

**USENIX Security '19:**  
**28th USENIX Security Symposium**  
**August 14–16, 2019**  
**Santa Clara, CA, USA**

**Wireless Security**

<b>A Study of the Feasibility of Co-located App Attacks against BLE and a Large-Scale Analysis of the Current Application-Layer Security Landscape .....</b>	<b>1</b>
<i>Pallavi Sivakumaran and Jorge Blasco, Royal Holloway University of London</i>	
<b>The CrossPath Attack: Disrupting the SDN Control Channel via Shared Links .....</b>	<b>19</b>
<i>Jiahao Cao, Qi Li, and Renjie Xie, Tsinghua University; Kun Sun, George Mason University; Guofei Gu, Texas A&amp;M University; Mingwei Xu and Yuan Yang, Tsinghua University</i>	
<b>A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link .....</b>	<b>37</b>
<i>Milan Stute, Technische Universität Darmstadt; Sashank Narain, Northeastern University; Alex Mariotto, Alexander Heinrich, and David Kreitschmann, Technische Universität Darmstadt; Guevara Noubir, Northeastern University; Matthias Hollick, Technische Universität Darmstadt</i>	
<b>Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE .....</b>	<b>55</b>
<i>Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim, KAIST</i>	
<b>UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband .....</b>	<b>73</b>
<i>Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun, ETH Zurich</i>	

**Protecting Users Everywhere**

<b>Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors .....</b>	<b>89</b>
<i>Christine Chen, University of Washington; Nicola Dell, Cornell Tech; Franziska Roesner, University of Washington</i>	
<b>Clinical Computer Security for Victims of Intimate Partner Violence.....</b>	<b>105</b>
<i>Sam Havron, Diana Freed, and Rahul Chatterjee, Cornell Tech; Damon McCoy, New York University; Nicola Dell and Thomas Ristenpart, Cornell Tech</i>	
<b>Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA.....</b>	<b>123</b>
<i>Noah Athorpe, Sarah Varghese, and Nick Feamster, Princeton University</i>	
<b>Secure Multi-User Content Sharing for Augmented Reality Applications.....</b>	<b>141</b>
<i>Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner, University of Washington</i>	
<b>Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study .....</b>	<b>159</b>
<i>Eric Zeng and Franziska Roesner, University of Washington</i>	

**Hardware Security**

<b>PAC it up: Towards Pointer Integrity using ARM Pointer Authentication .....</b>	<b>177</b>
<i>Hans Liljestrand, Aalto University, Huawei Technologies Oy; Thomas Nyman, Aalto University; Kui Wang, Huawei Technologies Oy, Tampere University of Technology; Carlos Chinea Perez, Huawei Technologies Oy; Jan-Erik Ekberg, Huawei Technologies Oy, Aalto University; N. Asokan, Aalto University</i>	
<b>Origin-sensitive Control Flow Integrity .....</b>	<b>195</b>
<i>Mustakimur Rahman Khandaker, Wenqing Liu, Abu Naser, Zhi Wang, and Jie Yang, Florida State University</i>	

<b>HardFails: Insights into Software-Exploitable Hardware Bugs</b> .....	<b>213</b>
Ghada Dessouky and David Gens, <i>Technische Universität Darmstadt</i> ; Patrick Haney and Garrett Persyn, <i>Texas A&amp;M University</i> ; Arun Kanuparthi, Hareesh Khattri, and Jason M. Fung, <i>Intel Corporation</i> ; Ahmad-Reza Sadeghi, <i>Technische Universität Darmstadt</i> ; Jeyavijayan Rajendran, <i>Texas A&amp;M University</i>	

<b>uXOM: Efficient eXecute-Only Memory on ARM Cortex-M</b> .....	<b>231</b>
Donghyun Kwon, Jangseop Shin, and Giyeol Kim, <i>Seoul National University</i> ; Byoungyoung Lee, <i>Seoul National University</i> , <i>Purdue University</i> ; Yeongpil Cho, <i>Soongsil University</i> ; Yunheung Paek, <i>Seoul National University</i>	

<b>A Systematic Evaluation of Transient Execution Attacks and Defenses</b> .....	<b>249</b>
Claudio Canella, <i>Graz University of Technology</i> ; Jo Van Bulck, <i>imec-DistriNet, KU Leuven</i> ; Michael Schwarz, Moritz Lipp, Benjamin von Berg, and Philipp Ortner, <i>Graz University of Technology</i> ; Frank Piessens, <i>imec-DistriNet, KU Leuven</i> ; Dmitry Evtushkin, <i>College of William and Mary</i> ; Daniel Gruss, <i>Graz University of Technology</i>	

## Machine Learning Applications

<b>The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks.</b> .....	<b>267</b>
Nicholas Carlini, <i>Google Brain</i> ; Chang Liu, <i>University of California, Berkeley</i> ; Úlfar Erlingsson, <i>Google Brain</i> ; Jernej Kos, <i>National University of Singapore</i> ; Dawn Song, <i>University of California, Berkeley</i>	

<b>Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features</b> .....	<b>285</b>
Liang Tong, <i>Washington University in St. Louis</i> ; Bo Li, <i>UIUC</i> ; Chen Hajaj, <i>Ariel University</i> ; Chaowei Xiao, <i>University of Michigan</i> ; Ning Zhang and Yevgeniy Vorobeychik, <i>Washington University in St. Louis</i>	

<b>ALOHA: Auxiliary Loss Optimization for Hypothesis Augmentation</b> .....	<b>303</b>
Ethan M. Rudd, Felipe N. Ducau, Cody Wild, Konstantin Berlin, and Richard Harang, <i>Sophos</i>	

<b>Why Do Adversarial Attacks Transfer? Explaining Transferability of Evasion and Poisoning Attacks</b> .....	<b>321</b>
Ambra Demontis, Marco Melis, and Maura Pintor, <i>University of Cagliari, Italy</i> ; Matthew Jagielski, <i>Northeastern University</i> ; Battista Biggio, <i>University of Cagliari, Italy, and Pluribus One</i> ; Alina Oprea and Cristina Nita-Rotaru, <i>Northeastern University</i> ; Fabio Roli, <i>University of Cagliari, Italy, and Pluribus One</i>	

<b>Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography</b> .....	<b>339</b>
Felix Fischer, <i>Technical University of Munich</i> ; Huang Xiao, <i>Bosch Center for Artificial Intelligence</i> ; Ching-Yu Kao, <i>Fraunhofer AISEC</i> ; Yannick Stachelscheid, Benjamin Johnson, and Danial Razar, <i>Technical University of Munich</i> ; Paul Fawkesley and Nat Buckley, <i>Projects by IF</i> ; Konstantin Böttinger, <i>Fraunhofer AISEC</i> ; Paul Muntean and Jens Grossklags, <i>Technical University of Munich</i>	

## Planes, Cars, and Robots

<b>Wireless Attacks on Aircraft Instrument Landing Systems</b> .....	<b>357</b>
Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir, <i>Northeastern University</i>	

<b>Please Pay Inside: Evaluating Bluetooth-based Detection of Gas Pump Skimmers</b> .....	<b>373</b>
Nishant Bhaskar and Maxwell Bland, <i>University of California San Diego</i> ; Kirill Levchenko, <i>University of Illinois at Urbana-Champaign</i> ; Aaron Schulman, <i>University of California San Diego</i>	

<b>CANvas: Fast and Inexpensive Automotive Network Mapping</b> .....	<b>389</b>
Sekar Kulandaivel, Tushar Goyal, Arnav Kumar Agrawal, and Vyas Sekar, <i>Carnegie Mellon University</i>	

<b>Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging</b> .....	<b>407</b>
Richard Baker and Ivan Martinovic, <i>University of Oxford</i>	

<b>RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing</b> .....	<b>425</b>
Taegyu Kim, <i>Purdue University</i> ; Chung Hwan Kim and Junghwan Rhee, <i>NEC Laboratories America</i> ; Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, and Dongyan Xu, <i>Purdue University</i>	

## Machine Learning, Adversarial and Otherwise

### **Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms . . . . .443**

Qixue Xiao, *Department of Computer Science and Technology, Tsinghua University and 360 Security Research Labs*; Yufei Chen, *School of Electronic and Information Engineering, Xi'an Jiaotong University and 360 Security Research Labs*; Chao Shen, *School of Electronic and Information Engineering, Xi'an Jiaotong University*; Yu Chen, *Department of Computer Science and Technology, Tsinghua University and Peng Cheng Laboratory*; Kang Li, *Department of Computer Science, University of Georgia*

### **CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning . . . . .461**

Yisroel Mirsky and Tom Mahler, *Ben-Gurion University*; Ilan Shelef, *Soroka University Medical Center*; Yuval Elovici, *Ben-Gurion University*

### **Misleading Authorship Attribution of Source Code using Adversarial Learning . . . . .479**

Erwin Quiring, Alwin Maier, and Konrad Rieck, *TU Braunschweig*

### **Terminal Brain Damage: Exposing the Graceless Degradation in Deep Neural Networks Under Hardware**

### **Fault Attacks . . . . .497**

Sanghyun Hong, *University of Maryland College Park*; Pietro Frigo, *Vrije Universiteit Amsterdam*; Yiğitcan Kaya, *University of Maryland College Park*; Cristiano Giuffrida, *Vrije Universiteit Amsterdam*; Tudor Dumitraş, *University of Maryland College Park*

### **CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel. . . . .515**

Lejla Batina, *Radboud University, The Netherlands*; Shivam Bhasin and Dirmanto Jap, *Nanyang Technological University, Singapore*; Stjepan Picek, *Delft University of Technology, The Netherlands*

## Mobile Security 1

### **simTPM: User-centric TPM for Mobile Devices . . . . .533**

Dhiman Chakraborty, *CISPA Helmholtz Center for Information Security, Saarland University*; Lucjan Hanzlik, *CISPA Helmholtz Center for Information Security, Stanford University*; Sven Bugiel, *CISPA Helmholtz Center for Information Security*

### **The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends . . . . .551**

Omar Alrawi, *Georgia Institute of Technology*; Chaoshun Zuo, *Ohio State University*; Ruian Duan and Ranjita Pai Kasturi, *Georgia Institute of Technology*; Zhiqiang Lin, *Ohio State University*; Brendan Saltaformaggio, *Georgia Institute of Technology*

### **ENTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs. . . . .567**

Giuseppe Petracca, *Pennsylvania State University, US*; Yuqiong Sun, *Symantec Research Labs, US*; Ahmad-Atamli Reineh, *Alan Turing Institute, UK*; Patrick McDaniel, *Pennsylvania State University, US*; Jens Grossklags, *Technical University of Munich, DE*; Trent Jaeger, *Pennsylvania State University, US*

### **PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play . . . . .585**

Benjamin Andow and Samin Yaseer Mahmud, *North Carolina State University*; Wenyu Wang, *University of Illinois at Urbana-Champaign*; Justin Whitaker, William Enck, and Bradley Reaves, *North Carolina State University*; Kapil Singh, *IBM T.J. Watson Research Center*; Tao Xie, *University of Illinois at Urbana-Champaign*

### **50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System . . . . .603**

Joel Reardon, *University of Calgary / AppCensus Inc.*; Álvaro Feal, *IMDEA Networks Institute / Universidad Carlos III Madrid*; Primal Wijesekera, *U.C. Berkeley / ICSI*; Amit Elazari Bar On, *U.C. Berkeley*; Narseo Vallina-Rodriguez, *IMDEA Networks Institute / ICSI / AppCensus Inc.*; Serge Egelman, *U.C. Berkeley / ICSI / AppCensus Inc.*

## Side Channels

### **SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks . . . . .621**

Saad Islam and Ahmad Moghimi, *Worcester Polytechnic Institute*; Ida Bruhns and Moritz Krebbel, *University of Luebeck*; Berk Gulmezoglu, *Worcester Polytechnic Institute*; Thomas Eisenbarth, *Worcester Polytechnic Institute and University of Luebeck*; Berk Sunar, *Worcester Polytechnic Institute*

(continued on next page)

<b>Robust Website Fingerprinting Through the Cache Occupancy Channel</b> .....	639
Anatoly Shusterman, <i>Ben-Gurion University of the Negev</i> ; Lachlan Kang, <i>University of Adelaide</i> ; Yarden Haskal and Yosef Meltser, <i>Ben-Gurion University of the Negev</i> ; Prateek Mittal, <i>Princeton University</i> ; Yossi Oren, <i>Ben-Gurion University of the Negev</i> ; Yuval Yarom, <i>University of Adelaide and Data61</i>	
<b>Identifying Cache-Based Side Channels through Secret-Augmented Abstract Interpretation</b> .....	657
Shuai Wang, <i>HKUST</i> ; Yuyan Bao and Xiao Liu, <i>Penn State University</i> ; Pei Wang, <i>Baidu X-Lab</i> ; Danfeng Zhang and Dinghao Wu, <i>Penn State University</i>	
<b>SCATTERCACHE: Thwarting Cache Attacks via Cache Set Randomization</b> .....	675
Mario Werner, Thomas Unterluggauer, Lukas Giner, Michael Schwarz, Daniel Gruss, and Stefan Mangard, <i>Graz University of Technology</i>	
<b>Pythia: Remote Oracles for the Masses</b> .....	693
Shin-Yeh Tsai, <i>Purdue University</i> ; Mathias Payer, <i>EPFL</i> ; Yiyang Zhang, <i>Purdue University</i>	
<b>Mobile Security 2</b>	
<b>HideMyApp: Hiding the Presence of Sensitive Apps on Android</b> .....	711
Anh Pham, <i>ABB Corporate Research</i> ; Italo Dacosta, <i>EPFL</i> ; Eleonora Losiouk, <i>University of Padova</i> ; John Stephan, <i>EPFL</i> ; Kévin Huguenin, <i>University of Lausanne</i> ; Jean-Pierre Hubaux, <i>EPFL</i>	
<b>TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time</b> .....	729
Feargus Pendlebury, Fabio Pierazzi, and Roberto Jordaney, <i>King's College London &amp; Royal Holloway, University of London</i> ; Johannes Kinder, <i>Bundeswehr University Munich</i> ; Lorenzo Cavallaro, <i>King's College London</i>	
<b>Devils in the Guidance: Predicting Logic Vulnerabilities in Payment Syndication Services through Automated Documentation Analysis</b> .....	747
Yi Chen, <i>Institute of Information Engineering, CAS</i> ; Luyi Xing, Yue Qin, Xiaojing Liao, and XiaoFeng Wang, <i>Indiana University Bloomington</i> ; Kai Chen and Wei Zou, <i>Institute of Information Engineering, CAS</i>	
<b>Understanding iOS-based Crowdturfing Through Hidden UI Analysis</b> .....	765
Yeonjoon Lee, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, and XiaoFeng Wang, <i>Indiana University</i> ; Tongxin Li, <i>Peking University</i> ; Xianghang Mi, <i>Indiana University</i>	
<b>Crypto Means Cryptocurrencies</b>	
<b>BITE: Bitcoin Lightweight Client Privacy using Trusted Execution</b> .....	783
Sinisa Matetic, Karl Wüst, Moritz Schneider, and Kari Kostiainen, <i>ETH Zurich</i> ; Ghassan Karame, <i>NEC Labs</i> ; Srdjan Capkun, <i>ETH Zurich</i>	
<b>FASTKITTEN: Practical Smart Contracts on Bitcoin</b> .....	801
Poulami Das, Lisa Eckey, Tommaso Frassetto, David Gens, Kristina Hostáková, Patrick Jauernig, Sebastian Faust, and Ahmad-Reza Sadeghi, <i>Technische Universität Darmstadt, Germany</i>	
<b>StrongChain: Transparent and Collaborative Proof-of-Work Consensus</b> .....	819
Pawel Szalachowski, Daniël Reijnders, and Ivan Homoliak, <i>Singapore University of Technology and Design (SUTD)</i> ; Siwei Sun, <i>Institute of Information Engineering and DCS Center, Chinese Academy of Sciences</i>	
<b>Tracing Transactions Across Cryptocurrency Ledgers</b> .....	837
Haaroon Yousaf, George Kappos, and Sarah Meiklejohn, <i>University College London</i>	
<b>Intelligence and Vulnerabilities</b>	
<b>Reading the Tea leaves: A Comparative Analysis of Threat Intelligence</b> .....	851
Vector Guo Li, <i>University of California, San Diego</i> ; Matthew Dunn, <i>Northeastern University</i> ; Paul Pearce, <i>Georgia Tech</i> ; Damon McCoy, <i>New York University</i> ; Geoffrey M. Voelker and Stefan Savage, <i>University of California, San Diego</i> ; Kirill Levchenko, <i>University of Illinois Urbana-Champaign</i>	
<b>Towards the Detection of Inconsistencies in Public Security Vulnerability Reports</b> .....	869
Ying Dong, <i>University of Chinese Academy of Sciences and The Pennsylvania State University</i> ; Wenbo Guo, Yueqi Chen, and Xinyu Xing, <i>The Pennsylvania State University and JD Security Research Center</i> ; Yuqing Zhang, <i>University of Chinese Academy of Sciences</i> ; Gang Wang, <i>Virginia Tech</i>	

**Understanding and Securing Device Vulnerabilities through Automated Bug Report Analysis . . . . .887**  
Xuan Feng, *Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China*; Xiaojing Liao and XiaoFeng Wang, *Department of Computer Science, Indiana University Bloomington, USA*; Haining Wang, *Department of Electrical and Computer Engineering, University of Delaware, USA*; Qiang Li, *School of Computer and Information Technology, Beijing Jiaotong University, China*; Kai Yang, Hongsong Zhu, and Limin Sun, *Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China*

**ATTACK2VEC: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks . . . . .905**  
Yun Shen, *Symantec Research Labs*; Gianluca Stringhini, *Boston University*

## **Web Attacks**

**Leaky Images: Targeted Privacy Attacks in the Web . . . . .923**  
Cristian-Alexandru Staicu and Michael Pradel, *TU Darmstadt*

**All Your Clicks Belong to Me: Investigating Click Interception on the Web . . . . .941**  
Mingxue Zhang and Wei Meng, *Chinese University of Hong Kong*; Sangho Lee, *Microsoft Research*; Byoungyoung Lee, *Seoul National University and Purdue University*; Xinyu Xing, *Pennsylvania State University*

**What Are You Searching For? A Remote Keylogging Attack on Search Engine Autocomplete . . . . .959**  
John V. Monaco, *Naval Postgraduate School*

**Iframes/Popups Are Dangerous in Mobile WebView: Studying and Mitigating Differential Context Vulnerabilities . .977**  
GuangLiang Yang, Jeff Huang, and Guofei Gu, *Texas A&M University*

**Small World with High Risks: A Study of Security Threats in the npm Ecosystem . . . . .995**  
Markus Zimmermann and Cristian-Alexandru Staicu, *TU Darmstadt*; Cam Tenny, *r2c*; Michael Pradel, *TU Darmstadt*

## **Crypto Means Cryptographic Attacks**

**“Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails. . . . .1011**  
Jens Müller and Marcus Brinkmann, *Ruhr University Bochum*; Damian Poddebniak, *Münster University of Applied Sciences*; Hanno Böck, *unaffiliated*; Sebastian Schinzel, *Münster University of Applied Sciences*; Juraj Somorovsky and Jörg Schwenk, *Ruhr University Bochum*

**Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities . . . . .1029**  
Robert Merget and Juraj Somorovsky, *Ruhr University Bochum*; Nimrod Aviram, *Tel Aviv University*; Craig Young, *Tripwire VERT*; Janis Fliegenschmidt and Jörg Schwenk, *Ruhr University Bochum*; Yuval Shavitt, *Tel Aviv University*

**The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR . . . . .1047**  
Daniele Antonioli, *SUTD*; Nils Ole Tippenhauer, *CISPA*; Kasper B. Rasmussen, *University of Oxford*

**From IP ID to Device ID and KASLR Bypass. . . . .1063**  
Amit Klein and Benny Pinkas, *Bar Ilan University*

**When the Signal is in the Noise: Exploiting Diffix’s Sticky Noise . . . . .1081**  
Andrea Gadotti and Florimond Houssiau, *Imperial College London*; Luc Rocher, *Imperial College London and Université catholique de Louvain*; Benjamin Livshits and Yves-Alexandre de Montjoye, *Imperial College London*

## **IoT Security**

**FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation . . . . .1099**  
Yaowen Zheng, *Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China*; Ali Davanian, Heng Yin, and Chengyu Song, *University of California, Riverside*; Hongsong Zhu and Limin Sun, *Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China*



**Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks . . . . . 1115**  
Bing Huang, *The University of Texas at Austin*; Alvaro A. Cardenas, *University of California, Santa Cruz*; Ross Baldick, *The University of Texas at Austin*

**Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. . . . . 1133**  
Wei Zhou, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; Yan Jia, Yao Yao, and Lipeng Zhu, *School of Cyber Engineering, Xidian University*; *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; Le Guan, *Department of Computer Science, University of Georgia*; Yuhang Mao, *School of Cyber Engineering, Xidian University*; *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; Peng Liu, *College of Information Sciences and Technology, Pennsylvania State University*; Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; *School of Cyber Engineering, Xidian University*; *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences*

**Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps. . . . . 1151**  
Xueqiang Wang, *Indiana University Bloomington*; Yuqiong Sun and Susanta Nanda, *Symantec Research Labs*; XiaoFeng Wang, *Indiana University Bloomington*

**All Things Considered: An Analysis of IoT Devices on Home Networks . . . . . 1169**  
Deepak Kumar, *University of Illinois at Urbana-Champaign*; Kelly Shen and Benton Case, *Stanford University*; Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, and Rajarshi Gupta, *Avast Software s.r.o.*; Zakir Durumeric, *Stanford University*

## OS Security

**KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities . . . . . 1187**  
Wei Wu, *Institute of Information Engineering, Chinese Academy of Sciences*; *Pennsylvania State University*; *School of Cybersecurity, University of Chinese Academy of Sciences*; Yueqi Chen and Xinyu Xing, *Pennsylvania State University*; Wei Zou, *Institute of Information Engineering, Chinese Academy of Sciences*; *School of Cybersecurity, University of Chinese Academy of Sciences*

**PeX: A Permission Check Analysis Framework for Linux Kernel . . . . . 1205**  
Tong Zhang, *Virginia Tech*; Wenbo Shen, *Zhejiang University*; Dongyoon Lee, *Stony Brook University*; Changhee Jung, *Purdue University*; Ahmed M. Azab and Ruowen Wang, *Samsung Research America*

**ERIM: Secure, Efficient In-process Isolation with Protection Keys (MPK) . . . . . 1221**  
Anjo Vahldiek-Oberwagner, Eslam Elnikety, Nuno O. Duarte, Michael Sammler, Peter Druschel, and Deepak Garg, *Max Planck Institute for Software Systems, Saarland Informatics Campus*

**SafeHidden: An Efficient and Secure Information Hiding Technique Using Re-randomization. . . . . 1239**  
Zhe Wang and Chenggang Wu, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Yinqian Zhang, *The Ohio State University*; Bowen Tang, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Pen-Chung Yew, *University of Minnesota at Twin-Cities*; Mengyao Xie, Yuanming Lai, and Yan Kang, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Yueqiang Cheng, *Baidu USA*; Zhiping Shi, *The Capital Normal University*

**Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization. . . . . 1257**  
Mengyuan Li, Yinqian Zhang, and Zhiqiang Lin, *The Ohio State University*; Yan Solihin, *University of Central Florida*

## Phishing and Scams

**Detecting and Characterizing Lateral Phishing at Scale . . . . . 1273**  
Grant Ho, *UC Berkeley and Barracuda Networks*; Asaf Cidon, *Barracuda Networks and Columbia University*; Lior Gavish and Marco Schweighauser, *Barracuda Networks*; Vern Paxson, *UC Berkeley and ICSI*; Stefan Savage and Geoffrey M. Voelker, *UC San Diego*; David Wagner, *UC Berkeley*

**High Precision Detection of Business Email Compromise . . . . . 1291**  
Asaf Cidon, *Barracuda Networks and Columbia University*; Lior Gavish, Itay Bleier, Nadia Korshun, Marco Schweighauser, and Alexey Tsitkin, *Barracuda Networks*

<b>Cognitive Triaging of Phishing Attacks .....</b>	<b>1309</b>
Amber van der Heijden and Luca Allodi, <i>Eindhoven University of Technology</i>	
<b>Users Really Do Answer Telephone Scams .....</b>	<b>1327</b>
Huahong Tu, <i>University of Maryland</i> ; Adam Doupé, <i>Arizona State University</i> ; Ziming Zhao, <i>Rochester Institute of Technology</i> ; Gail-Joon Ahn, <i>Arizona State University and Samsung Research</i>	
<b>Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting ..</b>	<b>1341</b>
Arman Noroozian, <i>TU Delft</i> ; Jan Koenders and Eelco van Veldhuizen, <i>Dutch National High-Tech Crime Unit</i> ; Carlos H. Ganan, <i>TU Delft</i> ; Sumayah Alrwais, <i>King Saud University and International Computer Science Institute</i> ; Damon McCoy, <i>New York University</i> ; Michel van Eeten, <i>TU Delft</i>	
<b>Distributed System Security + Verifying Hardware</b>	
<b>Protecting Cloud Virtual Machines from Hypervisor and Host Operating System Exploits.....</b>	<b>1357</b>
Shih-Wei Li, John S. Koh, and Jason Nieh, <i>Columbia University</i>	
<b>WAVE: A Decentralized Authorization Framework with Transitive Delegation .....</b>	<b>1375</b>
Michael P Andersen, Sam Kumar, Moustafa AbdelBaky, Gabe Fierro, John Kolb, Hyung-Sin Kim, David E. Culler, and Raluca Ada Popa, <i>University of California, Berkeley</i>	
<b>in-toto: Providing farm-to-table guarantees for bits and bytes .....</b>	<b>1393</b>
Santiago Torres-Arias, <i>New York University</i> ; Hammad Afzali, <i>New Jersey Institute of Technology</i> ; Trishank Karthik Kuppusamy, <i>Datadog</i> ; Reza Curtmola, <i>New Jersey Institute of Technology</i> ; Justin Cappos, <i>New York University</i>	
<b>IODINE: Verifying Constant-Time Execution of Hardware .....</b>	<b>1411</b>
Klaus v. Gleissenthall, Rami Gökhan Kıcı, Deian Stefan, and Ranjit Jhala, <i>University of California, San Diego</i>	
<b>VRASED: A Verified Hardware/Software Co-Design for Remote Attestation .....</b>	<b>1429</b>
Ivan De Oliveira Nunes, <i>University of California, Irvine</i> ; Karim Eldefrawy, <i>SRI International</i> ; Norrathep Rattanavipanon, <i>University of California, Irvine</i> ; Michael Steiner, <i>Intel</i> ; Gene Tsudik, <i>University of California, Irvine</i>	
<b>Crypto Means Cryptography</b>	
<b>Mobile Private Contact Discovery at Scale. ....</b>	<b>1447</b>
Daniel Kales and Christian Rechberger, <i>Graz University of Technology</i> ; Thomas Schneider, Matthias Senker, and Christian Weinert, <i>TU Darmstadt</i>	
<b>EverParse: Verified Secure Zero-Copy Parsers for Authenticated Message Formats .....</b>	<b>1465</b>
Tahina Ramananandro, Antoine Delignat-Lavaud, Cédric Fournet, and Nikhil Swamy, <i>Microsoft Research</i> ; Tej Chajed, <i>MIT</i> ; Nadim Kobeissi, <i>Inria Paris</i> ; Jonathan Protzenko, <i>Microsoft Research</i>	
<b>Blind Bernoulli Trials: A Noninteractive Protocol For Hidden-Weight Coin Flips.....</b>	<b>1483</b>
Emma Connor and Max Schuchard, <i>University of Tennessee</i>	
<b>XONN: XNOR-based Oblivious Deep Neural Network Inference .....</b>	<b>1501</b>
M. Sadegh Riazi and Mohammad Samragh, <i>UC San Diego</i> ; Hao Chen, Kim Laine, and Kristin Lauter, <i>Microsoft Research</i> ; Farinaz Koushanfar, <i>UC San Diego</i>	
<b>JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT .....</b>	<b>1519</b>
Sam Kumar, Yuncong Hu, Michael P Andersen, Raluca Ada Popa, and David E. Culler, <i>University of California, Berkeley</i>	
<b>Passwords</b>	
<b>Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users .....</b>	<b>1537</b>
Ding Wang and Ping Wang, <i>Peking University</i> ; Debiao He, <i>Wuhan University</i> ; Yuan Tian, <i>University of Virginia</i>	
<b>Protecting accounts from credential stuffing with password breach alerting .....</b>	<b>1555</b>
Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, and Sarvar Patel, <i>Google</i> ; Dan Boneh, <i>Stanford</i> ; Elie Bursztein, <i>Google</i>	

(continued on next page)

<b>Probability Model Transforming Encoders Against Encoding Attacks .....</b>	<b>1573</b>
Haibo Cheng, Zhixiong Zheng, Wenting Li, and Ping Wang, <i>Peking University</i> ; Chao-Hsien Chu, <i>Pennsylvania State University</i>	

## Cryptocurrency Scams

<b>The Art of The Scam: Demystifying Honey pots in Ethereum Smart Contracts .....</b>	<b>1591</b>
Christof Ferreira Torres, Mathis Steichen, and Radu State, <i>University of Luxembourg</i>	
<b>The Anatomy of a Cryptocurrency Pump-and-Dump Scheme .....</b>	<b>1609</b>
Jiahua Xu, <i>École polytechnique fédérale de Lausanne (EPFL)</i> ; Benjamin Livshits, <i>Imperial College London</i>	
<b>Inadvertently Making Cyber Criminals Rich: A Comprehensive Study of Cryptojacking Campaigns at Internet Scale .....</b>	<b>1627</b>
Hugo L.J. Bijmans, Tim M. Booi, and Christian Doerr, <i>Delft University of Technology</i>	

## Web Defenses

<b>Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting .....</b>	<b>1645</b>
Shuijiang Wu, Song Li, and Yinzhi Cao, <i>Johns Hopkins University</i> ; Ningfei Wang, <i>Lehigh University</i>	
<b>Site Isolation: Process Separation for Web Sites within the Browser .....</b>	<b>1661</b>
Charles Reis, Alexander Moshchuk, and Nasko Oskov, <i>Google</i>	
<b>Everyone is Different: Client-side Diversification for Defending Against Extension Fingerprinting .....</b>	<b>1679</b>
Erik Trickett, <i>Arizona State University</i> ; Oleksii Starov, <i>Stony Brook University</i> ; Alexandros Kapravelos, <i>North Carolina State University</i> ; Nick Nikiforakis, <i>Stony Brook University</i> ; Adam Doupe, <i>Arizona State University</i>	
<b>Less is More: Quantifying the Security Benefits of Debloating Web Applications .....</b>	<b>1697</b>
Babak Amin Azad, Pierre Laperdrix, and Nick Nikiforakis, <i>Stony Brook University</i>	
<b>The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators .....</b>	<b>1715</b>
Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt, <i>Google</i>	

## Software Security

<b>RAZOR: A Framework for Post-deployment Software Debloating .....</b>	<b>1733</b>
Chenxiong Qian, Hong Hu, Mansour Alharthi, Pak Ho Chung, Taesoo Kim, and Wenke Lee, <i>Georgia Institute of Technology</i>	
<b>Back to the Whiteboard: a Principled Approach for the Assessment and Design of Memory Forensic Techniques ..</b>	<b>1751</b>
Fabio Pagani and Davide Balzarotti, <i>EURECOM</i>	
<b>Detecting Missing-Check Bugs via Semantic- and Context-Aware Criticalness and Constraints Inferences .....</b>	<b>1769</b>
Kangjie Lu, Aditya Pakki, and Qiushi Wu, <i>University of Minnesota</i>	
<b>DEEPVSA: Facilitating Value-set Analysis with Deep Learning for Postmortem Program Analysis. ....</b>	<b>1787</b>
Wenbo Guo, Dongliang Mu, and Xinyu Xing, <i>The Pennsylvania State University</i> ; Min Du and Dawn Song, <i>University of California, Berkeley</i>	
<b>CONFIRM: Evaluating Compatibility and Relevance of Control-flow Integrity Protections for Modern Software ..</b>	<b>1805</b>
Xiaoyang Xu, Masoud Ghaffarinia, Wenhao Wang, and Kevin W. Hamlen, <i>University of Texas at Dallas</i> ; Zhiqiang Lin, <i>Ohio State University</i>	

## Privacy

<b>Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor .....</b>	<b>1823</b>
Rob Jansen, <i>U.S. Naval Research Laboratory</i> ; Tavish Vaidya and Micah Sherr, <i>Georgetown University</i>	
<b>No Right to Remain Silent: Isolating Malicious Mixes .....</b>	<b>1841</b>
Hemi Leibowitz, <i>Bar-Ilan University, IL</i> ; Ania M. Piotrowska and George Danezis, <i>University College London, UK</i> ; Amir Herzberg, <i>University of Connecticut, US</i>	



**On (The Lack Of) Location Privacy in Crowdsourcing Applications . . . . .1859**  
Spyros Boukoros, *TU-Darmstadt*; Mathias Humbert, *Swiss Data Science Center (ETH Zurich, EPFL)*; Stefan Katzenbeisser, *TU-Darmstadt, University of Passau*; Carmela Troncoso, *EPFL*

**Utility-Optimized Local Differential Privacy Mechanisms for Distribution Estimation . . . . .1877**  
Takao Murakami and Yusuke Kawamoto, *AIST*

**Evaluating Differentially Private Machine Learning in Practice . . . . .1895**  
Bargav Jayaraman and David Evans, *University of Virginia*

## **Fuzzing**

**FUZZIFICATION: Anti-Fuzzing Techniques . . . . .1913**  
Jinho Jung, Hong Hu, David Solodukhin, and Daniel Pagan, *Georgia Institute of Technology*; Kyu Hyung Lee, *University of Georgia*; Taesoo Kim, *Georgia Institute of Technology*

**ANTI FUZZ: Impeding Fuzzing Audits of Binary Executables . . . . .1931**  
Emre Güler, Cornelius Aschermann, Ali Abbasi, and Thorsten Holz, *Ruhr-Universität Bochum*

**MOPT: Optimized Mutation Scheduling for Fuzzers . . . . .1949**  
Chenyang Lyu, *Zhejiang University*; Shouling Ji, *Zhejiang University & Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies*; Chao Zhang, *BNRist & INSC, Tsinghua University*; Yuwei Li, *Zhejiang University*; Wei-Han Lee, *IBM Research*; Yu Song, *Zhejiang University*; Raheem Beyah, *Georgia Institute of Technology*

**EnFuzz: Ensemble Fuzzing with Seed Synchronization among Diverse Fuzzers . . . . .1967**  
Yuanliang Chen, Yu Jiang, Fuchen Ma, Jie Liang, Mingzhe Wang, and Chijin Zhou, *Tsinghua University*; Xun Jiao, *Villanova University*; Zhuo Su, *Tsinghua University*

**GRIMOIRE: Synthesizing Structure while Fuzzing . . . . .1985**  
Tim Blazytko, Cornelius Aschermann, Moritz Schlögel, Ali Abbasi, Sergej Schumilo, Simon Wörner, and Thorsten Holz, *Ruhr-Universität Bochum*