

## Educating on Mobile Computing and Security Practices

Yusfrizal<sup>1</sup>, Yahya Tanjung<sup>2</sup>, Heri Gunawan<sup>3</sup>


<sup>1,3</sup>Department of Information Management, Gihon Polytechnic, Indonesia

<sup>2</sup>Management, Potensi Utama University, Indonesia

### ABSTRACT

With the increasing popularity of mobile devices, it has become essential to educate college and university students about mobile computing and security. This paper introduces eight course modules on mobile computing and security that we designed to integrate seamlessly into a computer science curriculum. These modules were showcased during a faculty workshop, where feedback was gathered through survey questionnaires and participants' reflective narratives. The evaluation results from the workshop are analyzed and discussed in this paper. These modules are adaptable for educators teaching mobile application development, cyber security, or other related subjects.

**Keyword:** mobile computing; security; mobile application.

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

#### Corresponding Author:

Yusfrizal,  
Department of Information Management  
Gihon Polytechnic  
Jl. Dalil Tani No.48, Tomuan, Siantar, Indonesia.  
Email : yusfrizal80@gmail.com

#### Article history:

Received Oct 19, 2024  
Revised Oct 23, 2024  
Accepted Oct 30, 2024

### 1. INTRODUCTION

Mobile devices have gained immense popularity and have emerged as a key platform for software developers. In 2014, global smartphone sales to end users reached 1.2 billion units, marking a 28.4 percent rise compared to 2013 (Thomas & Devi, 2021). According to Statista, the Google Play store offered 1.6 million apps, and global revenue from mobile apps reached \$34.99 billion in 2014 (Oh et al., 2022). This growth has led to a significant increase in job opportunities related to mobile app development.

As mobile devices continue to rise in popularity as both computing platforms and data storage tools, privacy and security concerns in mobile computing are also growing. These devices have become targets for both focused and large-scale attacks (Tabrizchi & Kuchaki Rafsanjani, 2020). For example, over 250,000 Android users were affected when they unknowingly downloaded malicious software disguised as legitimate apps from the Android Market. As more organizations implement "Bring Your Own Device" (BYOD) policies, where employees are permitted to use their personal mobile devices for work, mobile computing security issues are becoming increasingly critical (Hajare et al., 2021).

When integrated into computer science education, mobile devices offer students an opportunity to learn in a contemporary context. Mobile app development has emerged as a key topic in computing curricula, partly due to the widespread use of mobile devices and the shift toward mobile app development in the computing landscape. The security of mobile computing is crucial, considering the expanding user base and its impact on social, economic, and political systems (Parast et al., 2022). Hence, educating students in mobile computing and security has become essential for those studying computer science and related fields.

Many institutions have designed courses or modules that focus on mobile app development challenges. Fenwicks, J. B. et al. discussed their experiences in offering mobile device programming courses at two institutions. These courses involved projects where students proposed and developed mobile applications. Mahmoud and Popowicz recommended using mobile devices and app development as a method for teaching introductory programming to computer science, IT, and computer engineering students. Their argument is that this approach fosters more adaptable programmers, as students can apply mobile computing knowledge to traditional software development. Riley also shared insights from teaching C/C++ programmers how to develop object-oriented Java applications using the Android platform (Xu et al., 2024).

Although security is a common topic in computing curricula, mobile security is less frequently covered. Educational institutions like CMU, Stanford, and the SANS Institute offer mobile security courses, but these are usually aimed at professional development. These courses address various subjects, including mobile device threats, device architecture security, mobile application analysis, ethical hacking, location privacy, and network security. These topics were incorporated into our course modules. In traditional academic environments, Guo and his team developed Android Security Labware, which includes lab modules demonstrating key mobile security concepts, such as security threats, mobile malware, and secure app development (Lalande et al., 2019).

Supported by an NSF project, the Department of Computer Science at North Carolina Agricultural & Technical State University (NC A&T) set out to develop and test course modules on mobile computing and security within existing computer science courses. These modules cover similar topics to those found in the literature but are enriched with broader resources to accommodate diverse learning styles (Bryson & Andres, 2020). Our goal was to create materials that would be valuable for computer science educators across undergraduate programs interested in integrating mobile computing and security into their curriculum.

To foster widespread feedback and sharing of the developed course modules, a 2-day faculty workshop was organized in July 2015 at NC A&T (Education, 2021). The event saw 20 faculty members from 20 institutions participate, representing a range of academic environments, including research-focused universities, teaching-oriented institutions (both 2-year and 4-year), minority-serving colleges such as Historically Black Colleges and Universities (HBCUs), Hispanic Serving Institutions (HSIs), women's colleges, community colleges, and even a high school.

## 2. MODULES ON MOBILE COMPUTING AND MOBILE SECURITY COURSES

During the faculty summer workshop on mobile computing and security, eight course modules were introduced. These modules were created based on the key knowledge identified by the project principal investigators (PIs) as essential for students to learn in the fields of mobile computing and security. This was informed by their experiences, a review of related work, and the potential for smooth integration into existing computing curricula. Each module incorporates various learning materials, such as slides, handouts, historical context, activities, and assignments. The modules have been utilized in both classroom settings and teacher workshops, and they are designed to be implemented in a dedicated course or as part of separate courses (Dejene, 2019).

### A. Course Module: Basics of Mobile Programming

This module introduces the fundamental concepts required for students to start programming mobile devices that run on the Android operating system. It begins by providing context for mobile programming, including a brief history of mobile devices, an overview of common features in modern devices, and the platforms and tools available for mobile app development. The module then covers key topics such as installing the Android SDK and related tools, the development process, and creating Graphical User Interfaces (GUIs) using the Activity class (Dejene, 2019). The focus is on familiarizing students with general concepts and terminology, laying the groundwork for other mobile computing modules and independent exploration.

The learning objectives of this course module are as follows: After successfully completing the module, students will be able to set up and configure an Android development environment, build a basic Android application using the Activity component/class, and run the app on a physical Android device (or an Android Virtual Device (AVD) if no physical device is available) (Yasin, 2021).

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

A follow-up lab exercise provides a detailed step-by-step guide where students create a simple calculator app, including both the interface and the backend Java code to handle interface events for basic calculations. Comprehensive lab instructions, including screenshots for using both Eclipse and Android Studio, are provided. Additionally, a lesson plan to assist instructors in using this module is also included.

**B. Course Module: Development of Mobile Applications**

This module offers an overview of mobile application development through a graphical user interface (GUI), covering four main topics: 1) An introduction to mobile computing; 2) Creating an Activity (Android GUI); 3) Accessing content providers; 4) Using services and broadcast receivers. The module primarily aims to familiarize students with the techniques for integrating advanced features of an Android device, such as the camera, accelerometer, and GPS, into their applications (Reddy & Singaravelu, 2021).

The learning objectives of this course module are as follows: Upon completion of the module, students will have an enhanced understanding of the key Android components, including Activities, Content Providers, Services, and Broadcast Receivers. Students will also develop a more advanced Android application that incorporates an Activity and utilizes advanced features such as GPS and location services.

The materials for this course module include four sets of PowerPoint slides along with related documents that introduce the module's topics. The hands-on assignment guides students in creating an Android app that displays a location address on a map. Users will enter an address into a text box, click a button, and the app will update the map with a marker at the specified location.

**C. Course Module: New Security Challenges in Mobile Computing**

This module introduces mobile security concepts through real-world case studies and provides an overview of various vulnerabilities unique to mobile devices. It has been delivered as part of the senior-level COMP420 Applied Network Security course.

The learning objectives of this course module are as follows: Upon completing the module, students will gain an understanding of the vulnerabilities associated with mobile computing devices and learn the countermeasures to address them (Tahirkheli et al., 2021).

The module materials include two PowerPoint slide decks that introduce mobile device vulnerabilities and two case studies on mobile security. One case study discusses Masa Kagawa, who was arrested for operating an Android malware ring and a scam dating application. The other case study focuses on Stealth Genie, a spyware app capable of monitoring calls, texts, videos, and other communications on mobile devices without user awareness. Additionally, the module includes a homework assignment based on the slide presentations and case studies.

**D. Course Module: Malware on Mobile Devices**

This module covers mobile malware, exploring its various types, methods of propagation, and strategies to protect mobile devices from infection. It has been delivered as part of the junior-level COMP321 Computer System Security course.

The learning objectives of this course module are as follows: Upon completing this module, students will be able to discuss the purpose, behavior, and security impacts of mobile malware and suggest potential countermeasures (Damaraju, 2021).

The materials for this course module include a document introducing mobile malware, a related PowerPoint presentation, and a hands-on learning exercise. In the hands-on assignment, students will explore the functionality of the mobile malware AndroRAT. They will assess the security risks posed by the AndroRAT Trojan and create real-world scenarios in which AndroRAT could be used for malicious or ethical purposes. Additionally, students will utilize antivirus software to detect AndroRAT and analyze the results.

**E. Course Module: Mobile Computing Security Policies**

This module addresses the significance of security policies that guide protection measures within an organization. It covers topics like mobile security risks, guidelines for managing the security of mobile devices in the workplace, threats to mobile devices and strategies for mitigating them, security risks and challenges associated with Bring Your Own Device (BYOD), and BYOD-related policies. This module has been taught in the junior-level COMP320 Fundamentals of Information Assurance course.

The learning objectives of this course module are as follows: Upon completion of this module, students will be able to explain the risks associated with mobile devices in an enterprise setting and discuss strategies for mitigating these risks. Students will also be able to evaluate and develop security policies for mobile devices within an organization.

The materials for this course module include a document introducing the topic, along with related PowerPoint slides. Additionally, there are case study assignments where students will review several instances of government agencies implementing BYOD policies, and discuss how these agencies managed security risks, addressed other BYOD-related challenges, and benefited from BYOD adoption (Ratchford et al., 2022).

#### **F. Course Module: Operating Systems for Mobile Devices**

Mobile operating systems often adopt unique approaches to implementing standard OS features such as memory management, inter-process communication, access control, and virtual machine support. This module educates students about the various design choices made by handheld operating systems. It has been taught as part of the senior-level COMP450 Operating Systems course.

The learning objective of this course module is as follows: Upon completing this module, students will be able to explain the impact of design choices in operating systems used by handheld devices.

The course materials include lecture slides and a hands-on learning assignment. The PowerPoint slides provide an overview of the Android operating system and highlight design decisions that differentiate it from desktop operating systems. In the hands-on assignment, students will run concurrent memory stress programs and analyze the results on both Windows and Android systems. The memory stress program randomly accesses a large array, with approximately one in three accesses being a memory write. This random memory access pattern, which changes many memory pages, creates a worst-case scenario for virtual memory. Students will monitor the memory graph in the Task Manager while the stress programs run, observe CPU utilization changes, and explain the outcomes and their underlying reasons (Fu et al., 2022).

#### **G. Course Module: Mobile Internet Systems**

This module teaches students how to utilize the jQuery Mobile JavaScript library, which is built on top of the jQuery JavaScript library. This library offers an intuitive and efficient approach to creating web pages that are optimized for mobile device constraints. It has been implemented in the junior-level COMP322 Internet Systems course.

The learning objective of this module is as follows: Upon completing this module, students will be able to use the jQuery Mobile library to create web pages that are tailored to the constraints of mobile devices.

The course materials include lecture slides on jQuery Mobile and hands-on assignments. The focus is on using HTML5 custom data attributes to embed information within HTML elements, defining roles for these elements, and introducing the theming system in jQuery Mobile. In addition to the presentation, the module also covers custom events provided by jQuery Mobile and server communication. While jQuery Mobile typically uses Ajax for server interaction, the course covers non-Ajax communication methods to simplify the discussion (Joshi & Joshi, 2019). Hands-on assignments offer students the opportunity to practice all the topics presented in the lecture slides.

#### **H. Course Module: Android Cryptography**

This course module focuses on teaching students how to develop secure Android applications by properly utilizing Android's cryptography APIs. It specifically targets two areas prone to common programming errors: password-based encryption and SSL certificate validation. This module is designed for a senior-level COMP420 Applied Network Security course.

The learning objectives of this course module are as follows: Upon completing the module, students will be able to: 1) Utilize the Android cryptography SDK to implement password-based encryption correctly. 2) Properly validate digital certificates and establish secure communication between a mobile app and a web service using SSL. 3) Identify vulnerabilities in programs that use Android cryptography APIs. 4) Apply cryptographic knowledge to solve real-world problems (Masoodi et al., 2020).

The course materials include presentation slides and a hands-on learning assignment. The slides highlight common errors developers make when using Android cryptography APIs and SSL, and provide best practices for secure implementation.

In the hands-on assignment, students secure an existing Android app by applying cryptographic APIs. The app, an online contact list application, allows users to access their contacts from any Android device. Contacts are retrieved and stored on a web server using an XML-based web

service API. Both the web server and the source code of the insecure app are provided to the students for the assignment.

### 3. RESULTS AND DISCUSSION

The modules were showcased during a two-day instructor workshop aimed at evaluating their current and anticipated value. On the first day, participants shared brief summaries of their institutional goals and strategic directions. This was followed by interactive, hands-on learning sessions focused on the modules. Participant feedback was gathered through two methods: an opinion survey completed by all attendees and optional reflective narratives submitted by six participants several weeks later, allowing time for thoughtful evaluation.

#### A. Opinion Survey of Workshop Participants

A survey was administered to participants at the conclusion of the workshop to assess its effectiveness and gather their feedback. The overall satisfaction rating averaged 3.93 out of 5, with 5 representing the highest level of satisfaction. Table 1 provides the average ratings for various aspects of the workshop, including the effectiveness of presentations and lab sessions, as well as the relevance of the information to the participants' teaching and research. These ratings were also measured on a 5-point scale, where 5 indicates maximum effectiveness and usefulness.

Table 1. WORKSHOP SURVEY RESULTS

Presentation and Lab Session	Average Rating of Effectiveness	Average Rating of Usefulness
Introduction of Mobile Programming Presentation	4	3.81
Introduction of Mobile Programming Hands-on Activities	3.89	3.81
Mobile Program Development Presentation	3.94	3.62
Mobile Program Development Hands-on Activities	3.94	3.62
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	3.31
Mobile Malware Presentation	3.88	3.56
Mobile Malware Hands-on Activities	4.06	3.56
Mobile Policy Presentation	3.76	3.56
Mobile Operating System Presentation	4.38	3.63
Mobile Operating System Hands-on Activity	4.18	3.63
Hand-held Internet Systems Presentation	3.31	3.75

The average ratings for module effectiveness and usefulness, generally ranging from 3 to 4, suggest that the modules were moderately successful. Based on feedback from participants, improvements could be made by providing clearer instructions for some of the lab documents. Additionally, the workshop could benefit from clarifying the goals and objectives at the start of each session, as well as allowing more discussion after each exercise. Participants noted that the workshop was helpful for implementing the course modules in their classrooms and provided valuable networking, conversations, and resource-sharing opportunities. The workshop featured current information and well-structured hands-on projects.

#### B. Reflection from Workshop Participants

After the workshop, we reached out to participants for feedback on how they plan to incorporate mobile computing into their teaching, the perceived and actual usefulness of the course modules, which modules they believe would be especially beneficial for integration, and their thoughts on the future of mobile computing and mobile security education and research. Participation was voluntary but not anonymous. Six participants from various universities and schools provided reflective narratives. The insights from these narratives are summarized below.

Several workshop participants shared that their universities already offer one or two courses in mobile application development. They suggested incorporating the hands-on lab activities from the modules "Introduction to Mobile Programming" and "Mobile Application Development" into their courses' homework and projects. Some felt that these modules could serve as a preparatory foundation for mobile application development courses.

The "Cryptography on Android" module focuses on important programming skills such as password-based encryption and SSL certificate validation, essential for advanced developers handling

sensitive materials. This module could be taught in a single class session or extended with lab work and assignments across multiple sessions. If time is limited, a subset of the material, such as passwords, could be covered. Security-related issues could be evaluated through homework or a course project. This module could be integrated into mobile application development, cryptography, or cybersecurity courses, particularly those covering ciphers, public key systems, key management, certificates, etc.

One participant plans to incorporate the "Emerging Security Issues in Mobile Computing" module into the "Introduction to Information Assurance" course at their university, as well as the "Security Policy in Mobile Computing" module into the "Cyber Security Planning and Management" course.

Another participant intends to use the "Mobile Malware" module in the "Information Assurance and Digital Forensics" course, where students could design and implant custom malware on their mobile devices and control them remotely. Several participants also indicated their intention to integrate the "Mobile Operating Systems" module into their Operating Systems courses.

Workshop participants proposed ideas to extend the modules presented. One suggestion was to develop lab modules focused on intrusion detection, either through network traffic monitoring or host intrusion detection systems (HIDS) on students' devices. With additional time, students could evaluate the overheads and power consumption of exploits and HIDS. Tasks related to mobile-device forensics were also recommended, with the goal that students would learn to design and implement exploits that compromise mobile devices and evaluate countermeasures, employing secure forensic processes to collect and preserve evidence.

One participant from a 2-year community college plans to adapt the hands-on labs from "Introduction to Mobile Programming," "Mobile Application Development," "Mobile Operating Systems," and "Cryptography on Android" for their other course topics, such as iOS development, Windows Phone development, and cross-platform development. They also plan to adapt the mobile security policy content to focus on a software developer's perspective.

It was also suggested that the "Mobile Malware" module could be integrated into a cybersecurity course. To build the field of cybersecurity in the future, fostering interest at a younger age was emphasized. Potential future research could explore integrating cybersecurity curricula into 9-12 grade classrooms.

#### **4. CONCLUSION**

This paper presents a set of eight pre-designed modules on mobile computing and mobile security. These modules were featured in a two-day workshop attended by 20 participants. Despite the wide variety of program types, there was a general consensus that the repository provided value, as reflected in six reflective narratives submitted by attendees. A survey of all workshop participants indicated that the course modules were moderately successful. The reflective narratives highlighted that these modules could be incorporated into various courses within an undergraduate computer science curriculum at different institutions. The workshop covered a wide range of mobile topics that could inspire future educational research endeavors. Many of the institutions represented are developing courses, degrees, minors, and certifications that focus on mobile devices, mobile security, and related concepts such as mobile interfaces and cloud computing. A dedicated course module on Mobile Cloud Computing, where students could explore various cloud-based resources by studying Mobile Cloud Computing architecture, security, and privacy, could prove beneficial. This module could be offered as a standalone course or integrated into existing computer science or cybersecurity courses. Additional course modules on intrusion detection, mobile device forensics, and secure mobile development would also be valuable. Future work might also explore the integration of cybersecurity education into 9-12 grade classrooms.

## REFERENCES

- Bryson, J. R., & Andres, L. (2020). Covid-19 and rapid adoption and improvisation of online teaching: curating resources for extensive versus intensive online learning experiences. *Journal of Geography in Higher Education*, 44(4), 608–623.
- Damaraju, A. (2021). Mobile Cybersecurity Threats and Countermeasures: A Modern Approach. *International Journal of Advanced Engineering Technologies and Innovations*, 1(3), 17–34.
- Dejene, W. (2019). The practice of modularized curriculum in higher education institution: Active learning and continuous assessment in focus. *Cogent Education*, 6(1), Research-Article.
- Education, I. (2021). *Susan H. Rodger Professor of the Practice*.
- Fu, J., Wang, Y., Zhou, Y., & Wang, X. (2022). How resource utilization influences UI responsiveness of Android software. *Information and Software Technology*, 141, 106728.
- Hajare, R., Hodage, R., Wangwad, O., Mali, Y., & Bagwan, F. (2021). Data security in cloud. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, 8(3), 240–245.
- Joshi, B., & Joshi, B. (2019). jQuery. *Beginning Database Programming Using ASP. NET Core 3: With MVC, Razor Pages, Web API, JQuery, Angular, SQL Server, and NoSQL*, 227–278.
- Lalande, J.-F., Viet Triem Tong, V., Graux, P., Hiet, G., Mazurczyk, W., Chaoui, H., & Berthomé, P. (2019). Teaching android mobile security. *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 232–238.
- Masoodi, M., Moonsamy, V., & van den Broek, F. (2020). *Cryptographic (in) security in android apps*.
- Oh, S. W., Kim, K.-K., Kim, S. S., Park, S. K., & Park, S. (2022). Effect of an integrative mobile health intervention in patients with hypertension and diabetes: crossover study. *JMIR MHealth and UHealth*, 10(1), e27192.
- Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, 102580.
- Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, 31(3), 253–273.
- Reddy, J. K., & Singaravelu, G. (2021). Augmented reality (AR) in education-A New Prospect. *The Strad*, 8(6).
- Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, 76(12), 9493–9532.
- Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., & Kim, K.-I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. *Electronics*, 10(15), 1811.
- Thomas, C. G., & Devi, J. (2021). A study and overview of the mobile app development industry. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 5(1), 115–130.
- Xu, Y., Zhou, M., Gao, Q., Zhang, S., & Wu, Z. (2024). SWAT4J: Generating System Call Allowlist for Java Container Attack Surface Reduction. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 929–939.
- Yasin, H. N. S. (2021). *Graphical User Interface Test Case Generation for Android Apps Using Q-Learning*. University of Malaya (Malaysia).