Integrate Mobile Devices into CS Security Education

Hongmei Chi
Department of Computer and Information Sciences
Florida A&M University
1333 Wahnish Way
Tallahassee, FL 32307 USA
hchi@cis.famu.edu

ABSTRACT: *Mobile computing, popularized for social media, has emerged as a delivery vehicle of choice for commercial, medical and military applications. The ubiquity of wireless and satellite communication and the rapid evolution of powerful devices that exploit this infrastructure have pushed mobile application development, in many instances, ahead of the capabilities to ensure the secure and safe utilization of these applications. The gap between capabilities and the ability to safeguard information assets must not be ignored, given the documented rise in the number and sophistication of threats and the broadening vulnerabilities of mobile applications and systems worldwide. We are focusing on how to integrate mobile apps/devices into our cyber security courses. In addition, case studies and hands-on labs are discussed in our teaching practice.*

Keywords: Mobile Device, Malware Detection, Digital Forensic, Mobile Health, Active Learning, IA Education

Received: 8 July 2015, Revised 11 August 2015, Accepted 17 August 2015

1. Introduction

The smartphone is arguably the most utilized device on the planet. It is used for a variety of task including some that require secure transmission, such as bank transactions and transfers. It is predicted that the phone market this year will grow to over 1.8 billion devices and reach 2.6 billion by 2016 (http://www.canalys.com/newsroom/mobile-device-market-reach-26-billion-units-2016). With the Android operating system predicted to hold the lion's share of the mobile market at 79% by the end of the year, mobile security on this platform is a high priority [3, 5]. Due to the rapid demand and popularity of mobile devices, the security of mobile computing is vital to the growing army of users and for the future of our social, economic and political systems [16].

The standard bearer for mobile computing is the smartphone, which connects people anytime and anywhere. Smartphones also store a large amount of personal information and run applications that may legitimately, inadvertently, or maliciously manipulate this information. The relatively weak security models for smartphone applications, coupled with ineffective security verification and testing practices, have made smartphones an ideal target for security attacks. Advancing the science, technology and practices for securing mobile computing are essential to support the inevitable use of mobile computing in areas with even requirements for privacy, security and resistance to tampering. Hence, it is important and needed to develop hands-on learning materials on mobile security that produce a well-educated and trained workforce.

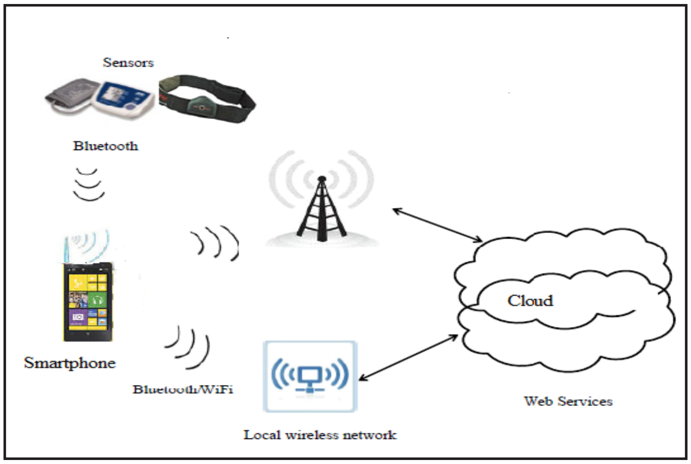


Figure 1. System structure of mobile health [3]

As shown in Figure. 1, mobile health (mHealth) is a growing and emerging field that infuses wireless technologies, security, policy, infrastructure and the integration capabilities of the United States and global healthcare systems [6]. Mobile health will help doctors to reach out effectively to rural and remote areas where healthcare is seriously or even totally lacking. Mobile health applications have the potential to provide more convenient health care services, improve or maintain the health status and quality of life for patients, and promote the development of the health industry as well as the health environment. Mobile health applications have been found to facilitate earlier and more effective intervention for both physical and mental illness. Mobile health applications offer unique opportunities for monitoring progress, providing education materials, receiving personalized prompts and support, collecting ecologically valid data, and using self-management interventions when and where they are needed.

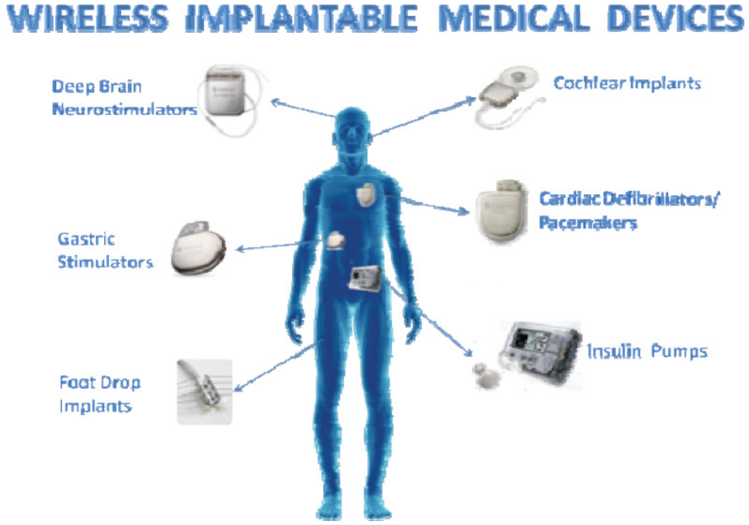

WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Cardiac Defibrillators/ Pacemakers
Gastric Stimulators
Insulin Pumps
Foot Drop Implants

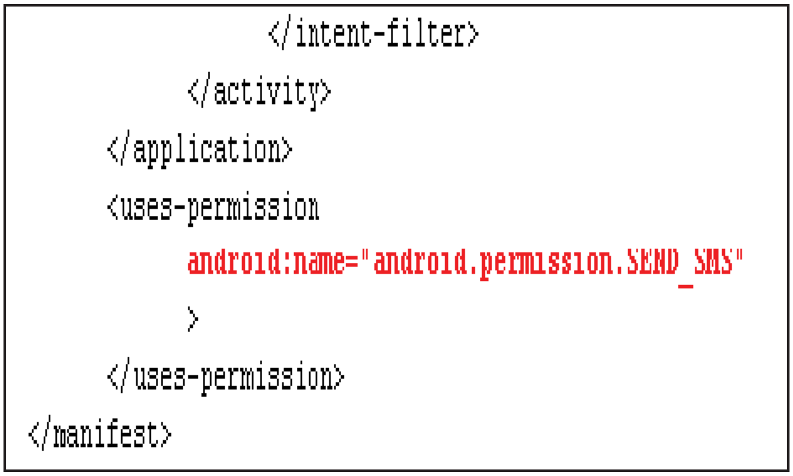
Figure 2. Securing implantable medical devices [8]

The variety of IA curricula and diverse educational models at universities has to provide their graduates with skills demanded by employers. Smartphone and cloud computing are skills that our graduates have to master before they go to job market. The levels of skills expected by employers and those graduates have acquired after completing their studies suggests a discrepancy. In this paper, we attempt to approach how we can make our IA education consistent with changing reality. Each student has his/her own smartphone, security issues in mobile devices are one of their interest. It depends our instructors how to inspire students to learn those

The rest of this paper is organized as following: in Section 2, an introduction to in-depth mobile malware. Section 3 provides related work. Section 4 will give details of our approaches in teaching practice. Section 5 will discuss a small number of student feedback and lessons we have learned. In Section 6, conclusions will be outlined.

2. Mobile Malware

It is reported that 17% of cell phone owners do most of their web browsing on their phones, rather than a computer or other device [2]. Improvements in mobile computing have allowed mobile devices to be used for tasks that were traditionally carried on desktop and laptop computers. Mobile devices now enable users to complete online banking, shopping, browsing, email and even navigation, on our mobile devices. Mobile applications and commerce hosting firm Branding Brand, recently announced that mobile traffic had accounted for 35% of all web traffic on their hosted services. Mobile devices today have integrated the use of technology such as GPS (Global Positioning System) to give user's a more personalized experience, but these conveniences come at a cost of security risk and mobile device resource depletion. Mobile devices lack the resources of larger desktop and laptop computers. Resources such as processing power, storage, memory, and network connectivity are all limited. Advances in technology have removed some of the constraints of mobile devices, enabling them to carry out more process intensive task such as video editing and gaming. Along with increases in network bandwidth and battery life, malicious hackers have taken notice and malware designed for mobile devices is on the rise, but much more active for the Android platform. The motivation for gaining access to mobile devices is obvious, access to Personally Identifiable Information [10]. This information includes location, calls logs, text messages, photos and any other information stored on the device. Mobile malware is increasing becoming more common in users mobile experience. Computer world recently published an article where they stated that the number of malicious number of applications on the Android platform had increased by 614 percent [9]. This highlights the growing threat that has to be addressed in order to protect users and their confidence in the Android operating system.



```
                </intent-filter>
            </activity>
        </application>
        <uses-permission
            android:name="android.permission.SEND_SMS"
            >
        </uses-permission>
</manifest>
```

Figure 3. Android.FakePlayer XML code for SMS permission

Malware for amusement does not pose a large threat to users, but as proven in the past with personal computers, malware always becomes more complex and is ultimately used for economic gains. The ultimate aim of the attacker is to monetized malware, below are some of the current schemes being used to monetize malware on the Android platform.

Premium rate number billing is one of the more common types of malware that generates revenue for the attacker. In this scheme the attackers setup one or multiple "short code numbers", for example www.gofast.com allows users to text there address to "777222" to use their taxi service, which is a legitimate use. Attackers however register these short code numbers, and use them in co-ordination with malware on mobile phones. These pieces of malware that are embedded into applications, silently send SMS messages to one of more of their pre-setup short code numbers which incurs extra cost on the user phone bill and generates revenue for the attacker. The attacker receives 30% - 70% of the entire rate; most carriers allow a premium rate of up to $10.00 per message. The Android Fake Player (Android.FakePlayer) is one of the many malwares that sends messages to premium short codes. It sent two it messages at the premium rate of $3.50 and $6 . Some of the other notorious apps known for sending premium rates are EXPLOIT/DIUTESEX.A ANDROID/FAKEINSTALLER.S [11].

Permissions and APIs used by threats		
Action	Permission Required	API
Intercept SMS messages	RECEIVE_SMS	BroadcastReceiver
Read SMS message	READ_SMS	getContentResolver()content://sms
Record audio	RECORD_AUDIO	AudioRecord.startRecording()
Read call logs	READ_CONTACTS	CallLog.Calls
Obtain GPS Coordinates	ACCESS_FINE_LOCATIONACCESS_COARSE_LOCATION	LocationManager

Table 1. Common permissions for data stealing application malware [12]

Mobile spyware is a malware that once installed on the mobile device, allows the attacker to track the mobile device owner by recording and transferring all SMS messages, call logs, emails, photos, GPS location and other data. Table -1 shows the common permissions required to enable a device to send call log, SMS and GPS information to the attacker.

The data being stolen can include location, credit card numbers and more. The location data can be used for targeted adWare and credit card numbers can be sold online. The AndroidOS.Tapsnake is a game that was available on the Google Play market. According to security firm Symantec, the description stated, "*Yet another modification of the Google Android Snake game. This one listens to the taps for its turn directions.*"[12]. the game played as you would expect it to however the satellite icon at the top bar appeared when the game was running. This indicated that the game was uploading GPS co-ordinates to a server. Embedded within the game was a Trojan that uploaded the user's GPS data to a remote server. In order to receive the GPS co-ordinates, a second paid-for application called "GPS SPY" must be installed on a second Android device, this device would track the device with Tap snake installed [12].

The AndroidOS.Tapsnake application is just one of the many apps embedded with Trojans that allow attackers to steal user data. The Uapush.A Android Trojan sends SMS messages and steals user data, the malware command and control server is located in China [36]. Most research firms believe that the trend of increased mobile malware is expected to continue.

Search engine poisoning is a method used to manipulate search engine website ranking. Search engines rank websites on a per visit basis. This is the same with smaller mobile versions that look specifically at mobile visits. Malicious applications can manipulate a search engine's ranking system by initiating search request for that web page, thus artificially raising its search rank. This allows the attacker to generate revenue using pay-per-click services. One example of this kind of malware is Android.Adrd. The malware is injected into a legitimate application, and reloaded onto the Android market place. Once installed on the compromised device the application attempts to steal hardware info (IMEI, IMSI), encrypts the data and send it through a local proxy, next it receives search parameters from a URL and send HTTP search request to this URL, "*wap.baidu.com/s?word=[ENCODED SEARCH STRING]&vit=uni&from=[ID]*" [13].

Attackers traditionally used key-loggers in order to steal user authentication strings from personal computer and mobile devices. Today malware is developed to specifically target financial institutions. The application was designed to steal the mobile transaction authentication numbers (mTANs) associated with banking transactions, which are the temporary passwords users receive from their banks via SMS message [13]. Many European banks use mTAN's to authorize transfer of funds. The Zues malware intercepts all incoming messages and transmits them to a phone or webserver controlled by the attacker. Thus giving the attacker the ability to sift through the data and search for mTAN numbers. The ZitMo malware is an Android version of the notorious Zues personal computer malware. The Zitmo mobile malware works in co-ordination with the Zeus banking Trojan to steal login information or funds from your accounts using a number of methods including, phishing, Trojan tempered apps, intercepting SMS messages and sending authentication credentials to command and control server [13].

3. Related Work

Currently, there are various courses are developing and offering courses on mobile programming and development [15]. Various hands-on labs for information assurance concepts other than mobile malware, such as network security, secure programming, secure web-programming, mobile security, Cloud security and inside threat [17]. But is it hard to find few training hands-on labs for mobile malware and how to detect such threat. Current and future IT professionals and workforce are required to understand security issues related to mobile devices.

The dominant pedagogical approach for security education has been to use security exercises in a lab setting, which might not deliver effective learning experiences due to the decontextualized learning, that is, lack of real world examples. Most existing security labs teach abstract concepts that are not situated in real-life contexts. A student who learns security concepts solely in a decontextualized setting might not be able to apply the necessary skills when facing real-life security threats [16].

4. Approach

It is our view that instruction must adapt to these demands. Reaching today's students can be a challenge when using primarily lecture-based instructional methods. Today's youth are visuo-spatially intelligent and talented [4] and may need to experience instruction that is visual and that requires active participation. Learning by Doing is best described by a Chinese famous educator Confucius who said two thousand years ago, "tell me and I will forget, show me and I may remember, involve me and I'll understand." When students with limited mobile and cloud computing background study information security fields, they face a steep learning curve. Hands-on labs that employ game playing help students to quickly grasp core content and topics.

Student-Led Current Event Reviews: To motivate students' interest and awareness in news related to smartphone security, we encourage students to pay attention to press news or technology news related to mobile malware and security topics. All Current event summations and presentations must respond to the following questions: (1) How does the topic you have chosen relate to mobile devices? (2) How do the topics discussed in your article(s) relate to the basic mobile security goals – Confidentiality, Integrity, and Availability (CIA)? (3) What is the global/societal impact of the topic(s) discussed in your article(s)?

Most students are enthused to complete those assignments.

Here are examples of topics chosen by students: (1) Android malware spies on you even after phone is shut down [18] ; (2) Android malware increasing, getting smarter [19] . This assignment helps to encourage our students to remain engaged in mobile security topics and concerns.

Hands-on lab exercises: A typical of our lab will include the following:

Case Description: What crimes have been committed? Give a scenario leading up to the investigation and stating why the computer may be a rich source of evidence.

Lab goal: What's the purpose of this lab? What new techniques in digital forensics will the student take away?

Some guidance as to how to go about the investigation: Small hints to guide the student in the right direction. Hints will be minimized as lab difficulty increases.

***Q*uestions related to lab**: In the last part of our lab, students have to response questions related to our lab procedure and you may not answer without completing the lab.

Term project: term project is designed to give students a chance to solve real-world problem by adopting what they have learned in our class. Students are given 1-2 month period to complete a project with a hands-on lab generated by students.

Active learning classroom: Through the NSF SCALAR (Student Centered Active Learning and Assessment Reform) Project, FAMU has been practicing the active learning classroom based teaching and learning method in the areas of biology, computer science, chemistry, mathematics, and physics. Figure 4 shows a typical active learning classroom setting at some universities. Each round table supports several laptops with switching technology that connects them to a projection system. The centered control station allows the instructor to select and display table-specific information. Multiple white boards are distributed around the perimeter of the classrooms. Instructors and students have to prepare before each class. Students are required to complete pre-class assignments before they come to class.

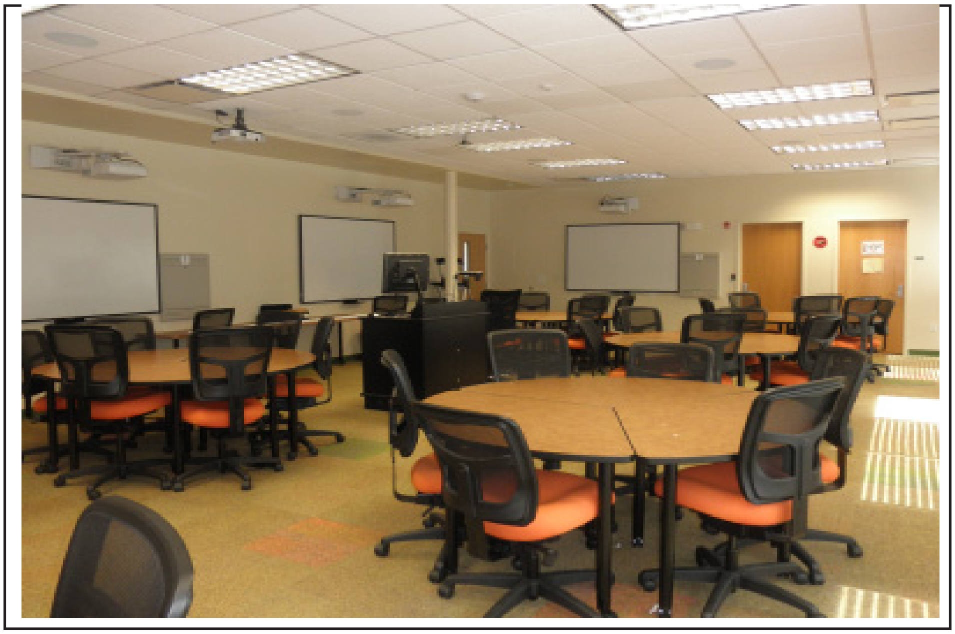


Figure 4. A typical active learning classroom setting

5. Student Feedback

Anecdotal feedback from students has been very encouraging. We collect responses for each course that including smartphone security topics at the end of each semester. Several responses are presented below to the following question: What did you like the best about this course?

"*I like those current event assignments and so much tech news related to mobile security.*"
" *The pre-class assignment helps me to prepare my learning effective*ly."
"*These assignments really opened my eyes to mobile security and how to protect my privacy*"
"*I like term project and the most interesting lab is that I can design my own labs and learn free source tools.*"
"*The hands on labs and the in-class discussions made me want to learn more about mobile security*."

6. Conclusions

We have discussed our approaches for integrating mobile security in CS-courses via active learning activities. In the future, we will continue to improve and expand the mentioned activities to include current trending topics and popular security tools. In addition, we will continuously retrieve student feedback to make activities better learning tools and more student-friendly.

In near future, we plan to develop mobile security activities/modules to be included in courses taught to non-CS majors as a way to increase mobile security awareness. In addition, we are planning on expanding mobile security education at FAMU by offering m-learning opportunities to our students and the community; we hope to incorporate our active learning approaches to support this effort.

7. Acknowledgements

This work has been supported in part by NSF #1332520 and Army Research Office grant No. 64622-CS-II. Any opinion, finding, conclusion or recommendation does not represent the views of NSF or Army Research Office.

References

[1] Avancha, S., Baxi, A., Kotz, D. (2012). Privacy in mobile technology for personal healthcare. ACM Computing Surveys (CSUR), 45 (1) 3.

[2] Burmester, M., Munilla, J. Pre vs Post State Update: Trading Privacy for Availability in RFID, 1-4.

[3] Chatmon, C., Chi, H., Davis, W. (2010). Active learning approaches to teaching information assurance. In 2010 Information Security Curriculum Development Conference (p. 1-7). ACM.

[4] Johnson-Laird, P. N. (2013). Mental models and cognitive change. *Journal of Cognitive Psychology*, 25 (2) 131-138.

[5] Paul, D., Chi, H., Allen, C. (2013). GPU-based simulation of wireless body area network. *In*: Proceedings of the 8th International Conference on Body Area Networks (p. 244-247). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[6] Mare, S., Sorber, J., Shin, M., Cornelius, C., Kotz, D. (2013). Hide-n-Sense: Preserving Privacy Efficiently in Wireless mHealth. Mobile Networks and Applications, 1-14.

[7] Pournaghshband, V., Sarrafzadeh, M., Reiher, P. (2013). Securing legacy mobile medical devices. *In*: Wireless Mobile Communication and Healthcare (p. 163-172). Springer Berlin Heidelberg

[8] Li, H., Zhang, T., Chi, H., Chen, Y., Li, Y., Wang, J. (2014). Mobile health in China: Current status and future development. Asian journal of psychiatry, 10, 101-104.

[9] West, D.M., Bleiberg, J. (2014). United States and China are Leading the M-Health Revolution, Brookings. http://www.brookings.edu/blogs/techtank/posts/2014/03/14-us-china-leading-mhealth-revolution (retrieved 09.05.15).

[10] Pittman, J. (2013). Understanding System Utilization as a Limitation Associated with Cybersecurity Laboratories–A Literature Analysis. Journal of Information Technology Education: Research, 12, 363-378.

[11] McAfee, Consumer Mobile Trends Report – June 2013, Free Apps, Freedom, And Free Money, from http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf

[12] Chien, E. (2014). Motivations of recent android malware, February. http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf

[13] Vanja, S. SophosLabs, When Malware Goes Mobile: Causes, Outcomes and Cures, https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/Sophos_Malware_Goes_Mobile.pdf?la=en.pdf

[14] Kevin, R. (2009). Lawrence and Hongmei Chi. 2009. Framework for the design of web-based learning for digital forensics labs. *In*: Proceedings of the 47*th* Annual Southeast Regional Conference (ACM-SE 47). Article 76 , 4 pages.

[15] Paul E. Dickson. (2012). Cabana: a cross-platform mobile development system. In Proceedings of the 43*rd* ACM technical symposium on Computer Science Education (SIGCSE '12). ACM, New York, NY, USA, 529-534

[16] Lo, D. C. T., Qian, K., Chen, W. (2015, October). Mobile security education on portable labs. In Frontiers in Education Conference (FIE), 2015. 32614 2015. IEEE (p. 1-4). IEEE.

[17] Hongmei Chi., Clement Allen., David Angulo Rubio. (2015). Design Insider Threat Hands-on Labs, *Information Security Education Journal*, 2 (1) (June 2015), 34-42.

[18] Android malware spies on you even after phone is shut down, http://mashable.com/2015/02/19/android-malware-spies-shut-down/

[19] Android malware increasing, getting smarter, http://www.foxnews.com/tech/2015/01/16/android-malware-increasing-getting-smarter/

7. Author biographies

Dr. Hongmei Chi is an Associate Professor of Computer & Information and Sciences at Florida A&M University. She currently teaches graduate and undergraduate courses in Information Security and researches in areas of applied security. Dr. Chi has published many articles related to security research and education. Her web page is www.cis.famu.edu/~hchi.