NEWS RELEASE

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

LEADING CYBERSECURITY CONFERENCE PLANS BLOCKBUSTER PROGRAM FOR 25TH ANNIVERSARY

CCS 2018 Program Includes Latest Innovations/Interdisciplinary Approaches

New York, NY, October 3, 2018 – 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 2018) from October 15-19 in Toronto, Canada. Now in its 25th year, CCS presents the leading scientific innovations in all practical and theoretical aspects of computer and communications security and privacy.

"In today's world, computer security is one of the most vital concerns, for individuals, for companies and for entire nations," said CCS 2018 General Co-Chair Mohammad Mannan of Concordia University. "We are proud of the reputation CCS has garnered for being a venue where the leading security researchers and practitioners convene and address the field's most pressing challenges." Added CCS 2018 General Co-Chair David Lie of the University of Toronto, "We expect record-breaking attendance for our milestone 25th anniversary conference. This year's program also reflects the CCS tradition of exploring the exciting frontiers of this field and incorporating interdisciplinary perspectives."

2018 CCS HIGHLIGHTS

Keynotes

"Achieving Meaningful Privacy in Digital Systems"
Helen Nissenbaum, Cornell Tech
Across a range of subfields, computer scientists and engineers have responded to society's call to safeguard privacy through technology, yielding scientific progress and impressive innovation. In her keynote, Nissenbaum argues that contextual integrity (CI) could serve as a much needed bridge between technical approaches and ethical and policy approaches. She will also identify promising directions for future work based on interesting technical applications of CI that have already emerged.

“Advanced Cryptography: Promise and Challenges”

Shai Halevi, IBM T.J. Watson Research Center

Halevi will discuss "advanced cryptography," namely cryptographic techniques beyond communication security, including topics such as zero knowledge, secure multi-party computation, homomorphic encryption, and the like. He will make the case that advanced cryptography is (a) needed, (b) must be fast enough to be useful, and (c) not "generally usable" yet.

Selected Research Papers

“Tiresias: Predicting Security Events Through Deep Learning”

Yun Shen, Symantec; Enrico Mariconti, University College London; Pierre-Antoine Vervier, Symantec; Gianluca Stringhin, University College London

With the increased complexity of modern computer attacks, there is a need for defenders not only to detect malicious activity as it happens, but also to predict the specific steps that will be taken by an adversary when performing an attack. The authors present Tiresias, a system that leverages recurrent neural networks (RNNs) to predict future events on a machine, based on previous observations.

“Threat Intelligence Computing”

Xiaokui Shu, Frederico Araujo, Douglas Schales, Marc Stoecklin, Jiyong Jang, Heqing Huang, and Josyula Rao, IBM Research

Today, threat hunters and cyber investigators are challenged by the sheer volume of data arising from computer systems and networks. To discover nefarious cyber threats lurking in the IT environment, they sift through millions of records and correlate across different data sources to potentially identify early symptoms and validate hypotheses. This paper introduces a novel paradigm, called threat intelligence computing, to tremendously speed up this time-consuming task. For the first time, the authors have formalized threat discovery as a graph computing problem across system events, network traces, and security knowledge. The paradigm enables an efficient programming model to solve threat discovery problems, equipping threat hunters with a suite of potent new tools for agile formulation of threat hypotheses, automated evidence mining, and interactive data inspection capabilities.

“How You Get Bullets in Your Back: A Systematical Study about Cryptojacking in the Real World”

Yuhong Nan, Zhibo Zhang, Min Yang ,Yuan Zhang, Fudan University; Zhiyun Qian, UC Riverside; Haixin Duan, Tsinghua University

In cryptojacking, an increasingly common phenomenon, hackers use someone else’s computer to mine cryptocurrency. Unsuspecting victims typically infect their computers with the cryptocode by clicking on an infected link or online ad with Javascript code that auto-executes once loaded into the victim’s browsers. After infection, victims are still unaware of the cryptojacking, as the code runs undetected in the background. The authors offer a first in-depth study of cryptojacking and propose CMTracker, a behavior-based detector with two runtime profilers for automatically tracking cryptocurrency mining scripts and their related domains. Their approach successfully discovered 2,770 unique cryptojacking samples from 853,936 popular web pages, including 868 among the top 100K in Alexa list of top websites around the globe.

"Voting: You Can't Have Privacy Without Individual Verifiability"
Véronique Cortier, Joseph Lallemand, Inria, Université de Lorraine
Electronic voting typically aims at two main security goals: vote privacy and verifiability. These two goals are often seen as antagonistic and some national agencies even impose a hierarchy between them: first privacy, and then verifiability as an additional feature. Verifiability typically includes individual verifiability (a voter can check that her ballot is counted); universal verifiability (anyone can check that the result corresponds to the published ballots); and eligibility verifiability (only legitimate voters may vote). The authors show that actually, privacy implies individual verifiability.

Pre- and Post-Conference Workshops (partial list)

Privacy in the Electronic Society
Over the last several years, there has been a massive increase in the collection, sharing and analysis of personal data. This workshop presents novel research on all theoretical and practical aspects of electronic privacy, as well as experimental studies of fielded systems. Other communities, such as law and business, are also invited to present their perspectives on technological issues.

Artificial Intelligence and Security
Artificial intelligence (AI), and machine learning, in particular, provide a set of useful analytic and decision-making techniques that are being leveraged by an ever-growing community of cybersecurity practitioners. The Artificial Intelligence and Security workshop (AISec) is the primary meeting for diverse researchers in security, privacy, AI, and machine learning, and as a venue to develop the fundamental theory and practical applications supporting the use of machine learning for security and privacy.

Cyber-Physical Systems Security and Privacy
Cyber-physical systems (CPS), such as power grids, medical devices, and autonomous vehicles, are safety-critical—in that their failure can cause irreparable harm to people and even nations at large. Securing CPS is therefore vitally important. The CPS workshop presents the latest research and practical applications, as well as interdisciplinary approaches to CPS security.