*Journal of Learning and Teaching in Digital Age, 2019, **4**(2), 1-9*
ISSN: 2458-8350 (online)
Research Paper

Increasing Students Awareness of Mobile Privacy and Security Using Modules

Lila Ghemri
(ORCID ID:0000-0002-7471-1214)
Texas Southern University, USA
lila.ghemri@tsu.edu

Shengli Yuan
(ORCID ID: 000-0002-4850-9848)
University of Houston-Downtown, USA
YuanS@uhd.edu

Received 02 August 2018, Revised 19 December 2018, Accepted 19 December 2018

ABSTRACT

Mobile devices are fast becoming the dominant computing platform for an increasing number of people. Indeed millions of people are using their mobile phones as the main way to access the internet and social and entertainment media. This surge in mobile devices usage has been accompanied by an increase in malware specifically designed to infect mobile devices. From an educational standpoint, it is then becoming imperative to inform students about the risks and threats of mobile devices, not only as users but also as developers of mobile software. However, the Computer Science and other IT related disciplines are suffering from an overcrowding of their respective curricula with an ever increasing number of topics and courses that need to be covered within a limited amount of time. A possible solution to this issue is the use of teaching modules. Modular teaching provides a framework in which new skills can be introduced with little time commitment on the part of the student and the instructor alike. It is also ideal for introducing subjects that are important to know and could fit within different subjects. This paper presents an experience in modular teaching of mobile security and privacy. Two modules have been designed and presented to two cohorts of students (n=14, n=10) and learning assessed through tests and surveys. Results show that the modular approach is indeed beneficial in filling students' knowledge gaps in mobile security and that interleaving hands-on activities with instructional material can yield better retention and understanding of the topic.

Keywords: *Computing Education, Mobile Devices, Mobile and Wireless Security, Web Applications Security, Privacy*

INTRODUCTION

Mobile devices have seen a surge in both interest and availability in the last few years. Indeed, the number of users of mobile devices has increased by 41% from 2010 to 2015 and reached 5.2 billion people. Additionally, for the first time, design and use of mobile media have surpassed design of desktop applications with almost 300 million apps downloaded in 2015. In the mobile environment, Google Android and Apple iOS have the lion's share of the market with a little more than 94% of mobile phones running one of these mobile operating systems (Leswing, 2015). Mobile applications (apps) usage also increased by 76% in 2014 (Perez, 2015), and recent reports have shown that people are using mobile apps for activities that involve financial transactions, such as shopping, checking bank or credit card accounts, paying mortgages (Smith, 2015). Indeed, numbers show that iOS sessions using shopping applications have increased by 174% in 2014, while on Android; the same sessions were up by 220% (Perez, 2015). As the use of mobile devices is spiraling up, this situation has also drawn the attention of hackers and mal intentioned programmers who are now devoting their efforts to designing malware for mobile devices. Between 2013 and 2014, there has been a notable 136% growth in mobile adware to 410,000 apps. Additionally, cyber-attacks are also becoming more sophisticated and dangerous, such as phishing attacks that give access to personal information stored in the device (Zorabedian, 2014), or ransomware attacks, that lock the mobile device and request a ransom for it to be released to its owner (Chickowski, 2016). Investment in technology to prevent security risks on mobile devices has not been accompanied with a similar growth in skilled labor within the field, so much so that 30% of organizations complain of lack of experts in the topics of security analytics and mobile security (Solis, 2015). The purpose of this paper is to present teaching modules that aim at alleviating this problem by introducing material related to mobile security and privacy. The material is organized as independent modules that can be used by an instructor to introduce each topic to his/her students. The modules have been designed so that they can be used off-the-shelf, without requiring much customization on the part of the instructor. We

***Correspondence to*:** *Lila Ghemri, Professor, Department of Computer Science, Texas Southern University, Email: lila.ghemri@tsu.edu*

believe that the modular approach will encourage an easy adoption by instructors and will offer students the opportunity to learn about this important topic in an easy and concise way. The rest of this paper is organized as follows; in the next section, we will discuss the characteristics of modular teaching and how suited it is to our work. The following sections will introduce in details the modules in terms of coverage and topics. We will next present an evaluation of the modules by two cohorts of students, discuss the results and then conclude.

MODULAR TEACHING

In computing related curricula, such as computer science (CS), management of information systems (MIS) and software engineering (SE), there is an increasing competition over topics to be included in the undergraduate curriculum. Indeed, with the advent of the Internet and its attending subjects such as web programming, wireless networking, mobile applications programming etc., there is a need to offer students courses in these topics so as to prepare them for a competitive job market and afford them better employment opportunities once they graduate. On the other hand, many such programs aim at reducing the number of required credit hours so as to attract a maximum number of students into their program and lure them with fewer credit hours to graduation. Consequently, it is becoming apparent that students will have limited exposure, both in time and depth, to a number of subjects. This is not necessarily detrimental to the student, if one subscribes to the idea that some exposure is better than none, and moreover this could help students acquire a lifelong, independent learning mindset if they are to be successful in a career, in which practitioners have to re-invent themselves every few years to keep up with the advances in the field. In our approach, we believe that modular teaching can present a viable solution to this situation. Modular teaching provides a framework in which new skills can be introduced with little time commitment on the part of the student and the instructor alike. Modular teaching allows teachers, whose expertise is in a topic and wish to experience a different but related area, to get enough exposure to a new topic to be functional. The approach is also ideal for introducing subjects that are important to know but do not require a whole quarter or semester of instruction, or for introducing a piece of knowledge that could fit into many subjects (Sejpal, 2013). Instructional modules provide flexibility in planning teaching schedules, in that instructors can elect to pick one or more modules depending on their need and time availability. Iqbal (Iqbal, 1993) stipulates that to be successful, a teaching module should have the following features:

- Clearly stated objectives
- Well defined scope
- Self-contained and complete
- Instructional material related to the objectives
- Learning activities ranging from easy short answers questions to open ended more challenging questions.
- Periodic assessment based on evaluation from students and instructors.

Modular teaching has been used in various disciplines, such as medical training (Karthikeyan & Kumar, 2014), chemistry (Stewart & Wilkinson, 1999), and engineering (Sonek, 2006). The most appealing aspect of the modular approach is that it incorporates various teaching modalities, which stimulate active participation from students and promotes learning. However, adopting a module based curriculum requires an overhaul of the entire instructional mindset for both the instructor, whose role becomes that of a facilitator, and the student, whose responsibility toward achieving their own learning becomes paramount. Additionally, modular teaching, when implemented in full, is very labor intensive for faculty and needs extensive time management and coordination. In this work, our goals are more modest, in that we hope that modules can be used to complement instruction within a traditional setting. Indeed, instructors can provide the students with the ready-made material to study at their own pace and assign activities to strengthen and reinforce students' knowledge.

MOBILE PRIVACY AND SECURITY

The "Enriching Security Curricula and Enhancing Awareness of Security" project is a collaboration of three Houston based universities: University of Houston, Texas Southern University and the University of Houston-Downtown. The project consists of several security related topics, which have been divided and designed as a set of teaching modules. Each module consists of relevant teaching material accompanied by exercises and open-ended questions. Each module can be offered individually or as part of a theme. The project includes three general themes: Security Analytics, Security and Privacy in Distributed Networks and Security beyond Computer Science. Modules range in difficulty from basic, with material accessible to non-CS students, intermediate, with material accessible to students whose discipline is in a CS related field, and advanced, with material appropriate for CS advanced or graduate students. In this work, we focus on the Mobile Privacy and Security topic that is part of the Security and Privacy in Distributed Networks theme. This topic is in turn divided into three modules a) Mobile Infrastructure Security, b) Mobile Devices Security and c) Mobile Applications Privacy and Security. These 3 modules provide, in our opinion, a comprehensive coverage of the mobile environment and afford the student a suitable working knowledge in the topic. The focus of this paper is on the two last units, namely Mobile Devices Security and Mobile Applications Privacy and Security as the first one was extensively discussed and presented in (Ghemri & Yuan, 2016).

Mobile Devices Security

Mobile devices usage has grown exponentially since the advent of mobile phones in the nineties of last century. In 2014, the number of mobile devices had surpassed the number of people inhabiting planet Earth (Boren, 2014), Furthermore, a recent Pew report, about smart phones usage, showed that smartphones and other mobile devices are being used for much more than calling, texting or basic internet browsing. Indeed, 57% of people interviewed stated that they have used their mobile device for online banking, 62% have used them to look up a health condition and 19% have limited means to access the internet besides their mobile device (Smith, 2015). This unfettered use of mobile devices brings about many security issues related to their physical mobility and to the data they store; it is then appropriate that students acquire principles of how to securitize mobile devices. The module on Mobile Devices Security aims at informing students about the security and privacy problems related to mobile devices use and how to mitigate them. Table 1 shows the scope, objectives and prerequisites for this module.

Topics Covered in Mobile Devices Security Module

-Introduction to Mobile Devices: This section introduces mobile devices and their characteristics, such as display screens, operating systems, Wi-Fi and GPS, etc. It presents features of smart versus non smart versus fake smart phones. It also discusses the physical security of mobile devices and mitigation approaches (Ruggiero & Foote, 2011); (Yu, 2012).

-Secure Local Data Storage: This section introduces the most common authentication methods used on mobile devices. It also presents types of sensitive data that mobile devices store and issues that prevent the adoption of strong authentication policies for mobile devices (Isaca, 2010).

-Safe Browsing Environments: The mobile computing environment with its limited display space presents various security challenges. This section presents these challenges and how they can be addressed (Siddharth & Doshi, 2010).

-Mobile Spyware, Malware and Phishing: There has been a surge in mobile malware (Trojans, ransomware) that spread through SMS –text messaging- or through downloading compromised apps or accessing fake links. This section presents most the common mobile malware by platforms and the way mobile operating systems handle device and software security (Felt, Finifter, Chin, Hanna & Wagner, 2011); (Suarez-Tangil, Tapiador, Peris-Lopez & Ribagorda, 2014).

- Security Risks of Mobile devices to "traditional" IT Systems: Corporations and organizations are faced with two choices when trying to integrate mobile devices into their IT infrastructure. They can either provide their employees with an approved company device that they manage, or adopt a BYOD (bring your own device) policy. This section presents these two options and what each entails on the part of a company's IT department (Isaca, 2010); (Miller, Voas & Hurlburt, 2012).

Suggested Learning Activities

In order to provide the student with hands experience with the topic, several activities are suggested. Some of these exercises require students to use a smart phone and perform independent research to answer open ended questions:

-Activity 1: Backing up a mobile device.

-Activity 2: Privacy and security of geolocation, study the pros and cons of saving the user location data in a cloud database versus the device.

Activity 3: Define device rooting and study the pros and cons of jailbreaking a device.

Table 1. Objectives and Scope of Mobile Devices Security

Mobile Devices Security Module

Learning Objectives

The purpose of this module is to learn the security threats of mobile devices. The student will :

- Understand the security and privacy threats to mobile devices
- Understand the basic strategies and approaches to enhance mobile device security and privacy: device configuration, user authentication, apps certification, data encryption.
- Be knowledgeable of corporate strategies for managing mobile devices.

Prerequisites

Concepts	Modules/Courses
(1) Wireless Networking	Mobile Infrastructure Security
(2) Operating Systems	Operating Systems
(3) Encryption	Computer Security
(4) Programming	Intrusion Detection

Expected Outcomes

At the conclusion of this module, the student will be capable of recognizing various threats to mobile devices; the benefits and risks of jailbreaking a device.

Time Required

Two hours of lecture and four hours of independent hands-on activities.

Subsequent module

Mobile Applications Privacy and Security

Table 2. Objectives and Scope of Mobile Applications Privacy and Security

Mobile Applications Privacy and Security

Learning Objectives

The purpose of this unit is to teach security risks of mobile applications. The student will learn:

- Coding vulnerabilities and safe coding practices.
- Android/Java vulnerabilities
- Apple/iOS vulnerabilities
- Mobile HTML Security
- Privacy and security threats of geolocation

Prerequisites

Concepts	Modules/Courses
(1) Programming, SQL	Programming
(2) Security	Database Systems
(3) Mobile App programming	Computer Security

Expected Outcomes

At the conclusion of this unit, the student will be capable of recognizing the security risks of mobile applications. They will have knowledge of how to address some vulnerabilities by applying secure programming techniques, how to manage applications permissions and how to gather data judiciously.

Time Required

Three hours of lecture and two hours per hands on activity

Subsequent module

N/A

Mobile Applications Privacy and Security

Mobile applications programming has become a very popular and requested topic for many students, so much so that a majority of computer science programs have included such courses in their curricula. The privacy and security of mobile applications module aims at providing students who have a background in mobile programming, with necessary knowledge of the security risks that applications may present, and some design principles that developers can apply to design more secure applications (Dwivedi, Clark & Thiel, 2010). The module scope and objectives are presented in Table 2.

Topics Covered in Mobile Applications Privacy and Security:

-*Vulnerabilities:* This part introduces security terms such as vulnerability, exploits, zero-day attacks, etc. It also introduces types of malware and how each type operates.

-*Coding Vulnerabilities:* This part introduces the array of security issues that could inadvertently be introduced through bad programming techniques, such as the unnecessary use of global variables, non-initialized variables, buffer overflow and SQL injections. Methods for writing secure code are presented (Viega and McGraw, 2001).

-*Mobile JAVA Security:* This topic discusses mobile JAVA that is used by the Android platform. It discusses the security approaches that are practiced, such as, sandboxing, controlling access and permissions to resources, limiting communication and signing an app to verify integrity and provenance (Gibler, Crussell, Erickson, & Chen, 2012).

-*Mobile iOS Security:* This section introduces the Apple iOS security framework. Encryption methods in iOS as well as the types of protections that an app is required to have, such as mandatory code signing and security enclaves (Apple, 2015).

-*Mobile HTML Security:* Mobile websites are slimmed down versions of regular websites for mobile devices use. Mobile HTML sites are growing in popularity as more devices can access them. Security challenges are introduced, such as cross-site scripting (XSS), HTTP redirect and phishing (Wassermann, 2008).

-*Privacy of Geolocation:* This section introduces the methods used for geolocation and the accuracy and precision of each. It also discusses the ways in which geolocation is implemented by the three major mobile environment players: Android, iOS and Microsoft Mobile. Security and privacy threats are also discussed and best practices to put in place to prevent privacy violations (Doty and Wilde, 2010).

Suggested Learning Activities

In order to strengthen students' knowledge of the security risks in mobile applications as well as mitigation methods, we designed a set of activities as well as used off-the-shelf, public domain lab exercises. Such public domain repositories are the Android Security Labware developed by Li Yang at the Information Security (InfoSec) Center, the University of Tennessee in Chattanooga (Yang, 2014) and at the Information Assurance and Security Education on Portable Labs (Lo, 2015). Most of these activities require a closed environment in which students use malware and learn how to mitigate threats.

Activity 1: Securing Code
Activity 2: Managing mobile application permissions using the Manifest file.
Activity 3: Geolocation sensors use and permissions.
Activity 4: RSA Encryption Decryption in Android
Activity 5: Spreading a Trojan through SMS.
Activity 6: SQL injection malware through SMS.

RESEARCH QUESTIONS

After the module design phase, the specific research questions we are interested in investigating are whether, conceptually, modules can be effectively integrated within a traditional curriculum and improve student learning, and how to best design these modules. Specifically (1) Do students show any learning gain of the module material? (2) What are the module characteristics that students liked and which ones were most helpful? Investigating modular teaching effectiveness and likeability is important because it can help guide the design and content of modules and validate the approach as a viable method to address gaps in student learning. Research question was addressed through the use of a multiple choice questionnaire with ten questions, each having a single correct answer. The questionnaire was administrated before the module was presented, so as to establish a baseline for each student's performance.

To evaluate students' opinion on the module and answer question two, we examined students' answers to a survey form with seven questions that related to the adequacy of the material presented in terms of organization, coverage and usefulness.

METHOD

Participants

Students taking two different courses provided the data used for this work. All 24 students were majoring in computer science and were either juniors or seniors. 90% of the students were minority students (African Americans and Hispanics). There were 23 males and (sadly only) one female student.

Modules Presentation

The two courses with which these modules were integrated, were 400 level CS electives: Wireless and Mobile Networks and Wireless Programming. The Wireless and Mobile Networks course covers these two main topics, namely wireless networks and mobile networks and had an enrollment of 14 students. The Wireless Programming course covers mobile website design and mobile applications programming using the Android platform and had 10 students enrolled. Neither course has coverage of security included in the curriculum.

Each module presentation started with a short talk that sensitized the students to the importance of the topic. It was followed by a study of the instructional material with a question/answer period. Ideally, this portion of the module would be the student's responsibility and done at his/her own pace. However, in our case, this was not a viable option. A relevant question was presented to elicit a group discussion. For the Wireless and Mobile Networks course, the group discussion question was: "Many firms conduct periodic risk assessment to identify cybersecurity threats, assume you are put in charge of assessing the security of the company mobile assets. What will you do?"

For the Mobile Applications Privacy and Security course, the discussion question was "App cloning is becoming a real concern for app developers, not only because of loss of income, but also because the clones can hide malicious code. As an app developer how would you protect your work? As an app distributor, how would you protect your customers?"

Study Design

In order to assess students' learning of each module, multiple choice questions, related to the mobile devices security and mobile applications privacy and security, were designed by the modules' authors. These questions were representative of the topics covered and were multiple-choice in which only one response was correct. Students' performance calculations were based on the number of correct answers selected. Before presenting the instructional material, students were administrated the multiple choice questionnaire (Q1) as a pre-test. Their answers represent the baseline to assess any subsequent gain in learning. The instructional content was presented during two class sessions of 70 minutes each. After this presentation, the students got an opportunity to answer the same questions presented in a different order (Q2). Due to scheduling constraints, no hands-on activities were performed for Mobile Devices Security module. However, the students who took Mobile Applications Privacy and Security worked on the learning activity 3 that related to geolocation privacy and security during one class session. After this activity, the multiple-choice questionnaire was again administrated (Q3). Figure1. shows the sequencing of the study design.

RESULTS AND ANALYSIS

Student Performance

Regarding the Mobile Devices Security Module, the average grade for Q1 was 50, with 90 as the highest grade and 20 as the lowest one. The average on Q2 was 80 with 100 as the highest grade and 40 as the lowest. The average student gain in learning for this module was 64%, based on the formula (Q2-Q1)* 100 /Q1. This gain is statistically significant at ($p < 0.05$).

Figure 2 shows the performance of each student on the pre and post-test for the Mobile Devices Security module.

On the Mobile Applications Privacy and Security module, the average student grade on Q1 was 55, with 70 as the highest grade and 40 as the lowest. One week after the presentation of the module, Q2 was administrated to the students; the average was 67, with 100 as the highest grade and 40 as the lowest. The average student gain in learning was 22%; this result was not statistically significant.

Students were then asked to work on learning activity 3. After they completed the activity, the multiple-choice questionnaire (Q3) was administrated. Results showed that the average grade on Q3 was 85, 50 being the lowest and 100 the highest grade. The average learning gain was 54%. This result was statistically significant ($p < 0.02$) and confirmed by a t-test on the null hypothesis that the means of the pre-test and post activity are equal.

Figure 3 shows the performance of each student on the pre-test(Q1) , post-test (Q2) and post activity (Q3) for this module.

Discussion of Student Performance

Assessing the students' learning was performed using a 10 question multiple choice test. The questions, included in the multiple choices, were designed so as to assess two aspects of learning. These two aspects, as described by the Bloom's taxonomy of learning, are remembering (A) and understanding (B) (Bloom, 1956).

For the Mobile Devices Security, 4 out of the 10 multiple choice questions were about recall of facts (A).

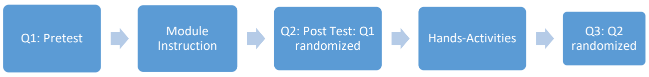

Figure 1. Quantitative Study Design

Results of the pre-test (Q1) showed that the correct answer was selected 2 times out of 4 for (A) and 3 times out of 6 for (B). The post-test results (Q2) indicated that students selected the correct answer 3 out 4 for (A) and 4 out of 6 times for (B).

Results for the Mobile Applications Privacy and Security were as follows: The multiple choice questions were divided into 5 questions from (A) and 5 from (B). The pre-test (Q1) results showed that students selected the correct answer 3.5 out of 5 for (A) and 3 out of 5 for (B). The post–test (Q2) results showed no difference in recall for (A), that is 3.5 out of 5 and a slight improvement to 3.5 correct answers out of 5 for (B). This modest improvement is in accordance with the slight increase in average grade between pre and post-tests. 6 questions were about identifying and recognizing concepts (B).

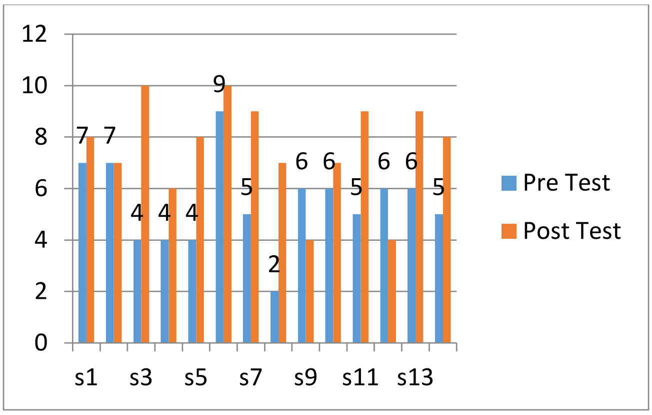

Figure 2. Student Performance on Mobile Devices Security

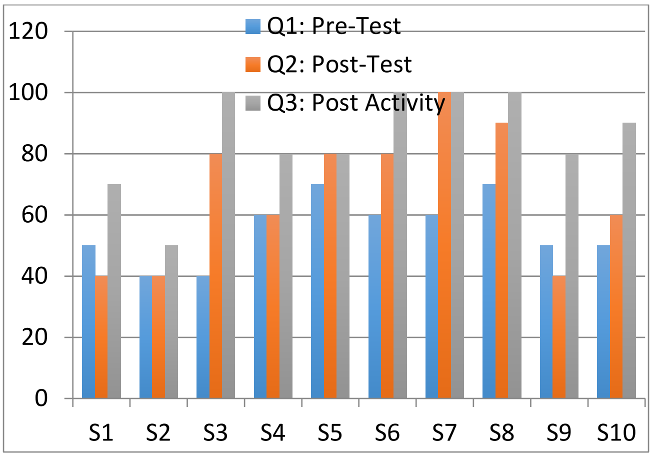

Figure 3. Student Performance on Mobile Applications Privacy and Security

The difference in results between the two modules results may be explained by the fact that the post-test was performed one week after the instructional material of the module which can be considered as a delayed response. The encouraging thing is that although the recall of information did not increase, it did not get worse and the students' understanding of concepts (B), actually slightly improved. Another explanation may be that the type (A) questions included in the test were of too general a nature and did not strongly relate to the material presented. This observation actually requires a careful review of the test questions.

After the learning activity was performed, the students' scores for post activity test (Q3) were as follows. For (A), students selected the correct answer 4 out of 5 times and 4.5 out of 5 for (B). These results indicate that the hands-on activity helped improve and advance students' knowledge of the topic.

Students Survey on Modules Quality

Each module content, presentation and suitability were assessed using a Likert scale survey containing seven questions in which answers ranged from 1 to 5, with 1 being the lowest rank and 5 being the highest rank. The survey results were analyzed and a scale of 5 or 4 was considered as "Good", a score of 3 was considered as "Average" and a score of 2 or 1 was taken as "Poor". Based on this, 96% of students found the modules content and presentation to be well organized and useful. Only about 61% of the students estimated that they had the necessary security background to understand the material presented in the two modules. This could indicate a gap in these students' background that would need to be addressed through additional learning experiences. 69% of students estimated that the supporting material was adequate, which may be because students did not have sufficient time to work on the activities related to each topic. Table 3 presents the cumulative results of students' evaluations of both modules.

Table 3. Students' Evaluation of Module Content and Presentation

Questions	Good (5/4)	Average 3	Poor (2/1)
How cohesive was the presentation of the material in the module?	96%	0.5%	3.5 %
How logical was the order of presentation of the materials in the module?	96%	3.5%	0.5%
How much background did you need outside of the module and beyond the prerequisites to understand the module?	61%	15%	23%
How is the coverage of module and security relevant topics in the module?	85%	7%	7%
How useful was the module?	92%	4%	4%
How adequate were the supporting materials provided by the module?	69%	24%	7%
How was the quality of the supporting materials provided by the module?	96%	4%	0

CONCLUSION

Mobile devices and applications present a new computing paradigm in which various security challenges need to be addressed. Two modules, with attending instructional material and learning activities, were presented that can help instructors in the task of informing their students about these topics. Results from testing these modules show that they hold promise in terms of complementing students' knowledge in the areas of interest and that they can advantageously be integrated into a traditional instructional setting. Results also indicate that hands-on activities improve and enhance learning.

Since modular teaching offers a comprehensive experience with practical learning activities, care has to be taken to make time for such activities. These modules are currently being tested for adoption and improvement at their home universities, as well as many other institutions.

The instructional material is freely available, with more security related modules, at http://capex.cs.uh.edu.

We hope that interested instructors will make use of this material and provide valuable feedback to the module developers.

ACKNOWLEDGMENTS

We are grateful to the students at our respective institutions for making this work possible. Special thanks Dr. Wenyaw Chan of the University of Texas Medical School and Dr. Rakesh Verma of the University of Houston for useful comments on earlier drafts of this paper.

REFERENCES

Apple, Inc. (2018). IOS Security iOS 11. Retrieved from http://www.apple.com/business/docs/iOS_Security_Guide.pdf

Bloom, B. S., Engelhard, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). Taxonomy of educational objectives; the classification of educational goals. *Cognitive Domain, Handbook 1,* Longman, New York.

Boren, Z.D. (2014). *There are officially more mobile devices than people in the world.* Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are- officially-more-mobile-devices-than-people-in-the-world- 9780518.html

Chickowski, E. (2015). *Ransomware Ranked Number One Mobile Malware Threat.* Retrieved from http://www.darkreading.com/endpoint/ransomware-ranked-number-one-mobile-malware-threat/d/d-id/1322886

Doty, N. & Wilde, E. (2010). Geolocation privacy and application platforms. *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (SPRINGL'10)*. ACM, New York, 65-69. DOI: http://dx.doi.org/10.1145/1868470. 1868485

Dwivedi, H., Clark, C., & Thiel. D. (2010). *Mobile Application Security.* McGraw-Hill Professional Publishing. New York, USA.

Ghemri, L. & Yuan, S. (2016). Teaching Mobile Security Using Modules. *Proceedings of the 12th International Conference on Frontiers in Education: Compute Science and Computer Engineering (FECS'16),* in conjunction with *2016 World Congress in Computer Science, Computer Engineering, & Applied Computing*. July 25-28, 2016, Las Vegas, USA.

Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012). Android Leaks: automatically detecting potential privacy leaks in android applications on a large scale. *Proceedings of the 5th International Conference on Trust and Trustworthy Computing (TRUST'2012).* Springer, Berlin

Heidelberg. 291-307.

Iqbal, J. M. (1993). *Modular Teaching*. Retrieved from http://cemca.org.in/ckfinder/userfiles/Javed_Iqbal_Muhammad0193.pdf

Isaca. (2010). *Securing Mobile Devices, White Paper Report.* Retrieved from http://www.isaca.org/KnowledgeCenter/Research/Documents/SecureMobileDevices_whp_Eng_0710.pdf?regnum=29401

Karthikeyan, K., Kumar, A. (2014). Integrated modular teaching in dermatology for undergraduate students: A novel approach. *Indian Dermatology Online Journal*, *5*(3), 266-270. DOI: 10.4103/2229-5178.137774

Leswing, K. (2015). *Android and iOS are nearly tied for U.S. Smartphone Market Share*. Retrieved from https://gigaom.com/2015/02/04/android-and-ios-are-nearly-tied-for-u-s- smartphone-market-share/

Lo, D. (2018). *Information Assurance and Security Education on Portable Labs.* Retrieved from https://sites.google.com/site/iasoncs/home

Miller, K. W., Voas, J., & Hurlburt G. F. (2012). BYOD: Security and privacy considerations. *IEEE IT Professional.* (September 2012), 53-55. DOI: http://doi.ieeecomputersociety.org/10.1109/MITP.2012.93

Perez, S. (2015). *App Usage Grew 76% in 2014, With Shopping Apps Leading the Way*. Retrieved from http://techcrunch.com/2015/01/06/app-usage-grew-76-in-2014-with-shopping-apps-leading-the-way/

Porter Felt, A., Finifter, M., Chin, E., Hanna, S. & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'11).* ACM New York, NY, 3-14. DOI: http://dx.doi.org/1145/2046614.2046618

Ruggiero, P., & Foote, J. (2011). Cyber Threats to Mobile Phones. Retrieved from http://www.uscert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

Sejpal K.K. (2013). Modular Method of Teaching. *International Journal for Research in Education, 2*(2), 169-171.

Siddharth, S., Doshi. P. (2010). *Five common Web applications vulnerabilities.* Retrieved from http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities

Smith, A. (2015). *U.S. Smartphone Use in 2015.* Pew Research Center. Retrieved from http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf

Solis, B. (2015). Disruptive Technology Trends 2015-2016. Retrieved from http://www.briansolis.com/2015/01/25-disruptive-technology-trends-2015-2016/

Sonek, G. J. (2006). A Modular Approach to Teaching the Engineering Challenges of Physiology. *Proceedings of the American Society for Engineering Education New England Section 2006 Annual Conference.* Retrieved from https://www.wpi.edu/News/Conf/ASEE/papers.htm

Stewart, J. L., & Wilkinson, V.L. (1999). *ChemConnections: A Guide to Teaching with Modules***.** Retrieved from chemlinks.beloit.edu/guide/superim.pdf

Suarez-Tangil, S., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, Detection and Analysis of Malware in Smart Devices. *IEEE Communications Surveys & Tutorials*, *16(*2), 961-987.

Viega, J., & McGraw, G. (2001). *Building Secure Software: how to avoid security problems the right way.* Addison-Wesley Professional Computing Series.

Wassermann, G., & Su, Z. (2008). Static detection of cross-site scripting vulnerabilities. *Proceedings of 30th ACM/IEEE Conference on Software Engineering (ICSE'08).* ACM New York, NY, 171-180.DOI: http://dl.acm.org/citation.cfm?doid=1368088.1368112

Yang, L. (2014). *Capacity Building through Curriculum and Faculty Development on Mobile Security.* Retrieved from http://www.utc.edu/faculty/liyang/mobilesecurity.php

Yu, R. (2012). *Lost cellphones added up fast in 2011*. Retrieved from http://usatoday30.usuatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1

Zorabedian, J. (2014). *What's causing the explosive growth in Android malware threats?* Retrieved from http://www.itbestofbreed.com/sponsors/sophos/best-tech/what%E2%80%99s-causing-explosive-growth-android-malware-threats