Mobile Application Security

Ying-Dar Lin, *National Chiao Tung University*
Chun-Ying Huang, *National Taiwan Ocean University*
Matthew Wright, *University of Texas at Arlington*
Georgios Kambourakis, *University of the Aegean*

With a multitude of mobile apps available in the market, most users are unaware of the security risks they bring. Strategies for coping with the diversity of these threats deserve a closer look.

Since the first major worm attack on mainframe machines in the 1980s, security has been a serious issue for computing systems. And although computer systems have changed a lot since that first Morris worm surfaced, threats and attacks have never been completely eliminated. On the contrary, malware and other cyber threats have grown exponentially due to various benefits earned by launching attacks.

As computing has moved resoundingly toward mobile platforms,[1] so too have attacks and malware shifted their targets to mobile computing. In 2013, Sophos[2] concluded that Android is the biggest target, and F-secure[3] reported that the number of mobile malware samples grew from several hundreds to more than 50,000 in just two years. The ubiquitous and popular use of mobile devices has made mobile application security a pressing issue. Because these devices contain large amounts of sensitive personal information, they are attractive targets for attackers seeking financial gain. However, Symantec[4]

0018-9162/14/$31.00 © 2014 IEEE

showed 57 percent of adult users are still unaware that security solutions exist for mobile devices. Reports also show that about half the attacks are intended to steal personal information and track users. Complicating matters further is the fact that mobile devices have limited computational power and a restricted user interface, making it easier for attackers to hide their malicious activities.

MOBILE SECURITY RESEARCH

To address this growing challenge, researchers are exploring a variety of security strategies for mobile platforms. Some work focuses on the analysis, detection, and evaluation of malicious applications. Like traditional approaches applied to system security, an analysis can be done with static techniques, dynamic techniques, or both. Other work focuses on designs meant to improve data security—for example, controlling permission usage or isolating the execution environment.

However, mobile application security should not simply focus on data and applications. Mobile platforms are used in various new settings and impact users in ways that could never apply to a PC. An attacker could compromise systems connected to mobile devices through vulnerabilities identified at any point. The rise of mobile botnets is a characteristic example of such a case. Furthermore, as we anticipate a shift from mobile platforms to wearable devices (smart watches, glasses, and the like), there are even more reasons to worry. Thus, we argue that it is much more interesting and challenging for security communities to work on mobile application security—not only because it is an emerging topic, but also because it could have a much greater impact on how we think about system security research as a whole.

IN THIS ISSUE

This special issue presents high-quality articles describing security algorithms, protocols, policies, and frameworks for applications running on modern mobile platforms such as Android, iOS, and Windows Mobile. We received a total of 28 submissions, and after a rigorous review process, we selected five articles covering the subject from different perspectives.

Detecting malicious behavior

Malware creators often hide malicious behavior in seemingly innocent applications. "Thwarting Obfuscated Malware via Differential Fault Analysis," by Guillermo Suarez-Tangil, Juan Tapiador, Flavio Lombardi, and Roberto Di Pietro, proposes a tool called Alterdroid that identifies obfuscated malicious components in an app package. The authors explain that Alterdroid first selects the suspicious components using statistical analysis against predefined models. It then injects a fault into a randomly selected suspicious component and repackages the modified component with the original application. The tool runs both the modified and original app in the Android containers and detects malicious behavior by comparing the execution traces using differential analysis. The approach is similar to fuzzing, but instead of manipulating program input, the authors manipulate the program directly to uncover malicious activity.

Rooting and jailbreaking

Although it can jeopardize device security, many users attempt to root their mobile devices and obtain superuser access rights for full control and customization. In "RootGuard: Protecting Rooted Android Phones," Yuru Shao, Xiapu Luo, and Chenxiong Qian propose a custom app to complement standard root-privilege management tools on the Android OS. The authors summarize the negative security effects of rooting a device. They then explain how RootGuard intercepts system calls from processes started via a superuser and then applies several default or user-defined policies to them. The tool—evaluated on realistic malware and handwritten demo exploits—is shown to provide a more secure environment for rooted devices.

A secure environment cannot solely rely on a mobile device itself: the security of the entire operation and usage environment must be considered as well.

App store security

A secure environment cannot solely rely on a mobile device itself: the security of the entire operation and usage environment must be considered as well. "Smart AppStore: Expanding the Frontiers of Smartphone Ecosystems" by Félix Gómez Mármol, Gregor Rozinaj, Sebastian Schumann, Ondrej Lábaj, and Juraj Kačur presents a case study (in the context of an EU research project) of an application store for smartphones and other smart devices (like smart TVs). The authors show how their device-agnostic approach can be used in the project's context. In addition, they demonstrate how objectives of usability, friendliness, and security can be considered simultaneously. Their app store is an interesting system with features including advanced security, biometric authentication, multilevel authorization, gesture navigation, application reputation scoring, and identity management.

The BYOD paradigm

Expansion of mobile device use has led to the emerging BYOD trend, in which enterprises and organizations allow employees to bring their private devices to work. This trend creates new challenges for balancing convenience and security. "Securing the 'Bring Your Own Device' Paradigm" by Alessandro Armando, Gabriele Costa, Luca Verderame, and Alessio Merlo discusses security issues related to mobile devices in the BYOD environment. The authors propose a secure metamarket architecture supporting the definition and enforcement of BYOD policies. They also implement an Android-based prototype named BYODroid and present experimental results on its runtime. It is an interesting read, and it shows how to address a major problem that organizations face due to BYOD's popularity and the proliferation of Android malware.

Security in open source and Web-based mobile OSs

"Security in the Firefox OS and Tizen Mobile Platforms" by Olga Gadyatskaya, Fabio Massacci, and Yury Zhauniarovich introduces two emerging mobile operating systems and discusses their security designs. Compared to mainstream mobile OSs, a distinguishing feature of these systems is the native integration of Web applications. After an overview of these OSs, the authors introduce and discuss their security designs and features. Because the two systems are also Linux based, they compare the differences between these and Android as well.

While the articles here cover diverse topics in mobile application security, security is always an arms race between attackers and defenders. Any new application can bring new security challenges. As mobile applications grow, we believe mobile application security will continue to be a rich research field. C

Reference

1. "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments on Pace to Grow 7.6 Percent in 2014: Android to Surpass One Billion Users across All Devices in 2014," Gartner, 2014; www.gartner.com/newsroom/id/2645115.
2. *Security Threat Report 2013: New Platforms and Changing Threats*, tech. report, Sophos, 2013; www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf.
3. *Mobile Threat Report 2013*, tech. report, F-Secure, 2013; www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf.
4. *Internet Security Thread Report 2014*, tech. report, vol. 19, Symantec, 2014; www.symantec.com/security_response/publications/threatreport.jsp.

Ying-Dar Lin *is a professor of computer science at National Chiao Tung University in Taiwan. His research interests include design, analysis, implementation, and benchmarking of network protocols and algorithms, quality of service, network security, deep packet inspection, and embedded hardware/software codesign. Lin received a PhD in computer science from the University of California, Los Angeles. He is a Fellow of IEEE. Contact him at ydlin@cs.nctu.edu.tw.*

Chun-Ying Huang *is an associate professor of computer science and engineering at National Taiwan Ocean University. His research interests are in the fields of computer networks, system security, and multimedia systems. Huang received a PhD in electrical engineering from National Taiwan University. He is a member of IEEE, ACM, the Institute of Information & Computing Machinery, and the Chinese Cryptology and Information Security Association. Contact him at chuang@ntou.edu.tw.*

Matthew Wright *is an associate professor of computer science and engineering at the University of Texas at Arlington. His research interests include the robustness of anonymous communications, secure and sybil-resistant P2P systems, security and privacy in mobile and ubiquitous systems, and understanding the human element of security and privacy. Wright received a PhD in computer science from the University of Massachusetts. He is a member of IEEE and ACM. Contact him at mwright@cse.uta.edu.*

Georgios Kambourakis *is an assistant professor of information and communication systems security at the University of the Aegean, Greece. His research interests are in the fields of mobile and wireless networks security and privacy, VoIP security, public-key infrastructure, DNS security, and mLearning. Kambourakis received a PhD in information and communication systems security from the University of the Aegean, and an EdM from the Hellenic Open University. He is a member of IEEE and the Greek Computer Society. Contact him at gkamb@aegean.gr.*