Wednesday, August 10

Low-Level Attacks

Flip Feng Shui: Hammering a Needle in the Software Stack
Kaveh Razavi, Ben Gras, and Erik Bosman, Vrije Universiteit Amsterdam; Bart Preneel, Katholieke Universiteit Leuven; Cristiano Giuffrida and Herbert Bos, Vrije Universiteit Amsterdam

One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation
Yuan Xiao, Xiaokuan Zhang, Yinqian Zhang, and Radu Teodorescu, The Ohio State University

PIkit: A New Kernel-Independent Processor-Interconnect Rootkit
Wonjun Song, Hyunwoo Choi, Junhong Kim, Eunsoo Kim, Yongdae Kim, and John Kim, Korea Advanced Institute of Science and Technology (KAIST)

Verification and Timing

Verifying Constant-Time Implementations
José Bacelar Almeida, HASlab/INESC TEC and University of Minho; Manuel Barbosa, HASlab/INESC TEC and DCC FCUP; Gilles Barthe and François Dupressoir, IMDEA Software Institute; Michael Emmi, Bell Labs and Nokia

Secure, Precise, and Fast Floating-Point Operations on x86 Processors
Ashay Rane, Calvin Lin, and Mohit Tiwari, The University of Texas at Austin

ÜBERSPARK: Enforcing Verifiable Object Abstractions for Automated Compositional Security Analysis of a Hypervisor
Amit Vasudevan and Sagar Chaki, Carnegie Mellon University; Petros Maniatis, Google Inc.; Limin Jia and Anupam Datta, Carnegie Mellon University

Software Attacks

Undermining Information Hiding (and What to Do about It)
Enes Göktaş, Vrije Universiteit Amsterdam; Robert Gawlik and Benjamin Kollenda, Ruhr Universität Bochum; Elias Athanasopoulos, Vrije Universiteit Amsterdam; Georgios Portokalidis, Stevens Institute of Technology; Cristiano Giuffrida and Herbert Bos, Vrije Universiteit Amsterdam

Poking Holes in Information Hiding
Angelos Oikonomopoulos, Elias Athanasopoulos, Herbert Bos, and Cristiano Giuffrida, Vrije Universiteit Amsterdam

What Cannot Be Read, Cannot Be Leveraged? Revisiting Assumptions of JIT-ROP Defenses
Giorgi Maisuradze, Michael Backes, and Christian Rossow, Saarland University

Password and Key-Fingerprints

zxcvbn: Low-Budget Password Strength Estimation
Daniel Lowe Wheeler, Dropbox Inc.

Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks
William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor, Carnegie Mellon University
An Empirical Study of Textual Key-Fingerprint Representations .................................................. 193
Sergej Dechand, University of Bonn; Dominik Schürmann, Technische Universität Braunschweig; Karoline Busse, University of Bonn; Yasemin Acar and Sascha Fahl, Saarland University; Matthew Smith, University of Bonn

Network Security
Off-Path TCP Exploits: Global Rate Limit Considered Dangerous .................................................. 209
Yue Cao, Zhiyun Qian, Zhongjie Wang, Tuan Dao, and Srikanth V. Krishnamurthy, University of California, Riverside; Lisa M. Marvel, United States Army Research Laboratory

Website-Targeted False Content Injection by Network Operators .................................................. 227
Gabi Nakibly, Rafael—Advanced Defense Systems and Technion—Israel Institute of Technology; Jaime Schcolnik, Interdisciplinary Center Herzliya; Yossi Rubin, Rafael—Advanced Defense Systems

The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO .......... 245
Kun Du and Hao Yang, Tsinghua University; Zhou Li, IEEE Member; Haixin Duan, Tsinghua University; Kehuan Zhang, The Chinese University of Hong Kong

A Comprehensive Measurement Study of Domain Generating Malware .......................................... 263
Daniel Plohmann, Fraunhofer FKIE; Khaled Yakdan, University of Bonn; Michael Klatt, DomainTools; Johannes Bader; Elmar Gerhards-Padilla, Fraunhofer FKIE

Applied Cryptography
Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing ............... 279

Faster Malicious 2-Party Secure Computation with Online/Offline Dual Execution ............................ 297
Peter Rindal and Mike Rosulek, Oregon State University

Egalitarian Computing ...................................................................................................................... 315
Alex Biryukov and Dmitry Khovratovich, University of Luxembourg

Post-quantum Key Exchange—A New Hope ...................................................................................... 327
Erdem Alkim, Ege University; Léo Ducas, Centrum voor Wiskunde en Informatica; Thomas Pöppelmann, Infineon Technologies AG; Peter Schwabe, Radboud University

Thursday, August 11
Software Security
Automatically Detecting Error Handling Bugs Using Error Specifications ........................................ 345
Suman Jana and Yuan Kang, Columbia University; Samuel Roth, Ohio Northern University; Baishakhi Ray, University of Virginia

APISAN: Sanitizing API Usages through Semantic Cross-Checking .................................................. 363
Insu Yun, Changwoo Min, Xujie Si, Yeongjin Jang, Taesoo Kim, and Mayur Naik, Georgia Institute of Technology

On Omitting Commits and Committing Omissions: Preventing Git Metadata Tampering That
(Re)introduces Software Vulnerabilities .......................................................................................... 379
Santiago Torres-Arias, New York University; Anil Kumar Ammula and Reza Curtmola, New Jersey Institute of Technology; Justin Cappos, New York University

(Thursday, August 11, continues on next page)
Hardware I

Defending against Malicious Peripherals with Cinch ......................................................... 397
Sebastian Angel, The University of Texas at Austin and New York University; Riad S. Wahby, Stanford University; Max Howald, The Cooper Union and New York University; Joshua B. Leners, Two Sigma; Michael Spilo and Zhen Sun, New York University; Andrew J. Blumberg, The University of Texas at Austin; Michael Walfish, New York University

Making USB Great Again with USBFILTER ................................................................. 415
Dave (Jing) Tian and Nolen Scaife, University of Florida; Adam Bates, University of Illinois at Urbana–Champaign; Kevin R. B. Butler and Patrick Traynor, University of Florida

Micro-Virtualization Memory Tracing to Detect and Prevent Spraying Attacks .................. 431
Stefano Cristalli and Mattia Pagnozzi, University of Milan; Mariano Graziano, Cisco Systems Inc.; Andrea Lanzi, University of Milan; Davide Balzarotti, Eurecom

Web Security

Request and Conquer: Exposing Cross-Origin Resource Size ......................................... 447
Tom Van Goethem, Mathy Vanhoef, Frank Piessens, and Wouter Joosen, Katholieke Universiteit Leuven

Trusted Browsers for Uncertain Times ........................................................................... 463
David Kohlbrenner and Hovav Shacham, University of California, San Diego

Tracing Information Flows Between Ad Exchanges Using Retargeted Ads ......................... 481
Muhammad Ahmad Bashir, Sajjad Arshad, William Robertson, and Christo Wilson, Northeastern University

Cyber-Physical Systems

Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos .......... 497
Yi Xu, True Price, Jan-Michael Frahm, and Fabian Monrose, The University of North Carolina at Chapel Hill

Hidden Voice Commands .............................................................................................. 513
Nicholas Carlini and Pratyush Mishra, University of California, Berkeley; Tavish Vaidya, Yuankai Zhang, Micah Sherr, and Clay Shields, Georgetown University; David Wagner, University of California, Berkeley; Wenchao Zhou, Georgetown University

FlowFence: Practical Data Protection for Emerging IoT Application Frameworks ................ 531
Earlence Fernandes, Justin Paupore, and Amir Rahmati, University of Michigan; Daniel Simionato and Mauro Conti, University of Padova; Atul Prakash, University of Michigan

Low-Level Attacks and Defenses

ARMageddon: Cache Attacks on Mobile Devices ......................................................... 549
Moritz Lipp, Daniel Gruss, Raphael Spreitzer, Clémantine Maurice, and Stefan Mangard, Graz University of Technology

DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks ....................................... 565
Peter Pessl, Daniel Gruss, Clémantine Maurice, Michael Schwarz, and Stefan Mangard, Graz University of Technology

An In-Depth Analysis of Disassembly on Full-Scale x86/x64 Binaries ................................ 583
Dennis Andriesse, Xi Chen, and Victor van der Veen, Vrije Universiteit Amsterdam; Asia Slowinska, Lastline, Inc.; Herbert Bos, Vrije Universiteit Amsterdam

Machine Learning and Data Retrieval Systems

Stealing Machine Learning Models via Prediction APIs ................................................. 601
Florian Tramèr, École Polytechnique Fédérale de Lausanne (EPFL); Fan Zhang, Cornell University; Ari Juels, Cornell Tech; Michael K. Reiter, The University of North Carolina at Chapel Hill; Thomas Ristenpart, Cornell Tech
Oblivious Multi-Party Machine Learning on Trusted Processors .................................619
Olga Ohrimenko, Felix Schuster, and Cédric Fournet, Microsoft Research; Aastha Mehta, Microsoft Research and Max Planck Institute for Software Systems (MPI-SWS); Sebastian Nowozin, Kapil Vaswani, and Manuel Costa, Microsoft Research

Thoth: Comprehensive Policy Compliance in Data Retrieval Systems .........................637
Eslam Elnikety, Aastha Mehta, Anjo Vahldiek-Oberwagner, Deepak Garg, and Peter Druschel, Max Planck Institute for Software Systems (MPI-SWS)

Crypto Attacks

Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage ..................655
Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan, Johns Hopkins University

Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys ..................................673
Mathy Vanhoef and Frank Piessens, Katholieke Universiteit Leuven

DROWN: Breaking TLS using SSLv2 .................................................................689
Nimrod Aviram, Tel Aviv University; Sebastian Schinzel, Münster University of Applied Sciences; Juraj Somorovsky, Ruhr University Bochum; Nadia Heninger, University of Pennsylvania; Maik Dinkel, Münster University of Applied Sciences; Jens Steube, Hashcat Project; Luke Valenta, University of Pennsylvania; David Adrian and J. Alex Halderman, University of Michigan; Viktor Dukhovni, Two Sigma and OpenSSL; Emilia Käser, Google and OpenSSL; Shaanan Cohn, University of Pennsylvania; Susanne Engels and Christof Paar, Ruhr University Bochum; Yuval Shavitt, Tel Aviv University

All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption .............................707
Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou, University of Maryland

Malware

Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software ...............721

Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services ..................739
Platon Kotzias, IMDEA Software Institute and Universidad Politécnica de Madrid; Leyla Bilge, Symantec Research Labs; Juan Caballero, IMDEA Software Institute

UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware .............................757
Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda, Northeastern University

Towards Measuring and Mitigating Social Engineering Software Download Attacks ..................773
Terry Nelms, Georgia Institute of Technology and Damballa; Roberto Perdisci, University of Georgia and Georgia Institute of Technology; Manos Antonakakis, Georgia Institute of Technology; Mustaque Ahamad, Georgia Institute of Technology and New York University Abu Dhabi
Network Security II

Specification Mining for Intrusion Detection in Networked Control Systems .................................................. 791
Marco Caselli, University of Twente; Emmanuele Zambon, University of Twente and SecurityMatters B.V.;
Johanna Amann, International Computer Science Institute; Robin Sommer, International Computer Science
Institute and Lawrence Berkeley National Laboratory; Frank Kargl, Ulm University

Optimized Invariant Representation of Network Traffic for Detecting Unseen Malware Variants .......... 807
Karel Bartos and Michal Sofka, Cisco Systems, Inc.; Vojtech Franc, Czech Technical University in Prague

Authenticated Network Time Synchronization .................................................. 823
Benjamin Dowling, Queensland University of Technology; Douglas Stebila, McMaster University; Greg
Zaverucha, Microsoft Research

Hardware II

fTPM: A Software-Only Implementation of a TPM Chip .................................................. 841
Himanshu Raj, ContainerX; Stefan Saroiu, Alec Wolman, Ronald Aigner, Jeremiah Cox, Paul England, Chris
Fenner, Kinshuman Kinshumann, Jork Loeser, Dennis Mattoon, Magnus Nyström, David Robinson, Rob Spiger,
Stefan Thom, and David Wooten, Microsoft

Sanctum: Minimal Hardware Extensions for Strong Software Isolation .................................................. 857
Victor Costan, Illia Lebedev, and Srinivas Devadas, MIT CSAIL

Ariadne: A Minimal Approach to State Continuity .................................................. 875
Raoul Strackx and Frank Piessens, Katholieke Universiteit Leuven

Cyber-Physical Systems II

The Million-Key Question—Investigating the Origins of RSA Public Keys .................................................. 893
Petr Švenda, Matúš Nemec, Peter Sekan, Rudolf Kvašňovský, David Formánek, David Komárek, and Vashek
Matyáš, Masaryk University

Fingerprinting Electronic Control Units for Vehicle Intrusion Detection .................................................. 911
Kyong-Tak Cho and Kang G. Shin, University of Michigan

Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems .......... 929
Flavio D. Garcia and David Oswald, University of Birmingham; Timo Kasper, Kasper & Oswald GmbH; Pierre
Pavlídès, University of Birmingham

Distributed Systems

OBLIVP2P: An Oblivious Peer-to-Peer Content Sharing System .................................................. 945
Yaoqi Jia, National University of Singapore; Tarik Moataz, Colorado State University and Telecom Bretagne;
Shruti Tople and Prateek Saxena, National University of Singapore

AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels .......... 963
Bradley Reaves, Logan Blue, and Patrick Traynor, University of Florida

You Are Who You Know and How You Behave: Attribute Inference Attacks via Users’ Social Friends
and Behaviors .................................................. 979
Neil Zhenqiang Gong, Iowa State University; Bin Liu, Rutgers University

Web Measurements

Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking
from 1996 to 2016 .................................................. 997
Adam Lerner, Anna Kornfeld Simpson, Tadayoshi Kohno, and Franziska Roesner, University of Washington