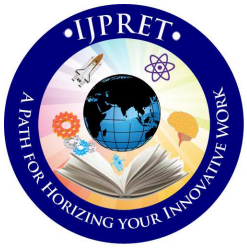
Research Article *ISSN: 2319-507X*
Akhil Jaiswal, IJPRET, 2013; Volume 1(8): 276-286 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY IN MOBILE COMPUTING

AKHIL M. JAISWAL[1], PROF. P. L. RAMTEKE[2]

1. M.E First year, H.V. P.M. C.O.E.T, Amravati.
2. Asst. Prof & H.O.D, H.V. P.M. C.O.E.T, Amravati.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Mobile Computing, Mobile Computing Security, Distributed Systems Security, Encryption.

Corresponding Author

Mr. Akhil M. Jaiswal

Abstract

The rise in mobile computing is explosive. Every day we see new statistics about mobile data growth, tablet adoption and smart phone use that exceeds the most aggressive forecasts. The productivity increases are a boon to enterprises and worker satisfaction. On the other hand, the proliferation of corporate data on a rapidly increasing variety of devices is a big risk for IT departments. In this paper, we discuss operational and security issues arising from the use of mobile components in distributed systems. We discuss security problems that can be applied to each one of the three main components of our mobile computing model. We try to overcome each of the threats that can hinder the integrity or efficiency of the of the system and which is intended to be implemented in a health care paradigm, where special conditions and emergency needs are imposing the use of services supported with mobile computing. Mobile devices provide significant productivity benefits; they also pose new risks to an organization's security by Network attacks. Enhancements in their power and their storage capacities make their physical loss much more damaging to the organization. As importantly, they become increasingly attractive to profit-motivated cyber criminals, who view them as both valuable and easy targets, especially during an economic downturn.

1. INTRODUCTION

The traditional network perimeter is eroding, or at least evolving. More and more users are relying on notebook computers and other mobile computing devices as their primary means of productivity. Organizations can realize efficiency and productivity gains by embracing mobile computing, but they also need to comprehend and defend against the unique security issues introduced by mobile computing. Mobile devices such as notebooks, personal digital assistants, Smartphone's and USB storage drives have become ubiquitous, and for an increasing number of employees, their jobs would be challenging without the mobility provided by these devices. Nevertheless, poorly managed mobile devices greatly increase the potential for security failures and information compromise. Stolen or lost notebooks, Blackberry's, USB sticks and other devices loaded with sensitive information, such as confidential e-mails, customer data and financial figures, can fall into the wrong hands. The loss of highly sensitive information and the potential associated media scandal is a huge problem in itself, but the impact might be greater — failure to protect certain information can be construed as a violation of regulations such as the Health Insurance Portability and Accountability Act. Desktop systems that exist inside the network perimeter have the benefit of antimalware and firewall protection implemented at the network level, as well as the physical security present at the office site. For mobile computing devices, organizations have to ensure the device can protect itself. Administrators need to implement solutions at the device level to safeguard against infection and unauthorized access, and protect the data contained on the device. In addition, administrators need to ensure that the organization's network is protected from potential compromise from the wandering device and wandering data. There are many ways that confidential or private data can leave an organization's network. Users may copy files to notebook PCs to take work home or copy data to portable storage devices, such as Universal Serial Bus flash drives, cell phones, digital cameras or MP3 players. Data can be intentionally or inadvertently sent out via e-

mail, which makes it tough to protect against information leakage. The best way to protect the ever-expanding network is to centralize data stores as much as possible, secure devices and USB ports, protect the network with firewalls and encrypt data. To maximize this, follow these simple, but practical mobile security best practices.

2. SECURITY PROBLEMS IN MOBILE COMPUTING

The first question for many IT leaders is how to cope with the rise in employee use of both corporate and personally owned mobile devices and the need to protect corporate data. Mobile computing, that is the ability of having computing and communication abilities on the move, depends on the existence of a suitable distributed systems infrastructure. So, security considerations of mobile computing can be seen as extensions to those of distributed computing. We will, therefore, examine the security issues in mobile computing on the basis of known security issues of information systems. Current thinking of information systems security is that the issues centre on confidentiality, integrity, availability, accountability and non-repudiation.

Security breaches in computer systems are related to the notions of exposures, vulnerabilities, threats and controls. Exposure includes disclosure of data, modifications of data, denial of legitimate access to computing. Vulnerability is a weakness in the security system that might be exploited to cause loss or harm. Threat to computing system is a circumstance that has the potential to cause loss or harm. Control is a protective measure that reduces vulnerability. The major threats to the security of a computing system are interruption, modification, interception and fabrication. Interruption takes place when an asset of the system becomes lost or unavailable. Modification happens when some unauthorized party has gained not only access but tampers with an asset. Interception takes place when some unauthorized party has gained access to an asset. Fabrication happens when some unauthorized party fabricates objects for a computing system

3. BEST PRACTICE: SECURE THE DEVICE

One of the first measures to protect a notebook computer is to set or enable a BIOS or hard drive password. This password is required when the computer is turned on and provides security at the hardware level before the operating system even begins to boot. Beyond that, antimalware, personal firewalls and wireless protocol encryption provide multiple layers of security for the mobile device. Even on desktop systems inside the network perimeter, most organizations have some sort of client-level antimalware and personal firewall solution in place. For roaming mobile devices that have to protect themselves, these security measures become even more imperative.

3.1 Download updates directly from manufacturers: Administrators need to take into consideration that the mobile device may go days or weeks without connecting to the organizations, but it still needs to get the latest signature updates. For mobile devices, the software should be configured to download updates straight from the manufacturers' servers rather than relying on internal servers on the organization's network.

3.2 Patch religiously: Monitor security patches released by the manufacturers of the software installed on your mobile devices. Just like on the desktop, discovering and installing security patches as soon as possible can significantly reduce the number of security incidents.

3.3 Manage connectivity mechanisms: Turn off Bluetooth when you are not using it. Do the same with other connectivity mechanisms. Use the highest possible security settings for wireless connections.

3.4 Password-protect the device: Most devices come with basic password protection for device use. Turn it on. If possible, install third-party applications that implement stronger authorization mechanisms than basic login passwords.

3.5 Use physical locks for notebooks: Physical locks will prevent miscreants from picking up your notebooks and walking away with them. Provide physical locks to your employees, and instruct them to use the locks whenever they use the notebooks outside the organization's premises.

3.6 Securely wipe devices before retiring them: Confidential information has been recovered from mobile devices sold through

online auction sites. Needless to say, most of those cases have been media disasters for the organizations involved. It is not enough to just delete the files before retiring devices — deleted files can be recovered easily. Destroying data completely from disks and making it unrecoverable is a difficult job. Use enterprise-grade disk-wiping software for all mobile devices before retiring them.

3.7 Use software designed to recover or destroy lost or stolen devices: Software applications are available that "phone home" or connect to monitoring services and report their location whenever they are connected to the Internet. Such applications can help in tracking, locating and recovering stolen or lost notebooks. Some devices have a remote-wipe feature that lets you remotely delete all data or perform a hard reset if they are lost or stolen.

4. SECURING USB PORTS

Portable media has always been an issue when it comes to securing data. If you do not have control over the data once it is stored on the portable media, how can you monitor or control where it goes or who has access to it? From a security perspective, the confidentiality and integrity of the data are both at risk once it becomes portable. When portable media meant 5.25-inch-wide square floppy disks that only stored 360KB of data, the risk wasn't quite as big. Not that 360KB isn't enough to store some sensitive or confidential information, but portable media today increases the risk exponentially. Now, users can store 8GB on a USB drive smaller than their thumb. This increases the risk both from the perspective that a user can house significantly more data on portable media, and from the perspective that the small thumb drives are easier to lose or misplace.

USB flash drives also pose a malware risk. Users may bring in USB flash drives that have been compromised and unwittingly infect the network with a virus, worm or other malware. Allowing users to bring in unauthorized storage devices and attach them to computer resources on the internal network exposes your organization to threats that bypass most, if not all, of the layers of security in place to protect the network. In addition to the risk of compromising data or transporting

malicious code, regulations require that certain types of information, especially personally identifiable information and customer data, be protected. Noncompliance or breaches of these requirements can be quite costly. It is important for organizations to understand the risk posed by USB flash drives and other removable media, and take proactive steps to manage users' ability to use them. The list below details some things you can do to lock down access for USB flash drives and protect your data from the risks of portable media.

4.1 Written policy: The first step in reigning in the use of USB flash drives and other portable media is to define your policy in a written document. Letting users know when, or if, or under what conditions the use of USB flash drives is acceptable will raise user awareness of the risks and reduce your exposure.

4.2 Restrict access: You can use Group Policy to restrict or deny access to prevent the computers on your network from reading data from or writing data to USB flash drives or other removable media entirely.

4.2Antimalware: You should have desktop-level antimalware software in place and ensure that it is updated regularly to detect current threats. Antimalware software will scan and detect threats before allowing a file on the USB flash drive to execute, and it provides protection against rogue USB flash drives infecting your whole network.

4.3 Encrypt data: To prevent the compromise of data in the event that a USB flash drive is lost or stolen, implement security measures on the USB flash drive itself, such as encrypting the data.

4.4 Rights management: By implementing Windows Rights Management Services (WRMS), you enable a much higher level of control and flexibility in managing access rights for the data on your network. WRMS allows you to control not only whether groups or individuals are able to view or modify a file, but also whether they can forward or print the file.

In addition to controlling access to USB ports, port management tools may also control a combination of FireWire, serial, printer and infrared ports, floppy/CD/DVD drives, and USB connected Wi-Fi or Bluetooth adapters. Some of the tools also

let you restrict access for MP3 media players, handhelds, and Compact-Flash and Smart-Media, as well as USB flash drives. With port-blocking software, you don't need to physically remove, change or block any of your computer hardware. Instead, simply install the software which may install small "agent" programs on each computer to be controlled and assign appropriate privileges to each end user. You shouldn't need any new hardware to run the administrative software, as one of your current Windows computers should be sufficient.

5. RESTRICT ACCESS WITH A PERSONAL FIREWALL

Mobile devices should also be protected by some form of personal firewall. Many security suites include a personal firewall component that can be used for mobile devices as well. As with the antimalware component, the firewall software on mobile devices should be configured to download updates from a publicly accessible source rather than relying on a connection to servers on the internal network. All data entering or leaving your organization will pass through the firewall. It can keep out unwanted intruders but also hamper critical connectivity. For example, your firewall may interfere with links to your website, access to other websites, remote virtual private network users, wide area network connections, Internet updates and Voice over Internet Protocol telephone calls. It may also interact with server certificates, web e-mail, handheld device connections and domain name system requests. To make sure you understand what you want your future firewall to keep out, thoroughly catalog and prioritize all your needs. There may not be a system within your price range that meets all of your diverse needs, and ultimately some things may need to be left out or more money must be budgeted. But there is another dark and insidious reason: maintaining VPN services.

Once a VPN is available, users expect it to work at all times from all locations, yet not all firewalls will accept a connection from the built-in Microsoft Windows client. Additionally, some firewalls on the remote end will block VPN connections. Meanwhile, your remote users may instinctively seek out locations around the globe where a VPN

connection is nearly impossible and then call in asking that you remedy the situation.

6. ENCRYPTION

Encrypting the entire disk or other storage is probably the most important thing you can do to prevent the theft of confidential information from a mobile device. An encrypted disk will be the final layer of defense in case a device falls into the wrong hands. Good encryption makes the data inaccessible to illegitimate users. Many commercial software applications do this automatically while remaining completely transparent to the user. Another, albeit weaker, approach is to encrypt individual sensitive files and folders instead of encrypting the entire disk. This tactic can be used in situations where encrypting the entire disk is not an option. Configure the devices to always use the highest available encryption standard for wireless connections. All connections to the internal organizational network must be over a virtual private network.

6.1 Encrypting Wireless Communications:

Mobile devices are commonly used to connect to wireless networks. The wireless network may be at the office, at home, in a hotel, or at the coffee shop on the corner. Wireless networking is convenient but also represents unique security concerns. Namely, anybody within range can intercept the data as it is beamed through the air.

To protect the data being transmitted to and from the mobile device, a wireless encryption protocol such as WPA2 should be used whenever possible. In addition, any connections from outside of the network should only be allowed via a secured connection such as an encrypted VPN tunnel. At public hotspots that are not configured for encryption, users must be aware that their data is unprotected and exercise caution in the types of sites they visit and the information they transmit across the network.

6.2 Encrypting the Data: If you read the news headlines, it seems as if there isn't a week that goes by without some security breach resulting from a lost or stolen notebook. The rise in the use of mobile computing devices brings with it a rise in the number of lost and stolen mobile computing devices and a need to implement some protection for the data

contained on the mobile device in the event it falls into unauthorized hands.

7. PROTECTING THE NETWORK

Eventually the wandering mobile device will return to base and want to connect with the home network directly. In order to protect the internal network from any system compromises or nasty malware infections the mobile device may have picked up while it was away, it is a good idea to have some sort of NAC (Network Access Control) solution in place.

NAC products will analyze the mobile device (and any other device connecting to the network) and ensure that it is patched, has the appropriate security software installed, running and up to date, and that it otherwise meets the organization's security policy requirements before allowing it to connect to internal network resources. Most NAC solutions offer an option between simply rejecting connections from noncompliant clients, or redirecting them to a site or server with information and resources to enable the device to become compliant.

NAC is more than a mere firewall that grants recognized computers access, or a password scheme that lets privileged members log on. At its best, NAC ensures that any notebook computer, server or handheld device trying to access the network has up-to-date antivirus software and meets specified security standards.

8. NETWORK ATTACKS

Mobile devices must also be protected against network-based attacks. Mobile devices (notebooks running off-the-shelf operating systems, for example) are vulnerable to the same varieties of attacks as any other computer system. Because they need to operate in foreign networks, such as coffee shops, airport kiosks or other hotspots, mobile devices have extra stringent security needs. They can't rely on the organization's firewall for protection. And the organization needs a means of managing security configuration, patch deployment and antivirus updates on their devices in the field. Even systems running special-purpose operating systems have some vulnerabilities. Forced de-authentication attacks, in which an attacker transmits packets intended to convince a mobile end-point to drop its network connection and reacquire a new signal, can

insert a rogue infrastructure device between a mobile device and the legitimate network.

9. SCALING SECURITY

The specific issues relating to security increases in complexity as various components within the mobile network increases in number and in their mode of interaction. The increase in the number of mobile units and their wider geographic distribution across regional and political boundaries will result in the need for the new specific solutions to mobile computing. The potential for the proliferation of mobile units may result in the need for increase in the size and the capacity of the infrastructure supporting the network. With the increase in number and geographic distribution of mobile units, some basic security functionalities will be required to be provided by the Mobile Support Stations and Location Servers. Examples of these functionalities include large scale key distribution and key management solutions, the provision of security and authentication across large geographic boundaries with minimal delay, and the secure management of parts of the mobile network which are under different management bodies. International security policies to regulate trans-border data flows will also need to be established as nomadic mobile units wander in and out of countries and sensitive regions. However, new solutions will also need to be designed and implemented if security is to scale properly in the mobile network.

10. CONCLUSION

The use of mobile resources in distributed environments provides important benefits. Serious security problems are derived, however, from the essential attributes of mobile computing. In this paper, we presented the general technological infrastructure, the mobile system model used for our experiments. Future work includes a systematic definition of at least two different security policies that are used by different backbone networks. Mobile units and their delegates are provoked to overcome those different situations and to complete their tasks. Further work also includes the implementation of special authentication and access control techniques.

REFRENCES

1. T. Imielinski and B. R. Badrinath, "Data management for mobile computing," SIGMOD RECORD, vol. 22, no. 1, pp. 34-39, 1993.

2. Douglas B. Terry, Systems Issues in Mobile Computing, Slides of a talk at Stanford University, 1994.

3. George H. Forman and John Zahorjan, The Challenges of Mobile Computing, IEEE Computer, April 1994, pp. 38-47.

4. Tomasz Imielinski and B. R. Badrinath, Mobile Wireless Computing: Challenges in Data Management.

5. Henning Koch, Lars Krombholz, and Oliver Theel, A Brief Introduction into the World of 'Mobile Computing'.

6. Campbell, R.; Sturman, D. and Tock, T. (1994) Mobile Computing, Security and Delegation. International Workshop on Multidimensional Mobile Communication, Japan.

7. The WWW Virtual Library: Mobile and Wireless Computing. A weekly updated index of ongoing projects on mobile and wireless computing.