Research Journal of Applied Sciences 8 (3): 161-166, 2013
ISSN: 1815-932X

Insider Threats+Disruptive Smart Phone Technology = New Challenges to Corporate Security

Ahmed Al-Haiqi, Kasmiran Jumari and Mahamod Ismail
Department of Electrical, Electronic and Systems,
Faculty of Engineering and Built Environment,
University Kebangsaan Malaysia, 43600 Bangi, Malaysia

Abstract: Wireless portable computing technology is proving itself as the ultimate disruptive technology to enterprises and new threats have already been a concern for media and industry. Unlike most available advisories and public guidelines, the focus of this study is on the intersection of two aspects of these new challenges; the indispensable smart phones in the hands of malicious insiders to the corporate. Many new threats could be less than obvious with the combination of these two aspects. Researchers provide a general classification for these threats, present some challenging scenarios and finally discuss the solutions that already had been considered or could be taken into consideration to eliminate or mitigate the new threats.

Key words: Insider threats, disruptive technology, smartphones, corporate security, mobile security, network security

INTRODUCTION

This study concentrates on two aspects of corporate security. The first is the threat of insiders, i.e., the attackers internal to the corporate, typically disgruntled or paid employees. The other element is the threat of new mobile device disruptive technology, in particular smart phones with which PDAs also share most of the threats. Together, the combination of these two threat elements forms the scope of the study. This restriction of the scope allows for a more thorough treatment of the topic, otherwise more difficult to handle like in most other more general reviews.

The justification for choosing the insider threat exclusively is that insiders are reportedly responsible for a large percentage of corporate security breaches. In the few past years, many surveys estimated the insider incidents to range between 40 and >80% and even more of all incidents reported, e.g. as by Pfleeger and Stolfo (2009), Liu *et al*. (2009), Application Security Inc. (2007) and Fyffe (2008). More recently, The 2010 CyberSecurity Watch Survey reported that although outsiders are the main perpetrators in general, the most costly or damaging attacks are more often caused by insiders (CERT, 2010).

Furthermore while measures have been developed to mitigate insider threats in traditional corporate environments, new disruptive technology like smart phones often opens new avenues for insiders. In the same last survey (CERT, 2010), 20% of the 500 + respondent organizations have indicated smart phones as mechanisms used by insiders to commit electronic crimes.

The impact of new disruptive technology has attracted the attention of many researchers (Conger and Landry, 2009). The researchers suggested the requirement of paradigm shift in securing data, due to the emerging of new eminent technologies. They discussed the disruptive effects of three threats: RFID chips, GPS and smart motes. For smart phones in particular, quite few articles in media pointed out the issue of their security related to corporate environment rather than to individual's privacy (Rege, 2009; Metzler and Taylor, 2010; Dearing, 2009). University researchers also attempted to demonstrate the new threats of smart phones as by Rutgers University (2010). Mostly, the emphasis here is on the user of smart phone as a victim, used by malicious parties to access corporate data (stored in compromised smart phone) or to access corporate network (through privileged applications and accounts installed on smart phones). The focus is little on the role of smart phone user as an insider and the vast potentials of smart phones in the context of insider threats. Also, mainly the threats discussed are reflections of the usual threats found in traditional computer systems and networks like malware, eavesdropping and unauthorized access to device resources; little insight is given into the unusual potential threats posed by smart phones. However, a more comprehensive research is the guidelines published by NIST on cell phone and PDA

Corresponding Author: Ahmed Al-Haiqi, Department of Electrical, Electronic and Systems,
Faculty of Engineering and Built Environment, University Kebangsaan Malaysia, 43600 Bangi, Malaysia

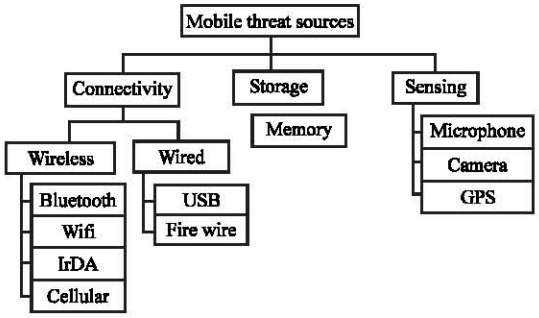

Fig. 1: General classification of smart phone threat sources

Fig. 2: Tethering using the smartphone as a modem

security (Jansen and Scarfone, 2008). These guidelines are wider and provide balanced insight from both the perspective of the personal users and of the organizations. Yet because of the broad coverage of the guidelines, some individual topics such as possible threats by insiders are not tackled in great depth.

Contribution: The main contribution of this research is to elaborate on the new and less obvious threats of smart phones rather than the well-known and more obvious ones and in the context of the user as an insider threat rather than the victim as in the most available reviews. To put the discussion into order, a classification of these threats is also provided in Fig. 1.

CONNECTIVITY THREATS

Connectivity of devices could be between a smart phone and another smart phone between a smart phone and a corporate computer or between a smart phone and the corporate network.

Connectivity between a smartphone and a computer: A smart phone can connect to a corporate PC or laptop in a variety of ways some of which are wireless like Bluetooth and IrDA and others are wired like USB cables. Legal purposes exist for these kinds of connectivity so their availability is not questionable per se. An example of valid and common application for such connectivity is using SyncML standard to synchronize data between a smart phone and another smart phone or computer (Alliance, 2007).

Bluetooth connectivity: Bluetooth interfaces are built-in in most laptops or could be provided through USB adapters. This connectivity could be used to transfer files from the computer to the smart phone or the other way around. An intruder can use his smart phone to copy corporate sensitive/copy-right data or load the computer with malware. Some types of malware can act as a backdoor to further malicious intrusion, possibly from outside the corporate network.

Tethering: Smart phones could be used to provide computers with Internet connection through a method called tethering. This connectivity could be accomplished using a USB cable or Bluetooth. Normally, this method is useful when there is no Internet access around and the cellular network provider offers this service so a computer user can use a mobile phone as a modem to connect the computer to the Internet through the cellular network (Fig. 2). Obviously, this connectivity bypasses the corporate network's secure entry points and provides external access into the perimeter of the network. In effect, this threat resembles the old one of using card modems to allow Internet access into the secured corporate network.

Another similar scenario is to use the mobile hotspot capability to provide wireless access point for corporate devices into the Internet (3G mobile Internet). Some smart phones have the ability to act as WIFI router so it can share its 3G Internet connectivity with other few computers. These computers would access the Internet through the smart phone bypassing corporate security measures. Moreover, the smart phone user now has the control over all traffic utilizing its hotspot, the least advantage of which is to eavesdrop on other employees data.

Connectivity between a smartphone and the corporate network

3G Internet: Provided a service package is obtained from the 3G cellular network provider, a smart phone can access the Internet with increasingly high speeds using 3G mobile Internets. This implies that a smart phone should be regarded as another remote computer-relative to the corporate network-connecting through the Internet, although physically it is internal to this network. Many organizations allow their employees to access the

corporate network using their smart phones or other personal computers from home through the Internet (often presumably utilizing the corporate VPN), in order to increase productivity. In this regard, smart phones bear the same threat as employee-owned PCs and laptops that are granted corporate network access from the wild Internet with the difference that smart phones are still less suspicious in some way perhaps due to their size and recentness. Also, the insider with this capability have the advantage of simultaneous connectivity from inside the network (using his/her workstation) and from outside the network (through the Internet using his/her smart phone). This advantage can give the insider more flexibility in breaching corporate network security, e.g., subverting the corporate firewall through interactive tunneling.

WIFI: Recent smart phones have WIFI support which provide them the ability to connect to WIFI hotspots in any neighborhood and access to wireless local networks. In this way, a smart phone can be regarded as an extra workstation to the corporate network, provided the insider employee has enough information to connect to the corporate wireless access point (this could be the case if the security administrator gives out this information for WLAN clients, like laptops, to the employees). Now a days, smart phones could also have dual mode WIFI/3G connectivity in which the smart phone can connect to local WIFI access point while still preserving 3G cellular network connection.

Connectivity between two smartphones

Malware: An insider may utilize social engineering or otherwise exploiting compromised smart phones in the same organization, to connect to these smart phones, mainly through Bluetooth. The obvious purpose of this connectivity is to transfer malicious software that could be used later to access personal/corporate data stored/accessed by the compromised phone. Furthermore, this malware is necessary to enable other attacks presented later in the category of smart phone sensing threats.

Mobile hot spot: Another type of threat that a smart phone may impose, is the ability to provide wireless access point as explained above. An insider can set a smart phone with this capability to impersonate a legitimate public (or yet better, if possible, a legitimate internal) access point. Afterward, the insider himself/herself could use this hotspot to access the Internet from his/her local workstation and any other employees who connect to this hotspot (either by virtue of curiosity or deception) would actually connect to the smart phone. This connection could be exploited by the insider to collect confidential data (e.g., WLAN connection credentials), misdirect the traffic to suspect sites or deliver malicious code to the participating nodes.

STORAGE CAPABILITIES

USB flash drives have been a nightmare for corporate IT administrators for almost a decade by now. Part of their problem is being the main source of malware into the corporate workstations and the other part is their storage capability that permits an insider to copy tremendous amount of corporate data or even software. Smart phones share USB devices this later capability through their increasingly expanding memory cards (up to 32 GB). The real problem is though smart phones storage capacities are comparable to those of USB drives, they are not perceived as storage devices, yet. This status gives smart phones an advantage over USB storage devices, from the point of view of the insider.

MOBILE SENSING THREATS

Typically, smart phones are supplied with a set of embedded sensors, some of which may be used as surveillance devices. Examples of common sensors are the camera, microphone, GPS receiver and digital compasses (Lane *et al*., 2010). Although, smart phone GPS could provide sensitive location-based information of corporate personnel or corporate assets, it is more related to privacy concerns. A more relevant concern to the scope of this research is the potentials of using the camera and microphone in collecting information.

An apparent threat is to use the smart phone as a camera to photocopy/scan hardcopy documents (Litchfield, 2009). Documents, carts or otherwise copy-righted material circulated in meetings, found casually or otherwise accessed illegally could be scanned with a reasonable resolution, using an average smart phone's camera and saved as images in the phone's memory. Some scanner software could even be used to convert these images into standard PDF or MSWORD formats. An already common use of this feature is to photograph meeting whiteboards. This threat is not restricted to hardcopy documents, softcopy material like charts, worksheets or other data could be captured off the computer screen and kept in memory, in case transferring data through corporate network to remote destinations proved challenging for the insider. Often, certain statistics or plans are sensitive to the organization and simply cannot be memorized or even understood by the human insider.

Another related threat is the capability of some smart phones to function as a surveillance camera, remotely controlled. An application, e.g., M-Surveillance (M-Surveillance, 2009) is used to order a smart phone, remotely, through SMS messages, to record video and audio or capture pictures, possibly without the knowledge of the smart phone holder. A typical scenario is for the insider to get access to the smart phone of a fellow employee, assumingly with authority to attend meetings beyond the privileges of the attacker. The chance to obtain physical access to a mobile phone is very likely, especially by an insider in a local, trusted environment such as a corporate office. The attacker should then configure the surveillance application in the compromised smart phone to accept commands from his own phone number. Afterward, the attacker can send specific format SMS to the breached phone to begin recording or capturing audio or pictures while being in a meeting. The application in the case of M-Surveillance stores the captured audio/pictures/video in the SD card and it could not be viewed until the smart phone is connected to a computer and the memory is mounted on it. This provides the insider with the opportunity to collect back the recorded content.

This kind of attack does not have to use vendor-provided applications; rootkits, a class of malware could be used to eavesdrop on conversations or meetings with the smart phone user being none the wiser. Researchers at Rutgers University have demonstrated in one test (Rutgers University, 2010) how a rootkit could be exploited by an attacker who sends an invisible text message to the infected phone causing it to issue a call and turn on the microphone.

SOLUTIONS

In this study, researchers present solutions either in practice or have been recommended to mitigate the threats associated with new smart phone technology in particular. Researchers also provide some thoughtful discussion about new options and problems with various suggestions. It is important to note that we deliberately skim quickly over user-oriented measures that are often found in mobile device security advisories and guidelines (Jansen and Scarfone, 2008). Those measures are concerned mainly with protecting phone user privacy or protecting phone-reachable corporate assets provided the cooperation of the user. Obviously, this has little to do in the context of insiders where the user is the source of threat. Examples of usual user-oriented measures are (Jansen and Scarfone, 2008; ISO, 2005; NUIT, 2012):

- Protect the physical access of the phone and to promptly report lost or stolen devices
- Enable user authentication through passwords or PIN identification numbers
- Backup data
- Reduce storage of sensitive information as much as possible on the devices
- Disable options and applications and even wireless interfaces that are not used
- Use protection software like firewalls, antivirus, IDS, anti-spam, VPN and other tools
- Use data encryption
- Follow-up safe disposal practices
- Update device software
- Use common sense when dealing with unknown sources of applications or messages

The more important view to countermeasure insider threats is to view the security related to smart phones as a responsibility of the organization rather than individual employees. This involves many steps, the first of which is recognizing the real new threat then taking the decision and actually proceeding to plan, implement and maintain a mobile device policy that complement and integrate with the hopefully the existing corporate security policy.

Another central measure to deal with these threats is to consider more carefully the bottom line of security; i.e., the operating system. Several mechanism of OS security can be combined to defeat many aforementioned threats.

Finally, researchers discuss defenses related to physical security as an essential component to countermeasure some of the most difficult troubles to deal with using earlier measures.

Realizing the threat and adopting mobile device policy: The most essential step is for the organizations to realize the new threats and recognize the smart phones as an extended component of the organization's infrastructure (Jansen and Scarfone, 2008) and a corporate asset. This implies the need for careful planning for an extended policy that manage new mobile devices, built on risk assessment of their new threats and issues and then this policy should be thoroughly deployed and continuously maintained. It is important during this process to realize that smart phones are in effect an evolution of personal computers (BlackBerry, 2010) though they lack many security features of them and add also few other issues.

One principle strategy for organizations is to force centralized management of mobile devices (BlackBerry, 2010). This could be accomplished only by having control over the devices used by employees, at least in corporate perimeter, through organization-issued smart phones.

Although, an insider might always attempt to use his personally owned smart phone, the configuration of only smart phones issued by organization to access corporate data eliminates many risks. For example, this configuration should prevent the insider from loading malware or using unauthorized software while connecting to the corporate network.

In this direction, some vendors already supply mobile device management solutions, providing an infrastructure in which all organization-issued devices and their communication with corporate back-end data could be controlled and configured centrally. An example of a well known technology of this kind is the BlackBerry Enterprise Solution security (BlackBerry, 2012). An apparent problem with this strategy would be for the insider to use his own smart phone to conduct some breaches. Or he/she may still abuse the authorized access to corporate network through the organization-issued smart phone to steal data for example. Nevertheless, the issue of customized smart phone for business is much more advantageous, to protect the enterprise network and date from outsiders in the first place and to restrict access to enterprise data by insiders to preconfigured and fully controlled applications. This certainly limits the options of the insider and left less threats to other measures.

Another responsibility of the organization is to provide adequate training for its employees on the security of their smart phones and best practices in using them as discussed above regarding user-oriented measures. Besides the usual benefits of this type of training, this should also help to deprive the insider from exploiting other's smart phone to perform some attacks.

The principle of least privilege: This principle is a standard security measure on the level of the operating system and states that every user should have security permissions just adequate to fulfill the required functions and nothing more. Many of the threats associated with insiders in general could be eliminated by ensuring that every user has the least privileges necessary to his/her work. In this case, no insider should be able to access sensitive data beyond his/her permissions or install software (or attach devices) that facilitates any security breaches. Moreover, all connectivity settings of workstations or routers should be available only for high-privileged administrators.

USB ports: Related closely to the earlier point is the well-known problem of USB ports. Many connectivity options to computers, wired or wireless, depend on USB interfaces either directly or through special adapters. Examples of these connections are Bluetooth adapters and USB cables that enable tethering. Connectivity threats of these types are not possible if the USB ports are disabled. Disabling the ports is one extreme and could be done physically, on BIOS level or on operating system level. Sometimes, this option is not feasible since, many legal peripheral devices use the USB interface (e.g., printers). A common alternative is to use third party utilities to apply USB port access privileges to specific users, user groups and even USB device classes such as Palm, USB phone and others (Pham *et al*., 2010). It is also always possible to utilize the least privilege principle by the native operating system to ensure that the user can not install USB device drivers or foreign software that control connectivity through USB ports (e.g., tethering applications).

Physical security: Some of the threats imposed by smart phones, particularly those related to mobile sensing cannot be countered by the earlier solutions. Organization policy should handle such cases by enforcing reasonable physical security measures. First and for most, access to corporate assets should be protected physically. Unauthorized personnel should not be granted entry to sensitive spots or access to classified documents. But still, there are situations where the mere bearing of a smart phone implies a threat of some kind for instance the ability to record audio and/or video during meetings. Gangster members in movies have learned this lesson since a while ago and members are required to hand over their mobile phones before joining a (classified) meeting. This is inconvenient of course in corporate environments and even leads to the more unlikely requirement of manually inspecting the participants as hiding smart phones is easy duo to their size. In effect as more sensors are embedded in smart phones and sensor technology advances, smart phones could be sorted in the same category of smart motes as spying tools.

CONCLUSION

New computing technology has been always disruptive to the established security measures in home and corporations. Smart phones are the coming IT Swiss army knife with wondrous benefits for individuals and enterprises alike but also with new unforeseen threats. Combine that with a malicious insider smart phone user and the result is a serious challenge to corporate security. Connectivity features, storage capacities and sensing abilities are the basic sources of the new threats of which researchers have presented some of the main potential attack scenarios they make possible. Many solutions to these challenges are already in place but no single

measure can remedy the whole situation. Implementing a thorough corporate policy for mobile device security is a must, without which little control could be held over insider opportunities. Much risks could be eliminated provided the principle of least privilege is ensured and a clear policy to control USB ports can fix great deal of the trouble. Finally, physical security is of no substitute to reduce insiders' risks.

REFERENCES

Alliance, O.M., 2007. OMA technical section-affiliates-syncml. Open Mobile Alliance Ltd., USA. http://www.openmobilealliance.org/tech/affiliates/syncml/syncmlindex.html.

Application Security Inc., 2007. Addressing the insider threat: Improving database security to manage risk within the federal government. Application Security Inc., New York. http://www.appsecinc.com/techdocs/whitepapers/Addressing-the-Insider-Threat-Fed.pdf.

BlackBerry, 2010. Secure smartphone apps: The next generation. White Paper. Research in Motion Limited, Canada. http://us.blackberry.com/business/leading/Secure_Smartphone_Apps.pdf.

BlackBerry, 2012. Black berry enterprise solution security. Research In Motion Limited, Canada. http://docs.blackberry.com/en/admin/deliverables/16648/BlackBerry_Enterprise_Solution_security_834422_11.jsp.

CERT, 2010. Cybersecurity watch survey: Cybercrime increasing faster than some company defenses. http://www.sei.cmu.edu/newsitems/cyber_sec_watch_2010_release.cfm.

Conger, S. and B. Landry, 2009. Disruptive Technology Impacts on Security. In: Handbook of Research on Information Security and Assurance, Gupta, J.N.D. and S.K. Sharma (Eds.). IGI Global Snippet, USA., ISBN: 9781599048550, Pages: 557.

Dearing, D., 2009. Smartphone: From threat to asset. http://www.networkworld.com/columnists/2009/091125-insiderthreat.html.

Fyffe, G., 2008. Addressing the insider threat. Network Security, 2008: 11-14.

ISO, 2005. Mobile device security and usage guideline. Carnegie Mellon University, Information Security Office, Pittsburgh PA.http://www.cmu.edu/iso/governance/guidelines/mobile-device.html.

Jansen, W. and K. Scarfone, 2008. Guidelines on cell phone and PDA security. Special Publication 800, 124, National Institute of Standards and Technology.

Lane, N.D., E. Miluzzo, H. Lu, D. Peebles, T. Choudhury and A.T. Campbell, 2010. A survey of mobile phone sensing. Commun. Mag., 48: 140-150.

Litchfield, S., 2009. How to: Use your phone as a scanner. http://www.allaboutsymbian.com/features/item/How_to_Use_your_phone_as_a_Scanner.php.

Liu, D., X.F. Wang and L.J. Camp, 2009. Mitigating inadvertent insider threats with incentives. Proceedings of the 13th International Conference Financial Cryptography and Data Security, February 23-26, 2009, Accra Beach, Barbados, pp: 1-16.

M-Surveillance, 2009. FAQ-M-surveillance. http://androuniverse.net/?page_id=75.

Metzler, J. and S. Taylor, 2010. Security for mobile devices on the corporate network. http://www.networkworld.com/newsletters/ 2010/032210wan1.html.

NUIT, 2012. Mobile device security guidelines. Northwestern University Information Technology.

Pfleeger, S.L. and S.J. Stolfo, 2009. Addressing the insider threat. Secur. Privacy, 7: 10-13.

Pham, D.V., A. Syed, A. Mohammad and M.N. Halgamuge, 2010. Threat analysis of portable hack tools from USB storage devices and protection solutions. Proceedings of the International Conference on Information and Emerging Technologies, June 14-16, 2010, Karachi, Pakistan, pp: 1-5.

Rege, O., 2009. Their phone, your headache. http://www.networkworld.com/columnists/2009/091016-insiderthreat.html.

Rutgers University, 2010. New security threat against smart phone users, researchers show. ScienceDaily. February 22, 2010. http://www.sciencedaily.com/releases/2010/02/100222121624.htm.