IoT S&P 2017: First Workshop on Internet of Things Security and Privacy

Theophilus Benson
Brown University
tabenson@cs.brown.edu

Peng Liu
Penn State University
pliu@ist.psu.edu

Srikanth Sundaresan
Princeton University
srikanths@princeton.edu

Yuqing Zhang
University of Chinese Academy of Sciences, China
zhangyq@ucas.ac.cn

ABSTRACT

The First Workshop on Internet of Things Security and Privacy is held in Dallas, TX, USA on November 3, 2017, co-located with the ACM Conference on Computer and Communications Security (CCS). The workshop aims to address the security and privacy challenges of the emerging Internet-of-Things landscape. The workshop aims to bring together academic and industrial researchers, and to that end, we have put together an exciting program offering a a mix of current and potential challenges. The workshop will also features 12 papers, 4 posters, and an invited keynote.

KEYWORDS

Internet-of-Things; Security; Privacy

ACM Reference Format:
Theophilus Benson, Peng Liu, Srikanth Sundaresan, and Yuqing Zhang. 2017. IoT S&P 2017: First Workshop on Internet of Things Security and Privacy. In *Proceedings of CCS '17, October 30-November 3, 2017, Dallas, TX, USA, ,* 2 pages.
https://doi.org/10.1145/3133956.3137053

1 INTRODUCTION

The future of the Internet-of-Things is already upon us — a variety of sensors and devices are already available in the market, ranging from smart light bulbs to juicers, barbecues, and security systems. This has implications for privacy — what sort of information are these sensors collecting about users? — and security, with recent Internet-scale DDoS attacks caused by thousands of cheap, poorly patched devices.

Motivated by an increasing number of attacks and information leaks, IoT device manufactures, cloud providers, and researchers are working to design systems to secure to control the flow of information between devices, to detect new vulnerabilities; and to provide security and privacy within the context of user and the devices. While researchers continue to tackle IoT security and privacy, many questions remain open.

CCS '17, , October 30-November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3137053

Further, with the growing adoption of IoT devices, we will see a growth in the number of security and privacy issues. The goal of the First ACM CCS Workshop on IoT S&P is to 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.

2 SCOPE OF THE WORKSHOP

IoT S&P'17 encouraged the submission of previously unpublished, work-in-progress papers in the area of design, implementation, management, and deployment of secure and private IoT frameworks as well as measurement and analysis of the privacy and security of existing IoT devices and packages. The topics included the following:

- Security and privacy issues in IoT
- Network architectures and protocols for scalable, robust, secure, and privacy enhancing IoT
- Network services and management for IoT
- Measurement of IoT privacy leakage
- Measurement of Industrial IoT
- Usable security and privacy frameworks for home networks
- Threat Models and Attack Strategies in IoT
- Intrusion and Malware Detection
- Security Architectures for the IoT Stack
- System and Data Integrity
- Identity and access management in IoT
- Trustworthiness in IoT
- Secure Operating Systems in IoT
- Automated armoring and patching
- Cross-layer IoT security
- IoT ecosystem-level security analysis
- Clean-slate IoT security design

3 THE WORKSHOP

We received 30 submissions, of which we accepted 12 papers; a further four were invited to be presented as posters. The program was divided into four sessions; two for discussing existing IoT systems that requires urgent attention, one for defense against IoT hacks, and one discussing building blocks for next-gen defense. The workshop, held over one day, also included a keynote by Earlence Fernandes, a research associate at the University of Washington. Earlence's keynote, titled "Computer Security and Privacy for the

Physical World", discussed recent results in securing emerging IoT systems, and outlined directions of future research.

4 ORGANIZERS

Theophilus Benson, TPC co-chair, (Brown University, USA): received his BS from Tufts University, and his MS and PhD degrees from University of Wisconsin – Madison in 2012. Dr. Benson is an Assistant Professor of Computer Science at Brown University. Dr Benson's research focuses on solving practical networking and systems problems, with a focus on Software Defined Networking, data centers, clouds, and configuration management. To this end, his group works on developing abstractions, algorithms and frameworks for using programmable data planes (Software-Defined Networking) to improve the reliability, performance and security of enterprise, ISP, home networks, and networks in developing regions. Dr Benson has served on program committee for multiple workshops/conferences (SIGCOMM, IMC, CoNext, SoSR, SoCC, Usenix ATC, HotCloud, HotMB), the publicity chair for several workshops/conferences (CoNext'14 Workshop, SoSR'17) and as the Workshop Co-Chair for several successful workshops (HotMB'16, CoNext Workshop'15).

Peng Liu, General co-chair, (Penn State University, USA): received his BS and MS degrees from the University of Science and Technology of China, and his PhD from George Mason University in 1999. Dr. Liu is a Professor of Information Sciences and Technology, founding director of the Center for Cyber-Security, Information Privacy, and Trust, and founding director of the Cyber Security Lab at Penn State University. His research interests are in all areas of computer and network security. He has published a monograph and over 260 refereed technical papers. His research has been sponsored by NSF, ARO, AFOSR, DARPA, DHS, DOE, AFRL, NSA, TTC, CISCO, and HP. He has served as a program (co-)chair or general (co-)chair for over 10 international conferences (*e.g.*Asia CCS 2010) and workshops (*e.g.*, MTD 2016). He chaired the Steering Committee of SECURECOMM during 2008-14. He has served on over 100 program committees and reviewed papers for numerous journals. He is an associate editor for IEEE TDSC.

Srikanth Sundaresan, TPC co-chair, (Princeton University, USA): Srikanth's research interests include the design and measurements of networked systems with a focus on quality of experience for end users—including performance, privacy, and security. He has experience building large-scale IoT systems at Samsara Networks, and successful academic network monitoring systems, including BISmark and Lumen Privacy Monitor. He has served on program committees for IMC 2017, PAM 2016, and several workshops.

Yuqing Zhang, General co-chair, (University of Chinese Academy of Sciences, China) received his PhD in Cryptography from Xidian University, China. Dr. Zhang is a Professor of Computer Sciences and the Director of the National Computer Network Intrusion Protection Center at University of CAS. His research interests include network and system security, cryptography, and networking. He has published more than 100 research papers in many international journals and conferences, such as ACM CCS, IEEE Transactions on Parallel and Distributed Systems, and IEEE Transactions on Dependable and Secure Computing. His research has been sponsored by NSFC, Huawei, Qihu360 and Google. He has served as a program chair for over 5 international workshops (*e.g.*, SMCN-2017). He has been the PC member for more than 10 international conferences in networking and security, such as IEEE Globecom 16/17, IEEE CNS 17, and IFIP DBSec 17.

ACKNOWLEDGMENTS

We would like to acknowledge the authors who submitted their research to the conference, and also the program committee members who contributed to putting together the exciting program. We would also like to thank the keynote speakers, and the organizers of the CCS conference.