2017 IEEE Symposium on Security and Privacy
SP 2017
Table of Contents

Message from the General Chair.................................................................xi
Message from the Program Committee Co-Chairs..................................xv
Organizing Committee.............................................................................xvi
Program Committee................................................................................xvii
External Reviewers..................................................................................xix

Session #1: Privacy and Learning
Membership Inference Attacks Against Machine Learning Models ........3
   Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov
SecureML: A System for Scalable Privacy-Preserving Machine Learning .....................19
   Payman Mohassel and Yupeng Zhang
Towards Evaluating the Robustness of Neural Networks ................................39
   Nicholas Carlini and David Wagner
Is Interaction Necessary for Distributed Private Learning? ..........................58
   Adam Smith, Abhradeep Thakurta, and Jalaj Upadhyay
Pyramid: Enhancing Selectivity in Big Data Protection with Count Featurization ..........78
   Mathias Lecuyer, Riley Spahn, Roxana Geambasu, Tzu-Kuo Huang, and Siddhartha Sen

Session #2: Getting Security Right
   Cormac Herley and P. C. van Oorschot
Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security ..............................................................................121
   Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl
Obstacles to the Adoption of Secure Communication Tools ..........................137
   Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith
Comparing the Usability of Cryptographic APIs ................................................................. 154
   Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim,
   Michelle L. Mazurek, and Christian Stransky

SoK: Cryptographically Protected Database Search .......................................................... 172
   Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen,
   Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell,
   and Robert K. Cunningham

Session #3: Attacks

IoT Goes Nuclear: Creating a ZigBee Chain Reaction ........................................................ 195
   Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O’Flynn

SoK: Exploiting Network Printers .................................................................................... 213
   Jens Müller, Vladislav Mladenov, Juraj Somorovsky, and Jörg Schwenk

How They Did It: An Analysis of Emission Defeat Devices in Modern
Automobiles ....................................................................................................................... 231
   Moritz Contag, Guo Li, Andre Pawlowski, Felix Domke, Kirill Levchenko,
   Thorsten Holz, and Stefan Savage

The Password Reset MitM Attack ...................................................................................... 251
   Nethanel Gelernter, Senia Kalma, Bar Magnezi, and Hen Porcilan

An Experimental Security Analysis of an Industrial Robot Controller ................................. 268
   Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi,
   Andrea Maria Zanchettin, and Stefano Zanero

Session #4: Systems Security and Authentication

Protecting Bare-Metal Embedded Systems with Privilege Overlays .................................. 289
   Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab,
   Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer

NORAX: Enabling Execute-Only Memory for COTS Binaries on AArch64 .......................... 304
   Yaozh Chen, Dongli Zhang, Ruowen Wang, Rui Qiao, Ahmed M. Azab,
   Long Lu, Hayawardh Vijayakumar, and Wenbo Shen

Securing Augmented Reality Output ................................................................................. 320
   Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner

SysPal: System-Guided Pattern Locks for Android ............................................................ 338
   Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song,
   and Hyoungshick Kim

Multi-touch Authentication Using Hand Geometry and Behavioral Information .................... 357
   Yunpeng Song, Zhongmin Cai, and Zhi-Li Zhang
Session #5: Bitcoin and Distributed Systems

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies .................................................................375
  Maria Apostolaki, Aviv Zohar, and Laurent Vanbever

Catena: Efficient Non-equivocation via Bitcoin .................................................................................393
  Alin Tomescu and Srinivas Devadas

IKP: Turning a PKI Around with Decentralized Automated Incentives ..........................................410
  Stephanos Matsumoto and Raphael M. Reischuk

Augur: Internet-Wide Detection of Connectivity Disruptions .........................................................427
  Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson

Scalable Bias-Resistant Distributed Randomness .............................................................................444
  Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly,
  Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford

Session #6: TLS Session Security

Implementing and Proving the TLS 1.3 Record Layer .........................................................................463
  Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss,
  Jonathan Protzenko, Aseem Rastogi, Nikhil Swamy,
  Santiago Zanella-Beguelin, Karthikeyan Bhargavan, Jianyang Pan,
  and Jean Karim Zinzindohoue

Verified Models and Reference Implementations for the TLS 1.3 Standard ........................................483
  Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi

SymCerts: Practical Symbolic Execution for Exposing Noncompliance in X.509 .........................503
  Sze Yiu Chau, Omar Chowdhury, Endadul Hoque, Huangyi Ge, Aniket Kate,
  Cristina Nita-Rotaru, and Ninghui Li

HVLearn: Automated Black-Box Analysis of Hostname Verification in SSL/TLS Implementations ........521
  Suphannee Sivakom, George Argyros, Kexin Pei, Angelos D. Keromytis,
  and Suman Jana

CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers .................................539
  James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove,
  and Christo Wilson
Session #7: Software Security

Finding and Preventing Bugs in JavaScript Bindings ...............................................................559
Fraser Brown, Shravan Narayan, Riad S. Wahby, Dawson Engler, Ranjit Jhala,
and Deian Stefan

Skyfire: Data-Driven Seed Generation for Fuzzing ...............................................................579
Junjie Wang, Bihuan Chen, Lei Wei, and Yang Liu

VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery .......................................595
Seulbae Kim, Seunghoon Woo, Heejo Lee, and Hakjoo Oh

NEZHA: Efficient Domain-Independent Differential Testing ..................................................615
Theofilos Petsios, Adrian Tang, Salvatore Stolfo, Angelos D. Keromytis,
and Suman Jana

Backward-Bounded DSE: Targeting Infeasibility Questions on Obfuscated Codes ................595
Sébastien Bardin, Robin David, and Jean-Yves Marion

Session #8: Information-Flow Channel Security

Leakage-Abuse Attacks against Order-Revealing Encryption ...............................................655
Paul Grubbs, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed,
and Thomas Ristenpart

Side-Channel Attacks on Shared Search Indexes ...................................................................673
Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash,
and Thomas Ristenpart

From Trash to Treasure: Timing-Sensitive Garbage Collection ..............................................693
Mathias V. Pedersen and Aslan Askarov

Verifying and Synthesizing Constant-Resource Implementations with Types .......................710
Van Chan Ngo, Mario Dehesa-Azuara, Matthew Fredrikson, and Jan Hoffmann

CoSMeDis: A Distributed Social Media Platform with Formally Verified Confidentiality Guarantees ..................................................................................................................729
Thomas Bauereiß, Armando Pesenti Gritti, Andrei Popescu, and Franco Raimondi

Session #9: Underground Economics

How to Learn Klingon without a Dictionary: Detection and Measurement of Black Keywords Used by the Underground Economy .......................................................751
Hao Yang, Xiulin Ma, Kun Du, Zhou Li, Haixin Duan, Xiaodong Su, Guang Liu,
Zhifeng Geng, and Jianping Wu

To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild .................................................................................................................................770
Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani,
Haikuo Yin, Stevens Le Blond, Damon McCoy, and Kirill Levchenko
A Lustrum of Malware Network Communication: Evolution and Insights .................................................788
Chaz Lever, Platon Kotzias, Davide Balzarotti, Juan Caballero, and Manos Antonakakis

Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks ....................................................................................805
Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, Xiaofeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy

Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits ..................................................824
Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, and David Brumley

Session #10: Cryptography

Optimized Honest-Majority MPC for Malicious Adversaries — Breaking the 1 Billion-Gate Per Second Barrier ..................................................................................................................843
Toshinori Araki, Assi Barak, Jun Furukawa, Tamar Lichter, Yehuda Lindell, Ariel Nof, Kazuma Ohara, Adi Watzman, and Or Weinstein

vSQL: Verifying Arbitrary SQL Queries over Dynamic Outsourced Databases .................................................863
Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou

A Framework for Universally Composable Diffie-Hellman Key Exchange .........................................................881
Ralf Küsters and Daniel Rausch

One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation ....................................................901
Jan Camenisch, Liqun Chen, Manu Drijvers, Anja Lehmann, David Novick, and Rainer Urian

Cryptographic Function Detection in Obfuscated Binaries via Bit-Precise Symbolic Loop Mapping .................................921
Dongpeng Xu, Jiang Ming, and Dinghao Wu

Session #11: Privacy

XHOUND: Quantifying the Fingerprintability of Browser Extensions .................................................................941
Oleksii Starov and Nick Nikiforakis

Identifying Personal DNA Methylation Profiles by Genotype Inference ..........................................................957
Michael Backes, Pascal Berrang, Matthias Bieg, Roland Eils, Carl Herrmann, Mathias Humbert, and Irina Lehmann

Counter-RAPTOR: Safeguarding Tor Against Active Routing Attacks ...............................................................977
Yixin Sun, Anne Edmundson, Nick Feamster, Mung Chiang, and Prateek Mittal

Machine-Checked Proofs of Privacy for Electronic Voting Protocols ..............................................................993
Véronique Cortier, Constantin Cătălin Drăgan, François Dupressoir, Benedikt Schmidt, Pierre-Yves Strub, and Bogdan Warinschi
Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts ..............................................................1009
Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis, and Michalis Polychronakis

Session #12: Authorization

Hardening Java’s Access Control by Abolishing Implicit Privilege Elevation ..................................................1027
Philipp Holzinger, Ben Hermann, Johannes Lerch, Eric Bodden, and Mira Mezini

Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop ........................................................1041
Yanick Fratantonio, Chenxiong Qian, Simon P. Chung, and Wenke Lee

SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices .....................................................1058
Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux

The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences ..................................................1077
Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov

IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks ..................................................1094
Paul Marinescu, Chad Parry, Marjori Pomarole, Yuan Tian, Patrick Tague, and Ioannis Papagiannis

Author Index