Applying Mobile and Pervasive Computing Security Projects in CS Courses

Yujian Fu[1], **Di Ma**[2]
[1]Department of EE & CS, Alabama A&M University, Huntsville, AL, USA
[2]Department Computer Science, University Of Michigan at Dearborn, Dearborn, Mi, USA

Abstract - *In the information era, the Internet provides an unlimited platform and supports the mobile and pervasive computing in everyone's daily life, from oven, microwaver to the space craft. Today more and more users favorite the hand-held devices, mobile in a computer aided environment. Pervasive computing is in our life everyday. Security education in academic has been raised to an unanticipated level due to the proliferation of hand-held devices and applications. In this paper, we will presented an implementation of integrating mobile and pervasive computing security projects to computer science curriculum. This is a collaborative effort implemented by faculties at two national recognized institutions – Alabama A&M University and University of Michigan at Dearborn. The research study has involved several classes in undergraduate and graduate level with over 50 students participated, and demonstrated very exciting results in both pedagogical and scientific aspects among participated institutions. The developed projects with regarding to the curriculum design are presented and discussed.*

Keywords: Mobile security, pervasive computing, information assurance, cyber security, information security education

1 Introduction

In the information era, the Internet provides a unlimited platform and supports the mobile and pervasive computing in everyone's daily life, from oven, microwaver to the space craft. Today more and more users favourites the hand-held devices, mobile in a computer aided environment. Pervasive computing is in our life everyday. Security education in academic has been raised to an unanticipated level due to the proliferation of hand-held devices and applications. According to [1], malware attacks to hand-held devices has increased by 25 percent across all platforms since 2012. The McAfee Labs count of new suspect URLs set a three-month record with more than 18 million, a 19% increase over Q4 and the fourth straight quarterly increase. Among these attacks of various platforms, Android is the platform favorited by the most malware with most growth. 67.7% of host locations in North America. From mobile report of F-Secure [2], 91% new families or threats was identified, and among these new families of malware on mobile device 99% on Android platform. To reduce and mitigate the security threats and increase the defence capabilities of benign apps, traditional Intrusion Detection Systems (IDSs) has been shown inefficient. New behaviour-based IDSs are paid attention to by many mobile security researchers [3, 4]. In addition, a single or individual approach without the support of formal specification has been proved with more false positives in the results. The needs of formal specifications to provide the sound theories are more and more desired.

From the side of the educational point of view, the needs of the security issues of mobile and pervasive computing fall in the requirements of stakeholders, expectations of users at industry and academic. The needs of cyber security job market has increased 3.5 times percent since 2012 among all IT and information jobs according to CIO report from The Journal of Wall Street [5]. In addition, salary of cyber security position is 17% more than average of IT positions. To teach and train the next generation of cyber security workforce is kind of first need of current education in computer and STEM curriculum. This is one of the ultimate goal of this NSF supported project which is aligned with one of objectives of NSF SaTC program.

Two objectives of this NSF project are: First, enhancing the information security education through curriculum development. Second, enhancing students in the IA security through hands-on lab development. Before we illustrate the implementation towards these objectves, we will first introduce the current status of cyber security education in the institutions. After that, the course and lab development will be discussed in the next section.

1.1 Current Cyber Security Education at AAMU

The computer science department at Alabama A&M University is one of the oldest department of Alabama state since 1960s'. The information security and forensics curriculum of computer science was included in 2009 to fulfill ABET requirements and satisfy the evaluation criteria. Both courses does not have programming language courses as prerequisite courses, students with any level can register. This attracts many students but increases the concerns of the learning results and teaching quality in the content of information security. In addition, due to short of faculties in

the area, our students cannot be exposed enough security in theories and short of hands-on labs.

In 2011, driven by the needs of marketing, supported by Deans office, computer science annouced a cyber security concentration in undergraduate student curriculum. This cyber security concentration includes six courses: CMP 381 Computer Organization, CMP 384 Operating Systems, CMP 386 Cryptography, CMP 321 Principle of Information Security, CMP 414 Forensic Computing, CMP 421 Computer Security. Except for the core courses of CMP 381 and CMP 384, the other four courses offered once per year, and the student number registered to other four courses per semester is around 14 to 25. The peak of registration was reached by 2012. By the 2013 fall, the registration started to drop. These four courses are taught by 3 faculties and one adjunct professor. There is no pervasive computing and mobile courses offered in computer science curriculum.

There are several reasons of the student number droped in these security courses. One of the reasons is lack of the interesting and research related, hands-on lab. Some of the new research findings and security detections are not included and exposed, nor well designed lab, short of security theory and design analysis in the lectures. Second reason, there is no new topics to feed current millimum era students. This generation of students are grown up with electronics and internet. Information and electronics are their whole life. Traditional teaching and content are far from enough to satisfy our current students. Last reason is due to the limited number of students, there are not enough students to register these courses. There is an obvious need of the security in the pervasive and mobile computing from current computer science curriculum.

The paper is organized as follows. In the next section, we introduce the course design and curriculum development supported by this NSF program. In Section 3, the developed labs regarding to the mobile and pervasive computing are presented. Section 4 discusses the current evaluation by the survey in AAMU campus. In Section 5, a short discuss of pedagogical results will be described. Finally, we conclude our work in section 6.

2 Applied Course and Design

In this section, we will present the courses that are integrated with the security contents and projects. Furthermore, a new course developed in UMD was presented here.

Several courses that were updated with security and integrated with security projects in both AAMU and UMD campus. In AAMU campus, we have simply attempted security projects in software engineering (CS 401) and senior design classes (CS 403).

2.1 Software Engineering Course (CS 401)

CS 401 is software engineering class which requires senior standing. This course is designed to explore the traditional approach to software development & construction life cycle, software crisis, and software characteristics. In the course description, it is to cover various software engineering paradigms, and the fundamental concepts of analysis, design, coding, testing and maintenance [6]. Besides, this course introduces various CASE tools that support these methodologies.

Three student learning outcomes are covered from the current syllabus:

a) Understand the traditional approach of software development process, software characteristics, software quality, ethics issues, crisis issues and software development cost and management.

b) Understand and be able to use basic software engineering methodologies to solve large scale software/software-intensive system development. Understand and be knowledgable about existing tools of some software engineering methodologies. *Understand and be able to design and implement cyber physical systems with critical concerns including security aspects.*

c) Be knowledgable of software testing strategies and be able to use basic software testing technologies to validate program.

Security issues have brought a lot of attention of system analysts and software engineering. The earlier to detect and identify errors and faults, the more to reduce the cost of failure. It remains challenge to identify vulnerabilities in the software design models of systems and applications. To help students to understand how design level can help reduce the system crash due to malicious attack, we have updated the courses with two aspects – in lecture and in the hands-on projects, as follows:

In lecture, UML sec was introduced to develop the model of the secure system. In addition, to identify the security properties of the applications, OCL (Object Constraints Language) was introduced to the class in three levels – the syntax, the semantics and practice questions. We have introduced complete set of OCL syntax by combining OCL security specification with the UML diagram. To help student to have a better understanding, we introduce segment of systems based on the context and domains. The hands-on project selected is testing of SMS message passing on Android. This hands-on project will be introduced next section.

2.2 Updated Senior Design Course (CS 403)

The senior design course is a core course for undergraduate students at AAMU that requires CS 401. The course aims at exposing students to various types of systems and development processes. Development and successful completion of a sponsored software development project. Specific objectives include the development of effective project management, communication, and technical skills, experience with the implementation and testing phases of a realistic product design cycle, and an ordered transition from a

classroom-oriented academic environment to a performance-oriented professional environment. Student learning outcomes:

1. Improve the ability to apply knowledge of computing, mathematics, science and engineering.
2. Improve the ability to design, implement and validation a computer-based system, process, component, or program to meet desired needs.
3. Enhance the ability to analyze a problem, and identify, formulate and use the appropriate computing and engineering requirements for obtaining its solution.
4. To be understanding an understanding of professional, ethical, legal, security and social issues and responsibilities.
5. Prompt the ability to use current techniques, skills, and tools necessary for computing and engineering practice.

In the project designed in this course, we particularly increase the project pool with a couple of Android and security projects – including SMS message passing, testing on the cryptography algorithm in SMS app, Android app of AAMU faculty info. Students have shown great interest in the android apps and security projects. In the data collected, it shows that one group worked on Andriod app, and one group worked on the security testing of SMS app.

In addition to the above two courses, we have designed and implemented other mobile security projects and used in the Object oriented design (CS521), and Software Engineering Methodology (CS561). The detailed project description will be presented in Section 3.

2.3 New Course Development at UMD

A new course of pervasive computing and mobile computing was developed by UMD last year. The course aims at integrating the latest research results in pervasive computing and mobile security to the current CS curriculum. In addition, this course is designed to a thorough analysis of the major trends in pervasive and mobile computing and explain the implications in terms of security and privacy. For every security and privacy issue, we will give a detailed description of the problem and a precise explanation of mainstream solutions wherever they exist, and of potential solutions otherwise. Tentatively, a total of nine topics were developed. A brief description of each topic is given as follows.

Topic 1: Introduction to Pervasive & Mobile Computing. This topic covers the wireless communication and security & privacy risks.

Topic 2: Wi-Fi LAN and cellular network security. This topic introduces network access security requirements, wifi security, cellular network security.

Topic 3: RFID security and privacy. This topic exposes students with RFID technology and applications, security and privacy threats, defenses mechanism, and NFC & mobile payment systems.

Topic 4: Smartphone security. This topic brings the current research study in smart phone systems, security models, attacks on android permission, smartphone malware detection, and BYOD security.

Topic 5: Vehicle and vehicular Ad-Hoc (VANET) security and privacy. The cutting-edge research studies on the intelligent transportation systems, in-vehicle data & communication systems and vulnerabilities, IEEE 802.11p for wireless access in vehicular environments and IEEE 1609.2 for VANET security are discussed.

Topic 6: Secure device paring. This topic includes Bluetooth-enabled device pariting and other device pairing mechanisms through SMS, directory service, multiple antenna.

Topic 7: Secure ranging. This topic covers the relay attack, relay attack defense.

Topic 8: Secure neighbor discovery. The wormhole attack, centralized and decentralized approach for wormhole detection will be discussed.

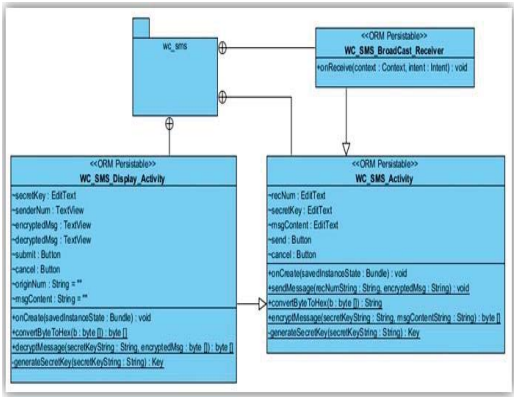
Topic 9: Secure localization and location privacy. This topic focuses on the device localization and vulnerability, secure localization based on own measurements, and location privacy in VANET.

3 Project and Lab Design of Mobile Security and Pervasive Computing Design

In this section we will present the projects developed for mobile and pervasive computing project that were used to integrate with the updated courses and lab development. These projects are developed by two institutions in the past project year.

3.1 Testing – SMS Encryption Algorithm

SMS messaging [7] is a mobile and stronger version of "any time" and "any where" service. A switched-on mobile device is able to receive or send a message regardless of if a voice or data call is in progress. To secure the private data and ensure the correctness of the system implementation, this project is developed in three phases: I) develop a SMS app that is able to pass simple message with AES. Through this phase, student will be exposed to fundamental skills of Android apps, the simple AES algorithm (Fig.1. (b)). II) Develop a class diagram of the SMS message passing (Fig. 1 (a)). In addition, define the authentication security properties in OCL on the class model. Through this phase, students will be able to understand the software design methodology, security properties in a simple format (UML diagram). III) Install JUnit and run assertions on the OCL properties to demonstrate if the cryptographic algorithm implemented correctly by a set of properly designed security properties. By doing this, students will have a better understand of the system quality, crisis, how to ensure the correct implementation, and crash cost bring by the vulnerability.



(a)

Figure 1. The design and snapshot of Android security testing

3.2 WiFi Sniffing on Android

Traffic monitoring is one of the key approaches in the network security to detect the potential vulnerabilities and/or attacks. Rooted on various types of methodologies, many tools are developed regarding to the monitoring aspects and flow strategy. One of the most powerful spying tools is Intercepter-NG [8]. It is a free application with unrestricted functionality and is virtually universal: works on Windows, Linux, Mac OSX, iPhone and Android. It is a multifunctional network toolkit for various types of IT specialists [9]. It has functionality of several famous separate tools and more over offers a good unique alternative of wireshark for Android. After connected to the AAMU WiFi using Intercepter-NG, we can run the scan command to see all the devices with IP addresses that are connecting to AAMU WIFI. Result is shown in Fig. 2, where a list of AAMU WiFi address was recognized and displayed to the screen.

(b)

Figure 1. The design and snapshot of Android security testing

Figure 2. Snapshot of WiFi Sniffing – AAMU WiFi

3.3 Permission ID based Security Analysis

The Android OS system runs each application under the privileges of different "user". A unique user ID to each of them is assigned when the application request is coming. Applications are required to declare in a manifest that can take place in the course of execution [10]. This project is designed to expose the different security levels of permission ID in the Android systems, and if sensitive permission ID is required. It is straightforward to predicate that an application overprivileged needs to be suspected (Fig. 3).

Figure 3. Snapshot of permission ID based security analysis

3.4 Man-in-the-middle Attack Exploiting Certificate Verification Flaws In Smartphone Apps

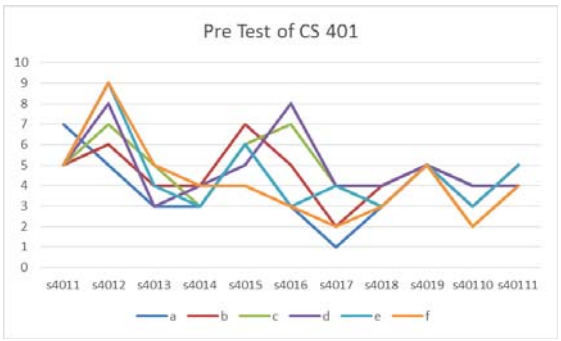
On the smartphone app market, apps are developed by developers with various level of security knowledge and many of them are suspected to be flawed in certificate validation. In this project, a student is expected to conduct a serial of experiments to find flawed apps and further analyze the cause.

3.5 WebView Information Stealing

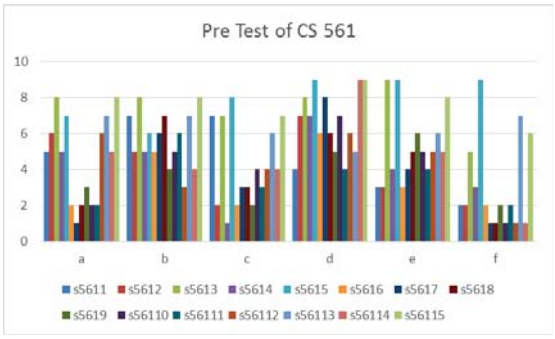
Web applications relies on several TCB (trustworthy computing base) components to achieve security. One important TCB component is the use of trustworthy browsers. However, WebView (embedded browser for mobile apps) changes the picture of TCB for web security. The lacking of security support for cross-application interface embedding in mobile platforms allows a malicious host to eavesdrop on input intended for embedded interface only. In this lab, students are required to mount a password-grabbing attack by using JavaScript injection.

d) How much important do you evaluate security regarding to a quality software?
e) Do you think system design place a key role on the software quality?
f) How much do you know about software testing?

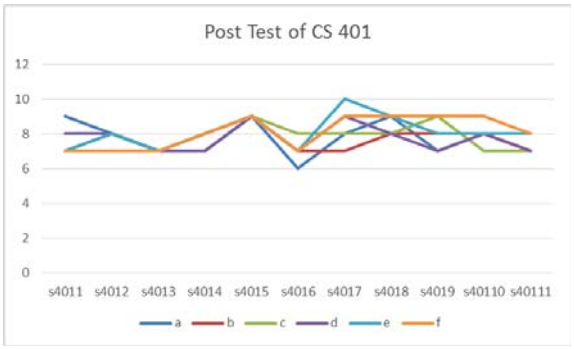
For classes in Spring 2014, it was interviewed at 11 students in CS 401 and 15 CS 561. A statistic results regarding to questions are shown in Fig 4. It is clearly shown from both classes that many students do not consider the security and cyber attacks play a critical role in the reliability of the system development. After this class, the students had changed their mind and the collected data indicated that most considered the



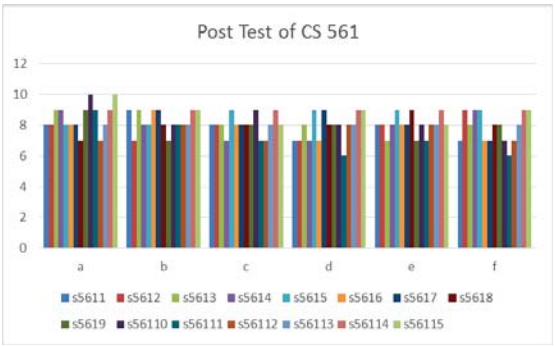
(a) Pre test of CS 401



(c) Pre test of CS 561



(b) Post test of CS 401



(d) Post test of CS 561

Figure 4. Data collection for courses cs 401 and cs 561.

4 Evaluation and Discussion

Class evaluation is done regular each semester. Other the regular class evaluation, for CS 401 and 403 at AAMU, the instructor has developed pre and post set of questions to evaluate these courses.

The pre/post test question for CS 401 is listed as following. The answer is given from 1(no knowledge) to 10 (very much know).

a) How much do you know about Software Engineering?
b) How do you consider System quality is critical during software development process?
c) Do you consider cyber attacks and security holes in the system as one of the key factors that cause software system crash and cost a lot?

security is one of the key concerns of the reliable system design. For CS 561, we have shown the value of each answers pre- and post test, in addition to the line chart. Even some graduate students have shown the knowledge of reliability regarding to security in the system design at the software engineering aspect, there is still an increase of the value regarding to these questions.

We also conducted the pre and post tests of CS 403 and CS 521 (object oriented design and implementation). Since these two courses are less in common, the question sets are a little bit different. Due to the space, the pre/post test questions for CS 403 and CS 521 are not listed.

5 Pedagogical Issues

We summarize pedagogical significance regarding to the project – motivation. Motivation is a topic that remains to be challenge to all education researchers how to motivate students in different areas. Project based learning (PBL) is one of the traditional technology that has been proved effective in the student motivation, provided that the topics are very interesting and the ideas are novel, the skills is simple and the knowledge are not too much. On the contrary, students will be easily to loss interest and PBL will not make sense for the purpose of improve student learning outcomes. Regarding to these concerns, and our projects are designed in the large extent to maintain constant student interests on the point of this final results on the Android security is rooted in daily life and the topic is attractive.

6 Conclusions and Future Works

In this paper, we presented a study of integrating pervasive and mobile computing to CS curriculum at AAMU and UMD in the past year. Several updated courses, one new developed course, and hands on lab were discussed. Student evaluation was presented. This work demonstrated that properly integrating new cutting edge research projects to CS curriculum can motivate students in pursuing higher degree or continue on the computer science study even if the CS market right now is not taking the lead position of all jobs. Students always love to see new research results and are exciting about the using and applying the ideas to a not complicated project. In the future, on top of current result, we expect to i) to develop more interesting projects that are rooted from current research study and is able to fit for CS or STEM curriculum; ii) conduct more study especially tracking students in the high level grade and/or graduate study.

Acknowledgements

The research work was supported by National Science Foundation of USA under Grant No. 1419295 and Grant No. 1419280.

7 References

[1] MacFee Report. Mobile Malware Report. June 2014.
[2] F-Secure Report. Mobile Malware Report. June 2014.
[3] Mu Zhang, Yue Duan, Heng Yin, and Zhiruo Zhao. "Semantics-Aware Android Malware Classification using Weighted Contextual API Dependency Graphs", In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS'14), November 2014.
[4] Mu Zhang and Heng Yin, "AppSealer: Automatic generation of vulnerability-specific patches for preventing component hijacking attacks in Android applications", In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14), February 2014.
[5] Steve Rosenbush. Demand for Cyber Security Jobs is Soaring. March 2013. CIO Journal. The Wall Street Journal. Retrieved From: http://blogs.wsj.com/cio/2013/03/04/demand-for-cyber-security-jobs-is-soaring/
[6] Ye Wu, Mei-Hwa Chen, and Jeff Offutt. "UML-based Integration Testing for Component-based Software". *Proceedings of the Second International Conference on COTS-Based Software Systems*, Lecture Notes In Computer Science; Vol. 2580, pages: 251 – 260, 2003.
[7] Sagheer, A.M.; Abdulhameed, A.A.; AbdulJabbar, M.A., "SMS Security for Smartphone," In proceedings of The *Sixth International Conference on Developments in eSystems Engineering (DeSE), 2013*, pp.281-285, 16-18 Dec. 2013
[8] Intercepter-NG. Available from: http://intercepter.nerf.ru/
[9] XDA Developers Forum. Available from: http://forum.xda-developers.com/showthread.php?p=35159281
[10] Z. Aung, and W. Zaw. "Permission-Based Android Malware Detection." International Journal of Scientific and Technology Research, Vol. 2, Issue 3, March 2013.