Sixth Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2016)

Long Lu
Stony Brook University
Stony Brook, NY, United States
long@cs.stonybrook.edu

Mohammad Mannan
Concordia University
Montreal, QC, Canada
m.mannan@concordia.ca

ABSTRACT

Mobile security and privacy issues are receiving significant attention from the research community. The SPSM workshop was created to provide a venue for researchers and practitioners interested in such issues to get together and exchange ideas. Following the success of the previous editions, we present the sixth edition of the workshop. It brings together the expertise of an international program committee, comprising of 22 mobile security experts from the academia and the industry. The workshop received 31 submissions (regular and short papers combined) from a diverge set of authors located in 19 countries.

1. MOTIVATION

Mobile devices such as smartphones and Internet tablets have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. For example, the widespread presence of information-stealing applications raises substantial security and privacy concerns. The operating systems supporting these new devices have both advantages and disadvantages with respect to security. On one hand, they use application sandboxing to contain exploits and limit privileges given to malware. On the other hand, they routinely collect and organize many forms of security- and privacy-sensitive information and make that information easily accessible to third-party applications.

2. TOPICS

Recognizing smartphone security and privacy as an emerging area, this workshop intends to provide a venue for interested researchers and practitioners to get together and exchange ideas. Topics of interest include (but are not limited to) the following subject categories:

- Device/hardware security
- OS/middleware security
- Application security
- Authenticating users to devices and services
- Mobile web browsers
- Usability
- Privacy
- Rogue application detection and recovery
- Vulnerability detection and remediation
- Secure application development
- Cloud support for mobile security
- Mobile device management
- Mobile ads
- Dual persona management and isolation

We also encourage novel paradigms and controversial ideas that are not on the above list. The workshop is to act as a venue for creative debate and interaction in security- and privacy-sensitive areas of computing and communication impacted by smartphones. We favor submissions that are radical, forward-looking, and open-ended, as opposed to mature work on the verge of conference or journal publication; in SPSM 2016, we reduced the page length requirement to encourage such submissions (e.g., 8–10 pages for regular papers, instead of 12 pages). Submissions that discuss a real-world problem without a solution are encouraged.

3. TECHNICAL PROGRAM COMMITTEE

We are grateful to the following PC members (and their sub-reviewers) for helping out SPSM 2016 with their valuable feedback on the excellent submissions we received.

- Konstantin Beznosov, University of British Columbia
- Mihai Christodorescu, Qualcomm Research Silicon Valley
- Jeremy Clark, Concordia University
- Lucas Davi, Technische Universität Darmstadt
- Manuel Egele, Boston University
- Ragib Hasan, University of Alabama at Birmingham
- Urs Hengartner, University of Waterloo
- Suman Jana, Columbia University
- Xiapu Luo, Hong Kong Polytechnic University
- Ian Molloy, IBM TJ Watson Research Center
- Muhammad Naveed, University of Southern California
- Damien Octeau, University of Wisconsin-Madison
- Xinming Ou, University of South Florida

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2990487

- Sebastian Porst, Google
- Ahmad-Reza Sadeghi, Technische Universität Darmstadt
- Kapil Singh, IBM TJ Watson Research Center
- Julie Thorpe, University of Ontario Institute of Technology
- Tao Wan, Huawei, Canada
- Glenn Wurster, BlackBerry
- Mingyuan Xia, McGill University
- Xiaoyong Zhou, Samsung Research America
- Yajin Zhou, Qihoo 360

4. STEERING COMMITTEE

- N. Asokan, Aalto University and University of Helsinki
- William Enck, North Carolina State University
- Xuxian Jiang, North Carolina State University
- Patrick Traynor, University of Florida

5. ACKNOWLEDGEMENT

We thank all the authors who submitted their work to the workshop. We acknowledge and greatly appreciate the time and effort as put forward by the PC members and external reviewers. We would also like to thank the 2016 ACM CCS organizers, specifically, the workshop co-Chairs Mathias Payer and Stefan Mangard for accepting and supporting this workshop.

6. PC CO-CHAIRS

Long Lu is an assistant professor of computer science at Stony Brook University. He directs the RiS3 Lab and is a core member of the National Security Institute at Stony Brook. He earned his PhD in computer science from Georgia Tech in 2013. Lu's research aims at protecting software, systems, and their users against critical or emerging threats. Focused on securing mobile apps and operating systems, Lu's recent work has produced comprehensive app vulnerability checkers, in-app security enforcement mechanisms, and new security primitives and designs for mobile OS, which were published at the top security and systems conferences, including CCS, S&P, USENIX Security, NDSS, and MobiSys.

Mohammad Mannan is an associate professor at the Concordia Institute for Information Systems Engineering, Concordia University, Montreal. He has a Ph.D. in Computer Science from Carleton University (2009) in the area of Internet authentication and usable security. He was a postdoctoral fellow at the University of Toronto from 2009 to 2011. His research interests lie in the area of Internet and systems security, with a focus on solving high-impact security and privacy problems of today's Internet. He is involved in several well-known conferences (e.g., program committee: ACM CCS 2016, ACSAC 2014, USENIX Security 2010), and journals (e.g., ACM TISSEC, IEEE TDSC, IEEE TIFS).