Mobile Security and Vulnerability Exploitation as a Flipped Classroom Security Curriculum

Richard P. Mislan, Ph.D. and Tae Oh, Ph.D., *Senior IEEE*

Abstract— **While mobile devices have become essential to the daily social fabric of our lives they have also become a popular platform to exploit. The security of mobile devices is a growing necessity, yet many in our population are woefully inexperienced in providing proper security measures. In an effort to address this need, this paper discusses the development of a unique classroom model based on the flipped classroom that provides a repository website of integrated course resources and virtualized laboratories for the education of "Mobile Device Security and Vulnerability Exploitation." Given the specific needs of this type of mobile security modeling, it is imperative that the students participate in a secured laboratory setting. To meet this necessity, the development of a website repository and the inclusion of video lectures, presentations, and virtualized laboratory exercises specific to the course is proposed.**

Index Terms— **Mobile Device, Exploitation, Security, Curriculum, and Flipped Model**

I. Introduction

As THE proliferation of mobile devices continues to rise in the personal and professional world, there is a growing need for better understanding and awareness of mobile device security and forensics. Currently in the United States, there are more wireless mobile devices connected than there are people (331.6M/311.5 at 106%) and the number of devices is projected to continue to rise [4]. As the ultimate human computer interface of the 21st century, the mobile device allows almost everyone to do almost everything, almost everywhere they go. Consolidating many bleeding edge technologies into a single unit, the mobile device allows us to transcend space and time through multiple communication, transaction and entertainment tools.

As mobile devices have become essential to the social fabric of our lives, the past year has seen a 2,180% increase in unique malware variant attacks [5]. With always-connected capabilities, mobile devices have become the ultimate access point to a person's most private and personal information. Once a device has been maliciously compromised, personal data is exposed, leaving the owner violated and picking up the pieces. Blurring the line between personal and professional is the critical issue of Bring Your Own Device (BYOD), which impacts all sectors.

As important as mobile communications tools have become, the security of mobile devices is still overlooked by our society. The authors, as members of a highly technical community and as users of such devices, feel a strong sense of urgency to resolve the issues related to mobile device vulnerabilities through increased awareness and mitigation [6], [7].

Therefore, the authors have decided to design a course to introduce the topics of mobile device vulnerability exploitation with the goal of understanding existing mobile exploits to build better defenses. The breadth of academic research in mobile device vulnerability exploitation has not yet matured, leaving this field a ripe opportunity for exploration and discovery.

This paper introduces the meaning and purpose of the flipped classroom model and discusses why this model is being selected as a development framework for this course. The paper then describes how the mobile device vulnerability exploitation course is designed, including class materials, lab exercises, an online repository, complementary courses and other materials. Finally, the paper concludes with expectations, future work, and other opportunities for discussion.

II. Flipped Classroom Model

While not a new teaching model, the flipped classroom is rapidly becoming a popular choice amongst innovative educators [1]. The flipped classroom model inverts traditional teaching methods by delivering instruction outside of the class using online resources, thus shifting traditional homework exercises into the classroom [9]. Before attending a class session, students are assigned online lectures to view at home or any other location they may be, and to communicate with fellow students and faculty via online discussions [3]. During the classroom session, student engagement occurs by working through small problem sets and exercises, assimilating previously learned information, and creating new ideas within the provided time with the guidance and/or assistance from the instructor.

This paragraph of the first footnote will contain the date on which you submitted your paper for review. It will also contain support information, including sponsor and financial support acknowledgment. For example, "This work was supported in part by the U.S. Department of Commerce under Grant BS123456".

The next few paragraphs should contain the authors' current affiliations, including current address and e-mail. For example, F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

The flipped classroom was created to address the lack of achieving learning outcomes, and to increase the limited concept engagement of the traditional classroom model [9]. In this case, the authors will be using the flipped classroom model for two reasons: 1) to provide students with an immediate immersion into the field through an online repository of readings, presentations, and videos related to mobile device security and vulnerability exploitation, and 2) to maximize the classroom time for supportive application of theories and practices of mobile device securitya nd vulnerability exploitation and various hands-on exercises.

As published in numerous articles and journals, the flipped classroom promotes a stronger student/teacher relationship and creates a collaborative learning environment in the classroom. By shifting the preparation of the student to an online component, the in-class laboratory exercises will be much more meaningful and provide time for collaboration and curiosity.

III. Course Objectives

To increase student knowledge of mobile device security and vulnerability exploitation, the following objectives are defined:

Objective 1: Development of lectures

In developing the lectures specific to the subject area, videos will be 5-7 minutes in length. Major topics will be broken into much smaller "digestible" topics. These will be built for preparing the student for the laboratory exercises to be conducted during class.

Objective 2: Development of an online repository of integrated course resources

To support the development of the flipped classroom, an online repository of integrated course resources and virtualized laboratories will be built. This website will categorize the information related to each weekly topic. Each week will have resources categorized as: "Laboratories," "Presentations," "Research," "Videos," and "Assessments." These will be used both in class and out of class.

Objective 3: Development of virtualized laboratories

The unique situation of mobile exploitation is that most laboratory exercises must be performed off of the mobile carrier network. To that end, the laboratory exercises must either be virtualized in an online simulation or carried out through a privately established low-power network. The former option is much less expensive and much more controllable. For that reason alone, it is necessary to establish virtualized laboratory exercises.

Objective 4: Development of assessment tools

In an effort to continually improve the process of flipped classroom learning, students will be assessed through a variety of pre- and post- type of assessments. Online resources will survey students' knowledge before viewing video lectures or presentations. These same online resources will survey students' gained knowledge after viewing the presentation. Short answer questions related to the content as well as multiple choice and true-false type assessment tools will be employed to validate strengths and weaknesses of the provided lectures and/or presentations.

To finalize the project, all curricula, lab information, key findings, and pilot results will be transparently shared through presentation, reports, and the specific curriculum website. Through the deployment of this project, students will obtain critical skills and knowledge directly related to security and vulnerability exploitation in a mobile environment. In the most basic terms, through its curriculum, academic sharing of materials, and collaborative research opportunities, this project will increase the number of students capable and qualified to teach others about mobile device security and vulnerability exploitation. By extension, this will also increase student learning in this critical area, increasing the workforce pipeline of qualified graduates to support and secure our mobile cyber infrastructure.

IV. Methodology

To create a standard expectation for the course curriculum, the objectives for each course will be aligned to the stated outcomes used for accreditation by ABET/Middle States. Once these objectives are defined, weekly course materials for mobile device vulnerability exploitation topics will be built. Through this course, students will learn about a) mobile communications technologies, b) mobile operating systems, c) current threats, d) mobile malware, vulnerabilities, and exploits, and e) code and application analysis tools and techniques. For many of these topics, the flipped classroom model and hands-on lab exercises will reinforce the students' learning.

Through the use of a flipped classroom curriculum and various collaboration opportunities, this effort will enhance and strengthen the capabilities of RIT students and faculty. Ongoing research and development exercises of mobile device vulnerability exploitation will be created and developed to encourage participation of other faculty and students as well as other Universities [11].

V. Course Topics and Materials

For the 15 week semester, there will be 15 topics covered (See Table I). The first week will be an introduction to the topic of mobile device vulnerability exploitation. This will be followed by a two weeks of the technical and social topics of mobile devices. The next two topics will cover the data storage methodologies of application data. After that, the students will be introduced to current mobile exploits, and then will explore the popular smartphone operating systems and the specific exploit that exists for each. The course will end with a short introduction to advanced mobile device security and exploitation techniques, somewhat preparing them for their next class.

TABLE I
COURSE OUTLINE FOR MOBILE SECURITY AND VULNERABILITY EXPLOITATION

(i)	Topics
1	Introduction to Mobile Devices, History/Appreciation
2	Network Stacks and Mobile Firmware
3	OS's: Android, Apple, Blackberry, Windows
4	Forensics: Procedures/Principles, Tools, Techniques
5	Forensics: Basic Phone

6	Forensics: Smartphones
7	Malware: Introduction/History/Appreciation
8	Mods: Jailbreak, Root, Unlock
9	Apps: Security and Vulnerabilities
10	Attacks: Hardware and Device
11	Attacks: Software
12	Attacks: User Layer
13	Strategy: Threat Preparedness and Mitigation
14	Strategy: Threat Response and Recovery
15	Legal/Ethical/Moral Issues

VI. Labs

During the semester, the students will use hands-on exercises that will allow them to explore the intricacies of the mobile application environment as shown in Table II. Each lab activity will include previously imaged, specific operating system mobile devices for student exploration and examination. Lab exercises will provide foundational focus on:

- The identification of operating system specific user data storage locations.
- The identification of operating system specific user data storage methodologies.
- The identification of common application data storage methodologies.
- The usage of common mobile exploits for specific operating systems.
- The effects of common mobile exploits on specific operating systems.

The labs will be spread throughout the semester and will be offered after the topic has already been presented and discussed online. These exercises will be designed to promote various ways to effectively increase knowledge and comprehension of the concepts, especially to those students who are kinesthetic learners.

TABLE II
Course Lab for Mobile Security and Vulnerability Exploitation

Topics
Introduction to Mobile Devices
Mobile Device Forensics
Mobile Device Security
Mobile Attacks Vectors Classes and Attack Models
Mobile Strategy, Policy and Risk Management
Legal/Ethical/Moral issues

VII. Digital Smartphone Corpus

As noted by other security and forensics researchers, "real data is often unsuitable for education purposes" in large part because of confidential information found in digital devices [2]. Most attempts at this often end up as insufficiently realistic. Usually, in these attempts to mimic real-world devices, the data sets become more complex than is necessary. Given those challenges, there is still a need for the development of a corpus of smartphone device images for these courses. To that end, a corpus of operating system specific devices will be created to demonstrate and highlight:

- data storage locations
- data storage methodologies
- attack vectors for exploiting
- the effects of exploits

The idea for a corpus of digital data is not new. Currently, there are two small public corpora of non-smartphone mobile devices. Created by Simson Garfinkel and supported in part by NSF Grant DUE-0919593, the Real Data Corpus (RDC) is a collection of raw data extracted from data-carrying devices that were purchased on the secondary market around the world [2], [13]. The other corpus is the Computer Forensic Reference Data Sets (CFReDS) for digital evidence provided by the National Institute for Standards and Technology [8]. Both of these reference data sets provide documented sets of data from hard drives, cell phones, USB memory sticks, and other data-carrying devices. Neither of them currently house any smartphone images.

VIII. Online Repository

We are building an online repository of information for students to immerse themselves into this burgeoning field of study. This repository will include curriculum, a virtual lab, an assessment system, and a faculty/student outreach vehicle for dissemination and collaboration. Borrowing from the previous successful efforts of other network security educational projects such as the NSF funded SEED program from Syracuse University[1] and the related SWEET program from Pace University[2], and the Security Injection program from Towson University[3], this tool will be used to share curriculum ideas, the corpora of smartphone images, and online resources for other educational opportunities [12]. It will also provide support for existing, ongoing, and future mobile exploitation research, collaboration, and dissemination. Ideally, access to these materials will directly benefit the educational community in mobile security and vulnerability exploitation, as well as the general population as it pertains to securing our world of mobile devices.

IX. Course Evaluation

The evaluation of this project will be conducted through a variety of formative and summative tools. The process evaluation tools that will be used to determine the effectiveness of the flipped classroom model and its correlated laboratory exercises include following measurement techniques.

A. Quizzes-Measure Understanding of Classroom Materials

Before class starts, each student will take short quizzes from the previous-to-classroom viewed materials. The results of the quiz will indicate the comprehension level of the students. If the score is low, the instructor will determine reasons for the low grade and update the course materials to adjust the course

[1] http://www.cis.syr.edu/~wedu/seed/
[2] http://csis.pace.edu/~lchen/sweet/
[3] http://triton.towson.edu/~cssecinj/secinj/

delivery methods.

B. Surveys - Measure Video Lecture Effectiveness

Before and after each instructor prepared video lecture related to course concepts, each student will take a short online survey to assess pre- and post- knowledge and comprehension. Short answer questions related to the content as well as multiple choice and true-false type assessment tools will be employed to validate strengths and weaknesses of the provided lectures and/or presentations. If the average scores are too low or too high, the instructor will determine reasons for the low or high scores and update the course materials to improve the course delivery methods.

C. Laboratory Exercises - Measure Hands-on Learning Effectiveness

The laboratory exercises will apply the concepts from lectures and video demonstrations and the grade from laboratory report will indicate the students' comprehension, understanding and learning level.

D. Course Evaluation - Measure Effectiveness of this Course

The third measure will from the student feedback about this course. The instructor will be very interested in their interest level and learning effect. Collecting student's ideas and suggestions will improve the course. The progress will be closely monitored through classroom discussion as well as online discussion boards from the course website.

At the end of the semester, the course will be evaluated and restructured as necessary. Not all measurements are required to be implemented in the course and it's up to the instructor to select what measurements to be used and how often they are needed to meet the goals and purpose of the course.

X. Complementary Courses

The authors are also developing complementary classes in mobile device security and vulnerability exploitation for advanced studies and a capstone class for the advanced learner to test their abilities in exploiting and securing this trend in mobile devices. Brief description of those courses is described below.

A. Mobile Device Security

This course will introduce students to the various technologies employed in mobile device security. Emphasis will be placed on evaluating different types of mobile device malware and applications to determine the type of access and information disclosure threats that they represent [9]. Different types of malware detection solutions will also be identified and reviewed.

B. Mobile Device Vulnerability Exploitation

This course will introduce students to the various types of exploits available to attack mobile devices. Emphasis will be placed on evaluating different types of mobile device exploits and tools to determine the types of access and information available through each type of attack.

C. Capstone: Mobile Device Security and Vulnerability Exploitation

This course will further explore the various systems and technologies employed by mobile devices. Emphasis will be placed on the forensic identification of threats and vulnerabilities of specific mobile device operating systems and technologies and the application of and techniques for mobile device hardening.

XI. Current Status

As part of the curriculum development, funding was sought out through the Rochester Institute of Technology and was awarded through the Provost's office. Funds will go to towards the development of the course website and repository as well as to current mobile devices for lab work. To date, the website, curriculum, and repository is being built and hosted at MobiSploit.com. All information regarding development and progress on the curriculum can be viewed at the website.

Interactive labs for mobile device security are being created to instruct students how to evaluate and examine the behavior of the malware. The labs also teach students how to perform dynamic malware analysis and teach different analysis techniques in the malware analysis methods. Several tools will be introduced for the labs as well. Currently, there are four different labs are developed. The first lab is a brief introduction of Android emulator and introduces steps for setting up the testing environment. The second lab introduces SMS malware and the students can evaluate the behavior of the malware using different evaluation tools. The third and fourth labs introduce more sophisticated malware such as Trojan and botnets. Additional lab materials are needed and will be developed to support the understanding of mobile malware and Android architecture.

XII. Conclusion

Almost every student has a mobile phone; however, many of these students have no foundational understanding of mobile security and the weaknesses that lie within these devices. To that end, it is the authors' intent to develop a new course curriculum using the flipped classroom in mobile device vulnerability exploitation. This curriculum model will emphasize a hands-on approach by providing virtualized laboratory exercises using mobile device images and related mobile device emulator tools.

The core philosophy of the flipped classroom is that the authors encourage students to find and seek information and answers, thus promoting out of box thinking. The greatest benefit of this model is that students will learn from their investigative research and from each other through online presentations, discussions, and lab exercises. By implementing the flipped classroom model with virtual lab exercises, students will gain a practical level of knowledge about mobile device vulnerability exploitation, while the hands-on experiences will promote curiosity while producing better prepared, security minded students.

Sun Tzu, the ancient Chinese warrior taught his men to "know your enemy" before going into battle. His wisdom suggested that if "you know your enemy and know yourself, you need not fear the result of a hundred battles." But he also warned, "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat." The authors are taking this wisdom to heart as we develop this new curriculum. Not only are we studying, teaching, and researching the arts and methodologies of security, but we are also studying, teaching, and researching the vulnerabilities and exploitations of these mobile devices. As we prepare our students for their eventual future, it is critical that they know the vulnerabilities and exploits of the mobile devices as well as they know the methods of security.

As the authors continue to develop these courses, other more specific papers will be submitted in the future regarding the results of the flipped classroom, the usage of the online repository, and the development of the other complementary courses.

References

[1] M. Becher, F.C. Freiling, J. Hoffmann, T.Holz, S. Uellenbeck, C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," 2011 IEEE Symposium on Security and Privacy. M. DeFour, "New 'flipped classroom' learning model catching on in Wisconsin schools," McClatchy - Tribune Business News, Feb. 2013.

[2] S. Garfinkel, (n.d.). Real data corpus. [Online]. Available: http://digitalcorpora.org/corpora/disk-images/rdc-faq

[3] K. Janz, K. Graetz, and C. Kjorlien, "Building collaborative technology learning environments," in Proceedings of the ACM SIGUCCS 40th annual conference on Special interest group on university and college computing services, New York, NY, USA, 2012, pp. 121–126.

[4] L. Liu, X. Zhang, G. Yan, and S. Chen, "Exploitation and threat analysis of open mobile devices," in Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, New York, NY, USA, 2009, pp. 20–29.

[5] Y. Lv, D. Lymberopoulos, and Q. Wu, "An exploration of ranking heuristics in mobile local search," in Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, New York, NY, USA, 2012, pp. 295–304.

[6] R. Mahmood, N. Esfahani, T. Kacem, N. Mirzaei, S. Malek, and A. Stavrou, "A whitebox approach for automated security testing of Android applications on the cloud," in 2012 7th International Workshop on Automation of Software Test (AST), June, pp. 22–28.

[7] S. Moran, "Security for mobile ATE applications," in 2012 IEEE AUTOTESTCON, Sept., pp. 204–208.

[8] National Institute for Standards and Technology Computer Forensic Reference Data Sets. [Online]. Available: http://www.cfreds.nist.gov/

[9] B. Starzee, "'Flipped classroom' model leaps to Long Island," Long Island Business News, Apr. 2012.

[10] A. Stavrou, J. Voas, T. Karygiannis, and S. Quirolgico, "Building Security into Off-the-Shelf Smartphones," Computer, vol. 45, no. 2, pp. 82–84, Feb.

[11] V. Tirronen and V. Isomöttönen, "On the design of effective learning materials for supporting self-directed learning of programming," in Proceedings of the 12th Koli Calling International Conference on Computing Education Research, New York, NY, USA, 2012, pp. 74–82.

[12] M. Vorsino, "Teachers explore 'flipped' class," Honolulu Star - Advertiser, Jul. 2012.

[13] K. Woods, C. Lee, S. Garfinkel, D. Dittrich, A. Russell, K. Kearton (2011). Creating realistic corpora for security and forensic education. ADFSL Conference on Digital Forensics, Security and Law, 2011. p. 123-134. [Online]. Available: http://simson.net/clips/academic/2011.ADFSL.Corpora.pdf