CONTACT: Jim Ormond
212-626-0505
ormond@hq.acm.org

CCS 2017 Advances the Science of Cybersecurity

Computer and Communications Security Conference Includes Several Tracks that Showcase State-of-the-Art Technologies by World's Leading Researchers

NEW YORK, October 27, 2017 – ACM, the Association for Computing Machinery, has a longstanding interest in computer security, and improving the security of computing systems is increasingly essential for modern life. The 24th annual ACM Conference on Computer and Communications Security (CCS 2017), a flagship conference on computer and network security, will be held from October 30 through November 3 in Dallas, Texas. CCS 2017, organized by ACM's Special Interest Group on Security, Audit and Control (SIGSAC), brings together leading information security researchers, practitioners, developers, and users to discuss a range of topics including secure hardware, implementing cryptosystems securely, adversarial machine learning, and privacy-preserving applications.

"We are honored to host ACM CCS in Dallas, Texas and so far we have close to 1,000 registrations," said ACM CCS 2017 General Chair Bhavani Thuraisingham, University of Texas at Dallas. "This is the highest number of attendees so far for an ACM CCS held in North America. At ACM CCS, our aim is to provide a platform for advancing cutting-edge ideas and research in the field of information security from all around the world."

2017 ACM CCS Highlights

Keynote Address: ***Security and Machine Learning***
David Wagner, University of California, Berkeley
Machine learning has seen increasing use for a wide range of practical applications. Recent research suggests that modern machine learning methods are fragile and easily attacked, which raises concerns about their use in security-critical settings. Wagner will explore several attacks on machine learning and will survey directions for making machine learning more robust against attack.

Selected Research Papers

- **Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2**
  Mathy Vanhoef and Frank Piessens, KU Leuven, imec-DistriNet
  All protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. In this

paper, the authors demonstrate that the 4-way handshake is vulnerable to a key reinstallation attack. A successful attack is achieved by manipulating and replaying handshake messages. The authors also demonstrate that every Wi-Fi device is vulnerable to some variant of these attacks.

- **Automated Crowdturfing Attacks and Defenses in Online Review Systems**
  Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, Ben Zhao, University of Chicago
  Malicious crowdsourcing forums are gaining traction as sources of spreading misinformation online; but are limited by the costs of hiring and managing human workers. In this paper, the authors identify a new class of attacks that leverage deep learning language models (recurrent neural networks) to automate the generation of fake online reviews of products or services. Using Yelp reviews as an example platform, the authors show how a two-phased customization attack can produce reviews that are indistinguishable by state-of-the-art statistical detectors.

- **The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli**
  Matus Nemec, Petr Svenda, Dusan Klinec, Vashek Matyas, Masaryk University Marek Sys, Masarykova University
  The authors discovered a vulnerability in the generation of RSA keys used by a software library adopted in cryptographic smartcards, security tokens and other secure hardware chips. Manufactured by Infineon Technologies, AG allows for a practical factorization attack, in which the attacker computes the private part of an RSA key. The attack is feasible for commonly used key lengths, including 1024 and 2048 bits, and affects chips manufactured as early as 2012, that are now commonplace.

- **How Unique Is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services**
  Rebekah Overdorf, Rachel Greenstadt, Drexel University, Marc Juarez, KU Leuven, Claudia Diaz, Gunes Acar, Princeton University
  Recent studies have shown that Tor onion (hidden) service websites are particularly vulnerable to website fingerprinting attacks due to their limited number and sensitive nature. In this work we present a multi-level feature analysis of onion site fingerprintability, considering three state-of-the-art website fingerprinting methods and 482 Tor onion services, making this the largest analysis of this kind completed on onion services to date.

- **Economic Factors of Vulnerability Trade and Exploitation: Empirical Evidence from a Prominent Russian Cybercrime Market**
  Luca Allodi, Eindhoven University of Technology
  Cybercrime markets support the development and diffusion of new attack technologies, vulnerability exploits, and malware. Whereas the revenue streams of cyber attackers have been studied multiple times in the literature, no quantitative account currently exists on the economics of attack acquisition and deployment. This understanding is critical to characterize the production of (traded) exploits, the economy that drives it, and its effects on the overall attack scenario. In this paper, Allodi provides an empirical investigation of the economics of

vulnerability exploitation, and the effects of market factors on likelihood of exploit. His data is collected first-hand from a prominent Russian cybercrime market where the trading of the most active attack tools reported by the security industry occurs.

- **DolphinAttack: Inaudible Voice Commands**
  Guoming Zhang, Chen Yan, Xiaoyu Ji, Taimin Zhang, Tianchen Zhang, Wenyuan Xu, Zhejiang University
  Various systems have turned into voice controllable systems (VCS) and systems such as Siri or many voice-controllable Google products are becoming increasingly popular. This makes VCS vulnerable to hidden voice commands. This presentation will show a few proof-of-concept attacks, which include activating Siri to initiate a FaceTime call on iPhone, activating Google Now to switch the phone to the airplane mode, and even manipulating the navigation system in an Audi automobile. Researchers will also propose hardware and software defense solutions, including detection of DolphinAttack by classifying the audios using supported vector machine, and redesigning VCS to become resilient to inaudible voice command attacks.

- **SGX-BigMatrix: A Practical Encrypted Data Analytic Framework with Trusted Processors**
  Fahad Shaon, Murat Kantarcioglu, Zhiqiang Lin, Latifur Khan, University of Texas at Dallas
  Recently, using secure processors for trusted computing in the cloud has attracted a lot of attention. Over the past few years, efficient and secure data analytic tools (e.g., map-reduce framework, machine learning models, and SQL querying) that can be executed over encrypted data using trusted hardware have been developed. However, these prior efforts do not provide a simple, secure and high level language-based framework that is suitable for enabling generic data analytics for non-security experts who do not understand concepts such as "oblivious execution." In this paper, the authors provide such a framework that allows data scientists to perform the data analytic tasks with secure processors using a Python/Matlab-like high-level language.

- **Concurrency and Privacy with Payment-Channel Networks**
  Giulio Malavolta, Friedrich-Alexander University Erlangen Nuernberg; Pedro Moreno-Sanchez and Aniket Kate, Purdue University; Matteo Maffei, TU Wien; Srivatsan Ravi, University of Southern California
  Permissionless blockchain protocols such as Bitcoin are inherently limited in transaction throughput and latency. Current efforts to address this issue focus on off-chain payment channels that can be combined in a Payment-Channel Network (PCN) to enable an unlimited number of payments without requiring access to the blockchain other than to register the initial and final capacity of each channel. While this approach allows for low latency and high throughput of payments, it raises several privacy concerns as well as technical challenges related to the inherently concurrent nature of payments. In this paper, the authors lay the foundations for privacy and concurrency in PCNs, presenting a formal definition in the Universal Composability framework as well as practical and provably secure solutions.

- **Machine Learning Models that Remember Too Much**
  Congzheng Song, Cornell University, Thomas Ristenpart, Vitaly Shmatikov,
  Cornell Tech
  Machine learning (ML) is becoming a commodity. Numerous ML frameworks and services are available to data holders who are not ML experts but want to train predictive models on their data. It is important that ML models trained on sensitive inputs (e.g., personal images or documents) not leak too much information about the training data. The authors present algorithms which create models that have high predictive power yet allow accurate extraction of subsets of their training data.

- **Viden: Attacker Identification on In-Vehicle Networks**
  Kyong-Tak Cho, Kang G. Shin, University of Michigan
  There are various proposed defense schemes, which can determine the presence of an attack on an in-vehicle network. However, all of them fail to identify which electronic control unit (ECU) actually mounted the attack. Clearly, pinpointing the attacker ECU is critical for fast/efficient forensic, isolation, security patch, etc. To meet this need, researchers propose a novel scheme, called Viden (voltage-based attacker identification), which can identify the attacker ECU by measuring and utilizing voltages on the in-vehicle network.

Pre- and Post-Conference Workshops (partial list)

Click here for a full list of conference workshops

Moving Target Defense (MTD)

The static nature of current computing systems makes them easy to attack. The idea of moving-target defense is to make systems dynamic and therefore harder to explore and predict. This workshop seeks to bring together researchers from academia, government, and industry to discuss the latest research efforts in moving-target defense.

Managing Insider Security Threats (MIST)

According to a recent Gartner Research Report, information leakage caused by insiders who are legally authorized to have access to some corporate information is increasing dramatically. The objective of this workshop is to showcase the most recent challenges and advances in security technologies and management systems to prevent leakage of organizations' information caused by insiders.

Women in Cyber Security (CyberW)

As gender imbalance continues in the field of cybersecurity, this workshop will bring together all underrepresented cybersecurity professionals, students, and researchers to engage in a vibrant security and privacy discussion. In addition, it will provide opportunities for the participants to network, as well as share career development experiences.

Internet of Things Security and Privacy (IoT S&P)

Given the increasing number of attacks and information leaks, IoT device manufactures, cloud providers, and researchers are working to design systems to secure and control the flow of information between devices, to detect new vulnerabilities, and to provide security and privacy within the context of the user and the devices. This workshop will bring together academic and industry researchers from the security and communication communities to design, measure, and analyze secure and privacy enhancing systems for IoT devices.

Artificial Intelligence and Security (AISec)

AISec brings together diverse researchers in security, privacy, AI, and machine learning, to develop the fundamental theory and practical applications supporting the use of machine learning for security and privacy. The key topics discussed as part of this work include learning in game-theoretic adversarial environments, privacy-preserving learning, and use of sophisticated new learning algorithms in security.

Tutorials (Partial List)

Click here for a full list of conference tutorials

- **Private Information Retrieval** by Ryan Henry (Indiana University)
- **Web Tracking Technologies and Protection Mechanisms** by Nataliia Bielova (Inria, France)
- **Cliptography: Post-Snowden Cryptography** by Qiang Tang (New Jersey Institute of Technology), Moti Yung (Snap Inc/Columbia University)

Additional papers, tutorials, and demonstrations will be presented throughout the multi-day conference. For a complete list of papers and a full schedule of activities, please visit: https://www.sigsac.org/ccs/CCS2017/.

About ACM SIGSAC

The ACM Special Interest Group on Security, Audit and Control's (SIGSAC) mission is to develop the information security profession by sponsoring high quality research conferences and workshops. SIGSAC conferences address all aspects of information and system security, encompassing security technologies, secure systems, security applications, and security policies.

About ACM

ACM, the Association for Computing Machinery (www.acm.org**),** is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###