Mobile Device Espionage

Deborah Carstens, Ph.D., PMP[1]
John Mahlman, M.S.[1]
Jeffrey Miller, Ph.D.[2]
Matthew Shaffer, Ph.D.[2]
[1]*Florida Institute of Technology*
[2]*Oak Ridge Associated Universities*
carstens@fit.edu; jmahlman2016@my.fit.edu; jeff.miller@orau.org; matthew.shaffer@orau.org

Abstract

Malware and hacking activities are growing among today's most popular mobile devices. These security risks are prompting companies, federal facilities, and other institutions to enact policies aimed at mitigating the amount of espionage and illegal events that can transpire on a cell phone or other mobile device. With all of the new devices and applications, publicly available, new security-related vulnerabilities continue to arise. These devices and applications are targets for attacks from malicious outside sources. Each day provides a new potential threat aimed at taking advantage of some security exploit in cell phones and mobile devices. Security analysts and experts are at a disadvantage in this war against threats because they are fighting a war without clear rules. The focus of this literature review is on cell phone and electronic device vulnerabilities, espionage in the workplace, and security solutions. This will provide an understanding of risks, threats and solutions that exist in the modern era of cell phones and mobile devices.

1. Introduction

The purpose of this research is to provide a literature review on cell phone and electronic device vulnerabilities, espionage in the workplace, and security solutions. Cell phones and other mobile devices have become ubiquitous in everyday life. According to Jones and Chin (2015), the number of mobile devices, 7.22 billion, has surpassed the worlds' population of 7.19 billion. The number of application (app) downloads is also just as staggering. Tong and Yan (2017) suggest "mobile app downloads are expected to reach 224,801 billion in 2016" (p. 22). With all of the new devices and applications publicly available, new security-related vulnerabilities have arisen. Traditional personal computers are not the only electronic devices that can be hacked or infected with viruses. Cell phones and wearable mobile devices are vulnerable to being hacked and infected as well (Shaulov & Point, 2016). These devices and applications are targets for attacks from malicious outside sources. An example of one of these external sources is a virus application acting autonomously with the goal of making mobile devices inoperable from both a software and hardware level. Any internet-of-things device is a ubiquitous device with every user representing an enticing prospect for the would-be hacker or criminal (D'Orazio & Choo, 2017). Security firms are on the front line of fighting external and internal security threats, at home and from abroad. Security analysts and experts are at a disadvantage in this war against threats because they are fighting a war without clear rules. Attackers continuously create new and innovative exploits at a lightning pace, and this technology can only be anticipated to a certain degree (D'Orazio, Lu, Choo,

& Vasilakos, 2017; Shaulov & Point, 2016; Wilosinski, 2016). Security firms can only offer protection to its customers against exploits that are known and not necessarily emerging vulnerabilities. The focus of this literature review is to provide an overview of cell phone and electronic device vulnerabilities, espionage in the workplace, and security solutions.

2. Literature Review

2.1 Cell Phone and Electronic Device Vulnerabilities

This section addresses vulnerabilities to unsuspecting cell phone and electronic device users that have the potential for their device to be hacked. D'Orazio et al. (2017) suggest that mobile security issues are not just for a particular user but also users' internet infrastructure and place of business, making workplaces vulnerable for security infractions. For example, an employee at a nuclear power plant exercising poor security practices with their cell phone could result in their device functioning as a spy for a malignant organization, unbeknownst to the employee. Smartphones have been used before as spying devices (e.g., recording audio, GPS positions, etcetera), with the user utterly oblivious to the malicious activity transpiring (Wilosinski, 2016). This section will provide an overview of currently known, published cell phone vulnerabilities that exist within modern technology.

Research has shown that cell phone attacks can reside within one of four major domain areas (Bitton, Finkelshtein, Sidi, Puzis, Rokach, & Shabati, 2018). The first area is man-in-the-middle attacks (MiTM), that consists of hijacking, interceptions, and eavesdropping activities (Bransfield-Garth, 2010). The second area is a phishing attack that consists of fake websites, links, and other fraudulent pages to coax information out of victims. The third area includes application attacks comprised of Trojan applications and pop-ups. Lastly, weak authentication attacks, which consist of password cracking and/or an absence of or failure to utilize a device locking mechanism on a cellular phone (Bitton et al.; Shaulov & Point, 2016). These domain areas represent the currently known external cell phone vulnerability avenues.

Jones and Chin (2015) suggest that participants did not have appropriate smartphone security practices in place. They also suggest that participants were more likely to trust downloaded applications on their smartphone device, without question, and assume that nothing negative can come from such actions. This research coincides with research by Thompson, McGill, and Wang (2017), which suggests that users do not often understand the technology associated with these devices used daily and do not quite understand how to protect themselves adequately. In both of these studies by Jones and Chin (2015) and Thompson et al. (2017), participants' behaviors were risky and not focused on being security conscious. Examples of unsafe behavior included: not logging off potentially sensitive sites (e.g., email), opening unknown attachments, downloading unknown applications, and storing pins and passwords. The findings indicate that until users become more aware that security risks exist, they would continue to be cavalier in their actions (Jones & Chin, 2015). And while app stores purport to screen applications for malicious intent, these are not infallible processes. In early 2016, the security application Lookout reported over a dozen separate applications available for download that they identified as malicious, having snuck through Google's review process (Schiwy, 2016).

These previously identified risky behavior practices allow what Wilosinski (2016) refers to as social engineering to transpire. A simple example of this is a compromised wireless hotspot resulting in a user granting unlimited access to their device. Social engineering consists of four types of attacks, called phishing, vishing, smishing, and exploiting social media accounts. Each of these four attacks result in a tricked victim taken advantage of while using a mobile device.

Phishing refers to "masquerading as a trustworthy entity" (Wilosinski, 2016, p. 2). Vishing refers to "tricking a victim into calling a phone number and revealing sensitive information" (Wilosinski, 2016, p. 2). Smishing refers to "tricking someone via messaging into downloading malware onto their mobile device" (Wilosinski, 2016, p. 2). Lastly, exploiting social media accounts refer to utilizing publicly available information found on social media for exploitation. Social media consists of applications similar to, but not limited to Facebook and Twitter. According to Chen et al. (2017), a scammer can utilize social media accounts to specifically tailor a con to a person to the point where it looks and feels authentic. However, an attacker could use any combination of the four types of attacks of social engineering to be able to cause damage to a target (Wilosinski, 2016).

Lock screen passcodes are often the first line of defense against physical attacks. In 2014, over 5 million mobile phones were either lost or stolen from Americans and without a passcode to enter the device, data stored on the phone or online accounts, such as banking, could be easily accessed. Yet, a 2016 Mobile Security Report discovered that as high as 43 percent of mobile device users do not have "a passcode, Personal Identification Number (PIN), or pattern lock" enabled (NowSecure, 2016).

However, when Android users do elect to have a locking mechanism on their phone, they use a password system identified by a password pattern drawn by the user's finger. If the device is left unattended, a malicious source could do what Aviv, Gibson, Mossop, Blaze, and Smith (2010) call a smudge attack. The researchers concluded that they could crack into a user's Android device by extracting the pattern of hand-oil residue left on an Android cellular phone. Further, Android devices have been infamous for being left unpatched against known vulnerabilities, fixes that frequently come with software updates. In 2016, NowSecure reported results of a mobile security test run via an open-source application that revealed 82 percent of Android devices that ran their app were susceptible to at least one vulnerability and almost 25 percent of mobile applications include at least one high-risk flaw in their security (NowSecure, 2016). There are also risks for iOS devices. When a device pairs with another device through Bluetooth or USB, a folder is stored on each of the devices. This folder contains the pairing record information to all the devices that trust this source. However, according to Zdziarski (2014), this pairing folder can be used to crack into the other devices. Another area of risk for iOS devices is fraudulent authorization certificates. These authorization certificates tell a device that it is genuine and not malignant that resulted in applications uploaded to the Apple application store that masqueraded as valid applications that actually contained malware (D'Orazio & Choo, 2017).

Wearable devices that are standalone or paired with cellular phones, as well as personal computers, are becoming more widespread and socially acceptable (Mills, Watson, Pitt, & Kietzmann, 2016). Some wearable devices are life-imperative such as a real-time blood-glucose contact lens monitor which has the potential to be hacked through providing erroneous messages. This has the potential to hospitalize the user or result in a fatality. Wearable devices and cell phone devices are not regulated and therefore cannot be safeguarded from security infractions.

2.2 Espionage in the Workplace

The thought of espionage conjures up potentially accurate portrayals of images in popular culture such as of James Bond in a fancy tuxedo secretly traveling to exotic locales (Beim, 2018). It can be defined in many ways but is described by using human agents or technology to gain access to information not publicly available (Espionage, 2018). Winkler (2005) who is a former National Security Agency employee had his team perform an espionage simulation at a Fortune 500 company on the U.S. East Coast to identify how simple it can be for corporate spies to infiltrate a company. However, the theft of intellectual property is an invention that dates back to the

invention of private enterprises (Tales from the front line of corporate espionage, 2012). The Chinese guarded their monopoly on silk production but approximately 1,800 years ago, monks smuggled silkworm eggs out of China using bamboo walking sticks that was the first step to breaking the early Chinese monopoly. This section addresses deliberate theft of confidential information for espionage. Today, with the use of mobile devices, organizations are challenged with safeguarding against espionage as taking photographs of factories and businesses of trade secrets classifies as espionage (King and Bravin, 2000). Pacini et al. (2008) discusses how espionage activities can be conducted by an array of individuals such as "current and former employees, competitors, foreign governments, independent contractors, vendors, business intelligence analysts, and others" (p. 131). Furthermore, "trade secret fraud activities include customer lists, pricing strategies, formulas, compilations, financial information, processes, design manuals, strategic and marketing plans, and other proprietary information" (Pacini et al., 2008, p. 131).

Espionage activities are common among developed nations and many lesser-developed ones in activities involving spying and eavesdropping even outside of hostile states (Baker, 2003; Beim, 2018; Coppins, 2010). News articles continuously reveal cyber-attacks ranging from sabotaging government websites to stealing important information immediately to even delayed-action malware acting as time bombs in gaining access to critical infrastructure information (Kingsbury, 2010; CNBC, 2017). Pun (2017) suggests that espionage is not any different in the challenges brought by cyber space making cyber defense protections more necessary due to the growing amount of information stored and potentially available. Pun (2017) also suggests how there are "According to NATO Secretary General, Anders Fogh Rasmussen, there are now more than 100 daily cyber intrusion attempts on NATO headquarters, and over 1,000 daily cyber intrusion attempts on U.S. military and civilian networks" (p. 355-356).

Das and Khan (2016) suggest that employees' use of their personal smartphones has pushed the Bring-Your-Own-Device (BYOD) phenomena and makes it widely supported by organizations. However, the challenge with BYOD programs is the potential for security infractions. These programs bring additional anytime-anywhere capability to organizational computing (Harris & Patten, 2014) while bringing about a mobile revolution while creating a gap between academic and business aspects of information security (Silic & Back, 2014). Salifu (2008) conducted a literature review on the impact of internet crime on individuals, organizations, businesses and government. The practical implications identified is internet crime is a global issue requiring the support of both developed and developing countries to resolve because internet crime investigations trace evidence from more than one country requiring partnerships between multiple countries in order to conquer espionage. Pun (2017) suggests that espionage's permissibility under international law remains largely unsettled building upon Salifu (2008) research with espionage being a global matter.

2.3 Security Solutions

Pacini et al. (2008) suggests steps businesses can take that to preserve secrecy to include legal remedies and internal controls to protect trade secrets that refer to any information that has value because it is not common information. The primary means of enforcement available to those that fall victim of their trade secrets being pirated is a civil lawsuit filed under the Uniform Trade Secrets Act (UTSA). In order to pursue a civil suit for damages, a claimant must be able to prove five items. These items include the claimant being able to prove an existence of an actual trade secret, the reasonable steps the claimant took to preserve secrecy, the independent economic (potential) value the trade secret holds, the misappropriation of the trade secret, and the actual loss incurred

by the misappropriation. Organizations will need to provide evidentiary support to indicate that information is a secret and that the defendant secured the secret using improper means (Grubbs, 2005). Organizations can protect against internal threats by having employees sign a confidentiality agreement to ensure understanding by the employee to protect a trade secret and to have any facility visitors such as customers, suppliers or employee family members to sign a non-disclosure agreement (Gaffney & Ellison, 2003; Van Arnam, 2001). Furthermore, employers must formally remind employees to continue to protect the company's trade secret as a duty of confidentiality even after employment with the company has ceased (Gaffney & Ellison, 2003). According to the UTSA, obtaining knowledge of trade secret using improper means includes anything from theft to breach of a duty to maintain secrecy to any form of espionage such as through electronic portable devices (Pacini et al., 2008). Pacini et al. (2008) discusses how the claimant under the UTSA must establish that the defendant used or disclosed to another party the trade secret in addition to wrongful acquisition of the secret. The Economic Espionage Act of 1996 (EEA) also applies because it is a federal statute that criminalizes the theft of trade secrets by industrial spies and foreign governments. The definition under the EEA includes theft that could include a portable electronic device to steal trade secrets such as taking pictures, uploading, downloading and transmitting trade secrets.

However, organizations can also be proactive in organizational solutions to security through enhanced communication. Organizations need practices, policies, procedures and processes in place to help safeguard their trade secrets through providing training to employees. The training would involve topics such as avoiding risky behavior, social media practices, password practices, device specific vulnerabilities including cell phone brands and wearable devices, and public hotspot vulnerabilities. New employees need training on these and existing employees need refresher training. The training could target employees and any individuals in close proximity to secured areas with ways to avoid risky behavior practices making individuals vulnerable to social engineering (Wilosinski, 2016). This could reduce the risk of the four types of social engineering attacks consisting of phishing, vishing, smishing, and exploiting social media accounts. This brings us to social media practices for employees so that employees keep personal social media accounts free of information tied to their workplace. The social media policy could create awareness for employees and other closely affiliated individuals to an organization to be cautious of information placed on public social networks due to risks of information used to create fake accounts asking colleagues for sensitive work information (Chen et al., 2017). The training could also include password policies that extend not to their work devices but also to their personal devices where work email is still accessible. This policy could encourage device-locking mechanisms on personal cellular phones (Bitton et al., 2018; Shaulov & Point, 2016). The training could also utilize device specific information to alert employees of vulnerabilities that affect their personal devices. For instance, Android users that elect to have a password pattern drawn by their finger for their personal device are at risk for that pattern being stolen if they leave their device unattended (Aviv et al., 2010). The training also could provide caution for wearable device technology users because this sector is advancing faster than subsequent laws, policies, and security systems and these devices could be hacked (Mills et al., 2016). Lastly, the training could provide a reminder of vulnerabilities with public wireless hotspots and the importance of not accessing sensitive information or using devices tied to work information while on these hotspots (Wilosinski, 2016).

Another security solution exists with malware. Malware detection has improved alongside the increase in malware prevalence. Research into malware detection mechanisms centers upon two predominant methods: dynamic analysis and static analysis (Tong & Yan, 2017). A static analysis consists of analyzing the application in question to determine if it has malicious code, without actually executing the application. This was identified as an acceptable initial screening indicator as

to the nature of an application and its intended purpose. A dynamic analysis consists of analyzing the behavior of a particular application to see if the application in question is doing anything out of the ordinary. Another form of dynamic analysis, called an Android intent analysis, examines the intents, or requested permissions, by applications both explicit and implicit. According to Tong and Yan (2017), 97 % of malware programs, including but not limited to Trojans and viruses, target Android devices. Overall, organizations can help guard against security vulnerabilities through incorporating of better processes and technology.

3. Conclusion

Malware and hacking activities are growing amongst today's most popular mobile devices. These security risks are prompting organizations to enact policies aimed at mitigating the amount of espionage and illegal events that can transpire on a cell phone or other mobile device. The rise of cybercrime and cyberterrorism is not something that dwells in the realm of science-fiction novels, but exists in the real world, today, and is punishable by law (Cornell Law, Gathering, Transmitting or Losing Defense Information, 2012; Cornell Law, Gathering or Delivering Defense Information to Aid Foreign Government, 2012; Cornell Law, Disclosure of Classified Information, 2012). Pacini et al. (2008) suggests steps to preserve secrecy to include legal remedies and internal controls to protect trade secrets. Organizations can provide training to help safeguard against vulnerabilities by unsuspecting employees that could include topics such as avoiding risky behavior, social media practices, password practices, device specific vulnerabilities including cell phone brands and wearable devices, and public hotspot vulnerabilities. However, infected mobile device exposure is growing at an alarming rate, and Shaulov and Point (2016) report that, "on average, over one in 1,000 devices globally [are] infected," demonstrating the widespread proliferation of compromising methodologies (p. 5). Financial losses in 2014 reported more than $800 million due to scamming activities (Chen, Beaudoin, & Hong, 2017). The purpose of this literature review was to provide an overview of cell phone and electronic devices vulnerabilities, espionage in the workplace, and security solutions in the understanding of risks and threats in existence for cell phones and mobile devices. Future research is necessary to understand the threat of security infractions due to mobile devices within workplaces. Mobile devices continue to become more widely accepted while companies embrace BYOD programs but more research is necessary to lessen the gap in the research between academic and business aspects of information security (Silic & Back, 2014). Research focuses on attitudes and intentions with respect to information security policy with very limited studies on actual behavior necessitating the need for more research to identify interventions that reduce security vulnerabilities in the workplace (Sommestad et al., 2014).

4. References

Aviv, A., Gibson, K., Mossop, E., Blaze, M., & Smith, J. (2010). Smudge attacks on smartphone touch screens. Department of Computer and Information Science Paper, University of Pennsylvania. Retrieved from https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Baker, C.D. (2003). Tolerance of international espionage: A functional approach. American University International Law Review, 19(5), Article 2, 1091-1113. Retrieved from http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1176&context=auilr

Beim, J. (2018). Enforcing a prohibition on international espionage. Chicago Journal of International Law, 18(2), 647-672. Retrieved from https://search-proquest-com.portal.lib.fit.edu/docview/2012381493?accountid=27313

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers & Security, 73. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404817302316

Bransfield-Garth, S. (2010). Mobile phone calls as a business risk. Network Security, 9. Retrieved from https://www.sciencedirect.com/science/article/pii/S1353485810701148

Chen, H., Beaudoin, C., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior, 70. http://dx.doi.org/10.1016/j.chb.2017.01.003

CNBC (July 4, 2017). Germany big target of cyber espionage and attacks: Government Report. Retrieved from https://www.cnbc.com/2017/07/04/germany-big-target-of-cyber-espionage-and-attacks-government-report.html

Coppins, M. (July 21, 2010). Spies Among Us: Modern-Day Espionage. Newsweek. Retrieved from http://www.other-news.info/2010/07/spies-among-us-modern-day-espionage/

Cornell Law. (2012). 18 USC 793: Gathering, transmitting or losing defense information. Retrieved from http://law.cornell.edu/uscode/uscprint.html

Cornell Law. (2012). 18 USC 794: Gathering or delivering defense information to aid foreign government. Retrieved from http://law.cornell.edu/uscode/uscprint.html

Cornell Law. (2012). 18 USC 795: Photographing and sketching defense installations. Retrieved from http://law.cornell.edu/uscode/uscprint.html

Das, A., and Khan, H.U. (2016). Security behaviors of smartphone users. Information & Computer Security, 24(1), 116-134. https://doi.org/10.1108/ICS-04-2015-0018

D'Orazio, C., Lu, R., Choo, K., & Vasilakos, A. (2017). A markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps. Applied Mathematics and Computation, 293. Retrieved from http://dx.doi.org/10.1016/j.amc.2016.08.051

D'Orazio, C., & Choo, K. (2017). A technique to circumvent SSL/TLS validations on iOS devices. Future Generations Computer-Systems, 74. Retrieved from http://dx.doi.org/10.1016/j.future.2016.08.019

Espionage, Security Service M15, Retrieved from https://perma.cc/N857-RP93

Gaffney, G. and Ellison, M. (2003). A primer on Florida trade secret law: unlocking the 'secrets' to 'trade secret. University of Miami Business Law Review, 11, 1-76.

Grubbs, J. (2005). Give the little guys equal opportunity at trade secret protection: why the 'reasonable efforts' taken by small businesses should be analyzed less stringently. Lewis & Clark Law Review, 9, 421-45.

Harris, M.A. & Patten, K.P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. Information Management & Computer Security. 22(1), 97-114. doi: 10.1108/IMCS-03-2013-0019

Jones, B., & Chin, A. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. International Journal of Information Management, 35. http://dx.doi.org/10.1016/j.ijinformgt.2015.06.003

King, N., Jr. and Bravin, J. (2000). Call it mission impossible, inc. – corporate spying firms thrive, Wall Street Journal, 3, p. B1.

Kingsbury, A. (April 14, 2010). Documents reveal Al Qaeda cyberattacks. U.S. News & World Report. Retrieved from https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks

Mills, A., Watson, R., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. Business Horizons, 59. Retrieved from http://dx.doi/10.1016/j.bushor.2016.08.003

NowSecure. (2016). Mobile Security Report. Retrieved from https://www.nowsecure.com/resource/2016-nowsecure-mobile-security-report/

Pacini, C., Placid, R., and Wright-Isak, C. (2008). Fighting economic espionage with state trade secret laws. International Journal of Law and Management, 50 (3), 121-135. https://doi-org.portal.lib.fit.edu/10.1108/17542430810877454

Pun, D. (2017). Rethinking espionage in the modern era. Chicago Journal of International Law, 18(1), 353-391. Retrieved from https://search-proquest-com.portal.lib.fit.edu/docview/1991564080?accountid=27313

Salifu, A. (2008). The impact of internet crime on development. Journal of Financial Crime, 15(4), 432-443. https://doi-org.portal.lib.fit.edu/10.1108/13590790810907254

Schiwy, Nick. (2016). PSA: Lookout recently found 13 new malicious apps on Google Play. Published January 6, 2016.

Shaulov, M., & Point, C. (2016). Bridging mobile security gaps. Network Security. January 2016. https://doi.org/10.1016/S1353-4858(16)30006-X

Silic, M. & Back, A. (2014). Information security: critical review and future directions for Research. Information Management & Computer Security, 22(3), 279-308. doi: 10.1108/IMCS-05-2013-0041

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance. Information Management & Computer Security, 22(1), 42-75. doi: 10.1108/IMCS-08-2012-0045

Tales from the front line of corporate espionage: The fight to safeguard intellectual property is fiercer than ever (2012). Strategic Direction, 28 (9), 29-32. https://doi.org/10.1108/02580541211256530

Thompson, N., McGill, T., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. Computers and Security, 70. Retrieved from http://dx.doi.org/10.1016/j.cose.2017.07.003

Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. Parallel and Distributed Computing, 103.http://dx.doi.org/10.1016/j.jpdc.2016.10.012

Van Arnam, R. (2001). Business war: economic espionage in the U.S. and European Union and the need for greater trade secret protection. North Carolina Journal of International Law and Commercial Regulation, 27, 95-139.

Wilosinski, L. (2016). Mobile computing device threats, vulnerabilities and risk factors are ubiquitous. Information Systems Audit and Control Association Journal, 4. Retrieved from https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Mobile-Computing-Device-Threats-Vulnerabilities-and-Risk-Factors-Are-Ubiquitous_joa_Eng_0716.pdf

Winkler, I. (2005). Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day. Indianapolis, IN: John Wiley & Sons.

Zdziarski, J. (2016). Identifying back doors, attack points, and surveillance mechanisms in iOS devices. Digital Investigation, 11. http://dx.doi.org/10.1016/j.diin.2014.01.0001