Authentic Learning of Mobile Security with Case Studies

Minzhe Guo, Prabir Bhattacharya
School of Computing Sciences and Informatics
University of Cincinnati
Cincinnati, OH
guome@mail.uc.edu

Kai Qian
Department of Computer Science
Southern Polytechnic State University,
Marietta, GA
kqian@spsu.edu

Li Yang
Department of Computer Science
University of Tennessee at Chattanooga
Chattanooga, TN
Li-Yang@utc.edu

***Abstract*— This work-in-progress paper presents an approach to authentic learning of mobile security through real-world-scenario case studies. Five sets of case studies are being developed to cover the state-of-the-art of mobile security knowledge and practices. Some of the developed case studies are being implemented in related courses and the preliminary feedback is positive.**

Keywords- Authentic Learning, Case Study, Mobile Security

I. INTRODUCTION

Owing to their ultra-portability, enriched functionality, and ease of use, smart mobile devices, such as Android and iOS based smartphones and tablets, play more and more important roles in many aspects of our society. Users increasingly use their mobile devices to access to the wealth of information available on the Internet, to store sensitive data, to communicate and entertain, and to process many of their daily tasks. These, however, also attract attackers to extend their targets to mobile platforms, resulting in a rapidly increasing number of mobile threats and a growing sophistication of mobile attacks [1-4]. In this work, we use the notion of mobile security to cover the topics of security and privacy issues, attacks, and defenses involved in the use of smart mobile devices. The mobile security is at the intersection of wireless communication, mobile computing, and computer security; and has its unique characteristics, such as introducing new and unique mobile security threats. Few existing security courses cover the full spectrum of mobile security topics; in addition, dedicated courses and effective materials on mobile security are sparse. This calls for efforts to promote mobile security education and to foster qualified mobile security professionals.

This work-in-progress paper presents an approach to authentic learning of mobile security through real-world-scenario case studies. Authentic learning situates students in learning contexts where they encounter activities that involve problems and investigations reflective of those they are likely to face in their real world professional contexts [5, 6]. A recent report pointed out that rather than only teaching students abstract concepts and assigning students abstract exercises, engaging students in real-world settings will benefit student effective learning in security education [7]. In this work, we approach to authentic learning of mobile security via the design of learning materials into real-world scenario cases, and take advantage of mobile device as the authentic learning platform, which will also help create a portable and affordable security-learning tool.

Courses focused on mobile security remain sparse in most computing curricula. Tague offered a mobile security course at the Carnegie Mellon University [8, 9]; however, it was a project-based course that provided students with topics for discuss and explore. In contrast, our work emphasizes on learning mobile security through real-world case analysis and hands-on experience, and we develop the materials for the learning. The application of Android in the education of various computer science subjects is obtaining increasing interests. For example, Andrus and Nieh [10] developed a series of five Android kernel programming projects and an Android virtual laboratory to teach an introductory operating system course; Kurkovsky [11] used mobile game development as a motivational tool to engage students early in the curriculum; and Loveland [12] described the use of Google Android mobile platform and Google's Web Toolkit to provide students with experience in designing and implementing user interfaces for mobile and web applications. The above works showed that the use of Android engaged students' interests in learning and improved effectiveness. Our work focuses on using Android to promote the study of mobile security and we directly use mobile devices and applications for security analysis and practice.

II. CASE STUDY DESIGN

To implement the authentic learning for mobile security, this work employs the following strategies in the development of the case studies, including: 1) connecting the abstract security concepts to real-world mobile security cases so that students can better understand the concepts and can work more actively and effectively with facts and realistic problems; 2) designing each case from both of the attack and defense perspectives so that students can gain more insights and can design better defense solutions via the experience with actual attacks; 3) infusing hands-on practices in the course of case studies and designing most of the practices in such a way that they can be performed on mobile devices directly; 4) encouraging students to identify for themselves the mobile security issues; and 5) providing students with opportunity of reflection in action so that they can learn how and when to use particular strategies for problem solving. Following the above

strategies, we are developing five sets of case studies, including:

- Mobile Malware. Case studies that 1) discuss the mobile malware attacking strategies and demonstrate instances of real-world Android malware; and 2) discuss the defense methods and instruct on practicing defense solutions.
- Secure Mobile Coding. Case studies that 1) use code examples to demonstrate the security weakness or unsecure coding patterns in the development of different Android app components, including *Activity*, *Intent*, *Service*, *Content Provider*, and *Broadcast Receiver*; and 2) discuss the best practices for improving the security of the Android app coding, such as using explicit *Intent Filter* to avoid *Intent* spoofing.
- Cryptography on Mobile Devices. Case studies that 1) discuss how to utilize the built-in cryptography mechanisms (e.g., SSL or VPN settings) to improve the security of data in device (database storage, shared memory, shared preferences, internal and external storage), on Cloud, or in the course of network communications; and 2) discuss how to program with Android/Java cryptography libraries to enhance the security of mobile apps.
- Access Control. Case studies that 1) discuss the Android permission model, including its basic concepts, use cases, weaknesses, and enhancements; and 2) discuss other access control and authentication mechanisms for mobile devices and application, including single sign-on and two-factor authentication.
- Mobile Privacy. Case studies that demonstrate the leakage of privacy-related data from mobile devices and communications (e.g., location information, user behavior and usage patterns), and discuss the configurations and best practices for mobile privacy enhancement.

As an example, the set of mobile malware case studies consists of an introductory case study and a set of individual malware case studies. The introductory case study summarizes the state-of-the-art mobile malware research (e.g., [13, 14]) and the malware reports from leading mobile security companies. Each individual malware case study introduces a family of real-world mobile malware, covering the topics of the attackers' incentives (e.g., Premium Calls/SMS or Information Stealing), attacking strategies (e.g., repackaging or update attacks), and existing defense solutions. It is observed that the number of new instances and variants of existing mobile malware families increases rapidly, but the number of new malware families grows rather slowly [14]. We will prepare for each case study at least one real instance of mobile malware in the family so that students can experience the actual attacks in a sandbox environment (i.e., an Android emulator on a virtual machine with experimental settings and data) and analyze the malicious behaviors and features. Each individual malware case study will also instruct student on practicing defense methods. Current mobile malware defense methods include app analysis (static/dynamic/permission analysis), configuration of system security settings, watchdogs, and user education. As the mobile malware evolves, the introductory case study will be updated and new cases will be developed and added into our individual malware case study set.

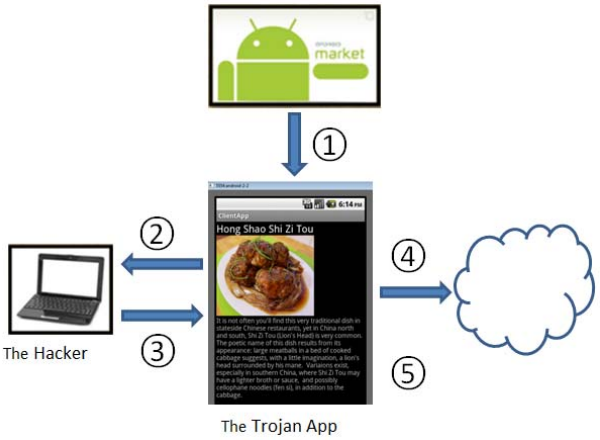

Fig. 1. Work Flow of a Premium SMS Android Trojan App in Our Mobile Malware Case Studies. (① the Trojan app is downloaded and installed on the victime's device; ② when the Trojan app is activated by the victim, it sends a notification with the victim's information to the hacker; ③ the hacker sends the commands to the Trojan app to ④ send SMS to premium numbers or send Ad SMS to others; and ⑤ the trojan app clears messaging history.)

Fig. 1 illustrates the work flow of an instance of Android Trojan in one of our individual malware case studies. The Trojan app pretends itself as an Asian Gourmet Android app, performs command and control communication with the hacker, and stealthily sends short messages (SMS) to premium numbers or advertisements to others. In the defense practices, students will be instructed on developing an Android SMS Monitoring App, which monitors the messaging actions in the background and sends notifications to users when suspicious messaging are detected. Note that in the latest version of Android 4.2 (Jelly Bean), Google provides similar kinds of control of premium SMS to enhance the Android security.

III. CONCLUSION

This work-in-progress paper presents an approach to authentic learning of mobile security through real-world-scenario case studies. We describe our strategies in developing the five sets of mobile security case studies and present more detail design of the set of mobile malware case studies.

Some of the developed case studies are being implemented in CS mobile security class and IT wireless security class. The preliminary feedback from students is positive. Students have gained hands-on real world experiences on mobile security with Android mobile devices, which also greatly promoted students' self-efficacy and confidence in their mobile security learning.

In the future work, we will continue to improve the design of the case studies, complete the case study development, and conduct extensive evaluations.

ACKNOWLEDGMENT

The work is partially supported by the National Science Foundation under award: NSF SFS #1241651. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Lookout, Inc., "Lookout Mobile Security Report 2011," August 2011, accessed on Oct 12, 2011, https://www.mylookout.com/mobile-threat-report.

[2] Juniper Networks, Inc., "2011 Mobile Threats Report," Juniper Networks, Feb. 2012, accessed on Mar. 01, 2012http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf.

[3] McAfee® Labs™, "2012 Threats Predictions," McAfee, 2011, accessed on Mar. 1, 2012, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf.

[4] C. Nachenberg, "A Window Into Mobile Device Security," Symantec, 2011, http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_mobilesecuritywp, accessed on Mar. 01, 2012.

[5] J. Brown, A. Collins, and P. Duguid, "Situated Cognition and the Culture of Learning, Educational Researcher, 18, n1, pp.32-42, 1989.

[6] J. Lave and E. Wenger, Situated Learning: Legitimate Peripheral Participation (Learning in Doing: Social, Cognitive and Computational Perspectives), Cambridge University Press, 1991.

[7] EDUCAUSE, "The Future of Mobile Computing," 04/2011, http://net.educause.edu/ir/library/pdf/ESPNT1b.pdf, accessed on Mar. 10, 2012.

[8] P. Tague, "14-829: Mobile Security - Fall 2010," http://wnss.sv.cmu.edu/courses/14829-f10, 2010, accessed in Feb. 2012.

[9] P. Tague, "14-829: Mobile Security - Fall 2011," http://wnss.sv.cmu.edu/courses/14829-f11, 2011, accessed in Feb. 2012.

[10] J. Andrus and J. Nieh, "Teaching Operating Systems Using Android," SIGCSE'12, Feb. 29 – Mar. 3, Raleigh, NC, USA.

[11] S. Kurkovsky, "Engaging Students through Mobile Game Development," SIGCSE' 09, Chattanooga, TN, Mar. 2009.

[12] S. Loveland, "Human computer interaction that reaches beyond desktop applications," In Proceedings of SIGCSE 2011, March 9-12, 2011, Dallas, Texas, USA.

[13] A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A Survery of Mobile Malware in the Wild," *Proceedings of ACM Workshop on Security and Privacy in Mobile Devices (SPSM)*, 2011.

[14] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2012.