

MAY 21-23, 2018 AT THE HYATT REGENCY, SAN FRANCISCO, CA

39th IEEE Symposium on Security and Privacy

Agenda

May 20

Registration and Reception

04:00PM – 07:00PM

May 21

Registration

07:00AM – 05:00PM

Breakfast

07:30AM – 08:20AM


Opening Remarks  (<https://youtu.be/bhU7bISrtrc>)

08:20AM – 08:40AM

Session #1: Machine Learning

08:40AM – 10:20AM

AI²: Safety and Robustness Certification of Neural Networks with Abstract Interpretation

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a948-abs.html>) (<https://youtu.be/LJnjCMV8KzA>)


Timon Gehr (ETH Zürich), Matthew Mirman (ETH Zürich), Dana Drachler Cohen (ETH Zürich), Petar Tsankov (ETH Zürich), Swarat Chaudhuri (Rice University), Martin Vechev (ETH Zürich)

Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a931-abs.html>) (<https://youtu.be/ahC4KPd9ISY>)

Matthew Jagielski (Northeastern University), Alina Oprea (Northeastern University), Battista Biggio (University of Cagliari, Italy; Pluribus One, Italy), Chang Liu (UC Berkeley), Cristina Nita-Rotaru (Northeastern University), Bo Li (UC Berkeley)

Stealing Hyperparameters in Machine Learning

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a629-abs.html>) (<https://youtu.be/rpRVqfjW0AA>)

Binghui Wang (ECE Department, Iowa State University), Neil Zhenqiang Gong (ECE Department, Iowa State University)

A Machine Learning Approach To Prevent Malicious Calls Over Telephony Networks

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a561-abs.html>) 

(<https://youtu.be/97TrCZ4egUc>)

Huichen Li (Shanghai Jiao Tong University), Xiaojun Xu (Shanghai Jiao Tong University), Chang Liu (University of California, Berkeley), Teng Ren (TouchPal Inc.), Kun Wu (TouchPal Inc.), Xuezhi Cao (Shanghai Jiao Tong University), Weinan Zhang (Shanghai Jiao Tong University), Yong Yu (Shanghai Jiao Tong University), Dawn Song (University of California, Berkeley)

Surveyance: Automatically Detecting Online Survey Scams

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a723-abs.html>) 

(<https://youtu.be/JrkqrzgXeko>)

Amin Kharraz (University of Illinois Urbana-Champaign), William Robertson (Northeastern University), Engin Kirda (Northeastern University)

Session Chair: Tudor Dumitras

Break (30 Minutes)

10:20AM – 10:50AM

Session #2: Privacy

10:50AM – 12:30PM

Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a221-abs.html>) 

(<https://youtu.be/Lp-lwYvxGpk>)

Giridhari Venkatadri (Northeastern University), Athanasios Andreou (EURECOM), Yabing Liu (Northeastern University), Alan Mislove (Northeastern University), Krishna P. Gummadi (MPI-SWS), Patrick Loiseau (Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG and MPI-SWS), Oana Goga (Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG)

Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency --- Choose Two

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a170-abs.html>) 

(<https://youtu.be/y89Bh5OfME>)

Debajyoti Das (Purdue University), Sebastian Meiser (University College London), Esfandiar Mohammadi (ETH Zurich), Aniket Kate (Purdue University)


Locally Differentially Private Frequent Itemset Mining

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a578-abs.html>) 

(https://youtu.be/-0uF_kXxyeE)

Tianhao Wang (Purdue University), Ninghui Li (Purdue University), Somesh Jha (University of Wisconsin-Madison)

EyeTell: Video-Assisted Touchscreen Keystroke Inference from Eye Movements

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a253-abs.html>) 

(<https://youtu.be/qFPZQ0t3-GM>)

Yimin Chen (Arizona State University), Tao Li (Arizona State University), Rui Zhang (University of Delaware), Yanchao Zhang (Arizona State University), Terri Hedgpeth (Arizona State University)

Understanding Linux Malware

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a870-abs.html>) 

(<https://youtu.be/bTkVFqF9VAw>)

Emanuele Cozzi (Eurecom), Mariano Graziano (Cisco Systems, Inc.), Yanick Fratantonio (Eurecom), Davide Balzarotti (Eurecom)

Session Chair: Carmela Troncoso

Lunch

12:30PM – 01:30PM

Session #3: Side Channels

01:30PM – 03:10PM

Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a388-abs.html>) 

(<https://youtu.be/uZIC1y76L4w>)

Guoxing Chen (The Ohio State University), Wenhao Wang (Indiana University Bloomington & SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences), Tianyu Chen (Indiana University Bloomington), Sanchuan Chen (The Ohio State University), Yinqian Zhang (The Ohio State University), XiaoFeng Wang (Indiana University Bloomington), Ten-Hwang Lai (The Ohio State University), Dongdai Lin (SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences)

Grand Pwning Unit: Accelerating Microarchitectural Attacks with the GPU

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a357-abs.html>) 

(<https://youtu.be/HdMLcdhIFes>)

Pietro Frigo (Vrije Universiteit Amsterdam), Kaveh Razavi (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam)


SoK: Keylogging Side Channels

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a420-abs.html>) 

(<https://youtu.be/1vwGx7PpF-8>)

John Monaco (U.S. Army Research Laboratory)

FPGA-Based Remote Power Side-Channel Attacks

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a805-abs.html>) 

(<https://youtu.be/-NVm1yei4hY>)

Mark Zhao (Cornell University), G. Edward Suh (Cornell University)

Another Flip in the Wall of Rowhammer Defenses

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a489-abs.html>) 

(https://youtu.be/_JPhsqJzV5I)

Daniel Gruss (Graz University of Technology, Graz, Austria), Moritz Lipp (Graz University of Technology, Graz, Austria), Michael Schwarz (Graz University of Technology, Graz, Austria), Daniel Genkin (University of Pennsylvania and University of Maryland, USA), Jonas Juffinger (Graz University of Technology, Graz, Austria), Sioli O'Connell (University of Adelaide, Adelaide, Australia), Wolfgang Schoecl (Graz University of Technology, Graz, Austria), Yuval Yarom (University of Adelaide and Data61, Adelaide, Australia)

Session Chair: Kevin Fu

Break (30 Minutes)

03:10PM – 03:40PM

Session #4: Computing on Hidden Data

03:40PM – 05:40PM

EnclaveDB: A Secure Database using SGX

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a405-abs.html>) 

(<https://youtu.be/haxFgPLPQ-8>)

Christian Priebe (Imperial College London), Kapil Vaswani (Microsoft Research), Manuel Costa (Microsoft Research)

Oblix: An Efficient Oblivious Search Index

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a740-abs.html>) 

(<https://youtu.be/laORiYIn68c>)

Pratyush Mishra (UC Berkeley), Rishabh Poddar (UC Berkeley), Jerry Chen (UC Berkeley), Alessandro Chiesa (UC Berkeley), Raluca Ada Popa (UC Berkeley)


Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a001-abs.html>) 

(<https://youtu.be/uM1-IPr7sb8>)

Marie-Sarah Lacharite (Royal Holloway, University of London), Brice Minaud (Royal Holloway, University of London), Kenneth G. Paterson (Royal Holloway, University of London)

Bulletproofs: Short Proofs for Confidential Transactions and More

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a319-abs.html>) 

(https://youtu.be/Adrh6BCc_Ao)

Benedikt Bünz (Stanford University), Jonathan Bootle (University College London), Dan Boneh (Stanford University), Andrew Poelstra (Blockstream), Pieter Wuille (Blockstream), Greg Maxwell

FuturesMEX: Secure, Distributed Futures Market Exchange

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a453-abs.html>) 

(<https://youtu.be/cOGgB9GdPT0>)

Fabio Massacci (University of Trento, IT), Chan Nam Ngo (University of Trento, IT), Jing Nie (University of International Business and Economics Beijing, CN), Daniele Venturi (University of Rome "La Sapienza", IT), Julian Williams (University of Durham, UK)

Implementing Conjunction Obfuscation under Entropic Ring LWE

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a068-abs.html>) 

(<https://youtu.be/ODLNfw2pGs8>)

David Bruce Cousins (Raytheon BBN Technologies), Giovanni Di Crescenzo (Applied Communication Sciences / Vencore Labs), Kamil Doruk Gür (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Kevin King (Massachusetts Institute of Technology), Yuriy Polyakov (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Kurt Rohloff (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Gerard W. Ryan (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Erkey Savaş (NJIT Cybersecurity Research Center, New Jersey Institute of Technology)

Session Chair: Yinqian Zhang

Poster Reception

06:00PM – 08:00PM

May 22

Registration

07:00AM – 05:00PM

Breakfast

07:30AM – 08:20AM


Awards

08:20AM – 08:40AM

Session #5: Understanding Users


08:40AM – 10:20AM

Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a134-abs.html>) 
(https://youtu.be/9fL_pcZTP7U)


Daniel Votipka (University of Maryland), Rock Stevens (University of Maryland), Elissa Redmiles (University of Maryland), Jeremy Hu (University of Maryland), Michelle Mazurek (University of Maryland)

Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a807-abs.html>) 
(<https://youtu.be/9YluZQXMU3E>)


Kiron Lebeck (University of Washington), Kimberly Ruth (University of Washington), Tadayoshi Kohno (University of Washington), Franziska Roesner (University of Washington)

Computer Security and Privacy for Refugees in the United States

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a373-abs.html>) 
(<https://youtu.be/T3r2ybV9Rsw>)


Lucy Simko (University of Washington), Ada Lerner (Wellesley College), Samia Ibtasam (University of Washington), Franziska Roesner (University of Washington), Tadayoshi Kohno (University of Washington)

On Enforcing the Digital Immunity of a Large Humanitarian Organization

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a302-abs.html>) 
(<https://youtu.be/mn-42zZxT2o>)

Stevens Le Blond (École Polytechnique Fédérale de Lausanne), Alejandro Cuevas (École Polytechnique Fédérale de Lausanne), Juan Ramón Troncoso-Pastoriza (École Polytechnique Fédérale de Lausanne), Philipp Jovanovic (École Polytechnique Fédérale de Lausanne), Bryan Ford (École Polytechnique Fédérale de Lausanne), Jean-Pierre Hubaux (École Polytechnique Fédérale de Lausanne)

The Spyware Used in Intimate Partner Violence

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a993-abs.html>) 

(<https://youtu.be/CEglyiG015A>)

Rahul Chatterjee (Cornell Tech), Periwinkle Doerfler (NYU), Hadas Orgad (Technion), Sam Havron (Cornell Univ), Jackeline Palmer (Hunter College), Diana Freed (Cornell Tech), Karen Levy (Cornell Tech), Nicola Dell (Cornell Tech), Damon McCoy (NYU), Thomas Ristenpart (Cornell Tech)

Session Chair: Sascha Fahl

Break (30 Minutes)

10:20AM – 10:50AM

Session #6: Programming Languages

10:50AM – 12:30PM

Compiler-assisted Code Randomization

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a472-abs.html>) 

(<https://youtu.be/xIAeyLJ0hKw>)

Hyungjoon Koo (Stony Brook University), Yaohui Chen (Northeastern University), Long Lu (Northeastern University), Vasileios P. Kemerlis (Brown University), Michalis Polychronakis (Stony Brook University)

Protecting the Stack with Metadata Policies and Tagged Hardware

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301b072-abs.html>) 

(<https://youtu.be/tR4YphteHTM>)

Nick Roessler (University of Pennsylvania), Andre DeHon (University of Pennsylvania)

Impossibility of Precise and Sound Termination-Sensitive Security Enforcements

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a787-abs.html>) 

(<https://youtu.be/C7oUCuMFZHw>)

Minh Ngo (INRIA, France), Frank Piessens (imec-DistriNet, KU Leuven, Belgium), Tamara Rezk (INRIA, France)

Static Evaluation of Noninterference using Approximate Model Counting

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a885-abs.html>) 

(<https://youtu.be/w3DZO7VS5j4>)

Ziqiao Zhou (University of North Carolina at Chapel Hill), Zhiyun Qian (University of California, Riverside), Michael K. Reiter (University of North Carolina at Chapel Hill), Yinqian Zhang (The Ohio State University)

DEEPSEC: Deciding Equivalence Properties in Security Protocols -- Theory and Practice

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a525-abs.html>) 

(<https://youtu.be/vPLLYj0pPWk>)

Vincent Cheval (Inria Nancy & Loria), Steve Kremer (Inria Nancy & Loria), Itsaka Rakotonirina (Inria Nancy & Loria)

Session Chair: Deian Stefan

Lunch

12:30PM – 01:30PM

Session #7: Networked Systems

01:30PM – 03:10PM

Distance-Bounding Protocols: Verification without Time and Location

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a152-abs.html>) 

(<https://youtu.be/nNHhhboCwa8>)

Sjouke Mauw (CSC/SnT, University of Luxembourg), Zach Smith (CSC, University of Luxembourg), Jorge Toro-Pozo (CSC, University of Luxembourg), Rolando Trujillo-Rasua (SnT, University of Luxembourg)


Sonar: Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a086-abs.html>) 

(https://youtu.be/JKi_0mRrDIY)

Christian Peeters (University of Florida), Hadi Abdullah (University of Florida), Nolen Scaife (University of Florida), Jasmine Bowers (University of Florida), Patrick Traynor (University of Florida), Bradley Reaves (North Carolina State University), Kevin Butler (University of Florida)


OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a019-abs.html>) 

(<https://youtu.be/f1pyaAZ7bj0>)

Eleftherios Kokoris-Kogias (École Polytechnique Fédérale de Lausanne), Philipp Jovanovic (École Polytechnique Fédérale de Lausanne), Linus Gasser (École Polytechnique Fédérale de Lausanne), Nicolas Gailly (École Polytechnique Fédérale de Lausanne), Ewa Syta (Trinity College), Bryan Ford (École Polytechnique Fédérale de Lausanne)

Routing Around Congestion: Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a506-abs.html>)  (<https://youtu.be/yl31rFy9bdU>)

Jared M Smith (University of Tennessee, Knoxville), Max Schuchard (University of Tennessee, Knoxville)

Tracking Ransomware End-to-end

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a773-abs.html>) 

(<https://youtu.be/H5bPmzsVLF8>)  (errata/errata-22-3.pdf)

Danny Yuxing Huang (Princeton University), Maxwell Matthaios Aliapoulos (New York University), Vector Guo Li (University of California, San Diego), Luca Invernizzi (Google), Elie Bursztein (Google), Kylie McRoberts (Google), Jonathan Levin (Chainalysis), Kirill Levchenko (University of California, San Diego), Alex C. Snoeren (University of California, San Diego), Damon McCoy (New York University)

Session Chair: Cristina Nita-Rotaru

Break (20 Minutes)

03:10PM – 03:30PM

Session #8: Program Analysis


03:30PM – 05:30PM

The Rise of the Citizen Developer: Assessing the Security Impact of Online App Generators

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a102-abs.html>) 


(<https://youtu.be/a7obdwkcOn4>)

Marten Oltrogge (CISPA, Saarland University), Erik Derr (CISPA, Saarland University), Christian Stransky (CISPA, Saarland University), Yasemin Acar (Leibniz University Hannover), Sascha Fahl (Leibniz University Hannover), Christian Rossow (CISPA, Saarland University), Giancarlo Pellegrino (CISPA, Saarland University, Stanford University), Sven Bugiel (CISPA, Saarland University), Michael Backes (CISPA, Saarland University)

Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a240-abs.html>)  (<https://youtu.be/1PqB3OFDEsA>)

Yuqi Chen (Singapore University of Technology and Design), Christopher M. Poskitt (Singapore University of Technology and Design), Jun Sun (Singapore University of Technology and Design)

Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a270-abs.html>)  (<https://youtu.be/B1JEE84f8G0>)


Meng Xu (Georgia Institute of Technology), Chenxiong Qian (Georgia Institute of Technology), Kangjie Lu (University of Minnesota), Michael Backes (CISPA Helmholtz Center i.G.), Taesoo Kim (Georgia Institute of Technology)

CollAFL: Path Sensitive Fuzzing

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a660-abs.html>)


Shuitao Gan (State Key Laboratory of Mathematical Engineering and Advanced Computing), Chao Zhang (Tsinghua University), Xiaojun Qin (State Key Laboratory of Mathematical Engineering and Advanced Computing), Xuwen Tu (State Key Laboratory of Mathematical Engineering and Advanced Computing), Kang Li (Cyber Immunity Lab), Zhongyu Pei (Tsinghua University), Zuoning Chen (National Research Center of Parallel Computer Engineering and Technology)

T-Fuzz: fuzzing by program transformation

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a917-abs.html>)  (<https://youtu.be/wjvjST0FLhg>)

Hui Peng (Purdue University), Yan Shoshitaishvili (Arizona State University), Mathias Payer (Purdue University)

Angora: Efficient Fuzzing by Principled Search

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a758-abs.html>)  (<https://youtu.be/S4VChMYzpgc>)

Peng Chen (ShanghaiTech University), Hao Chen (University of California, Davis)

Session Chair: Thorsten Holz

Break (10 Minutes)

05:30PM – 05:40PM

Short Talks

05:40PM – 06:40PM

Digital Forensics, Digital Futures - SADFE 2018

Michael Losavio (University of Louisville), Glenn Dardick (Embry-Riddle Aeronautic University), Abe Baggili (University of New Haven)

Droplet: Decentralized Authorization for IoT Data Streams

Hossein Shafagh (ETH Zurich)

Efficiently Authenticated Data Storage with Blockchain

Yuzhe (Richard) Tang, Zihao Xing, Ju Chen (Syracuse University)m Cheng Xu, Jianliang Xu (HKBU)

Encouraging Diversity in Security and Privacy Research and a report on GREPSEC: A Workshop for Women in Computer Security Research

Terry Benzel (University of Southern California - ISI), Hilarie Orman (Purple Streak)

IEEE SecDev 2018

Rob Cunningham, Dinara Doyle, Daphne Yao

Impact Analysis of Vulnerabilities on Business Processes in a Cloud Environment

Anoop Singhal (NIST), Peng Liu (Penn State University)

Kangacrypt 2018

Yuval Yarom (University of Adelaide and Data61)

Let "The Hulk" Protect Your Personal Information

Nicholas Micallef, Gaurav Misra (University of New South Wales)

Processing Publicly Disclosed Personal Data According to the GDPR - A Nole in the Privacy Regulation Framework

Gianluigi Maria Riva (University College Dublin)

Towards Image Privacy against Automated Classifiers

Arezoo Rajabi, Rakesh B. Bobba (Oregon State University)

seL4-US Center of Excellence Grand Opening

Jason Li (Intelligent Automation Inc)

S&P TC Business Meeting

06:40PM – 07:40PM

May 23

Registration

07:00AM – 06:00PM

Breakfast

07:30AM – 08:20AM

Closing Remarks

08:20AM – 08:30AM

Session #9: Web


08:30AM – 10:30AM

FP-STALKER: Tracking Browser Fingerprint Evolutions Along Time

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a054-abs.html>)

Antoine Vastel (University of Lille / INRIA), Pierre Laperdrix (INSA / INRIA), Walter Rudametkin (University of Lille / INRIA), Romain Rouvoy (University of Lille / INRIA)

Study and Mitigation of Origin Stripping Vulnerabilities in Hybrid-postMessage Enabled

Mobile Applications (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a709-abs.html>)  (https://youtu.be/F9g_3giFnFo)

Guangliang Yang (Texas A&M; University), Jeff Huang (Texas A&M; University), Guofei Gu (Texas A&M; University), Abner Mendoza (Texas A&M; University)

Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies &

Vulnerabilities (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a646-abs.html>)

 (<https://youtu.be/13oh2W9pZ-E>)

Abner Mendoza (Texas A&M; University), Guofei Gu (Texas A&M; University)

Enumerating Active IPv6 Hosts for Large-scale Security Scans via DNSSEC-signed Reverse

Zones (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a438-abs.html>) 

(<https://youtu.be/YpaaZla7hV8>)

Kevin Borgolte (University of California, Santa Barbara), Shuang Hao (University of Texas at Dallas), Tobias Fiebig (Delft University of Technology), Giovanni Vigna (University of California, Santa Barbara)


Tracking Certificate Misissuance in the Wild

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a288-abs.html>) 

(<https://youtu.be/INBoEDUbri0>)

Deepak Kumar (University of Illinois, Urbana-Champaign), Zhengping Wang (University of Illinois, Urbana-Champaign), Matthew Hyder (University of Illinois, Urbana-Champaign), Joseph Dickinson (University of Illinois, Urbana-Champaign), Gabrielle Beck (University of Michigan), David Adrian (University of Michigan), Joshua Mason (University of Illinois, Urbana-Champaign), Zakir Durumeric (University of Michigan), J. Alex Halderman (University of Michigan), Michael Bailey (University of Illinois, Urbana-Champaign)

A Formal Treatment of Accountable Proxying over TLS

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a339-abs.html>) 

(<https://youtu.be/Q60JBECPLyk>)

Karthikeyan Bhargavan (INRIA de Paris, France), Ioana Boureanu (Univ. of Surrey, SCCS, UK), Antoine Delignat-Lavaud (Microsoft Research, UK), Pierre-Alain Fouque (Univ. of Rennes 1, IRISA, France), Cristina Onete (Univ. of Limoges, XLIM, CNRS, France)

Session Chair: Nikita Borisov

Break (20 Minutes)

10:30AM – 10:50AM

Session #10: Authentication

10:50AM – 12:30PM

Secure Device Bootstrapping without Secrets Resistant to Signal Manipulation Attacks

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a900-abs.html>) 

(<https://youtu.be/62ctwRfAPuk>)

Nirnimesh Ghose (University of Arizona), Loukas Lazos (University of Arizona), Ming Li (University of Arizona)

Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing using Different Sensor Types (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a678-abs.html>) 

(<https://youtu.be/qolka5JiC04>)

Jun Han (Carnegie Mellon University), Albert Jin Chung (Carnegie Mellon University), Manal Kumar Sinha (Carnegie Mellon University), Madhumitha Harishankar (Carnegie Mellon University), Shijia Pan (Carnegie Mellon University), Hae Young Noh (Carnegie Mellon University), Pei Zhang (Carnegie Mellon University), Patrick Tague (Carnegie Mellon University)

On the Economics of Offline Password Cracking

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a035-abs.html>) 

(<https://youtu.be/lVezbhinKIU>)

Jeremiah Blocki (Purdue University), Benjamin Harsha (Purdue University), Samson Zhou (Purdue University)

A Tale of Two Studies: The Best and Worst of YubiKey Usability

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301b090-abs.html>) 

(<https://youtu.be/ugD-YxDuSX8>)

Joshua Reynolds (University of Illinois at Urbana-Champaign), Trevor Smith (Brigham Young University), Ken Reese (Brigham Young University), Luke Dickinson (Brigham Young University), Scott Ruoti (MIT Lincoln Laboratory), Kent Seamons (Brigham Young University)

When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts (<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a853-abs.html>) 

(<https://youtu.be/O6TGK2wIHi4>)

Simon Eberz (University of Oxford), Giulio Lovisotto (University of Oxford), Andrea Patanè (University of Oxford), Marta Kwiatkowska (University of Oxford), Vincent Lenders (armasuisse), Ivan Martinovic (University of Oxford)

Session Chair: Gang Tan


Lunch

12:30PM – 01:30PM

Session #11: Cryptography

01:30PM – 03:10PM

vRAM: Faster Verifiable RAM With Program-Independent Preprocessing

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a203-abs.html>) 

(<https://youtu.be/dFZbAHMmgqk>)

Yupeng Zhang (University of Maryland), Daniel Genkin (University of Maryland and University of Pennsylvania), Jonathan Katz (University of Maryland), Dimitrios Papadopoulos (Hong Kong University of Science and Technology), Charalampos Papamanthou (University of Maryland)

Doubly-efficient zkSNARKs without trusted setup

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a975-abs.html>) 

(<https://youtu.be/yq2AfLIMww0>)

Riad S. Wahby (Stanford), Ioanna Tzialla (New York University), Abhi Shelat (Northeastern), Justin Thaler (Georgetown), Michael Walfish (New York University)


xJsark: A Framework for Efficient Verifiable Computation

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301b011-abs.html>) 

(<https://youtu.be/GruzWxGejDM>)

Ahmed Kosba (University of Maryland), Charalampos Papamanthou (University of Maryland), Elaine Shi (Cornell University)

PIR with Compressed Queries and Amortized Query Processing

(<https://www.computer.org/csdl/proceedings/sp/2018/4353/00/435301b011-abs.html>) 

(<https://youtu.be/OWR7Q5BTY14>)

Sebastian Angel (UT Austin and NYU), Hao Chen (Microsoft Research), Kim Laine (Microsoft Research), Srinath Setty (Microsoft Research)

Secure Two-party Threshold ECDSA from ECDSA Assumptions

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a595-abs.html>)

Jack Doerner (Northeastern University), Yashvanth Kondi (Northeastern University), Eysa Lee (Northeastern University), abhi shelat (Northeastern University)

Session Chair: David Evans

Break (30 Minutes)

03:10PM – 03:40PM

Session #12: Devices

03:40PM – 05:20PM

Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a116-abs.html>) 

(<https://youtu.be/f86Oe-ylkK8>)

S Abhishek Anand (University of Alabama at Birmingham), Nitesh Saxena (University of Alabama at Birmingham)

Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a189-abs.html>) 

(<https://youtu.be/tsrOKeLeLc>)

Kai Jansen (Ruhr-University Bochum), Matthias Schäfer (University of Kaiserslautern), Daniel Moser (ETH Zurich), Vincent Lenders (armasuisse), Christina Pöpper (New York University Abu Dhabi), Jens Schmitt (University of Kaiserslautern)

SoK: "Plug & Pray" Today - Understanding USB Insecurity in Versions 1 through C

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a613-abs.html>) 

(https://youtu.be/PYFo366_4u0)

Jing Tian (University of Florida), Nolen Scaife (University of Florida), Deepak Kumar (University of Illinois at Urbana-Champaign), Michael Bailey (University of Illinois at Urbana-Champaign), Adam Bates (University of Illinois at Urbana-Champaign), Kevin Butler (University of Florida)

Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a821-abs.html>) 

(<https://youtu.be/v0yh9fG00zo>)

Connor Bolton (University of Michigan), Sara Rampazzi (University of Michigan), Chaohao Li (Zhejiang University), Andrew Kwong (University of Michigan), Wenyuan Xu (Zhejiang University), Kevin Fu (University of Michigan)

The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter

(<https://csdl.computer.org/csdl/proceedings/sp/2018/4353/00/435301a695-abs.html>) 

(<https://youtu.be/OzUy5Plv7pg>)

Nolen Scaife (University of Florida), Christian Peeters (University of Florida), Camilo Velez (University of Florida), Hanqing Zhao (University of Florida), Patrick Traynor (University of Florida), David Arnold (University of Florida)

Session Chair: Matthew Hicks

NITRD Panel: ML/AI and Cybersecurity

05:40PM – 07:40PM

Machine Learning has become an indispensable technology that allows us to extract insights from vast quantities of data in many industries and applications. Advances in areas such as perception, language recognition, medical diagnosis, or self-driving have been spectacular. In security, ML has been instrumental in identifying threats, attacks, and abnormal activities. However, ML algorithms have not been designed to operate in the presence of adversaries. Furthermore, securing and defending ML systems is very hard because we lack theoretical tools for developing principled ML defenses. Can ML/AI give defenders the upper ground or are we consigned to another security whack-a-mole? Panelists will discuss Federal Government's research in ML/AI and cybersecurity and issues to drive further R&D.

Panelists:

Dr. Kenneth Calvert, Division Director, NSF/CISE

Dr. Ahmad Ridley, Senior Researcher, NSA

Ms. Sharothi Pikar, Associate Director for Cyber Strategies, OUSD(R&E), DoD

Moderator: Dr. Tomas Vagoun, National Coordination Office for NITRD

Symposium/Workshops Bridging Reception

06:00PM – 08:00PM

Speed Mentoring

07:00PM – 09:00PM

May 24

Workshops Breakfast

07:30AM – 08:30AM

Workshops Opening Remarks

08:45AM – 09:00AM

Workshops Session #1

09:00AM – 10:15AM

Workshops Break (30 Minutes)	10:15AM – 10:45AM
Workshops Session #2	10:45AM – 12:30PM
Workshops Lunch	12:30PM – 01:30PM
Workshops Session #3	01:30PM – 03:15PM
Workshops Break (30 Minutes)	03:15PM – 03:45PM
Workshops Session #4	03:45PM – 05:30PM
Workshops Closing Remarks	05:30PM – 05:45PM