WIRELESS NETWORK SECURITY
UNIT – III (PART – I)
CHAPTER 4
Security Considerations for Wireless Devices

INTRODUCTION

Most wireless devices are designed to be small and mobile. Many times these devices are quite expensive. The security of these devices and the data contained on them is important. Keeping the devices secure can prevent theft or loss that may result in a needless expense or a compromise of a wireless application. Securely storing data on wireless devices can prevent information leakage or unauthorized access to wireless network resources.

WIRELESS DEVICE SECURITY ISSUES

This section considers the general security issues that are common to m ost wireless devices. If we examine many common wireless applications, we will find that the devices generally fall into four categories: laptops, personal digital assistants (PDAs), wireless infrastructure (bridges, access points, and so on), and mobile phone handsets. After examining the security issues that apply to all wireless devices, we will discuss device specific issues in detail.

A) PHYSICAL SECURITY : Mobility is one of the key enablers for wireless applications. However, because wireless devices are mobile, they are very easy to lose or steal. Therefore, the possibility of theft and loss of wireless devices must be an important factor when designing a wireless application. Taking some simple precautions for the physical security of the devices can drastically reduce the loss of wireless devices and thus reduce the overall cost of a wireless application.

Be Aware

A little common sense goes a long way in protecting devices. People want to steal things. Laptops are common targets for thieves because they are very small and valuable. Laptops are also easy to sell on the black market or at online auctions because there is a large demand for them. Airports are a common place for laptop theft. Thieves are aware that many business travelers are equipped with laptops. Thieves might also strike when a traveler is being questioned, when a bag is being searched, or when a traveler is required to repeatedly go through the metal detectors or be searched by hand-held metal detectors. Airport restrooms are another common place where thieves often strike unsuspecting

travelers. Some travelers will turn their back on their luggage while using the facilities. Some thieves have been known to grab bags out from under restroom stalls while the traveler is occupied. The thief may quickly disappear into a crowd before the victim can even see him or her. Be sure that your business travelers are aware of these threats so they can take reasonable precautions to prevent theft.

Lock It Up

If your environment is static and your devices cannot travel, then use device cables to lock them down. Banks even do this with their pens. You can also utilize security cameras to monitor hostile environments. Most laptops and PDAs can be secured with an inexpensive cable to a large object such as a desk or table. Infrastructure devices such as access points can be bolted down or locked in a container to prevent theft.

Uniquely identifying devices may help with the inventory and recovery of devices. This can be done with labels, distinguishing marks, or asset tags. Checking out devices to employees or customers and making them financially responsible for the safety of the device is an effective way to make sure the devices are returned. Tracking the serial numbers of devices and keeping receipts may prove to be valuable aids in recovering equipment that has been seized by law enforcement.

B) Information Leakage

Most wireless devices contain data storage capabilities. Some wireless devices are designed to store application data during intervals between wireless connectivity to the network. For example, laptops are commonly configured to store e-mail for offline reading and sending. The storage capabilities of wireless devices are constantly expanding and are capable of storing large amounts of very sensitive data. Reasonable steps must be taken to secure sensitive data. The loss of data may bring about additional expenses for recreating the data or recovering the loss of intellectual property to a competitor. In order to make a decision of what reasonable steps to take to secure a wireless device, consider the amount of sensitive information that may be contained in the device. A single laptop with a small hard drive can contain large amounts of data including customer lists, employee information, intellectual property, source code, password lists, calendars, e-mail, or current projects. PDAs normally have an address book, calendar, and to-do list and can be used to store documentation or execute applications.

Cryptographic keys may also be stored on wireless devices. Many laptop users have been known to write passwords on a sticky note or use the Remember Password options common to many applications. A good backup policy may reduce the amount of effort needed to recover from a lost device. Frequently, business travelers will not back up their data, which leads to a large loss when the data is lost, stolen, or destroyed.

C) Device Security Features

Some devices contain password-protection or lockout options that are supposed to keep data safe. These features may keep an unskilled attacker out, but most of them can be easily defeated when an attacker gains physical access to the device.

Palm-OS-based PDAs have a password-protection feature that can be used in various ways to protect data. Research has proven that the password can be recovered by using a modified HotSync program to another PDA or desktop computer. Embedded debug features can even be used to retrieve that password out of a locked device.

Mobile handsets normally have a lockout feature to prevent unauthorized access that uses a password or Personal Identification Number (PIN) code provided by the user. Many mobile handsets have factory or master passwords that can be used to completely bypass any security mechanism.

Many programs for PDAs and laptops are used for secure data or password storage. Security researchers have found problems with some of the programs that use poor encryption methods that enable the data to be retrieved by an attacker. In most cases, the data for these programs is unlocked by providing a password.

D) Application Security

With client-side security, security features of a client/server application are enforced or enabled by the end user's client software. For example, consider an e-commerce site that uses a web browser for purchasing products. During the final checkout process, the client often submits information to the server, such as a credit-card number, shipping address, and other processing information. Sometimes the server will also pass the price to the client in a hidden field and rely on the client to submit the price back to the server for final payment processing because many times the checkout process may involve the use of many servers.

Another common mistake that programmers make is embedding passwords

or cryptographic keys into an application. This leads to many problems with the application. Malicious users may reverse-engineer the program to reveal the passwords or secret cryptographic keys. Network attacks may sniff a session to reveal embedded passwords that can be used for malicious purposes.

Another fault in using client-side security is that the only thing required to access a sensitive application is the client software. In this case, a lost or stolen wireless device may be used to access an application. As a result, a complete rewrite of the application and distribution of the new application may be necessary.

DETAILED DEVICE ANALYSIS

1. **LAPTOPS :** Laptops are common wireless devices in corporate and Small Office Home Office (SOHO) wireless networks. The low cost of wireless network gear has made wireless laptops a common appearance in the corporate enterprise and in home environment

   PROBLEMS :

   The smaller the laptop, the easier it is to steal, and thus the greater the loss to the company. The loss of data encryption keys, such as Wired Equivalent Privacy (WEP) keys, soft tokens, remembered passwords, or private keys (such as Pretty Good Privacy [PGP] keys), is a large problem that needs to be considered when creating an application. Once an attacker has obtained physical custody of a laptop, most security mechanisms can be circumvented. The attacker can install his or her own software on the laptop. Once the attacker controls the software, most software-based security mechanisms can be defeated.

   The mobile nature of laptops also means that they are likely to connect to other networks that are not protected by the corporate firewall. These may be Internet connections, customer networks, vendor networks, or other public networks such as hotels or trade shows where competitors may located. The digital security of laptops in these environments needs to be considered.

   SOLUTIONS :

   Because laptops are frequently stolen, securing and backing up the data on the laptop is important. Data encryption programs can be used to secure files or create encrypted volumes on hard drives to keep data secure. These encrypted volumes normally require a private key protected by a password for decrypting the data. Some e-mail programs also offer to store local mail in an encrypted format, although not all e-mail data store encryption is well implemented.

The storage of passwords and keys, such as WEP keys, on laptops should be considered. Some wireless cards store WEP keys in the Windows registry in clear text. If you are relying on WEP for security (which is not recommended), you should consider choosing a card that does not store the WEP keys on the machine, but rather stores them in nonvolatile random access memory (NVRAM) on the Personal Computer Memory Card International Association (PCMCIA) card. Also, if private keys are stored on the machine, such as PGP keys or host keys for Secure Shell (SSH), these should be password-protected and revoked as soon as a laptop is detected to be missing by the system administrator.

Information leakage can also occur when laptop users are in a public environment. Airplanes are a common place for business travelers to do work. Other travelers on the plane could easily "shoulder-surf" the user and read sensitive information directly off the screen. Many laptop users will also likely connect to the Internet unprotected via a dial-up or broadband connection. Therefore, HIDS, personal firewall software, and antivirus software are recommended.

Disabling boot up from a floppy or CD will help prevent an attacker from installing his or her own software or booting to another operating system to access sensitive data.

The basic input/output system (BIOS) and hard disk passwords can help prevent a thief from using a stolen laptop or at least accessing the data. Make sure blank passwords are not used for any accounts and that unnecessary accounts have been disabled. These tips cannot prevent a skilled attacker or thief from compromising data on a laptop when he or she has physical custody. Many thieves are not interested in the data that may be contained on a stolen device.

2. PERSONAL DIGITAL ASSISTANTS (PDAs):

Many types of PDAs are used in wireless applications. Some are used in a corporate environment. Other specifically designed PDAs are used in medical, industrial, or airport environments. Most special-purpose PDAs run Palm OS or Windows CE and have additional features such as internal wireless cards, barcode scanners, long-life batteries, or magnetic-strip readers. The primary feature of these devices is that they are easy to use.

PROBLEMS :

Most PDAs have a number of input mechanisms. These include wireless cards, infrared ports, memory devices, serial connections, universal serial bus

(USB) connections, or Bluetooth. All of these input mechanisms are attack vectors that can be used to compromise the PDA. In addition, most PDAs have been designed to provide application developers with easy ways to debug applications. These debug interfaces can compromise the device.

PDAs suffer from the same kind of attacks that many Internet applications are vulnerable to—namely, buffer overflows and format string attacks. Because PDA programmers are not used to programming for security, many of these vulnerabilities will probably continue to exist. Data on a PDA can be easily compromised by an attacker.To make matters worse, memory devices can be copied or backed up without leaving any trace so the user might not be aware that the data on the PDA has been compromised.

SOLUTIONS:

One way to secure the data that a PDA accesses is by not storing it on the PDA. This can be accomplished by having the PDA pull information off a secure back-end database or by using a Java or thin client application. Then the data is input from the PDA and displayed on it, but it does not require remote storage on the PDA. The drawback to this is that the application will only be accessible in the wireless coverage area.

As mentioned multiple times in this book, do not rely on client-side security. Client-side security is any mechanism that relies on trusting the client, which may be in malicious hands, to enforce a security mechanism.

Encryption keys should be rotated on a regular basis. If a key is compromised, the window of attack can be reduced. Many PDAs have password lock features.We discussed that these features cannot be relied upon, but they will slow down an attacker. Sometimes an attacker will only have a limited time with the compromised device. The PDA lockout features will also make it more difficult for a thief to recover an application or data, and the thief can just reset the PDA and erase all the data to be able to use the stolen device.

Historically, the PDA-based encryption mechanisms have been found to be vulnerable to a number of attacks, but they will slow down an attacker and may obscure the data from an attacker who was only after the device. If speed is a problem, consider using Elliptic Curve Cryptography (ECC) for all sensitive data. Even casual PDA users may store sensitive data, such as passwords or credit-card numbers. In addition to encrypting the data, always deploy a power-on and screen-lock password.

3. WIRELESS INFRASTRUCTURE DEVICES:

This section discusses the security issues pertaining to devices used for the infrastructure of wireless networks. This section primarily focuses on wireless networking components, such as access points and bridges, but the principles can be used for a variety of applications.

PROBLEMS :

Many wireless infrastructure devices are deployed in hostile environments. These environments include public places such as coffee shops, airports, or outdoors at the corporate campus. These devices are expensive and a target of thieves. Others may want access to these devices to either disable security features like the Extensible Authentication Protocol (EAP) or WEP, or reveal information about the configuration in order to compromise the network.

SOLUTIONS :

Management functions can be secured on a wireless infrastructure device by using secure protocols to access it, such as SSH, Secure Sockets Layer (SSL), or Simple Network Management Protocol version 3 (SNMP v3). In addition to using the secure management protocols, if available, insecure protocols such as telnet, cleartext Hypertext Transfer Protocol (HTTP), and SNMP v1 should be disabled.

Inexpensive terminal servers can be used to manage the access points with the added benefit of out-of-band access and can also be used for other networking gear such as routers, modems, and switches that are in the same location. Do not forget to bolt down or lock up equipment in a hostile environment, especially if it is outside. Keeping access points mounted in high places can help prevent theft.

4. HANDSET DEVICES :

The security considerations for mobile phone handsets should mirror their larger siblings (laptops and PDAs). The problems that the security research community has discovered to date in mobile handsets are similar to those in any other mixture of hardware of software.

PROBLEMS:

Mobile handsets are vulnerable to the same types of digital attacks that have been discussed for the other types of wireless devices. These attacks Normally take advantage of buffer overflows, format string attacks, or parsing errors, and enable an attacker to run code on the compromised device.

An example of this is the short message service (SMS). Recent attacks have shown that the SMS handlers in mobile handsets are vulnerable to attacks resulting in a denial of service (DoS) or execution of commands on the handset. These problems have affected a large number of vendors including Nokia and Siemens, and more open platforms like PDA-based handsets.

In addition, a number of Subscriber Identity Module (SIM) manufacturers have included methods of developing additional proprietary functionality and deploying these applications via a wireless interface usually provides SMS to the relevant subscriber base.
Certain implementations rely on the Data Encryption Standard (DES); however, the same DES key is used for each SIM. This is a very good example of the potential to introduce and execute malicious code on a mobile platform from a totally wireless attack vector.

SOLUTIONS:

Always use a password or the handset-equivalent PIN. SIM PIN can be used to secure phones based on the Global System for Mobile Communications (GSM). To make the best use of this feature, be sure to use all the PINs available. Also, make sure that you note your International Mobile Equipment Identity (IEMI) (the serial number of your phone) and store it in a safe place.
When using your handset to send sensitive information, be sure to encrypt it. When using WAP to send credit-card numbers or other personal details, make sure that you are using Wireless Transport Layer Security (WTLS) (SSL-secured connections). In addition, a large number of attacks against the algorithms used within GSM enable an attacker to clone the SIM of the phone. These attacks normally require physical custody of the phone so be sure to keep your phone secure and notify your mobile operator in the event of loss or theft.

THE END