Work in Progress: Real World Relevant Security Labware for Mobile Threat Analysis and Protection Experience

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

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

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

***Abstract*— to address the need for innovative mobile security learning materials and for promoting mobile threat and protection education, this paper presents a work-in-progress effort on developing a real world relevant security labware to provide students with mobile threat analysis and protection experience. A preliminary evaluation has been conducted on the pilot labs and has received positive and encouraging feedback.**

Keywords-Labware, Mobile Threat and Protection, Real World Relevant, Smartphones and Tablets

I. INTRODUCTION

The computing landscape is shifting towards mobile devices [1] and today's digital-native students are increasingly associate computing technology with mobile devices, such as smartphones and tablets, rather than with desktop computers [2]. Unfortunately, threats to mobile devices and applications are also growing explosively and threatening nearly all aspects of our society. Recent information security reports [3, 4] have witnessed the rapidly growing number and sophistication of mobile attacks. However, the explosive growth in mobile threats has not been accompanied by substantial educational activities particularly in the area of mobile security. To our best knowledge, very few courses have been initiated for teaching mobile security and there are little well-prepared learning materials to provide students with the state-of-the-art mobile security knowledge and hands-on experience. Because of mobile devices and applications' ubiquitous form of computation, new ways of communication, and distinctive user behaviors, traditional security threats, such as malware and phishing, are evolving to stay active in this new environment, and there are also new and unique mobile security threats, such as SMS attacks and location issues, that emerge and endanger the systems and users. This calls for innovative educational activities and learning materials to promote the exposure of students to this emerging and important security area and well prepares them for growing industry needs.

To address the above needs and challenges, this paper presents our work-in-progress effort on developing a real world relevant labware to provide students with mobile threat analysis and protection experience. The labware employs an innovative learning approach that couples the in-depth threat analysis with the detail hands-on implementation of corresponding protection mechanisms. In addition, the labware aims at providing real world relevant learning, which means that the labware will reflect the up-to-date mobile threats and protections, provide materials close to students' everyday lives, and instruct students implementing protection apps that are workable in practice.

TABLE I. LAB LIST

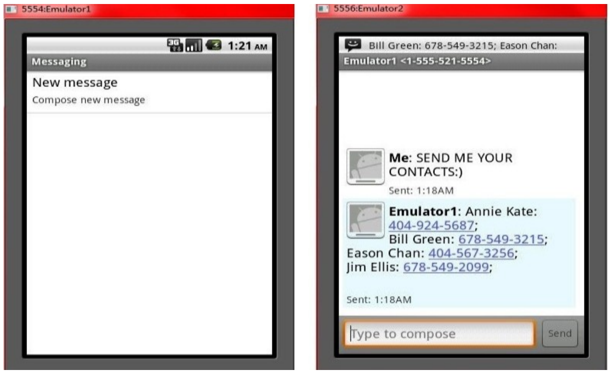
Lab	Mobile Threat Analysis & Protection	Security Area
1	Threats of Lost or Stolen Mobile Devices	Mobile Device & Data Security
2	Unauthorized Mobile Resource Access	
3	Data & Location Privacy Threat	
4	Mobile Malware	Mobile App Security
5	Mobile Spyware	
6	Mobile Coding Vulnerability	
7	Mobile Messaging Threats	Mobile Network & Communication Security
8	Mobile Banking Threats	
9	Mobile Phishing Threats	
10	Mobile Network Exploits	

II. LABWARE DESIGN

To provide students with the state-of-the-art mobile security knowledge, we collect and analyze a number of recent mobile security reports from both academy research and security companies, e.g., Lookout, McAfee, and Symantec. Table 1 lists the ten labs that we design in the labware. It covers important threats in most areas of mobile security, including mobile device, application, operating system, and network communication. Each lab focuses on one type of mobile threats and develops multiple forms of learning materials for the threat analysis and protection, including lecture, multimedia, attack instance analysis, demonstration, and hands-on mobile app development. Rather than implementing a comprehensive mobile security resource center, the labware is intended to create real world relevant learning materials and to provide students with in-depth threat analysis and hands-on protection implementation experience.

III. Example Lab

This section demonstrates the labware using *Lab 7: Mobile Messaging Threats*. Mobile messaging services, e.g., Short Message Service (SMS) and Multimedia Messaging Service (MMS), have become a lucrative playground for various attacks and frauds such as spamming, phishing, and spoofing [5]. These threats are unique to the mobile computing system and are seldom applicable to other information systems. The *Lab 7: Mobile Messaging Threats* aims at providing students with mobile messaging threat analysis and protection experience. In the threat analysis part, this lab first introduces the attacking surface of mobile messaging and analyzes instances of SMS phishing and spoofing; then it provides a mobile app to demonstrate an SMS attack instance. Fig. 1 shows two screenshots of this threat demonstration app. In this demo, an attacker installs a malicious SMS broadcast listener on the victim's mobile phone, then he sends a malicious SMS to the victim and steal victim's contact (right figure of Fig. 1), and the victim has no information about the attacker's malicious SMS activities (left figure of Fig. 1).



Me: SEND ME YOUR CONTACTS:)
Sent: 1:18AM

Emulator1: Annie Kate: 404-924-5687;
Bill Green: 678-549-3215;
Eason Chan: 404-567-3256;
Jim Ellis: 678-549-2099;
Sent: 1:18AM

Figure 1. Screenshots of a Mobile SMS Attack Demo.

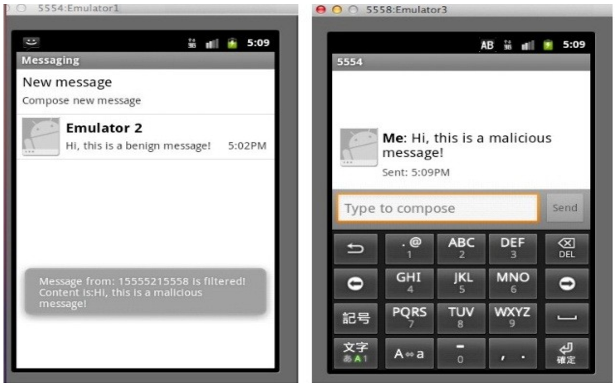
In the protection part, the lab first gives an overview of the protection mechanisms, e.g., using white list or black list to block or filter messages, and the user education. In response to the SMS attack demo, the lab instructs students implementing a mobile app for preventing from the attack using SMS filtering. Fig. 2 shows two screenshots of the mobile SMS protection app. In this protection app, the students implement a filter to block suspicious SMS messages (left Figure of Fig. 2) from unknown users (right Figure of Fig. 2). The app is workable in practice. Students can easily install their developed apps in their own devices such that they can obtain an instant gratification and confidence from the hands-on practice and they can be encouraged to create their own apps.

IV. Preliminary Evaluation

Pilot labs have been presented to 14 undergraduate students in the course "Wireless Security" for preliminary evaluation. Table II shows the evaluation question and students' feedbacks. On average, about 90% of students gave non-negative feedbacks on all evaluation questions, and about 70% agreed with our design objectives of the labware. Especially, we are pleased and encouraged to see that about 65% students felt that the labs are easy to follow and practice, since none of the 14 students has previous mobile development experience.

V. Conclusion

This paper presents our work-in-progress effort on developing a real world relevant labware to provide students with mobile threat analysis and protection experience. A preliminary evaluation has been conducted on the pilot labs and has received positive feedbacks. In the future work, we will complete the labware development, refine the design of the labware, and conduct extensive evaluations.



Emulator 2
Hi, this is a benign message! 5:02PM

Message from: 15555215558 is filtered!
Content is:Hi, this is a malicious message!

Me: Hi, this is a malicious message!
Sent: 5:09PM

Figure 2. Screenshot of a Mobile SMS Protection App.

TABLE II. Preliminary Evaluation

Evaluation Question	Feedback[a]
1) The labware helps me understand better about the mobile security concepts in the project.	71.43 / 21.43 / 7.14
2) The labware provides me with more hands-on experience on learning mobile security.	71.43 / 28.57 / 0
3) The labware is easy to follow and practice.	64.29 / 7.14 / 28.57
4) The labware promotes my interest and engagement in security.	71.43 / 21.43 / 7.14
5) The labware promotes my interest and engagement in mobile app development.	57.14 / 28.57 / 14.29
6) I gained real world security experience from the real world relevant hands-on mobile labs	71.43 / 21.43 / 7.14

a. the format of feedback data is Agree / Neutral / Disagree, e.g., the feedback to question 1 is 71.43% agree, 21.43 neutral, and 7.14 disagree

References

[1] J. Andrus and J. Nieh, "Teaching Operating Systems Using Android," *SIGCSE'12*, February 29–March 3, 2012, Raleigh, North Carolina, USA.

[2] O.H. Mahmoud, "Integrating Mobile Device into Computer Science Curriculum," *Frontiers in Education Conference*, Oct. 22-25, 2008.

[3] Juniper Networks, Inc., " 2011 Mobile Threats Report," Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf, on Apr. 10, 2012.

[4] McAfee, Inc., "2012 Threats Predictions," Retrieved on 04/10/2012 from www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf..

[5] G. Yan, S. Eidenbenz, and E. Galli, "SMS-Watchdog: Profiling Social Behaviors of SMS Users for Anomaly Detection," in *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID'09)*, Sept., 23-25, 2009, Saint-Malo, Brittany, France.