Editors: Cynthia Irvine, irvine@nps.edu | Alec Yasinsac, yasinsac@southalabama.edu

Learning Mobile Security with Labware

Prabir Bhattacharya | University of Cincinnati
Li Yang | University of Tennessee at Chattanooga
Minzhe Guo | University of Cincinnati
Kai Qian and Ming Yang | Southern Polytechnic State University

Over the past decade, the use of mobile devices for both personal and business purposes has exploded. In 2011, manufacturers shipped about 400 million iOS and Android smartphones and tablets, compared to 350 million netbooks, notebooks, and desktop machines.[1] More important, more than 600,000 apps have been available for iOS and Android devices,[2] turning them into powerful general-purpose computing platforms.

As mobile platforms become increasingly popular, so do the incentives for attackers, especially when mobile payment transactions are projected to reach almost US$630 billion by 2014.[2] Recent security surveys describe the rapidly increasing number and sophistication of mobile attacks.[2] Mobile devices' prevalence and mobile threats' rapid growth have resulted in a shortage of mobile-security personnel.

In addition, traditional security threats—for example, malware or social engineering—are evolving in this new mobile environment. For example, attackers are using new vectors or adapting to the new platforms. Also, new components (such as GPS) and services (such as short message service [SMS] and mobile payments) in mobile platforms introduce new sources of risks.

Few security courses cover the spectrum of mobile security, especially those new and unique mobile-security threats. Also, there's a shortage of effective mobile-security learning materials, compared to the rich learning materials available for general computer security or other special security areas. In addition, there's a lack of hands-on laboratory resources.

To meet the need for mobile-security education, we're exploring an approach that exploits the benefits of mobile devices and best practices in information security education. This approach aims to promote students' interests and increase their self-efficacy. To improve learning, we developed a collection of labware using Android devices.

Mobile Security in a Nutshell

Mobile security covers threats to, attacks on, and defenses of mobile-computing platforms; it spans secure coding, cryptography, physical security, secure communication, and policy management. You can compare mobile-OS security models in terms of

- traditional access control approaches,
- application provenance that stamps an application with its author's identity,
- encryption that conceals data at rest to address device loss or theft,
- isolation (sandboxing) that limits an application's ability to access the sensitive data or systems on a device, and
- access control that grants a set of permissions to each application, thereby restricting each application to the device data or systems within its permissions' scope.

Types of Threats

Threats to mobile applications come in various forms. For example, mobile malware can collect data without a user's knowledge or approval, gather sensitive or personally identifiable information, or leave a security hole in the device. Mobile-malware functions include activity monitoring and data retrieval, system modification, and unauthorized dialing.

Web- and network-based threats exploit flaws of web-based applications and networks. They include user interface impersonation, client-side attacks such as cross-application scripting attacks, server-side attacks such as Android drive-by-download attacks, unauthorized network connectivity, and Wi-Fi sniffing.

Another type of threat occurs

1540-7993/14/$31.00 © 2014 IEEE Copublished by the IEEE Computer and Reliability Societies

Table 1. The seven modules in the Android security labware.

Category	Modules	Information assurance and security (ISA) topics
Mobile-device security and privacy	Lost or Stolen Mobile Devices	ISA fundamental concepts
	Unauthorized Mobile-Resource Access	Security architecture and system administration
	Mobile Privacy Threat	Cryptography
Mobile-app security	Mobile Malware	ISA fundamental concepts
	Secure Mobile-App Development	Secure software design and engineering
		Security architecture and system administration
Mobile network and communication security	Mobile SMS (short message service) Security	ISA fundamental concepts
	Mobile Phishing Threats	Cryptography
		Network security
		Security policy and governance

when someone's mobile device is lost or stolen. In such cases, personal information on the device, such as contacts and locations, might be at risk.

Threats also come from vulnerabilities due to errors in application design or implementation. These vulnerabilities can expose the mobile data to interception by attackers. They can also expose the mobile device or cloud applications used with the device to unauthorized access.

Securing Mobile Devices and Applications

You can employ several approaches to make mobile devices and applications secure. Secure coding and development involves input validation; blacklists; whitelists; the avoidance of storing secrets in mobile-application code; a least-privilege model for system access; isolating file systems and databases; security testing for buffer overflows, integer overflows, and vulnerabilities from formatting strings; and so on. Cryptography can protect data at rest and in transit and can be used in mobile authentication and security protocols. Security policies are needed when you're managing permissions to subsystems such as networking, messaging, address books, and GPS. Finally, security governance is useful in digital signing models, vetting, and distribution channels. For example, an enterprise sandbox as a governance approach can divide the device's content into different zones for different data types.

A Learning Approach to Mobile Security

We employ experience-based learning that couples mobile-threat analysis with protection solution practices. In particular, to make the learning more effective, for each specific mobile threat, students experience an actual attack instance. Then, they learn how to implement a protection solution.

Employing Threat Analysis

In traditional computer security classes, the protection principles and practices are the central topics. However, by experiencing actual attacks, students gain more insight, which enables them to design and implement better protections.[3] Such an attack/defend approach is considered highly effective for learning information security.

We adopted the idea of understanding the protection task better from threat analysis, but our approach differs from the traditional attack/defend approach in three ways. First, we develop multimedia or mobile apps that demonstrate attack instances. Second, students don't design attacks and don't perform them to harm servers or peers' mobile devices. Finally, the attack apps aim only to help students analyze mobile threats. The apps are hard-coded; the complete source code is hidden from students and isn't distributed.

Relevant Real-World Learning

A recent report pointed out that rather than only teaching abstract concepts and assigning abstract exercises, courses that also engage students in real-world settings will promote effective security education.[4] We approach such relevant real-world learning in three ways:

First, step-by-step tutorials help students learn to develop mobile apps for real devices. Each app implements a specific protection solution. Students can develop and debug apps with emulators or real devices, and they can install their apps on real devices. This provides instant gratification, builds confidence from hands-on practice, and encourages students to create their own apps. This not only facilitates their learning of mobile-programming skills but also heightens their

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 what their consequences are.
- 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:

- Prelab 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 application package file [apk], eclipse project with code)
- Postlab Activities
  - ☐ Case Study: An Instance of Smishing Attack (slides)
  - ☐ Review questions
  - ☐ Assignments

Figure 1. The Mobile SMS (short message service) Security module. The pairing of SMS threat analysis and protection practices helps students understand how the mobile attacks and protection solutions take effect.

awareness and understanding of secure-programming principles.

Second, we cover current mobile threats and protections. We provide students with the state-of-the-art mobile-security knowledge. We design the course materials by collecting and analyzing recent mobile-security papers from academia and industry.

Finally, our students perform hands-on experiments with mobile devices. We design most of the exercises such that students can perform them directly on mobile devices. This helps strongly connect the students' academic study with the reality of their lives and engages them in the educational process.

The Android Security Labware

Our Android labware provides students with hands-on mobile-security experience that will further promote their interest and engagement in security. It enables them to gain real-world experience in securing mobile devices, developing secure mobile apps, and conducting penetration testing for mobile devices and mobile apps.

Our labware comprises seven self-contained modules covering important threats related to mobile-device security and privacy, mobile-app security, and mobile network and communication security (see Table 1). Each module includes

- prelab activities (concept introduction and lab preparation),
- two hands-on lab activities (one on analyzing the threat and the other on the related protection solution), and
- postlab activities (review questions, assignments, and a case study).

To host the labware for wide access and collaboration, we developed an open repository. More information on the labware is at https://sites.google.com/site/mobilesecuritylabware/home.

Figure 1 shows the design of the Mobile SMS Security module. In the module's threat analysis part, an attacker installs a malicious SMS broadcast listener on the victim's

Related Work in Mobile-Security Education

Mobile-security courses remain sparse in most computing curricula. Patrick Tague offered a project-based mobile-security course at Carnegie Mellon University that provided students with topics for discussion and exploration.[1] In contrast, we emphasize learning mobile security through hands-on experience, and our program offers a fully developed lab environment and learning materials. Our use of Android engages students' interests in learning and has improved our teaching's effectiveness.

Reference

1. P. Tague, "14-829: Mobile Security—Fall 2011," 2011; http://wnss.sv.cmu.edu/courses/14829-f11.

mobile phone. By remotely controlling the listener, the attacker gains unauthorized access to contact lists on the victim's phone. The victim has no idea of the attacker's messages.

In the protection solution part, the students implement a mobile app for protecting against this attack. In this app, students practice using a filter to block suspicious SMS messages from unknown users.

We integrated our labware into two information security courses in two semesters.[5] Forty students participated in the initial evaluation of our approach and materials. Most of them provided positive feedback and enjoyed the Android security practices.

We plan to add more modules, such as ones on mobile-browser security and Wi-Fi and Bluetooth communication security. We'll also improve the lab environment setup and the lab instructions. In addition, we'll work on offering a dedicated undergraduate mobile-security course.

For a look at another approach to mobile-security education, see the sidebar. ■

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant Nos. 1241651, 0942097, 0942140, and 0942581. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

1. P. Alto, "Smart Phones Overtake Client PCs in 2011," Canalys, 3 Feb. 2012; www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011.
2. E. Geier, "2012 in Security: Rising Danger," *PCWorld*, 20 Oct. 2011; www.pcworld.com/article/242174/2012_in_security_rising_danger.html.
3. "The Future of Mobile Computing," EDUCAUSE, 2011; http://net.educause.edu/ir/library/pdf/ESPNT1b.pdf.
4. S. Loveland, "Human Computer Interaction That Reaches beyond Desktop Applications," *Proc. 42nd ACM Tech. Symp. Computer Science Education* (SIGCSE 11), 2011, pp. 595–600.
5. M. Guo et al., "Learning Mobile Security with Android Security Labware," *Proc. 44th Ann. ACM Tech. Symp. Computer Science Education* (SIGCSE 13), 2013, pp. 675–680.

Prabir Bhattacharya is a professor at the University of Cincinnati's Department of Electrical Engineering and Computing Systems. Contact him at bhattapr@ucmail.uc.edu.

Li Yang is an associate professor in the Department of Computer Science and Engineering at the University of Tennessee at Chattanooga. Contact her at li-yang@utc.edu.

Minzhe Guo is a PhD candidate at the University of Cincinnati's School of Computing Sciences and Informatics. Contact him at guome@mail.uc.edu.

Kai Qian is a professor of computer science at Southern Polytechnic State University. Contact him at kqian@spsu.edu.

Ming Yang is an associate professor in Southern Polytechnic State University's Information Technology Department. Contact him at mingyang@spsu.edu.