ENHANCING SECURITY IN MOBILE COMPUTING DEVICES

[1]Ojeme B. O and [2]Odabi I Odabi
[1,] Department of Mathematics and Computer Science
Delta state University, Abraka, Delta State, Nigeria

[2]Department of Mathematics and Computer Science
Benson Idahosa University, Benin City, Nigeria

ABSTRACT
Increasingly, societies and nations --- far and near --- and economies are highly dependent on information and information infrastructure for survival, enhancing service delivery efficiency and increasing productivity. Security threats or not, there's no denying that networks have become integral to how the general work force operates in the digital age. The devices give workers the ability to be more efficient without being constrained by the physical boundaries of the office. With all the added capabilities of mobile computing devices comes a rapidly growing security threat that experts say appear a little more advanced and aggressive. News reports on data leakage have become a regular feature and cause huge embarrassment to organizations, impacting their image and damaging the relationship with customers. This paper looked at modern preventive and management security measures to secure company data and protect mobile computing devices, without decreasing employee flexibility and business productivity.

INTRODUCTION
Over the past few years, mobile computing devices security attacks have become easier to use, stealthier, more sophisticated and powerful with techniques to bypass, subvert and even target today's security defences such as firewalls, intrusion detection/prevention systems, and antivirus software (La Polla *et al.,* 2013). A plethora of research has been devoted to designing and devising more effective, intelligent, adaptive and active defence systems and mechanisms.

MOBILE COMPUTING
Mobile computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link (Masoud *et al.,* 2012).

Mobile Computing Device
Masoud *et al.* (2012) *defined Mobile Computing Device as* a small, lightweight, portable handheld device containing wireless Internet access.

Mobile computing devices can store large amounts of data and are frequently unprotected: they are easy to steal or lose, and unless precautions are taken, an unauthorized person can gain access to the information stored on them. Even if not stolen or lost, intruders can sometimes gain all the access they need if the device is left unprotected, if data is "sniffed out of the air" during wireless communications, or if malware is installed. The results can include crippled devices, personal data loss, disclosure of non-public University data, and disciplinary actions for the device owner. There are a number of devices classed as mobile computing devices, including Personal Digital Assistant (PDA), smartphones (Blackberry, Iphone, Android etc.), web phone, laptop computer, notebook, tablet computer, portable data terminals or any one of numerous other devices that allow the user to complete computing tasks without being physically connected to a network (Masoud *et al.,* 2012).

LIMITATIONS FOR MOBILE COMPUTING DEVICES.
According to Masoud *et al.* (2012), the following are some general limitations for mobile computing devices:

Insufficient bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS

and EDGE, and more recently HSDPA and HSUPA 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

Power consumption: When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

Potential health hazards: People who use mobile devices while driving are often distracted from driving and are thus assumed more likely to be involved in traffic accidents. (While this may seem obvious, there is considerable discussion about whether banning mobile device use while driving reduces accidents or not. Cell phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health have been raised.

Human interface with device: Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

Mobile computing device security refers to those tools and techniques that are particularly useful for mitigating the types of threats mobile devices are commonly exposed to, specifically theft, loss, and communication over insecure public networks such as the Internet or wireless hotspots **(**CISCO systems, 2001**)**.

NEED FOR DATA AND MOBILE DEVICES SECURITY

According to Yap (2005), Confidentiality, Integrity, and Availability of data and mobile devices are the reasons for securing mobile computing devices. These are explained briefly.

Confidentiality

Maintaining confidentiality is the prevention of unauthorized disclosure of information. Strict controls must be implemented to ensure that only those persons who need access to certain information have that access. In some situations, such as those with confidential and secret information, people should only have access to that data which is necessary to perform their job functions. Many computer crimes involve compromising confidentiality and stealing information.

Integrity

Integrity ensures that system information exists in the same state as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. The consequences of using inaccurate information can be disastrous. If improperly modified, data can become useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times. When the validity of information is critical, it is often helpful to design application controls and checks to ensure accuracy. It may be important to ensure that information is useless if it is stolen.

Availability

Availability is the property of being accessible and useable upon demand by an authorized entity. This applies not only to information, but also to networked devices and other aspects of the technology infrastructure. The inability to access those required resources is called “denial of service.”

THREATS TO DATA AND MOBILE DEVICES

As with any type of crime, Kartik (2004)

noted that the threats to mobile devices, privacy and integrity of data come from a very small minority of vandals, discussed bellow:

Crackers
Crackers are those who commit evil acts by breaking the security features of software. These individuals are either driven by personal interests, curiosity, or are paid to crack software or a network system by companies that hire them. Crackers use different tools and methods to break the security of a system. Some of these methods are Trojan Horse, Snooper, Virus, Worm, Vulnerability and Port Scanner, Exploit, Social engineering, Root Kit, Packet Sniffing, and many other methods (Kartik, 2004).

Trojan Horse
Trojan Horse is delivery vehicle for destructive code. Trojans appear to be harmless or useful software programs, such as computer games, but they are actually enemies in disguise. Trojans can delete data, mail copies of themselves to e-mail address lists, and open up computers to additional attacks. Trojans can be contracted only by copying the trojan horse program to a system, via a disk, downloading from the Internet, or opening an e-mail attachment. Neither trojans nor viruses can be spread through an e-mail message itself—they are spread only through e-mail attachments.

Snoops
Whether content or disgruntled, some employees might also be curious or mischievous. Employees known as "snoops" partake in corporate espionage, gaining unauthorized access to confidential data in order to provide competitors with otherwise inaccessible information. Others are simply satisfying their personal curiosities by accessing private information, such as financial data, a romantic e-mail correspondence between co-workers, or the salary of a colleague. Some of these activities might be relatively harmless, but others, such as previewing private financial, patient, or human resources data, are far more serious, can be damaging to reputations, and can cause financial liability for a company.

Viruses
Viruses are the most widely known security threats, because they often garner extensive press coverage. Viruses are computer programs that are written by devious programmers and are designed to replicate themselves and infect computers when triggered by a specific event. For example, viruses called macro viruses attach themselves to files that contain macro instructions (routines that can be repeated automatically, such as mail merges) and are then activated every time the macro runs. The effects of some viruses are relatively benign and cause annoying interruptions such as displaying a comical message when striking a certain letter on the keyboard.

Worm
A worm is an application that looks for weaknesses in a system or a network, and reproduces itself on that system till the system crashes.

Vulnerability and Port Scanner
Vulnerability Scanner is a tool that is used to check if a computer on a network has a known weakness. There are also port scanners that enable the cracker to determine the open port that can be accessed through to the computer.

Packet Sniffing
Packet Sniffing can be used for network monitoring, and for troubleshooting. It can be a powerful tool to gather information that helps compromise the network.

Social Engineering
Social engineering is the increasingly prevalent act of obtaining confidential network security information through non-technical means. For example, a social engineer might pose as a technical support representative and make calls to employees to gather password information. Other examples of social engineering include bribing a co-worker to gain access to a server or searching a colleague's office to find a password that has been written in a hidden spot.

Hackers
A hacker can be described as a brilliant pro-

grammer, a computer criminal, a gray hat, or a white hat hacker (Wikipedia, 2004). A brilliant programmer is someone who can write code very fast, and produces a program that delivers ideas as intended. These kinds of individuals are mainly harmless and will not bother with hacking programs unless asked to by their company. When these hackers start writing code to break the security features of programs, systems, and network, they will mainly be identified as crackers.

Unaware Staff

As employees focus on their specific job duties, they often overlook standard network security rules. For example, they might choose passwords that are very simple to remember so that they can log on to their networks easily. However, such passwords might be easy to guess or crack by hackers using simple common sense or a widely available password -cracking software utility. Employees can unconsciously cause other security breaches including the accidental contraction and spreading of computer viruses.

Disgruntled Staff

Angry employees, often those who have been reprimanded, fired, or laid off, might vindictively infect their corporate networks with viruses or intentionally delete crucial files. This group is especially dangerous because it is usually far more aware of the network, the value of the information within it, where high-priority information is located, and the safeguards protecting it.

Vandals

Web sites have come alive through the development of such software applications as ActiveX and Java Applets. These devices enable animation and other special effects to run, making Web sites more attractive and interactive. However, the ease with which these applications can be downloaded and run has provided a new vehicle for inflicting damage. A vandal is a software application or applet that causes destruction of varying degrees. A vandal can destroy just a single file or a major portion of a computer system.

Data Interception

Data transmitted via any type of network can be subject to interception by unauthorized parties. The perpetrators might eavesdrop on communications or even alter the data packets being transmitted. Perpetrators can use various methods to intercept the data. Internet Protocol (IP) spoofing, for example, entails posing as an authorized party in the data transmission by using the IP address of one of the data recipients.

TECHNIQUES FOR ENHANCING SECURITY OF MOBILE COMPUTING DEVICES

Here, we discuss some tools for securing data and mobile computing devices:

Intrusion Detection System (IDS)

Intrusion Detection System (IDS) monitors network traffic for suspicious activities and alerts the system or network administrator (Passive IDS), or in certain cases, blocks the user or the source IP address from accessing the network (Scarfone and Mell, 2007).

Intrusion detection provides the following:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files

The installation of the IDS's sensors is demonstrated in the figure 1.0 below:

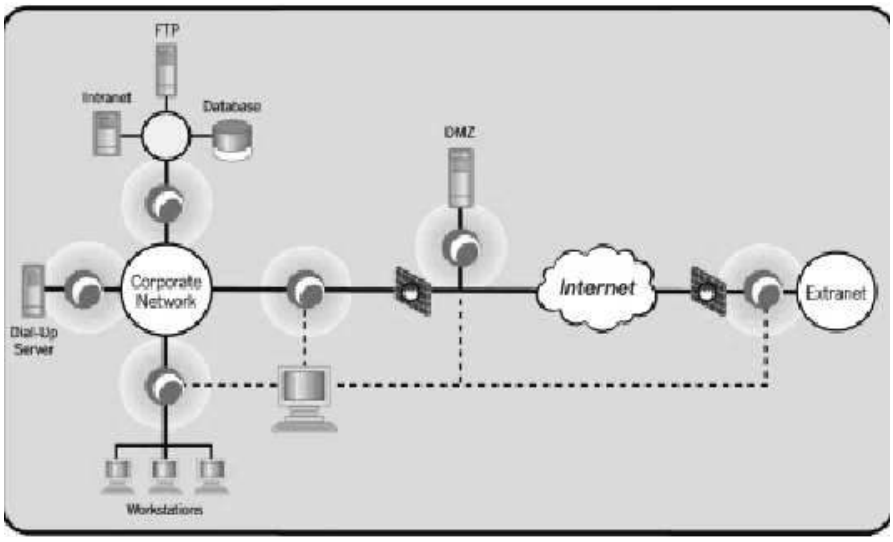

Figure 1.0: Sensors are represented by round blue dots

As you can see on a figure , the logical places for the sensors are:

- Between your network and Extranet
- In the DMZ before the Firewall to identify the attacks on your servers in DMZ
- Between the firewall and your network, to identify a threat in case of the firewall penetration
- In the Remote access environment
- If possible between your servers and user community, to identify the attacks from the inside
- On the intranet, ftp, and database environment

The idea is to establish your network perimeter and to identify all possible points of entry to your network. Once found IDS sensors can be put in place and must be configured to report to a central management console. The dedicated administrators would logon to the console and manage the sensors, providing it with a new-updated signature, and reviewing logs. Remember to ask the vendor if the communication between your sensors and management console is secure.

Encryption

Encryption or enciphering is the process by which plaintext is converted into ciphertext (Avinash, 2012). In other words, encryption Encryption scrambles data in a way that it can only be read by someone who possesses the corresponding decryption key. If an unauthorized individual obtains access to a device with encrypted data, but does not have the decryption key, they see only random gibberish instead of sensitive data. . Encryption mitigates the most prevalent threats associated with mobile devices. Though, encryption does nothing to prevent a mobile device from being lost or stolen, *encrypting data at rest* mitigates the disclosure of data when a mobile device is lost or stolen. *Encrypting data in motion* mitigates the threats (e.g. eavesdropping) associated with the transmission of sensitive data over insecure public networks that mobile devices often connect to.

Encryption is important because, besides actually protecting confidential data from unauthorized disclosure, encryption has the added benefit of saving you the cost and embarrassment of having to notify potentially affected individuals when your mobile device is lost, stolen, confiscated

CONCLUSION

Mobile Computing Devices have changed the way companies do business, allowing a growing number of small and medium-sized firms to pay bills, conduct financial transactions with partners and sell goods and services to customers online. But Mobile Computing De-

vices have also made it more possible for sensitive company information and private customer information to be tracked and gathered and stolen online, including credit card numbers, social security numbers, bank account data, and other sensitive information that could be exploited if it ends up in the wrong hands. To combat these threats from fraud, hackers, virus, Trojan horse and worms, this report recommended the Intrusion Detection System security (IDS) and Encryption techniques. Until these countermeasures are implemented, mobile devices and data held in them are continuously at risk.

RECOMMENDATIONS

The following recommendations are necessary to prevent and manage security threats to mobile computing devices and data.

1. General policy. General policy restrictions of particular interest for mobile device security include the following:

i. Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.
ii. Restrict user and application access to the built-in web browser, email client, application installation services, etc.
iii. Manage wireless network interfaces (Wi-Fi, Bluetooth, etc.).
iv. Automatically monitor, detect, and report when policy violations occur.

2. **Data Communication and Storage**

Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of encryption.

Strongly encrypt stored data on both built-in storage and removable media storage. Removable media can also be "bound" to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.

Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party. A device often can also be configured to wipe itself after a certain number of incorrect authentication attempts.

3. **User and Device Authentication**

Require a password/passcode and/or other authentication (e.g., domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).

If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.

Have the device automatically lock itself after it is idle for a period e.g., 5 minutes).

Remotely lock the device, if it is suspected that the device has been left in an unlocked state in an unsecured location.

4. Applications

- Restrict which applications may be installed through white listing (preferable) or blacklisting.
- Install, update, and remove applications.
- Restrict the use of synchronization services (e.g., local device synchronization, remote synchronization services and websites).
- Digitally sign applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
- Distribute the organization's applications from a dedicated mobile application store.
- Limit or prevent access to the enterprise based on the mobile device's operating system version (including whether the device has been rooted/jailbroken) or its mobile device management software client version (if applicable). Note that this information may be spoofable.

REFERENCES

Avinash, K. (2012). Lecture Notes on Computer and Network Security: Classical Encryption Techniques. Purdue University, West Lafayette.

CISCO systems (2001). Beginner's guide to Network Security, Cisco Systems, Incorporated, San Jose.

Scarfone, K. and Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *Recommendations of the National Institute of Standards and Technology (NIST special publication).* Gaithersburg, MD 20899-8930

Kartik, K (2004). Project Report on Hackers: Detection and Prevention obtained from www4.ncsu.edu/-kksivara/sfwr4c03/ projects

La Polla, M., Martinelli, F. and Sgandurra, D. (2013). A Survey on Security for Mobile Devices. I*EEE Communications Surveys & Tutorials* **15 (1):** 446-471

Masoud N., Ronak, K. and Hojat, A. H. (2012). Mobile Computing: Principles, Devices and Operating Systems. *World Applied Programming* **2 (7):** *399-408*

Souppaya, M and Scarfone, K. (2012). Guidelines for Managing and Securing Mobile Devices in the Enterprise. National Institute of Standards and Technology (NIST) special publication

Randy, K. (1996). *Challenges of Mobile Computing.* Computer Science Division, University of California, Berkeley.

Yap, R. (2005). Home and business user computer security conference proceedings on Compendium on Information Network Security, (MCMC, 2005). Pp 19-26. Ixaris Sdn Bhd, Malaysia

Wikipedia, The Free Encyclopedia, (2004). [Online] Available at: http:// en.wikipedia.org/wiki/Hacker