Editorial

Network Attacks and Defense Systems

Prof Wanlei Zhou\(^1\), Yang Xiang\(^2\) and Minyi Guo\(^3\)

\(^1\)Deakin University, Australia. E-mail: wanlei@deakin.edu.au
\(^2\)Central Queensland University, Australia. E-mail: y.xiang@cqu.edu.au
\(^3\)The University of Aizu, Japan. E-mail: minyi@u-aizu.ac.jp

In recent years, there has been significant increase in attacks via wired, wireless and optical transmission platforms, such as DDoS, viruses, worms, spyware, and malware, etc, causing huge economical and social damage. While the network attack systems have become more easy-to-use, sophisticated, and powerful, interest has greatly increased in the field of building more effective, intelligent, and active defense systems which are distributed and networked. Today’s network defense systems face significant challenges to provide protection to networks and hosts. We focus on the theme of “Network Attacks and Defense Systems” in this special issue for International Journal of Computer Systems Science and Engineering. It covers the aspects of authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability issues in network attacks and defense systems.

In view of this, the 2007 International Workshop on Network and System Security (NSS 2007) provided a leading edge forum for researchers and industry developers in network and system security communities to exchange ideas and establish professional relationships. NSS 2007 received 80 submissions from 9 countries in America, Europe, Oceania, and Asia. 35 regular and short papers were accepted in the workshop proceedings. For this special issue, we only selected the best 3 papers from the large number of submissions. We also received another 11 submissions from the special issue call-for-papers. We selected 5 out of them into this special issue. All the papers were selected on the basis of their originality, technical quality and significance. Each paper was under rigorous technical review by at least 2 international reviewers. These 8 papers present the cutting edge research results in network attacks and defense systems.

In the first paper, Vo and Kim present a secure mutual authentication scheme with key agreement using smart card from bilinear pairings. Remote authentication is an important mechanism to control user access to remote systems nowadays. Many remote authentication schemes are not secure under the proposed impersonation attacks in which any adversary can be authenticated successfully with probability 1 at no extra cost. The proposed solution by the authors is secure and more efficient in terms of computational complexity than the previous schemes.

Distributed denial of service (DDoS) attacks are one of the complex problems in the current Internet. TCP SYN and Reflection DDoS attacks have some distinct features which make them even more difficult to deal. Tupakula and Varadharajan in the second paper present a hybrid model which comprises an enhanced automated model integrated with selected existing techniques to counteracting DDoS attacks. This model makes efficient usage of the advantages present in different techniques and minimizes their disadvantages. The evaluation results indicate the potential usefulness of the proposed model in counteracting DDoS attacks in practice.

In the third paper, Li et al. propose a cross-authentication model for heterogeneous domains in active networks. Currently there is coexistence of different authentication mechanisms in heterogeneous domains. Therefore this problem is challenging. The authors give the security proof of this cross-authentication model. The implementation which utilizes mutual entity authentication among heterogeneous domains based on PKI and ID-PKC demonstrates that the proposed system possesses the properties of high security and stability.

Intrusion detection has become a basic infrastructure to guarantee the security of most internetworking applications. It consumes huge computation power to process the information passing the network. In the fourth paper, Li et al. propose a new concept of variable-length signature, along with feature selection, to compress the behavior models of traditional intrusion
detection systems. It achieves high detection rates for known intrusions with significantly reduced false alarm rates.

In the fifth paper, Li et al. propose a request-driven role mapping framework for secure interoperation in multi-domain environments. To support flexible policy expression and inter-domain policy mapping, they present an effective method to perform the privilege query in general hybrid role hierarchies for special external requests based on the minimal unique set (MUS). This framework ensures the external user requests be satisfied and the local role hierarchies be furthest preserved.

In the sixth paper, Horng et al present their research work on intrusion detection systems from the viewpoint of improving true positive rate and eliminating false alarm rate. The proposed defense system is specifically used to protect web server. The core algorithm is based on smooth support vector machine (SSVM). It achieves high true positive rates, e.g., 99.40% for known attacks in the experiment, and true positive rates ranging from 65.13% to 97.33% for unknown or even novel attacks.

Zhu et al. in the seventh paper propose an efficient verifier-based client-to-client password-authenticated key exchange protocol that is resilient to server compromise. This protocol resists dictionary attacks mounted by either passive or active network intruders, allowing, in principle, even weak password phrases to be used safely. It also offers forward secrecy, which protects past sessions and passwords against future compromises.

In the last paper, Li et al present a security problem in anonymous routing protocol with authenticated key exchange in wireless ad hoc networks, from the point of view of attackers. We believe that only by fully understanding the attack mechanisms can we perform effective and comprehensive defense. After analyzing the vulnerability, the authors also provide a simple solution to it.

We sincerely hope that you will enjoy reading these 8 papers and find them very useful. We thank all the international reviewers for their professional services. We deeply thank Prof Tharam Dillon, the Editor-in-Chief of the International Journal of Computer Systems Science and Engineering for providing the opportunity to publish this special issue. Without his continuous support, encouragement and guidance throughout this publishing project, the success of this special issue is impossible.