Mobile and Wireless Security Challenges

[1] Prof. Shalaka Kulkarni, [2] Prof. RupaliThorat

[1]Asst. Professor, [2]Asst. Professor
[1]MCA Department,[2]MCA Department

[1] D. Y. Patil Institute Of Management, Ambi,Talegaon-Dabadhe, India

Abstract:Organizations heavily depend upon mobile devices like smartphones, PDAs, laptops and USB drives, to increase productivity & reduce the cost of doing business. With this, important data is easily available to employees at remote places. This small size, large storage capacity and network connectivity of mobile devices make them susceptible to loss, theft and misuse if not properly protected. As a result, unsecured devices can pose a risk to the entire enterprise.

This paper proposes a solution that will help the user to cope with security problems like virus infection, information stealing, using different technologies like biometric authentication, firewalls, data encryption, electronic signatures and awareness programmes, to utilize the mobile devices in secure fashion.

Keywords: PDAs, USB Drives, Threats, viruses, PenOp, Bluetooth, Biometrics.

I. Introduction

The paper is based on secondary data references given at the end. Handheld computing devices are among the most creative forms of technology in the business workplace. Personal Digital Assistants (PDA) are likely to use for note-taking applications as providing a wireless link to the office e-mail server via packet radio services. Mobile phones not only provide traditional voice communications and text-messaging (SMS), but also a wireless link to file resources and electronic mail. Greater software compatibility and low cost consumer devices have made the technology available to a wider audience, including confidence miscreants. But with developing technology security threat is also increased.

The battle between technology and security seems to be never-ending. Most of the users store their confidential and critical information on their handheld devices, it may be personal or company's data, without enabling the basic security features present on the system.

Information such as customer contacts, e-mail details, passwords and bank account details are getting stored in devices without much consideration to security.

As a result, a lost PDA or smartphone with no protection makes easy pickings for thieves, hackers or competitors with regard to corporate information. This could have an impact on customer confidence and damage a company's reputation.

In order to secure the device from misuse or attack and to meet regulatory requirements, IT organizations must give consideration to the wireless and centralized deployment of device security policies. These policies include measures regarding authentication, encryption of data, prevention from virus infection and device featuredisablement. Other solutions could be creating awareness, conducting training, and using passwords.

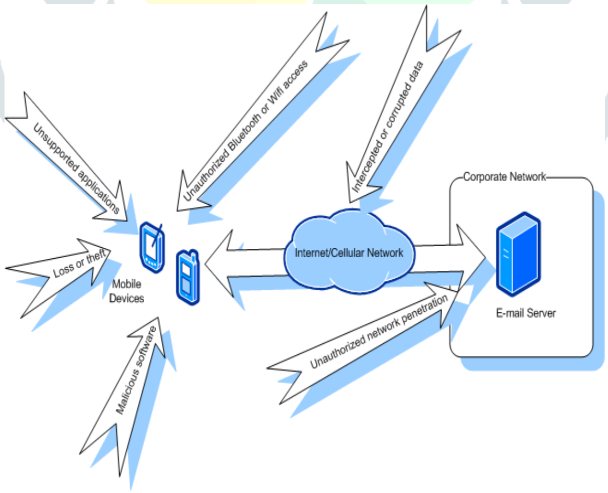
Unsupported applications
Unauthorized Bluetooth or Wifi access
Intercepted or corrupted data
Corporate Network
Loss or theft
Mobile Devices
Internet/Cellular Network
E-mail Server
Malicious software
Unauthorized network penetration

Figure 1 issues in mobile devices' security

II. The Risks in Mobile Computing:

Mobile devices such as notebooks, personal digital assistants, smartphones 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. Mobile Computing Devices contain "lots" of memory and they are highly portable and frequently unprotected. In other words, they are relatively easy to steal or lose, and unless precautionary measures are taken, an unauthorized person can gain access to all the information that is stored on them, he can quickly and silently copy the data from your unprotected device. In the worst case, an intruder can install a spyware program that secretly captures the owner's keystrokes such as credit card numbers, passwords and other sensitive information. The loss of highly sensitive information with the potential associated media scandal is a huge problem in itself, but the impact might be greater –failure to protect certain information can be constructed as a violation of regulation such as the health Insurance Portability and Accountability Act.

III. Security Issues:

Since radio signals travel through the open atmosphere where they can be intercepted by individuals who are constantly on the move. Thus it is difficult to track down. Secondly, wireless solutions are, almost universally dependent on public-shared infrastructure where user has much less control of, and knowledge about the security discipline employed. It may possible that hackers scan airwaves and capture cellular ID numbers for misuse.

While it may not be possible to make any system completely secure, there are certain steps that can be and must be taken to ensure that the risk of security breaking is minimized.

- **Virus attack:**

Mobile devices are increasingly coming under attack from viruses. Mobile handsets with Wi-Fi cards are prone to these attacks as they connect to a public network and, at the same time the organization's network. Other services on mobile phones that might make them vulnerable include the ability to open e-mail attachments and removable storage cards. Due to the rising popularity of data-centric mobile phones and PDAs, these devices could become an attractive target for virus writers in the future.

- **Stealing Information:**

It is common for individual's intention on industrial spying to gather up vast quantities of information by placing small scanners at appropriate locations and searching with very powerful algorithms. Credit card numbers and bank account numbers are among the most common types of information stolen.

- **Security in Broad Sense:**

Securing information from unauthorized access is a major problem for any network. Wireless Security, in a broad sense, focuses on network security, system security, information security, and physical security. It involves multiple technologies that solve numerous authentication, information integrity, and identification problems. It includes – firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection, and VPNs.

IV. Designing for Security in Mobile Computing

There are several steps that can be considered while designing security in mobile computing networks and applications. Some of them are,

- **Authentication:**

One of the first strategy to protect a mobile device is to set password. The password is required when the computer is turned on and provides security at the hardware level before the operating system even begins to boot. The alternative is: Biometric authentication.

- **Biometric authentication:**

Biometric security is emerging as a promising solution to the above problems Biometrics-based authentication schemes use biological traits such as fingerprints, face, iris, hand-geometry, and palm-prints, etc., which are unique for any individual.

There are several scenarios in which behavioral Biometrics can be used:

I. **Log-In Verification :**

Whenever the user logs to his local computer or to a service on the internet or the intranet by typing a user name and password these are monitored and verified.

II. **Continues Verification**

After the user performs login to the computer or to the web service, his/her entire interaction, through keyboard, mouse activities are continuously monitored to verify that it remains him.

III. **Password Reset:**

When the user has forgotten his credentials for login, the user is asked to perform a behavioral biometric verification process /task instead of contacting a telephone or visiting the office of the administrator.

- **Use 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. All data entering or leaving your organization will pass through the firewall. It can keep out unwanted intruders but also hamper critical connectivity If the device is a laptop computer, keep the patches up to date. This reduces the possibility that a system can be compromised by an attacker, or some kind of malware.

Use of a personal firewall is strongly recommended. It will effectively defend a computer from many of the most pervasive and dangerous network attacks.

- **Data Encryption Process in Mobile Computing**

Encrypting the entire disk or the storage is probably the most important thing you can do to prevent the theft of confidential information from a mobile device. The most reliable way to prevent people from viewing confidential data is to encrypt it. If your devices store Category 'A' (confidential and critical) data, you need to make sure that this data is encrypted.

Encryption is the translation of data into a secret code. It is the most effective way to achieve data security. Encryption involves scrambling digital information-bits with mathematical algorithms and is the most potent protection available against security intrusions into wireless and wire line communications. Different encryption schemes have been proposed and implemented.

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.

Unfortunately, the last segment i.e., between the end user device and the cell, or base station, cannot be encrypted and this is where all the theft occurs. For end-to-end security, the only answer is to build encryption/decryption capabilities into the end user device itself. Unfortunately, this can be done only with end user devices on digital cellular networks and digital cellular is still not everywhere.[i]

Encryption Key Types

There are three types of keys used in encrypting data:

1. A private key known only by the sender and the recipient
2. A private/public key combination
3. A one-time key

In private-key systems, the two parties have a secret key which they use to encrypt and decrypt data.

The private/public key combination is more secure. However, in this scheme, the recipient's public key, available to all who need it to send encrypted data is used to encode information for transmission. The recipient uses a private key associated with the set to decode the information.

The one-time key method is based on the generation of a new key every time data is transmitted. A single-use key is transmitted in a secure (encoded) mode and once used, becomes invalid. In some implementations, the central system will not issue a key for a new connection until the user supplies the previously used key. [v]

The two basic approaches are:

1. To encrypt individual files and/or folders that contain confidential information, or
2. To encrypt the entire disk or device.

Each of these approaches has some advantages and disadvantages.

The main advantage to approach (1) is that it's relatively easy and straightforward. Microsoft and Apple provide OS-level support for this and several third-party vendors do as well. Third-parties also provide encryption software for Palm and Pocket PC devices.

The main disadvantage to approach (1) is that it can require some discipline to ensure that all confidential data is created and stored only in encrypted locations (including when it is backed up).

Full disk encryption can be more complicated to set up and generally requires a third-party solution.

a) Electronic Signatures in Wireless Applications

Electronic signatures can be used to ensure that users are who they claim to be. With the appropriate hardware and software, like PenOp from Peripheral Vision in the U.K., a system can literally demand a valid signature. While the primary use of such software is in contract-related applications (mortgages, loans, etc.).

PenOp is based on a biometrics signature-verification technique. It supports a variety of signature capture methods, ranging from low cost digitizers attached to desktop PCs, through to hand-held PDAs or pen computers.

b) While using wireless connectivity features (e.g., Bluetooth) make sure the device's security settings are set "as strong as possible".

Even though the state of wireless security has improved significantly in the last few years, it is recommended that this technology still be regarded with doubt. Thus, never send or receive sensitive data over a wireless link unless another more secure end-to-end encryption technology is also being used. Examples of more secure technology include: SSL, SSH, and VPNs. All modern web browsers support SSL.[iii]

c) Bluetooth uses the safer algorithm for authentication and key generation

The initialization key and master key are generated using the E22 algorithm. The E0 stream cipher is used for encrypting packets. This makes listen to private conversation on Bluetooth-enabled devices more difficult.

d) Awareness programmes to the rescue

The first step towards security in a mobile environment starts with the framing of policies, followed by an awareness programme for users.

Awareness among users is required. Create awareness so that the user is fully aware of the type of data he is carrying in his device, the threats associated with this, and so on. Once the user is aware, the next step is the configuration of devices and having a centralized control.[iv]

V. Application:

As the security is improving day by day this mobile computing is used for storing confidential and curial information of business and individuals.

1. Building the Mobile Business with a Unified Wireless Network is easy with secured computing. With different mobile devices employees, customers, agents at remote location can be attached to company's database and updated information is obtained at every time. With this, decision making is happening at Internet speed. Providing information in real time helps the business to create sustainable competitive advantage.
2. With biometric authentication technique, notebooks may be used in security departments also, where security is must.
3. With security, in medical science, mobile computing solutions revolutionize the way medicine is delivered and practiced. With mobile solutions, physicians can access patient information quickly, efficiently and securely from any location, at any time. These solutions will help improve patient safety, reduce the risk of medical errors and increase physician productivity and efficiency.
4. Mobile devices are emerging as the stethoscopes of the 21st century. Physicians nationwide are independently purchasing mobile devices with standalone clinical solutions to retrieve accurate, up to date information to help diagnose illnesses determine treatment protocols and prescribe medications, as they now believe on mobile computing.

VI. Future Direction:

With the introduction of Biometric authentication techniques by Lenovo's notebook, the same security system shall be used for other handheld devices like PDAs.

Like fingerprint and facial reorganization, voice and retina scan reorganization also get applied for the mobile devices.

Day by day new antiviruses are created to prevent form viral and other malware. All this may lead to threat free computing in future and use of mobile devices in different areas.

Cost will be one important factor which may increase with involvement of secured technology. Users will have to pay more money on technologies like biometric authentication, encryption/decryption, electronic signatures and firewalls. And of course user will pay it, because security is more important than money.

VII. Conclusion

As with any form of modern technology, the security risk is proportional to the sensitivity of data stored on it. For any corporate executive, this data may include everything from remote access passwords, to intellectual property and details of sensitive business matters.

Including mobile platforms as part of the overall security program is a healthy step to averting threats that are alarming on the horizon.

There are some policies available to secure mobile computing, but the need is to start an awareness programme to make the new policy known within and outside the organization.

Awareness seems to be the best way to avoid security issues. IT organizations and Government should create security awareness through posters, mailers, TV advertisements, and e-learning sessions.

Cost to secure the data will increase with new technologies like biometric authentication, and others, and user should be ready to pay for this.

Implementing the appropriate technical controls, with continuous updates, combined with user awareness and education are the most effective weapons in fighting this ongoing battle.

References:

[1] www.information-age.com
[2] www.wikipedia.org
[3] www.expresscomputeronline.com
[4] www.cs.yale.edu
[5]http://securlinx.blogspot.in