ISSN: 2473-3857
v2 n4059

Mobile Forensics and Security Certificate: An Addition to a Cyber Security Degree

Karen Paullet
paullet@rmu.edu

Jamie Pinchot
pinchot@rmu.edu

Sushma Mishra
mishra@rmu.edu

Computer and Information Systems
Robert Morris University
Moon Township, PA 15108, USA

Abstract

Cyber Security degrees are being offered at institutions all over the world due to the increase and demand for trained professionals. There is a serious gap in cyber security education in regard to mobile technologies. The surge in the use and reliance on mobile technology, combined with the scarcity of programs that prepare specialists in this area, creates a need for Universities to add mobile forensics and security to their curriculum. To fulfill the needs of industry, Robert Morris University has developed a Mobile Forensics and Security Certificate. This paper describes the rationale, development and implementation of this new certificate.

Keywords: mobile forensics, mobile security, cyber security, education

1. INTRODUCTION

Cyber Security degrees are being offered at institutions all over the world due to an increase and demand for trained professionals. As of July 2016, there is a serious gap in cyber security education in regard to mobile technologies. The surge in the use and reliance on mobile technology, combined with the scarcity of programs that prepare specialists in this area, creates a need for Universities to add mobile forensics and security to their curriculum.

Mobile security courses are lacking in higher education while mobile security threats are becoming a top concern for businesses. It is a critical need to the field of cyber security to have well-trained specialists because the use and dependency on mobile technology is growing at an exponential rate.

Every day, individuals and businesses become more reliant on mobile devices. Smartphones and tablets have become essential communication gear carried by business professionals as well as individuals of all ages and professions. It is not uncommon to look around a crowded room, bus, or restaurant and see the majority of people using mobile devices. With this widespread use of mobile technology comes a varied list of security concerns. Hackers with malicious intent can target mobile devices as entry points into personal or business data. Breaches of personal mobile devices could result in data theft, identity theft and financial loss, or serious damage to reputation. Breaches of mobile devices that contain business data could result in leakage of sensitive business information, reputation damage, disruption of business services, damage to IT systems, and longer-lasting consequences such as customer turnover due to lack of trust and regulatory actions or lawsuits.

Trends in mobile security continue to grow at a rapid pace due to the Internet of Things. People are now connecting FitBits, toys, smart watches, medical devices, appliances and clothing to their mobile devices via Bluetooth technology (Trends, 2016). The connectivity of hundreds of devices is causing an area of concern in mobile security.

There are currently a number of courses addressing cyber security (which includes general information and network security) in higher education, and this is reflected in Robert Morris University's Computer and Information Systems curriculum. However, there are no courses that examine new security risks posed by the introduction of mobile technology, and discuss the role of cyber security and mobile policy in terms of incident prevention, compliance, and governance. To address this gap a certificate in Mobile and Forensics and Security has been developed at the University.

2. MOBILE SECURITY NEEDS

Security issues in the mobile environment are becoming more problematic and complex. More than 72% of adults in the United States own a smart phone, which expand their mobile access to the Internet and allow for use of mobile apps (Poushter, 2016). Mobile phones are used for more than just talking. They can be used for taking pictures and videos, text messaging, obtaining driving directions, accessing and searching the Internet, and listening to music. However, the conveniences of mobile technology are counterbalanced by the threat of criminal activity. Mobile devices have consistently proven to be an instrument or accessory of criminal activity. New ways of abusing wireless and mobile devices to facilitate the commission of technology-enabled crime continue to emerge (Choo, Smith & McCusker, 2007).

Mobile malware is on the rise and is projected to continue its upward trajectory, propelled by the large continually growing smart phone user base and increasingly mobile workforce, which provide enticing targets for hackers (Levitt, 2011). As of August 2015, the number of malware threats reached over 45 million (Symantec, 2016). Malware is any computer program designed to infiltrate, make use of, or cause damage to a device without the owner's consent. "Hostile", "intrusive", and "annoying" are all connotations commonly associated with the term malware, which is derived from "malicious software" (LaPolla et al., 2013). Mobile malware is any type of malware that is specifically targeted toward smart phones, tablets, and other mobile devices. The main goals of most mobile malware include stealing private data, incurring charges on calls to premium phone numbers, or gaining access to a user's financial accounts (LaPolla et al., 2013). Mobile malware poses a serious threat and is predicted to soon rival that of traditional computer malware (Felt et al., 2011).

Information security for mobile devices has not evolved at a sufficient pace to match the rise in mobile malware (Frost, 2013; Webroot, 2016). Cyber criminals are targeting mobile devices due to the lack of security measures in place. Attacking mobile devices has become extremely attractive to criminals due to the plethora of information that is stored on the device. Such information includes e-mail accounts, phone numbers, calendar information, network or login credentials, confidential notes or files, and contact lists to name a few.

The trend of workers becoming more mobile is likely to continue, and consequently, mobile and wireless devices will become increasingly important tools for accessing information when desktop computers are unavailable. Mobile devices and networks will continue to become more sophisticated and better able to support a wider range of communication and collaboration functions. Such devices will, however, continue to be used to store unencrypted personal data, as well as sensitive corporate information. The ease with which deleted data on such devices can be recovered increases their attractiveness to criminals.

Career opportunities in cyber security exist in both the public and private job sectors. The U.S. Bureau of Labor Statistics projects that the number of Cyber Forensics Investigators, to include mobile forensics, will grow 22% from 2008 to 2018 in the public sector. In the private sector, the overall employment of Computer and Mobile Security Specialists is expected to grow by 30% from 2008 to 2018 (Bureau of Labor Statistics, 2016). Additionally, it has been projected that approximately 286,600 new Computer Security Specialists, to include mobile security specialists, will be added over the same 10-year period. Growth in both sectors is considered by the Bureau of Labor Statistics to be much faster than the average for all occupations.

A CompTIA (2013) survey of 198 IT business executives showed that 44% of executives reported a skills gap in mobile security within their organizations. When rating their IT staff, 36% of these executives described their staff as "moderately deficient" in security expertise. The results of the study are further underscored by Stewart Tan (Vice President of Information Risk Management and Security at Accretive Solutions), who noted to InfoWorld, "Mobile is the biggest factor changing IT right now. Building mobile apps, architecting mobile strategies, and securing those devices are the top concerns facing the enterprise today" (Strohmeyer, 2011). The same InfoWorld study listed *Mobile Technology Expert* as the number four "hot" IT job. It is increasingly important today for corporations to have the expertise to deal with mobile security issues, such as lost and stolen devices, mobile "phishing," mobile malware, and violations of corporate data policies. There is a clear trend showing that the need for IT professionals with expertise in the areas of mobile forensics and security is growing.

Fischer, Kuo, and Huang (2012), discuss three shifts in mobile device security: mobility, device sensors, and constant connectivity. Increased mobility has created confusion and risk regarding mobile device surroundings, in particular on Wi-Fi networks. Wi-Fi can be secured or unsecured. Using public Wi-Fi at an airport or restaurant is an example of an unsecured network, while corporate networks are typically secure. Mobile device users must have an awareness of how and where they are connecting to Wi-Fi to mitigate threats from attacks targeted at unsecured networks. The second shift noted in mobile device security is related to the sensors that are installed on most modern mobile devices. These include GPS for location tracking, cameras, Bluetooth for connectivity to other devices, Radio Frequency Identification (RFID), and Near Field Communication (NFC) which is often used for mobile payments. The automatic installation of sensors on mobile devices has led to a new area for infiltration and attack. The third shift in mobile security is the concept of constant connectivity. Mobile devices have constant access to the Internet, and mobile device users tend to carry their devices with them at all times. This is also attractive to cyber criminals, as it provides for more opportunities for attacks by making it easier to locate potential targets. A cyber criminal often must only be sitting or walking near the potential target who is using his or her mobile device. This has many implications for public spaces including retail stores, airports, buses, restaurants, parks, etc.

3. MOBILE FORENSICS AND SECURITY CERTIFICATE

In the world of security, half of the battle is a good prevention strategy. While all types of attacks to mobile technology cannot be anticipated, businesses need to have policies and infrastructure in place to best prepare their organizations for mobile security incidents. This certificate will critically address these concerns, covering mobile forensics, the life cycle of cyber and mobile security policy development, and infrastructure solutions such as mobile device management (MDM) and mobile application management (MAM) that can aid an enterprise in managing the mobile devices of employees. Students will learn about the different types of policy frameworks, policy writing, and challenges to implementing and enforcing security policies. This certificate will also address a variety of mobile security-related topics including risks, threats, and mitigation strategies for the mobile ecosystem.

This certificate will address mobile security topics that are currently lacking in higher education, filling a serious gap in cyber security education. Educating students on mobile security threats, mobile forensics and the need for cyber and mobile security policies will prepare them for jobs related to cyber security such as forensic examiner, exploitation analyst, security analyst, or information security officer.

The new Mobile Forensics and Security Certificate is designed for students to be able to complete in one year. Students who complete the certificate will be immediately employable, or they can continue the program to earn a B.S. in Cyber Forensics and Information Security, Computer Information Systems, or Information Sciences within the University. As of September 2016, it is determined that five institutions within the Tri-State area of Robert Morris University offer either an Associates degrees in Computer Forensics or Information Security. Bachelor's and Master's granting institutions in the area offer either a degree in Cyber Security or a degree in Computer Forensics, but none, other than Robert Morris University, offer a combined degree with Cyber Forensics and Information/Cyber Security. Implementing a certificate in Mobile Forensics and Security will help the region train professionals in an under-represented area of security.

The Mobile Forensics and Security Certificate will consist of seven courses. Students enrolled in the certificate will need to take the four required courses and will then choose three electives from a list of five courses. Note that one of the required courses, Introduction to Decision Support Systems, is required for all students at the university. However, this course can be waived upon admission to the certificate program if the applicant has taken a comparable course elsewhere or has comparable business experience. Eight of the nine courses needed are currently being taught as part of the Cyber Forensics and Information Security degree.

Required Courses

- Introduction to Decision Support Systems
- Cyber and Mobile Security Policy and Management
- Introduction to Computer Forensics
- Mobile Forensics

Elective Courses

- Digital Evidence Analysis
- Cyberlaw
- IT Security, Control and Assurance
- Computer and Network Security
- Network Forensics

Program Outcomes

1) Demonstrate the use of various computer and mobile forensics software tools and techniques, as well as, follow proper legal procedures for obtaining, analyzing, and reporting digital forensics evidence from computers and mobile phones
2) Properly report findings of a cyber/mobile investigation in both written form (using proper grammar, writing style, and citation) and in oral form (i.e. within the context of a trial, hearing, or deposition
3) Identify and analyze legal issues within technology, such as; online contracts, computer crime, fraud, privacy, defamation, hate speech, indecency, obscenity, cyber-squatting, and intellectual property
4) Demonstrate various techniques for preventing unauthorized attacks to computer networks and mobile devices and apply measures for minimizing the damage caused by intruders

4. CONCLUSION

In summary, this paper has presented a way to expand the knowledge of cyber security by adding a mobile security component. As of July 2016, mobile forensics and security is an underrepresented area of cyber security. In order to help fill the need for trained experts in the field, universities need to start teaching courses around the growing dependence of mobile technology.

The material in this paper is based upon work supported by the National Science Foundation under Grant #1515256. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

5. REFERENCES

Felt, A.P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices,* ACM, 3-14. Retrieved from http://www.cs.berkeley.edu/-daw/papers/mobilemal-spsm11.pdf

Fischer, I., Juo, C., & Huang, L. (2012). Short Paper: Smartphones: Not smart enough? *SPSM'12*, October 19, 2012, Raleigh North Carlolina. Retrieved on June 29, 2016 from http://www2.berkeley.intel-research.net/-hling/research/spsm12.pdf

Fox, S., & Duggan, M. (2012). Mobile Health 2012. Pew Research Internet Project. Retrieved from http://www.pewinternet.org/2012/11/08/mobile-health-2012/

Frost & Sullivan, (2013). The many shades of mobile app risk: Understanding and mitigating mobile threats effectively. Retrieved from http://www.brightcloud.com/pdf/MobileSecurity-Webroot_20131021110609-43358.pdf

LaPolla, M., Martinelli, F., & Sgandura, D. (2013). A survey on security for mobile devices. IEEE Communications Surveys and Tutorials, 15(1), 446-471.

Leavitt, N. (2011). Mobile security. Finally a serious problem? *Computer, 44(6),* 11-14 Retrieved from http://www.leavcom/com/pdf/Mobilesecurity.pdf

Poushter, J. (2016). Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. Pew Research Center. Retrieved from http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

Strohmeyer, R. (2011). 5 location tracking rights you should demand. *Information Week,* Retrieved from http://www.informationweek.com/mobile/mobile-devices/5-location-tracking-rights-you-should-demand/d/d-id/1099939

Symantec. (2016). 2016 Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center/threat-report

Trends 2016. (2016). Trends in Security Everywhere. Retrieved from http://www.welivesecurity.com/wp-content/uploads/2016/01/eset-trends-2016-insecurity-everywhere.pdf

U.S. Department of Labor Statistics, (2016). Economic Releases. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm