Wednesday, August 15

7:30 am–8:45 am
Continental Breakfast

8:45 am–9:00 am
Opening Remarks and Awards
Program Co-Chairs: William Enck, North Carolina State University, and Adrienne Porter Felt, Google

9:00 am–10:00 am
Keynote Address
Q: Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?
A: Because Keynote Speakers Make Bad Life Decisions and Are Poor Role Models
James Mickens, Harvard University

10:00 am–10:30 am
Break with Refreshments

10:30 am–12:10 pm
Track 1

Security Impacting the Physical World
Fear the Reaper: Characterization and Fast Detection of Card Skimmers
Nolen Scaife, Christian Peeters, and Patrick Traynor, University of Florida

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid
Saleh Soltan, Prateek Mittal, and H. Vincent Poor, Princeton University

Skill Squatting Attacks on Amazon Alexa
Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey, University of Illinois, Urbana-Champaign

CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition
Xuejing Yuan, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences; Yuxuan Chen, Florida Institute of Technology; Yue Zhao, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences. School of Cyber Security, University of Chinese Academy of Sciences; Yunhui Long, University of Illinois at Urbana-Champaign; Xiaokang Liu and Kai Chen, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences; Shengzhi Zhang, Florida Institute of Technology; Heqing Huang, IBM Thomas J. Watson Research Center; Xiaofeng Wang, Indiana University Bloomington; Carl A. Gunter, University of Illinois at Urbana-Champaign

12:10 pm–1:40 pm
Lunch (on your own)

The Career Luncheon for Students and Recent Grads will occur at this time.
<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Understanding How Humans Authenticate</strong></td>
<td><strong>Vulnerability Discovery</strong></td>
<td><strong>Invited Talks</strong></td>
</tr>
<tr>
<td>Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse</td>
<td>ATTention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem</td>
<td>Privacy for Tigers</td>
</tr>
<tr>
<td>Sanam Ghorbani Lyastani, CISPA, Saarland University; Michael Schilling, Saarland University; Sascha Fahl, Leibniz University Hannover; Sven Bugiel, CISPA, Saarland University; Michael Backes, CISPA Helmholtz Center i.G.</td>
<td>Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, and Patrick Traynor, University of Florida; Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace, Samsung Research America</td>
<td>Ross Anderson, Cambridge University</td>
</tr>
<tr>
<td>Forgetting of Passwords: Ecological Theory and Data</td>
<td>Charm: Facilitating Dynamic Analysis of Device Drivers of Mobile Devices</td>
<td>Cybersecurity: Is It about Business or Technology</td>
</tr>
<tr>
<td>Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, and Janne Lindqvist, Rutgers University; Antti Oulasvirta, Aalto University</td>
<td>Seyed Mohammadjavad Seyed Talebi and Hamid Tavakoli, UC Irvine; Hang Zhang and Zheng Zhang, UC Riverside; Ardalan Amiri Sani, UC Irvine; Zhiyun Qian, UC Riverside</td>
<td>Donna Dodson, Chief Cybersecurity Advisor, National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Ingolf Becker, Simon Parkin, and M. Angela Sasse, University College London</td>
<td>Nassim Corteggianni, EURECOM, Maxim Integrated; Giovanni Camurati and Aurélien Francillon, EURECOM</td>
<td></td>
</tr>
<tr>
<td>Rethinking Authentication and Access Control for the Home Internet of Things (IoT)</td>
<td>Acquisitional Rule-based Engine for Discovering Internet-of-Thing Devices</td>
<td></td>
</tr>
<tr>
<td>Weijia He, University of Chicago; Maximilian Golla, Ruhr-University Bochum; Roshni Padhi and Jordan Ofek, University of Chicago; Markus Durmuth, Ruhr-University Bochum; Earlene Fernandes, University of Washington; Blase Ur, University of Chicago</td>
<td>Xuan Feng, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; Qiang Li, School of Computer and Information Technology, Beijing Jiaotong University, China; Haining Wang, Department of Electrical and Computer Engineering, University of Delaware, USA; Limin Sun, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China</td>
<td></td>
</tr>
<tr>
<td>3:20pm–3:50 pm Break with Refreshments Grand Ballroom</td>
<td>3:50 pm–5:30 pm</td>
<td></td>
</tr>
<tr>
<td><strong>Invited Talks</strong></td>
<td><strong>Track 1</strong></td>
<td><strong>Track 2</strong></td>
</tr>
<tr>
<td>Rethinking Architectures and Abstraction for a World Where Security Improvements Matter More than Performance Gains</td>
<td><strong>Web Applications</strong></td>
<td><strong>Anonymity</strong></td>
</tr>
<tr>
<td>Cristian-Alexandru Staicu and Michael Pradel, TU Darmstadt</td>
<td>NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications</td>
<td>Towards Predicting Efficient and Anonymous Tor Circuits</td>
</tr>
<tr>
<td>Abeer Alhuzali, Rigel Gjomemo, Birhanu Esheste, and V.N. Venkatakrishnan, UIC</td>
<td>Abeer Alhuzali, Rigel Gjomemo, Birhanu Esheste, and V.N. Venkatakrishnan, UIC</td>
<td>Armon Barton, University of Texas at Arlington; Matthew Wright, Rochester Institute of Technology; Jiang Ming and Mohsen Imani, University of Texas at Arlington</td>
</tr>
<tr>
<td>Wei Meng, Chinese University of Hong Kong; Chenxiang Qian, Georgia Institute of Technology; Shuang Hao, University of Texas at Dallas; Kevin Borgolte, Giovanni Vigna, and Christopher Kruegel, University of California, Santa Barbara; Wenke Lee, Georgia Institute of Technology</td>
<td>Abeer Alhuzali, Rigel Gjomemo, Birhanu Esheste, and V.N. Venkatakrishnan, UIC</td>
<td>Nirvan Tyagi, Cornell Tech; Muhammad Haris Mughees, Cornell Tech and UIUC, Thomas Ristenpart and Ian Miers, Cornell Tech</td>
</tr>
<tr>
<td></td>
<td>Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks</td>
<td>An Empirical Analysis of Anonymity in Zcash</td>
</tr>
<tr>
<td></td>
<td>Wei Meng, Chinese University of Hong Kong; Chenxiang Qian, Georgia Institute of Technology; Shuang Hao, University of Texas at Dallas; Kevin Borgolte, Giovanni Vigna, and Christopher Kruegel, University of California, Santa Barbara; Wenke Lee, Georgia Institute of Technology</td>
<td>George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn, University College London</td>
</tr>
</tbody>
</table>
Wednesday, August 15 (continued)

6:00 pm–7:30 pm

**USENIX Security ’18 Symposium Reception**
Mingle with fellow attendees at the USENIX Security ’18 Reception, featuring dinner, drinks, and the chance to connect with other attendees, speakers, and symposium organizers.

7:30 pm–8:30 pm

**USENIX Security ’18 Lightning Talks**
This is intended as an informal session for short and engaging presentations on recent unpublished results, work in progress, or other topics of interest to USENIX Security attendees. As in the past, talks do not always need to be serious and funny talks are encouraged! This year, USENIX will generously sponsor awards for the most engaging talks. Bragging rights and small cash prizes can be yours for a great talk! For full consideration, submit your lightning talk via the lighting talk submission form, which will be available here soon, through July 27, 2018. Only talks submitted by this deadline will be considered for the awards. You can continue submitting talks via the submission form or by emailing sec18lightning@usenix.org until Wednesday, August 15, 2018, 12:00 pm EDT.
<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy in a Digital World</strong></td>
<td><strong>Attacks on Crypto &amp; Crypto Libraries</strong></td>
<td><strong>Invited Talks</strong></td>
</tr>
<tr>
<td>Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes</td>
<td>Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels</td>
<td>Analogy Cyber Security—From 0101 to Mixed Signals</td>
</tr>
<tr>
<td>José González Cabañas, Ángel Cuevas, and Rubén Cuevas, Department of Telematic Engineering, Universidad Carlos III de Madrid</td>
<td>Damian Poddebniak, Münster University of Applied Sciences; Jens Müller, Ruhr University Bochum; Christian Dresen, Fabian Ising, and Sebastian Schinzel, Münster University of Applied Sciences; Simon Friedberger, KU Leuven; Juraj Somorovsky and Jörg Schwenk, Ruhr University Bochum</td>
<td>Wenyuan Xu, Zhejiang University</td>
</tr>
<tr>
<td>Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide?</td>
<td>The Dangers of Key Reuse - Practical Attacks on IPsec IKE</td>
<td>Title TBA</td>
</tr>
<tr>
<td>Wajih Ul Hassan, Saad Hussain, and Adam Bates, University Of Illinois Urbana-Champaign</td>
<td>Martin Grothe, Dennis Felsch, and Jörg Schwenk, Ruhr-University Bochum; Adam Czubak and Marcin Szymanek, University of Opole</td>
<td>Vijay Balasubramaniyan, CEO and Founder, Pindrop</td>
</tr>
<tr>
<td><strong>AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning</strong></td>
<td><strong>One&amp;Done: A Single-Decryption EM-Based Attack on OpenSSL’s Constant-Time Blinded RSA</strong></td>
<td><strong>DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries</strong></td>
</tr>
<tr>
<td>Jinyuan Jia and Neil Zhenqiang Gong, Iowa State University</td>
<td>Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic, Georgia Tech</td>
<td>Samuel Weiser, Graz University of Technology; Andreas Zankl, Fraunhofer AISEC; Raphael Spreitzer, Graz University of Technology; Katja Miller, Fraunhofer AISEC; Stefan Mangard, Graz University of Technology; Georg Sigl, Technical University of Munich</td>
</tr>
<tr>
<td>Hamza Harkous, EPFL; Kassem Fawaz, University of Wisconsin-Madison; Rémi Lebret, EPFL; Florian Schaub and Kang G. Shin, University of Michigan; Karl Aberer, EPFL</td>
<td>Howard Wu, Wenenting Zheng, Alessandro Chiesa, Raluca Ada Popa, and Ion Stoica, UC Berkeley</td>
<td>Nethide: Secure and Practical Network Topology Obfuscation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Roland Meier and Petar Tsankov, ETH Zurich; Vincent Lenders, armasuisse; Laurent Vanbever and Martin Vechev, ETH Zurich</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Towards a Secure Zero-rating Framework with Three Parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zhiheng Liu, Zhen Zhang, Yinzhi Cao, Zhaohan Xi, and Shihaoying, Lehigh University; Humberto La Roche, Cisco Systems</td>
</tr>
</tbody>
</table>

**Thursday, August 16**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 am–9:00 am</td>
<td>Continental Breakfast</td>
</tr>
<tr>
<td>9:00 am–10:40 am</td>
<td>Track 1 sessions</td>
</tr>
<tr>
<td>10:40 am–11:10 am</td>
<td>Break with Refreshments</td>
</tr>
<tr>
<td>11:10 am–12:00 pm</td>
<td>Track 2 sessions</td>
</tr>
<tr>
<td>12:00 pm–1:30 pm</td>
<td>Track 3 sessions</td>
</tr>
<tr>
<td>12:30 pm–1:30 pm</td>
<td>USENIX Security ’18 Luncheon</td>
</tr>
</tbody>
</table>

*Sponsored by Facebook*

The Internet Defense Prize will be presented at the Symposium Luncheon.
### Thursday, August 16 (continued)

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:30 pm–3:10 pm</td>
<td>Fuzzing and Exploit Generation</td>
<td>TLS and PKI</td>
<td>Vulnerability Mitigations</td>
</tr>
<tr>
<td></td>
<td>MoonShine: Optimizing OS Fuzzer Seed Selection with Trace Distillation</td>
<td>The Secure Socket API: TLS as an Operating System Service</td>
<td>Debloating Software through Piece-Wise Compilation and Loading</td>
</tr>
<tr>
<td></td>
<td>Shankara Palloor, Andrew Aday, and Sumant Jana, Columbia University</td>
<td>Mark O’Neill, Scott Heidbrink, Jordan Whitehead, Tanner Perdue, Luke Dickinson, Torstein Collett, Matthew Martindale, Kent Seamons, and Daniel Zappala, Brigham Young University</td>
<td>Anh Quach and Aravind Prakash, Binghamton University; Lok Kwong Yan, Air Force Research Laboratory</td>
</tr>
<tr>
<td></td>
<td>QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing</td>
<td>Return Of Bleichenbacher’s Oracle Threat (ROBOT)</td>
<td>Precise and Accurate Patch Presence Test for Binaries</td>
</tr>
<tr>
<td></td>
<td>Insu Yun, Sangho Lee, and Meng Xu, Georgia Institute of Technology; Yeongjin Jang, Oregon State University; Taesoo Kim, Georgia Institute of Technology</td>
<td>Hannu Böck, unaffiliated; Juraj Somorovsky, Ruhr-Universität Bochum, Hackmanit GmbH; Craig Young, Tripwire VERT</td>
<td>Hang Zhang and Zhiyun Qian, University of California, Riverside</td>
</tr>
<tr>
<td></td>
<td>Automatic Heap Layout Manipulation for Exploitation</td>
<td>Bamboozling Certificate Authorities with BGP</td>
<td>From Patching Delays to Infection Symptoms: Using Risk Profiles for an Early Discovery of Vulnerabilities Exploited in the Wild</td>
</tr>
<tr>
<td></td>
<td>Sean Heelan, Tom Melham, and Daniel Kroening, University of Oxford</td>
<td>Henry Birge-Lee, Yixin Sun, Annie Edmundson, Jennifer Rexford, and Prateek Mittal, Princeton University</td>
<td>Chaowei xiao and Armin Sarabi, University of Michigan; Yang Liu, Harvard University; Bo Li, University of California, Berkeley; Mingyan Liu, University of Michigan; Tudor Dumitras, University of Maryland</td>
</tr>
<tr>
<td></td>
<td>Wei Wu, University of Chinese Academy of Sciences; Yueqi Chen, Jun Xu, and Xinyu Xing, Penn State University; Wei Zou and Xiaorui Gong, University of Chinese Academy of Sciences</td>
<td>Doowon Kim and Bum Jun Kwon, University of Maryland, College Park</td>
<td>Dongliang Mu, Nanjing University; Alejandro Cuevas, The Pennsylvania State University; Limin Yang, East China Normal University; Hang Hu and Gang Wang, Virginia Polytechnic Institute and State University; Xinyu Xing, The Pennsylvania State University, Bing Mao, Nanjing University</td>
</tr>
</tbody>
</table>

### 3:10 pm–4:30 pm

**Track 1**

**Side Channels**

**Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder Than You Think**
Stephan van Schaik, Kaveh Razavi, Cristiano Giuffrida, and Herbert Bos, Wij University Amsterdam

**Translation Leak-side Buffer: Defeating Cache Side-channel Protections with TBL Attacks**
Ben Gras, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida, VU University Amsterdam

**Meltdown: Reading Kernel Memory from User Space**
Moritz Lipp, Michael Schwarz, and Daniel Gruss, Graz University of Technology; Thomas Prescher and Werner Haas, Cyberus Technology; Anders Fogh, G DATA Advanced Analytics; Jann Horn, Google Project Zero; Stefan Mängard, Graz University of Technology; Paul Kocher, unaffiliated; Daniel Genkin, University of Pennsylvania and University of Maryland; Yuval Yarom, University of Adelaide and Data61; Mike Hamburg, Rambus, Cryptography Research Division

**Foreshadow: A Speculative Execution Attack against Enclave Execution**
Jo Van Bulck, Frank Piessens, and Raoul Strackx, imec DistrNet, KU Leuven

### 3:40 pm–5:20 pm

**Break with Refreshments**

### 4:40 pm–6:00 pm

**Cybercrime**

**Plug and Prey? Measuring the Commodityof Cybercrime via Online Anonymous Markets**
Rolf van Wegberg and Samaneh Tajalizadehkoohb, Delft University of Technology; Kyle Soska, Carnegie Mellon University; Ugur Akyazi, Carlos Hernández Ganán, and Bram Klievink, Delft University of Technology; Nicolas Christin, Carnegie Mellon University; Michel van Etten, Delft University of Technology

**Reading Thieves’ Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces**
Kan Yuan, Indiana University; Bloomington; Haoran Lu and Xiaojing Liao, College of William & Mary; Xiaofeng Wang, Indiana University; Bloomington

**The Droste Effect: Profiling the Stakeholders in the Remote Access Trojan Ecosystem**
Mohammad Rezaeeirad, George Mason University; Brown Farinholt, University of California, San Diego; Hitesh Dharmadasani, Informant Networks; Paul Pearce, University of California, Berkeley; Kirill Levchenko, University of California, San Diego; Damon McCoy, New York University

**The aftermath of a crypto-ransomware attack at a large academic institution**
Leah Zhang-Kennedy, University of Waterloo; Stratford Campus; Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, and Sonia Chiaisson, Carleton University

**Invited Talks**

**The Law and Economics of Bug Bounties**
Amir Elazari Bar On, Doctoral Candidate, Berkeley Law, Center for Long-Term Cybersecurity Grantee

**Panel: The Future of Automated Online Content Moderation**
Moderator: Nick Feamster, Princeton University
### Thursday, August 16 (continued)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:00 pm–7:30 pm</td>
<td>Poster Session and Happy Hour</td>
</tr>
</tbody>
</table>

Check out the cool new ideas and the latest preliminary research on display at the Poster Session and Happy Hour. Take part in discussions with your colleagues over complimentary drinks and snacks. View the list of accepted posters at www.usenix.org/usenixsecurity17/posters.

### Friday, August 17

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 am–9:00 am</td>
<td>Continental Breakfast</td>
<td></td>
<td>Invited Talks</td>
</tr>
<tr>
<td>9:00 am–10:40 am</td>
<td></td>
<td>Malware</td>
<td></td>
</tr>
</tbody>
</table>

**Web and Network Measurement**

We Still Don’t Have Secure Cross-Domain Requests: an Empirical Study of CORS
Jianjun Chen, Tsinghua University; Tsinghua National Laboratory for Information Science and Technology; Jian Jiang, Shape Security; Haixin Duan, Institute for Network Science and Cyber Space, Tsinghua University; Tao Wan, Huawei Canada; Shuo Chen, Microsoft Research Redmond; Vern Paxson, UC Berkeley, ICSI; Min Yang, Fudan University

End-to-End Measurements of Email Spoofing Attacks
Hang Hu and Gang Wang, Virginia Tech

Who Is Answering My Queries: Understanding and Characterizing Illegal Interception of DNS Resolution Path at ISP Level
Baojun Liu, Chaoyi Lu, Haixin Duan, and Ying Liu, Tsinghua University; Zhou Li, IEEE member; Shuang Hao, University of Texas at Dallas; Min Yang, Fudan University

End Users Get Maneuvered: Empirical Analysis of Redirection Hijacking in Content Delivery Networks
Shuai Hao, CAIDA/UC San Diego; Yubao Zhang and Haining Wang, University of Delaware; Angelos Stavrou, George Mason University

### Track 2

**Malware**

SAD THUG: Structural Anomaly Detection for Transmissions of High-value Information Using Graphics
Jonathan P. Chapman, Fraunhofer FKIE

FANCI: Feature-based Automated NXDomain Classification and Intelligence
Samuel Schuppen, RWTH Aachen University; Dominik Teubert, Siemens CERT; Patrick Herrmann and Ulrike Meyer, RWTH Aachen University

An Empirical Study of Web Resource Manipulation in Real-world Mobile Applications
Xiaohan Zhang, Yuan Zhang, Qianqian Mo, Hao Xia, Zhemin Yang, and Min Yang, Fudan University; Xiaofeng Wang, Indiana University; Long Lu, Northeastern University; Haixin Duan, Tsinghua University

Fast and Service-preserving Recovery from Malware Infections Using CRIU
Ashton Webster, Ryan Eckenrod, and James Purtilo, University of Maryland

### Track 3

**Invited Talks**

The Second Crypto War—What’s Different Now
Susan Landau, Bridge Professor of Cyber Security and Policy, Tufts University

Medical Device Cybersecurity Through the FDA Lens
Suzanne B. Schwartz, US Food and Drug Administration

### Subverting Hardware Protections

The Guard’s Dilemma: Efficient Code-Reuse Attacks Against Intel SGX
Andrea Biondo and Mauro Conti, University of Padua; Lucas Davi, University of Duisburg-Essen; Tommaso Frassetto and Ahmad-Reza Sadeghi, Technische Universität Darmstadt

A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping
Subehun Han, Wook Shin, Jun-Hyeok Park, and HyungChun Kim, National Security Research Institute

More Malware

Tackling runtime-based obfuscation in Android with TIRO
Michelle Y. Wong and David Lie, University of Toronto

Discovering Vulnerabilities in Security-Focused Static Analysis Tools for Android using Systematic Mutation
Richard Bonett, Kaushal Kafle, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk, College of William & Mary

### More Malware

Attacks on Systems That Learn

With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning
Bolu Wang, UC Santa Barbara; Yuanshun Yao, Bimal Viswanath, Haitao Zheng, and Ben Y. Zhao, University of Chicago

When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks
Octavian Suciu, Radu Marginean, Yigitcan Kaya, Hal Daume III, and Tudor Dumitras, University of Maryland

### Break with Refreshments

Grand Ballroom

### Lunch (on your own)

Friday, August 17 continues on next page
Friday, August 17 (continued)

1:30 pm–3:10 pm

**Track 1**

**Smart Contracts**
- teEther: Gnawing at Ethereum to Automatically Exploit Smart Contracts
  - Johannes Krupp and Christian Rosso, CISPA

**Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts**
- Lorenz Breidenbach, ETH Zurich; Phil Daian, Cornell Tech; Florian Tramer, Stanford University; Ari Juels, Cornell Tech Jacobs Institute

**Arbitrum: Scalable smart contracts**
- Harry Kalodner, Steven Goldfeder, Xiaomi Chen, Matt Weinberg, and Edward Felten, Princeton University

**Erays: Reverse Engineering Ethereum’s Opaque Smart Contracts**
- Yi Zhou, Deepak Kumar, Surya Bakshi, Joshua Mason, Andrew Miller, and Michael Bailey, University of Illinois, Urbana-Champaign

**Track 2**

**Executing in Untrusted Environments**
- DelegaTEE: Brokered Delegation Using Trusted Execution Environments
  - Sinisa Matetic and Moritz Schneider, ETH Zurich; Andrew Miller, UIUC; Ari Juels, Cornell Tech; Srdjan Capkun, ETH Zurich

**Simple Password-Hardened Encryption Services**
- Russell W. F. Lai and Christoph Egger, Friedrich-Alexander-University Erlangen-Nürnberg; Manuel Reihert, Saarland University; Sherman S. M. Chow, The Chinese University of Hong Kong

**Track 3**

**Web Authentication**
- Vetting Single Sign-On SDK Implementations via Symbolic Reasoning
  - Ronghai Yang, Wing Cheong Lau, Jiongyi Chen, and Kehuan Zhang, The Chinese University of Hong Kong

- Mohammad Ghasemifar, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, and Jason Polakis, University of Illinois at Chicago

**WPSE: Fortifying Web Protocols via Browser-Side Security Monitoring**
- Stefano Calzarava and Riccardo Focardi, Università Ca’ Foscari Venezia; Matteo Maffei and Clara Schneidewind, TU Wien; Marco Squarzina and Mauro Tempesta, Università Ca’ Foscari Venezia

**Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer**
- Thanh Bui and Siddharth Prakash Rao, Aalto University; Markku Antikainen, University of Helsinki; Viswanathan Manihatty Bojan and Tuomas Aura, Aalto University

3:10 pm–3:40 pm

Break with Refreshments

3:40 pm–5:20 pm

**Blockchains**

**All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems**
- Kexiong (Curtis) Zeng, Virginia Tech; Shinan Liu, University of Electronic Science and Technology of China; Yuanchao Shu, Microsoft Research; Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang, Virginia Tech

**Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors**
- Yizhou Tu, University of Louisiana at Lafayette; Zhiqiang Lin, Ohio State University; Insup Lee, University of Pennsylvania; Xial Hei, University of Louisiana at Lafayette

**Modeling and Analysis of a Hierarchy of Distance Bounding Attacks**
- Tom Chothia, Univ. of Birmingham; Joeri de Ruiter, Radboud University Nijmegen; Ben Smyth, University of Luxembourg

**Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secret**
- Weiteng Chen and Zhiyuan Qian, University of California, Riverside

**Neural Networks**

**Formal Security Analysis of Neural Networks using Symbolic Intervals**
- Shuqi Wang, Kexin Pei, Justin Whitehouse, Jinfeng Yang, and Suman Jana, Columbia University

**Turning Your Weakness Into a Strength: Watermarking Deep Neural Networks by Backdooring**
- Yossi Adi and Carsten Baum, Bar Ilan University; Moustapha Cisse, Facebook AI Research; Benny Pinkas and Joseph Keshet, Bar Ilan University

**A4NT: Author Attribute Anonymity by Adversarial Training of Neural Machine Translation**
- Rakshith Shetty, Bernt Schiele, and Mario Fritz, Max Planck Institute for Informatics

**GAZELLE: A Low Latency Framework for Secure Neural Network Inference**
- Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan, MIT

**Information Tracking**

**FlowCog: Context-aware Semantics Extraction and Analysis of Information Flow Leaks in Android Apps**
- Xiang Fan, Google Inc.; Yinzhi Cao, Lehigh University; Kuechao Du, Zhejiang University; Gan Fang, Northwestern University; Rui Shao, Zhejiang University; Yan Chen, Northwestern University

**Sensitive Information Tracking in Commodity IoT**

**Enabling Refinable Cross-host Attack Investigation with Efficient Data Flow Tagging and Tracking**
- Yang Ji, Sanghoo Lee, Mattia Fazzino, Joey Allen, Evan Downing, Taesoo Kim, Alessandro Orso, and Wenke Lee, Georgia Institute of Technology

**Dependence-Preserving Data Compaction for Scalable Forensic Analysis**
- Md Nahid Hossain, Junao Wang, R. Sekar, and Scott D. Stoller, Stony Brook University