Learning Mobile Security with Android Security Labware

Minzhe Guo, Prabir Bhattacharya
School of Computing Sciences and Informatics
University of Cincinnati
Cincinnati, OH 45221
guome@mail.uc.edu, bhattapr@ucmail.uc.edu

Ming Yang, Kai Qian
School of Computing and Software Engineering
Southern Polytechnic State University
Marietta, GA 30060
mingyang@spsu.edu,kqian@spsu.edu

Li Yang
Department of Computer Science and Engineering
University of Tennessee at Chattanooga
Chattanooga, TN 37403
Li-Yang@utc.edu

ABSTRACT
As smart mobile devices grow increasingly in popularity, so do the incentives for attackers. Recent surveys on mobile security describe the rapidly increasing number and sophistication of mobile attacks. Newer sources of risks are being introduced or explored in the mobile computing paradigm where traditional security threats are also evolving. The prevalence of mobile devices and the rapid growth of mobile threats have resulted in a shortage of mobile security personnel. Educational activities are needed to promote mobile security education and to meet the emerging industry and education needs. This paper presents our initial effort on exploring a learning approach to mobile security, which aims at taking advantages of the benefits of mobile devices and the best practices in learning information security, promoting students' interests, and improving students' self-efficacy. An Android security labware is designed to implement the environment and materials for the learning approach. We integrated the pilot modules of the labware into two security courses in two semesters. The majority of the students provided positive feedback and enjoyed the Android security practices.

Categories and Subject Descriptors: K.3.1 [**Computers and Education**]: Computer Uses in Education-*distance learning*; K.3.2 [**Computers and Education**]: Computer and Information Science Education-*computer science education*; D.4.6 [**Operating Systems**]: Security and Protection; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection.

General Terms: Design, Experimentation, Security

Keywords: Android, Mobile Security, Labware

1. INTRODUCTION
Over the last decade, the use of mobile devices for both personal and business purposes has exploded. The arrival of smart mobile devices (smartphones and tablets) and the booming of mobile applications (apps) in recent years have only accelerated this trend. For the year 2011, the shipments of Apple-iOS-based and Google-Android-based smartphones and tablets were about 400 million units, compared to the 350 million units of netbooks, notebooks, and desktops in total [1]. More importantly, there have been more than 600,000 apps available for iOS and Android devices [2], turning these devices into powerful general-purpose computing platforms. More and more users and businesses use mobile devices for processing personal, financial, and commercial data, or use them to organize their work and private life. As mobile platforms grow increasingly in popularity, so do the incentives for attackers, especially when the value of mobile payment transactions is projected to reach almost $630 billion by 2014 [2]. Recent security surveys [2-5] describe the rapidly increasing number and sophistication of mobile attacks. According to the study, mobile infections will continue to rise significantly in these years [6]. The prevalence of mobile devices and the rapid growth of mobile threats have resulted in a shortage of personnel trained to handle mobile security [7].

Mobile security is an emerging security area of growing importance and increasing needs, but is a relatively weak area in the current computing curriculum at most schools. In this paper, we informally define mobile security as a subject at the intersection of wireless communication, mobile computing, and computer security, which covers the various security threats and protections involved in the use of smart mobile devices, especially the iOS-based and Android-based smartphones and tablets. The growing need for promoting mobile security education has been pointed out [8] and several security organizations have started to offer short-term training courses on mobile security, e.g., [9-11]. More and more academic institutions plan to integrate mobile security into their undergraduate computing curriculum. However, we find that there are at least two challenges in promoting the mobile security education. The first challenge is the unique characteristics of mobile security. Mobile security is new and evolving. Traditional security threats, e.g., malware or social engineering, are evolving in this new environment, such as using new attack vectors or adapting to the new platform. More importantly, new components (e.g., Global Positioning System (GPS)) and services (e.g., short message service (SMS) and mobile payment) in mobile platforms introduce new sources of risks. Few security courses cover the full spectrum of mobile security, especially those new and unique mobile security threats. The second challenge is the shortage of effective mobile security learning materials. Compared to the rich learning materials available for general computer security or other special security areas, e.g., web security or network security,

SIGCSE'13, March 6–9, 2013, Denver, CO, USA.

systematic materials designed specifically for mobile security remain sparse, not to mention the hands-on laboratory resources.

This paper presents our initial effort on dealing with the challenges through the exploration of a learning approach to mobile security, which takes advantage of the benefits of mobile devices and the best practices in learning information security, and the development of an Android security labware, which covers important mobile security knowledge and implements the environment and materials for the learning approach. We integrated the pilot modules of the labware in two security courses in two semesters. The majority of students surveyed provided positive feedback and enjoyed the Android security practices.

The reasons for our using Android as the platform for learning mobile security are as follows: (1) Android platform is open-sourced, while Apple iOS platform has license restrictions; (2) up to March 12, 2012, Android was ranked as the top mobile platform with 51 percent U. S. market share [12]; (3) the Android platform has become the chief target for malicious hackers [13]; (4) the Java-based app development on Android platform would impose a short learning curve for both students and faculties; and (5) many of the important mobile threats identified in the Android platform are common to all mobile platforms, though the detail implementations of the attacks and defenses can be different. The threat analysis and protection practice on Android platform can help students understand the mobile security in other platforms.

The rest of this paper is organized as follows. Section 2 presents the characteristics of the our learning approach to mobile security; Section 3 presents the Android security labware and demonstrates an example module in the labware; Section 4 discusses our experience in integrating the labware in security courses; Section 5 reviews the related work; and Section 6 concludes the paper and describe our future work.

2. A LEARNING APPROACH TO MOBILE SECURITY

For effective learning of mobile security, we desire a learning approach that takes advantages of the benefits of mobile devices (e.g., mobility and the closeness to students' daily lives) and the best practices in learning information security, promotes students' interests, and improves students' self-efficacy. This section presents the main characteristics of our learning approach that attempts to achieve these objectives.

(1) Experience-based Threat Analysis and Protection Practice

The first characteristic of our learning approach is its experience-based learning that couples mobile threat analysis with protection solution practices. The importance of experience-based learning or hands-on learning has long been recognized in the learning theory literature [14]. We develop hands-on materials specifically for mobile security. In addition, to make the learning more effective, for each specific mobile threat, our experience-based approach will first let students experience an actual attack instance, then instruct students on how to implement a protection solution using step-by-step tutorials. A protection solution practice can be a mobile app development (e.g., implement a filter to block malicious SMS), an open-sourced security tool practice (e.g., using reverse engineering tools *apktool* and *dex2jar*), or a configuration (e.g., configuration of Android app permission).

In traditional computer security classes, the protection principles and practices are the central topics. However, some academics have identified that, by experiencing actual attacks, the students will gain more insight, and that will enable them to design and implement better protections [15]. This attack/defend approach has been recognized as a highly effective approach to learning information security [16].

Our approach adopts the idea of understanding the protection task better from threat analysis, but ours differs from the attack/defend approach [15] in the following aspects: 1) we develop multimedia or mobile apps to demonstrate instances of attacks; 2) students will not design attacks and will not perform real attacks to harm servers or peers' mobile devices; 3) the developed attack apps are to facilitate students in analyzing mobile threats; they will be hard-coded and will not be effective in practice; and the complete source code is hidden from students and is not distributed.

(2) Real-world relevant learning

The second characteristic of our learning approach is its real-world relevant learning. A recent report pointed out that rather than teaching students only abstract concepts and assigning them abstract exercises, engaging students in real-world settings would benefit student effective learning in security education [17]. We approach real-world relevant learning in the following ways:

- Mobile app development with real devices. Unlike existing efforts on using mobile game development to improve engagement [18] or using mobile apps to help illustrate programming concepts [19], we directly use mobile app development as a means of protection solution practice. Students will be provided with step-by-step tutorials on developing mobile apps. Each app implements a certain protection solution. Students can debug and develop apps with emulators or real devices, and they can install their developed apps on real devices. This will help students obtain an instant gratification and confidence from the hands-on practice and encourage them to create their own apps. This also has the additional benefits of not only facilitating students to learn mobile programming skills but also heightening their awareness and understanding of secure programming principles.
- Up-to-date mobile threats and protections. We will provide students with the state-of-the-art mobile security knowledge. The materials are designed by collecting and analyzing a number of recent mobile security literatures from academics and industry [2-5, 20].
- Hands-on experiments with mobile devices directly. The mobile device itself is more relevant than other existing learning platforms to real world applications. It is close to the concepts and applications in students' daily lives. We design most of the security exercises in a way that they can be performed on mobile devices directly. This will help in creating a strong connection between the academic study and the reality of student's lives and engage student learning in mobile security.

(3) Mobile Learning

The last but not least characteristic of our learning approach is its mobile learning. The slides, tutorials, and demonstrations are designed to be friendly to mobile devices. Security exercises can be performed using mobile devices except those app development practices that use Eclipse IDE in personal computers. Materials

are accessible from our dedicated repository using mobile devices.

3. THE ANDROID SECURITY LABWARE

To provide the environment and materials for our learning approach, we are developing an Android security labware, which is a collection of self-contained modules that provide both necessary concept introduction and hands-on laboratory exercises on mobile security. It consists of seven modules to introduce important mobile threats in three aspects of mobile security, including mobile device security & privacy, mobile app security, and mobile network & communication security. Each module includes pre-lab activities (concept introduction and lab preparation); hands-on lab activities (pairs of hands-on labs on analysis for the threats and their protection practice with smart devices); and post-lab activities (review questions, assignments, and case study). An open repository is developed to host the labware for wide access and collaboration. This section presents and demonstrates the design of the Android security labware.

3.1 Lab Modules

The modules in the labware are designed based on: (1) the ACM Computer Science Curricula 2013: Strawman Draft [21], (2) the authors' teaching experience on embedded systems and information security, and (3) recent mobile security reports [2-5, 20]. Table 1 presents the seven modules in the labware. They cover the important mobile threats in three aspects of mobile security, including: (1) mobile device security and privacy - mobile threats that are related to the security issues in a physical device and a mobile operating system; (2) mobile app security - mobile threats that are germane to the security issues in the development and distribution of mobile apps; and (3) mobile network and communication security - mobile threats that are relevant to security issues in mobile communication channels, network protocols, and mobile network/web activities. The Information Assurance and Security (IAS) topics, which are defined in ACM Computer Science Curricula 2013: Strawman Draft [21], are covered among the labs. All modules will follow the same pattern of design. We demonstrate an example module to illustrate the design in Section 3.2. In the following, we briefly present each module.

M 1: Threats of Lost or Stolen Mobile Devices. As a unique threat to mobile devices, lost or stolen mobile devices would result in leakage of the sensitive information stored in the device, such as contacts, passwords, bank information, or authorizations to business access. This module introduces to students the risks of lost or stolen mobile devices, and teach them protection methods to reduce their loss, including data encryption, data wiping for device lost, stolen phone locating, and device authentication.

M 2: Unauthorized Mobile Resource Access. This module introduces to students the threats of unauthorized access of users to mobile devices, the unauthorized access of apps to system resources, and the unauthorized inter-application resource access. For protection solutions, this module will provide students with the experience in the Android permission system. Students will learn the authentication protocols and practice the configuration of system permission and app permission.

M 3: Mobile Privacy Threats. This module introduces to students the privacy threats in mobile devices. Privacy threats may be caused by applications those are not necessarily malicious, but gather or use more sensitive information (e.g., location or user identity) than is necessary to perform their function or than a user is comfortable with [2]. Students will learn to know how firms or app developers can obtain their private data, and learn how to reduce the privacy leaks and how to use cryptography as a means to protect against theft of private information.

M 4: Mobile Malware. Mobile malware is mobile app designed to engage in malicious behavior on a mobile device [2]. This module will introduce to students the types of mobile malware, the attack vectors of mobile malware, the methodologies and tools to analyze mobile malware, the user education, and the tools for preventing damage from or detecting the mobile malware. It will demonstrate and analyze an app with a malicious payload. Students will also learn to use Android reverse engineering tools to analyze mobile malware.

M 5: Secure Mobile App Development. This module has two foci: secure mobile coding and tamper-resistant app development. On secure coding, this module will introduce the coding threats, e.g., buffer over-flow and injection. For preventing damage from coding threats, students will learn how to create a security-aware mobile app by enforcing the device management policies and practicing the mobile coding tips of Android *Activity*, *Intent*, *Broadcast*, and *ContentProvider*. On tamper resistance part, students will learn the threat of app tampering and learn how to anti-tamper using obfuscation.

Table 1. Lab Modules in the Android Security Labware

Category	Mobile Threat Analysis & Protection Modules	IAS Topics
Mobile Device Security & Privacy	M 1: Threats of Lost or Stolen Mobile Devices	• Fundamental Concepts • Security Architecture and Systems Administration • Cryptography
	M 2: Unauthorized Mobile Resource Access	
	M 3: Mobile Privacy Threat	
Mobile App Security	M 4: Mobile Malware	• Fundamental Concepts • Secure Software Design and Engineering • Security Architecture and Systems Administration
	M 5: Secure Mobile App Development	
Mobile Network & Communication Security	M 6: Mobile SMS Security	• Fundamental Concepts • Cryptography • Network Security • Security Policy and Governance
	M 7: Mobile Phishing Threats	

Mobile SMS Security

Description: Short Message Service (SMS) is one of the most popular functions in mobile devices. However, it also becomes a lucrative playground for various attacks and frauds. Mobile SMS threats are increasing, and will continue to do so over the coming years. This module introduces the SMS-based threats and protections. An instance of SMS attack will be demonstrated and students will develop strategies to protect against damage from this attack.

Learning Objectives:

- Students understand the SMS threats: what are the SMS-based threats , how the attacks happened, and their consequences;
- Students understand the principles of protection strategies; students know the best practices to ensure safe SMS messaging; students practice SMS filtering on Android devices.

Targeting Courses: Mobile Security, Mobile Computing, Mobile Programming

Activities:

- Pre-Lab Activities
  - Introduction to SMS (slides)
  - SMS Messaging in Android (slides)
  - Introduction to SMS-based Threats and Protections (slides)
  - User Education on Secure SMS Messaging Practices (slides)
- Lab Activities
  - Threat Analysis: Malicious SMS (slides, app-demo-on-emulator, video-demo-on-youtube)
  - Threat Protection: SMS Filtering (instructions, android-apk, eclipse project with code)
- Post-Lab Activities
  - Case Study: An instance of Smishing Attack (slides)
  - Review questions
  - Assignments

Figure 1. The Design of Mobile SMS Security Module

M 6: Mobile SMS Security. This module will introduce the mechanisms of SMS in mobile devices, the SMS-based attacks, and the protection solutions. An app-based SMS attack demonstration will be developed. Students will learn to develop filter-based protection solutions. The prototype of this module has been developed and integrated in class for evaluation.

M 7: Mobile Phishing Threats. Social engineering attacks, such as phishing, leverage social engineering to trick the user into disclosing sensitive information or installing malware [2]. So far, neither iOS nor Android devices have built-in security approaches to protect users from such attacks [5]. This module will introduce to students the mobile phishing threats and their protection solutions. The mobile phishing attack vectors will be discussed and an attack instance will be demonstrated. For protection, this module provides user education and detection tool practices. This module is under development.

M3 and M6 have been developed and evaluated in courses (Section 4 presents the evaluation results); M1 and M4 are developed and will be integrated into courses for evaluation soon; M2, M5, and M7 are under intensive development. In addition to the above seven modules, an *M0: Getting Started* module will be provided to introduce to students the setup of Android development environment and the fundamental concepts in information security and mobile computing. Students can learn basic programming skills with Android and know the ethics in information security. More modules will be designed in the future, such as the modules for mobile browser security.

3.2 Example Module

In this section, we briefly demonstrate an example module to illustrate the learning approach and labware. Figure 1 shows the design of the *Mobile SMS Security* Module, which aims at providing students with SMS threat analysis and protection experience. SMS is a distinctive function of mobile computing systems. However, the convenience and popularity of SMS have also made the service a lucrative playground for various attacks and frauds such as spamming, phishing, and spoofing [22]. This module first provides the pre-lab activities that include the introduction to the SMS service in Android, threat types of SMS, the attacking surface of SMS, and the strategies for SMS threat protection solutions. The lab activities provide a pair of hands-on labs on threat analysis and protection practice. In the threat analysis part, the lab introduces important SMS attack principles with a mobile-app-based demonstration of an instance of SMS attacks. In the demo, an attacker installs a malicious SMS broadcast listener on the victim's mobile phone, which has four contacts, and then the attacker sends a malicious SMS message to the victim and steals the victim's contact. The victim has no idea of the attacker's messages. In the protection practice part, the lab instructs students on implementing a mobile app for protecting against this attack using SMS filtering. In the protection app, students practice using a filter to block suspicious SMS messages from unknown users. This app is workable in practice. Students can install the app in Android devices such that they can obtain an instant gratification from the hands-on practice and they can be encouraged to create their own apps. The post-lab activities include review questions, assignments, and case studies.

The intention of pairing up the threat analysis and protection practice is to help students to understand how the actual mobile attacks and protection solutions take effect and to help to foster students' knowledge of mobile security so that they can detect new types of attacks and develop corresponding protection solutions.

4. COURSE EXPRIENCE

The modules in the labware are designed to be self-contained so that they can both be used in a dedicated mobile security course and be integrated into existing courses. In this section, we present our experience in using pilot modules in a wireless security

course in Spring 2012 (14 students) and in an information security course in Summer 2012 (26 students). In the wireless security course, labs in the *Mobile SMS Security* module were offered as part of the hands-on labs of the course; and in the information security course in Summer 2012, the RSA Encryption/Decryption labs in the *Mobile Privacy Threat* module and the labs in *Mobile SMS Security* Module were offered as part of the hands-on labs of the course. Students who participated were asked to complete a survey that consists of the following six questions to evaluate the idea and the effectiveness of the labware:

Q1. The labware helps me understand better about the mobile security concepts in the project.

Q2. The labware provides me with more hands-on experience on learning mobile security.

Q3. The labware is easy to follow and practice.

Q4. The labware promotes my interest and engagement in security.

Q5. The labware promotes my interest and engagement in mobile app development.

Q6. I gained real world security experience from the real world relevant hands-on mobile security labs.

Forty students participated in the lab activities and completed the survey. Figure 2 shows the students' feedback. On average, about 90% of students gave non-negative feedback on all evaluation questions, and about 70% students agreed with the design objectives of the labware. Since none of the forty students had prior mobile development experience, the result of Q3 is still satisfactory that over 60% students gave non-negative feedback.

Students also provided their comments. We list representative positive feedback in the following. Students found the labs fun, educational, and promoting their interests in both mobile security and Android app. They enjoyed the real hands-on experience with the Android security labs and gained self-efficacy from the practices.

- *This project gave me the interest of Android app and Mobile security. The topic of this project is one that we all could face on any daily basis. With the help of this lab, I am now more than ever interested in design an app.*
- *It was a real and more hands-on experience, which I really like and always wish to do with all courses.*
- *The project was very challenging which is something I like. It actually feels rewarding to see the project working and performing what you want it to do.*
- *I really liked the challenge of this lab. Much as the instructions was easy to follow. This lab has really raised my level of interest in android apps development.*

The representative negative comments provided by students are listed in the following. Their concerns were concentrated around the installation of the lab environment and the precision of lab instructions. This provides an explanation for the relatively high disagreement rate in the survey result of Q3 in Figure 2. In the future, we will work on reducing the complexity of the lab environment setup and improve the lab instructions. Some students suggested providing equivalent lab exercises on iPhone platform. While we explained our reasons for choosing Android in Section 1, we are also investigating the possibility of developing the security practices on iPhone platform.

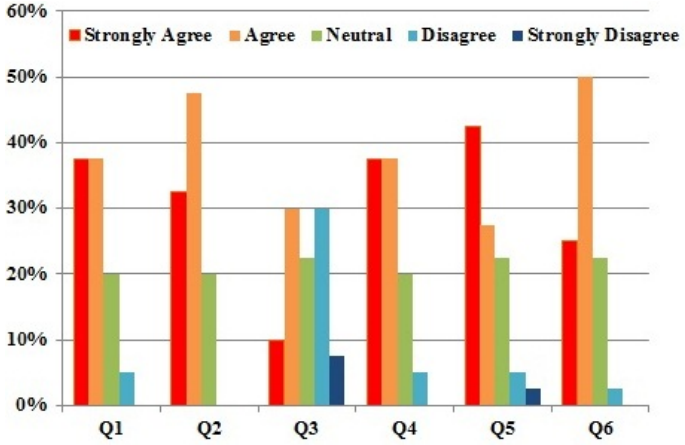

Figure 2. Survey Results

- *I liked the experience of building the project. The instructions could have been more precise.*
- *I really liked this project. Some of the problems I had with the software I had to Google for help and fortunately, it was there. The lab was not too hard, was not too easy. The only thing I found confusing was the links in the original word doc given us to us did not work.*
- *I would suggest having the lab environment set up before the assignment so that the emphasis can be on coding, programming, and applying cyber security concepts…*
- *Maybe because I am an iPhone fan, I wish we I had an option to choose (Apple or android), and I wish the lab was prepare and ready before we begin working on it.*

To sum up, our Android security labware and learning approach to mobile security received positive feedback from students and progress was made towards the objectives of promoting students' interests and improving their experience in mobile security and Android app development.

5. RELATED WORK

Courses focused on mobile security remain sparse in most computing curricula. Tague offered a mobile security course at the Carnegie Mellon University [23, 24]; however, it was a project-based course, which provided students with topics for discuss and exploration. In contrast, our work emphasizes learning mobile security through the hands-on experience, and we develop the lab environment and 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 [25] developed a series of five Android kernel programming projects and an Android virtual laboratory to teach an introductory operating system course; Kurkovsky [18] used mobile game development as a motivational tool to engage students early in the curriculum; and Loveland [19] 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. They all 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 apps for threat analysis and use mobile app development as a means of protection solution practice.

6. CONCLUSION

Mobile security is an emerging security area of growing importance and increasing needs, but is a relatively weak area in the current computing curriculum at most schools. This paper presents our initial effort on exploring the learning approach to mobile security and developing an Android-based security labware. We integrated the labware in two information security courses in two semesters. Forty students participated in the initial evaluation of our mobile security learning approaches and materials. The majority of students surveyed provided positive feedback and enjoyed the Android security practices. In the future, we plan to add more modules into the labware, such as the modules for mobile browser security, and Wi-Fi/Bluetooth communication security. We will improve the lab environment setup and the lab instructions. We will also work on offering a dedicated undergraduate mobile security course.

8. ACKNOWLEDGMENTS

The work is partially supported by the National Science Foundation under DUE award: SFS #1241651: Capacity Building in Mobile Security Through Curriculum and Faculty Development and CCLI #0942097, #0942140: Portable, Modular, and Modern Technology Infused labware for Broader Embedded Systems Education. 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

9. REFERENCES

[1] P. Alto, "Smart phones overtake client PCs in 2011," Canalys, Feb. 2012, accessed in Feb 2012, http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011.

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

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

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

[5] 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.

[6] E. Geier, "2012 in Security: Rising Danger," PCWorld.com, Oct. 20, 2011, accessed on Mar. 10, 2012, http://www.pcworld.com/article/242174/2012_in_security_rising_danger.html.

[7] M.J. Schwartz, "Best Paying IT Security Jobs In 2012," InformationWeek.com, Nov. 25 2011, http://www.informationweek.com/news/security/management/232200152, accessed on Apr. 5, 2012.

[8] S. Diaz, "Mobile security needs more than just software, needs education," July 1, 2010, http://www.zdnet.com/blog/btl/mobile-security-needs-more-than-just-software-needs-education/36437, accessed on Jan 20, 2012.

[9] Stanford University, "XACS215 Mobile Security," accessed on May 1, 2012, http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=13070857.

[10] SANS.org, "Mobile Device Security," https://www.sans.org/security-training/mobile-device-security-5021-tid, accessed on Mar. 20, 2012.

[11] TONEX.com, "Course 90018: Mobile Applications Security Training - Mobile App Security Training course-Mobile Security Training," http://www.tonex.com/BootCamps/751, accessed on May 5, 2012.

[12] comSCORE, Inc., "comScore Reports March 2012 U.S. Mobile Subscriber Market Share," http://www.comscore.com/Press_Events/Press_Releases/2012/5/comScore_Reports_March_2012_U.S._Mobile_Subscriber_Market_Share, May 1, 2012, accessed on May 2, 2012.

[13] D. Reisigner, "Android Security Is a Major Threat: 10 Reasons Why," Apr. 04, 2012, http://mobile.eweek.com/c/a/Mobile-and-Wireless/Android-Security-Is-a-Major-Threat-10-Reasons-Why-148798, Apr. 06, 2012.

[14] W. Du, K. Jayaraman, and N. Gaubatz, "Enhancing Security Education with Hands-on Laboratory Exercises," In *Proceedings of the fifth Annual Symposium on Information Assurance (ASIA '10)*, June 16-17, 2010, Albany, New York.

[15] S. Caltagirone, P. Ortman, S. Melton, D. Manz, K. King, and P.W. Oman, "RADICL: A Reconfigurable Attack-Defend Instructional Computing Laboratory," *Security and Management*, Jun. 20-23, 2005, Las Vegas, Nevada, USA.

[16] W. Yurcik and D. Doss, "Different Approaches in the Teaching of Information Systems Security," in *Proceedings of the 2001 Information Systems Education Conference (ISECON'01)*, Nov. 2001, Cincinnati, OH, USA.

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

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

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

[20] M. Ahamad, et al., "Emerging Cyber Threats Report 2012," Oct. 2011, accessed on Apr. 20, 2012, http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf.

[21] ACM/IEEE the Joint Task Force on Computing Curricula, Computer Science Curricula 2013: Strawman Draft, Feb. 2012, http://ai.stanford.edu/users/sahami/CS2013/strawman-draft/cs2013-strawman.pdf, accessed on Mar. 12, 2012.

[22] 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.

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

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

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