NEWS RELEASE

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

MAJOR CONFERENCE EXPLORES CHALLENGES AND OPPORTUNIES IN CYBERSECURITY

CCS 2019 Program Addresses Security in Variety of Environments, Including Cloud, IoT, Social Media and Elections

New York, NY, October 31, 2019—The Association for Computing Machinery's Special Interest Group on Security, Audit and Control (ACM SIGSAC) will hold its flagship annual Conference on Computer and Communications Security (CCS 2019) on November 11-15 in London, United Kingdom. Now in its 26th year, CCS presents the leading scientific innovations in all practical and theoretical aspects of computer and communications security and privacy.

"As new types of computing technologies emerge, corresponding cybersecurity challenges appear in turn," said CCS 2019 Program Co-chair XiaoFeng Wang of Indiana University. "This year's CCS 2019 is where the world's leading security researchers and practitioners will convene to solve today's and tomorrow's challenges facing not only the computing field, but much of society."

Added CCS 2019 Program Co-chair Jonathan Katz of George Mason University, "This year's CCS program features more than 100 research papers and a robust schedule of presentations addressing systems security, cryptography, network security, privacy, and more. These papers represent many of the most striking recent advances in cybersecurity from academic and industry researchers."

2019 CCS HIGHLIGHTS

Keynotes

"The Need for Hardware Roots of Trust"
Ingrid Verbauwhede, Katholieke Universiteit Leuven, Flanders, Belgium
Electronics are shrinking and penetrating all aspects of our lives, from IoT devices, to self-driving cars, and to wearable health-sensing technology. Adding security and cryptography to these resource-constrained devices is a considerable challenge. Hardware roots of trust is at the foundation upon which software and cryptographic security protocols are built. This presentation will focus on the design methods for hardware roots of trust in general and more specifically on Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNG), two essential roots of trust.

“Hardware-Assisted Trusted Execution Environments — Look Back, Look Ahead”
Nadarajah Asokan, University of Waterloo, Waterloo, Ontario, Canada
Over the last two decades, hardware-based isolated execution environments, commonly known as “trusted execution environments” or TEEs, have become widely deployed. However, concerns about vulnerabilities, and potential for abuse have been persistent and have recently become increasingly pronounced. This talk will review the history of (mobile) TEEs, what motivated their design and large-scale deployment, and how they have evolved during the last two decades. It will also discuss some of their shortcomings and potential approaches for overcoming them. This talk will also explore other types of hardware security primitives that are being rolled out by processor manufacturers and the opportunities they offer for securing computing.

Best Paper Award
"Where Does It Go? Refining Indirect-Call Targets with Multi-Layer Type Analysis"
Kangjie Lu and Hong Hu, Georgia Institute of Technology
System software commonly uses indirect calls to realize dynamic program behaviors. However, indirect-calls also bring challenges to constructing a precise control-flow graph that is a standard prerequisite for many static program-analysis and system-hardening techniques. In this paper, the authors propose a new approach, namely Multi-Layer Type Analysis (MLTA), to effectively refine indirect-call targets for C/C++ programs. MLTA relies on an observation that function pointers are commonly stored into objects whose types have a multi-layer type hierarchy; before indirect calls, function pointers will be loaded from objects with the same type hierarchy “layer by layer.”

Research Papers (Partial List)
For a full list of papers, visit the CCS 2019 accepted papers page.

“Principled Unearthing of TCP Side Channel Vulnerabilities”
Yue Cao, Zhongjie Wang, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, University of California, Riverside; Paul Yu, US Army Combat Capabilities Development Command Army Research Laboratory
Recent work has showcased the presence of subtle TCP side channels in modern operating systems, that can be exploited by off-path adversaries to launch pernicious attacks such as hijacking a connection. Unfortunately, most work to date is on the manual discovery of such side channels, and patching them subsequently. In this work the authors ask “Can we develop a principled approach that can lead to the automated discovery of such hard-to-find TCP side-channels?” The authors introduce a tool that they call SCENT (for Side Channel Excavation Tool) that addresses these challenges in a mostly automated way.

"Seems Legit: Automated Analysis of Subtle Attacks on Protocols that use Signatures"
Dennis Jackson, University of Oxford; Cas Cremers, CISPA Helmholtz Center for Information Security; Katriel Cohn-Gordon, Independent Scholar; Ralf Sasse, ETH Zurich
The standard definition of security for digital signatures—existential unforgeability—does not ensure certain properties that protocol designers might expect. In this paper, the authors give a hierarchy of new symbolic models for signature schemes that captures these subtleties, and thereby allow the

analysis of (often unexpected) behaviors of real-world protocols that were previously out of reach of symbolic analysis. The authors implement their models in the Tamarin Prover, yielding the first way to perform these analyses automatically, and validate them on several case studies.

"Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings"
Mary Maller, University College London; Sean Bowe, Electric Coin Company; Markulf Kohlweiss, University of Edinburgh; Sarah Meiklejohn, University College London
Ever since their introduction, zero-knowledge proofs have become an important tool for addressing privacy and scalability concerns in a variety of applications. The authors describe a zero-knowledge SNARK, Sonic, which supports a universal and continually updatable structured reference string that scales linearly in size. They also describe a generally useful technique in which untrusted "helpers" can compute advice that allows batches of proofs to be verified more efficiently.

"Analyzing Subgraph Statistics from Extended Local Views with Decentralized Differential Privacy"
*Haipei Sun***,** *Qatar Computing Research Institute, Stevens Institute of Technology; Xiaokui Xiao, National University of Singapore; Issa Khalil, Qatar Computing Research Institute; Yin Yang, Hamad Bin Khalifa University; Zhan Qin, Zhejiang University; Hui (Wendy) Wang, Stevens Institute of Technology; Ting Yu, Qatar Computing Research Institute*
Many real-world social networks are decentralized in nature, and the only way to analyze such networks is to collect local views of the social graph from individual participants. Since local views may contain sensitive information, it is often desirable to apply differential privacy in the data collection process, which provides strong and rigorous privacy guarantees. In many practical situations, the local view of a participant contains connections of neighbors, which are private and sensitive for the neighbors, but not directly so for the participant. The authors study two fundamental problems related to such extended local views: how do we correctly enforce differential privacy for all participants, and how can the data collector obtain accurate estimates of global graph properties?

"How to (Not) Share a Password: Privacy Preserving Protocols for Finding Heavy Hitters with Adversarial Behavior"
Moni Naor, Weizmann Institute of Science; Benny Pinkas, Bar Ilan University; Eyal Ronen, Tel Aviv University
Bad choices of passwords were and are a pervasive problem. Users choosing weak passwords do not only compromise themselves, but the whole ecosystem. For example, common and default passwords in IoT devices were exploited by hackers to create botnets and mount severe attacks on large Internet services, such as the Mirai botnet DDoS attack. The authors present a method to help protect the Internet from such large-scale attacks. Their method enables a server to identify popular passwords (heavy hitters), and publish a list of over-popular passwords that must be avoided.

Pre- and Post-Conference Workshops (partial list)
For a full list of workshops, visit the CCS 2019 workshops page.

2019 Cloud Computing Security Workshop (CCSW)
CCSW, is the world’s premier forum bringing together researchers and practitioners in all security aspects of cloud-centric and outsourced computing, has historically acted as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds. Among the many topics to be addressed in the workshop are secure cloud resource virtualization mechanisms, secure data management outsourcing practical privacy and integrity mechanisms for outsourcing, and the foundations of cloud-centric threat models.

18th Workshop on Privacy in the Electronic Society (WPES)
This workshop discusses the problems of privacy in the global interconnected society and possible solutions. The increased power and interconnectivity of computer systems available today create the ability to store and process large amounts of data, resulting in networked information accessible from anywhere at any time. It is becoming easier to collect, exchange, access, process, and link information. This global scenario has inevitably resulted in an increasing degree of awareness with respect to privacy.

5th ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)
CPS-SPC aims to be the premier workshop for research on security of Cyber-Physical Systems (such as medical devices, manufacturing and industrial control, robotics and autonomous vehicles). These systems are usually composed of a set of networked agents, including sensors, actuators, control processing units, and communication devices. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications in areas such as medical devices, autonomous vehicles, and smart infrastructure.

12th ACM Workshop on Artificial Intelligence and Security (AISec)
For more than a decade, AISec has been the primary meeting place for researchers working at the intersection of artificial intelligence, machine learning, deep learning, security and privacy. The workshop has favored the development of fundamental theory and practical applications supporting the use of machine learning for security and privacy. Its main topics include adversarial and privacy-preserving learning, and novel learning algorithms for security.

2nd Workshop on the Internet of Things Security and Privacy (IoT S&P)
The workshop aims to bring together researchers from academia, government, and industry to discuss the challenges and solutions regarding practical and theoretical aspects of IoT security and privacy. The Internet of Things (IoT) is believed to be the next generation of the Internet and has deeply influenced our daily lives. While bringing convenience to our lives, IoT also introduces potential security hazards. Since increasing IoT devices directly process user-generated data, once compromised, users or even the entire smart society can be at risk.

1st Workshop on Cyber-Security Arms Race (CYSARM)
The goal of CYSARM workshop is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various facets and trade-offs of cybersecurity and how new security technologies and algorithms might impact the security of existing or future security models.

About SIGSAC
The ACM Special Interest Group on Security, Audit and Control's 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, is the world's largest educational and scientific computing society, uniting 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.

###