THE FUTURE OF DIGITAL FORENSICS

Young B. Choi, Regent University, USA (ychoi@regent.edu)

Ronald Stamm, Regent University, USA (ronasta@mail.regent.edu)

ABSTRACT

The IT industry in an ever-changing landscape and now digital crimes continue to rise with many people falling prey to ransomware, corporate spearfishing and whaling exploits, mobile devices, and theft of sensitive private data. Digital forensics analysis is still in its' beginning changes, but that will all change very quickly in the next 10 years and beyond, digital forensics will become almost as commonplace as traditional crime scene investigation. This paper will examine the current landscape of digital forensics and identify shortfalls and hindrances in this field of investigatory work. This paper will also look into the future of digital forensics in areas such as Digital Forensics as a Service (DFaaS), how to conduct investigations in the cloud, automation, artificial intelligence, and various tools that will become available to this field in the future.

Keywords: digital forensics, DFaaS, breach, acquisition, investigation

INTRODUCTION

On Black Friday of 2013, the beloved store Target was the victim of a data breach. Over the next month, unbeknownst to Target, upwards of 70 million customers had their personal information compromised. According to the Senate Committee on Commerce, Science, and Transportation, Target inadvertently gave internal network access to a third-party HVAC vendor, and those credentials were stolen. These credentials allowed the attackers to move "...from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets" (2014). This data was stolen via emails infected with malware. It was reported that costs associated with the data breach "...topped $200 million, a report from the Consumer Bankers Association and Credit Union National Association finds, " (Clark, 2014) for things such as purchasing identity theft protection for its' customers, laying off employees, public relations, and recovering public trust. The target breach was one of the more prominent times in the United States that digital forensics was discussed on a broader scale. This massive data breach brought to light the fact that we rely so much on technology and that we must safeguard our personally identifiable information (PII). When we cannot do this, the importance of digital forensics to bring those who would seek to harm us to justice. Without tools such as what was used after the Target breach, investigators might have never known how the breach occurred and what to do to prevent it from happening again in the future.

New technologies emerge all the time in this innovative world of technological wonders. These technologies come in the form of the data-on-demand ability of cloud technologies, the convenience of mobile platforms, the promising future of artificial intelligence, and even the amazing and awesome use of automation technology in motor vehicles. While these technologies are amazing in their own right, they unfortunately come with their own unique challenges as it relates to digital forensics. This research paper is about the challenges of these technologies as they become more prevalent in the future.

CLOUD TECHNOLOGIES

Cloud technology has come a long way from when it was first introduced with the Amazon Mechanical Turk back in 2002. The cloud has since become a more inexpensive (in terms of equipment and operating costs) and efficient way to store a company's data and manage various applications that they may need as part of their functionality. This technology is a great tool for businesses, but it presents its' own challenges.

One such challenge it that the physical locations of the data can vary, and can even be housed in a completely different country. According to Damshenas (et al.), cloud data can be "...saved in different locations, [with] limited access to obtain evidences from cloud and even the issue of seizing the physical evidence for the sake of integrity validation or evidence presentation" (2012). This creates an issue because the data that resides in the cloud, while able to be accessed from most anywhere, might actually by physically located in a different country such as Australia or even India, which have different laws governing digital forensics than the United States does. This also can exponentially increase the workload that digital forensics investigators have, because "...discovery and acquisition of digital evidence from remote, elastic, provider-controlled Cloud platforms differs considerably from the discovery and acquisition of digital evidence from local suspect devices such as Laptops, PCs and Servers" (Plunkett, Le-Khac, & Kechadi, 2015).

Another issue facing the cloud is that it can be accessed from anywhere. With mobile devices becoming more prevalent, and being used to access cloud environments, it becomes increasingly more difficult to pinpoint the device and other hardware that a forensics investigator would need to access in order to obtain forensic images and investigate any physical devices.

To fight the issues of extreme backlog investigators face when conducting cloud forensics investigations, developed by the Netherlands Forensics Institute in 2010, is called Digital Forensics as a Service (DFaaS). The DFaaS platform leverages the power of the cloud, "...enabling detectives to directly query the data, improving the turnaround time between forming a hypothesis in an investigation, its confirmation based on the evidence, and facilitating easier collaboration between detectives working on the same case" (Lillis et al., 2016).

Encryption of data within the cloud presents its' own challenges as well. A digital forensics investigator would need the cooperation of the data owner, or if the Service Level Agreement allowed it, the Cloud Service Provider in order to decrypt the data so that a forensic analysis could even being to be conducted. If a malicious entity encrypted files in the cloud as part of the crime they committed, an investigator would need to either brute force the encryption on the files, or somehow figure out if there is a decryption mechanism for the files. This could prove a bit easier is the perpetrator were caught and had the desire to be cooperative.

On the back end as well, much of the data in the cloud at some point in processing is unencrypted and thus vulnerable to outside malicious activities. According to Sengupta, Kaulgud, and Sharma, one possible solution is called Information Centric Security (ICS). A proposed solution is the use of "…Policy based or Role based access controls which can be defined in a language like Extensible Access Control Markup Language (XACML) which governs context-based access rules in policy enforcement point of the data" (2011). Having the ability to actually inspect the data from the inside can provide a much more powerful security tool giving clients peace of mind when it comes to the security of their data in the cloud.

MOBILE PLATFORMS

On December 2, 2015, Syed Rizwan Farook killed 14 people and injured 22 others in a terrorist attack in San Bernadino, California. He was later killed in a shootout with police. As the investigation progressed, his iPhone 5c became a national topic of controversy as FBI digital forensics investigators made attempts to access the data on this device. In an attempt to gain access to iCloud backups online, forensics investigators reset the iCloud password. According to the National Institute of Standards and Technology (NIST), "incorrect procedures or improper handling of a mobile device during seizure may cause loss of digital data" (2015, p. 27). This slip in judgment, whether it was directed from a more senior official or due to the lack of knowledge on the part of the forensics investigator, "...likely prevented the iPhone from doing an auto-backup, which could have yielded useful information about Farook's activity leading up to the shooting" (Heath, 2016). The following statement was issued by the FBI to justify these actions and place the blame back on Apple for not cooperating in the first place.

Through previous testing, we know that direct data extraction from an iOS device often provides more data than an iCloud backup contains. Even if the password had not been changed and Apple could have turned on the auto-backup and loaded it to the cloud, there might be information on the phone that would not be accessible without Apple's assistance as required by the All Writs Act Order, since the iCloud backup does not contain everything on an iPhone.

This lack of forethought underscores an important issue when it comes to new technologies such as smart phones. These devices are essentially tiny computers according to NIST, which states, "...while personal computers may differ from mobile devices from a hardware and software perspective, their functionality has become increasingly similar" (2015, p.15). Care must be taken when dealing with these devices or the consequences could be disastrous.

Another issue with mobile devices is remote data wiping. This is a security feature built into most smart phones that allows a user to send a text or log into a website and then remotely erase all personal data from a phone, rendering it back to a factory state. While this is great for the end user, this can prove to be an issue for a forensics investigator attempting to conduct an investigation on a smart phone. Some potential solutions to this issue include, turning the phone off and removing the battery, placing the phone in "airplane mode," or, to make sure little to no radio frequencies can reach the phone but it can remain on, place it into a Faraday cage. These solutions have their drawbacks, however. A powered off device may ask for an authentication code or fingerprint when turned back on. A phone in "airplane mode" still has its' GPS enabled. A Faraday cage eliminates most radio frequency signals from reaching the phone, but the "...risk of improperly sealing the Faraday container (e.g., bag improperly sealed, exposed cables connected to the forensic workstation may act as an antenna) and unknowingly allowing access to the cell network" (NIST, 2015, p. 29) is a potential issue.

Another potential issue when it comes to smart phones is that there are just too many of them. According to forensics professionals, "there are more than 10,000 models of mobile phones being used today from as many as 3,000 manufacturers" (Jackson, 2014). Because of these variances in smart phones, each one will not fit into the functionality of mobile device digital forensics programs. Many devices will on some level have the same basic characteristics (i.e.: volatile and non-volatile memory, screens for performing physical acquisition, etc.) and, given the right cable, forensics programs should be able to perform logical acquisitions on many of those devices.

As far as extraction goes, NIST has outlines five different methods. Manual extraction is simply looking at the screen and seeing what the investigator can access by navigating through the phone and then taking pictures to document what is found. This of course becomes a challenge if there is a passcode on the phone of the screen is broken. The next method is logical extraction. After successfully connecting the device to a forensics workstation and using a program such as Oxygen Forensics, "...sending a series of commands over the established interface from the computer to the mobile device" (NIST, 2015, p.17). Once the connection is established, the device sends information back to the program and an image of the contents of the phone is taken. This will allow the investigator to interact with the data on the image and leave the original evidence on the mobile device intact.

The next methods, Hex dumping and Joint Test Action Group (JTAG), allow the examiner to access data stored in the flash memory of the device. Hex dumping involves loading a "...modified boot loader (or other software) into a protected area of memory" (p.18). The device in then placed in a diagnostic mode by the forensics program and then captures the data that resides in flash memory and send it over to the forensics computer. The JTAG method of extraction works much the same way, but interfaces specifically with devices that follow that form factor.

The next method, chip-off, involves accessing the devices memory chip directly by physically removing it and making a clone of it. This is most likely one of the methods that was used with Syed Farook's iPhone 5c. The flash memory is cloned to another physical flash memory device and then a brute force attack is continuously performed on the cloned flash memory. In Farook's case, since he had a 4 digit passcode, "which would result in 10,000 permutations, a low enough number to be possible to brute force" (MrTopStep, 2016), but a number that would have been high enough to take at least 2 weeks to conduct this type of acquisition.

The final method of mobile device extraction, micro read, involves a very expensive and expert-level analysis that "...looks at [NAND and NOR] logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media" (Nelson, 2016, p.467). This method is typically used in matters involving national security when all other acquisition methods have been exhausted. According to NIST, no government agency is using this method and there are no commercially available Micro Read tools (NIST, 2015, p.20).

Mobile device forensics is an ever-changing landscape and, as technology progresses, new forensics tools must be created to meet new demands. The future on smart phone could be that there aren't any, and that these devices are actually a part of what is affectionately referred to as "wearable technology," involving contact lenses that are the cell phone screen and a chip implanted into one's wrist that houses the entire phone hardware and storage. Access

would be via a wireless-only connection. All of these major changes are leaps and bound from what current digital forensics tools can handle. Innovation, however, breeds more innovation.

Robots and Artificial Intelligence

Robots have become more or less a part of our society at this point. They assemble our cars and do other things at manufacturing plants, they zoom around our houses like a little dog following behind to clean up after us, they even make us yogurt in the mall. Robots are a part of our everyday lives as much as our morning cup of coffee. They help us, and that is a good thing. What happens then when a robot goes awry and ends up causing damage of even hurting a human? In this event a forensic investigation must take place. These investigations would be much like conducting an investigation on a computer, just on a different scale. An investigator would isolate the robot, take an image of its code, and then bring that code to the lab for investigation. The big difference here would be that, since this code is most likely proprietary, and investigator would most likely need to outsource to the manufacturer or other expert for assistance in parsing through the code for either an error or for some sort of malicious activity. According to Ryan Calo (2015), a law professor at the University of Washington, "...robots run on code, anticipating and accounting for robot behavior represents at least as difficult a task as accounting for user behavior in the context of personal computers or smartphones" (p. 534). The point here is that the code behind the robots is actually the issue and not the robots themselves. Since robots cannot actually think for themselves, all they can do is what their code tells them to do.

Artificial intelligence (AI) has been gaining more attention lately. Differing from robots, artificial intelligence is actually programmed to make decisions based on environmental factors around it. These decisions can range from a smart refrigerator refilling the ice in a freezer to a driverless car swerving to avoid a car but then running another car off the road killing an entire family. In that extreme case, which is very possible with the advent of driverless and other autonomous care like the Tesla. In May of 2016, man was driving his Tesla using the Autopilot system when a semi-truck with a white trailer turned left across the lane the Tesla was in. Neither the driver nor the Autopilot system applied the brakes, causing the Tesla to collide with the truck killing the driver instantly. There was an investigation by the National Highway Traffic Safety Administration (NHTSA), which concluded that "...although Autopilot did not prevent the accident, the system performed as it was designed and intended, and therefore did not have a defect" (Boudette, 2017). It can be speculated that this investigation most likely involved some sort of digital forensics aspect where the NHTSA, working with Tesla software coders as experts, reviewed the code that would have been applicable in that specific circumstance. It can also be speculated that this investigation occurred much the same as it would with any other piece of software. The difference here would be a legal one. Since the car's Autopilot software did not make the decision to apply the brakes is the car responsible for the driver's death or is there not a case because the car was not programmed to make the type of decision required for this unique circumstance? The NHTSA, as stated above, determined that the Autopilot system was operating as designed when this accident occurred and therefore the driver was actually to blame for the accident due to his inattention to his surroundings, which he unfortunately paid the ultimate price for.

CONCLUSION

Technology has made leaps and bounds in the past 10 years and will continue to exponentially increase beyond our wildest thoughts and dreams as time progresses. Whether it be an email containing a virus on an unsuspecting user's computer, or an artificial intelligence that can nearly mimic human thoughts and behaviors to the point of hurting someone, digital forensics will always have a place in this world. It will take innovative minds teeming with creative solutions to tackle the forensics issues that technology will cause us to face in the future. It is up to the current generation to help pave the way for them. As the Word of God says in Proverbs 19:20, "Listen to advice and accept instruction, that you may gain wisdom in the future" (ESV).

REFERENCES

Boudette, N. E. (2017, January 19). Tesla's Self-Driving System Cleared in Deadly Crash. Retrieved from https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html

Calo, R. (2015, May 13). Robotics and the Lessons of Cyberlaw. Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=852002002112007098072109028084122071121046022072028063018098016109094021067124113096001012057097017112026090000016073066125021021001010026044027019085014067086097029038073022104000088020023102067107114095096027116095075080098072070029006008083071098098&EXT=pdf

Clark, M. (2015, December 05). Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer. Retrieved from http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

Committee on Commerce, Science, and Transportation. (2014, March 26). A "Kill Chain" Analysis of the 2013 Target Data Breach. Retrieved July 22, 2017, from https://www.omegasecure.com/wp-content/uploads/2016/03/Target_Kill_Chain_Analysis_FINAL-1.pdf

Damshenas, M., Dehghantanha, A., Mahmoud, R., & bin Shamsuddin, S. (2012). Forensics investigation challenges in cloud computing environments. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE. https://doi.org/10.1109/cybersec.2012.6246092

Heath, A. (2016, February 21). The FBI confirmed it screwed up and reset the San Bernardino shooter's iCloud password. Retrieved from http://www.businessinsider.com/fbi-confirms-shooters-icloud-password-reset-2016-2

Jackson, W. (2014, June 16). Can Digital Forensics Keep up With Smartphone Tech? Retrieved from https://gcn.com/articles/2014/06/16/forensics-technology-race.aspx

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016, April 13). Current Challenges and Future Research Areas for Digital Forensic Investigation [Scholarly project]. In Arxiv.org. Retrieved from https://arxiv.org/pdf/1604.03850.pdf

MrTopStep. (2016, March 23). Here's How the FBI Plans to Crack Terrorist's iPhone. Retrieved August 05, 2017, from https://mrtopstep.com/heres-how-the-fbi-plans-to-crack-terrorists-iphone/

Miller, G. (2017, June 03). The Moral Hazards and Legal Conundrums of Our Robot-Filled Future. Retrieved from https://www.wired.com/2014/07/moral-legal-hazards-robot-future/

Nelson, B. (2016). Guide to Computer Forensics and Investigations, 5th Edition. [CengageBrain Bookshelf]. Retrieved from https://cengagebrain.vitalsource.com/#/books/9781305176089/

Plunkett, J., Le-Khac, N., & Kechadi, M. (2015, January 26). Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement. Retrieved from https://www.insight-centre.org/sites/default/files/publications/16.013_ifip_cloud_forensics_plk.pdf