BCC 301 Cyber Security Notes Unit 2

cybersecurity (GL Bajaj Institute of Technology and Management)

BCC 301 Cyber Security Notes Unit 2

Table of Contents

1. CYBER CRIME: Mobile and Wireless Devices-Introduction

1.1 Wireless and Mobile Device Attacks

Wireless and mobile devices have become ubiquitous in today's society, and with this increased usage comes the potential for security threats. Wireless and mobile device attacks are a growing concern for individuals, businesses, and governments.

1.1.1 Common types of Wireless and Mobile Device Attacks

- **SMiShing**: Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links.
- **War driving** : War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.
- **WEP attack**: Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption. WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.
- **Bluejacking:** Bluejacking is used for sending unauthorized messages to another Bluetooth device.
- **Replay attacks**: In a Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.
- **RF Jamming**: Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.
- **Wi-Fi Spoofing**: Wi-Fi spoofing involves setting up a fake wireless access point to trick users into connecting to it instead of the legitimate network. This attack can be

used to steal sensitive information such as usernames, passwords, and credit card numbers.

- **Packet Sniffing**: Packet sniffing involves intercepting and analyzing the data packets that are transmitted over a wireless network.
- **Malware**: Malware is software designed to infect a device and steal or damage data. Malware can be distributed through email attachments, software downloads, or malicious websites.

Wireless and mobile device attacks can have severe consequences, including the theft of sensitive data, identity theft, financial loss, and reputational damage. To protect against these attacks,

- users should always use strong passwords,
- keep their devices and software up-to-date,
- avoid connecting to unsecured networks,
- and use reputable app stores.
- Businesses should also implement security measures such as firewalls, intrusion detection systems,
- and employee training to protect against wireless and mobile device attacks.

2. Proliferation of Mobile and Wireless Devices

- Today, incredible advances are being made for mobile devices.
- The trend is for smaller devices and more processing power.
- choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities.
- A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls.

3. Trends in Mobility

- Mobile computing is moving into a new era, which promises greater variety in applications and have highly improved usability as well as speedier networking.

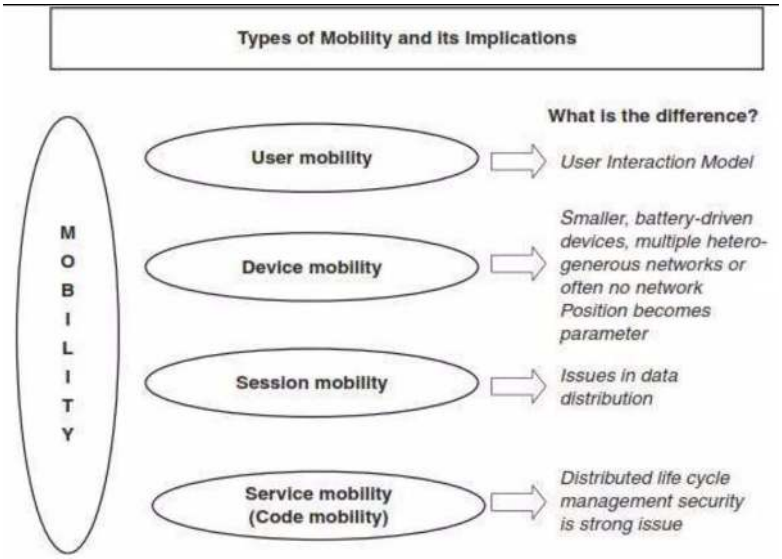

Figure 3.1 Trends in Mobility

4. Credit Card Frauds in Mobile and Wireless Computing Era

- These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M- Commerce) and mobile banking (M-Banking).
- Credit card frauds are now becoming commonplace given the ever- increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.
- Mobile credit card transactions are now very common; new technologies combine lowcost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.
- Today belongs to "mobile computing," that is, anywhere anytime computing.
- Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.
- It is most often used by businesses that operate mainly in a mobile environment.

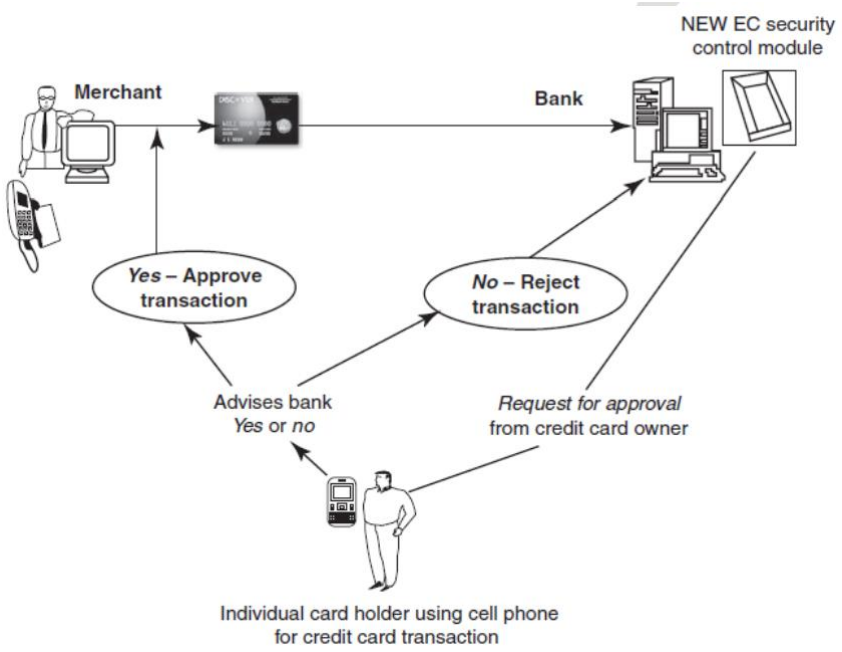

Figure 4.1 Closed loop environment for wireless. Source: Nina Godbole (2009), Information Security. Wiley India.

4.1 Prevention from Credit Card Frauds

- Put your signature on the card immediately upon its receipt.
- Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
- Change the default personal identification number (PIN) received from the bank before doing any transaction.
- Always carry the details about contact numbers of your bank in case of loss of your card.
- Carry your cards in a separate pouch/card holder than your wallet.
- Keep an eye on your card during the transaction, and ensure to get it back immediately.
- Preserve all the receipts to compare with credit card invoice.
- Reconcile your monthly invoice/statement with your receipts.
- Report immediately any discrepancy observed in the monthly invoice/statement.
- Destroy all the receipts after reconciling it with the monthly invoice/statement.
- Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
- Ensure the legitimacy of the website before providing any of your card details.

- Report the loss of the card immediately in your bank and at the police station, if necessary.

4.2 Types and Techniques of Credit Card Frauds

4.2.1 Traditional Techniques

The traditional and the first type of credit card fraud is paper-based fraud – application fraud, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) to open an account in someone else's name.

Application fraud can be divided into

- **ID theft**: Where an individual pretends to be someone else
- **Financial fraud**: Where an individual gives false information about his or her financial status to acquire credit. Illegal use of lost and stolen cards is another form of traditional technique.

4.2.2 Modern Techniques

- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing.

5. Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity:

- first, on the hand-held devices, information is being taken outside the physically controlled environment and
- second remote access back to the protected environment is being granted.

As the number of mobile device users increases, two challenges are presented:

- at the device level called "microchallenges" and
- at the organizational level called "macrochallenges."

Some well-known technical challenges in mobile security are:

- managing the registry settings and configurations,
- authentication service security,
- cryptography security,
- Lightweight Directory Access Protocol (LDAP) security,
- remote access server (RAS) security,
- media player control security,
- networking application program interface (API) security, etc.

6. Registry Settings for Mobile Devices

Registry settings are a key component of the operating system, used to store configuration information for various software applications, hardware devices, and system settings. The registry is like a giant database that keeps track of all the settings and preferences on your computer. Each program and device that you install or use on your computer has its own set of registry settings, which are stored in a hierarchical structure of keys, subkeys, and values.

A key is a container that holds configuration information for a particular software application, hardware device, or system setting. Subkeys are keys that are located within other keys, forming a nested structure. Subkeys can be created within other subkeys as well. Values are individual pieces of information stored within keys and subkeys. Each value has a specific name, data type, and data content. Values can be edited or deleted to modify the configuration/settings.

Registry settings are used in a variety of scenarios to manage software applications, hardware devices, and system settings on Windows computers. Here are a few common use cases:

Customizing application settings: Many software applications store their configuration settings in the Windows Registry. Users can modify these settings to customize the behavior of the application.

Troubleshooting application issues: For example, if an application is crashing on startup, you might need to delete its registry key to force the application to create a new key with default settings.

Managing hardware devices: Drivers for hardware devices such as printers, scanners, and sound cards often store configuration information in the registry.

Configuring system settings: The Windows Registry stores many system settings that control the behavior of the operating system itself, such as startup and shutdown behavior, security settings, and network settings.

Automating software deployment: IT professionals can use registry settings to automate the deployment of software applications across multiple computers. By modifying the registry settings on a central server, they can ensure that all computers in the network have the same configuration settings for a given application.

The Registry Settings Configuration enables you to modify the values in the registry centrally and for several users.

7. Authentication Service Security

There are two components of security in mobile computing: security of devices and security in networks.

- A secure network access involves mutual authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services.
- No Malicious Code can impersonate (imitate) the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.
- Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.
- Authentication services security is important given the typical attacks on mobile devices through wireless networks:
    - DoS attacks,
    - traffic analysis,
    - eavesdropping,
    - man-in-the middle attacks
    - and session hijacking.

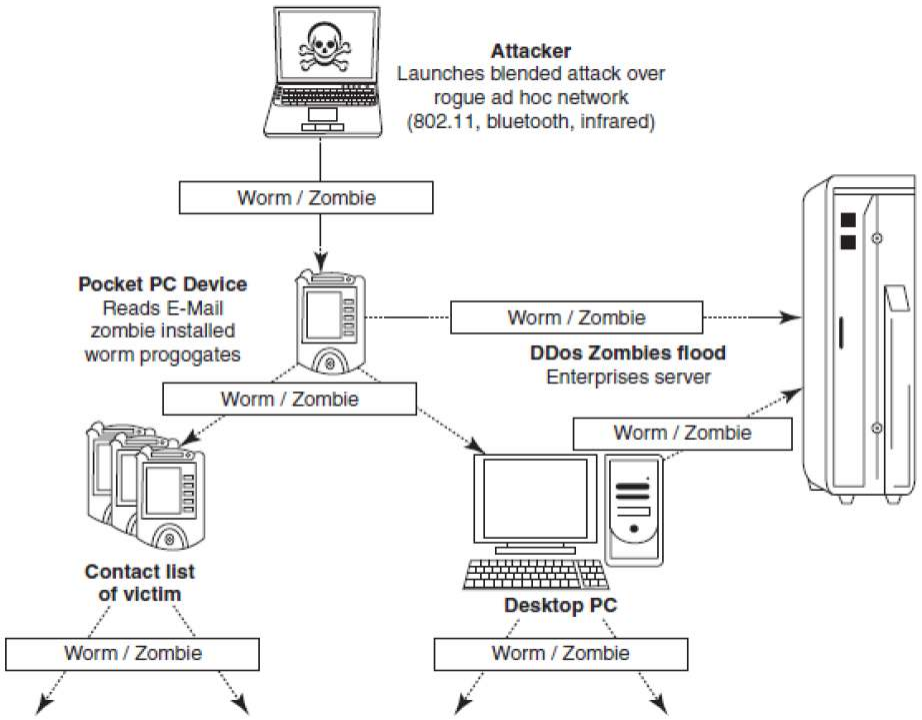

Figure 7.1 Push attack on mobile devices. Source: Nina Godbole(2009), Information systems security, Wiley india.

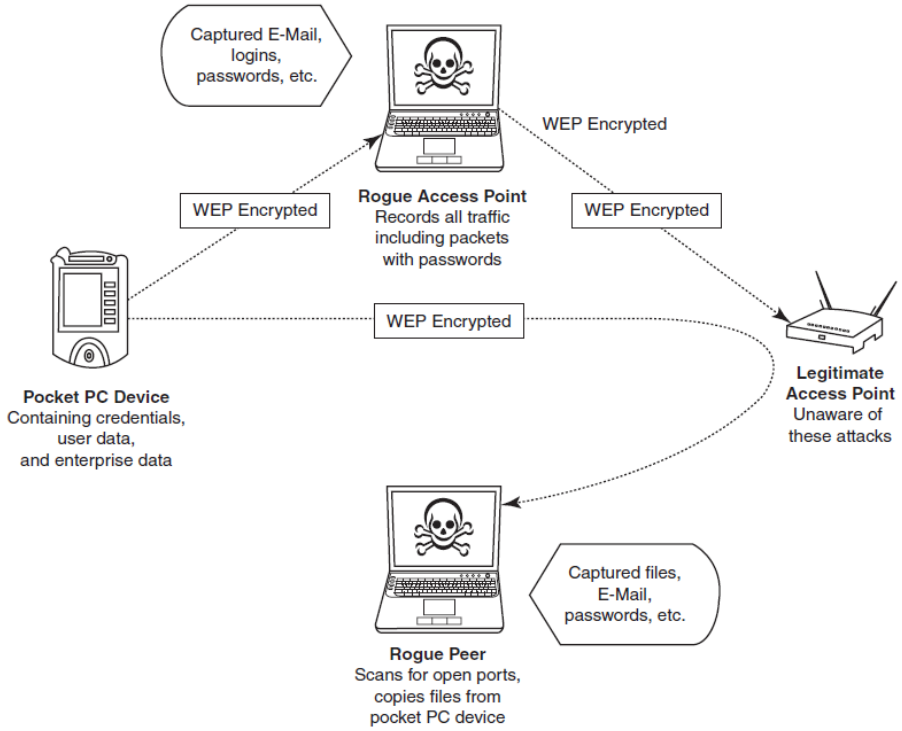

Figure 7.2 Pull attack on mobile devices. Source: Nina Godbole(2009), Information systems security, Wiley india.

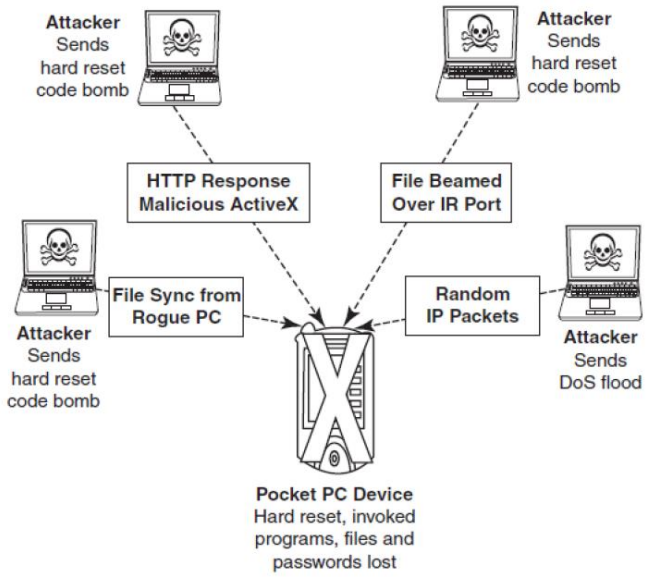

Figure 7.3 Crash attack on mobile devices. Source: Nina Godbole(2009), Information systems security, Wiley india.

8. Attacks on Mobile/Cell Phones

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)", that really matter, are lost One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

8.1 Vulnerabilities of Mobile/Cell Phones

The following factors contribute for

- Enough target terminals: Enough terminals or more devices to attack.
- Enough functionality: The expanded functionality ie. office functionality and applications also increases the probability of malware.
- Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

8.2 Securing your Cell/Mobile Phone

- Secure details of mobile phones: phone number; the make and model; PIN and/or security lock code; and IMEI number.
- antitheft software(s) on mobile phone
- Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
- If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
- If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
- Download and install antivirus software for mobile devices.

9. Mobile Devices: Security Implications for organizations

Cybersecurity is always a primary concern to Most organizations. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered to the organization.

10. Organizational Measures for Handling Mobile

- Encrypting Organizational Databases - Critical and sensitive data reside on databases and with the advances in technology, access to these data is possible through mobiles. Through encryption we can protect organization data.
- Security Strategy
    - Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.

- secure access to the company information through a firewall, such as mobile VPNs.
- Develop a system of more frequent and thorough security audits for mobile devices.
- User accounts are monitored for any unusual activity for a period of time.

11. Organizational Security Policies and Measures in Mobile Computing Era.

- Determine whether the employees in the organization need to use mobile computing devices or not.
- Implement additional security technologies like strong encryption, device passwords and physical locks.
- Standardize the mobile computing devices and the associated security tools being used with them.
- Develop a specific framework for using mobile computing devices.
- Maintain a record of who is using what kinds of devices.
- Establish patching procedures for software on mobile devices.
- Label the devices and register them with a suitable service.
- Establish procedures to disable remote access for any mobile.
- Remove data from computing devices that are not in use
- Provide education and awareness training to personnel using mobile devices.