Teaching mobile computing and mobile security

Xiaohong Yuan, Kenneth Williams
Department of Computer Science
North Carolina Agricultural & Technical State University
Greensboro, NC, USA

Kelvin Bryant, Jinsheng Xu, Albert Esterline
Department of Computer Science
North Carolina Agricultural &Technical State University
Greensboro, NC, USA

Scott McCrickard
Department of Computer Science
Virginia Tech
Blacksburg, VA, USA

Anyi Liu
Department of Computer Science
Indiana University-Purdue University Fort Wayne
Fort Wayne, Indiana, USA

Charles Hardnett
Department of Computer Science
Gwinnett Technical College
Alpharetta, GA, USA

Selvarajah Mohanarajah
Department of Computer Science
Claflin University
Orangeburg, SC, USA

Litany H. Lineberry
Department of Computer Science
Voorhees College
Denmark, SC, USA

Rachel Rutledge
Dept. of Computer Science
Charleston County School District
Charleston, SC, USA

***Abstract*—Due to the popularity of mobile devices, it is important to teach mobile computing and security to students in colleges and universities. This paper describes eight course modules on mobile computing and security we developed that could be integrated into a computer science curriculum. These course modules were presented at a faculty workshop. Workshop evaluation includes a survey questionnaire and reflective narratives from participants. The workshop evaluation results are discussed in this paper. The course modules can be adopted by instructors teaching mobile application development, cyber security or other related courses.**

Keywords— Java; Android; Education; Course

I. INTRODUCTION

Mobile devices have become extremely popular and have become an important platform for software developers. Worldwide unit sales of smartphones to end users in 2014 totaled 1.2 billion, a 28.4 percent increase from 2013 [1]. According to Statista, the number of apps available in Google Play store was 1.6 million, and worldwide mobile app revenue reached $34.99 billion in 2014 [2]. Such growth has resulted in a large number of jobs related to mobile app development.

As mobile devices grow in popularity as computing platforms and data storage units, privacy and security issues for mobile computing are increasing. Mobile devices have attracted both targeted and mass-scale attacks. In one mobile attack, over 250,000 Android users were compromised when they downloaded malicious software disguised as legitimate applications from the Android Market [3]. As many organizations are adopting “Bring Your Own Device" (BYOD) where employees are allowed to bring their own mobile devices, the security issues related to mobile computing are becoming ever more important.

When used as teaching platforms in computer science education, mobile devices enable students to learn in a modern context. Mobile application development has become an important topic in computing curricula partly due to the popularity of consumer mobile devices and a shift in the computing landscape towards mobile app development. The security of mobile computing becomes vital to the growing population of users and for the future of our social, economic and political systems. Therefore, it is vitally important to provide education in mobile computing and security to students in computer science and other related disciplines.

Many schools have crafted courses or course modules that address mobile application development issues. Fenwicks, J. B. et al. [4] reported experiences in offering mobile device programming courses in two schools. Both courses include a project in which students proposed and developed a mobile application. Mahmound and Popowicz [5] proposed the approach of using mobile devices and mobile application development as a mechanism to teach introductory programming to computer science, information technology, and computer engineering students. Their rationale is that such an approach can produce more flexible programmers since students could apply knowledge gained in mobile computing to traditional development. Riley [6] reported the experience of teaching C/C++ programmers how to develop OO Java software using the Android mobile operating system platform.

While security is a popular topic in computing curricula, it is rarer to find examples of mobile security. Educational venues like CMU, Stanford, and the SANS Institute offer courses on mobile security, though they tend to be professional development courses [7,8,9]. Such courses cover a wide range of topics, including mobile device threats, mobile device architecture security and management; mobile code and application analysis, ethical hacking of mobile devices, mobile location privacy; and ad hoc, mesh, and sensor network security. All of these security-related topics were considered for our course modules. In more traditional academic settings, Guo and his colleagues developed the Android Security Labware [10, 11] including lab modules that demonstrate mobile security concepts such as threats to mobile security, mobile malware, and secure mobile app development.

With the support of an NSF project, the Department of Computer Science at North Carolina Agricultural &Technical State University (NC A&T) sought to develop course modules on mobile computing and mobile security, testing them in existing computer science courses. Our modules cover similar topics as described in the literature, but with broader resources, encouraging different learning styles. We sought to develop course module materials that would be beneficial to computer science educators across the undergraduate curriculum who are considering including mobile computing and mobile security.

To encourage broad feedback and dissemination of the course modules we developed a 2-day faculty workshop held in July 2015 at NC A&T. Twenty faculty members from 20 different institutions attended the workshop. The workshop attendees are from diverse settings, including research-oriented universities, teaching-oriented universities (2-year and 4-year), minority institutions such as Historically Black Colleges and Universities (HBCUs), Hispanic Serving Institutes (HSIs), and a woman's college, as well as 2-year Community Colleges, and a high school.

This paper reports our experience of holding the workshop. Section 2 describes the course modules on mobile computing and security presented at the workshop. Section 3 presents the findings from the evaluation of the workshops. Section 4 offers conclusions and future work.

II. Course Modules on Mobile Computing and Mobile Security

Eight course modules were presented during the faculty summer workshop on mobile computing and mobile security. These modules were developed based on what the project PIs identified as important knowledge in mobile computing and security fields that students should learn, based on experiences, related work review, and opportunities for seamless integration into existing computing curricula. Each module includes multiple learning tools, including slides, handouts, historical perspectives, activities, and homework assignments. The modules have been used in classroom situations as well as in a teachers' workshop, and they are designed to be used in a dedicated course or in separate courses. All teaching materials are available at: http://williams.comp.ncat.edu/mobile/

A. Course Module: Introduction to Mobile Programming

This module introduces the core aspects necessary for students to begin programming mobile devices running the Android operating system. It first provides context to programming mobile devices by presenting a brief history of mobile devices, a description of common features found in current mobile devices and available platforms and related tools for mobile application development. It then covers topics such as setting up the Android SDK and related tools, the development workflow and creating Graphical User Interfaces (GUIs) using the Activity class. Emphasis is placed on exposing general concepts and terminology to serve as a foundation for other mobile computing learning modules and personal investigation. This module has been taught in the freshman-level general engineering course GEEN165 Computer Program Design at North Carolina A&T State University.

The learning objectives of this course module are: Upon successfully completing this module, students will be able to install and configure an Android development environment, create a simple Android application based on the Activity component/class, and execute the app on an actual Android mobile device (or an Android Virtual Device (AVD) if an actual device is not available).

The course module materials include two PowerPoint presentations that instructors can use for class presentation and a hands-on learning assignment. For the hands-on learning assignment, students will install the Android SDK and the Android Development Tool Plug-in to enable development using the Android Studio IDE. They will then create an Android project using provided source code and complete the development life cycle by loading and running the compiled application.

A subsequent laboratory-based exercise describes a complete walkthrough in which students author a simple calculator app consisting of an interface and the backend Java code for responding to the interface events for performing simple calculations. Detailed lab instructions with screenshots for using Eclipse and the Android Studio development environments are provided. A lesson plan that guides the instructor's use of this course module is also provided.

B. Course Module: Mobile Application Development

This module provides a graphical user interface (GUI) based overview to mobile application development, covering four topics: 1) Introductory material for mobile computing; 2) Creating an Activity (Android GUI); 3) Accessing content providers; 4) Leveraging services and broadcast receivers. The focus of the module is to expose the student to the techniques used to utilize some of the advanced features of an Android device (camera, accelerometer, GPS, etc.) in their apps. This course module has been taught in a junior-level COMP365 Programming Methodologies and Concepts course.

The learning objectives of this course module are: Upon successfully completing this module, students gain a deeper understanding of the major Android components: Activities, Content Providers, Services and Broadcast Receivers. Students will create a more advanced Android app that not only includes an Activity but also uses more advanced concepts (GPS and Location features).

The course module materials include four sets of PowerPoint slides and associated documents that introduce the topics of this module. The hands-on learning assignment guides the student through creating an Android app that will display a given location address on a map. The user will input a location in a textbox, click a button and the app will then update a map displaying a marker at the supplied address.

C. Course Module: Emerging Security Issues in Mobile Computing

This module teaches mobile security concepts using real-world case studies. It also includes an introduction to various vulnerabilities specific to mobile devices. This module has been taught in a senior-level COMP420 Applied Network Security course.

The learning objectives of this course module are: Upon successfully completing this module, students will understand the vulnerabilities of mobile computing devices and know the countermeasures against them.

The course module materials include two PowerPoint slide sets introducing the vulnerabilities of mobile devices, and two case studies on mobile security. One case study is about Masa Kagawa, who was arrested for running an Android malware ring and operating a scam dating site in the form of an Android application. Another case study is about Stealth Genie, a spyware application (mobile app) that could monitor calls, texts, videos and other communications on mobile phones without the user’s awareness. The course module also includes a homework assignment based on the presentation slides and the case studies.

D.Course Module: Mobile Malware

This module focuses on mobile malware, including different types, its spread and how to protect mobile devices from infection. This module has been taught in a junior-level COMP321 Computer System Security course.

The learning objectives of this course module are: Upon successfully completing this module, students will be able to discuss the intent, behavior, and security consequences of mobile malware and propose possible countermeasures.

The course module materials include a document introducing the topic of mobile malware, a PowerPoint slide that is associated with the document, and a hands-on learning exercise. In the hands-on learning assignment, students will exploit the functions of the mobile malware AndroRAT. The students will analyze the security risks caused by the AndroRAT Trojan and create real-life scenarios where AndroRAT can be used for attacking or for benevolent purposes. The students will also use AntiVirus Software to detect AndroRAT and observe the results.

E. Course Module: Security Policy in Mobile Computing

This module discusses the importance of security policies that drive the protection procedures in an enterprise. It covers topics such as mobile security risks, guidelines for managing the security of mobile devices in the enterprise, threats to mobile devices and mitigation strategies, Bring Your Own Device (BYOD) security risks and challenges, and policies for BYOD. This module has been taught in a junior-level COMP320 Fundamentals of Information Assurance course.

The learning objectives of this course module are: Upon successfully completing this module, students will be able to explain the risks of mobile devices in an enterprise, and discuss mitigation strategies. Students should also be able to critique and develop security policies for mobile devices in an enterprise.

The course module materials include a document introducing the topic, and associated PowerPoint slides. They also include case study assignments. Students will read several cases of how government agencies deployed BYOD, and discuss how these agencies addressed security risks and other issues of BYOD as well as the benefits of BYOD.

F. Course Module: Mobile Operating Systems

Operating systems for mobile devices sometimes take a different approach to implementing the usual OS features such as memory management, inter-process communication, access control and virtual machine support. This module teaches the students the different design options taken by hand-held operating systems. This course module has been taught in a senior-level COMP450 Operating Systems course.

The learning objective of this course module is: Upon successfully completing this module, students will be able to explain the impact of OS design choices used by hand-held operating systems.

The course module materials include lecture slides and a hands-on learning assignment. The PowerPoint slides cover an overview of the Android operating system and details on design decisions that differ from desktop OS. In the hands-on learning assignment, students run concurrent memory stress programs and observe the results on the Windows system and the Android operating system. The memory stress program randomly accesses a large array. About one in three accesses to the array is a memory write. With a random memory access pattern that changes many of the memory pages, this creates a worst case scenario for virtual memory. Students will watch the memory graph of the Task Manager while the memory stress programs are running. Students will also observe the changes of CPU utilization, and explain what happened and why.

G. Course Module: Hand-Held Internet Systems

This module teaches students how to use the jQuery Mobile JavaScript library, which is built on top the jQuery JavaScript library. This library provides an intuitive and efficient way to create web pages that accommodate the constraints of mobile devices. This module has been used in a junior-level course COMP322 Internet Systems.

The learning objective of this module is: Upon successfully completing this module, students will be able to use the jQuery Mobile library to create web pages that accommodate the constraints of hand-held devices.

The course module materials include lecture slides on JQuery Mobile and hands-on learning assignments. We concentrate on HTML5 custom data attributes for embedding attributes on HTML elements, show how to define roles for elements, and present the theming system used in jQuery Mobile. Besides presentation, we also cover the custom events offered by jQuery Mobile and communication with the server. Even though jQuery Mobile ordinarily communicates with the server with Ajax, we cover communication without Ajax to keep the discussion simple. Hands-on assignments provide practice in all the topics covered in the lecture slides.

H.Course Module: Cryptography on Android

This course module teaches students how to develop secure Android applications by correctly using Android's cryptography APIs. This course module is targeted at two areas where programmers commonly make many mistakes: password based encryption and SSL certificate validation. This module will be taught in a senior-level COMP420 Applied Network Security course.

The learning objectives of the course module are: Upon completion of the course module, students will be able to do the following: 1) Use the Android cryptography SDK to correctly implement password based encryption. 2) Correctly validate digital certificate and secure communication between a mobile app and web service using SSL. 3) Identify the weaknesses in programs that use Android Cryptography APIs. 4) Apply knowledge of cryptography to real-world problem solving.

The course module materials include presentation slides and a hands-on learning assignment. The presentation slides introduce common mistakes programmers make when developing apps that use Android cryptography APIs and SSL. The slides also present recommendations of good practices for using cryptography APIs and SSL. In the hands-on learning assignment, students are asked to secure an existing Android app by using cryptographic APIs. This Android app is an online contact list app that allows users to access their contacts from anywhere and from any Android device. The app retrieves and stores the contacts on a web server with a XML based web service API. The web server, and the source code of the insecure app are provided to the students

III. WORKSHOP ASSESSMENT

The modules were featured in a 2-day instructor workshop to assess the value (and projected value) of each module. Participants gave brief overviews of their institutional goals and directions on the first day, then took part in interactive hands-on learning sessions centered on the modules in Section 2. Feedback from the participants was collected in two ways: via an opinion survey (summarized in Section A) that all participants completed, and optional reflective narratives completed by 6 of the workshop participants several weeks after the workshop, giving time for reflection (summarized in Section B).

A. Workshop participant opinion survey

A survey of the participants was conducted at the end of the workshop to evaluate the effectiveness of the workshop and collect feedback from the participants. The average rating of participants' overall satisfaction with the workshop is 3.93 out of 5 (where 5 corresponds to most satisfied). Table 1 lists the average ratings of the effectiveness of workshop presentations and lab sessions, and the usefulness of the information presented at the workshop as it relates to the workshop participants' teaching and research on a 5 point scale (where 5 corresponds to most effective and useful).

TABLE I. WORKSHOP SURVEY RESULTS

Presentation and Lab Session	**Average Rating of Effectiveness**	**Average Rating of Usefulness**
Introduction of Mobile Programming Presentation	4.0	3.81
Introduction of Mobile Programming hands-on Activities	3.89	
Mobile Program Development Presentation	3.94	3.62
Mobile Program Development Hands-on Activities	3.94	
Emerging Security issues in Mobile Computing Presentation	3.5	3.73
Cipher Programming in Mobile Devices Presentation	3.65	3.31
Cipher Programming in Mobile Devices Hands-on Activities	3.06	
Mobile Malware Presentation	3.88	3.56
Mobile Malware Hands-on Activities	4.06	
Mobile Policy Presentation	3.76	3.56
Mobile Operating System Presentation	4.38	3.63
Mobile Operating System Hands-on Activity	4.18	
Hand-held Internet Systems Presentation	3.31	3.75

With most of the average ratings of module effectiveness and usefulness in the 3 to 4 range, it indicates the modules were moderately successful. Based on the suggestions from workshop participants, the course modules could be improved by providing clearer instructions on some of the lab document. The workshop could be improved by making the goals/objectives of each session clear at the beginning of each session; and by having more discussion after each exercise.

The participants commented that the workshop helped the attendees to implement the course modules in their classrooms; and provided good networking, conversation, and resource sharing opportunities. The workshop included up-to-date information and well-designed hands-on projects.

B. Reflection from Workshop Participants

After the workshop, we followed up with workshop participants and asked them to comment on their teaching approaches to mobile, the utility (actual and perceived) of the course modules, anticipation of course modules that seem particularly useful for adoption, and ideas about future education and research in the field of mobile computing and mobile security. Their participation is voluntary, but not anonymous. Six workshop participants from diverse universities/school provided reflective narratives. The findings from the reflective narratives are presented below.

Several workshop participants reported that their universities already offer one or two courses on mobile application development. They mentioned that the course modules “Introduction to Mobile Programming” and “Mobile Application Development” could be adopted by incorporating the hands-on labs of the modules in homework and projects of the their mobile application development courses. Some mentioned that these two modules could be used as a preparation for their mobile application development courses.

The course module “Cryptography on Android” focuses on programming-related skills (e.g., password-based encryption, SSL certificate validation) that are important for any advanced designer who might be working with sensitive materials. The module could be covered quickly in a single course session, or extended with the module's lab unit and an activity or homework to cover multiple sessions. If time is at a premium, a portion of a class session could focus on a subset of the material (e.g., passwords). Knowledge of security-related issues could be assessed through homework and a course project. The “Cryptography on Android” module could be integrated into a mobile application development course, a cryptography course, or a cyber security course that introduces ciphers, public key systems, key management, certificate, etc.

One participant plans to integrate the course module “Emerging Security Issues in Mobile Computing” into the course “Introduction to Information Assurance” in his university. He also plan to integrate the course module “Security Policy in Mobile Computing” into the course “Cyber Security Planning and Management”.

One participant plans to integrate the “Mobile Malware” module into the course “Information Assurance and Digital Forensics” at his university. Students can construct and implant their customized malware on their mobile devices, and control it remotely. Several participants mentioned they will integrate the “Mobile Operating Systems” module into their Operating Systems courses.

Workshop participants also generated ideas to extend the course modules presented at the workshop. One suggestion is that, some intrusion detection-related lab modules can be developed to detect the breaches by either monitoring the networking traffic or running host intrusion detection system (HIDS) on students’ devices. With more time, students can also evaluate the overheads and power consumptions for the exploits and HIDS. In addition, students can also be assigned some tasks related to mobile-device forensics. As the expected learning outcome, students should be able to design and implement exploits that compromise the current mobile devices. More importantly, they should be able to evaluate and justify different countermeasures against the exploits and employ the secure forensic process to collect and preserve the evidence.

One participant from a 2-year community college plans to extend the course modules presented in the workshop by porting the hands-on labs in “Introduction to Mobile Programming”, “Mobile Application Development”, “Mobile Operating Systems”, and “Cryptography on Android” to their other course topics: iOS development, Windows Phone development, and cross-platform development. They also plan to adapt the mobile security policy materials to have the perspective of a software developer.

It has also been pointed out that Mobile Malware course module may be suited for a cyber security course in K-12 public education. To truly build the field of Cyber Security in our nation in the future, interest should be developed at a younger age. Future research opportunities could include issues dealing with integration of a Cyber Security curriculum in a 9-12 classroom.

IV. Conclusion and Future Work

This paper describes a collection of eight ready-to-use modules on mobile computing and mobile security. The modules were featured in a two-day workshop with 20 attendees. Despite a great range of program types, there seemed to be consensus that there was value in this type of repository, as reflected in six reflective narratives from attendees. A survey of all workshop attendees revealed that the course modules were moderately successful. It was found from the reflective narratives that these course modules could be adopted in a variety of courses in an undergraduate computer science curriculum, in diverse institutions.

The workshop touched on a broad range of mobile topics that can foster educational research pursuits. Many of the schools represented at the workshop are developing courses, degrees, minors, and certificates that focus on mobile devices, mobile security, and related concepts like mobile interfaces, and cloud computing. A course module dedicated to Mobile Cloud Computing where students could explore different cloud based resources by looking at the architecture of Mobile Cloud Computing, Security and Privacy could prove useful. It could be offered as a standalone course or adopted into any computer science or cyber security course already in existence. Course modules on intrusion detection, mobile device forensics, and secure mobile development could also be useful. Future work could also include integrating Cyber Security in a 9-12 classroom.

Acknowledgment

This work is partially supported by National Science Foundation (NSF) under the award HRD-1332504. 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 NSF.

References

[1] Gartner, "Gartner Says Smartphone Sales Surpassed One Billion Units in 2014", March 2015, http://www.gartner.com/newsroom/id/2996817

[2] Statista, "Statistics and facts about Mobile App Usage", June 2014, http://www.statista.com/topics/1002/mobile-app-usage/

[3] Lookout Mobile Security Blog (March 2011), "Update: Security Alert: DroidDream Malware Found in Official Android Market," Retrieved on August 28, 2015, from http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/

[4] Fenwick, James, Kurtz, Barry, Hollingsworth, Joel, "Teaching mobile computing and developing software to support computer science education", in *Proceedings of the 42nd ACM technical symposium on Computer science education (SIGCSE '11)*, pp 589-594

[5] Qusay H. Mahmoud and Pawel Popowicz, "A Mobile Application Development Approach to Teaching Introductory Programming", *Frontiers in Education Conference (FIE), 2010 IEEE*, T4F-1 - T4F-6, Oct. 27-30, 2010, Washington, DC, DOI:10.1109/FIE.2010.5673608

[6] Riley, D., "Using mobile phone programming to teach Java and advanced programming to computer scientists", in *Proceedings of the 43rd ACM technical symposium on Computer Science Education (SIGCSE'12)*, pp 541-546.

[7] Wright, J. (2014). "SEC575: Mobile Device Security and Ethical Hacking", *SANS Institute* Retrieved on July 8th, 2014, from http://www.sans.org/course/mobile-device-security-ethical-hacking

[8] Boneh, D., Daswani, N., Mitchell, J. XACS215 - Mobile Security. *Stanford Center for Professional Development*. Retrieved on July 8th, 2014, from http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=13070857

[9] Tague, P (2013). "14-829: Mobile Security", *Carnegie Mellon University*. retrieved on July 21, 2014, from: http://wnss.sv.cmu.edu/courses/14829/f13/

[10] Bhattacharya, P. "SMART: Real World Relevant Security Labware for Mobile Threat Analysis and Protection Experience", *Mobile Security Labware*. Retrieved July, 21, from https://sites.google.com/site/mobilesecuritylabware/home

[11] Guo, M., Bhattacharya, P., Yang, M., Qian, K., Yang, L (2013), "Learning Mobile Security with Android Security Labware", *In: Proc. of the 44th ACM technical symposium on Computer science education (SIGCSE'13)*, pp 675-680.