Editorial

Advances in Mobile Security Technologies

Jeong Hyun Yi,¹ Aziz Mohaisen,² Sean Yang,³ and Ching-Hsien Hsu⁴

¹*School of Software, Soongsil University, Seoul 06978, Republic of Korea*

²*Department of Computer Science and Engineering, The State University of New York, University at Buffalo, Buffalo, NY 14260, USA*

³*Information Technology, Georgia Gwinnett College, Lawrenceville, GA 30043, USA*

⁴*Department of Computer Science and Information Engineering, Chung Hua University, Hsinchu 30012, Taiwan*

Correspondence should be addressed to Jeong Hyun Yi; jhyi@ssu.ac.kr

Received 6 June 2016; Accepted 6 June 2016

Copyright © 2016 Jeong Hyun Yi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobile devices such as smartphones and Internet tablets have achieved computing and networking capabilities comparable to traditional personal computers. An explosion of mobile devices being used for work 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. Recently, there has been an explosion of the Internet of things which will make us increasingly rely on intelligent, interconnected devices in every aspect of our lives. Examples include smart systems, smart vehicles, and wearable devices such as smart watches and digital glasses. In such always connected environment, mobile devices still will be an essential gateway from the personal point of view and cross-linking of things offers new possibilities to influence business intelligence and to exchange various data items. This may also lead to a variety of new potential risks concerning both security and privacy, which must be considered. Thus, it is tremendously essential to develop security technologies for mobile system, in particular, dealing with mobile devices.

Hence, the main motivation for this special issue is to bring together researchers, practitioners, policy makers, and hardware and software developers of mobile systems to explore the latest understanding and advances in the security and privacy for mobile devices, applications, and systems.

We received 36 submissions covering all areas of mobile security. Every submission received at least three reviews. Based on the paper topics, review feedback from the reviewers, and follow-up discussions among guest editors, we selected seven papers for this special issue.

The paper titled “The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform” by S. Song et al. proposes an effective method to prevent the attacks of modified ransomware on Android platform. The proposed technique specifies and intensively monitors processes and specific file directories using statistical methods based on processor usage, memory usage, and I/O rates so that the process with abnormal behaviors can be detected. The proposed technique can detect ransomware even if you do not save its patterns. Its speed of detection is very fast because it can be implemented in Android source code instead of mobile application.

The paper titled “Learning-Based Detection of Harmful Data in Mobile Devices” by S.-W. Jang and G.-Y. Kim proposes a method to assess the harmfulness of input images automatically based on an artificial neural network. The proposed method first detects human face areas based on the MCT features from the input images. Next, based on color characteristics, this study identifies human skin color areas along with the candidate areas of nipples, one of the human body parts representing harmfulness. Finally, the method removes nonnipple areas among the detected candidate areas using the artificial neural network.

The paper entitled “Enhancing the Security of Personal Identification Numbers with Three-Dimensional Displays” by M.-K. Lee et al. provides a novel solution based on three dimensions, particularly suitable for glasses-free three-dimensional (3D) displays found in many smartphones and handheld game consoles. A user at the “3D spot” may log in easily, while nearby shoulder-surfers gain no advantage. A detailed experimental usability analysis is performed to

demonstrate the effectiveness of the proposed scheme in comparison to the existing methods.

The paper “Anomaly Detection for Internet of Vehicles: A Trust Management Scheme with Affinity Propagation” by S. Yang et al. introduces a trust-based anomaly detection scheme for IVs, where some malicious or incapable vehicles are existing on roads. The proposed scheme works by allowing IVs to detect abnormal vehicles, communicate with each other, and finally converge to some trustworthy cluster heads (CHs). Periodically, the CHs take responsibility for intracluster trust management. Moreover, the scheme is enhanced with a distributed supervising mechanism and a central reputation arbitrator to assure robustness and fairness in detecting process.

The paper titled “Security Analysis and Improvement of Fingerprint Authentication for Smartphones” by Y.-H. Jo et al. identifies a few vulnerabilities in one of the currently deployed smartphones equipped with fingerprint verification service by analyzing the service application. Y.-H. Jo et al. demonstrate actual attacks via two proof-of-concept codes that exploit these vulnerabilities. By the first attack, a malicious application can obtain the fingerprint image of the owner of the victimized smartphone through message-based interprocess communication with the service application. In the second attack, an attacker can extract fingerprint features by decoding a file containing them in encrypted form.

The paper entitled “Function-Oriented Mobile Malware Analysis as First-Aid” by J. Jang and H. K. Kim proposes a novel method for function-oriented malware analysis approach based on analysis of suspicious API call patterns. Instead of extracting API call patterns for malware in each family, J. Jang and H. K. Kim focus on extracting such patterns for certain malicious functionalities. The proposed method dumps memory sections, where an application is allocated and extracts suspicious API sequences from bytecode by comparing with predefined suspicious API lists. By matching API call patterns with our functionality database, the proposed method determines whether they are malicious.

The paper titled “A Novel Iterative and Dynamic Trust Computing Model for Large Scaled P2P Networks” by Z. Tan et al. presents an iterative and dynamic trust computation model named IDTrust (Iterative and Dynamic Trust model) according to these properties. First of all, a three-layered distributed trust communication architecture was presented in IDTrust so as to separate evidence collector and trust decision from P2P service. Then an iterative and dynamic trust computation method was presented to improve efficiency, where only latest evidences were enrolled during one iterative computation. On the basis of these, direct trust model, indirect trust model, and global trust model were presented with both explicit and implicit evidences.

In closing, we believe the readers will find these papers interesting and useful, and we hope that they will enjoy them.

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. David Taniar, for his support in bringing forth this special issue. We also appreciate Global Research Laboratory Project through the National Research Foundation (NRF-2014K1A1A2043029) that tremendously helped support our effort.

*Jeong Hyun Yi
Aziz Mohaisen
Sean Yang
Ching-Hsien Hsu*

Acknowledgments

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