Issues in Information Systems
Volume 18, Issue 1, pp. 173 -179, 2017

IMPLEMENTING A SUCCESSFUL TRAIN-THE-TRAINER PROGRAM IN MOBILE FORENSICS AND SECURITY

Karen Paullet, Robert Morris University, paullet@rmu.edu
Jamie Pinchot, Robert Morris University, pinchot@rmu.edu
Sushma Mishra, Robert Morris University, mishra@rmu.edu

ABSTRACT

Mobile forensics and security skills pose a serious gap in cybersecurity education. The surge in the use and reliance on mobile technology, combined with the scarcity of programs that prepare students and educators in this area needs to be addressed. Implementing a train-the-trainer program on mobile forensics and security, where skilled faculty can train other faculty across the country, can assist in expanding the knowledge. The training would provide faculty the skills to implement mobile forensics and security into their existing cybersecurity or information technology programs.

Keywords: mobile forensics, mobile security, information technology, train-the-trainer

INTRODUCTION

The implementation of a train-the-trainer program on mobile forensics and security can provide educators an opportunity to learn industry needed skills which can then be taken back to their institutions to apply into their existing cybersecurity and information technology programs. Mobile security topics are lacking in higher education when mobile security remains a top concern for businesses. Mobile devices have become essential to daily activities. Cybersecurity has become a major focus for higher education institutions, yet the area of mobile security is a major challenge (Gordon, 2015). Mobile devices, including smart phones, GPS, tablets, e-Readers, IoT devices and the cloud have become a target for data theft and security breaches. As people continue to rely on mobile technology, the need for trained professionals on mobile forensics and security become a priority. Mobile security encompasses a variety of things including protection from physical device theft and unauthorized device access to hacking, data theft, system access threats, and identity theft .Mobile forensics is the use of computer software to search the contents of a mobile device for evidence. This is typically done by law enforcement but can also be a tool used by organizations for monitoring employee devices. (Al-Hadadi, et. al., 2013).

Implementing a Mobile Forensics and Security Train-the-trainer Program

The researchers implemented a Mobile Forensics and Security train-the-trainer program at Robert Morris University as part of a National Science Foundation Grant #1515256 where faculty from approximately 20 institutions were trained as of May 2017. The training has made a broader impact in the area of mobile forensics by educating those teaching in the field of cybersecurity or information systems. When faculty can implement needed skills into their curriculum, it will increase the number of students achieving the credentials, which can then prepare them for careers in mobile forensics and security. The goal of this program is to enhance the cybersecurity educational community's capacity to train specialists in mobile forensics and security.

Success of train-the-trainer programs

Train-the-trainer programs have proven to be powerful in creating new ways of disseminating innovative knowledge in academia and the workforce (Corelli et al, 2007). The impact of training educators in higher education has been documented to be effective and well received. New curricular ideas can be encouraged for widespread adoption by providing appropriate training for faculty members of relevant disciplines and ensuring adequate resources in form of content knowledge to increase the confidence of participants. This is a common approach in higher education to increase adoption of relatively newer topics in various disciplines.

Higher education uses train-the-trainer programs for equipping faculty with resources but there is a lack of such programs in mobile forensics and security domain. Studies in other disciplines document the importance of such programs for infusion of new content in classrooms. Masamichi (2013) argues that train-the-trainer programs is an effective tool in engaging experts in the area to start a meaningful dialogue that leads to further adoption of the content in mainstream curriculum in higher education.

In a train-the-trainer program in pharmacogenomics, faculty members who participated reported increased confidence in teaching those topics to their students. A number of participants also indicated high willingness to adopt the particular program at their home institution (Lee et al, 2012). Corelli et al (2007), in an national train-the- trainer program on perception of Rx for change tobacco cessation program, found that participants self-rated ability to teach the content of the training program increased significantly. The training material was viewed highly compatible for integration in curricula. The study concluded that participation in such a training program increased faculty members' perceived ability to teach related courses and the participants indicated high likelihood of adopting such program in their schools.

Moss (1997) identifies success factors for good train-the-trainer programs. This study is in health care context of an advanced trauma life support program but the learnings and experiences are applicable to variety of training-the-trainer programs. The factors are: *training manual quality* (trainer should have mastery over the domain area and great documentation to support the training), *ongoing mentorship during the training period* (requires high degree of interaction between trainees and trainers), *interactive learning modules* (keeps the attention of trainees on the topic), *self and peer group critique* (helps in learning the training material), *problem based learning strategies* (emphasizes learn by doing philosophy), *support of training staff* (helps is retaining the material), *continuous assessment of the program* (measuring the performance of trainees objectively) and *educational input in working manner* (presenting underlying theoretical concepts in interactive way).

Before preparing content for a train-the-trainer program it is imperative to define the audience and the expectations and outcomes of the training. In doing so, participant needs must be taken into consideration for success. The goals of the course, along with a clear set of objectives should be well-defined so that it will attract the proper audience for the training. The big question that needs to be answered is "what do we hope to accomplish with the training" (Solter, et.al. 2007)? The items below need to be determined for successful training:

- Assess the need for the training
- Planning and development of the training
- Objectives of the training course
- Develop content for the course
- Identify participants
- Pre-Test the knowledge of those being trained
- Implementation of the training
- Evaluation of the training
- Post-Test the knowledge after the training
- Analyze the pre and post-tests to gauge the knowledge learned from the training and identify areas of improvement
- Training follow-up to see if the trainers are implementing the new skills

IDENTIFYING THE NEED FOR MOBILE FORENSICS AND SECURITY TRAINING

Security issues surrounding the mobile environment are becoming more prevalent. Mobile payment services, terrorism, such as the San Bernandino, CA and Paris incidents, the rise in mobile web browser hacking, remote eavesdropping and highjacking of information, mobile DDos attacks, mobile malware and the Internet of Things are some of the issues surrounding the mobile environment (Hong, 2015). Companies are now permitting employees to Bring Their Own Device (BYOD) to make it convenient for employees and cost effective for the companies have also added to the area of concern for protecting company assets. Additionally, with healthcare going mobile there are severe vulnerabilities with Internet connected medical devices (RSA, 2016). These, among other reasons, have led to mobile becoming a valuable target for cybercriminals.

A Pew Research Center 2015 study on Technology Device Ownership states that smartphone ownership is nearing its saturation point with approximately 86% of the population of groups of people between the ages of 18-29 and 83% of people between the ages of 30-49 owning smart phones (Anderson, 2015). Smart phone usage might be facing its saturation point, but connected "things" such as the use of fit bits, smart TV's, smart homes, Internet, Wi-Fi, Bluetooth connected cars, smart cities, etc, is up 31% in 2017 from the previous year (Gartner, 2017). Gartner, Inc. (2017) forecasts 8.4 billion connected things will be in use worldwide by the end of 2017 with Greater China, North America and Western Europe representing 67% of the world number. The inter-connectivity of devices is part of the mobile platform and mobile security. With the excessive use in mobile technology comes the need for trained practitioners in the field of mobile.

Career opportunities in mobile forensics and security exist in both the public and private sectors. The U.S. Bureau of Labor Statistics projects the number of security professionals to increase at a rate of 18% per year until the year 2024. Additionally, it has been projected that approximately 286,600 new Computer and Cyber Security Specialists, to include mobile security specialists, will be added to the same time period. Growth in the field is considered by the Bureau of Labor Statistics to be much faster than the average for all occupations (Bureau of Labor, 2017).

MOBILE FORENSICS AND SECURITY TRAINING

Topics to Address in Mobile Forensics and Security Training

The train-the-trainer program took place at Robert Morris University in July 2016. Faculty attending the training were taught hands on in a lab using Paraben's Device Seizure which is a tool used to analyze mobile technologies such as smart and cell phones, GPS devices, tablets, and wearables to name a few. Having been set the task of training faculty members to teach in the areas of mobile forensics and security, the researchers considered the topics that should addressed. The training focused on the following topics:

- Why teach mobile forensics and security?
- The Evolution of Mobile Forensics
- Types of Phones and their Features
- Evidentiary Procedures for Handling and Storing Mobile Devices
- Mobile Security Overview
- Mobile Security Policy
- Introduction to a Mobile Forensics Software Package
- Legal Concerns for Teaching Faculty Mobile Forensics

The researchers feel that any learning session should begin with the students' understanding of the importance of the subject matter. Therefore, the training began with a short segment describing the importance of mobile forensics and security and the need for additional trained professionals entering the workforce in these areas.

The Evolution of Mobile Forensics

In order to better understand something, it can be helpful to know its origins. The training covered a short history of computer crime and the need for computer forensics to gain evidence in crimes where a computer was utilized. Due to increased use of computers and the Internet, computer forensics was often needed. The researchers then described how mobile forensics has become an area of priority in order to meet the demands of modern law enforcement. Police officers and other agencies deal with a variety of crimes on a daily basis, and most of those crimes now include mobile device evidence. Due to the rapid rise in smartphone usage, it is rare in 2017 for an individual not to carry a phone with them at all times. Because of this simple fact, most people who commit crimes are carrying mobile devices. These devices often need to be searched for evidence. This issue is becoming a serious problem for law enforcement agencies across the United States, as many departments are understaffed to handle these types of investigations and thus have a backlog of mobile devices waiting to be analyzed (Spurr, 2016) .

Types of Phones and their Features

The researchers devoted some time to discussing the different types of mobile devices that are in use today. In 2017, the major smartphone platforms are Android and Apple iOS. Other platforms include Windows Phone and BlackBerry. Android, iOS, and Windows Phone can run on both smartphones and tablet devices. While most attendees at the training were aware of the types of devices that are in use today, many admitted that they were familiar with only one or two platforms. The training covered the device models and general feature sets of each platform. When performing mobile forensics on a device, the investigator must be familiar enough with the features of the phone to adjust settings, disable security features, and navigate the phone interface without error. The ability to do so effectively can be a critical skill for a mobile forensics investigator. If a phone is mishandled, even due to user confusion, it could legally invalidate any findings. One exercise that the researchers implemented was to have faculty switch phones in the classroom and show each other the main interface and settings sections of their phones. So, for instance, faculty with iPhones running iOS would switch with faculty running Android. This gave the faculty a realization of how comfortable they were using their own preferred type of device and, perhaps, an understanding of what they need to know about other types of devices that they are not as familiar with.

In addition to modern smartphones, the researchers stressed that it is not good enough for mobile forensics investigators to just be familiar with the latest model phones. In fact, many crimes include the use of feature phones rather than smartphones. Feature phones are phones that have limited connectivity to the Internet but can call and send text messages (Klingebiel, et. al, 2015). Flip phones and "burner" phones that can be bought at a store and activated without a full data plan are both types of feature phones. Mobile forensics investigators need to be as familiar with these types of phones as possible as well.

Evidentiary Procedures for Handling and Storing Mobile Devices

The next part of the training covered the basics of following procedures for safely handling and storing mobile devices. How an investigator interacts with a device is extremely important for evidentiary purposes. An investigator must ensure that the cellular signal to the device is blocked immediately, so that no additional data can be sent or received on the device. Faraday technology is one of the most common techniques used to block a signal from a mobile device. Most often a Faraday bag is used to isolate the mobile device to ensure that it cannot connect remotely (Katz, 2010). All activities that are part of the investigation must be logged and recorded in an investigation report.

Mobile Security Overview

The training gave a general overview of mobile security topics including unauthorized data access or physical loss of a device, data theft threats, and system access threats. Many types of threats that are typical for wireless networks also apply to mobile devices. These topics were reviewed. Time was also spent discussing topics that are particular to mobile devices. For instance, a mobile device is often hacked in order to gain access to another application (perhaps a company VPN or other internal app). A system access or data theft threat like this is a critical concern for many organizations that allow their employees to access organization data or apps from a mobile device. If an employee uses his or her own mobile device for this access, it is considered a Bring Your Own Device (BYOD) model that is used by the organization. BYOD can bring many security risks to an organization. Risk management for BYOD usually involves Mobile Device Management (MDM) and Mobile Application Management (MAM) software to help control the mobile environment at the organization (Barthwal, D. 2016**).** All of these topics were covered in detail.

Mobile Security Policy

Policy is an extremely important topic in mobile security. With the plethora of Internet-enabled mobile devices that may have access into an organization's data or apps, it is critical that an organization set policy to control use of mobile devices. It is also critical that they enforce the policy.

Introduction to a Mobile Forensics Software Package

The largest part of the training was spent giving the faculty hands-on experience with Paraben's mobile forensics software package. The faculty completed ten hands-on lab assignments during the training. They learned how to physically connect a smartphone to the computer and acquire an image from it, as well as how to sort and search for

evidence within the image. While the mechanics of the software were taught, the researchers also worked to instill a sense of how to "think like an investigator" while searching for evidence. Forensics can be a tedious and frustrating field. Often, you may search through gigabytes of data looking to find anything at all related to a crime or situation. Faculty got the chance to experience this through the labs that they completed. The labs all asked faculty to find specific pieces of information on the phone image. This was met with varying levels of success. At the end of the training, faculty was asked to take a practical exam. On this exam, faculty were given a scenario and a phone image to search, but no specific questions! This shocked many of the faculty because they realized what it would be like for a real investigator who has only limited knowledge and has to search through the entire contents of a phone to try to find anything that might be related with very little guidance.

The training also covered techniques for taking notes within the image and generating reports that highlight the evidence found. Faculty were also taught how to use the software to aid in detection of suspicious apps that might be installed on the phone.

Legal Concerns for Teaching Faculty Mobile Forensics

The researchers finished the training by talking about some true classroom experiences while teaching faculty mobile forensics and security. They noted that it is often necessary to have students sign an agreement that they will not use classroom forensics software or the skills learned with the class to conduct any unauthorized or illegal searches of phones.

Pre and Post Test Results

Prior to the start of the 5-day Mobile Forensics and Security train-the-trainer course faculty were given a pre-test. Upon completion of the 5-day Mobile Forensics and Security training course they received the post-test. Attendees were asked a total of 25 questions in regard to mobile forensics and security to include, True/False, Multiple Choice and Short Answer questions. A total of 21 people were in the training with all taking both the pre and post-tests. Of the 25 questions asked, participants did better in the post test on 23 of the questions. One question remained identical and one question was thrown out because it was not worded correct for the answer expected from the trainers. This increase in knowledge in regard to mobile forensics and security shows a positive outcome indicating that the faculty learned a significant skillset are prepared to take the lessons learned from the training back to their institutions to implement mobile forensics courses and to train additional faculty.

CONCLUSION

Mobile forensics is a fast growing area and there is a lack of relevant educational material or quality sources of reference for this domain. There is seemingly a gap between the need for skills in this area and knowledge centers proving such education and training. In this context, train-the-trainer program is suitable for wide scale of dissemination of knowledge in the area. Train-the-trainer is an effective dissemination strategy to equip faculty with necessary knowledge and training material to integrate provided content in their existing classroom courses (Lee et al, 2012). The training session, when provided with hands-on activities is more effective for the participants.

The implementation of the above training in mobile forensics and security has put new skills into the hands of faculty in a much needed area of security. Twenty academic institutions participated in the train-the-trainer program. After completion of the program, the faculty had achieved the skills to implement a course or add content on mobile forensics and security into their curriculum. A survey was conducted 6 months after the training to see if faculty had indeed implemented the skills learned in the training. Fourteen trained faculty responded to the survey in which thirteen out of fourteen implemented mobile forensics and security into their cyber security programs. Train-the-trainer programs work when a proper implementation of the training is put in place.

ACKNOWLEDGMENT

The material in this paper is based upon work supported by the National Science Foundation under Grant #1515256. Any opinion, 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.

REFERENCES

Al-Hadadi, M., & AlShidhini, A. (2013). Smartphone Forensics Analysis: A Case Study. *International Journal of Computer and Electrical Engineering, 5*(6), December 2013.

Anderson, M., (2015). *Technology Device Ownership: 2015*. Pew Research Center: Internet, Science and Tech. Retrieved on March 28, 2017 from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/

Barthwal, Diksha. (2016 July). *Mobile device management (MDM) in organizations*. ResearchGate. Retrieved on May 5, 2017 from https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations

Bureau of Labor Statistics (2017). Occupational employment statistics. Occupational employment and wages, May 2016. Retrieved on April 30, 2017 from https://www.bls.gov/oes/current/oes151122.htm

Corelli, R., Fenlon, C., Kroon, L. Prokhorov, A. & Hudmon, K. (2007). Evaluation of a train-the-trainer program for Tobacco cessation. *American Journal of Pharmaceutical Education, 71*(6).

Davis, N., Preston, C. & Sahin, I. (2009). Training teachers to use new technologies impacts multiple ecologies: Evidence from a national initiative. *British Journal of Educational Technology*; Coventry 40.5 (Sep 2009) 861-878.

Gartner. (2017 February). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Retrieved on April 25, 2017 from http://www.gartner.com/newsroom/id/3598917

Gordon, C.J. (2015). Addressing security risks for mobile devices: What higher education leaders should know. *Educational Administration; Thesis, Dissertations, and Students Research,* Paper 248. Retrieved on April 20, 2017 from http://digitalcommons.unl.edu/cehsedaddiss/248

Hong, M. (2015 December). The top 6 mobile security threats for 2016. Retrieved on April 2, 2017 from https://venturebeat.com/2015/12/27/the-top-6-mobile-security-threats-for-2016/

Katz, E. (2010). A field test of mobile phone shielding devices. College of Technology Masters Theses. Paper 33. Retrieved on April 29, 2017 from http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters

Klingebiel, R & Joseph, J. (2015). Entry timing and innovation in feature phones. *Strategic Management Journal. 1002-1020*

Lee, K., Ma, J., Hudmon, K. & Kuo, G. (2012). A train-the-trainer approach to a shared pharmacogenomics Curriculum for US colleges and schools of pharmacy. *American Journal of Pharmaceutical Education 76*(10), Article 193

Masamichi, M., Judi, S. Nariyoshi, S. & Whitby, S. (2013). Implementing biosecurity education: Approaches, Resources and programmes. SciEng Ethics 19, 1476-1486

Moss, G. (1997). Effective training of trainers: The ATLS approach, education & training; 39(4/5), ProQuest Central, p. 168

"Protecting Against the Top Mobile Security Threats in 2016" (2016). RSA Conference. Retrieved on April 3, 2017 from https://www.rsaconference.com/blogs/protecting-against-the-top-mobile-security-threats-in-2016

Solter, C., Duc, P., & Engelbrech, S. (2007). *Trainers guide: Advanced training of trainers.* Pathfinder International, Watertown, MA

Spur, K. (2016 March). Waiting game: Law enforcement faces backlog in searching technology. Retrieved on May from http://www.dailyastorian.com/Local_News/20160318/waiting-game-law-enforcement-faces-backlog-in-searching-technology