 The results using benchmarks

Fig 2 shows the distribution of the basic block size for the benchmarks. As you can see in the figure, most of the basic block size is less than 25. For 4 benchmarks, about 95 percent of the blocks have no more than 15 instructions and about 71 percent of the blocks have no more than 5 instructions. It represents that about 17 percent of the basic blocks have one instruction. Therefore, it’s possible to detect abnormal execution patterns using our method.

4 Conclusion

To tackle unknown security attacks, we presented a novel approach for detecting the anomaly execution behaviors of an application program, based on the basic block information of each application. We examined how to identify the boundary of normal execution behaviors effectively. The basic block information is used for finding an anomaly execution behavior of an application program.

References

Multi-resolution Image Authentication Watermarking Based on Progressive Image Transmission

Piyu Tsai¹, Yu-Chen Hu², Hsiu-Lien Yeh¹,³ and Wei-Kuan Shih³,

¹Department of Computer Science and Information Engineering
National United University, Miaoli, Taiwan, 36003
²Department of Computer Science and Information Management
Providence University, Taichung, Taiwan, 40006
³Institute of Information Systems and Applications
National Tsing Hua University, Hsinchu, Taiwan 30013
pytsai@nuu.edu.tw, ychu@pu.edu.tw, {hsiulien,wshih}@cs.nthu.edu.tw

Abstract. In this paper, a watermarking for multi-resolution image authentication is proposed. The most important image content with progressive characteristic is taken as the authentication code. The authentication code is then embedded/extracted according to multi-resolution image coding. The experimental results show the validity of the proposed scheme. The significant tampering can be detected firstly and slight tampering is detected in the later authentication stages. Furthermore, the positions of the tampered areas can be located correctly.

Keywords: Watermarking, image authentication.

1 Introduction

The digitalization and the Internet promote the digital multimedia distribution. However, the security issues of the digital multimedia over the Internet are becoming more and more crucial. To deal with the security issue, several approaches on how to authenticate digital multimedia are proposed [1]. They can be classified into digital signature-based and watermarking-based authenticators. The digital signature-based authenticator attaches the authentication code in file header [2]. Watermarking-based approach inserts authentication code into multimedia contents.

On progressive image transmission, the images will be reconstructed from rough to detail. However, the rough image should also be authenticated to assure the transmission security. A few of multi-resolution image authenticators have been proposed. In [2], SPIHT encoding stage number is the authentication code. The authentication code indicated magnitude is compared with the new magnitude to determine the authentication. In [3], the bit-stream of a certain resolution image is hashed as authentication code. The new and the original authentication codes are compared. In [4], the wavelet-based and network-conscious concepts are incorporated to develop a blind signature. Each multi-resolution image can be authenticated in real time. In [5], multi-resolution watermark is embedded into DWT sub-bands.
In this paper, a multi-resolution image authentication watermarking is proposed. The rest of this paper is organized as follows. In Section 2, the proposed image authentication scheme is introduced. The experimental results are shown in Section 3. Finally, some conclusions are given in Section 4.

2 The Proposed Scheme

To develop the image authentication scheme, the authentication code is first considered. In the proposed scheme, the authentication code is extracted from the image content which should contain the feature to authenticate the multi-resolution images. According that, the LL sub-band coefficients are taken as the authentication code. To embed the authentication code in image with imperceptibility, the authentication code is further scaled. The scaled authentication code is further rearranged. The first MSB of each LL coefficient is first extracted to form an MSB bit plane. And then, the second and the third MSB bit planes are generated. From that, the authentication code can be embedded according to their importance.

According to progressive image transmission encoding, the proposed three authentication bit planes will be embedded into HH, HL and LH sub-bands, respectively. The location of the embedding bit is determined according to the encoding threshold. Furthermore, compensation mechanism is explored to reduce the embedding distortion.

To authenticate multi-resolution images, the authentication bit plane is extracted according to their embedding sequence. Since the multi-resolution images can be progressively authenticated from rough to detail, the significant tampering will be detected in earlier authentication procedure and slight modification will be located in later authentication procedure. The authentication of the first and second authentication bit planes can be formulated as:

\[
\text{Authentication\_bits} = \begin{cases} 
11 & \text{est\_mag} \geq 192 \\
10 & 128 \leq \text{est\_mag} < 192 \\
01 & 64 \leq \text{est\_mag} < 128 \\
00 & \text{est\_mag} < 64 
\end{cases}
\] (1)

3 Experimental Results

Several simulations were implemented to evaluate the proposed scheme performance. Test gray-level images of 512x512 pixels were first transformed into four-level DWT coefficients by using the CDF 9/7 transformation. The authentication code is generated in which the first three MSBs of LL coefficients were extracted. There are 3072 authentication bits will be embedded.

Three authentication bit planes were embedded into HH, HL and LH sub-bands in encoding thresholds (T=8,4,2), respectively. The watermarked image shown in Fig. 1(f) was tampered with. The simulation results shown in Fig. 1 indicated that the
embedding distortion is less and the marked image preserves a good imperceptibility. Three resolution tampered images were verified and the tampered areas were marked.

![Images of original, watermarked, and detected images](image.png)

**Fig. 1** The multi-resolution original, Watermarked and Detected images

### 4 Conclusions

In this paper, a multi-resolution images authenticator is presented. The size of the authentication code can be adaptive to reduce embedding distortion and improve authentication precision. The experimental results show the reconstructed images can be authenticated according to the extracted authentication bits. Furthermore, the tampered areas can be located according to the degree of the tampering with.

**Acknowledgments.** This research was supported by the National Science Council, Taiwan, R.O.C. under contract NSC 100-2221-E-239-030.

### References

An Introduction to Privacy Critical Location-Sharing Services

Fei Xu1, Jingsha He2, Jing Xu1, and Yuqiang Zhang1

1 College of Computer Science and Technology
2 School of Software Engineering
Beijing University of Technology
Beijing 100124, China
{ xfei,hxj,yuqzh}@emails.bjut.edu.cn, jhe@bjut.edu.cn

Abstract. This is an introduction paper to privacy critical location-sharing services. We separate location-sharing services from location-based services in literature. The paper discusses the difference between location-sharing services and location-based services. We classify location-sharing services into several types and explain each service type in detail. Especially, we point out the location privacy concerns and current privacy protection methods in each service type.

Keywords: location privacy; location-sharing services; privacy protection.

1 Introduction

There has been little discussion in the literature about the differences between location sharing services and location based services. In some papers, location sharing services and location based services are referred as the same thing. But In this paper, we consider location sharing services as a special kind of location based services.

Location based services allows users to use their location real-time or historical information online. Different types of location-based services contains the following [1]: (1) navigation, use location information to navigate to another certain places; (2) information, use location information to get other information, such as travel and tourist guides or shopping guides; (3) tracking, use location information to track people, vehicle or product; (4) emergency, location information used in emergency calls or automotive assistance; (5) management, use location information to manage security or infrastructure; (6) leisure, buddy finder or instant messaging; (7) others.

In our paper, location sharing services refer to services that allow users to share their location with another user. Although location sharing services only refer to those services in which users can share their locations with others, there are different types of location sharing. Each type has its own features and privacy considerations. We introduce each type of location sharing service in the following sections.
2 Location Sharing Services

This kind of location sharing services is specially designed by service provider for location sharing. There are thousands of specialized location-sharing services right now. Google Latitude [2] allows a mobile phone user to allow certain people to track their locations. Latitude allows users to share their locations with their family and friends in real time. Users can adjust their privacy setting by choosing (1) which friends can see your locations; (2) how much information to share with each friend; and (3) where the location is and when to share it.

Loopt [3] is another example of location sharing services that allows users to share their location information with friends and user location information to get other information user need. Several privacy features that Loopt offers includes (1) 100% permission-based; (2) end user privacy controls; (3) closed private networks for “Live” location sharing; (4) frequent privacy reminders; and (5) privacy policy.

3 Location Sharing in Online Social Networks

Online social networks by its nature are to provide ways for users to connect, express themselves, and share content. As the need of users to share location continues to grow, many online social networks have added location sharing features to their applications.

Twitter [4] users can add their current location to their tweets. Although there are advantages of location sharing within Twitter, most of the reactions to location sharing are negative due to user's privacy concerns. Some users think turning on location Tweets is just asking for stalkers.

Facebook [5] launched location sharing feature “Places” on August 2010. The “Places” allows Facebook users to "check in" and announce their locations to members of their social network. Through a feature dubbed "Here Now," users can see which other Facebook users have recently checked into the same location. Facebook gives users really weak protection, even if not zero protection, on their location information.

4 Location Sharing in Certain Places

This kind of location sharing considers sharing location between users when the users are both in the same place. Conference Assistants is a typical type of this kind of location sharing. The purpose of Conference Assistants is to track individual attendees as they move around or to detect when they interact with each other.

SpotMe [6] provides a hand-held device called Spotme to users. With a Spotme device, users can identify themselves and provide their location information to the system. Participants in a conference can know who is around them within a certain range, if a certain person is nearby, and be notified when a searched person approaches. SpotMe users are not aware of who is seeing their locations and information. The users are continuously being tracked when the devices are on.
FLAVOUR [7] enables conference participants to determine their locations locally. The system cannot track the users and the users can decide who has access to their location information, when, and for how long. FLAVOUR also uses encryption to enhance privacy when share location information.

5 Ad Hoc Location Sharing

Ad hoc location sharing allows user to actively select who can receive their location information for a fixed period of time in a specific given situation. Users of ad hoc location sharing can share location with each other without the need of user subscriptions or accounts.

Disposable Maps [8] considers a particular location sharing situation when providing meeting participants with real-time location information of each other, which can enhance the process of people meeting each other. Disposable Maps allows users to select contacts from their phone’s address book to decide who can receive their up-to-date location information. User's location information is displayed on a web-based map. The approach also applies mechanisms such as peer-to-peer notification mechanism and unique URLs to enhance user privacy.

6 Conclusion

In this paper, we discussed the difference between location sharing services and location based services in which we classified existing location sharing services into four types. We introduced each type of location sharing service in detail and discussed privacy concerns and privacy protection methods. As location sharing services grow at an amazing speed, we believe that in order to better protect user location privacy in location sharing services, more work needs to be done in both research and practices.

References

3. LOOPT. http://www.loopt.com
Sybil Attacks VS Identity Clone Attacks in Online Social Networks

Lei Jin, Xuelian Long, Hassan Takabi, James B.D. Joshi

School of Information Sciences
University of Pittsburgh, Pittsburgh, PA, USA
{lej17, xul10, hat26, jjoshi}@pitt.edu

Abstract. Sybil attacks and Identity Clone attacks (also known as Profile Cloning attacks) have become significant security and privacy concerns for online social network (OSN) systems integrated with reputation or evaluation mechanisms. In both attacks, adversaries first create multiple identities and then launch attacks to compromise reputation or evaluation mechanisms in OSN systems. In this paper, we discuss and distinguish these two attacks. The comparisons between them are presented based on pre-requirements, network topology and attack impacts.

Keywords: Sybil Attack, Identity Clone Attack, Online Social Networks

1 Introduction

Some Online social networks (OSN) systems, such as YouTube and Digg, are integrated with reputation and/or evaluation mechanisms. One of the striking features in these OSN systems is that the popularity and the value of a resource, such as a video in YouTube and a piece of News in Digg, are driven by users’ participations and feedbacks. However, this feature is also attractive to adversaries who have incentives to distort the popularity and value of the resource. Generally, adversaries can launch Sybil attack or Identity Clone attack to achieve their malicious purposes. Sybil attacks [1] focus on creating multiple online user identities (Sybil identities) and try to achieve malicious results through these identities. In an Identity Clone attack (also called Profile Cloning attack) [2, 3], an adversary first creates similar or even identical profiles to impersonate victims in an OSN system. He then distorts the reputation and the value of a resource through the network involving faked profiles.

Sybil attacks and Identity Clone attacks look somehow similar in appearance since both attacks need to create a number of online identities, and use these identities to compromise the reputation and evaluation mechanisms in OSN systems. These similar attack patterns could confuse administrators of OSN systems. As a result, administrators may have difficulties in distinguishing between Sybil attacks and Identity Clone attacks and they may not deploy appropriate and efficient defense approaches against them. Therefore, it is vital for them to first distinguish between Sybil attacks and Identity Clone attacks. In this paper, we analyze and compare Sybil attacks and Identity Clone attacks in OSN systems based on their characteristics. To
the best of our knowledge, our work is the first attempt to identify the differences between a Sybil attack and an Identity Clone Attack.

2 Comparisons between Sybil Attack and Identity Clone Attack

In this section, we present the distinguishing characteristics of a Sybil attack and an Identity Clone attack based on the pre-requirements, network topologies and impacts of the attacks.

2.1 Pre-Requirements of Attacks

To launch a Sybil attack on an OSN system, an adversary needs to create multiple identities. According to our earlier survey [4], most OSN systems require a user to choose a username or input his e-mail address during the account registration process. This result indicates that adversary needs to have multiple unique usernames or a huge number of e-mail addresses for launching the attack. Thus, the adversary also needs to compromise this restriction in the registration process, in order to create many identities automatically.

To launch an Identity Clone attack, an adversary also requires a number of unique usernames and e-mail addresses for creating identities in an OSN system. Additionally, the knowledge of a victim (identity that is cloned) is another pre-requirement in an Identity Clone attack.

2.2 Network Topology

As shown in Figure 1, when a Sybil attack is present, a social network graph can be conceptually divided into two parts: one consisting of all genuine identities and the other consisting of all Sybil identities. The link connecting a genuine node to a Sybil node is called an attack edge [5].

In the network of an Identity Clone attack, there are two types of nodes: genuine nodes and cloned nodes. For example, in Figure 2, a large solid sphere is the target node while a large hollow sphere is the cloned identity created by an adversary and impersonating the target. The small solid squares are the other genuine nodes and the hollow squares are the rest of the cloned nodes created by the adversary to impersonate the target’s friends or potential friends.
2.3 Attack Impacts

A Sybil attack can be used to affect the popularity, reputation, value and other characteristics of resources in OSN systems by using Sybil nodes. An adversary can boost invaluable resources and resource providers who have bad reputations. He can also downgrade valuable resources and reputable resource providers. In addition, the adversary can launch spam attacks by requesting the Sybil identities to propagate malicious messages to their neighbor nodes. Similar to Sybil attacks, Identity Clone attacks can affect the popularity, reputation, value of resources in OSNs using fake profiles. Additionally, such attacks can also influence the choices made by victims’ friends using the trust built in friendships.

3 Conclusions

As the value of OSN systems is widely recognized, the incentive to attack such systems is rapidly growing. In this paper, we analyze two attacks: Sybil attacks by creating Sybil nodes and Identity Clone attacks by creating cloned profiles. Both attacks require adversaries to create multiple identities and focus on distorting reputation and/or evaluation mechanisms in OSN systems. In order to distinguish these two attacks, we have also discussed and compared their characteristics. We have demonstrated that the pre-requirements, network topology and attack impacts can be distinguished. We believe that researchers and administrators of OSN systems could use these different characteristics to understand Sybil attacks and Identity Clone attacks more comprehensively and then have more confidence to deploy appropriate defense approaches against them. As future work, we plan to develop a defense framework that works for both Sybil attacks Identity Clone attacks based on characteristics and differences we proposed in this paper. We will also validate our defense approaches in a real OSN system.

References

A Resilient Privacy Ensuring Protocol for Smart Metering in Smart Grid

Waleed Akram Baig, Faraz Idris Khan, Ki-Hyung Kim, Seung-Wha Yoo

Department of Information and Computer Engineering
Ajou University, Suwon, South Korea
{waleedbaig, fikhan00, kkim86, swyoo} @ajou.ac.kr

Abstract. The next era is foreseen to revolutionize the utility application with the technological advancements in IT and telecommunication. Intelligence will be seen in industrial machines equipped with embedded technologies enabling communication using low power wireless technology. Smart meter has recently gained lot of attention from the research community as this has raised unique challenges especially w.r.t security. Privacy preservation in such an environment is discussed to be critical as it may lead to devastating effects or even blackout which has been witnessed before. In this paper, we propose a privacy preserving algorithm which ensures resiliency against credentials theft with cryptographic operations where they are transported in a secure manner. We evaluated different encryption algorithms RC5, MD5, SHA1 in terms of computational and communication resources consumed by them in the proposed privacy preserving algorithm. In future, extensive evaluations and proofs of cryptographic algorithms will be included.

Keywords: Privacy, Wireless Sensor Network Security, Public Key Infrastructure, Smart Grid Security, Smart Metering Cyber Security, Secure Payment

1 Introduction

In the near future, advances in IT infrastructure have broadened its horizon to utility management system. As an example, Smart metering application which collects electricity usage in real time and periodically report them to collector devices in the neighborhood. The collector transports the aggregated data to the control centers for pricing. There is a chance that data at any point of the collection process might get modified, dropped, eaves dropped or forged which affects the pricing. In addition, there is a risk of overwhelming the metering network resources often termed as LLN (Low Power and Lossy Network) characterized by resource constraints. It can be inferred that security schemes for such nature of network should be lightweight with low computational and communication cost. In literature, we encounter some efficient schemes as in [1] where data in batch is authenticated using cryptographic techniques from network security. Moreover, privacy is indicated to be of prime concern in Smart Grid deployment [2]. Revealing meter reading data leaks personal information.
This exposes customer habits and behaviors which assists the agent in making decision and launching devastating attacks destroying the network. DoS attack is one such kind of attack where eaves dropped data can be replayed elsewhere exhausting network resources.

Recently, WSN (Wireless Sensor Networks) has gained widespread attention over the years. It is considered to be one of the hot candidates over the years for various industrial applications i.e. process monitoring, industrial automation. Lately, it is been considered for Smart metering network where meters will be equipped with sensors assisting in collecting and aggregating data in the network [3].

Preserving privacy in WSN is already indicated to be an area that needs acute attention from the researchers as mentioned in [4]. WSN paradigm works in a similar fashion as that of Smart metering network as they collect, transmit and analyze the aggregated data. Privacy is indicated to be of concern especially for applications like medical monitoring application which monitors patient’s parameters like blood pressure, sugar level of critical privacy concern [4]. In [4], a comprehensive taxonomy can be found where the privacy preserving issue is classified into Data oriented privacy protection (protection of private data) and Context oriented privacy protection (protects location of data source and base station). The preserving techniques for WSN can be found feasible to implement in smart metering network due to its similarity. Data oriented privacy protection schemes which in summary ensure privacy of the aggregated data at various levels is quite relevant to AMI (Advanced Metering Infrastructure).

Security is a critical issue in a modern smart metering application. In case, of a common attack if a third party learning the behavior of the customer maliciously can use the information to achieve their own objective. It is important that the supplier should ensure the trustworthiness of consumption profiles. There is a chance that with the alteration of profile the output of the billing system results in a lower or higher value. This leads to a desire need of a whole security system constituting of cryptographic algorithms which signs and verifies the collected data at various stages of the collection process. One such work can be found in [5] where authors have proposed a plugin privacy component that acts as a mediator between the metering network and the system at the control center billing on the basis of the collected data. The suppliers ensure the integrity of the generated bill with some proposed operations signed data and tariff to come to the conclusion that the bill is to be trusted.

In this paper, a resilient privacy preserving algorithm is proposed for smart metering application preventing malicious server from stealing credentials. For this, we propose a protocol is proposed that uses simple cryptographic operations at each phase of the payment protocol.

2 Privacy Preserving Scheme

Privacy Preservation scheme is summarized in Fig.1.

Setup Phase

1. Key Generation Process
   KeyGen,seed) := (PubK, PrivKp)
   KeyGen,seed) := (PubK, PrivKu)
KeyGen\text{seed}(seed) = (PubK_m, PrivK_m)
KeyGen\text{encrypt}(seed) = (PubK_{encrypt}, PrivK_{decrypt})

2. Secure broadcast of $\text{KeyGen}_{encrypt}(seed)$

3. Encryption and Decryption process at the Provider
   \[ \text{Encrypt}(\text{Keys}) := E_{encrypt}(PubK_{encrypt}, PrivK_p) \]
   \[ \text{Encrypt}(\text{Policy}) := E_{encrypt}(PubK_{encrypt}, P) \]
   \[ \text{Decrypt}(\text{Keys}) := D_{decrypt}(PrivK_{decrypt}, Encry(\text{Keys})) \]
   \[ \text{Decrypt}(\text{Policy}) := D_{decrypt}(PrivK_{decrypt}, Encry(\text{Policy})) \]

Meter Usage Phase
Signining and Verification at Meters
\[ S(M) := \text{Sign}(PubK_m) \]
\[ V(M) := \text{Verify}(PrivK_m) \]

Payment Phase
Signining and Verification of Payments at the provider
\[ S(P) := \text{Sign}(PubK_u) \]
\[ V(P) := \text{Verify}(PrivK_u) \]

Fig.1. Privacy preserving algorithm

3 Conclusions and Future Work

In this paper, we have proposed a more resilient privacy preserving protocol for Smart Metering infrastructure. A typical smart metering payment protocol in general works in three phase: setup phase, meter data usage phase and payment. Furthermore, we devise an attack model where a malicious server can steal security credentials and impersonate to force the customers to pay it. A privacy preserving algorithm is proposed which provide resiliency by using the keys generated at the setup phase where the key used for encryption is broadcasted securely to the users. This step ensures secure transaction later on with payment made to authentic provider server. For future work we plan to look into suitable lightweight cryptographic algorithms and with the derivation of their proofs. Furthermore, we plan to look into tradeoffs when providing resiliency and ensuring light weight algorithm.

References

A User Oriented Negative Access Control Model in Cloud Computing

Xiaohui Li¹, Jingsha He¹,², Ting Zhang¹

¹College of Computer Science and Technology, Beijing University of Technology
100124 Beijing China
²School of Software Engineering, Beijing University of Technology
100124 Beijing China
lixiaohui@emails.bjut.edu.cn

Abstract. Cloud Computing provides an easy, convenient service that is mostly transparent to the user. Unfortunately, the side effect of flexible service is information overload. Information overload causes cloud users to lose their ability to manage thoughts and ideas. In this paper, we propose a negative access control model enhanced with user independent right to select information. Our main contributions include followings. (1) We propose a novel conception of negative access control which adopts first control last access to optimize performance and improve efficiency. (2) Cloud users can select key words or characters for their own required information, which is a user oriented way to obtain service. (3) Our model can be used in various information service with the more user information provided, the more accurate services available.

Keywords: User oriented; Information overload; Negative access Control; Cloud Computing

1 Introduction

As information growth continues to expand at an exponential rate, we are drowning in a rising sea of information. Cloud computing redefines information service and offers a value proposition based on convenient services that you pay for as you go. But we enjoy the same benefits and suffer the same frustrations of the exploding information. How to ensure the information we receive is exactly what we want.

In this paper, we propose a user oriented negative access control model in cloud computing for optimization of information services, improve cloud users satisfaction. The model is flexible enough to provide the cloud users with the capability of giving their selective preferences and making access decisions at their own discretion.
2  Related Work

To our knowledge, there is already some access mechanism to control excessive and useless information.

Personalized access control [1-4] and access filter [5] can be used to choose value information through subjective, but access filter is the way to add a barrier by subject while receiving the results; personalized access control is still to provide the more information, more access to the information service. They are both based on the static information and adopt first access last control mode. In essence, they do not reduce the burden of the vast amounts of information to the user and system. In the cloud computing environment, the cloud terminal is resource-constrained, these methods are not applicable. So we propose a novel negative access control model to handle individuals and systems to select the information needed in cloud computing (the high convergence occasions) from a new point of view in this paper.

3  Negative access Control Model

In the section, we first introduce the entities in the negative access control model and describe the architecture and the components that make up our model in details.

3.1  Entities in the model

Our model is made up of three types of entities:

- User’s proper information include: Users’ requirement, such as active input, feedback; Context information, such as identity, habit, hobby, history of information service.
- Cloud user: the user of information services in the cloud computing environment, All the information service must be directly or indirectly made by the user.
- Cloud server: The main part of model to make negative access decision, through the user's proper information to offer the Cloud user information needed, the information comes from two parts: the public useful information of read rate as a standard; the information collection of user's proper information as input conditions.

3.2  Architecture of the model

The architecture of our negative access control model can be described five building blocks. To get a good picture of our model we should describe:

- Cloud user segment: Specify as cloud computing environment information service users
- Requirement segment: User active require information services by request or feedback
• Context segment: Relatively active requirement speaking, this segment generates filter term of whole information for user without users’ any instruction
• Cloud server segment: The most important activities performed to implement our model
• Information service: The bundles of services that satisfy our user segment’s needs.

As the most important part of the model, the following describes the cloud segment in details.

Cloud server segments: this module process the context information by four steps.

Step1. Scan the context information that consists of the users' requirement and context information as the input conditions, Based on user interest categories A1, A2, ..., An, To ensure that A1, A2, ..., An, independent, there is no intersection.

Step2. let A be a finite universe \( U = \{X_1, X_2, ..., X_n\}\) fuzzy sets, \( U \) is the collection of all information in the cloud server, A is the collection of cloud user information composed by \( A_1, A_2, ..., A_n \), \( X \) is the element of \( U \) in the cloud server, that is the composition of our cloud user information service set.

According to formula 2, \( A = \mu_1/x_1+\mu_2/x_2+...+\mu_n/x_n \) Where "+" shows a concepts of collection, not the sum of arithmetic. The denominator is the element of domain, molecule is the membership degree of element to A.

Step3. According to the previous formula, select \( \mu_A(x) \leq 0.6 \), Choose to meet a fuzzy set \( A_1 \) of all \( x \), delete operation. for \( A_1 \cap A_2, ..., \cap A_n \subseteq \cdots, \subseteq A_1 \cap A_2 \subseteq A_1 \).

Step4. The information service results include two parts: a public concern (selected according to the read rate); one is the selection results of the third step.

4 Conclusions

In this paper we describe a novel negative access control model to better improve user’s satisfaction to information services in cloud computing. Our model has at least three advantages. First, it is very novel of first control last access and can support user oriented information requirements in cloud computing. Second, the users provide the more information themselves the more accurate information obtained. Third, the cloud users can decide their information obtained from cloud server without requiring any additional burden.

References

6. L. A. Zadeh.: Fuzzy sets. Information and Control 8 (3) 338 – 353(1965)
Encryption Extensions Model based on Hidden Attribute Certificate

LI Yu1,2,3, ZHAO Yong1,2,3, GONG Bei1

1 College of Computer Science and Technology, Beijing University of Technology, Beijing, China
2 State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China
3 Key Laboratory of Information and Network Security, 3rd Research Institute, Ministry of Public Security, Shanghai, China
liyue_mail@163.com, zhaoyonge_mail@sina.com, tekkman_blade@126.com

Abstract. An encryption extensions model based on hidden attribute certificate is proposed in this paper, which can represent any key by using "and", "or" logic and the threshold monotony of the access rules, and in order to resist the collusion attack, multiple users use a combination of their keys to decrypt the ciphertext, it virtually eliminates the possibility of a conspiracy to know the key.

Keywords: identity-based; attribute-based; hidden attribute; certificate

1 Introduction

In the cross-domain large Internet network, in order to ensure users’ own security, before the communication with others, users must first assume whether the others are potentially malicious objects, only after the full test of the mutual contact and authorization certificates interaction, communication and transactions subjects can establish trusted relationships in distributed environment. The existing hidden certificates has obvious drawbacks in the following: in an open environment such as the Internet when users cooperate with unfamiliar parties (such as permission for access to resources), it often based on the requesting party of some vague set of features, but the identity of the requesting party is not clear. To solve the problems above, this paper proposed an improved ABE program, which can represent any key by using "and", "or" logic and the threshold monotony of the access rules. In order to resist the collusion attack, multiple users use a combination of their keys to decrypt the ciphertext, each attribute certification body has a pseudo-random function PRF for random distribution of keys. In this way, it virtually eliminates the possibility of a conspiracy to know the key.
2 System Construction

$A_u$ is the attribute set of $u$, $A_c$ is the user’s attribute set which is used to generate ciphertext.

A hidden certificate extended model includes the following:
1. System configure function: Setup, which is run by the authority center, it will generate the public parameter params and the main key master-key;
2. Certificate distribution function: CA_Issue, which is run by the authority center, it will random select polynomials to create the certificate for each user and issue the certificate to each user, each certificate component correspond to a user’s attribute; when user acquires the certificate from the authority center, the user can use the only disguise name nym;
3. The encryption function: $CT=HCE(R \cdot nym \cdot A_c)$, which is run by the authority center, it uses $A_c$ as the public key to encrypt the resource $R$, the receiver of $R$ is nym, CT is the ciphertext, $A_c$ is the access control policy, it is contained in CT;
4. The decryption function: $R=HCD (CT \cdot Cred)$, which is run by the authority center, it decrypt the ciphertext CT, the public key of the certificate cred is $A_c$, and if and only if $|A_c \cap A_u| \geq d$ is true, it can decrypt the resource $R$, $d$ is the determined threshold.

It is worth noting that this system does not give the user a certificate issued for each attribute, but the system issues the certificate for each user, a certificate for each component corresponds to an attribute of the user. If the "issuing a certificate for each attribute" method is used, multiple users will be easy to collude with their attributes that they cannot decrypt the certificate to decrypt the ciphertext alone, the system will be vulnerable to collusion attack.

3 Trust negotiation process of multi-sides

Trust negotiation process of multi-sides based on ABE hidden certificate (User A requests a file $R$ which satisfies the access control policy from all the users) is shown in Figure 1:
1. A sends $Ta=HEs$ (request, Prequest) to every user;
2. When the user who receives the request can not satisfies Prequest. It will not decrypt the request, and it can not acquire the access control information, the certificate set of B is CB, and the certificate set of D is CD, if B an D satisfies Prequest, it can decrypt request=HDs(Ta, CB) =HDs(Ta, CD);
3. B sends $Tb=HEs(Rb, PRb)$ to A, D sends the resources $Td=HEs(Rd, PR d)$;
4. The certificate set of A is CA, if A can satisfies PRb, it can decrypt $Rb=HDs(Tb, CA)$, if A satisfies PRd, it can decrypt $Rd=HDs(Td, CA)$
Fig. 1. Trust negotiation process of multi-sides

Trust negotiation and trust of both parties in the process of encryption and decryption of the request, encryption and decryption resources use the basic ABE technology.

4 Conclusion

In this paper based on IBE / ABE's Web security technology, we proposed an improved ABE scheme which can represent any key by using "and", "or" logic and the threshold monotony of the access rules. In hidden the ABE certificate extended model, since each user only has a certificate, it needs only one chance to decrypt the information; it increases the efficiency of the system.

Acknowledgements. This research is funded by Open Research Project of State Key Laboratory of Information Security in Institute of Software Chinese Academy of Sciences, the program "Core Electronic Devices, High-end General Purpose Chips and Basic Software Products" in China (No. 2010ZX01037-001-001), Funds of Key Lab of Fujian Province University Network Security and Cryptology (20110009) and Doctor Launch Fund in Beijing University of Technology (X00700054R1764).

References

An Encrypted Verification Method for Effective Black Hole Attack in Mobile Ad Hoc Networks

Firoz Ahmed, Seok Hoon Yoon, Hoon Oh

School of Electrical Engineering, University of Ulsan, P.O. Box 18, Ulsan 680-749, Korea
jewelraaz@yahoo.com,{seokhoonyoon,hoonoh}@ulsan.ac.kr

Abstract. We propose an Encrypted Verification Method (EVM) that effectively detects a black hole attack. A detection node that receives an RREP from a suspicious node sends an encrypted verification message directly to destination along the path included in the RREP for verification. Simulation shows that it reduces control overhead and increases detection probability.

1 Introduction

We address the black hole attack problem when AODV [1] is used for routing in MANETs. A malicious node sends an RREP with a high destination sequence number in response to an RREQ in order to intercept data packets destined for destination. Black hole attack has been tackled in various ways. Some focused on verifying the correctness of the obtained path through the downstream node of the RREP initiator [2], [3]. In SNV [4], every RREP initiator sends a message to destination to ask for the destination to report its current sequence number to the source. However, the above first two approaches may not work appropriately if two black hole nodes cooperate with each other and the third approach produces high control overhead.

The approaches discussed above suffer from high overhead as well as the failure to address colluding attack. An encrypted verification method (EVM) proposed in this paper can resolve this problem effectively through two step approaches: Identification of a suspicious node and the verification of the suspicious node using an encrypted verification message.

2 Encrypted Verification Method (EVM)

2.1 Identification of Suspicious Node

For identifying a suspicious node, each node collects data by overhearing packets that its neighbors transmit and maintains a data collection table \((DCT_i)\) with those data as follows. \(DCT_i = (j, \text{From}_j, \text{Through}_j, \text{Suspicious}_j), j \in i.N\), where \(i.N\) is a collection of node \(i\)'s neighbors, \(\text{From}_j\) indicates whether or not node \(i\) has received a packet from node \(j\) ever, \(\text{Through}_j\) indicates whether or not node \(i\) has routed a packet via node \(j\) ever and \(\text{Suspicious}_j\) indicates whether or not node \(j\) is suspicious based on the
combination of \( \text{From}_j \) and \( \text{Through}_j \) fields. The values of \( \text{From}_j \), \( \text{Through}_j \), and \( \text{Suspicious}_j \) are given true (1), false (0), non-decidable (x).

Fig. 1. An example topology to define \( DCT \)

<table>
<thead>
<tr>
<th>( j )</th>
<th>( \text{From}_j )</th>
<th>( \text{Through}_j )</th>
<th>( \text{Suspicious}_j )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1</td>
<td>x</td>
</tr>
</tbody>
</table>

Table 1. An example of \( DCT_3 \)

Take a look at Fig. 1 and Table 1. Node 5 observes the data forwarding behaviors of its neighbors and records them in its data collection table, \( DCT_5 \). Node 5 has received data packet from nodes 1 and 2 (\( \text{From}_1 = \text{From}_2 = 1 \)). Thus it determines that both are reliable (\( \text{Suspicious}_1 = \text{Suspicious}_2 = 0 \)). However, node 3 did not send data to anyone, including node 5 and is determined to be suspicious (\( \text{Suspicious}_3 = 1 \)). As for node 4, node 5 cannot know whether node 4 has forwarded to a reliable node or a malicious node, and thus determines node 4 to be non-decidable (\( \text{Suspicious}_4 = x \)).

For the non-decidable node, we need further observation. It may be reasonable to assume that multiple different paths can go through the non-decidable node. A decision node can count the number of different downstream nodes to which the non-decidable node forward data packet by using the watchdog mechanism. If the number is over some threshold, it can determine the non-decidable node to be reliable.

### 2.2 Encrypted Verification Process

A node that receives RREP from a suspicious node, initiates a verification process to check if the suspicious node is a black hole. The node (detection node) extracts destination sequence number (\( dsn_1 \)) from the RREP and stores it in its cache. It then generates a Test Request message, \( TREQ = (\text{detection node address}, \text{destination node address}, \text{timestamp}) \) where the timestamp indicates a current time, and then encrypts it using public key cryptosystem and sends it along the path specified in the RREP. Upon receiving the TREQ, the destination creates a Test Reply message, \( TREP = (\text{detection node address}, \text{destination node address}, \text{timestamp}, dsn_2) \), and then encrypts it and sends it along the reverse path to the detection node. If \( dsn_1 >> dsn_2 \), the detection node judges the suspicious node is a black hole. Otherwise, if the detection node is not a source, it forwards the RREP towards a source node.

### 3 Performance Evaluation

Using the NS-2 [5], we compare EVM and SNV with Random Waypoint model, dimension of 1000\( \times \)1000 (m\(^2\)), 50 nodes, CBR with 4 packets per second, and simulation time of 300 seconds. We obtained an average value of five runs per each metric.
Fig. 2 and Fig. 3 show packet delivery rate and control overhead with varying number of malicious nodes, respectively. The packet delivery rate of AODV dramatically drops from 88 percent to 21 percent in the presence of one black hole node and it becomes worse as the number of black hole nodes increase. EVM has control overhead lower than SNV since it can send an encrypted verification message directly to destination which is protected from the modification of other nodes. EVM can detect a black hole more reliably for the same reason. The control overhead of AODV sharply decreases as the number of malicious nodes increases since a black hole node tends to hinder normal protocol operation such as message forwarding. EVM shows control overhead lower than SNV since it does not use flooding.

4 Concluding Remarks

The proposed EVM method can pin down multiple black hole nodes effectively by employing an encryption mechanism. We showed by simulation that the EVM could handle the black hole problem in terms of delivery ratio and control overhead.

References

A Model-driven Approach to Secure Development Lifecycle *

Zhendong Ma¹, Christian Wagner¹, Arndt Bonitz¹, Thomas Bleier¹, Robert Woitsch², and Markus Nichterl²

¹ Safety & Security Department, Austrian Institute of Technology
Siebersdorf 2444, Austria
firstname.lastname@ait.ac.at
² BOC Asset Management GmbH
Bäckerstraße 5, 1110 Vienna, Austria
firstname.lastname@boc-eu.com

Abstract. Building security into software development lifecycles and doing it right is hard. To address the challenge, several prominent organizations have published process-oriented security guidelines to bring security activities into a structured way. Often they are too verbose and fuzzy to be implementable in a development lifecycle involving people with different skillsets. In this paper, we propose the model-driven secure development lifecycle (MD-SDL), an approach that leverages on modeling methods and the advances in model-driven security to simplify the process of efficiently integrating security into development lifecycles.

1 Introduction

Building security into software systems requires specialized skills and collaborations among different participants. A large number of activities related to security needs to be performed throughout a software’s development lifecycle. In the past, two promising approaches appeared to address security challenges in security engineering in software development lifecycles. The first is model-driven security [1–3], which applies models in security engineering to gain more focused views of complex systems and uses levels of abstraction to assist non-security experts (e.g., developers) to implement security in a correct and efficient way. The second approach is the definition of guidelines for security activities involved in a software’s development lifecycle. Several organizations comprise lists of “todos” [4–6], i.e., activities regarded as best practices on the technical as well as the organizational level.

In this paper, we propose the model-driven secure development lifecycle (MD-SDL). Our approach combines rigid modeling methods and efficiency gained from model-driven security with process-oriented security development lifecycle guidelines to produce structured, practical, and efficient security engineering practices in software development lifecycles.

* This work was partly funded by the Austrian security-research programme KIRAS and by the Federal Ministry for Transport, Innovation and Technology.
2 Model-driven Secure Development Lifecycle

“Model-driven” in this paper refers to: (1) use security engineering techniques that follow principles defined in model-driven architecture, (2) use modeling method engineering to structure and support security activities in a development lifecycle, and (3) use models as a part of the artifacts in the development lifecycle. By adopting a model-driven approach to SDL, we aim at achieving the following goals: (1) To tackle complexity in software system. (2) To bring software into tangibility. (3) To conduct security engineering in a structured as well as flexible way. (4) To facilitate clear and effective communications among stakeholders. (5) To provide accurate and extensive documentation support.

The model architecture is designed to be a framework for the MD-SDL process. Our design reflects the opinions from both the security experts and the modeling experts. It also reflects our accumulated experiences in security research projects, modeling projects, and software development projects. Figure 1 shows the overall model architecture. Notice that as a first attempt to apply model-driven approach to secure development lifecycle, we focus only on the requirement, design, and implementation phase since our work centers around security design and proof-of-concept implementation. The model architecture is designed to fulfill the aforementioned goals. A part of the architecture consists of loosely connected existing security engineering techniques and tools. Each development phase includes several model components. A model component might further include several sub-components. The model architecture connects these components into a holistic framework and ensure that the artifacts and documents from one component is related to the other corresponding components.

![Fig. 1. Architecture overview of MD-SDL](image)

In our approach we choose the platform provided by the Open Model Initiative [7]. Beside our consideration to avoid proprietary software, the main reason for choosing this platform is that it provides a community-based working environment and hence applies the open source concept to modeling method engineering. With regard to modeling method engineering, the Open Model Initiative provides foundational material, tools, and platforms. It also supports different modeling method engineering with specification, implementation and
deployment of modeling methods. Using the Administration Toolkit and Modeling Toolkit provided by Open Model, we can define meta models on an abstract level and then develop concrete instance models. On the Open Model platform, meta models are defined by classes and relation classes with certain attributes. The defined class is available as an object in the Modeling Toolkit and can be used for implementing model instance. The graphical representation of objects is defined by GraphRep attributes of the class. Furthermore, we add semantics to the models by defining relation classes that control the objects’ connectivities. We adopt a hybrid approach to implement the MD-SDL framework, such that we can take advantage of the latest development in the field. Currently, the models serve as an integration framework that bundles and “glues” existing methods and tools. For example, for system modeling we use UML modeling techniques; for threat modeling we adopt the Microsoft SDL Threat Modeling approach; and for code generation we use code generator developed in [8].

3 Conclusion

This paper proposed a new approach to integrate security activities into software development lifecycles based on modeling methods and the progress made in model-driven security. Our goal is to have a framework that is practical, extendible, and reproducible for different security-critical software development and research projects. Our next step is to apply the MD-SDL approach in our ongoing and upcoming security activities and promote the usage among our project partners. The results and feedbacks will be used to improve the framework and provide evidence on the feasibility of this approach.

References

Analysis of Human Identification based on Soft Biometrics in Video Surveillance System

Min-Gu Kim¹, Hae-Min Moon², Sung Bum Pan³,⁴

¹ Dept. of Control and Instrumentation Engineering, Chosun University
375 Seosuk-dong, Dong-gu, Gwangju, Korea
happy9433@gmail.com

² Dept. of Information and Communication Engineering, Chosun University
375 Seosuk-dong, Dong-gu, Gwangju, Korea
bombilove@gmail.com

³ Dept. of Control, Instrumentation and Robot Engineering, Chosun University
375 Seosuk-dong, Dong-gu, Gwangju, Korea
sbpan@chosun.ac.kr

Abstract. Biometrics was divided into traditional biometrics and soft biometrics. Traditional biometrics is a method using information on face, iris, and fingerprint. Soft biometrics is a method using information on gender, ethnicity, height, and so on. Recently, many researchers have been researched human identification using soft biometrics in long distance environment. In this paper, we analyze human identification with applying traditional biometrics or soft biometrics suitable for video surveillance system. Also, we propose framework to solve problems such as lighting, occlusion and shadow.

Keywords: video surveillance, soft biometrics, human identification.

1 Introduction

Traditional biometrics has advantages of excellent accuracy and high universality. However, it is difficult to extract the feature of face as the distance between camera and target is far, and in case of fingerprint, it has the disadvantage of requiring cooperation with the user. On the other hand, soft biometrics has narrow accuracy compared to traditional biometrics but it can be used in various environments and can verify the identity without cooperation with the user. However, since soft biometrics has low distinctiveness and permanence, it is not enough to recognize the individual if it is used by a single biometrics. Recently multi-modal biometrics is researched to verify the identity in various environments that are not controlled while achieving high recognition performance using traditional biometrics and soft biometrics together. In this paper, we analyzed biometrics for identification in video surveillance system and proposed framework to solve problems such as lighting, occlusion and shadow.

* Corresponding author
2 Framework of Human Identification using Soft Biometrics

2.1 Traditional Biometrics

Face and fingerprints are researched the longest among biometric information and are used in various fields because it has higher recognition rate than other biometric information. Identification technique using face is the most excellent in terms of convenience of the user because it can be recognized naturally without contact. But it is sensitive to the facial expression of the user or changes in lighting, and it also has a weakness in the change of face over the years. As the distance between camera and the user increases, it is also difficult to extract the face feature needed for identification.

2.2 Human Identification using Soft Biometrics

Recently, soft biometrics is researched to allow identification without various environments applicable to video surveillance system and cooperation with the user. But, it appeared that the elements like age, gender, ethnicity and occupation can affect performance of biometric system [1]. Therefore, Jain proposed the multi-modal biometric system that verifies the identity using Bayes Theorem [2]. However, if multi-modal biometric information is used, each of biometric information can have different results in identification. Thus, different weighted values were assigned in each of biometric information.

The clothing color is one of the information to verify the identity of a subject. First, the quantization technique is used to distinguish clothing color. The octree-based color quantization technique can configure the similar palette to the pixel value obtained from image because its memory utilization is low if an appropriate octree depth is specified, the velocity of quantization is also fast and it configures the dynamic tree for input image [3].

2.3 Framework Applicable to Long-Distance Human Identification

We propose the framework suitable for long-distance human identification as shown in Fig. 1. The experimental environment of proposed framework is assumed to be inside the building. The proposed framework obtains information on face, fingerprint, height and clothing color needed for identification from video surveillance camera and fingerprint sensor in short distance to determine the access of the subject at the entrance of the building.

If a subject is working inside the building where no fingerprint sensor is installed, the fingerprint information can’t be obtained because the fingerprint sensor is not used not like the environment of building entrance. If the subject is entered the building again after moving outside of the building, the information on height and clothing color can be changed. In this case, the identity can be verified by storing the new information on subject's height and clothing color in the database.
3 Conclusion

In this paper, we analyzed the identification technique using biometrics suitable for video surveillance system. Also, the framework was proposed to complement the problems of decreasing recognition performance due to lighting, occlusion and shadow. The human identification system using proposed framework is expected to improve the recognition performance by using various biometric information even though the feature extraction is difficult due to the environmental factors such as lighting, shadow and occlusion.

Acknowledgments. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2009-0086148) and was financially supported by the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation

References

A Semantic Rule-based Detection Scheme against Flooding Attacks on Application Layer

Chu-Hsing Lin¹, Chen-Yu Lee², Shin-Pin Lai¹, Wei-Shen Lai³,

¹Department of Computer Science, Tunghai University, Taichung, Taiwan, {chlin,g99350002}@go.thu.edu.tw
²Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan chenyu@cs.nctu.edu.tw
³Department of Information Management, Chienkuo Technology University, Taichung, Taiwan weishenlai@gmail.com

Abstract. With the progress the Internet, more and more applications provide Web services. The presentation of web page has evolved to be dynamic. You also can interact with the web page. Some malicious users have malicious browsing behaviors, such as flooding attack, to waste the resources and bandwidth of the host for web page. Nowadays, more and more web services are developed on cloud computing. Flooding attack on the application layer has no ability to cause denial of service to a Web server on cloud computing. But resources on cloud mean cost. Any waste of resource will cause unnecessary cost. Therefore, in this paper we analyze PHP dynamic pages. According to analysis, we propose a method based on semantic concept to formulate rules to identify malicious browsing behaviors in order to reduce the cost.

Keywords: Clouds, Flooding attack, Web service, Semantic web

1 Introduction

Dynamic web page servers face all kind of users and browsing behaviors and among these browsing behaviors some are malicious, such as flooding attack. The flooding attack is easy to detect on the network layer but is harder to detect when occurring on the application layer. Flooding attack on the application layer usually makes normal connection with web page server, and then through browsing behaviors, it wastes the resources of web page, such as CPU time, memory, and bandwidth. It is not easy to cause total denial of service on web page servers built on the cloud by way of flooding attack on the application layer, since this time the attackers are faced with high computation power and high bandwidth web page servers as following development of cloud computing technology. But continuous waste of web page server resources due to attackers will become unnecessary cost that cannot be overlooked by enterprise.

In this paper we proposed three algorithms to evaluate the cost of each critical page with the thresholds to determine whether the attacks occur.
2 Threats on the cloud web service

Many web sites have moved to cloud platforms as following development of Cloud Computing [1][2][3][4]. Web sites built on the cloud platform still suffer from HTTP Flooding attack, which will not break down the web page system completely but will still cause waste and extra cost on the system resources.

2.1 Cloud computing environment

We mainly focus on web page service on the cloud platform, of which web servers and application servers are constructed via the virtualization method.

2.2 Attack model

A web site breaks down under attacks such as HTTP Flooding attack. It is due to the facts of resource limitations of computing power and processing ability of the host servers. We grouped all the threats into three types:

a) Computation: attackers cause the system to perform substantial operations by sending specific request packets to increase the computation cost of servers.

b) Communication: attackers download large files repetitively from the web server to waste its network bandwidth.

c) Security: many threats, such as SQL Injection, XSS, and password guessing attacks belong to this type.

3 Computation algorithm

We use algorithm Initial_Setup to define malicious threshold and score of every page. We will determine the max request time $T_{max}$ of pages and set its score $S_{Tmax}$ as 10. Then we let the calendar page be standard. Its score supposes 10. Scores $S[i]$ of other pages refer the standard. Scores of every page are 0.86, 0.65, ..., 10, 0.65, 0.2. Finally, we compute the total score $S_{Total}$.

\[ S_{Total} = \sum_{i=0}^{n-1} S[i], \quad n = \text{size of site}; \]

Algorithm Initial_Setup()

begin

$T_{max} = Max(R_{req}[i]), \quad i = 0..n-1;$

$S_{Tmax} = 10$

$S[i] = (R_{req}[i] / T_{max}) S_{Tmax}, \quad i = 0..n-1;$

$S_{Total} = \sum_{i=0}^{n-1} S[i], \quad n = \text{size of site};$

end.

If user changes pages under limit time, we record the page of request by user and compute the score and compare with $S_{Total}$. If the score of user is over the $S_{Total}$, we can identify the user that is malicious.
For dynamic page, we use algorithm Update1 to update the malicious threshold and score of every page to detect SQL injection. We dynamically record the dynamic request time from user and calculate the total request time Total, average dynamic request time $R_{\text{average}}$ and $S'[i]$. Finally, we compute the total score $S_{\text{Total}}$.

Algorithm Update1 ()
begin
    For $i = 0$ to $n-1$
        For $j = i$ to $n$
            $Total = Total + R_d[i][j];$
            $Number++;$
            $R_{\text{average}} = Total / Number;$
        For $i = 0$ to $n-1$
            $S'[i] = \frac{R_n[i]}{R_{\text{average}}} \times S_{\text{max}};$
            $S_{\text{Total}} = \sum_{i=0}^{n-1} S'[i], \quad n = \text{size of site};$
end.

4 Conclusions

In this paper, we proposed three algorithms and policies to identify malicious users by figuring out some characteristics of malicious users and to evaluate the cost of each critical page with the thresholds to determine whether the attacks occur in real time. For the future work, we planned to figure out more and more characteristics to make our method completed and to verify its efficiency, the detection rate, and the false decision rate, and to compare it with other detection methods.

Acknowledgment. This work was supported in part by Taiwan National Science Council under grant: NSC 99-2221-E-029-039-MY3.

Reference

A Cloud-aided RSA Signature Scheme for Digital Forensics Applications

Chu-Hsing Lin¹, Chen-Yu Lee², Tang-Wei Wu¹,

¹Department of Computer Science, Tunghai University
407 Taichung, Taiwan
{chlin, g99350031}@thu.edu.tw
²Department of Computer Science, National Chiao-Tung University
1001 Ta-Hsueh Road, HsinChu, 30050, Taiwan
chenyu@cs.nctu.edu.tw

Abstract. The privacy of data or plain is an important issue in cloud computing. Therefore, to solve the problem, we establish the environment of cloud computing to process data with privacy and apply our scheme in the area of digital forensics for RSA signature algorithm. We experiment with efficiency of RSA signature in cloud computing. As a result, our scheme can reduce the loading of computing; besides, the clients don’t need to waste storage spaces to save the results. The most important of all, we can take full advantage of the cloud computing for computing of large data and storage spaces.

Keywords: Cloud computing, Digital forensics, RSA signature, Privacy

1 Introduction

Recently, cloud computing have been a new fashion noun in Information Technology, and the data security have become a new issue in the cloud computing. Most mobile devices, such as cell phone, can’t process large size data; they depend on the cloud services with rich resources.

The storage of sealed digital evidences of crime forensics [1][2][3] would change from traditional photo, video types stored in a specific building to cloud services via Internet. The powerful computation and high speed communication cloud services will speed up the sealing process, logistical forensics engineering. However, it would be unsecure at the first part of the scenario, the digital evidences sent from the mobile devices at the first line to the cloud service. The evidence would be sent in plain text, without encryption to the cloud service through the Internet, but it would suffer from eavesdropping by any malicious people. If the evidences need to be sent under encryption, nevertheless the mobile devices would have insufficient computation power to perform the necessary actions.

In the paper, we improved a secure protocol model [4] to propose a novel scheme that achieves the requirements needed in the mentioned scenario to make sure the security of sealing and storing the digital evidences from first line people to the cloud services. The rest of the paper is summarized as follows. Section 2 enhances the
protocol to be better in burden of computing and storage. Section 3, we will analyze the results of experiment between tradition and cloud structure. Finally, conclusions are given in Section 4.

2 The Proposed Structure in Forensics

In this section, we described the steps of uploading the digital evidences to the data center of forensics with privacy and downloading for verification. The cloud data center of forensics are divided into two services, cloud computing center and cloud storage center. Suppose that the forensics officers want to store the digital evidences \( DE \) on the forensics data center in the cloud. The stored digital evidence should be encrypted by the aid of the cloud server as \( C = DE^d \mod n \), where \( n = p \cdot q \), and \((p, q)\) are two distinct prime numbers.

In the cloud computing center, the cloud data center couldn’t know what the forensics officers upload, and still finish the work forensics officers want to do. On the other hand, forensics officers permute the \( DE \) by using the low computing functions and send it to the computing center. After the encryption at the computation center, it is then sent to storage center to seal up for keeping. The detailed steps are described as follows.

Forensics officers’ part:

1. **Step1:** Generate \( t \) random numbers \( a_1, a_2, \ldots, a_t \) such that \( p \) and \( q \) are not divisors of \( a_i \) and compute \( a_0 = (DE^{r} \prod_{i=1}^{r} a_i) \mod n \), for some \( r < t \).

2. **Step2:** Compute \( b_i = a_i^2 \mod n \), for \( i = 0,1,2,\ldots,t \) and compose the results to a vector \( B = G(DE,(a_0,a_1,\ldots,a_t)) = (b_0,b_1,\ldots,b_t) \). Last, forensics officers send the result \( B \) to the cloud computing center.

Cloud computing center:

3. **Step3:** On receiving \( B \), the cloud computing center permute on \( B \) by using random permutation \( \psi \). Let \( B' = \psi(B) = (b'_0,b'_1,\ldots,b'_t) \).

4. **Step4:** Compute a vector \( V = F(B') = (v_0,v_1,\ldots,v_t) \), where \( v_i = (b'_i)^{(d-1)/2} \mod n \). Finally, send the signature \( V \) to cloud storage center.

Cloud storage center:

5. **Step5:** On receiving \( V \), the cloud storage center compute \( U = \psi^{-1}(V) = (u_0,u_1,\ldots,u_t) \) where \( \psi^{-1} \) is the inverse permutation of \( \psi \). Note that \( U = F(B) \).

6. **Step6:** Compute \( C = (u_0a_0)\left(\prod_{i=1}^{r} u_i\right)\left(\prod_{i=1}^{r} a_i\right)^{-1} \mod n = DE^d \mod n \).

Finally, store the result \( C \) in this center.

Verifier:
Step 7: Download the result $C$ from cloud storage center, and verify the $C$ by $e$ associated public key to obtain the result is $DE = C^e \mod n$.

3 Experimental Results and Analysis

We would like to compare the efficiency of computation with the cloud structure and the traditional structure on the same experimental experiment. Among them, we set the argument of RSA key length 1024, 2048 and 4096, the number of random number is 40, and run 100 times to obtain the average time. The results of the cloud structure represent a better efficiency than the traditional structure. The RSA-4096 in cloud structure is faster than the traditional structure about 0.68s, the RSA-2048 is about 0.14s, and RSA-1024 is about 0.06s. We find that if the key length is longer, and the execution time is lower. We can apply the cloud structure to some areas, such as digital forensics that we proposed in Section 2.

4 Conclusion

In this research, we propose a new digital forensics structure for RSA signature in cloud computing. This cloud structure can archive privacy, save computing power on mobile devices token by forensics officers. By RSA signature protocol, the verifier can verify the evidences in the court. Moreover, this protocol could be applied to many areas, such as digital forensics, online voting, or E-commercial, etc. We hope that we can accomplish online voting system in the future, and let it be used widely by people.

Acknowledgments. This work was supported in part by Taiwan National Science Council under grant: NSC 99-2221-E-029-039-MY3.

References

A Ticket based Authentication Scheme for Group Communication

Soobok Shin¹, Hongjin Yeh¹, Kangseok Kim²

¹ Graduate School of Information and Communications, Ajou University, Suwon, Korea
² Department of Knowledge Information Security, Ajou University, Suwon, Korea
{watermel, hjyeh, kangskim}@ajou.ac.kr

Abstract. With the advent of new generation of mobile access devices such as smartphone and tablet PC, there is coming a need for ubiquitous collaboration which allows people to access information systems independent of their access device and their physical capabilities and to communicate with other people in anytime and in anywhere. As the number of collaborators with a large number of disparate access devices increases in ubiquitous collaboration environment, the difficulties for protecting secured resources from unauthorized users as well as unsecured access devices will increase since the resources can be compromised by inadequately secured human and devices. In this paper we present an effective authentication scheme for secure and authorized end-to-end delivery mechanism of messages between entities (publishers and subscribers) for ubiquitous collaboration.

Keywords: Ubiquitous Collaboration, Authentication Scheme, Mobile Device

1 Introduction

In collaboration systems, a group of users generally work sharing collaborative applications and resources in their workgroups. The cooperation on the resources shared among them may hence produce new results on the shared resources. On the contrary, security is about restricting unauthorized access to resources and thus it is essential that security of collaboration environments as well as of collaborative applications running on them is ensured while providing openness only to users that are authorized to access them. Therefore, difficulties to deal with the conflicting goals of allowing and restricting accesses for resources among a group of users may happen in collaboration environment.

The study in [2, 4] presented a user authentication scheme using a ticket in mobile networks. Also the study in [1] presented a ticket based single sign on protocol among application systems. The benefit of the authentication using a ticket is that an authentication mechanism is based on the ticket given to a service server without the need of re-authentication. In heterogeneous networked environments including battery powered mobile devices, an authentication scheme should be lightweight. Therefore

¹ Author to whom correspondence should be addressed; E-Mails: kangskim@ajou.ac.kr
in this paper we present an effective authentication scheme to overcome limitations of mobile devices (with high network latency and low computing performance) in ubiquitous computing environment.

2 Authentication scheme for ubiquitous collaboration

In this section we present an authentication scheme for secure and authorized end-to-end delivery mechanism of messages between entities (publishers and subscribers) in our messaging system.

2.1 Overall authentication procedure

A conference manager (CM) manages information related to all the conferences. The manager resides on web server running on tomcat. The manager is responsible for user’s registration, issuing a ticket to entities, and managing revocation lists. The issued ticket is specified with a secret number for a participant, a set of sessions, a right information in the sessions, and a lifetime of the ticket. After a subscriber is registered, she transmits a join request message and her ticket to a chairperson (CP). The CP authenticates the subscriber through the ticket.

2.2 Proposed authentication scheme

The proposed scheme is divided into two phases. The first phase is for registration / ticket issue as shown in Fig. 1. The second is authentication / session joining phase through the ticket as shown in Fig. 2.

Fig. 1. Protocol for registration and ticket issue, where $E_k(M)$ means encryption of message $M$ using key $k$ and $D_k(M)$ means decryption of message $M$ using key $k$.

2.2.1 Registration and ticket issue phase. A user registers to CM for joining a conference and gets a ticket and group session keys issued from CM. The group session keys are generated from key management center (KMC [3]). A user $u_i$ transmits registration / ticket request message. CM generates $x_i$ (secret number), $P_i$ (information about registration), $K_i$ (group session keys) and the ticket $Ticket_i = (x_i, P_i, life-time)$ and transmits $Ticket_i$ and $K_i$ encrypted by $k_{login}$ to $u_i$. Also CM transmits $x_i$
encrypted by group key to related CPs. CPs decrypt the message received from CM and add \( x_i \) in session / presence list.

### 2.2.2 Authentication and session joining phase.

The participant submits the ticket issued from CM to a CP for joining a session. After a participant who wants to join a session \( t \) generates a time-stamp \( T_i \) and encrypts her ticket and the time-stamp by a group key \( k_t \) of the session \( t \), she transmits the encrypted message to \( CP_t \). The \( CP_t \) decrypts the message using \( k_t \) and verifies \( T_i \), \( x_i \) and life-time. Also \( CP_t \) computes a filter function \( F_t(P_i) \) and verifies the value. Finally the \( CP_t \) publishes a joining message of the new subscriber to other existing subscribers and then they update their session / presence list.

![Protocol diagram](image)

**Fig. 2.** Protocol for authentication and joining a session where \( CP_t \) means a chairperson of session \( t \), Mem means a member of session \( t \), \( T_i \) means time stamp generated by \( u_i \) and \( F_t \) means filter function of session \( t \).

### 3 Summary and future work

In this paper, we proposed an authentication scheme for users joining a conference with disparate access devices. In our proposed authentication mechanism, a user can join all sessions by a ticket which is issued by conference manager and the computation for authentication is not complex because the length of ticket is fixed. Thus, our proposed scheme is effective even as mobile devices are involved for group communication. In future work we will analyze the security and the performance of our proposed scheme. Also, we will show the practical evaluation of the proposed scheme.

**Acknowledgments.** This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA (Korea Internet Security Agency).

**References**


MalSig: Collaborative Malware Clustering and Signature Generation using Rendezvous-based Sharing

Huabiao Lu1,*, Xiaofeng Wang1, Jinshu Su1

1 Collage of computer science, National university of defense technology, Changsha, China
ccmaxluna@gmail.com, {xf_wang, sjs}@nudt.edu.cn

Abstract. The sheer volume of new malware found each day is growing at an exponential pace. Centralized systems that collect all malware samples to central servers can cause problems of single point of failure as well as processing bottlenecks. Previous works on distributed and scalable malware analysis are mainly applied for specific or simple malware. This paper presents MalSig, a collaborative malware analysis system which is applied for various malware and has well scalable. Each nodes in MalSig analysis their own malware samples accurately in-situ with a global view; then MalSig aggregates those analyses in a load-balance way. Our experiment results confirm that MalSig has comparable performance with centralized system, but much better scalability.

Keywords: malware analysis; scalability; local analysis; global aggregation, signature generation.

1 Introduction

The battle against malicious software (a.k.a. malware) is becoming more difficult. The volume of new malware, fueled by easy-to-use malware morphing engines, is growing at an exponential pace [1]. In 2010, Symantec detected more than 286 million unique by hash malware samples, average 783,562 unique malware samples per day [1]. At the same time, security organizations usually deploy numerous widespread sensors to monitor the comprehensive malware samples. How to organize large number of sensors and analysis such many malware samples is a challenge.

Centralized systems that collect all malware samples to central servers [3, 5] can cause problems of single point of failure as well as processing bottlenecks. And previous works [4] on distributed and scalable malware analysis are only applied for specific or simple malware.

This paper presents MalSig, a collaborative malware clustering and signature generation framework which is applied for various malware and well scalable. Nodes in MalSig share their local view of malware behaviors through a rendezvous-based information sharing structure (RenShare) to gain global view of malware behaviors. Based on the global view, each node analyzes its own malware samples locally and accurately. Finally, MalSig aggregates those analyses in a load-balance way.
2 Malware Clustering and Signature Generation (MalSig)

Fig. 1 shows the architecture of our MalSig where each node contains two phases: local analysis stage and global aggregation stage. In local analysis stage, the monitor module logs the behavior sequences generated by malware samples, such as system call sequences or network connection sequences.

![Architecture of our MalSig](image)

**Definition 1:** *Sequence Fragments with length q.* giving a behavior sequence \( C = C_1, C_2, C_3, \ldots, C_n \), the subsequences \((C_1, \ldots, C_q), (C_2, \ldots, C_{q+1}), \ldots, (C_{n-q+1}, \ldots, C_n)\) are called *Sequence Fragments with length q*, or *Fragments* for short.

Local filter receives behavior sequences from monitor module, cuts the sequences into fragments, selects representative fragment set, and then according to DHT, sends each fragment to RenShare carrying with the local number of samples that have the behavior containing the fragment.

RenShare is a concept component, which is embedded among all nodes; each node is responsible for computing statistics of some fragments. Node in RenShare receives fragments according to DHT, so, the fragments with same value will converge at the same node. Node calculates the statistics (e.g., the number of samples containing the behavior of the fragment, or the set of source nodes monitoring the behavior of the fragment) for each fragment, and returns the statistics to its source nodes.

After receiving the statistics (the number of samples containing the behavior of the fragment) from RenShare, the clustering module calculates a weight for each fragment using the TF*IDF [2], and transforms each sample to a weighted vector composed of weights of fragments it contains, then clusters samples by agglomerative hierarchical clustering algorithm. Finally, cluster-Sig extraction module generates local cluster-Sig for each cluster, and like local filter, cuts the behaviors in cluster-Sig into fragments and sends them to RenShare.

After receiving the statistics (the set of source nodes monitoring the behavior of the fragment) of each fragment of cluster-Sig, MalSig enters into the global aggregation stage. Each node computes neighbor nodes for each of its cluster-Sigs; then sends the cluster-Sig to its neighbors. The neighbor finds the most similar cluster-Sig as the neighbor-cluster and returns the cluster-Sig ID and similarity weight; MalSig builds
HDHTs (heuristic distributed hierarchical aggregation tree) for each kind of malware in a distributed fashion; at last, nodes aggregate their local cluster-Sig along those HDHTs; finally, global cluster-Sigs will be generated at each root of those HDHTs.

3 Evaluation

We use n-gram of network connections as behavior in this experiment, run MalSig on 10 machines and the centralized system on 1 machine with same configure. We obtained a set of almost 400,000 malware samples from mwanalysis.org. We selected only those samples for which the majority of the AV scanners reported as the same malware family, the number of samples in the family must greater than 20, and the pcap file of sample greater than 1KB. This resulted in a total of 917 samples. Their families are used as reference clustering. We turn the global cluster-Sig to a cluster whose elements are those samples that match the global cluster-Sig.

We setup three groups of comparison. Group 1: centralized system as reference, estimate the performance of MalSig. Group 2: reference clustering as reference, estimate the performance of MalSig. Group 3: reference clustering as reference; estimate the performance of centralized system. Table 1 describes the performance of each group using precision, recall (higher the value, better the performance) as metrics. From table 1, we can see that the performance of MalSig is comparable to the performance of centralized system, and well consistent with reference clustering.

<table>
<thead>
<tr>
<th></th>
<th>precision</th>
<th>recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>group 1</td>
<td>0.98</td>
<td>0.83</td>
</tr>
<tr>
<td>group 2</td>
<td>0.67</td>
<td>0.81</td>
</tr>
<tr>
<td>group 3</td>
<td>0.54</td>
<td>0.93</td>
</tr>
</tbody>
</table>

Acknowledgments. This work is supported by PCSIRT (No.IRT 1012), and the National Science Foundation of China under Grant No. 61003303.

References

Surviving under large scale CXPST-like Attack

Hongjun Liu¹, Xiaofeng Hu¹, Dan Zhao¹, and Xicheng Lu¹

¹National University of Defense Technology, Changsha, China
seeker_lhj@163.com, xfhu@nudt.edu.cn, danzhao.nudt@gmail.com, xcluu@163.com

Abstract. In this paper, we propose two mechanisms to protect Internet from CXPST-like attacks: to isolate attacks in local region, unnecessary updates are suppressed without affecting the correctness of routing; to break down the route flapping which repeatedly generates updates, the paths selected are validated to detour the attacked links, which diffuses the deliberately attacks to random attacks. Simulation shows our methods greatly decrease the number of updates under such attacks, and isolate the attacks in local region of network.

Keywords: Failure isolation, CXPST attack, BGP, Path exploration

1 Introduction

Nowadays, some attacks aiming to the underlying infrastructure (such as the Border Gateway Protocol, short for BGP) of internet may result in significant harm to individuals or institutions. The well known coremelt [1] and CXPST [2] attacks can severely disrupt the routing system, which leads to network instability and losing of connectivity and data. We refer to these attacks as CXPST-like attacks, for the attacks share the common idea of exhausting the resource of routers by generating enormous update messages which results from terminating of BGP sessions.

In this paper, to defend against CXPST-like attacks, we propose two mechanisms to eliminate unnecessary update messages. Firstly, to isolate attacks in local region, some unnecessary updates are suppressed without affect the correctness of routing. Secondly, to break down the route flapping caused by repeatedly attacking the recovered links, the selected paths are validated to detour the attacked links, which results in the attacks are diffused to avoid deliberately attacking one target.

2 Our approach

2.1 Suppressing Unnecessary Updates

BGP has very poor fault isolation properties, small-scale local perturbations can be propagated globally across network. To avoid the global visibility, it is rational to
insulate the effect of attacks in local region by only propagating necessary updates. In this paper, we propose the judging criteria by considering the path length variation of different types of updates.

**Theorem 1:** Given the best path from AS $v$ to prefix $d \in u$ is $best_d(v)$, and AS $m$ belongs to the path, i.e. $m \in best_d(v), m \neq u \neq v$. If the best path of $m$ to reach $d$ changes from $p_1$ to $p_2$, and the length variation is $0 < |p_2| \leq |p_1|$, advertising the updates that contain $p_2$ does not change the partial path between $m$ and $v$ in $best_d(v)$, i.e. $best_d(v)^{m-v}$.

According to theorem 1, we only advertise the updates containing paths whose length becomes longer, which leads to the selected path becoming longer as time goes on. To avoid this situation, we advertise some path with shorter length only if the path is the preferred path [3], which is the path to one prefix that remains in the routing table for the longest time during a long time period. Thus the criteria of hiding unnecessary updates for isolating attacks in local region include:

**C1:** when the path length stays unchanged,
**C2:** when the path length become shorter, and the path is not the preferred path.

### 2.2 Broken Route Flapping

As the deliberately selected links in CXPST-like attacks are repeatedly failed and restored, which form routing oscillation, we breakdown the oscillation by detouring the attacked links. Thus it is vital to infer the location of the attacked links. We only consider the stable paths of the nearest affected prefix $d$ after the link is failed or restored, and the stable paths of the prefix before and after the event are denoted as $p_1$ and $p_2$. If the path set of $p_1$ and $p_2$ appears several times continuously, we claim that there is oscillation between path $p_1$ and $p_2$. By intersecting the two paths, we affirm the link that belongs to $p_2$ and is directly connected to the nearest prefix $d$ is the attacked link, for the CXPST-like attack is well known to terminate BGP session, and $d$ is the nearest prefix.

### 3 Evaluation

We choose SSFNET to generate events terminating and reestablishing BGP sessions using internet like topology, which has 200 ASes and 359 links. We compare our method with the standard BGP on the metrics of the number of update messages and the affected scale which is measured by the number of ASes observing the attacks. Our method can isolate the effect of link failures and recovery to a smaller scale, and largely decrease the number of updates, as shown in figure 1 and 2.
Fig. 1. Effect of isolation on link tear-down: (a) affect scale (b) number of updates

Fig. 2. Effect of isolation on link recovery: (a) affect scale (b) number of updates

References

Action Based Access Control Model for Multi-level Security (MLS)*

Mang Su¹, Fenghua Li², Guozhen Shi³, Li Li³

¹National Key Laboratory of Integrated Services Network, Xidian University, Xi’an, Shaanxi 710071, China;
²Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China;
³Department of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

{sm1222@163.com;lfh@iie.ac.cn;sgz@besti.edu.cn;lili103@besti.edu.cn}

Abstract. The multi-level security management is widely used in operation systems and information management systems. Focus on the multi-level security problem in various network environments, this paper defines the security identity, environment and temporal state of object, based on the ABAC(Action Based Access Control), and shows the security level, access scope and the demand of environment and temporal state of accessing subject, then proposes a multi-level security access control mechanism. Finally, an application example is given.

Keywords: multi-level security; access control; action; security level; structured document

1 Introduction

Multi-level Security[1] mainly focuses on analyzing, management and access authorization of information, which ensure information on different security levels can only be accessed by users with corresponding permission. BLP [2] and Biba [3] models protect the confidentiality and integrity, performing mandatory access control strategy. Multi-level security models are widely used in operating systems, databases and large information management system, such as J-S model [4] based on classical BLP model and multi-level security model VMAC [5] based on view, etc.

This paper mainly focuses on the new requirement for access control. The description of object in the ABAC model will be extended. The definition of the subject-object security level will be given. And Action Based Access Control Model

* Foundation: The National Natural Science Foundation of China (No.61172051); The Key Program of Scientific and Technology Research of Ministry of Education (No.209156); The Beijing Natural Science Foundation (No.4102056); The Major Science and Technology Project of Press and Publication - Research and Development Project on Digital Rights Protection (No. GXTC-CZ-1015004/05)
for Multi-level security will be proposed, which can meet the demand of objectified and fine-grained access control for multi-level security of structured documents.

2 Action Based Access Control for Multi-level security

2.1 Action Based Access Control Model

The above models have taken into account temporal and location related with access control on the characters distributed computing and mobile computing. But all of them do not analyze the environment of the role in detail, including physical positions, hardware platforms, operation systems and networks. Ref [6] presents an Action Based Access Control model (ABAC). The Model describes abstractly role, environment, temporal and is suitable to the information management for distributed computing and mobile computing. But this model doesn’t define and describe the situation of multi-level security problem. In order to solve this problem, the security security-level and scope of subject and object will be defined.

2.2 Action Based Access Control Model for Multi-level security

Based the definitions of ABAC, environment state and temporal state of subject, the security identity for both of subject and object, the environment state and temporal state for object will be described for multi-level security management. Security identity including the security level and scope is defined to show the level of subject or object and the scope for access or being access. For example, some detailed information of department finance will be only accessed by the related person. The environment state and temporal state have direct influence on operation. Operation to the object with certain level will be deceived by the environment of temporal of subject. Different physical position, device and time of subject need to be taken into account when assigning the operation to objects.

To meet the system requirements of access control for multi-level, The Role of User is extended as follow:

\[
R = [RV|RS] \tag{1}
\]

RV shows the level of the user in the such information system. RS shows the scope of the user, which can be similar with the ID of department.

Also the security identity is described further as follow:

\[
V = [VC|VS] \tag{2}
\]

VC shows the level of the object in the such information system. VS shows the scope of the department in which the user can access this subject.

Referring to NIST RBAC [7] and ABAC (Action Based Access Control) [6] structure, the structure for Action Based Access Control Model for Multi-level security is shown as in Fig.1.
3 Conclusion

This paper mainly focuses on access control model and mechanisms. Firstly, the concept of security identity of subject and object is introduced, including security level and access scope, and the description of environment and temporal state are also given. Then, combined with Action Based Access Control model, a new access model based on action and multi-level security is proposed. This new model can meet the demand of multi-level access control in pervasive networks. Finally, a multi-level security management example is given.

![Action Based Access Control Model for Multi-level security](image)

Fig. 1. Action Based Access Control Model for Multi-level security

References

Using Defeasible Description Logic to formalise Semantic Security Policy

Luokai Hu

Computer School, Hubei University of Education, Wuhan, China, 430205
State Key Lab of Software Engineering, Wuhan University, Wuhan, China, 430072
luokaihu@gmail.com

Abstract. Policy has been widely used in field information security. Semantic policy has being widespread concerned by the academic and industry world due to its powerful ability of expression. While policy conflicts have become a key issue constraining its application. In this paper, first a Semantic Security Policy Language (SSPL) is introduced. And we propose a Defeasible Description Logic (DDL) based formal method for Semantic Security Policy. Finally, on the base of this formal method, we descried the conflict detection approach for SSPL in briefly.

Keywords: Defeasible Description Logic; Semantic Security Policy; Formal Method

1 Introduction

In the situation of existing many policies (such as distributed systems or cloud computing environment), policy-makers may be more than one person. Conflict, overlapping and redundant may arise among policies or rules of a policy. Policy analysis is the key technology for the policy optimization and to ensure that policies can be executed properly.

With the development and maturity of the Semantic Web, description and expression of policy in the semantic level has become an important research direction. Because of its own powerful ability of description, the problem of conflict detection and resolution for semantic policy are more complex. In this paper, Defeasible Description Logic (DDL)\(^1\) based formal method for semantic security policy provides a new way of thinking to the policy analysis.

2 Semantic Security Policy Language (SSPL)

The Semantic Security Policy Language (SSPL) in which the necessary syntax elements and appropriate semantic annotation are added is designed on the basis of language such as XACML\(^2\) and WSPL\(^3\), in order to meet a variety of network and database security needs. SSPL is composed by three parts that is rule, policy and...
policy set. The syntax of SSPL rule and its DDL mapping is shown in table 1. Each SSPL rule has several consequents and may have an antecedent or not. $\mathcal{O}$, $\mathcal{A}$ and $\mathcal{D}$ denote strict, defeasible and defeat rule respectively.

**Table 1. DDL semantics of SSPL rule**

<table>
<thead>
<tr>
<th>No.</th>
<th>SSPL Syntax</th>
<th>DDL mapping $\circ$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rule ::= [Pre] ± Con</td>
<td>for each Apply in Con: $\circ$(Pre) ± $\circ$(Apply)</td>
</tr>
<tr>
<td>2</td>
<td>± ::= $\mathcal{O}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>± ::= $\mathcal{A}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>± ::= $\mathcal{D}$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Con ::= Apply</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Con ::= Con ^ Con</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Apply ::= (attri-id attr-val afcn)</td>
<td>$\circ$(m(attr-id), m(attr-val), afcn)</td>
</tr>
<tr>
<td>5</td>
<td>m(attr-id), m(attr-val), afcn</td>
<td>Table 2.</td>
</tr>
</tbody>
</table>

**Table 2. DDL semantics of SSPL Arithmetic Operators**

<table>
<thead>
<tr>
<th>No.</th>
<th>afcn</th>
<th>DDL mapping $\circ$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>type-assign</td>
<td>m(attr-id)$^2$ m(attr-value) or m(attr-id) $? m(attr-value)$</td>
</tr>
<tr>
<td>2</td>
<td>type-great-than</td>
<td>m(attr-id)$^2$ ${ &gt; m(attr-value)}$</td>
</tr>
<tr>
<td>3</td>
<td>type-great-than-or-equal</td>
<td>m(attr-id)$^2$ ${ \geq m(attr-value)}$</td>
</tr>
<tr>
<td>4</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Due to space constraints, some arithmetic operators are omitted in table 2.

**SSPL Policy** is composed by several SSPL rules. The policy itself has no antecedent, so the consequent of a policy is the semantic overlay by the consequents of all the rules in the policy. For a policy $P$ with $n$ rules, the consequent of $P$ is denoted $\text{Con}(P)$. The strict, defeasible and defeat rules of $P$ are denoted $P.R_s$, $P.R_d$ and $P.R_{df}$ respectively. The rule set $P.R$ of $P$ can be formalized as:

$$P.R = P.R_s \setminus P.R_d$$ where, if $m = \#(P.R_s \setminus P.R_d)$ then $m \not\leq n$.

And, $P.R_{sd} = P.R_s \setminus P.R_d$, that is the rule set of non-defeat rules.

The consequent of policy $P$ can be formalized as:

$$\text{Con}(P) = \text{Con}(P.r_1) \circ \text{Con}(P.r_2) \circ \ldots \circ \text{Con}(P.r_m), P.r_i \setminus (P.R_s \setminus P.R_d) \not\leq i \leq m.$$ 

**Definition 1 (Literal)**. Literal of SSPL is defined as the description logic mapping of expression in conditions or consequents. That is, for a rule $r$, literal $\circ(\text{Pre}(r))$ or

Because of space constraints, the following are given only the strict reasoning, defeasible reasoning will not repeat them here.
+$\Delta \mathcal{Q} (\circ(\text{Con}(P)))$ can be formalized as:

+$\Delta \mathcal{Q} (\circ(\text{Con}(P)))$: we may append $\mathcal{Q} (\circ(\text{Con}(P)))(i+1) = a$ and $D(j+1) = +\Delta a$ if

$\#P.r \neq P.Rs[\sim a]$:

(1) \begin{align*}
\neg \circ(\text{Pre}(P.r)) \text{ either} \\
\text{(1.1)} &+\Delta \circ D(1..j) \text{ or} \\
\text{(1.2)} &D \neg
\end{align*}

and (2) \begin{align*}
\circ(\text{Pre}(P.t)) \text{ either} \\
\text{(2.1)} &+\Delta \circ D(1..j) \text{ or} \\
\text{(2.2)} &\neg \circ(\text{Pre}(P.t)) : (\neg \Delta \circ D(1..j) \text{ and } D \neg)
\end{align*}

Where, $\mathcal{Q} (\circ(\text{Con}(P)))$ is the set of assertions, which reasoning from strict rules, in conclusions of policy $P$. We have $\mathcal{Q} (\circ(\text{Con}(P))) \ni \{\circ(\text{Con}(P))\}$.

The DDL semantics of $Policy \ set$ $PS$ is defined through the mapping to DDL rules, that is:

$\neg \circ(\text{Pre}(P)) \circ \circ(\text{Pre}(P)) \ni \neg \circ(\text{Pre}(P))$

$\neg \circ(\text{Pre}(S)) \circ \circ(\text{Pre}(S)) \ni \neg \circ(\text{Pre}(S))$

Where, $PS.$ is the set of all the policy of the policy set, and $PS. >$ is the set of all the sub policy set of the policy set.

### 3 DDL Based Conflict Analysis for SSPL

On the basis of DDL semantics of SSPL, we can use the argumentation system to analyze the SSPL policy. A typical argumentation system contains the following basic elements: an underlying logic language, the argument process and states arguments. The argumentation system here uses the DDL as logical language. DDL is a non-monotonic logic. Because it cannot use monotonous argumentation, proof tree can be used to record argumentation states.

### References

A Faster Cryptographic Time-Memory Tradeoff

Jung Woo Kim, Jungjoo Seo, Jin Hong, and Kunsoo Park
Seoul National University, Seoul, South Korea
{jkim, jjseo, jinhong, kpark}@theory.snu.ac.kr

Abstract. There has been extensive research on cryptographic time-memory tradeoff for recent 30 years. Since Hellman’s work in 1980, some improved variants and techniques have been proposed, and the rainbow method is known as the best time-memory tradeoff. As for the memory size, however, the required number of bits per start point and end point was not explicitly considered in these works. With this in mind, we propose a new time-memory tradeoff. Also, we analyze the success probability and the expected cryptanalysis time, and compare the performances of the rainbow method and ours.

Keywords: Cryptanalysis, Cryptographic Time-Memory Tradeoff, Rainbow method

1 Introduction

Cryptographic time-memory tradeoff is an approach to invert a one-way function such as

\[ C(x) = E_x(P_0), \]

where \( E \) is any encryption scheme, \( x \) is the key of size \( N \), and \( P_0 \) is the known fixed plaintext. Cryptanalytic time-memory tradeoff was firstly introduced by Hellman in 1980. [3] Since then, there has been an extensive research on time-memory tradeoff to speed up cryptanalysis time. [1,2,4] In 2003, a new method, which is referred to as rainbow method, was suggested by Oechslin. 6 Up until now, the rainbow method is the most efficient one.

2 A faster time-memory tradeoff

In this section, we propose our time-memory tradeoff, which introduces more functions and spends less memory for each start point compared to the rainbow method by modifying the structure of the rainbow table. We divide the rainbow table into \( s \) sub-tables, each of which has \( m \) chains. The order of the computation of function \( f_i(\cdot) \) is shifted to the right by one position in each sub-table, where \( f_i(x) := R_i(E_x(P_0)) \), where \( R_i(\cdot) \) is a reduction function which creates a key from a ciphertext. Our table is shown in Figure 1. \( SP_{i,j} = j \) for \( 0 \leq i < s, 0 \leq j < m \).
In an online phase, given an image $y_0 = \mathcal{C}(x_0)$, we want to find $x_c$. For the $j$-th iteration, let $y_{i,j}$ be the end point of the online chain corresponding to the $i$-th sub-table. First, we compute $y_{i,1} = R_{t-1}(y_0) = f_{t-1}(x_0)$ and check whether it is an end point in the first sub-table. If so, we check whether it is a false alarm. If it is not an end point or the false alarm occurs, then we compute $y_{i,1} = R_{t-1}(y_0) = f_{t-1}(x_0)$ and check the false alarms for $i = 2, 3, \ldots, s$, sequentially. Next, in the $j$-th iteration, we compute

$$y_{i,j} = \begin{cases} f_{t-i}(y_{i+1,j-1}), & 0 < i < s \\ f_{t-s}(f_{t-s-1}(\cdots (f_{t-s-j+2}(R_{t-s-j+1}(y_0))) \cdots)), & i = s \end{cases}$$

and check the false alarms. Note that the value, $y_{i+1,j-1}$, which is computed in the $(j-1)$-th iteration, is reused to generate the online chain for $i = 1, 2, \ldots, s-1$.

3 Performance analyses and comparisons

3.1 Analyses

Let us denote the $j$-th column in the $i$-th sub-table by the $(i, j)$-th sub-column. The table has $s \times t$ sub-columns. We write $m_s(i, j)$ for the number of new points added by the $(i, j)$-th sub-column in the sub-columns to which the same $f$ function is applied, where $0 \leq i < s$ and $0 \leq j < t$. We first count the number of distinct points in each sub-column, and then analyze the success probability at each iteration. Based on these, the expected time will be calculated.

**Lemma 1.** $m_s(i, j)$ satisfies the following recurrence relation.
Lemma 2. The probability to fail until the k-th iteration is

\[ P_{\text{failure}}(k) = \prod_{i=0}^{t-k} \left( 1 - \frac{D(0, i)}{N} \right)^{s-i} \prod_{i=1}^{s-1} \left( 1 - \frac{D(i, t-k)}{N} \right) \]

where \( D(r, c) = \sum_{i=0}^{s-r-1} m_{s-r-1}(r + i, c + i) \) and \( 1 \leq k \leq t \).

Theorem 3. The success probability \( P_1 \) of a single table of \( s \times t \) sub-columns is

\[ P_1 = 1 - P_{\text{failure}}(t) = 1 - \prod_{i=0}^{t-1} \left( 1 - \frac{D(0, i)}{N} \right)^{s-i} \prod_{i=1}^{s-1} \left( 1 - \frac{D(i, 0)}{N} \right) \]

Corollary 4. The success probability \( P \) of \( l \) tables is

\[ P = 1 - (1 - P_1)^l \]

Theorem 5. Let \( z \) be the number of truncated bits in the end point. The expected time of our tradeoff with false alarms is

\[ T = l \left( t - 1 \right) \left( \frac{m_s}{2^r} + \frac{m_s}{N} \right) + \sum_{k=2}^r \left( k + s - 2 + (t-k) \left( \frac{m_s}{2^r} + \frac{m_s k}{N} \right) \right) P_{\text{failure}}(k-1) \]

where \( r = \lceil \log_2 N \rceil - z \).

Theorem 6. The memory size of the table is

\[ M = msl \left( \lceil \log_2 m \rceil + \lceil \log_2 N \rceil - \left\lceil \log_2 \frac{m}{\log_2 m} \right\rceil - z \right) + s l \cdot 2 \left\lceil \log_2 \left( \frac{m}{\log_2 m} \right) \right\rceil \log_2 m \]

Also, the memory size of the table without indexing technique is

\[ M = msl (\lceil \log_2 m \rceil + \lceil \log_2 N \rceil - z) \].
3.2 Comparisons

In this section, we compare the performance of ours with that of the rainbow method under a same success probability and memory size (GB). The success probability $P$ and the expected time $T$ of the rainbow method are calculated from Hong’s result 5.

Table 1 shows the performance of the rainbow and our method without and with indexing technique, respectively, for $N = 3.58 \times 10^{12}, P = 99\%$. We can see that the new method accelerates the cryptanalysis time by about 30% with indexing technique and 6% without that.

<table>
<thead>
<tr>
<th>$M$</th>
<th>$l$</th>
<th>$m$</th>
<th>$t$</th>
<th>$z$</th>
<th>$T$</th>
<th>$l$</th>
<th>$s$</th>
<th>$m$</th>
<th>$t$</th>
<th>$Z$</th>
<th>$T$</th>
<th>Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rainbow without indexing technique</td>
<td>Ours without indexing technique</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>26030104</td>
<td>128652</td>
<td>12</td>
<td>8588411884</td>
<td>6</td>
<td>4065</td>
<td>8190</td>
<td>100520</td>
<td>12</td>
<td>5792355136</td>
<td>33%</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>50233535</td>
<td>66665</td>
<td>11</td>
<td>2301841797</td>
<td>6</td>
<td>1900</td>
<td>32761</td>
<td>53771</td>
<td>11</td>
<td>1634110946</td>
<td>29%</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>97061407</td>
<td>34502</td>
<td>10</td>
<td>615490109</td>
<td>6</td>
<td>892</td>
<td>131020</td>
<td>28641</td>
<td>10</td>
<td>458046888</td>
<td>26%</td>
</tr>
<tr>
<td>Rainbow with indexing technique</td>
<td>Ours with indexing technique</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>39346566</td>
<td>85111</td>
<td>12</td>
<td>3859892949</td>
<td>6</td>
<td>156</td>
<td>261246</td>
<td>82169</td>
<td>12</td>
<td>3622527989</td>
<td>6.1%</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>76390703</td>
<td>43838</td>
<td>11</td>
<td>1021700547</td>
<td>6</td>
<td>151</td>
<td>523992</td>
<td>42322</td>
<td>11</td>
<td>962256822</td>
<td>5.8%</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>148425460</td>
<td>22562</td>
<td>10</td>
<td>270056536</td>
<td>6</td>
<td>37</td>
<td>4139067</td>
<td>21866</td>
<td>10</td>
<td>255169155</td>
<td>5.5%</td>
</tr>
</tbody>
</table>

Acknowledgements. This work was supported by the National Research Foundation of Korea (NRF) grants funded by the Korea government (MEST) (2011-0029923 and 2011-0005764).

5 References

Output Control of Three Phase AC Power Source System with SCR Rectifier and Linear Power Amplifier

Jeong-Chay Jeon\textsuperscript{1*}, Hun Oh\textsuperscript{2} and In Ho Ryu\textsuperscript{*}

\textsuperscript{1}Korea Electrical Safety Corporation
\#27 Sangcheon-ri, Cheongpyeoungh-myeon, Gapyeong-gun, Gyeonggi-do, 477-814, Rep. of Korea

\textsuperscript{2}Department of Electrical and Information Communication Engineering, WonKwang University Engineering
\#460, Iksandae-ro, Iksan-si, Jeonbuk, Rep. of Korea

\textsuperscript{3}Department of IT Applied System Engineering, Chonbuk National University
\#664-14, 1-ga, Duck-jin Dong Duck-jin Ku, Jeonju, 561-756, Rep. of Korea

kescoin@naver.com

Abstract. This paper presents the design and implementation of a three-phase AC Power Source with SCR and linear amplifier, which is capable of generating sinusoidal output voltages with adjustable output amplitude and frequency over a wide range as well as arbitrary waveforms. The developed AC Power source consists mainly of a power converter to generate and amplify waveform signals, a controller to control the desired output signal and measure the output parameters including voltage and current, and a control program to set the desired output and display the output values.

Keywords: Three-Phase, AC Power Source, SCR, Linear Amplifier, Control

1 Introduction

An AC power source provides sinusoidal output voltages whose amplitude and frequency can be programmed independently from each other. The waveform generating is based on the concept of the complex Fourier series \[1\]. Any periodic waveform can be reproduced by generating and summing together a set of harmonically related sine-waves with the proper magnitude and phase-shift components.

Most power sources available today are linear power amplifier types and pulse width modulated inverter types. The AC power source with pulse width modulated inverter has problem that switching losses increase with the elevation of the switching frequency \[2\][3]. And although its efficiency is poor and a large heat sink and a isolation transformer are required which increases the size and the weight of the systems, the ac power source with linear power amplifier allows the generation of any waveform and has merit that input-output characteristic is good. So, in this paper, the considered ac power source is linear power amplifier type.
This paper describes the design and implementation of three-phase ac power source, which is able to synthesize voltage waveforms and amplitude. In the system, harmonics can be added to the fundamental frequency, so arbitrary waveforms can be generated.

2 H/W Implementation of AC Power Source

The AC power source under consideration is depicted in Fig. 1. This consists mainly of power input, a power converter (SCR rectifier and power amplifier) to generate and amplify waveform signals, a controller to control the output signal and measure the output parameters, and a control program to program the desired output values and display the output parameters. Personal computer (PC) and control program are used to provide interface with the harmonic generator. PC and control program control the waveform’s shape with harmonic order and amplitude, and measure the output parameters including voltages and currents.

![Fig. 1. The block diagram of the system](image)

The output reference signal is first generated in the controller. In spite of the output voltage and waveform control of the ac power source being analogue, the reference signal as well as an on/off signal is generated by the controller in order to allow easy programming of the output voltage and waveform from PC. 8 bit microcomputer (PIC18F8720) and digital to analogue (DA) converter (AD 7523) are used to generate the output signal. And in order to maintain independently output function of DA converter when the microcomputer performs another work, latch-IC 74F573 between microcomputer and DA converter is used. To execute waveform output command from PC at high speed, 4Mbit static random access memory (S-RAM) was used. Also, in order to save the information of the waveform saved in the inside of the controller by modifying and saving command of waveform from PC, 4Mbit flash read only memory (F-ROM) is used. In the ac power source, in order to provide DC power for digital components and signal for power amplifier, silicon-controlled rectifier (SCR) is used. The generated signal by the controller is then sent a linear power amplifier module. The power amplifier module is consisted of power transistor 2SA1494 (PNP type) and 2SC3858 (NPN type). It has the output capacity of 5 kW and is designed so
that the enlargement of the capacity in the future is possible. Finally, the amplified voltage is sent to the 46/255 volt transformer to amplify the voltage level.

3 Test and results

The performance of the ac power source is tested by some measurements. In the experiment, the desired output voltage is set at 260 V (rms) and a fixed frequency of 60 Hz. A constant resistive load is connected to the output such that an output current of 7 A (rms) is drawn. As can be seen from the test results, there is no noticeable distortion of the output voltage and current, but the output voltage (a) and current (b) give about 255 V (rms) and 6.8 A (rms) with little error (about 5 V). It is guessed that the error was generated by the problems of linear AC power amplifiers and the other elements. Therefore, future work to reduce the output error will be need.

4 Conclusion

The 5kW three-phase ac power source with adjustable output voltage amplitude and frequency by computer program has been successfully developed. In this AC power source, in order to control the desired signal and measure the output signal, the controller using two 8 bit microcomputers are developed. And 5 kW linear power amplifiers to amplify the output signal and the control program to set and display the output of the ac power source are developed. The test results have demonstrated that there is little error of output voltage due to the linear power amplifiers but the desired waveform is obtained correctly. And it is clear as the test results that the power level of the developed ac power source is about 5 kW. Therefore, future work to reduce the output error and develop power amplifier with high accuracy and large capacity will be need.

References

Design and Implementation of Class B Power Amplifier for 5kW AC Power Source

Jeong-Chay Jeon¹, Hyoung-Keun Park² and Hyun Seob Cho³

¹Korea Electrical Safety Corporation
#27 Sangcheon-ri, Cheongpyeoung-myeon, Gapyeong-gun, Gyeonggi-do, 477-814, Rep. of Korea

² Department of Electronic Engineering, Namseoul University
#91 Daehak-ro Seonghwan-eup Sebuk-gu Cheonan-si, Chungcheongnam-do, Rep. of Korea

³ Department of Electronic Engineering, ChungWoon University
#San29, Namjang-ri, Hongseong-eup Hongseong-gun, Chungnam, Rep. of Korea
kescoin@naver.com

Abstract. This paper presents the design and implementation of class B linear power amplifier for 5 kW three-phase AC Power Source. The power amplifier was designed using power transistor 2SA1494(PNP) and 2SC3858(NPN), and was implemented so that the enlargement of the capacity in the future is possible. The developed amplifier was applied to the AC power source system and output accuracy and capacity were tested.

Keywords: Power Amplifier, AC power source,

1 Introduction

A single and three-phase AC power source using sliding mode control was proposed by Low and predictive control with pulse width modulated inverters was generalized [1][2]. The harmonic generator with pulse width modulated inverter has problem that switching losses increase with the elevation of the switching frequency [3][4]. And although its efficiency is poor and a large heat sink and an isolation transformer are required which increases the size and the weight of the systems, the ac power source with linear power amplifier allows the generation of any waveform and has merit that input-output characteristic is good. Linear amplifiers are classified into different classes such as A, B, C, and F according to their circuit configurations and methods of operation. These classes range from entirely linear with low efficiency to entirely non-linear with high efficiency [5]. This paper describes the design and implementation of 5kW class B power amplifier for AC power source.
2 Output stage of class B power amplifier

The class B amplifier is a two-transistor circuit that is designed to improve on the efficiency characteristics of class A amplifiers. A class B amplifier is shown in Fig. 1. The circuit shown is a complementary-symmetry amplifier, or a push-pull emitter follower. The circuit contains one npn transistor \((Q_1)\) and one pnp transistor \((Q_2)\).

The maximum power dissipation \(P_{D(max)}\) can be written as

\[
P_{D(max)} = \frac{4V_s^2}{\pi^2 RL} - \frac{2V_s^2}{\pi^2 RL} = \frac{2V_s^2}{\pi^2 RL}. \tag{1}
\]

In order to design an amplifier that has an output power of 200 W and drives a load of 25 \(\Omega\), the output voltage is calculated as

\[
P_L \leq 200 \rightarrow \frac{A^2}{2R_L} \leq 200 \rightarrow A \leq 35.36. \tag{2}
\]

Considering the saturation voltage of transistors, the supply dc voltage \(V_s\) of the amplifier should be larger than the maximum output voltage \(A_{max}\). The designed amplifier of Fig. 2 has power transistor 2SA1494(PNP) and 2SC3858(NPN), while the supply dc voltage \(V_s\) was chosen as 39.5 V.

![Fig. 1. A class B amplifier](image1)

![Fig. 2. The basic structure of the designed amplifier](image2)
3 H/W Implementation and test

The power amplifier module is consisted of power transistor 2SA1494 (PNP type) and 2SC3858 (NPN type). These linear AC power amplifiers are constructed as shown Fig. 3. It has the output capacity of 5 kW and is designed so that the enlargement of the capacity in the future is possible. The performance of the amplifier is tested by some measurements. Output Voltage test results indicated that the developed amplifier yielded less than 0.2 % error.

![Fig. 3. The developed linear power amplifier PCB(500W*10=5kW)](image)

4 Conclusion

This paper designed and implemented class B power amplifier for AC power source to test electric system and equipment. The developed amplifier was applied to the ac power system and output accuracy and capacity were tested. The test results have demonstrated that there is little error of output voltage due to the linear power amplifiers. Therefore, future work to develop power amplifier with high accuracy and large capacity will be need.

References

Development and Test of Simultaneous Power Analysis System for Three-Phase and Four-Wire Power System

Hun Oh¹, In Ho Ryu² and Jeong-Chay Jeon³*

¹Department of Electrical and Information Communication Engineering, WonKwang University Engineering, #460, Iksandae-ro, Iksan-si, Jeonbuk, Rep. of Korea
²Department of IT Applied System Engineering, Chonbuk National University
   #664-14, 1-ga, Duck-jin Dong Duck-jin Ku, Jeonju, 561-756, Rep. of Korea
³Korea Electrical Safety Corporation
   #27 Sangcheon-ri, Cheongpyeoung-myeon, Gapyeong-gun, Gyeonggi-do, 477-814, Rep. of Korea
   kescoin@naver.com*

Abstract. This paper presented voltage 8-channel and current 10-channel power measurement system that simultaneously can measure and analyze power components for both supply and demand side. The developed system was tested using ac power source. The test results showed that accuracy of the developed system is about 0.2 percent. Also, simultaneous measurement field test of the developed system was implemented by applying in the supply and demand side of three-phase power system.

Keywords: Multi-channel, Power Analysis, Three-Phase, Voltage, Current

1 Introduction

The various problems including malfunction of control devices, data loss of computer systems and overheating of cable and transformer have been generated. These problems and concerns created the needs of the measurement of power components such as active, reactive and apparent power, root-mean-square (rms) values of voltage and current, power factor and power quality [1, 2]. There are many variants of power measurement available in the field ranging from hand-held instruments to portable monitors. These instruments have voltage 4-channel and current 5-channel and provide three-phase and four-wire metering. Therefore, they can measure power components of only one side that is supply or demand side of three-phase and four-wire power system. But, in order to effectively improve energy efficiency and solve power disturbances, power components measurement for both supply and demand side of power system must be implemented before appropriate action on power problems is taken [3].

This paper presented voltage 8-channel and current 10-channel power measurement system that simultaneously can measure power components for supply and demand side of power system. The accuracy of active, reactive and apparent power measurement and harmonic analysis by the developed system was tested using ac
power source (PACIFIC 345AMX). The test results showed that accuracy is about 0.2 percent. In the field test of the developed system, the power components measurement for all phases of load and source side in three-phase power system was simultaneously implemented.

2 The system architecture

Figure 1 shows the basic block diagram of the proposed multi-channel power measurement system. The proposed system is largely consisted of analog signal input block with voltage 8-channel and current 10-channel measuring sensors, analogue to digital conversion (ADC) block converting analog signal into digital signal, digital signal processing block controlling circumference installations and performing operation function, programmable logic device (PLD) block performing system interface processing, memory block of static RAM (SRMA) and flash ROM (FROM), interface block to transfer the metering results to a personal computer via a serial link for display, and operation power source block supplying operation power of the proposed system. The proposed system was constructed on a single printed circuit board (PCB).

![Fig. 1. Block diagram of the proposed system](image)

3 Test and results

The first, accuracy of power (active, reactive and apparent power) measurement and harmonic analysis by the developed system was tested. Test system, which is consisted of programmable ac power source (PACIFIC 345AMX) and load, was constructed. Programmable ac power source can produce voltage with arbitrary magnitude and frequency. Test results indicated that the developed system yielded less than 0.2 % error in all case. In order to verify that the developed system can simultaneously measure power components for both supply and demand side of power system, the developed system was connected with load and source side of...
three-phase power system

4 Conclusion

The voltage 8-channel and current 10-channel power measurement system to simultaneously analyze power components and harmonics in several points of power system was designed and implemented. Voltage and current measurement errors of the developed system were revised, and accuracy of power (active, reactive and apparent power) and harmonic measurement was tested by comparing power components outputted in the programmable ac power source with that calculated by the developed system. All the test results showed that the measurement error is less than 0.2 percent. For field test, the developed system was connected with load and source side of three-phase power system that capacitor and inductor to improve power factor were installed. The result of field test showed measurement of power components for all phases of load and source side was simultaneously implemented.

As the results of field test, it was certificated that the measurements of power components such as voltage and current waveforms, reactive power and harmonics for all phases of load and source side using the developed system can be simultaneously implemented and the proposed system can be effectively applied to measure power components of power system in order to solve power disturbances.

References

Robust IPSec Key Recovery Solution for IKEv2 under Mobile and Wireless Environment

Yunjung Lee¹, Jungwon Cho²*, Keun-Wang Lee³

¹ Department of Computer Science and Statistics, Jeju National University, 102 Jejudaehakno, Jeju-si, Jeju-do 690-756, South Korea rheej@jejunu.ac.kr
² Department of Computer Education, Jeju National University, jwcho@jejunu.ac.kr
³ Department of Multimedia, Chungwoon University, San 29 Namjang-ri, Hongseong-eup, Hongseong-gun, Chungnam 350-701 South Korea kwlee@chungwoon.ac.kr

Abstract. This paper presents the key recovery mechanism that is applied to IKEv2 in IPSec for mobile communication environments. It results to have compatibility with IPSec and IKEv2, reduces network overhead, and performs key recovery without depending on key escrow agencies or authorized party.

Keywords: IPSec, Key Recovery, IKEv2

1 IPSec Key Recovery Mechanism supporting IKEv2

We propose new key recovery mechanism suitable to IKEv2 in IPSec. In other to use IPSec in mobile communication environment, it is necessary to satisfy IKEv2 standard. We propose new mechanism that applies SA negotiation for key recovery to IKEv2. For this purpose, we modify the message exchanges of IKEv2 and KRF format of KRA for transfer of key recovery information.

1.1 SA Negotiation for Key Recovery Information in IKEv2

In original IKEv2, session key and IPSec-SA are negotiated in 4 message exchanges[1][2]. In the first and the second message exchanges, authentication between both communication entities is accomplished and IKE-SA is created for secure transfer of next third and fourth message exchanges[3][4][5]. In the third and the fourth, IPSec-SA and session key for IPSec protocol (AH and ESP) is negotiated securely under IKE-SA.

We modify the third and the fourth messages, and insert SA negotiation for deriving session-key-recovery key in IKEv2 messages without additional message exchange. Session-key-recovery key is used in other to encrypt the session key for secure data transfer in ESP or AH. Encrypted the session key will be transferred in Key

---

* Corresponding Author.
Recovery Header (KRH) in IPSec packet. And if needed, corresponding session key is recovered by decrypting the encrypted session key with session-key-recovery key. Figure 1 shows proposed KRH format.

<table>
<thead>
<tr>
<th>Next Header</th>
<th>Length</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Security Parameter Index (SPI)</td>
</tr>
<tr>
<td>KRF Length</td>
<td></td>
<td><strong>Key Recovery Field (KRF), variable length</strong></td>
</tr>
<tr>
<td>Validation Field type</td>
<td>Validation Field Length</td>
<td></td>
</tr>
<tr>
<td>Validation Field Value, variable length</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fig. 1. Proposed KRH Format**

The KRF must be sent, since the session key is not escrowed. Hence, the KRF is sent several times according to an accepted degradation bandwidth. TS is not included in KRH format compared with PS-KR[6], therefore can reduce overhead from TS field.

### 1.2 Key Recovery Process

There are several cases that need session key recovery in IPSec. One is when one of Alice and Bob lose the session key on the session. Both Alice and Bob can recover the session key $SK$ by decrypting $E_{SK}^{1}_{K_{skr}}$ with their own $K_{skr}$.

$$SK = D(E_{SK}^{1}_{K_{skr}})_{K_{skr}}$$ (1)

Other case that needs key recovery is when Authority Party (AP) such as government requires the session key recovery to decrypt the corresponding IP Packets. AP can receive $(x, TS, child, g, p)$ from Alice’s TTP and $(x, TS, child, g, p)$ from Bob’s TTP if it has permissions from both Alice and Bob. Then it derives $K_{sky}$ and gets $SK$.

$$K_{sky} = f^2(g^{xy} \mod p, TS)$$

$$SK = D(E_{SK}^{1}_{K_{skr}})_{K_{skr}}$$ (2)

### 2 Mechanism Analysis and Evaluation

We compare existing protocols and our proposed protocol. In table 1, we show the comparison between proposals of RHP, KRA, PS-KR and our proposed.
Table 1. Comparison of protocols (O: high support Δ: low support X: not support)

<table>
<thead>
<tr>
<th></th>
<th>RHP</th>
<th>KRA</th>
<th>PS-KR</th>
<th>The Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility with IETF</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Compatibility with IKEv2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Robustness</td>
<td>Δ</td>
<td>X</td>
<td>Δ</td>
<td>O</td>
</tr>
<tr>
<td>Reducing overhead of network</td>
<td>O</td>
<td>Δ</td>
<td>Δ</td>
<td>O</td>
</tr>
<tr>
<td>Right of Communicating Entities of Key Recovery</td>
<td>X</td>
<td>O</td>
<td>Δ</td>
<td>O</td>
</tr>
</tbody>
</table>

3 Conclusion and Future Works

We propose the key recovery mechanism that is applied to IKEv2 of IPSec. It results to have compatibility with IPSec and IKEv2, reduce network overhead, and perform key recovery without depending on key escrow agencies or authorized party. We design a key recovery protocol for IKEv2 that is suitable for mobile communication environments and more robust than existing protocols.

As future works, we plan to implement the proposed mechanism and to evaluate the performance of it.

Reference

1. The Internet Key Exchange (IKE) (RFC 2409)
2. Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
3. The Oakley Key Determination Protocol (RFC 2412)
4. IP Authentication Header (AH) (RFC 2402)
5. IP Encapsulating Security Payload (ESP) (RFC 2406)
Bus bar formation process was designed by multi-layer metal deposition

Soo-Bon Koo¹, Young-Hun Lee²*

¹Dept. of Electronic Eng., Hannam University, 133 Ojeong-dong, Daedeok-gu, Daejon 306-791, Korea. Phone:+82-42-939-9568, Email: sbkoo@elk.co.kr
²Dept. of Electronic Eng., Hannam University, 133 Ojeong-dong, Daedeok-gu, Daejon 306-791, Korea. Corresponding Author, Phone:+82-42-629-7565, Email: yhlee@hnu.ac.kr

Abstract. In on-cell type touch panel structure, screen printing technology which uses Ag paste on ITO film is one of the general processes for Bus bar formation. Considering the growing of capacitance touch panel industry and slim design trend, decreasing the Bezel width is necessary. The high technology should be developed for Bus bar printing. Thus, Bus bar formation process was designed by metal deposition and photo lithography in this theory. By applying multiple layers structure process, the comparisons of adhesion strength between ITO films, resistances and pitch width were proceeded. Based on the comparisons, Mo/Al/Mo structure was known as the best for fine pitch bus bar formation process.

Keywords: touch panel, screen print, photo lithography, bus bar

1 Introduction

After launching I-phone of Apple Co., touch panel industry prefer capacitance and focus on technical development of it.

Resulting from needs-growing of user's multi-touching and advance in mobile phone technology, decreasing the Bezel width is necessary. The development of high integrated Bus bar is emerging.

The realization of Bus bar in TSP recently commercialization apply printing-skill using Ag paste.

This technology can be applied by relatively simple process, but it is impossible to use line width of below 50um. [1],[3]

Thus, it is suggested that Photo lithography can realize Bus bar of line width of below 10um On-cell using ITO film of TSP in this theory

It is believed that high integrated Bus bar is realized by applying Photo Lithography process on Mo/Al/Mo multiple structure. Measuring resistance demonstrate that it has higher integration and weaker resistance than existing printing-skill. [4]
2  **Bus-bar electrode process**

Screen printing consists of three elements: the screen which is the image carrier; the squeegee; and ink. Screen printing ink is applied to the substrate by placing the screen over the material. Ink with a paint-like consistency is placed onto the top of the screen. Ink is then forced through the fine mesh openings using a squeegee that is drawn across the screen, applying pressure thereby forcing the ink through the open areas of the screen. Ink will pass through only in areas where no stencil is applied, thus forming an image on the printing substrate.

![Fig. 1 A theory of screen print](image1)

![Fig. 2 Process flow of photolithograph](image2)

![Fig. 5 The result of screen print process](image3)

![Fig. 6 The result of photolithography process](image4)

Photolithography process is to work out design component or to array trace in semiconductor industry.

Regarding to bus-bar element, particular materials were selected which is available for bus-bar electrode. Resistance and thickness of adequate element were indicated in Table.1.
The result of making bus-bar on Mo/Al/Mo structure, which was most pertinent to adhesion with ITO film that was successfully maintained the 10um line width. mClassfied by process method, test result was showed in Table.2.

<table>
<thead>
<tr>
<th>Material</th>
<th>Thickness</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al</td>
<td>2.655</td>
<td>Available</td>
</tr>
<tr>
<td>Cr</td>
<td>1.29E-04</td>
<td>Thick</td>
</tr>
<tr>
<td>Mo</td>
<td>5.17</td>
<td>Available</td>
</tr>
<tr>
<td>Ag</td>
<td>1.59</td>
<td>High price</td>
</tr>
<tr>
<td>Cu</td>
<td>1.673</td>
<td>High price</td>
</tr>
</tbody>
</table>

Table 2. Compare result of process method

<table>
<thead>
<tr>
<th>Process Method</th>
<th>Material</th>
<th>Resistance</th>
<th>Line width</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen print</td>
<td>Ag paste</td>
<td>100Ω</td>
<td>50um</td>
</tr>
<tr>
<td>Multiple structure</td>
<td>Mo/Al/Mo</td>
<td>100Ω</td>
<td>10um</td>
</tr>
</tbody>
</table>

3 Conclusion

In this paper the bus-bar process flow are derived using multiple deposition structure on On-cell type of TSP. To review of process plan, photolithography process are adopted in Fig.5. And Mo/Al/Mo structure are selected considering the characteristic of ITO film. After formation of bus-bar electrode, photolithography process was better than screen print to lessen the line width. The derived output characteristics of a photolithography process can be usefully applied to the design of bus-bar electrode.

Acknowledgments. This paper has been supported by 2011 Hannam University Research Fund

References

[4] Dong-Jin Park, A study of 3-Dimensional micro structure fabrication using photolithography and abrasive machining, Dong-Eui University, 2004
Protection Profile for Mobile Device Management Systems*

Keunwoo Rhee¹, Woongryul Jeon¹, and Dongho Won¹,**

¹ Sungkyunkwan University
2066, Seobu-ro, Jangan-gu, Suwon, Gyeonggi-do 440-746, Korea
{kwrhee, wrjeon, dhwon} @security.re.kr

Abstract. This paper proposes the first Protection Profile for a Mobile Device Management system by modeling a threat and applying a security requirement engineering methodology based on Common Criteria.

Keywords: Mobile Device Management System, Common Criteria, Protection Profile

1 Introduction

The number of cases of confidential business information leakage via mobile devices has continued to rise. As such, enterprises are considering the adoption of a Mobile Device Management (MDM) system to manage not only the data stored in their employees’ mobile devices but also hardware such as the cameras and USB ports of mobile devices [1, 2]. However, no criteria have yet been established to evaluate whether such MDM systems fully provide the basic security functions needed by enterprises and whether such functions have been securely and reliably developed.

Therefore, this paper proposes the first Protection Profile (PP) for an MDM system. Consumers can refer to it to clearly present requirement of an MDM system for purchase. Moreover, the proposed PP can be used globally as it conforms to International Standard ISO/IEC 15408 – Common Criteria (CC). Developers can use the PP to improve the security and reliability of their products and evaluators of MDM systems can use it as a reference in their evaluation work.

2 Mobile Device Management System

The MDM system comprehensively manages mobile devices by monitoring their status and controlling their functions remotely using wireless communication technology such

---

* “This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program” (NIPA-2012-H0301-12-3007) supervised by the NIPA (National IT Industry Promotion Agency).

** Corresponding author.
as Over-the-Air (OTA) or Wi-Fi, as well as managing the required business resources. Fig. 1 shows the MDM system architecture and operation [3, 4, 5, 6, 7].

![Mobile Device Management System](image)

**Fig. 1. Mobile Device Management System**

3 Proposed Protection Profile

3.1 Threats and Security Objectives

Threats must be clearly identified in order to accurately deduce the security requirements. Table 1 shows the identified threats.

<table>
<thead>
<tr>
<th>Threat</th>
</tr>
</thead>
</table>

The security objectives provide high-level solutions to the identified threats. Table 2 shows the security objectives which correspond to the identified threats.

<table>
<thead>
<tr>
<th>Security Objective</th>
</tr>
</thead>
</table>
3.2 Security Functional Requirements

Security Functional Requirements (SFRs) are the set of security functions required to achieve the security objectives. In general, a developer, when creating PP, can select the SFRs to achieve the security objectives from CC document [8].

<table>
<thead>
<tr>
<th>Class</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Audit</td>
<td>FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3 FAU_STG.4</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>FAV_INT_EXT.1</td>
</tr>
<tr>
<td>Cryptographic Support</td>
<td>FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1</td>
</tr>
<tr>
<td>User Data Protection</td>
<td>FDP_ACC.1, FDP_ACF.1, FDP_APP_EXT.1, FDP_IFC.1, FDP_IFF.1, FDP_MDC_EXT.1, FDP_RIP.1, FDP_SDC_EXT.1, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_WIP_EXT.1</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2</td>
</tr>
<tr>
<td>Security Management</td>
<td>FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1</td>
</tr>
<tr>
<td>Protection of the TSF</td>
<td>FPT_ITC.1, FPT_ITT.1, FPT_ITT.2, FPT_STM.1</td>
</tr>
<tr>
<td>MDM System Access</td>
<td>FTA_MCS.1, FTA_SSL1, FTA_SSL.3</td>
</tr>
<tr>
<td>Trusted path/cannels</td>
<td>FTP_ITC.1, FTP_TUD_EXT.1</td>
</tr>
</tbody>
</table>

4 Conclusion

This paper proposes a protection profile which can be used as a request for a proposal to procure an MDM system, a guideline for developers to develop a secure MDM system, and criteria with which evaluators can evaluate the completeness of a developed system.

References

Text Hiding Scheme Using Big-5 Code

Jun-Chou Chuang\textsuperscript{1}, Chun-Chi Lo\textsuperscript{2}, Yu-Chen Hu\textsuperscript{3}, Piyu-Yu Tsai\textsuperscript{4}

\textsuperscript{1} Department of Computer Science and Communication Engineering
\textsuperscript{2} Department of Computer Science and Information Engineering
\textsuperscript{3} Department of Computer Science and Information Management
Providence University
lzchung@pu.edu.tw
\textsuperscript{4} Department of Computer Science and Information Engineering
National United University
pytsai@nuu.edu.tw

Abstract. This paper presents a text hiding scheme using Big-5 code. Some text-hiding schemes embed secret information at between-word and between-character by adding tabs or spaces. Liu et al, proposed a Chinese text data hiding scheme to divide the Chinese character into left and right parts for data embedding. However, the adjusted spaces or divided characters of between-word may look like strange and it may expose the risk of security. Therefore, we intend to design a text hiding scheme using Big-5 code. The secret is hidden into spaces between-word and between-character of a cover text by placing a Big-5 code either 20 or 7F. The visual quality of the stego-document is the same as the original document and therefore reducing the suspicious of attention by hackers. Experimental results show that the visual quality of the proposed scheme achieves good results and feasibility.

Keywords: Text hiding, data hiding, image hiding, Big-5.

1 Introduction

Text hiding schemes [1-6] can be classified into two types, content format and language semantic. The content format methods adjust the width of tracking, the height of leading, number of white spaces, font sizes, and etc. The language semantic methods change the meaning of a phrase or a sentence in a text document. The traditional text hiding schemes embed secret information at between-word and between-character by adding tabs or white spaces. However, the adjusted white spaces of between-word may look like strange. Therefore, we intend to design a text hiding scheme using Big-5 code. The secret is first converted into binary and then embedded into white spaces between-word and between-character of a cover text by placing a Big-5 code either 20 or 7F.
2 The Proposed Scheme

In our Scheme, the secret is hidden into spaces between-word and between-character of a cover text by placing a Big-5 code either 20 or 7F. The advantage of our scheme gets good visual quality of the stego document and it does not cause any visual distortion. The hexadecimal number of a white-space in the Big-5 table is 20. We can see that the Big-5 code 7F is a blank character and it can simulate as the white-space function. That is, we use the two Big-5 codes 20 and 7F to embed secret bit 0 or 1, respectively.

To embed secret into a cover text, we shall adjust the content of a cover text. We need to add a white-space in each between-word and between-character. Secret messages are sequentially converted into 0’s and 1’s binary stream. One white-space of between-word and between-character in a cover text is used to hide one secret bit. If we want to embed secret bit 0, the Big-5 code of white-space 20 is adopt. If we want to embed secret bit 1, the Big-5 code of blank character 7F is adopt. After finishing the secret embedding, we add an end-of-code 7F to indicate no secret of input. The hiding capacity of a cover text can be determined before data embedding. We can calculate the total number of white-spaces in a cover text. Assume a cover text contains \( w \) characters; the embedding payload of a cover text is \((w-1)\) bits.

In the extraction phase, the decoder sequentially scans the stego-text to find white-space of between–character and between-word. The extracted secret bit is “0” or “1” depends on the extracted Big-5 code is 20 or 7F. The length of the secret can be determined by scanning the location of the last 7F code in the stego text.

3 Experimental Results and Discussions

We have made two experiments on Chinese cover text and English cover text. The secret bits are randomly generated by the pseudo random number generator with a known seed. The embedding payload of the two cover texts in Fig. 1 are 243 bits and 141 bits, respectively. The evaluated criterion on the proposed method concerns on the embedding payload of the cover text. To demonstrate the hiding capacity, we compare the hiding capacity of our scheme, Liu’s scheme and Wang’s scheme in Table 1. The Liu’s method and the Wang’s method cause visual distortion of Chinese words and do not have enough embedding payload. From the experiment results in Table 1, the embedding payload of our scheme is better than Liu’s method and Wang’s method. Bessie, our scheme can apply to any kind of text format. On the other hand, our scheme does not adjust the width of white-space. Therefore, the visual quality of the proposed scheme achieves good results.
Table 1. Compare the embedding payload of Chinese cover text to our scheme, Liu’s method, and Wang’s method.

<table>
<thead>
<tr>
<th>Method</th>
<th>Payload (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liu et al. [5]</td>
<td>~63</td>
</tr>
<tr>
<td>Wang et al. [6]</td>
<td>~73</td>
</tr>
<tr>
<td>Our method</td>
<td>243</td>
</tr>
</tbody>
</table>

4 Conclusions

The paper presents a text hiding technique using Big-5 code. The proposed method applies two Big-5 codes 20 and 7F to encode the secret bit. The Big-5 code 20 is to represent secret bit “0” and the Big-5 code 7F is used to represent the secret bit “1”. The secret bit is hidden into the white-space of between-character and between-word in a cover text. Experimental results show that the visual quality of the proposed scheme achieves good results and feasibility.

References

Infrared Face Temperature Normalization in Fourier Domain

Xie Zhihua, Zeng Jie

Key Lab of Optic-Electronic and Communication, Jiangxi Sciences and Technology Normal University, Nanchang, Jiangxi, 330013
xie_zhihua@yahoo.com.cn

Abstract. This paper proposes a novel temperature normalization method in Fourier domain, which can lessen the effect on infrared face recognition from ambient temperature based on the idea of statistical learning in the transform domain. Firstly, the infrared face images in different ambient temperatures are transformed to Fourier domain. Secondly, based on statistical theory, the variances of phase spectrum and amplitude spectrum of the infrared face are used to describe the extent affected by the ambient temperature. Then, to achieve the robust information, those parts with big variances in the phase spectrum and amplitude spectrum are discarded and replaced by corresponding mean parts in training database. The main idea of this process is that one can set a suitable threshold for the variance of phase spectrum and amplitude spectrum and find those characteristic points that should be replaced. Finally, to verify the effectiveness of our temperature normalization method, the normalized infrared face can be applied to traditional face recognition system based on classic PCA method. Experimental results show our normalization method can get stable information in infrared face and improve the performance of the infrared face recognition system.

Keywords: Discrete Fourier Transform; Infrared face recognition; Temperature normalization; Variance

1 Introduction

Due to its extensive application in identification and security, face recognition has attracted a great many researchers and became a very active research in computer vision and biometrics [1-2]. Currently, most researches on face recognition focus on visual images. The reason is obvious: such sensors are cheap and visual images are widely used. However, the performance of visual face recognition is usually impacted by variations both in intrinsic (pose, expression, hairstyle etc) and extrinsic conditions (illumination, imaging system etc). The infrared radiation which the textures and structures of the face such as the blood vessels and its distribution emit will be a crucial element for the formation of the infrared face images. In addition, the coefficients of the thermal radiation for the faces are obviously different from those for the surrounding scenes and the faces can be easily distinguished from the scenes [3]. So, to some extent, the infrared face recognition technology can be used to compensate the defects existing in the visible face recognition technologies because of its advantages of the uniqueness, owning a good anti-interference performance,
escaping out of the effect of the visible light, preventing the disguises and frauds and so on \cite{4-6}. Several studies have shown that the use of infrared images can solve limitation of visible-image based face recognition, such as invariance to variations in illumination and robustness to variations in pose \cite{12}. However, there are also some limitations for applying the infrared face recognition technology \cite{4-7}. The variation of the ambient temperature can affect the results of the infrared face recognition with the same way as the variation of the illumination can affect the visible face recognition. The testing infrared face images and the training ones may be inevitably collected at different times. In fact, the faces which are collected at the different times usually own different temperatures. As a result, the performance of the infrared face recognition system will drop in this situation. To lessen the effect of ambient on infrared face recognition, the infrared faces in different ambient temperatures need be preprocessed to retain stable information. This process means temperature normalization. The accurate temperature normalization plays an important role in infrared face recognition \cite{3}.

In visible face recognition, a few illumination normalization algorithms are proposed based on frequency domain to lessen the effect of the ambient illumination on the recognition. The reference \cite{8} introduces an illumination normalization algorithm based on the wavelet domain, which converts a face image into the high frequency part and the low frequency part by applying wavelet transform and then process the different frequency elements with different operations. Ju etc \cite{9} proposes an illumination normalization method based on the frequency domain according to analyzing the properties of the phase spectrums and the amplitude spectrums of the face images, which reflects a strong robustness to the variation of the ambient illumination. In addition, the other scholars use the homomorphic filtering to restrain the low frequency elements in order to lessen the effects caused by the variation of the illumination \cite{10}. Inspired by those normalization illumination methods, this paper develops a novel temperature normalization method of infrared face based on transform domain. The main idea of this method is to extract the robust features in phase spectrum and amplitude spectrum of Fourier domain. The main contribution of this paper is that one can set the suitable thresholds both for the variance of phase spectrum and amplitude spectrum to find those characteristic points that are easily variable with the ambient temperature alteration.

2 Temperature Normalization in Fourier Frequency Domain

The process of the normalization in this paper can be introduced as follow:

Step one: The suitable threshold $T_1$ can be set. Those $\lambda_1$ which are higher than threshold $T_1$ are unstable information for infrared face recognition in variable ambient temperature.

Step two: In order to normalize the infrared face in Fourier amplitude spectrum, the amplitude coefficients of the characteristic points corresponding to those $\lambda_1$ are
replaced with the amplitude coefficients of the corresponding characteristic points in the sample-mean image $x_i$.

Step three: Considering the phase spectrum, the suitable threshold $T_2$ can be set to finds out those $\lambda_2$ which are higher than the $T_2$, and replaces the phase coefficients of the characteristic points corresponding to these $\lambda_2$ with the phase coefficients of the corresponding characteristic points in the sample-mean image $x_i$.

Step four: we can get the normalized amplitude spectrum $F_2^{(j)}$ and phase spectrum $\Phi_2^{(j)}$ of the M testing-sample images. Finally, an inverse Fourier transform is applied to gain the normalized testing-sample image $\overline{x_j^{(j)}}$, $j = 1, 2, ..., M$. The $M$ represents the number of the testing samples.

3 Experiment Results

To verify the efficiency of normalization, we use the normalized infrared face images and the original without normalization for infrared face recognition. Those normalization methods are introduced as follows: “RPS+T” means the replacement of the phase spectrum in the thermal infrared face images. “RPS+B” means the replacement of the phase spectrum in the blood perfusion infrared face images. “RAS+T” means the replacement of the amplitude spectrum in the thermal infrared face images. “RAS+B” means the replacement of the amplitude spectrum in the blood perfusion infrared face images. “RPAS+T” means the replacement of the phase and amplitude spectrum in the thermal infrared face images. “RPAS+B” means the replacement of the phase and amplitude spectrum in the blood perfusion infrared face images. “NN+T” means no normalization in the thermal infrared face images. “NN+B” means no normalization in the blood perfusion infrared face images.

In our experiments the best recognition rates of the different methods are shown in the following table.

<table>
<thead>
<tr>
<th>Methods</th>
<th>The recognition rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>$RPS+T$</td>
<td>60.61%</td>
</tr>
<tr>
<td>$RPS+B$</td>
<td>63.64%</td>
</tr>
<tr>
<td>$RAS+T$</td>
<td>57.58%</td>
</tr>
<tr>
<td>$RAS+B$</td>
<td>99.39%</td>
</tr>
<tr>
<td>$RPAS+T$</td>
<td>91.52%</td>
</tr>
<tr>
<td>$RPAS+B$</td>
<td>99.39%</td>
</tr>
<tr>
<td>$NN+T$</td>
<td>44.85%</td>
</tr>
<tr>
<td>$NN+B$</td>
<td>55.76%</td>
</tr>
</tbody>
</table>
References

A Reversible Data Hiding Scheme Using Segmentation Strategy and Histogram Adjustment

Yung-Chen Chou\textsuperscript{1}, Chun-Yi Huang\textsuperscript{1}, and Yu-Chen Hu\textsuperscript{2}

\textsuperscript{1} Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
\{yungchen,huangjannie\}@gmail.com

\textsuperscript{2} Department Computer Science and Information Management, Providence University, Taichung 43301, Taiwan
ychu@pu.edu.tw

Abstract. Because a stego medium is easier to cheat an unexpected user’s observation, Steganography technique is more suitable for delivering secret data. Histogram adjustment is a good way for concealing secret data into a cover image with small distortion. The proposed method is to increase the height of peak in difference histogram as many as possible.

Keywords: Data hiding, Histogram adjustment, Steganography

1 Introduction

Vleeschouwer et al. presented a reversible data hiding technique by using histogram adjustment \cite{6}. Ni et al. also utilized histogram adjustment concept to design a data hiding technique with reversibility \cite{5}. Ni et al.’s method analyzes the pixels distribution in a cover image to generate the histogram and then to figure out the peak point and zero point. After that the secret data is concealed into cover image by adjusting the histogram. Hwang, et al. presented a reversible data hiding technique \cite{1} to achieve the reversibility by extending Ni et al.’s method. Further, Lin and Hsueh utilized bin exchange to modify histogram for increasing pure embedding capacity and get lower distortion \cite{3}. Then, Kim et al. presented a histogram shift based reversible data hiding scheme which selects two peak points and zero points for increasing the embedding capacity \cite{2}. Luo et al. applies pixel prediction strategy to generate the prediction error \cite{4}. Because a higher peak point can get a larger embedding capacity in histogram modification based method. The proposed method uses segmentation strategy for trying to increase the height of peak point for improving the performance of data embedding.

2 The Proposed Method

The proposed method segments the range of difference between a maximum and minimum pixels in a block into several segments. For every segment, a pseudo
pixel will generated by calculating the central point of the segment. In order to achieve the reversibility, the border blocks will be reserved for concealing the extra data. Here, the extra data include the Left Zero (LZ), Left Peak (LP), Right Peak (RP), Right Zero (RZ), and non-embeddable blocks’ information. Further, the secret data stream $S = \{b_k | k = 1, 2, \ldots, N_S\}$, where $b_k \in \{0, 1\}$ and $N_S$ represents the length of the secret stream. For a block $B_i$, except reserved blocks, calculate the length $D_i = B_{\text{max}}B_{\text{min}}$ between the maximum pixel $B_{\text{max}} = \max\{x_j \in B_i\}$ and minimum pixel $B_{\text{min}} = \min\{x_j \in B_i\}$ in $B_i$. According to the proposed embedding procedure, some blocks that cannot be used to conceal data are called non-embeddable blocks when a block satisfies one of following cases.

**Case 1:** If $D_i < N_{\text{seg}}$, then do nothing.

**Case 2:** $B_{\text{min}} \leq N_{\text{seg}}$, then add $B_{\text{min}}$ to extra data and set $B_{\text{min}}$ as 0.

**Case 3:** $B_{\text{max}} \geq 255N_{\text{seg}}$ then add $B_{\text{max}}$ to extra data and set $B_{\text{max}}$ as 255.

In order to reduce the size of extra information, the extra information is compressed by using data compression algorithm.

Next, for embeddable block $B_i$, $B_{\text{min}}$ and $B_{\text{max}}$ where modified as $B'_{\text{min}} = B_{\text{min}} - N_{\text{seg}}$ and $B'_{\text{max}} = B_{\text{max}} + N_{\text{seg}}$. After that, segment the range $D_i$ into $N_{\text{seg}}$ segments. The original pixel will also be adjusted for prevent ambiguous problem. The adjusting rule is making a gap (2 pixels) between two neighboring segments. Then, generate the pseudo pixel for each segment. The pseudo pixel is calculated by $\lfloor (\text{seg}_{k}^{\text{max}} - \text{seg}_{k}^{\text{min}})/2 \rfloor$, where $\text{seg}_{k}^{\text{max}}$ and $\text{seg}_{k}^{\text{min}}$ represent the maximum and minimum value of $k$-th segment for a block, respectively.

Then, the difference image is generated by calculating the difference between original pixels and pseudo pixels. After that, the difference histogram can be gained by statistically counting the difference values from whole image. Then, scan the histogram to figure out LP and RP. Then, scan the histogram to figure out the LZ and RZ. Then decrease the difference histogram between LZ to LP-1 by one to make LP-1 become zero. Again, increase the histogram between RP+1 to RZ by one to make RP+1 become zero. Thus, the secret can be embedded by checking the pixel difference equivalent to LP or RP.

The extracting procedure is a reverse work from the embedding procedure. First, the extra information can be extracted by taking the LSB bits from the reserved blocks. Then, the LP, RP, LZ, and RZ information can be reconstructed. Then, calculate the difference $D_i$ between $B_{\text{min}}$ and $B_{\text{max}}$. If $D_i < 2 \times N_{\text{seg}}$, then the block is a non-embeddable block. Also, if $B_{\text{min}} = 0$ or $B_{\text{max}} = 255$, the block is embeddable, otherwise, the block is embeddable. In **Case 2**, the pixels equal to $B_{\text{min}}$ will be reconstructed by using the information from extra data. In **Case 3**, the pixels equal to $B_{\text{max}}$ will reconstructed by using the information from extra data. For an embeddable block, the segment length is calculated by $\lfloor D_i/N_{\text{seg}} \rfloor$.

After finishing the segmentation procedure, generate the pseudo pixel for every segment and calculate the difference between pixel and pseudo pixel. The secret data extraction can be done by using following rules.

**Rule 1:** If the difference equal to LP-1 or RP+1 then output secret bit ‘1’.
**Rule 2**: If the difference equal to LP or RP, then output secret bit ‘0’. If the difference is located in LP-2 to LZ then increase the difference by one. If the difference is located in RP+2 to RZ, then decrease the difference by one. After that, the pixels will be reconstructed by calculating pseudo pixel plus difference. Finally, the pixel is readjust to the original.

### 3 The Experimental Results

The visual quality of stego image and embedding capacity are two most important factors for evaluating a data hiding technique performance. Peak-signal-to-noise-ratio (PSNR) is adopted for measuring the visual quality of stego image. On the other hand, the embedding capacity is to count the total bits embedded into a cover image. From experimental results, we found that a complex content image (e.g., Baboon) will get higher embedding capacity when the segment number increased. In general content image (e.g., Lena), 5 is a suitable segment number. The proposed method has better performance than Luo et al.’s method in terms of embedding capacity when the segment number is greater than 1.

### 4 Conclusions

The proposed scheme utilizes the segmentation strategy for trying to increase the height of peak point in histogram as many as possible. From experimental results, the proposed method significantly improves the performance of Luo et al.’s method in terms of embedding capacity.

### References

Experiments of DDoS detect using Triangle Expectation with MapReduce

Jin-Hyun Yoon, Ho-Seok Kang and Sung-Ryul Kim

1 Division of Internet and Media, Konkuk University, Seoul, Republic of Korea
h2jhyoon@gmail.com, hsriver@gmail.com, kimsr@konkuk.ac.kr

Abstract. With the growing use of the Internet, Internet security has become important. Increasing damage has been done by Distributed Denial-of-Service attacks (DDoS). In this paper, a technique called "triangle expectation" is used, which works to find the sources of attack so that they can be identified and blocked. To analyze a large amount of collected network connection data, a sampling technique has been used and the proposed technique is verified by experiments.

Keywords: Triangle Expectation, Triangle Counting, Hadoop, Sampling

1 Introduction

With increasing use of the Internet, Internet attacks are on the rise. Distributed Denial-of-Service (DDoS) in particular is increasing more [3]. There are four main ways to protect against DDoS attacks: attack prevention, attack detection, attack source identification, and attack reaction. The protection approach proposed in this paper belongs to the attack source identification category.

Most DDoS attacks work by the following three components: the first attacker; the zombie PC; and the victim. Assume that a graph is constructed so that the nodes represent various computers on the Internet and the edges represent having histories of connections between the computers. If there are three nodes, which are connected with two edges, and another edge is needed in order to complete a triangle, then the situation is called a triangle expectation. Triangle expectation is the technique used to find this expected edge. The nodes of the triangle expectations found can be considered the attacker, the zombie PC, and the victim. For performance reasons, we used the sampling method of DOULION [1], which is implemented with MapReduce. We verify that the triangle expectation technique can identify attack patterns and also that the sampling strategy does not reduce the accuracy of triangle expectation.

2 Using Triangle Expectation defense mechanisms

In DDoS attacks zombie PCs connect to the server or router to cause an overload or to starve the server of resources and make service impossible. Illustrated in Fig. 1 (a), the
hacker uses the Command and Control (C&C) server [5] to send attacking command to zombie PCs, uses them to attack the victim. Thus there has to be many triangle expectation present between the C&C Server and the victim. Our system works by collecting network connection information from many routers for some time period. We can see that when an attack actually occurs, a large number of triangle expectations are generated between the C&C server and the victim.

Fig. 1. (a) Botnet Attack (b) Triangle Expectation of relationship

After the triangle expectations are computed, the zombie PCs are easily identified and blocked. Further, the C&C server is also identified so that it may be confiscated for further investigation.

For performance reasons, we have used the sampling method of DOULION. DOULION chooses each edge with probability $p$ and the total amount of computation reduced by a factor of $1/p^3$. We will later verify that the reduced computation does not result in the reduction of correctness of our results.

3 Experiment Result

The experiment was conducted in two ways to verify the triangle expectation technique and also to verify that the sampling technique is justified. We combined random connection patterns (RCP) and simulated DDoS connection patterns (SDCP) as one dataset. In RCP the nodes connect to generally popular sites (approximately 120,000 edges). SDCP are created using DDoS attacks patterns (2,000 edges). We combined the two datasets together. The experiments are performed using Map-Reduce (in Fig2) [4]. The actual algorithm is very similar to that of DOULION and is omitted in this version.

Fig. 2. Map-Reduce

The result is shown in Fig. 3(a). In the figure, the x-axis is the number of triangle expectations that are shared by one edge, and the y-axis is the number of occurrences of such edges. We can see that when the number of triangle expectation increases, the
number of edges decreases naturally. When the value of the triangle expectation is between 213 and 1,000, there is no edge shared by that many triangle expectations but at 1,000 we have found two edges that are shared by that many triangle expectation, which is an indication that the two nodes connected by any of the edges are the C&C server and the victim. Fig. 3 (b) just focuses on the important part of the graph in (a).

![Fig. 3](image)

Fig. 3. Number of edge occurred Triangle Expectation (a) Total View (b) Subset of (a) between 88 and 1,000 (c) Sampling view

Fig. 3(c) shows the result after the sampling technique is applied. We can clearly see that the edges connecting the C&C server and the victim can still be easily identified. A linear-time computation, which takes much less time than the triangle expectation, will also find the zombie PCs easily.

4 Conclusion

In this paper, we proposed a new method of DDOS detection using triangle expectation method. When a DDoS attack occurs, data are collected from many routers, and many triangle expectations are found for many sets of nodes, in order to find the attacker and the attack path. To analyze a large amount of collected data, sampling is used, reducing the amount of calculations needed and the time taken. The results are verified by experiments.

Acknowledgments. This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2012-H0301-12-3006)

5 References

Improving Clonal Selection Algorithm in Security Optimization

Long Li¹, Tao Gong¹,²,³, *, Changsheng Guo¹, Xiaolei Gong¹
¹ College of Information S. & T., Donghua University, Shanghai 201620, China
² Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education, Donghua University, Shanghai 201620, China
³ Department of Computer Science, Purdue University, West Lafayette 47907, USA
* Corresponding author: taogong@dhu.edu.cn

Abstract. To keep computer systems and networks secure, some optimization problems, such as optimal learning of unknown viruses, can be solved by clonal selection algorithm. In this paper, we improve the clonal selection algorithm with such selection operators as Roulette Wheel Selection operator, Tournament Selection operator, and Sampling Selection operator. The selection operators are useful for finding the optimal solutions more quickly and accurately. The experimental simulations show that the new clonal selection algorithms with the three selection operators have better results, such as best solution, worst solution and fitness, than the clonal selection algorithm with the traditional operator.

Keywords: Clonal selection; roulette wheel selection; tournament selection; sampling selection; security optimization.

1 Introduction

Unknown viruses are difficult to detect and learn in some security applications [1], because some traditional algorithms are not good for searching the optimal solutions for the unknown viruses. In this security optimization field, genetic algorithms (GA) and immune algorithms (IA) have been widely studied and used. There are analogous points between the two algorithms, though, they are totally different substantially. In recent decades, some researchers have attempted to integrate the two algorithms as new hybrid algorithms, which will perform better than the single algorithms. For example, Licheng Jiao et al. added immune methods into the GA and designed an immune genetic algorithm [2], which mainly includes two steps, i.e. vaccination and immune selection. Antariksha Bhaduri used GAIN, a hybrid mathematic algorithm based on GA and Artificial Immune Network, for optimizing university time table scheduling problem [3]. Selection operator is an essential of genetic algorithm, which determines the performances such as convergence, feasibility and efficiency of the whole algorithm. Apparently, it occupies position among the series of steps researchers concern mostly of immune algorithm. In this paper, selection operators usually employed in genetic algorithm and based on fitness are transplanted to clonal selection algorithm (CSA) after adjusted and improved to lead the CSA to perform
more astringently and multifariously. The simulation experiments suggest that the improved selection operators can be used in the CSA.

2 Improving Clonal Selection Algorithm

As similar to the GA, the CSA originated from biological mechanism in nature. Leandro Nunes de Castro designed the CSA in 2000, and successfully verified the algorithm can be feasibly applied in Partition Recognition, Multi-Modal Optimization and Travelling Salesman Problem [4].

The CSA mainly constitutes of selection operation, clonal operation, mutation operation, memory operation and several other steps. For example, in optimization problem the objective function value of the related antibody is commonly used, or in handwriting character recognition an equation contributes to the similarity between the normalized feature matrices of binary images [5]. Selection operation will save the antibody whose fitness supers and those of the other antibodies would be discarded. After the selection operation, the clonal operation makes the selected antibody cloned based on the size of the fitness. In the mutation operation, the mutation ratio is proportional to the fitness value. Greater antibody fitness determines smaller mutation rate, and vice versa. In order to improve the local search ability, the ratio tends to a decreasing trend according to the number of iterations.

In the CSA, to adjust or fix the randomness of sampling selection, the proportion accounted for the fitness of the total population is divided into parameter $s_n$ parts.

\[
  n_i = N \cdot \frac{F_i}{\sum_{j=1}^{N} F_j} \cdot \frac{1}{\text{Integer}(\max(F) - \min(F))}, \quad (1)
\]

3 Experiments and Analysis

To validate the feasibleness of applying the three strategies in the CSA, function 1, which has several peaks, one of them is the highest and one of them is close to the highest, is employed to do the test. Function 1 has two regions. One is called Highest Region which is a locate region of the highest peak, and the other called Sub-highest Region, also a locate region but of the sub highest peak. Because the stochastic element added into clonal selection algorithm should be proper, just replace the first selection in the algorithm to the top three strategies.

100 tests were processed applying the above strategies. In every test, we got a best fitness. Table 1 shows the statistics data on the best fitness value, the worst fitness value, number of individuals located in the Highest Region, number of individuals located in the Sub-highest Region, the mean value of fitness and the variance of fitness.
Table 1. Experimental results of different selection operators in the CSA.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Best solution</th>
<th>Worst solution</th>
<th>Right Region</th>
<th>Wrong Region</th>
<th>Mean Fitness</th>
<th>Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>raditional selection operator</td>
<td>111.5988</td>
<td>107.2897</td>
<td>63</td>
<td>37</td>
<td>109.2938</td>
<td>1.2448</td>
</tr>
<tr>
<td>Roulette selection operator</td>
<td>111.6650</td>
<td>109.0063</td>
<td>29</td>
<td>8</td>
<td>111.0783</td>
<td>1.0591</td>
</tr>
<tr>
<td>Tournament selection operator</td>
<td>111.6650</td>
<td>108.0164</td>
<td>67</td>
<td>14</td>
<td>110.7421</td>
<td>1.3136</td>
</tr>
<tr>
<td>Det Sampling selection operator</td>
<td>111.6650</td>
<td>106.8363</td>
<td>55</td>
<td>5</td>
<td>111.2906</td>
<td>0.8050</td>
</tr>
<tr>
<td>Sto Sampling selection operator</td>
<td>111.6650</td>
<td>106.9761</td>
<td>48</td>
<td>23</td>
<td>110.3836</td>
<td>1.9359</td>
</tr>
</tbody>
</table>

4 Conclusion

This paper applied some selection operators into the clonal selection algorithm to improve the performances such as the best solution, the worst solution and the fitness. Experimental simulations show that the new clonal selection algorithms of the Roulette selection operator, the Tournament selection operator and the Sampling selection operator perform better than that of the traditional selection operator. This improvement will result in better security optimization such as learning of unknown viruses of some computer systems and networks.

Acknowledgements

The work was supported by grants from Natural Science Foundation of Shanghai (08ZR1400400), the Shanghai Educational Development Foundation (2007CG42), the National Natural Science Foundation of China (60874113), and NSF-0242840.

References

Research on Immunizing Embedded Linux Core Against Viruses and Software Faults

Tao Gong¹,²,³, Changxing Du¹

¹ College of Information S. & T., Donghua University, Shanghai 201620, China
² Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education, Donghua University, Shanghai 201620, China
³ Department of Computer Science, Purdue University, West Lafayette 47907, USA

taogong@dhu.edu.cn

Abstract. Linux is more secure than other operation systems such as Windows, but the embedded Linux core need be more secure by its immunization against viruses and software faults. First, the embedded Linux is customized from the standard Linux by keeping the Linux core and deleting the unnecessary components. Immunization of the Linux core is designed into the process control, memory management, communication, driving programs, and file system. The artificial immune system of the embedded Linux core is built on the tri-tier immune model, and both viruses and software faults are detected as nonselfs. The selfs are the normal components and the nonselfs are foreign viruses, infected selfs, lost selfs and damaged selfs. This immunization technique will be tested on a prototype of embedded Linux core, by protecting the file system and repairing the damaged files.

Keywords: Embedded system; Linux core; immunization; virus; software fault.

1 Introduction

Unknown viruses are difficult to detect and learn in some security applications [1], and the operation systems such as Windows and Linux have vulnerability to the viruses and attacks. To repair the vulnerability, users need update the operation systems online to set up some new security patches. This updating often provides a new chance for the viruses and attacks to spread the damage through the network. So threat modeling is used to expose some circumstances or events having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service, and results in a vulnerability assessment. Similar to the threat model, the immune danger theory was proposed by Matzinger [2], and in this danger theory immune response distinguishes the danger signals that are generated by damaged cells. In the embedded Linux core, the threats are the damaged selfs and the foreign non-selfs such as the blackhole attacks and the virus-based wormhole attacks [3], so the threats are the non-selfs in nature. First, the blackhole attacks can transmit malicious broadcast information from a node that the node has the shortest path to the destination aiming to intercept messages. And the wormhole attacks can record
packets at one location in the network, tunnel them to other locations, and retransmit them there into the network via viruses.

In fact, the human immune system has another different and advanced security approach to protect the body [4], and this immunization approach emphasize more on selves (i.e. normal components such as normal cells, immune cells, and antibodies) than the nonselfs such as viruses and cancer cells.

Inspired from this natural powerful security system, a new idea of immunizing the embedded Linux core is proposed to build the normal models of selves and defend this core against the viruses and software faults, in this paper.

2 Immunizing embedded Linux core

Standard Linux is a complex operation system, which has too many components to be set up in embedded systems. So this standard Linux needs trimming to be customized in the embedded systems, and the Linux core should be revised and compiled. The embedded Linux core has some necessary files and directories. The immunization of the embedded Linux core is made in process control, memory management, communication, drivers and file system.

The embedded Linux core utilizes various data structures to organize the system processes in different ways, according to various requirements of the process control sub-system. Each process has its unique identification number (PID), and the immunity of the process control protects the core data structures, which the processes use. Memory is one of the most important resources in control of the Linux core, and the memory management sub-system is the most important and difficult part of operation system. The root file system is a necessary file system for running the Linux operation system. Driver design is an important step to develop embedded systems, and the drivers provide the interfaces for the applications to control the hardware. The normal embedded systems are based on the normal states of the drivers. The immunity of the driver is used to monitor the normal state of the driver and assure the proper output of the diver. The embedded systems often communicate with other embedded systems or foreign networks, and the security is not only based on the security of the communication protocol, but also relative with the security of the Linux core. If the immune Linux core can detect the data packages with such nonselfs as viruses by detecting the selves of this core first, this communication will be more secure. In many embedded systems, the data spaces of users are private, so the immunity of the Linux core protects this privacy.

3 Testing immune Linux core and NS2-based experiments

The immune Linux core is compiled according to the regular compiling method, and the step for compiling the immune programs is just after the step for building the normal model of the embedded system. After the immune programs are compiled, the files Makefile and Konfig are revised and generated. The mirror of the Linux core
uses the zImage mirror, and this mirror can be downloaded into the development board to test.

To validate the immunization approach for the embedded system, 2 embedded systems such as ARM9 and ARM11 and 3 notebooks build a real mobile ad hoc network. As one node was compromised by the blackhole attack, the routing table of this node was changed the attack, and so the client program of this node sent no any data to the other nodes. The wormhole attack changed the routing table of the compromised node, and spread the wormhole attack via the client program of this node into other nodes.

Due to the amount limit of notebooks, ARMs and Zigbee devices, the node amount of the real ad hoc network was as small as five, but the node amount of the simulations with the Network Simulator 2.35 was expanded to as large as 20. Comparing with the packet delivery ratios (PDR) of the network under the collaborative attacks and the network based on the regular Intrusion Detection System (IDS) against the attacks, the packet delivery ratio of the network with cooperative immunization was higher. This result shows that the cooperative immunization is faster and more effective against the collaborative attacks than the regular IDS.

4 Conclusion

The embedded Linux core is very important for many applications of the embedded systems, and the immunization of this embedded Linux core is important for its security. First, the normal model is useful to build the selfs and identify the normal state of this embedded system by the space-time properties. Then, based on this normal model, the viruses and software faults can be detected quickly and accurately, so the immunization can be created for the embedded system of such modules as process control, memory management, communication, drivers and file system etc.

Acknowledgements. The work was supported by grants from Natural Science Foundation of Shanghai (08ZR1400400), the Shanghai Educational Development Foundation (2007CG42), the National Natural Science Foundation of China (60874113), and NSF-0242840.

References

Secure Gauge Control System Based on ARM and Fuzzy PI Controller

Tao Gong1, 2, 3, Lei Qi1

1 College of Information S. & T., Donghua University, Shanghai 201620, China
2 Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education, Donghua University, Shanghai 201620, China
3 Department of Computer Science, Purdue University, West Lafayette 47907, USA
	taogong@dhu.edu.cn

Abstract. To minimize the longitudinal strip thickness error in the hydraulic cold rolling industries and improve traditional AGC control scheme on this problem, we put forward a secure gauge control system based on Advanced RISC Machines (ARM) and intelligent PI control strategy. The traditional automatic gauge control (AGC) scheme depended on personal experience about the parameters, and bad parameter values could lead to an accident of manufacture security. The new gauge control system decreases the longitudinal strip thickness error via fuzzy control and ARM-based computing. Besides, this new system can be smaller than the traditional AGC system, and so is much easier to transport. The Fuzzy control scheme can increase the robustness of the ARM-based gauge control system against some disturbances.

Keywords: Secure gauge control system; ARM; fuzz PI controller; longitudinal strip thickness error; AGC system.

1 Introduction

The automatic gauge control system, named as AGC, has been adopted widely in the hydraulic cold rolling industries. It is well known that the hydraulic cold rolling mill consists of screw-down system, backup roll, work roll and all kinds of sensors. The screw-down system, which generates power, is made up of cylinder, servo valve and the sensors of pressure and position. With pressure sensors, the feedback control of pressure comes into being. In like manner, with position sensors, the screw-down system can accurately track the cylinder’s position. Neither position nor pressure control of the screw-down system can be directly used to control the thickness error of sheet strips.

As we know, the traditional PI control took a useful role for the gauge control in the hydraulic cold rolling industries, but this control approach is challenged by the increasing requirement on error. It is recently discovered that the electromagnetic disturbance can decrease the effectiveness of the AGC system, so a new control system that can adjust the parameters by itself is necessary against the disturbance. Due to the wrong experience and random disturbance, the ineffective control may cause the
damage of the control object and the operators. For example, a control algorithm is proposed with neural network (NN) is investigated [1]. In this paper, a secure gauge control system is designed on the Advanced RISC Machines (ARM) and intelligent PI control strategy.

2 Design of controller based on ARM

With the requirement of the quality of sheet strips, especially the thickness deviation between 2~3 micrometer, the traditional AGC control strategy meets great challenges. Through the analysis of the dynamic model of the hydraulic cold rolling mill, we find that nonlinearities exist and it is terribly difficult to cope with slowly time-varying factors. It is more and more clear that classic control theory is not use for nonlinearities, time-varying and strong coupling factors, etc. Therefore, modern control theory and intelligent theory like fuzzy logic and fuzzy inference should be studied deeply and it is necessary to transplant these intelligent algorithms to modern process control industries. What is more important, traditional AGC system is realized by PLC or Industrial Computer, and gauge controller based on ARM is illustrated as follows. With the development of embedded technology, more and more embedded systems based on functional processors surge into the computer market. As for the nonlinear and time-varying characteristics of hydraulic screw-down servo system, it’s important to design a intelligent gauge controller based not on accurate mathematic models of objects with great stability and control precision. The root of the problem is that, the conventional PID does not have parameter self-setting function, and not address complex environment to make the adaptive parameter adjustment. Compared to traditional AGC system, the control scheme above takes some advantages. First, with the fuzzy controller, it’s no need to build the accurate mathematical models of hydraulic cold rolling mills. Second, experience from experts and even from operators becomes several basic principles and it leads to extent of satisfactory of system control.

As follows are the modules of the AGC fuzzy PID controller based on ARM. According to modular strategy, the fuzzy PID controller is made up of technological setting module, position signal sampling module, gauge signal sampling module, executing unit, signal processing unit and pressure signal sampling module, and so on.

In order to prompt the anti-interference ability of the ARM-based fuzzy PID controller, several measures have been taken. First, in the power supply of ARM chip, the join of decoupling capacitor improves the circuit of electromagnetic compatibility (EMC) ability. Second, photoelectric isolations assure that the electrical current cannot feedback to the fragile ARM chip.

3 Experimental simulations

First, build the transfer function of hydraulic screw-down servo system of the cold mill. The screw-down system consists of servo valve, amplifier and hydraulic cylinder. The functions of components of the screw-down system are given as below.
(1) Servo Amplifier

\[ G_{\text{amp}}(s) = K_a G_c(s) = 0.146 \cdot \frac{0.2s + 1}{2.4s + 1} \]  

(2) Servo Valve

\[ G_{sv}(s) = \frac{K_{sv}}{s^2 + \frac{2\xi_{sv}}{\omega_{sv}}s + 1} \]  

Hydraulic Cylinder:

\[ G_{cyl}(s) = \frac{39.32}{s\left(\frac{s^2}{182.7^2} + \frac{2 \times 0.35}{182.7}s + 1\right)} \]  

Position Sensor: \( G_p(s) = K_p = 100 \)

To sum up, the transfer function of the hydraulic screw-down servo system is showed as below.

\[ G_{\text{screw-down}}(s) = G_{\text{amp}}(s) \cdot G_{sv}(s) \cdot G_{cyl}(s) \cdot G_p(s) \]  

4 Conclusion

Compared with the conventional PID using in traditional AGC control system, the gauge control system based on ARM and fuzzy PI is more helpful to improve the system stability and less dependent on the accurate mathematics model of object. Based on the inherent nonlinearities of fuzzy control strategy, our design of combining fuzzy logic with conventional PID plays an important role in the hydraulic rolling industries.

Acknowledgements. The work was supported by grants from Natural Science Foundation of Shanghai (08ZR1400400), the Shanghai Educational Development Foundation (2007CG42), the National Natural Science Foundation of China (60874113), and NSF-0242840.

References

Abstract. In this paper, we present a smart grid monitoring system connected with electric vehicle charging system using anti-islanding method. The monitoring system was implemented in Local Area Monitor Module and it communicates with end modules wirelessly using Zigbee protocols. The charging of electric vehicles can be remotely controlled by the presented monitoring system more efficiently and more conveniently. It is shown by some experiments that the presented smart grid monitoring system provide useful information with electric power to electric vehicles while detecting anti-islanding in the smart grid.

Keywords: Electric Vehicles, Smart Grid, Anti-Islanding, Electric Vehicle charging.

1 Introduction

Traditional energy solutions cause unrecoverable damages to nature i.e., fossil fuel releases CO₂ in the atmosphere and nuclear power plant emits radioactive waste. Various types of vehicles are being actively developed which use electric energy in part or fully such as hybrid vehicles, fuel cell hybrid vehicles, electric vehicles, etc. We can imagine hundreds of electric vehicles are waiting for charging from electric power suppliers in the near future. Vehicle data communication and certification process are performed between EV and EV charging systems (EVSE: Electric Vehicle Supply Equipment) usually by using wired communication like CAN (Controller Area Network) protocol and power information between smart grid and the EVSE are communicated by using wireless network protocols [1]-[3].

In this paper, we propose a smart-grid remote power monitoring system using anti-islanding method. Smart grid system is connected EVSE for remote control of EV charging. Wired and wireless communication protocols are effectively used in the smart grid between devices including EVs. The basic communication between the smart grid and the EVSE use the ZigBee technology since it has low power requirements and a simple configuration and the EVSE communicates with EV using CAN protocol. The efficiency of this smart grid monitoring system was tested on an experimental system using HILS (Hardware-In-the-Loop-Simulation) of EV and EVSE.
2 Remote Monitoring System and HILS-based Experimentation

The block diagram of the proposed RMS is as shown in Figure 1 which is applied to a micro-grid. It consists of several different components, such as an End Monitor Module (EM), a Local Area Monitor Module (LAM), a Wide Area Monitor Module (WAM), and client devices.

![Figure 1. The block diagram of the RMS.](image1)

![Figure 2. HILS of EV and EVSE.](image2)

HILS developed for EV charging is composed of EVSE and EV. EVSE connected to smart grid having anti-islanding method, it is using smart grid power for EV charging. Because smart grid having Anti-islanding method, we can be expected EV charging to safety. The structure of the developed HILS is shown in Fig. 2.

Existing islanding detection methods have some problems. First, due to the conversion of the generator output signal to an arbitrary signal, the power quality is reduced. Second, existing anti-islanding methods have a NDZ (Non-Detect Zero) problem. Therefore, in this paper, to secure the above problems, EV charging through linking with smart grid having Anti-islanding method is proceeding smoothly and reliably seems to come true.

We can analyze the status of the distributed generator systems based on these waveforms and data. In addition, The EV charge using the power of the smart grid should proceed. Smart grid was use the normal household AC power for EV charge. EV charging status information can be seen of Using EV monitoring system. HILS miniature and monitoring system is shown in Fig. 3.

![Fig. 3. The experimental End Monitor Modules and the LAM monitor program.](image3)
Experimental setup is consists of two sensor nodes and LAM. One of LAM is EVSE. EV and EVSE charging connection has been progress. EVSE by connecting one of the LAM was charge in progress. We can check the charge process of during charging of EV from monitoring system. Sensor node using the smart grid monitoring system has solved the problem. The LAM get guarantees a short cut-off time to prevent islanding in less than 1 second. The result of experiment is shown in Figure 5. Figure 5 shows the detecting time of islanding and the status of EV charging voltage. If islanding occurred, EV charging voltage is a little drop down while replaced EM.

Figure 4. The Detecting time of islanding and EV charging voltage at occurred islanding

3 Conclusions

This paper presented the smart grid monitoring system with islanding detection method using a sensor network. The smart grid system consists of a WAM, LAMs and EMs. It was illustrated that the presented monitoring system can detect islanding and redirect power flow to another power source within tolerance time.

Acknowledgments

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2012-H0301-12-2007)

References

A Modular Transform Method of Crypto Algorithm for Optimized FPGA Synthesis

Dongsoo Kim\textsuperscript{1}, Hae-Wook Choi\textsuperscript{2}

\textsuperscript{1} Attached Institute of Electronics and Telecommunication Research Institute
Daejeon, Korea
\textsuperscript{2} Dept. of Electrical Engineering
Korea Advanced Institute of Science and Technology, 103-6 Munji-dong, Yuseong-gu
Daejeon 305-732, Korea
\textsuperscript{1}\{heavikim\}@ensec.re.kr, \textsuperscript{2}\{hwchoinew\}@kaist.ac.kr

Abstract This paper describes optimization methodology of FPGA implementation of crypto algorithm in embedded system. In USN (Ubiquitous Sensor Network) or Ubiquitous computing environment, security is taken accounted of as important element in implementation. But when security is applied to embedded system, it tends to have degrading effect on overall system performances of throughput and communication network bandwidth. One of the most influential factors is security throughput of embedded system. Key generation speed is critical to throughput and efficiency of security system. The methodology proposed in this paper is about how to enhance the security computation speed in embedded system. As a synthesis technique for increasing throughput, transform method from a sequential processing to a parallel processing is exploited in FPGA implementation. In this paper the non-algebraic shrinking key generator is explained to give an example of the transform method. The designs in VHDL were synthesized and implemented in Altera Cyclone 6000T devices.

Key words: modular transform, crypto algorithm, non-Boolean algorithm

1 Introduction

The rapid growth of computer and communication networks has enhanced the demand for security algorithm computations in embedded system that can handle high-speed data rate. Concerns about vulnerability of such a high rate system enforce complex-structured security algorithm to be embedded and executed at a high rate, so a lot of effort is needed to make complex-structured invulnerable security algorithm be hardware-friendly suited to high-speed applications. Two main implementation methods are exploited to optimize the trade off between high-speed and invulnerability.

1. Transform from a serial structure (sequential computation) to a combinational structure (parallel computation).
2. Computation with pipelining stages.

Implementation method 2 is generally applied to any structured algorithm, but implementation method 1 becomes more sophisticated to apply if the algorithm cannot be expressed in Boolean functions. One of most famous non-Boolean security algorithm is the shrinking key generator. Because it is non-Boolean and non-algebraic, up to date there exists no known attack method. No high-speed shrinking key generator hardware implementations have been reported in the recent literature.
2 Implementation

We coded the design in VHDL, simulated with Mentor Graphics ModelSim 5.7f and synthesized with Altera Quartus 3.1, targeting Altera Cyclone 6000T.

2.1 Sequential design

Fig. 1. Sequential computing structure

The sequential computing structure is composed of two Nth LFSR (one is the Nth selection LFSR and the other is the Nth source LFSR), the selection logic (diamond-shaped) and the Nth accumulating register. All three registers are circular right shifting registers as shown in Fig. 1.

S-stream is a sequence of consecutive s[0]s that are LSB (Least Significant Bit) of the selection LFSR for each clocking cycle and a-stream is a sequence of consecutive a[0]s that are LSB of the source LFSR for each clock cycle. The selection logic in Fig. 2 produces z-stream, which is a sequence of consecutive z[N-1]s that are MSB of the accumulating register, in a following way.

- If s[0] = 1 then z[N-1] = a[0] (1)
- If s[0] = 0 then z[N-1] = Null (2)

where Null means Non-existence of bit.

It was reported and proved that the shrinking key generator in Fig. 1 has periodicity \(2^{N-1}\) and linear complexity from \(N(2^{N-2})\) to \(N(2^{N-3})\) in [1].

The shrinking key generator in Fig. 1 is easy to implement in a sequential design, because only (1) and (2) need to be implemented.

Fig. 2. Schematic diagram of sequential design
In Fig. 2 if s[0] is 1, a[0] is inserted to z[N-1] and after clock edge the accumulating register shifts right, making z[n-2] equal to z[n-1]. If s[0] is 0, Null signal of the accumulating register is asserted and none inserted to z[N-1], making z[N-1] invariable, and after clock edge the accumulating register does not shift right, making z[n-2] invariable.

In Fig. 3 behavioral VHDL codes that synthesize the shrinking key generator are shown. In behavioral VHDL code A(i), B(i) and Q(i) represent the selection LFSR, the source LFSR and the accumulating register respectively.

\[
\text{if } A(i) = '1' \text{ then} \quad \text{(3)}
\]
\[
\text{temp (index)} := B(i); \quad \text{(4)}
\]
\[
\text{index := index + 1 ;} \quad \text{(5)}
\]
\[
\text{end if} \quad \text{(6)}
\]

Above codes (3) ~ (6) represent the selection logic in Fig. 1. We recognize that as N increases more than 4, timing simulation result after synthesis gets more different and deviatory from functional simulation result before synthesis, so that behavioral VHDL design is inadequate to implementing the shrinking key generator.

\[\text{if } A(i) = '1' \text{ then} \quad \text{(3)}
\]
\[\text{temp (index)} := B(i); \quad \text{(4)}
\]
\[\text{index := index + 1 ;} \quad \text{(5)}
\]
\[\text{end if} \quad \text{(6)}
\]

2.2 Combinational design

To advance generation speed of the shrinking key generator, the sequential computing structure must be transformed to the combinational (parallel) computing structure. In contrast to the sequential structure, the parallel computing structure is based on N-bit length bus architecture. Operation of the selection logic can be expressed in following pseudo-codes.

For \( (i = 0 ; i < N ; i++) \)

\{ 
  If \( s[i] = 1 \) then \( z[index++1] = a[i] \); (7) 
  If \( s[i] = 0 \) then NULL; (8) 
\}

If \( (\text{Index} = N) \) (9)

\{ 
  Load N bit word and produce N bit 
\}
As we recognize in 2.1, due to behavioral nature of above pseudo-codes it can not be converted to synthesizable VHDL code. Block diagram of the N-bit bus-based parallel computing structure is shown in Fig. 4. Only a difference between Fig. 2 and Fig. 4 is the selection logic and the index indicator. The selection logic must perform (7) ~ (11) pseudo-codes and the index indicator counts the number of 1 of $s[N]$ from the selection LFSR.

![Fig. 4. Schematic diagram of N bit bus architecture](image)

To make it simple, we propose divide-and-conquer scheme as design approach. In case of $N=4$, the selection logic functions as if it does in Fig. 5. As shown in Fig. 5, value of $s[3]$ is 1, which causes $z[3]$ equal to $a[3]$ that is 1, and value of $s[2]$ is 0, which causes $a[2]$ neglected. Continually value of $s[1]$ is 1, which causes $z[2]$ equal to $a[1]$ that is 0 and value of $s[0]$ is 0, which causes $a[0]$ neglected. The selection logic produces two bits of $z[3]$ and $z[2]$, each of them being 1 and 0 respectively. Be worthy of notice is that value of $a[0]$ is pushed to the place of $z[2]$, since previous two bits of $s[2]$ and $s[1]$ being 0 make corresponding $a[2]$ and $a[1]$ neglected. The selection logic is such that it produces $z[n]$ value depending on previous history of values of $s[n+1], s[n+2] ...$etc. Such a selection logic in case of $N=4$ can be designed with sophisticated combination of 2:1 MUXs, as shown in Fig. 6, which we define $4\times4$ Pushing logic.

![Fig. 5. Operation of Selection logic for N=4](image)

We define the composite of four through logic elements as $4\times4$ through logic which is shown in Fig. 7. It must satisfy any combination of $s[3], s[2], s[1], s[0]$.
In table 2, the truth table for the 4×4 through logic lists all possible combinations of \(s[3], s[2], s[1]\) and \(s[0]\). It was tested for the truth table for the 4×4 through logic and verified with simulation tool ModelSim 5.7f. We can expand the selection logic for \(N=8\) to one for \(N=16\), using the 4×4 pushing logic and the 4×4 through logic as a basic building block in a same method. The selection logic for \(N=16\) is derived from four \((1+1+1+1)\) 4×4 pushing logics and six \((1+2+3)\) 4×4 through logics.

**Fig. 6.** 4×4 Pushing logic design with 2:1 MUX

**Table 1.** Truth table for the 4×4 pushing logic

<table>
<thead>
<tr>
<th>(s[3])</th>
<th>(s[2])</th>
<th>(s[1])</th>
<th>(s[0])</th>
<th>(z[3])</th>
<th>(z[2])</th>
<th>(z[1])</th>
<th>(z[0])</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>(a[0])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
<td>(z'[1])</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>(a[1])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
<td>(z'[1])</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>(a[1])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(a[2])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
<td>(z'[1])</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>(a[2])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>(a[2])</td>
<td>(a[1])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>(a[2])</td>
<td>(a[1])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(a[3])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
<td>(z'[1])</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>(a[3])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>(a[3])</td>
<td>(a[1])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>(a[3])</td>
<td>(a[1])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(a[3])</td>
<td>(a[2])</td>
<td>(z'[3])</td>
<td>(z'[2])</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>(a[3])</td>
<td>(a[2])</td>
<td>(a[0])</td>
<td>(z'[3])</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>(a[3])</td>
<td>(a[2])</td>
<td>(a[1])</td>
<td>(z'[3])</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>(a[3])</td>
<td>(a[2])</td>
<td>(a[1])</td>
<td>(a[0])</td>
</tr>
</tbody>
</table>

**Fig. 7.** 4×4 through logic composed of four through logic elements

- 219 -
Table 2. Truth table for the 4×4 through logic

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>z'[2]</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>z'[2]</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>z'[2]</td>
<td>z'[1]</td>
<td>z'[0]</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>z'[3]</td>
<td>z'[2]</td>
<td>z'[1]</td>
<td>z'[0]</td>
</tr>
</tbody>
</table>

3 Statistics

Both sequential design and combinational design have the following I/O connections.

| input_source a[15:0] | 16 bit input from source LFSR |
| input_selection b[15:0] | 16 bit input from selection LFSR |
| output_accmulation z[15:0] | 16 bit output from accumulation register |
| clock | Clock signal |

We synthesize structural VHDL code of the schematics of Fig. 2 for implementing the sequential shrinking key generator and structural VHDL code of the schematics of Fig. 4 and Fig. 8 with Altera quartus 3.1 VHDL compiler, targeting Cyclone 6000T. Input_source a[15:0] and input_selectin b[15:0] are applied simultaneously every clock cycle. Clock frequency is 48 MHz. Implementation results for two designs are shown in Table 3. Notice that logic cell area of the combinational design is about 50 times more occupied than that of the sequential design in FPGA implementation. The speed of the combinational design is approximately 12 times faster than that of the sequential design. The transform from the sequential to the parallel structure improves overall performance of speed by 10 times faster than that of the previous conventional sequential implementation.
Fig. 8. Selection logic with two pipelining stages

Table 3. Comparison of implementation results of two design methods

<table>
<thead>
<tr>
<th></th>
<th>Combinational design</th>
<th>Sequential design</th>
</tr>
</thead>
<tbody>
<tr>
<td>N (Degree of LFSR)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>VHDL code size (lines)</td>
<td>900</td>
<td>50</td>
</tr>
<tr>
<td>Design size (Logic Cell)</td>
<td>5,700</td>
<td>120</td>
</tr>
<tr>
<td>Clock (Mhz)</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Date rate in Cyclone 6000T (Mbps)</td>
<td>192–256</td>
<td>16–24</td>
</tr>
</tbody>
</table>

4 Conclusions and Future Work

We transformed the shrinking key generator for N=16 to a composite of four 4x4 pushing logics and six 4x4 through logics and targeted it to an FPGA. The resulting design of the parallel computation structure using two pipelining stages runs at 192–256 Mbps. Part of the reason for executing this design is to determine the performance improvement gained from transform method of optimizations to the design. We intend to use this information to drive design automation software development. In this design we are able to improve performance by more than a factor of twelve by applying a transform from the sequential computing algorithm to parallel computing and by inserting the pipelining stage as shown in Fig. 8. An observation of the delays in Fig. 8, making pipelining registers inserted, shows that most of the delay in combinational implementations is due to interconnect routing.

As we recognize that as N (degree of LFSR) increases more than 16, fan-outs of the through logic element to next stage increase by number of 10. In case of FPGA implementation for N>16, fan-out problem requires pipelining registers inserted every adjunctive stage, degrading the overall speed by reciprocal of number of pipelining registers. Moreover in case of ASIC implementation for N >16, in addition to speed degradation fan-out problem makes place & route so complicated that the design can not be synthesized even if timing simulation result shows appropriateness for ASIC implementation. The next step in this investigation is to apply manual scheme or plot of floor planning and placement to reduce interconnect delay in ASIC implementation. We are also interested in
implementing additional key generator algorithms, with the intent that a system would load the algorithm of choice into the FPGA as needed.

References


