CRESP

Center for Research and Education in Cyber Security and Privacy

CENTER LAUNCH, WORKSHOP & KICK OFF

Friday, April 27, 2018 | 8:00 a.m. - 5:30 p.m. | Alumni & Visitors Center

AGENDA

8:00 a.m. **Continental Breakfast**

8:45 a.m. **Opening Remarks**
Chinya Ravishankar, Associate Dean of Research and Graduate Education, Marlan and Rosemary Bourns College of Engineering
Heng Yin, Director, CRESP

9:00 a.m. **Keynote by Xiaofeng Wang**
James H. Rudy Professor of Computer Science and Engineering, Indiana University Bloomington
Title: System Security Research: From Discovery to Innovation

10:00 a.m. **Short Talks**
Zhiyun Qian - Nael Abu-Ghazaleh - Hamed Mohesenian-Rad

11:00 a.m. **Break**

11:30 a.m. **Xiaoning Li**
Chief Security Architect, Alibaba Cloud
Title: Security Challenges in Public Trusted Cloud

12:15 p.m. **Lunch and Poster Session**

2:00 p.m. **Keynote by Stephen Chong**
Gordon McKay Professor of Computer Science, Harvard University
Title: Programming Languages for Security

3:00 p.m. **Short Talks**
Silas Richelson - Christophe Hauser, ISI/USC - Juston Moore, LANL

4:00 p.m. **Break**

4:30 p.m. **Fire-Side Chat with Shomit Ghose**
Partner, IT, ONSET Ventures

5:20 p.m. **Poster Award and Closing Remarks**

UCR | Marlan and Rosemary Bourns College of Engineering

CRESP

Center for Research and Education in Cyber Security and Privacy

SPEAKER BIOS & PROGRAM DESCRIPTIONS

9:00 a.m. - Keynote by Xiaofeng Wang

Dr. XiaoFeng Wang is a James H. Rudy Professor of Computing at Indiana University, Co-director of IU's Center for Security and Privacy in Informatics, Computing and Engineering, and the Vice Chair of the ACM SIGSAC (special interest group on security, audit and control). He is also a PC Co-Chair of the 2018 ACM Conference on Computer and Communications Security (CCS). Dr. Wang received his Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University. He is considered to be one of the most prominent system security researchers, among the most productive authors at leading security venues (#5 among over 6,000 authors in the past 18 years according to online statistics). Dr. Wang is known for his high-impact research on security analysis of real-world systems and biomedical data privacy. Particularly the projects he led on payment and single-sign- on API integrations, Android and iOS security and IoT protection have changed the way the industry built these systems. Also he is a pioneer researcher on human genome privacy and a co-founder of the iDASH Genome Privacy Competition that bridges the frontline security and cryptography research and the real-world demands for biomedical data sharing and computing protection. More recently, he is actively working on Data-Centric Intelligent Security, Cybercrimes, Hardware-support Protection and IoT Security. For his work, Dr. Wang has received numerous awards, including the Award for Outstanding Research in Privacy Enhancing Technologies (the PET Award) and the Best Practical Paper Award at the 32nd IEEE Symposium on Security and Privacy. His research has been extensively reported by the public media, including CNN, MSNBC, Forbes, Slashdot, Nature News, etc.

System Security Research: From Discovery to Innovation

Innovations in security research often come from the curiosity about how rules can be bent. The interdisciplinary nature of system security further presents the researcher a vast space to explore such opportunities. In this talk, I will share our experience in finding and understanding security weaknesses on the technology frontier, demonstrating how big questions can be asked to help discover subtle but fundamental security problems inside modern computing systems, and how such findings can reshape system security designs, bringing forth new techniques, new research directions. More specifically, using mobile and IoT as examples, I will show that discovery and analysis of their surprising side channel weaknesses (which can be exploited by even the apps without permissions to expose one's identity, locations, health information, etc.) questions the "security by construction" designs of these systems, identifying what need to be addressed to better protect them. Further to be presented is the preliminary effort to automate such a discovery process, by leveraging the knowledge automatically recovered from documents to guide detection of security-critical vulnerabilities. Finally, I will highlight the key insights of system security research and discuss the directions that might impact the development of new security technologies in the years to come.

11:30 a.m. - Xiaoning Li

Xiaoning Li is Chief Security Architect at Alibaba Cloud. Previously he was a security researcher and architect at Intel Labs. Focused on analyzing/detecting/preventing 0 day/malware with existing/new processor features. For the past 10+ years, his work has been focusing on both hardware/software security system co-design and advanced threat research. Xiaoning holds 20+ grant/filling patents in security areas including processor/system security and has published more than 20+ conference/invited talks including BlackHat, CanSecWest, ShmooCon, Source etc.

The Security Challenges in Public Trusted Cloud

Cloud is the most important technology trend now. How to build trust with customers is mission critical to bring sensitive data into cloud. Trusted cloud is one of the approaches to solve this problem, but current trusted cloud is not enough. In this talk, I will present the security challenges in current trusted cloud and comprehensively discuss trusted cloud in future.

2:00 p.m. - Stephen Chong

Stephen Chong is a Gordon McKay Professor of Computer Science in the Harvard John A. Paulson School of Engineering and Applied Sciences. Steve's research focuses on programming languages, information security, and the intersection of these two areas. He is the recipient of an NSF CAREER award, an AFOSR Young Investigator award, and a Sloan Research Fellowship. He received a PhD from Cornell University, and a bachelor's degree from Victoria University of Wellington, New Zealand.

Programming Languages for Security

Formal methods are the only reliable way to achieve security and privacy in computer systems. Formal methods, by modeling computer systems and adversaries, can prove that a system is immune to entire classes of attacks (provided that the assumptions of the model are satisfied). Programming languages provide a great basis for formal methods for security, in at least two ways. First, the field of programming languages has a rich history of formal approaches, and so has a wealth of techniques and tools to model computer systems and to prove properties about computer systems. Second, since we build systems using programming languages, formal language-based techniques for reasoning about the security of systems often lead to practical mechanisms to achieve security. In this talk, I'll present a project that takes this language-based approach to security: it defines and proves a notion of security in a language-based model of computer systems, and develops a practical mechanism from these models. Specifically, we will consider how to provide strong information security guarantees in concurrent settings. We extend the X10 concurrent programming language with coarse-grained information-flow control. Central to X10 concurrency abstractions is the notion of a place: a container for data and computation. By restricting what information may influence data and computation at a place, we can prevent dangerous information flows, including information flow through covert scheduling channels. For many common patterns of concurrency, our security mechanisms impose no restrictions.

4:30 p.m. - Fireside Chat with Shomit Ghose

Shomit's data-centric vision of the future has helped lead ONSET's investments in software. Prior to entering venture capital, he was a startup software entrepreneur with a career of operating excellence spanning 19 years. Shomit's startup roles included three highly successful IPOs as SVP of Operations at Tumbleweed Communications; VP of Worldwide Services at BroadVision; and software engineer at Sun Microsystems. He was also CEO and board member of ONSET portfolio company, Truviso, for two years leading to its acquisition by Cisco Systems. At ONSET since 2001, Shomit has represented ONSET on the boards of Adara, HyperGrid, Imanis Data, Pancetera (acquired by Quantum), Polymorph, Truviso, Vidder and Vindicia (acquired by Amdocs.) In his private life he has been committed to coaching girls' sports for many years in softball, high-level club soccer, and club and high school varsity and junior varsity lacrosse. At the age of 15, Shomit was awarded two academic scholarships to the University of California, Berkeley, and graduated with a degree in Computer Science. He serves on the advisory boards of UC Berkeley College of Engineering's Sutardja Center, Innovation Center Denmark's ScaleIT program, and the Lundbeck Foundation Clinical Research Fellowship Program.

SHORT TALKS

10:00 a.m. - Zhiyun Qian

Dr. Zhiyun Qian is an assistant professor at University of California, Riverside. His research interest is on system and network security, including vulnerability discovery, Internet security (e.g., TCP/IP), Android security, side channels. He has published more than a dozen papers at the top security conferences including IEEE Security & Privacy, ACM CCS, USENIX Security, and NDSS. His work has resulted in real- world impact with security patches applied in Linux kernel, Android, and firewall products. His work on TCP side channel attacks won the most creative idea award at GeekPwn 2016 and winner award at GeekPwn 2017. His work is currently supported by 8 NSF grants (including the NSF CAREER Award) and two industrial gifts.

When TCP Meets Side Channels

In this talk, I will discuss the history of off-path TCP attacks and their relationship with side channels. I will demonstrate the multitude of different ways realistic and powerful off-path TCP attacks can be conducted using a variety of side channels. Very recently, we show that a pure off-path attack can be carried out against Linux hosts without being able to run any malicious code on either the client or server. Essentially the attacker can infer if any two arbitrary hosts on the Internet are communicating using a TCP connection. Further, if the connection is present, such an off-path attacker can also infer the TCP sequence numbers in use, from both sides of the connection; this in turn allows the attacker to cause connection termination and perform data injection attacks. I will conclude by giving the insights on how to systematically discover and fix such problems.

SHORT TALKS

10:00 a.m. - Nael Abu-Ghazaleh

Nael Abu-Ghazaleh is a Professor in the CSE and ECE departments at the University of California, Riverside. His research looks at the role of computer architecture in system security including hardware vulnerabilities, secure architecture design, and hardware acceleration of security mechanisms.

Microarchitecture Side Channel Attacks and Their Role in Meltdown/Spectre

The architectural components of modern CPUs such as caches, branch predictors, memory ports, are shared among multiple executing programs for efficiency. This opens the door for side channel attacks where an attacker monitors the behavior of these shared structures to infer sensitive information about the victim. For example, in a cache-based side channel attack, the attacker can detect that the victim accessed a particular cache line if it replaces data that the attacker placed there, causing a cache miss. I will describe two recent side channel attacks on the branch predictor unit that also have the side effect of polluting the state this predictor. I will also discuss how one of these attacks is leveraged to mount the recent Spectre (variant 2) speculation attack.

CRESP

Center for Research and Education in Cyber Security and Privacy

SPEAKER BIOS & PROGRAM DESCRIPTIONS

SHORT TALKS

10:00 a.m. - Hamed Mohsenian-Rad

Dr. Hamed Mohsenian-Rad is an Associate Professor of Electrical and Computer Engineering at UC Riverside. He is the founding Director of the UC-National Lab Center for Power Distribution Cyber Security, a new $4 million cyber security research initiative across four UC campuses and two DoE National Labs. Dr. Mohsenian-Rad also serves as the Associate Director of the Winston Chung Global Energy Center, an endowed research center at UC Riverside. His research interests include monitoring, control, and physics-aware cyber-security of critical infrastructure, smart grids, and smart cities. He has received the National Science Foundation (NSF) CAREER Award, a Best Paper Award from the IEEE Power and Energy Society (PES) General Meeting, and a Best Paper Award from the IEEE International Conference on Smart Grid Communications. Two of his papers are currently ranked as the two most cited journal articles in the field of smart grids. Dr. Mohsenian-Rad received his Ph.D. in Electrical and Computer Engineering from the University of British Columbia, Vancouver, Canada in 2008. He currently serves as an Editor of the IEEE Transactions on Smart Grid, an Editor of the IEEE Power Engineering Letters, a Vice-Chair of the IEEE Smart Grid Communications Emerging Technical Subcommittee, and a co-Chair of the IEEE Power and Energy Society Working Group on Big Data Access and Research Integration. Dr. Mohsenian-Rad received the UC Riverside Bourns College of Engineering Distinguished Teaching Award in 2017.

Physics-Aware Cyber Security in Power Grids

The recent advancements in sensing, communication, and control capabilities across the electric power infrastructure have the potential to enormously enhance the performance of the power grids, but at the cost of increased vulnerabilities to deliberate attacks and accidental failures, threatening the grid's functionality and reliability. The cybersecurity of the power grid is different from the typical practice of cybersecurity in the IT sector. Due to the inter-connected nature of the electric grid, an attack against one sector of the grid can create physical cascading effects, affecting other sectors of the grid and even affecting other infrastructures, such as telecommunications and water networks. Recovery can be a long and extremely costly process. Safety is a crucial requirement because certain failures can lead to fire or explosions. In this talk, we briefly explore the concept of physics-aware cybersecurity, which can be thought of as an additional layer of security system that will be integrated with cyber-based security measures. Such reinforced cybersecurity strategy can monitor the entire or a selected subset of measurements and commands traffic, even those that are from authorized users, in order to detect such events, activities, or trajectories that may potentially move the system to an unsafe cyber and/or physical state. Accordingly, physics-aware cyber security is inherently a multi-disciplinary effort, spanning across computer science, data science, power systems, and control systems, among other fields.

CRESP

Center for Research and Education in Cyber Security and Privacy

SPEAKER BIOS & PROGRAM DESCRIPTIONS

SHORT TALKS

3:00 p.m. - Silas Richelson

Silas Richelson studies cryptography and complexity theory. His main research interests are in designing protocols which are secure against non-traditional adversaries which are more powerful than those normally considered in the realm of cryptography. He is an assistant professor here at UC Riverside, he joined in January 2018. Prior to this he was a postdoc in Boston with a joint appointment at MIT and BU, working with Vinod Vaikuntanathan and Ran Canetti. Prior to that he was a graduate student at UCLA, supervised by Rafi Ostrovsky.

How to Subvert Backdoored Excryption

In this work, we examine the feasibility of secure and undetectable point-to- point communication in a world where governments can read all the encrypted communications of their citizens. We consider a world where the only permitted method of communication is via a government-mandated encryption scheme, instantiated with government-mandated keys. Parties cannot simply encrypt ciphertexts of some other encryption scheme because citizens caught trying to communicate outside the government's knowledge (e.g., by encrypting strings which do not appear to be natural language plaintexts) will be arrested. The one guarantee we suppose is that the government mandates an encryption scheme which is semantically secure against outsiders: a perhaps reasonable supposition when a government might consider it advantageous to secure its people's communication against foreign entities. But then, what good is semantic security against an adversary that holds all the keys and has the power to decrypt? We show that even in the pessimistic scenario described, citizens can communicate securely and undetectably. In our terminology, this translates to a positive statement: all semantically secure encryption schemes support subliminal communication. Informally, this means that there is a two-party protocol between Alice and Bob where the parties exchange ciphertexts of what appears to be a normal conversation even to someone who knows the secret keys and thus can read the corresponding plaintexts. And yet, at the end of the protocol, Alice will have transmitted her secret message to Bob. Our security definition requires that the adversary not be able to tell whether Alice and Bob are just having a normal conversation using the mandated encryption scheme, or they are using the mandated encryption scheme for subliminal communication.

SHORT TALKS

3:00 p.m. - Christophe Hauser

Christophe Hauser is a research computer scientist at the Information Sciences Institute (ISI) of University of Southern California (USC). His research interests span across multiple areas of security, with a focus on binary program analysis, as well as OS and kernel security. Previously, he was a postdoctoral researcher at University of California, Santa Barbara, where he worked on building parts of the angr binary analysis framework. He received his Ph.D. in computer science from Supélec/University of Rennes (France) and Queensland University of Technology (Australia).

Retrofitting Security in Closed-Source Binary Programs

Despite the presence of increasingly sophisticated compiler-level verifications, testing frameworks and code audit tools, security bugs remain in the code of off-the- shelf software components. Unfortunately, software components presenting security risks may be developed and integrated in opaque, closed-source environments (e.g., as part of an embedded device's proprietary firmware). The process of automatically evaluating the security of software programs in such environments involves multiple challenges in terms of accuracy and scalability. We investigate solutions to address these challenges at scale based on lightweight heuristic-driven static analysis and symbolic execution at the binary level. Our initial focus is on memory corruption vulnerabilities caused by unsafe input parsing implementations.

SHORT TALKS

3:00 p.m. - Juston Moore

Juston Moore is a cybersecurity researcher in Los Alamos National Laboratory's Advanced Research for Cyber Systems group. Juston's research bridges statistics, machine learning, and information assurance. His work focuses on large-scale analytics for anomaly detection in unstructured data streams as well as cyber attack attribution.

Machine Learning in Adversarial Cyber Environments

The security industry is turning to machine learning to solve problems that have proven elusive with rule- based approaches, such as identification of obfuscated malware. A weakness of current machine learning systems is that false positives are uninterpretable. Analysts require interpretable alerts to quickly investigate alerts. I will describe work at LANL to address the interpretability gap in cyber security in two areas: malware authorship attribution and user behavior analytics.