Guest Editors’ Introduction: Special Issue on Security and Privacy in Mobile Platforms

Gail-Joon Ahn, Senior Member, IEEE, William Enck, Member, IEEE, and Dongwan Shin, Member, IEEE

Smartphones and similar mobile devices have become a primary means of computing for many users. Over the last five or six years, the area exploded with change, seeing the rise of iOS and Android as dominant platforms. A key driver for this change was the diversity and availability of applications through application markets such as Apple’s App Store and Google’s Play Store. As smartphones transitioned from devices for mobile Email and web access to platforms with hundreds of thousands of third-party applications, the risks changed and grew. The systems security research community responded in kind, providing many tens of solutions and new attacks.

In this IEEE Transactions on Dependable and Secure Computing (TDSC) special issue on Security and Privacy in Mobile Platforms, we sample several of these papers, touching on key aspects of security and privacy. In response to the call for papers, we received 29 submissions. After rigorous review and careful revision, the following five papers were included in this special issue.

The first paper “MOSES: Supporting and Enforcing Security Profiles on Smartphones,” by Yury Zhauiniarovich, Giovanni Russello, Mauro Conti, Bruno Crispo, and Earlene Fernandes, targets the broad challenge of bring your own device (BYOD). Many users wish to use one physical device for both personal and work purposes. Unfortunately, existing smartphones have limited support for separating data. MOSES provides a policy-based framework for enforcing isolation of applications and data on Android while allowing dynamic switching between profiles. This paper extends a previous version of the paper published at SACMAT 2012.

The second paper “Mobiflage: Deniable Storage Encryption for Mobile Devices,” by Adam Skillen and Mohammad Mannan, targets a different data threat model, namely deniable storage. Simply encrypting data on a device may not be enough: users may be forced to disclose decryption keys (e.g., at border crossings). Mobiflage extends existing desktop plausibly deniable encryption (PDE) schemes to mobile devices. To do so, it hides encrypted volumes on the Android SDcard. Based on the decryption password provided on boot, the phone will load either the normal image or the hidden image. This paper extends a previous version of the paper published at NDSS 2013.

The third paper “Generating Summary Risk Scores for Mobile Applications,” by Christopher Gates, Ninghui Li, Hao Peng, Bhaskar Sarma, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy, seeks to better identify malware and other undesirable Android apps. The approach extracts lightweight signals of risk, including permission and category combinations. The authors then apply different Bayesian machine learning models to identify malware. This paper consolidates and extends two previous papers published at SACMAT 2012 and CCS 2012.

The fourth paper “Effective Risk Communication for Android Apps,” by Christopher Gates, Jing Chen, Ninghui Li, and Robert W. Proctor, considers how to convey risk information to users installing Android applications. Android currently uses permissions to convey risk, but several studies have demonstrated that users do not understand permissions. This paper proposes a method that assigns a risk score to each app and displays a summary of risk information to the user.

The fifth paper “Hiding in the Mobile Crowd: Location Privacy through Collaboration,” by Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, considers users’ geographic location privacy. Location-based services (e.g., location-based search) have become an invaluable feature of smartphones and their applications. Unfortunately, each time users make location-based queries, they reveal slightly more about their paths through the physical world. This paper takes a novel approach wherein mobile devices in a region share information with one another, significantly reducing the frequency of query the location-based service provider.

In closing, we would like to thank all of the authors who have submitted their research to this special issue. We are also grateful for the many experts in the field who have participated in the review process and provided helpful suggestions to the authors for improving their work. We would like to express our gratitude to the Editor-in-Chief, Dr. Elisa Bertino and the former Editor-in-Chief, Dr. Ravi Sandhu, for their support in bringing forth this special issue. We hope you enjoy the papers.

Gail-Joon Ahn
William Enck
Dongwan Shin
Guest Editors

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org.
Digital Object Identifier no. 10.1109/TDSC.2014.2312738
Gail-Joon Ahn received the PhD degree in information technology from George Mason University, Fairfax, VA, in 2000. He is a professor in the School of Computing, Informatics, and Decision Systems Engineering, Ira A. Fulton Schools of Engineering and the director of Security Engineering for Future Computing Laboratory (SEF-COM), Arizona State University. His research has been supported by the US National Science Foundation, National Security Agency, US Department of Defense, US Department of Energy, Bank of America, Hewlett Packard, Microsoft, CISCO, Google, Samsung, and Robert Wood Johnson Foundation. He received the US Department of Energy CAREER Award and the Educator of the Year Award from the Federal Information Systems Security Educators Association. He is a senior member of the ACM, IEEE, and CISSP.

William Enck received the BS, MS, and PhD degrees in computer science and engineering from the Pennsylvania State University in 2004, 2006, and 2011, respectively. He is an assistant professor in the Department of Computer Science at NC State University. His research efforts centrally focus on systems security, addressing challenges in smartphones and mobile applications, operating systems, cloud services, telecommunications, and hardware architectures. In particular, his work in mobile application security has led to significant consumer awareness and changes within the space. He received the National Science Foundation CAREER Award and has served on program committees for several top conferences in security such as USENIX Security, IEEE Security and Privacy, and NDSS. He is a member of the ACM, IEEE, ISSA, and USENIX.

Dongwan Shin received the MS degree in computer science and engineering from the University of North Carolina at Charlotte in 1999 and 2004, respectively. He is currently an associate professor in the Computer Science and Engineering Department at New Mexico Tech and the founding director of the Secure Computing Laboratory. He is also the CTO of the startup company, Secure Apps, LLC, which focuses on mobile solution development and security. He was a visiting researcher at Software Engineering Institute (SEI) which is based at Carnegie Mellon University from August 2012 to October 2013. His research interests mainly include system security, software security, and usable security. He has published more than 60 technical papers in international journals and conferences. His research has been supported by US National science Foundation (NSF), DoD, Sandia Labs, Los Alamos Lab, Intel, VirtualBridge, and CAaNES. He has been actively involved in academic community, serving organizing committee members of several international conferences and workshop. He is a member of the IEEE.

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.