Web and Mobile Security

UNIT-III

Web and Mobile Security

1. Fundamental Concepts and Approaches
2. Sandboxing,
3. Client-Side and Server-Side Vulnerabilities
4. Mitigations.

1. Fundamental Concepts and Approaches

I. Appification
II. Webification
III. Application Stores

I. Appification

- **Definition:** Appification refers to the shift from web-based platforms to mobile applications for accessing online content.
- **Impact:** It has changed how software is produced, distributed, and consumed, making mobile devices the primary interface for web access.
- **Security Concerns:** The rise of appification has led to increased client-side security challenges. **Many apps use backend services for computation and storage, which can introduce vulnerabilities**.
- **Citizen Developers:** **Non-professional developers** often create apps using **easy-to-use tools, leading to security issues** such as reconfiguration and code injection attacks.

II. Webification

- **Definition**: **Webification refers to the use of web technologies** (e.g., JavaScript, Python, Ruby) in building applications for web browsers and mobile web applications.

Key Technologies:

- **Uniform Resource Locators (URLs):** URLs are used to locate and access web resources. Various segments, such as scheme, host, and resource path, make up a URL.

The syntax of an absolute URL is:

scheme://credentials@host:port/resourcepath?query_parameters#fragments.

URL segments

Segment	Optional	Description
scheme:	○	Indicates the protocol a web client should use to retrieve a resource. Common protocols in the web are http: and https:
//	○	Indicates a hierarchical URL as required by [1245]
credentials@	●	Can contain a username and password that might be needed to retrieve a resource from a remote server.
host	○	Specifies a case-insensitive DNS name *(e. g. cybok.org)*, a raw IPv4 *(e. g. 127.0.0.1)* or IPv6 address *(e. g. [0:0:0:0:0:0:0:1])* to indicate the location of the server hosting a resource.
:port	●	Describes a non-default network port number to connect to a remote server. Default ports are 80 for HTTP and 443 for HTTPS.
/resourcepath	○	Identifies the resource address on a remote server. The resource path format is built on top of Unix directory semantics.
?query_parameters	●	Passes non-hierarchical parameters to a remote resource, such as server-side script input parameters.
#fragment	●	Provides instructions for the browser. In practice, it is used to address an HTML anchor element for in-document navigation.

- **Hypertext Transfer Protocol (HTTP):** HTTP is the protocol used to **exchange web documents.** It supports features like cookies for session management.
- **Hypertext Markup Language (HTML)**: HTML is the language used to create **web documents**. Proper HTML syntax is crucial to avoid web security issues like cross-site scripting (XSS).
- **Cascading Style Sheets (CSS)**: CSS is used to **style HTML** documents. Security issues may arise when user-controlled values are improperly handled.
- **JavaScript**: A powerful scripting language for **client-side programming**, widely used for web applications. Security concerns include cross-site scripting (XSS) vulnerabilities.
- **WebAssembly (Wasm)**: A binary instruction format designed **for high-performance web applications.** It is **sandboxed and follows the same security policies as regular web code.**
- **WebViews**: Enable the **embedding of web content in mobile apps**, allowing interactions between web and app content. **This raises security concerns**, including **app-to-web and web-to-app attacks**.

III. Application Stores

- **Definition**: Centralized **platforms for distributing software**, such as Apple's App Store and Google Play.
- **Security Role**: Application **stores examine apps for security** before distribution, using static and dynamic analysis to prevent malicious software and vulnerabilities.
- **Security Features**: Require **developers to sign apps using certificates**, reducing the risk of unauthorized updates or malware. **On iOS, unsigned apps cannot be installed.**

Sandboxing

1. Overview of Sandboxing
2. Application Isolation
3. Content Isolation
4. Content Security Policy (CSP)

1. Overview of Sandboxing

- **Definition**: Sandboxing refers to the technique used by modern mobile and browser platforms to **isolate applications and websites** from each other, enhancing security.
- **Purpose**: It helps protect the platform from malicious applications and websites by restricting their interactions with each other and the system.

Sandboxing can be

- Application Isolation
- Content Isolation

2. Application Isolation

- **Mechanism**: **Each application runs in its own sandbox**, operating within a dedicated process with its own file system storage.
- **Security Enforcement**: In mobile platforms like **Android, sandboxing is set up at the kernel level**, using user and group IDs, as well as security contexts.
- **Access Control**: Applications are **prevented from accessing each other's resources,** with inter-app communication only allowed through controlled interfaces.

3. Content Isolation

1. Same-Origin Policy (SOP): In web browsers, **SOP isolates documents based on their origin** to prevent different documents (or websites) from interfering with each other.

- **Key Principle**: **Only documents from the exact same origin** (**matching host, protocol, DNS name, and port number**) **are allowed to interact with each other.**
- **Limitations of SOP**: It relies on DNS instead of IP addresses, meaning attackers who can alter DNS entries might bypass the policy.

2. Process-Based Isolation: Modern browsers **run websites in separate processes within a sandbox**, adding an extra layer of security to prevent attacks like cross-site scripting (XSS -code injection attack) and cookie theft.

4. Content Security Policy (CSP)

- **Objective**: CSP provides an additional defense mechanism, particularly against **code injection attacks such as XSS**.
- **Functionality**: Developers can use **CSP to limit the sources from which content, scripts, and media can be loaded**, thereby restricting the execution of malicious code.
- **Implementation**: CSP is implemented via **HTTP response headers or HTML meta tags.**

Example: Content Security Policy Header The following CSP allows users of a web application to include images from any origin, but to restrict media data (audio or video media) to the trusted trusted-media.com domain. Additionally, scripts are restricted to the trusted-scripts.com origin that the web developer trusts:

```
Content-Security-Policy: default-src 'self'; img-src *; media-src
trusted-media.com; script-src trusted-scripts.com
```

Client-Side Vulnerabilities and Mitigations

This section covers attacks and their countermeasures with a focus on the client.

1. **Phishing and Clickjacking**
2. **Client-Side Storage Vulnerabilities**
3. **Outdated Third-Party Libraries**

1. Phishing and Clickjacking

Phishing and clickjacking rely on **issues humans have with properly verifying URL**s and the **dynamic content of rendered HTML documents**.

Here we discuss about the following:

I. **Phishing**

II. **Clickjacking**

III. **Mobile Phishing & Clickjacking**

I. Phishing:

- The practice of **sending fraudulent communications** that appear to come from a legitimate and reputable source, usually through email and text messaging.
- A common **fraudulent attack** where attackers steal sensitive information such as **login credentials and credit card numbers**.
- Attackers **disguise** themselves as trustworthy entities (via email, websites, SMS, etc.).

Techniques include:

- **Address bar manipulation** via JavaScript to show fake URLs.
- **Forged websites** resembling legitimate ones (e.g., misspelled URLs or homograph attacks).

Example Attack:

A URL like **https://paymentorganization.secure.server.com** may appear authentic but actually redirects to **secure.server.com.**

How the trick works:

"paymentorganization.secure" is just a **subdomain**. It can make the URL **look** like it's from "paymentorganization", but it’s really a part of "server.com".

This is a **phishing trick** to make the ***URL look trustworthy***, but in reality, it's **controlled by the attacker**.

1. Homograph attacks:

A **homograph attack** is a type of phishing attack where an attacker tricks you into **visiting a fake website by using characters** in the website address (URL) that **look very similar to real ones but are actually different**. involve characters that are hard to distinguish (e.g., Latin "a" vs. Cyrillic "а")

Example:

A real URL: https://paypal.com

A fake URL (using a Cyrillic letter instead of a Latin letter): https://paypal.com

To the human eye, **these look almost identical**, but the second URL leads to a **fake website**, designed to steal your information.

How to protect yourself:

- Be cautious when clicking on links in emails or messages.
- Check URLs carefully, especially when they ask for sensitive information.
- Modern browsers often include protections, such as warnings for suspicious URLs, to help detect these attacks. **e.g., Google Chrome highlights deceptive characters**

2. Drive-by-downloads:

A **drive-by download** is a type of cyberattack **where harmful software (malware) gets downloaded to your computer or device automatically,** without you even knowing or giving permission. It can happen just by visiting an unsafe website or clicking on a malicious link or pop-up.

How to protect yourself:

- Keep your **browser and software updated** to close any security loopholes.
- Use a **reliable antivirus program** to detect and block suspicious downloads.
- **Avoid visiting suspicious websites or clicking on strange links or pop-ups.**

II. Clickjacking:

- Also known as **user interface redress attacks**, clickjacking tricks users into **clicking on elements that perform unintended actions**.
- Attackers overlay **invisible or transparent layers on websites**, fooling users into interacting with underlying content.
- Particularly dangerous when victims are **already logged into accounts**, allowing attackers to manipulate settings or perform harmful actions.

Prominent example:

- Adobe Flash plugin attack, where **attackers used invisible iFrames** to change security settings.
- An **iFrame** is like a little window inside a webpage that can show another webpage.
- The attackers placed a visible **fake button or link** on the webpage, and when users clicked it, they were actually **clicking on the invisible iFrame** underneath.
- Attackers hid the **Adobe Flash settings page** behind an invisible layer on a webpage. When users clicked a button on the page, they were unknowingly **changing Flash's security settings**, **potentially giving the attacker access to their microphone or camera**

Prevention Methods:

- **Client-side: Disable JavaScript** or use browser plugins like **NoScript** to control script execution (though this may break legitimate websites).
- **Server-side:** Use the X-FRAME-OPTIONS HTTP header set to DENY to prevent websites from being loaded inside **iFrames.**

III. Mobile Phishing & Clickjacking:

- **Mobile apps** are also vulnerable to phishing and clickjacking.

Techniques like

- **Abusing Android's Instant App feature**
- **Cloak & Dagger attacks** can steal credentials or take control of the UI.

I. Abusing Android's Instant App feature

The **Android Instant App** feature allows users **to run apps instantly without downloading and installing them fully** from the Google Play Store. This is convenient because you can **use part of an app immediately** (like to view a product or make a quick purchase) without waiting for the full installation.

How attackers abuse it:

1. **Tricking users**: Attackers can create fake Instant Apps that seem legitimate. When you run these apps, they might look like real apps but are actually designed to **steal your information** (like passwords or personal data).
2. **No installation needed**: Since you don't need to install the app, users might not suspect anything is wrong because it doesn't go through the usual app installation warnings.
3. **Phishing**: An attacker can use this Instant App to **mimic real apps**, like a bank or social media app, and steal your login credentials by making you believe you're entering your information into a trusted app.

II. Cloak & Dagger Attack

The **Cloak & Dagger** attack takes advantage of Android's permissions system to let attackers secretly control parts of your phone without your knowledge.

How attackers use it:

1. **Ask for Two Permissions**: The attacker's **app only asks for two basic permissions**:
    1. **Draw over other apps**: This allows the app to display things on top of other apps you're using.
    2. **Accessibility service**: This allows the app to interact with the phone's user interface (UI), like clicking buttons or typing text.
2. **Perform Hidden actions**: Once the app gets these permissions, it can secretly:
    1. **Overlay fake screens**: For example, it might show you what looks like a regular app screen, but underneath, it's stealing your keystrokes or clicking buttons.
    2. **Steal your clicks**: The app can make you click on things you didn't mean to, such as giving it more permissions or even unlocking your phone.
    3. **Keylogging**: It can record what you type, including passwords or sensitive data.

2. Client-Side Storage Vulnerabilities

Refers to areas on the client's browser or operating system where websites or mobile applications can store data.

Risks:

- Local storage manipulation: Attackers can potentially access or alter stored data, leading to security risks.
- Lack of server-side protection: Since client-side storage does not require server-side resources, it becomes vulnerable to unauthorized access.

Protection Mechanisms:

Implement robust security measures to protect client-side storage areas from malicious access

- Use HTTPS
- Same-Origin Policy
- Content Security Policy (CSP)
- Input Validation and Sanitization
- Secure Cookies
- Encryption of Stored Data
- Limit Storage Usage
- Access Control with JavaScript
- Regular Storage Cleanup
- Monitor for XSS (Cross-Site Scripting) Vulnerabilities

3. Outdated Third-Party Libraries

- Developers often use outdated libraries, which expose users to security risks due to unpatched vulnerabilities.
- Studies show a significant number of developers fail to update third-party libraries in Android and JavaScript applications, leading to security issues.
- Solution: Developers must continuously track vulnerabilities in the libraries they **use and update them regularly**.

CHAPTER 2
Cybercrime: Mobile and Wireless Devices

Cybercrime: Mobile and Wireless Devices

- Proliferation of Mobile and Wireless Devices
- Trends in Mobility
- Credit Card Frauds in the Mobile and Wireless Computing Era
- Security challenges posed by mobile devices
- registry settings for mobile devices
- Authentication Service Security
- Attacks on Mobile phones.

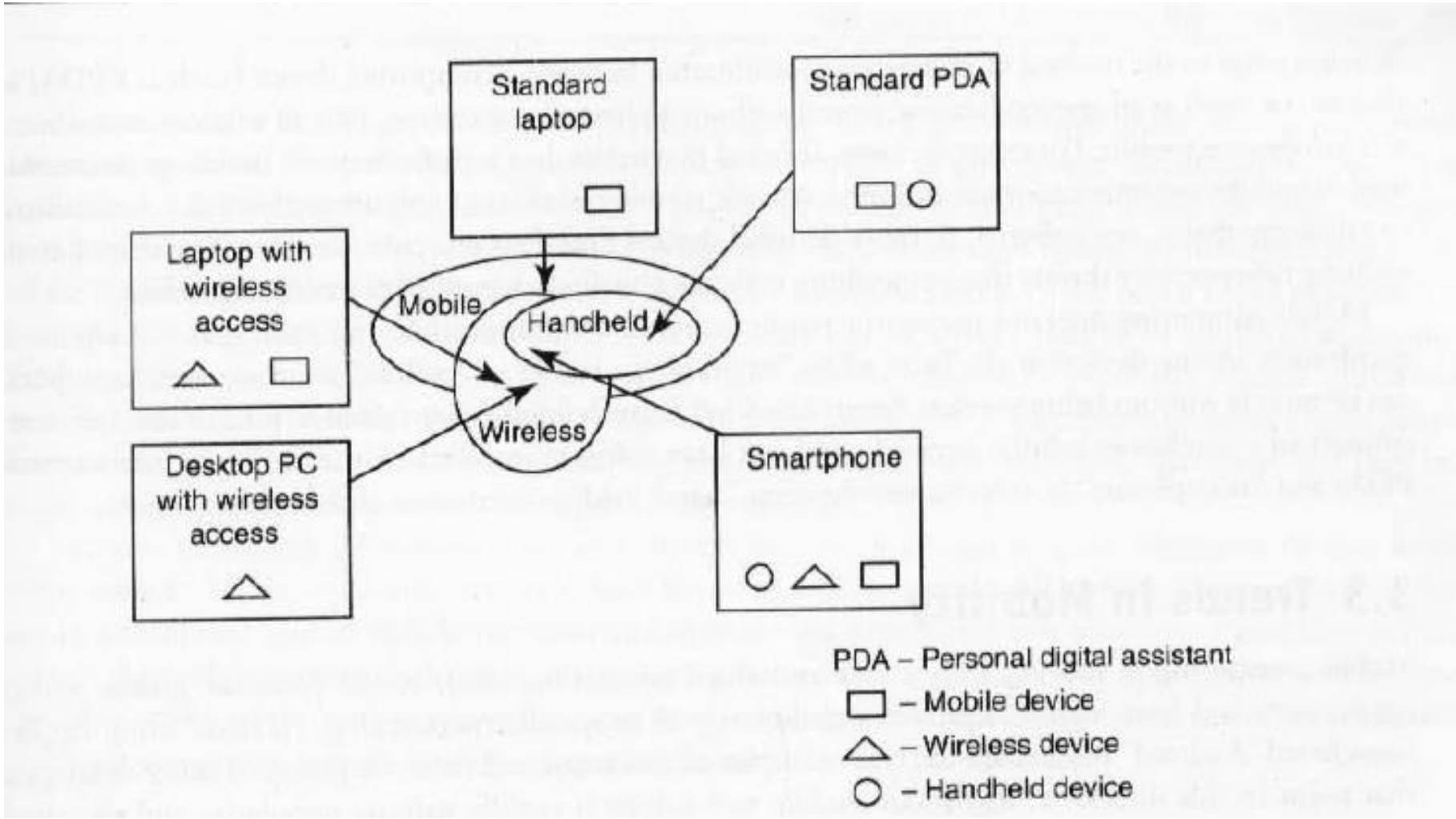
1. Proliferation of Mobile and Wireless Devices

- **Rapid Growth of Devices**: Mobile and wireless devices have seen an exponential increase in the past decade, including smartphones, tablets, laptops, wearable tech (smartwatches), and IoT (Internet of Things) devices.
- **Increased Connectivity:** The rise of 4G, 5G, and Wi-Fi technologies has made mobile devices more connected, leading to an increased attack surface for cybercriminals.
- **BYOD (Bring Your Own Device):** Many organizations now allow employees to use personal mobile devices for work, which increases security risks as these devices may not have the same level of protection as corporate devices.

Cont..

- **Data Storage and Usage:** Mobile devices now store vast amounts of sensitive data, including personal information, banking details, and confidential business data, making them prime targets for cybercriminals.
- **App Proliferation:** The number of mobile apps has exploded, with apps often requesting extensive permissions, creating potential security vulnerabilities (e.g., malicious apps).

Mobile, wireless and Handheld devices



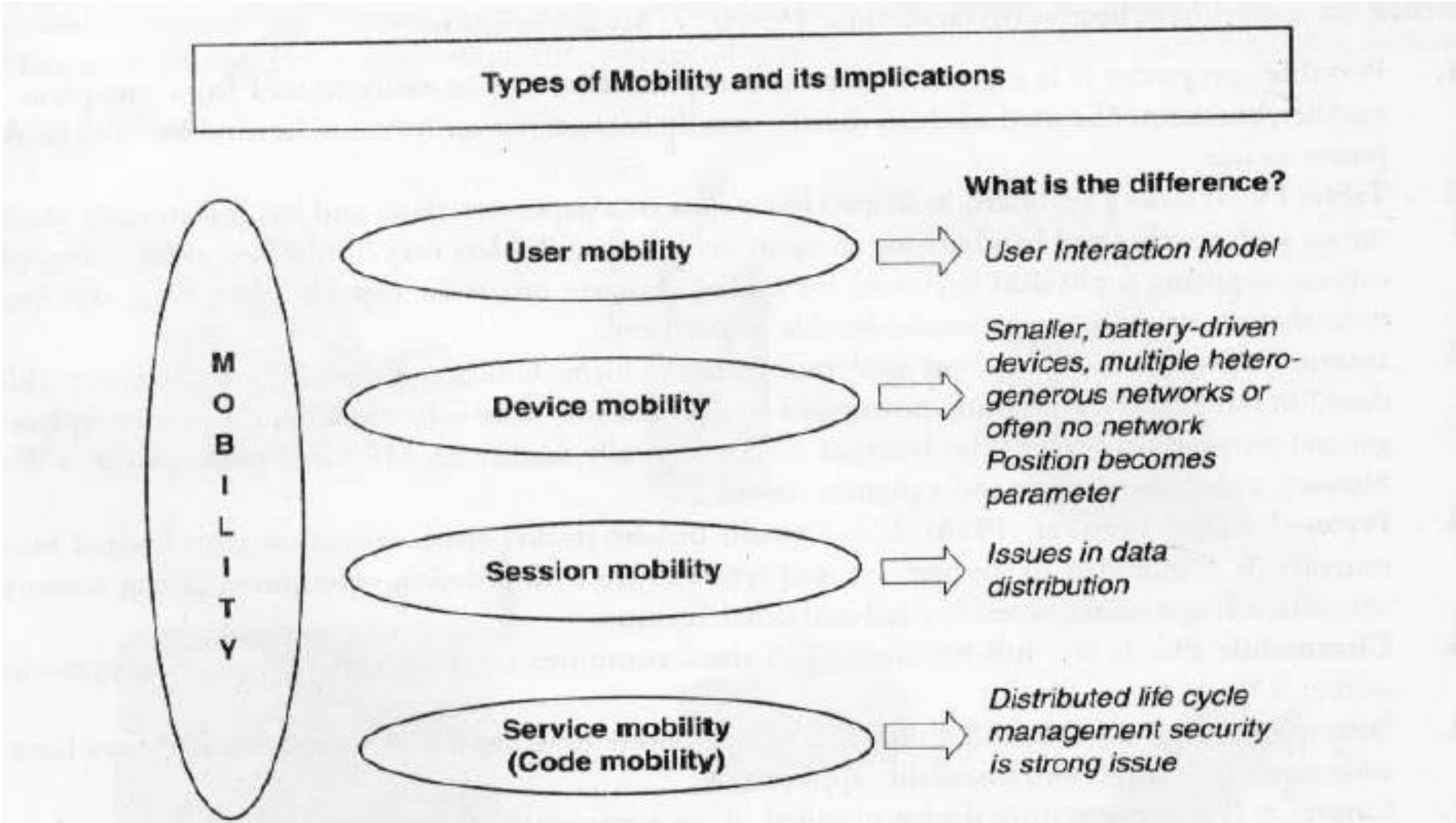
Mobile computing devices

- **Portable computer-**A lightweight, mobile computer, such as a laptop, designed for easy transport and use anywhere.
- **Tablet PC**- A portable computer with a touchscreen interface, typically larger than a smartphone but smaller than a laptop, often used with a stylus.
- **Internet Tablet**-A mobile device primarily designed for accessing the web and multimedia, often without cellular phone capabilities.
- **Personal Digital Assistants(PDA)-** Small, handheld devices used for managing personal information like contacts, calendars, and notes, popular before smartphones.
- **Ultramobile PC-** Acompact, portable computer with tablet-like features, designed for mobile productivity but smaller than a standard laptop.
- **Smartphone**- A mobile phone with advanced features like internet access, apps, and multimedia capabilities, combining the functionality of a computer.
- **Carputer-** A computer integrated into a vehicle, often used for navigation, entertainment, and diagnostics, blending technology with automotive systems.
- **Fly Fusion Pentop Computer-** A digital pen that writes on special paper and can convert handwriting into digital text, offering interactive learning and computing features.

2. Trends in Mobility

Mobility can be:

1. **User mobility**: The ability for a user to access services and information while moving across different locations or networks.
2. **Device mobility:** The capability of a device to move across networks without losing connectivity or requiring reconnection.
3. **Session mobility:** The ability to maintain an ongoing session (e.g., a video call or streaming) seamlessly while switching between devices or networks.
4. **Service mobility (code mobility):** The ability for services or applications to move across different environments or devices, adapting to different platforms or networks.


Types of Mobility and its Implications
What is the difference?
MOBILITY
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility (Code mobility)
Distributed life cycle management security is strong issue

popular types of attacks against 3G mobile networks

1. Denial of Service (DoS) Attacks

DoS attacks target **the network's resources to render them unavailable to legitimate users**.

This can involve:

Overloading the core network: Attacks flood the network with signaling messages (like authentication requests), overwhelming its ability to process them.

Exhausting bandwidth: Excessive data usage prevents other users from accessing the network.

Example: Sending a large volume of fake connection requests to overwhelm the authentication process.

2. Man-in-the-Middle (MitM) Attacks

In a MitM attack, an attacker **intercepts communication between a mobile device and a base station**.

Common techniques include:

Fake Base Station: Devices like "Stingrays“(fake cell towers) act as rogue base stations, tricking nearby mobile phones into connecting to them, allowing the attacker to monitor or alter the traffic.

Eavesdropping: If encryption is weak or disabled, the attacker can intercept and read sensitive information.

Example: Deploying a fake base station to intercept unencrypted SMS messages or voice calls.

3. Replay Attacks

Replay attacks occur when **attackers capture legitimate messages transmitted between a mobile device and the network and later retransmit them**. This can exploit the lack of fresh authentication tokens or nonce values.

Example: Reusing an intercepted authentication message to gain unauthorized access to a network.

4. Downgrade Attacks

In a downgrade attack, an attacker **forces a mobile device to switch to a less secure network standard** (e.g., from 3G to 2G). Older standards like 2G (GSM) use weaker encryption protocols, making interception easier.

Example: Forcing **a 3G phone to connect to a 2G network** where encryption may be bypassed.

5. SMS Spoofing and Interception

SMS-based attacks involve **spoofing SMS messages** (impersonating a legitimate sender) or intercepting SMS traffic. This is particularly **dangerous for users relying on SMS for two-factor authentication (2FA).**

Example: An attacker sends a fake SMS from a banking service to trick users into sharing sensitive information.

6. Authentication Attacks

3G networks use mutual authentication between the device and network, but **vulnerabilities in the authentication protocol can be exploited**:

Exploiting weak encryption algorithms: **Breaking the encryption** used during authentication (e.g., A5/1 used in older GSM).

Brute-force attacks on authentication credentials: Guessing or **deriving authentication keys** used in 3G networks.

7. Overbilling Attacks

Attackers exploit billing systems by generating fraudulent activities that are charged to legitimate users. These can include premium-rate service fraud, where attackers use vulnerabilities in billing platforms to trick users into making expensive calls or messages.

8. Malwares, viruses and worms:

Skull Trojan: This type of malware **targets older phones** that use the Symbian OS (a mobile operating system used in early smartphones). Once installed, it can damage the phone by **changing important icons to skulls,** making it difficult to use the phone.

Cabir Worm: This was the **first mobile phone worm**. It infects Symbian OS phones and **spreads by scanning for other nearby devices through Bluetooth.** When it finds a vulnerable device, it sends a copy of itself to infect that device. The dangerous part is that the **source code for this worm is available online**, making it easier for others to create variations of the virus.

•***Mosquito Trojan***: This malware **affects Series 60 smartphones** (early smartphones using Symbian OS). It disguises itself as a cracked (illegally modified) version of the "**Mosquitos" mobile phone game**, tricking people into downloading it.

•***Brador Trojan***: This Trojan **targets devices using Windows CE OS** (an early version of Windows for handheld devices). It creates **a file** called **svchost.exe** in the **device's start-up folder**, which allows the **hacker to take full control of the device**. The malware can **spread** through traditional methods like **email attachments**.

•***Lasco Worm:*** First discovered in 2005, this worm **targets PDAs** (Personal Digital Assistants) and mobile phones running Symbian OS. It is **based on the Cabir worm's code** and **spreads through Bluetooth** connections, just like Cabir.

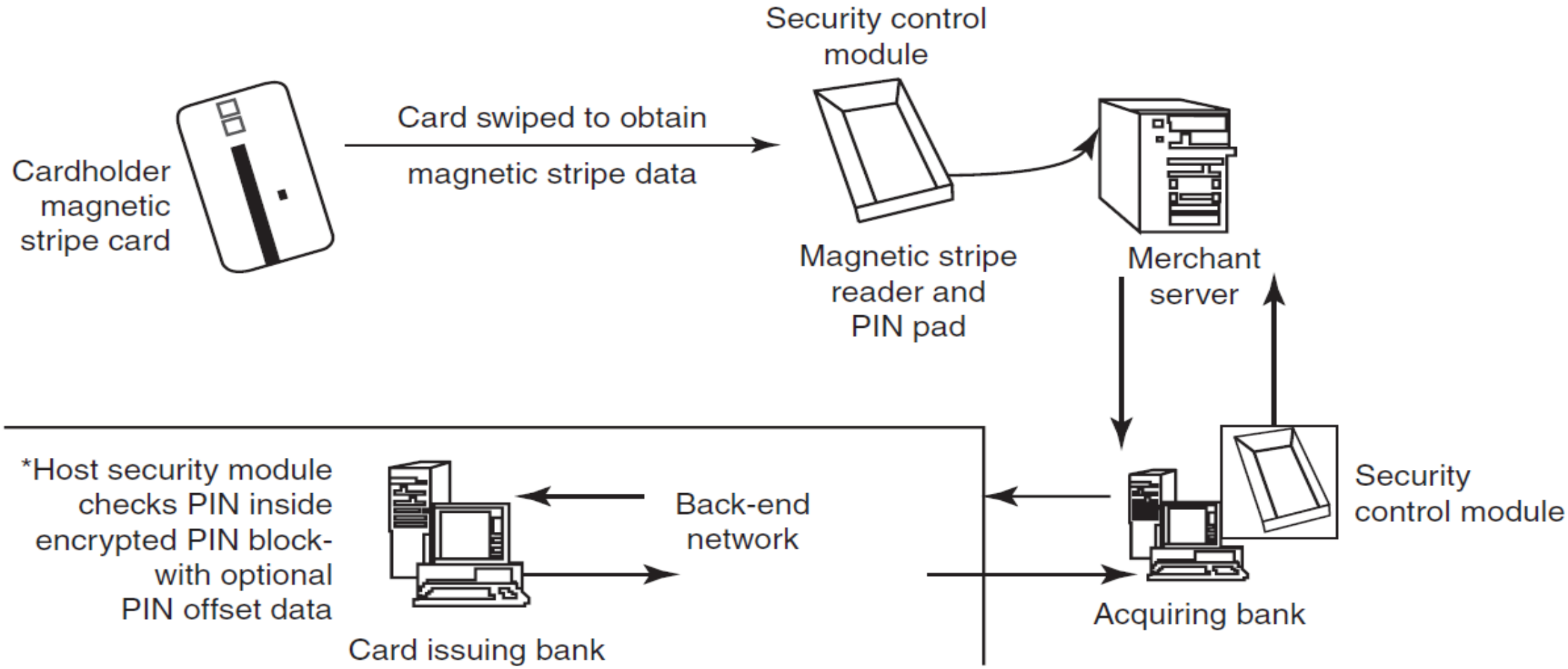
Mitigation Measures

1. **Strong encryption**: Implementing robust encryption standards (like AES) to protect communications.
2. **Mutual authentication**: Ensuring both user and network authenticate each other properly.
3. **Network monitoring**: Using tools to detect unusual traffic patterns that may indicate an attack.
4. **Security updates**: Keeping network components up to date to avoid known vulnerabilities.
5. **User education**: Informing users about phishing attacks and fake base stations.

3. 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 becoming commonplace given the **ever-increasing power** and the **ever-reducing prices** of mobile hand-held devices. These factors result in the easy availability of these gadgets to almost anyone.
- ***Mobile credit card transactions*** are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a **point-of-sale (POS) terminal**.
- Today belongs to "mobile computing," that is, ***anywhere anytime computing.***
- The developments in wireless technology have fuelled this new mode of working for white-collar workers.
- **Wireless credit card processing** is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.

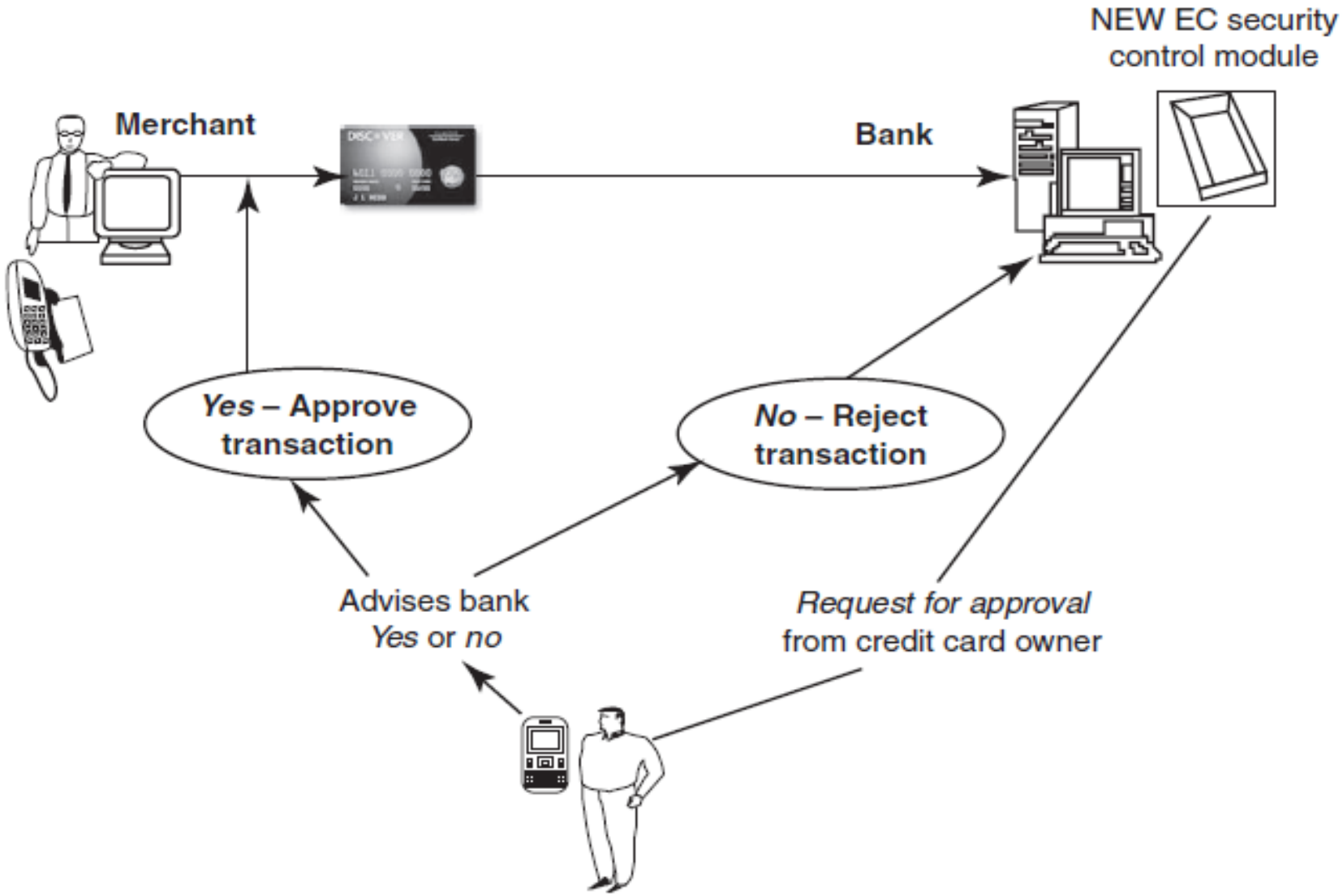
Figure 3.4 shows the basic flow of transactions involved in purchases done using credit cards.



- Credit card companies, normally, do a good job of helping consumers resolve **identity (ID) theft problems** once they occur.
- But they **could reduce ID fraud** even more if they give consumers **better tools to monitor** their accounts and limit high-risk transactions

the basic flow is as follows:

1. Merchant sends a transaction to bank;
2. The bank transmits the request to the authorized cardholder [not short message service (SMS)];
3. The cardholder approves or rejects (password protected);
4. The bank/merchant is notified;
5. The credit card transaction is completed.


NEW EC security
control module
Merchant
Bank
Yes – Approve
transaction
No – Reject
transaction
Advises bank
Yes or no
Request for approval
from credit card owner
Individual card holder using cell phone
for credit card transaction

Tips to Prevent Credit Card Frauds

Do's

1. Put your signature on the card immediately upon its receipt.
2. 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.
3. Change the default personal identification number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.

Cont..

7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Dont's

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/ to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin

Types and Techniques of Credit Card Frauds:

- **Traditional Techniques:**
  - **Application fraud**
  - **Illegal use of lost and stolen cards**

1. Application fraud

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:

1. **ID theft:** Where an individual pretends to be someone else
2. **Financial fraud:** Where an individual gives **false information about his or her financial status** to acquire credit.

2. Illegal use of lost and stolen cards is another form of traditional technique. **Stealing** a credit card is either by **pickpocket** or **from postal service** before it reaches its final destination

- **Modern Techniques**
  1. **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 **is copied** from one card to another.
  2. **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. Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink /website (i.e., they have been scammed).

Cont..

3. Triangulation: It is another method of credit card fraud and works in the fashion as explained further.

1. The **criminal creates a fake website** that looks like a real store and offers products at super low prices to attract people.
2. A **customer** visits the fake website, **registers with their personal information** (name, address, etc.), and provides their credit card details to buy the product.
3. **The criminal doesn't use the customer's credit card directly**.
4. Instead, **they use stolen credit card details from someone else to buy the same product from a legitimate website** and ship it to the customer's address.
5. The **customer receives the product**, so they think everything is fine.
6. Meanwhile, the **criminal keeps using stolen credit card details to make more purchases** for other customers and eventually shuts down the fake website to avoid getting caught.
7. Then, they start the whole process again with a new fake site.

Cont..

- The criminal **gains by making money from selling products that are paid for using someone else's stolen credit card**, while also reducing the risk of getting caught because they never physically handle the stolen goods themselves.

4. Credit card generators: It is another modern technique – computer emulation software – that creates **valid credit card numbers and expiry dates**. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

4. SECURITY CHALLENGES POSED BY MOBILE DEVICES

mobile devices bring two main problems to cybersecurity:

1. **Information leaving a secure area:** People take mobile devices like phones and tablets outside the controlled and secure environment of their workplace, which increases the risk of information being exposed or stolen.
2. **Remote access back into the secure area:** Mobile devices often connect back to the organization's secure systems remotely, which could open up new ways for hackers to attack.

Organizations need to be aware of these risks to set up proper security rules. As more people use mobile devices, **two types of challenges arise:**

- **Microchallenges**: These are challenges **on the individual device level**, such as how to protect data on each phone or tablet.
- **Macrochallenges**: These **affect the entire organization**, like how to manage security when many employees are using mobile devices.

Some well-known technical issues in mobile security include things like managing device settings, ensuring secure login methods, protecting data through **encryption, securing network connections, and controlling media players and apps on mobile devices**.

5. REGISTRY SETTINGS FOR MOBILE DEVICES

Registry settings for mobile devices are like a set of instructions or rules that tell the device how to behave. These settings control important functions, such as:

1. **What apps can be installed** or run on the device?
2. **How the device connects to the internet** or other networks.
3. **How security features** like passwords, encryption, or firewalls should work.
4. **System preferences**, like whether updates are automatically installed or how notifications are handled.

The issue of **registry settings on mobile devices** with an example:

- **Microsoft ActiveSync** is a tool that helps users synchronize (or transfer) data between their **Windows-powered PCs** and **Windows mobile devices**.
- This includes things like **emails, calendar events, notes, contacts, and even files like pictures**, music, and documents.
- Imagine you use **ActiveSync to make sure that everything on your PC is also available on your mobile device**, so you can access your emails, calendar, and files on the go.
- **ActiveSync** can also sync directly with the **Microsoft Exchange server, allowing your emails, contacts, and calendar to stay up-to-date** wirelessly even when you are far from your PC.
- Registry setting becomes **an important issue given the ease with which various applications allow a free flow of information**

- Mobile devices and computers face security risks from things like **Spyware, viruses, worms, malware**, and other harmful programs that can spread through networks and the internet.
- To fight these, there are **new mobile apps** being developed all the time to protect against these threats.
- One problem with **Windows devices** (both computers and mobile devices) is that when you first set them up, they **might not be fully secure**.
- Even if you go through all the settings in the **Control Panel** or other menus, the security might still not be strong enough.
- For example, **some important security settings can only be changed by modifying the registry**.
- The **registry is like a hidden control center for how the device operate**s, and certain security improvements can only be made by changing these settings, which are not always visible in regular menus.

6. 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.***

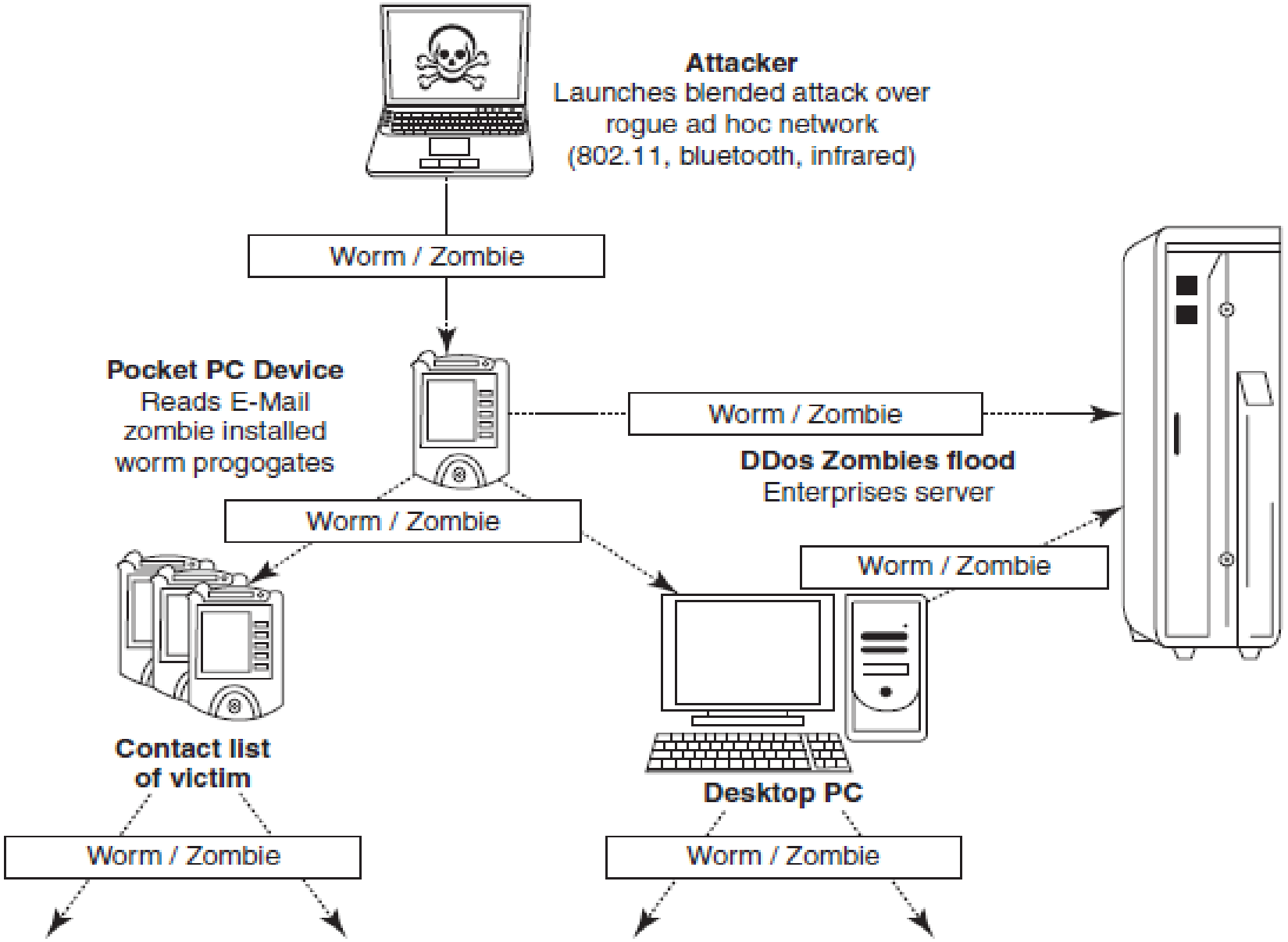


Figure 3.8 Push attack on mobile devices. DDoS implies distributed denial-of-service attack.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

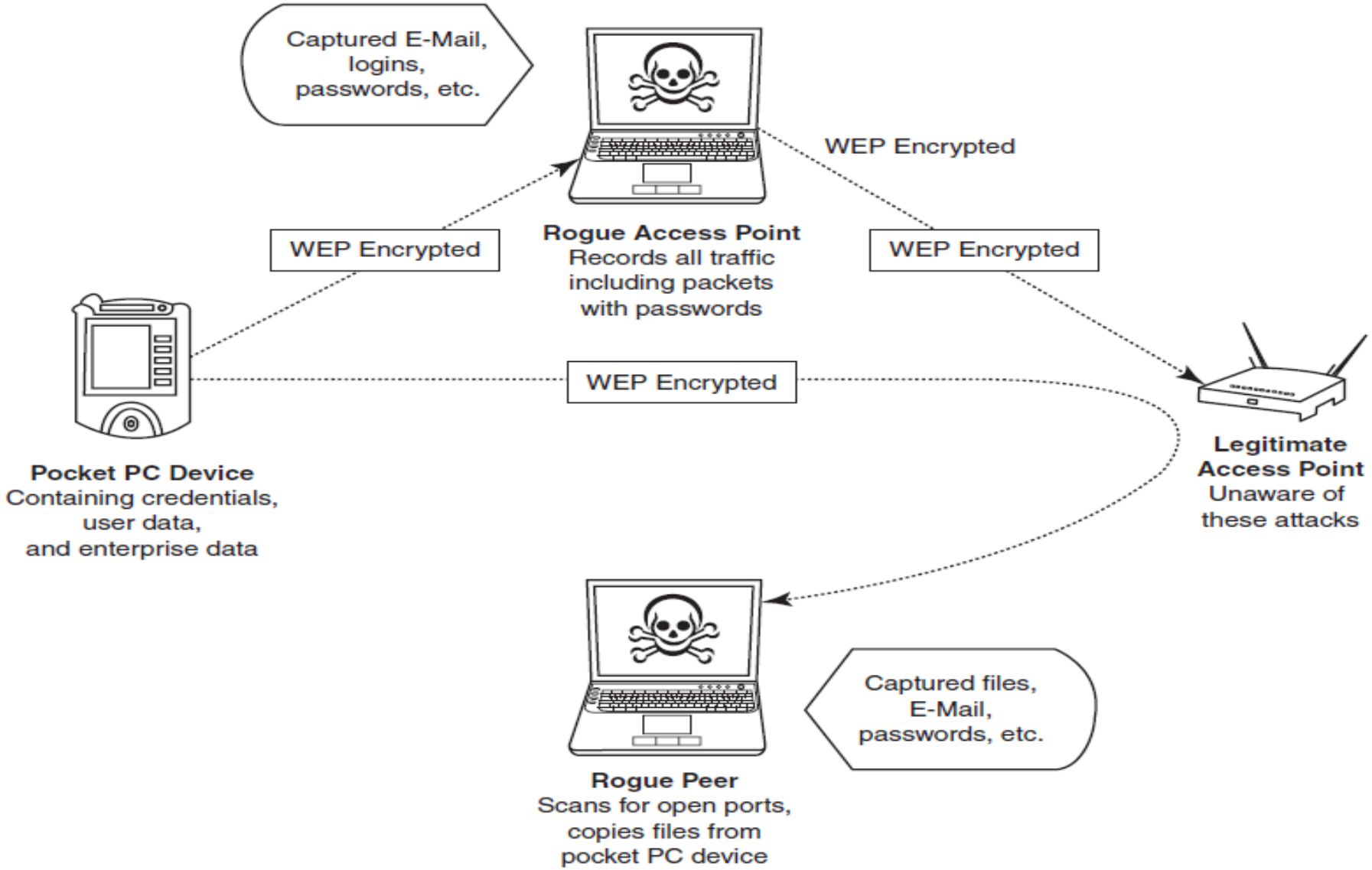


Figure 3.9 | Pull attack on mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

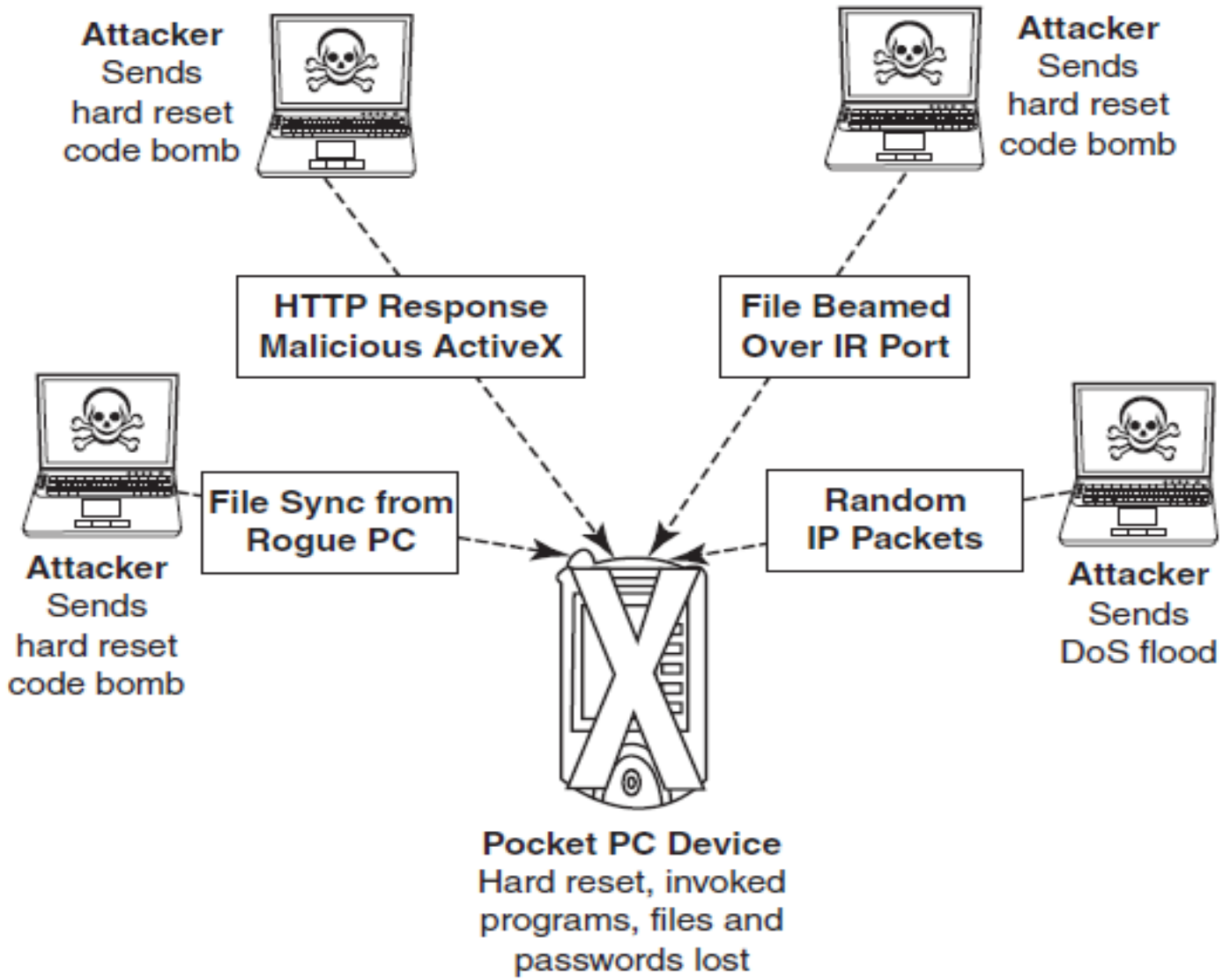


Figure 3.10 | Crash attack on mobile devices. DoS – Denial-of-service attack.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

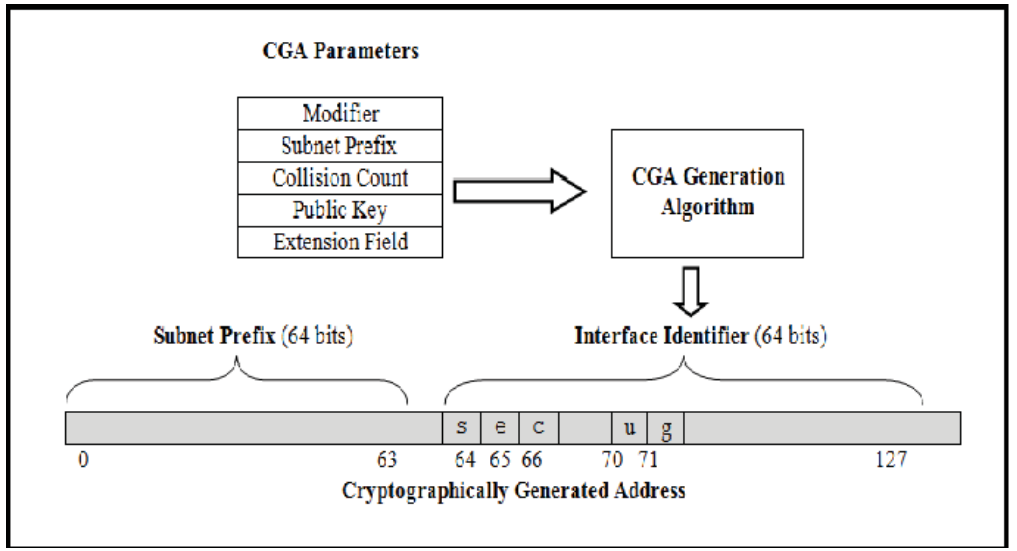
AUTHENTICATION SERVICE SECURITY

1. Cryptographic Security for Mobile Devices
2. LDAP (Lightweight Directory Access Protocol) Security for Hand-Held Mobile Computing Devices
3. RAS (Remote Access Server) Security for Mobile Devices
4. Media Player Control Security
5. Networking API Security for Mobile Computing Applications

1. Cryptographic Security for Mobile Devices

Use of Cryptographically Generated Addresses (CGA)

- **Part of IPv6 (Internet Protocol version 6)**
  - Addresses up to **64 bits** generated using a **cryptographic hash of the owner's public key.**



- **Private Key Ownership**
  - Owner uses the **private key to prove address ownership** and sign messages.
  - **No need for a central Public-Key Infrastructure (PKI)** for basic security.

Benefits of CGA-Based Authentication

- **No PKI Required**: CGA works without needing external security infrastructure.
- **Security at the IP Layer**: Protects IP-layer signaling protocols like:
  - Neighbor Discovery Protocol (NDP)
  - Mobility protocols (e.g., Mobile IPv6)
- **CGA in Opportunistic IPSec**
  - **Key Exchange**: **Enables secure key exchange** in Internet Protocol Security (**IPSec**) without prior setup.
  - **Verification**: CGA-based addresses help **verify identity and establish encrypted communication.**
- **PKI Benefits in Mobile Transactions**
  - **Added Security**: PKI can be used for **extra protection**, especially for financial transactions on mobile devices.
  - **Stronger Authentication**: PKI ensures **trusted, secure communication** when conducting sensitive tasks.

Cont..

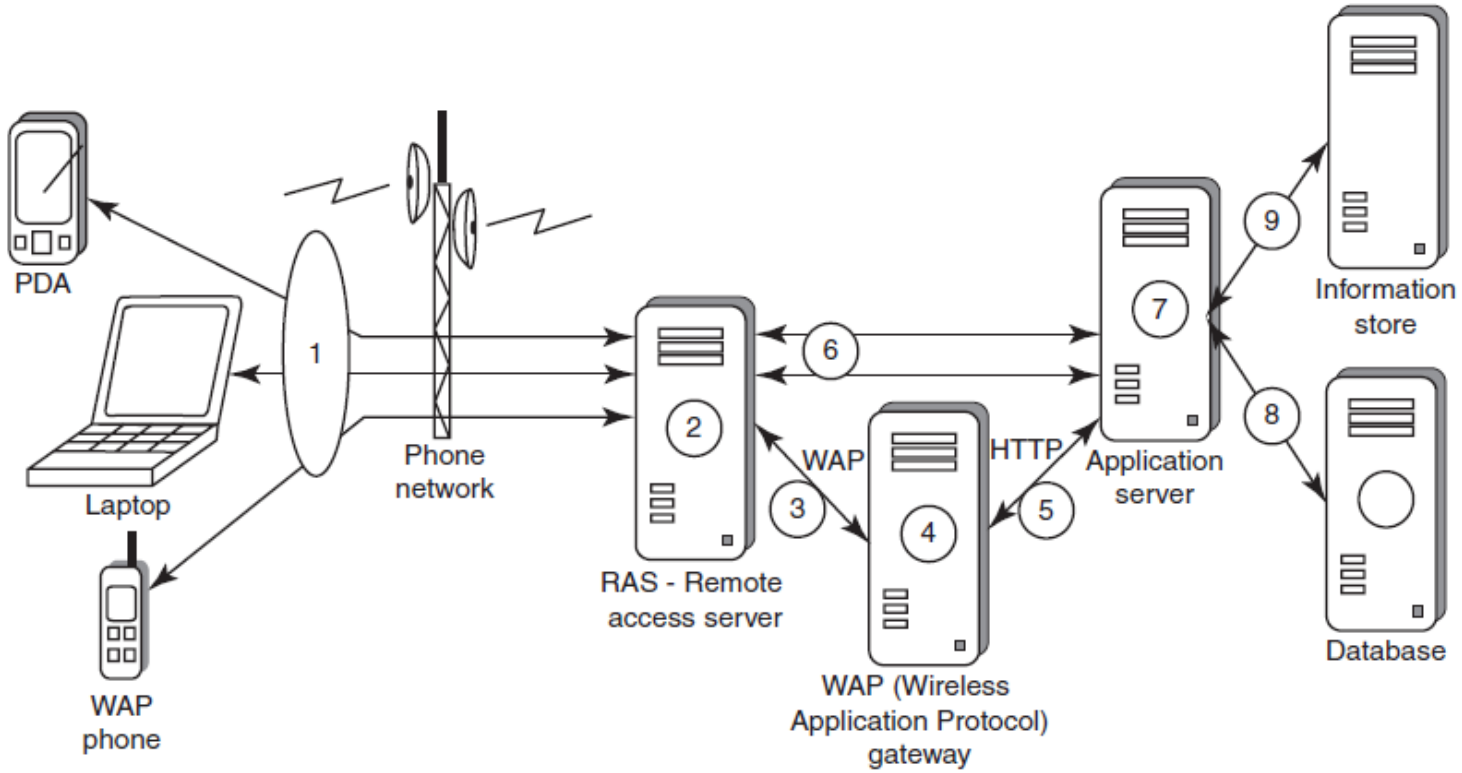
- **CGA in Mobile and Handheld Devices**
  - **Used in Context-Aware Mobile Computing**: **Secures** communications in mobile applications based on **context and location.**
  - **Palm Devices**: These are common handheld devices (like PDAs) in mobile computing that can take **advantage of cryptographic security features.**
  - **Cryptographic Security on Palm Devices** is provided by **Cryptographic Provider Manager (CPM) in Palm OS-5**:
    - Provides **systemwide encryption services**.
    - Allows applications to **encrypt selected data or all data** on the device for security.

2. LDAP (Lightweight Directory Access Protocol) Security for Hand-Held Mobile Computing Devices

- LDAP is a **software protocol for enabling anyone to locate individuals**, organizations, and other resources such as files and devices on the network (i.e., on the public Internet or on the organization's Intranet).
- In a network, a directory tells you where an entity is located in the network.
- LDAP is a light weight version of **Directory Access Protocol (DAP)** because it does not include security features in its initial version.

3. RAS (Remote Access Server) Security for Mobile Devices

- RAS (Remote Access Server) is an important consideration **for protecting the business sensitive data that may reside on the employees' mobile devices**.
- In terms of cybersecurity, mobile devices are sensitive. Figure 3.11 : organization's sensitive data can happen through mobile hand-held devices carried by employees.



Threats

- In addition to being **vulnerable** to **unauthorized access** on their own, mobile devices also provide a route into the systems with which they connect.
- By using a mobile device to appear as a registered user (**impersonating or masquerading**) to these systems, a would-be cracker is then able to **steal data or compromise corporate systems in other ways**.
- Another threat comes from the practice of **port scanning**.
  - First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer. A domain is a collection of sites that are related in some sense.
  - Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls.

Example:

- For instance, **File Transfer Protocol (FTP)** transmissions are typically assigned to **port 21.**
- If this port is left **unprotected**, it can be misused by the attackers.

- Protecting against port scanning requires **software that can trap unauthorized incoming data packets** and prevent a mobile device from revealing its existence and ID.
- A **personal firewall on a pocket PC** or **Smartphone** device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection.

4. Media Player Control Security

- Various leading software development organizations have been warning the users about the potential **security attacks on their mobile devices through the "music gateways."**
- There are many examples to show how a **media player can turn out to be a source of threat** to information held on mobile devices.
- For example, in the year 2002, Microsoft Corporation warned about this.
- According to this news item, Microsoft had warned people that a **series of flaws** in its **Windows Media Player** could allow a **malicious hacker to hijack people's computer systems** and perform a variety of actions.
- According to this warning from Microsoft, in the **most severe exploit** of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

5. Networking API Security for Mobile Computing Applications

- With the advent of electronic commerce (E-Commerce) and its further off-shoot into MCommerce, online **payments are becoming a common phenomenon** with the payment gateways accessed remotely and possibly wirelessly.
- Furthermore, with the advent of Web services and their use in mobile computing applications, **the API has become an important consideration.**
- Already, there are organizations announcing the development of **various APIs to enable software and hardware developers to write single applications**
- Most of these **developments are targeted specifically at securing a range of embedded and consumer products**, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).
- Technological developments such as these provide **the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices.** Providing a common software framework, APIs will become an important enabler of new and higher value services.

ATTACKS ON MOBILE/CELL PHONES

Task-4 : write in your note book about the following attacks on mobile phones, how they are performed (tools), and tips to secure from these attacks:

- **Mobile Phone Theft**
- **Mobile Viruses**
- **Mishing -> Mobile Phishing**
- **Vishing-> social engineering over the telephone**
- **Smishing -> SMS PhISHING**
- **Hacking Bluetooth**

Mobile Phone Theft

- 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.

Mobile Phone Theft

- 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.
- The following factors contribute for outbreaks on mobile devices:
    1. **Enough target terminals:** Enough terminals or more devices to attack.
    2. **Enough functionality:** The expanded functionality ie. office functionality and applications also increases the probability of malware.
    3. **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

Mobile Phone Theft

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

- Ensure to note the following details about your cell phone and preserve it in a safe place:
    1. Your phone number;
    2. the make and model;
    3. color and appearance details;
    4. PIN and/or security lock code;
    5. IMEI number.

Mobile Phone Theft

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

The International Mobile Equipment Identity (IMEI)

- It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.
- The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country.
- For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to “lock” the phone using its IMEI number.
- This will help to stop the usage of phone in that country, even if a SIM is changed.
- Visit the weblink http://www.numberingplans.com/?page=analysis&sub=imeinr to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

Mobile Phone Theft

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

- Following are few antitheft software(s) available in the market:
    1. GadgetTrak: http://www.gadgettrak.com/products/mobile/
    2. Back2u: http://www.bak2u.com/phonebakmobilephone.php
    3. Wavesecure: https://www.wavesecure.com/
    4. F-Secure: http://www.f-secure.com/

Mobile Viruses

- A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
- Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays.
- In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified.
- First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
- Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth activated phones
- MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

Mobile Viruses

How to Protect from Mobile Malwares Attacks

- Following are some tips to protect mobile from mobile malware attacks:
    1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
    2. 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.
    3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
    4. Download and install antivirus software for mobile devices.

Mishing

- Mishing is a combination of mobile and Phishing.
- Mishing attacks are attempted using mobile phone technology.
- M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
- A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with diferent reasons why they need this information from you.

Vishing

- Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V – voice and Phishing.
- Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

Vishing

- The most profitable uses of the information gained through a Vishing attack include:
    1. ID theft;
    2. purchasing luxury goods and services;
    3. transferring money/funds;
    4. monitoring the victims' bank accounts;
    5. making applications for loans and credit cards.

Vishing

How Vishing Works

- The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.
    1. Internet E-Mail:
    2. Mobile text messaging:
    3. Voicemail:
    4. Direct phone call:

Vishing

Following are the steps detailing on how direct phone call works:

- The criminal gathers cell/mobile phone numbers located and steals mobile phone numbers after accessing cellular company.
- The criminal often uses a dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.
- When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity.
- The message instructs the victim to call one phone number immediately.
- The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.

Vishing

Following are the steps detailing on how direct phone call works:

- When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
- Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
- Such calls are often used to gain additional details such as date of birth, credit card expiration date, etc.

Vishing

- Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:
    1. Automated message: Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.
        - ✓ **Press 1 if you need to check your banking details and live balance.**
        - ✓ **Press 2 if you wish to transfer funds.**
        - ✓ **Press 3 to unlock your online profile.**
        - ✓ **Press 0 for any other query.**
    2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: “The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key.”

Vishing

- Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:
    3. The victim enters his/her bank account number and hears the next prompt: “Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950.”
    4. The caller enters his/her date of birth and again receives a prompt from the automated system: “Thank you. Now please type your PIN, followed by the pound key.”
    5. The caller enters his PIN and hears one last prompt from the system: “Thank you. We will now transfer you to the appropriate representative.” At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

Vishing

How to Protect from Vishing Attacks

- Following are some tips to protect oneself from Vishing attacks:
    1. Be suspicious about all unknown callers.
    2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
    3. Be aware and ask questions, in case someone is asking for your personal or financial information.
    4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
    5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

Smishing

- Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing.
- The name is derived from “SMS PhISHING.”
- SMS can be abused by using different methods and techniques other than information gathering under cybercrime.
- Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI.
- The popular technique to “hook” (method used to actually “capture” your information) the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI.
- Smishing works in the similar pattern as Vishing.

Smishing

How to Protect from Smishing Attacks

- Following are some tips to protect oneself from Smishing attacks:
    1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
    2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

Smishing

How to Protect from Smishing Attacks

- Following are some tips to protect oneself from Smishing attacks:

3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

Hacking Bluetooth

- Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile device.
- Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication.
- The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.
- When Bluetooth is enabled on a device, it essentially broadcasts “I’m here, and I’m able to connect” to any other Bluetooth-based device within range.
- This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers.

Hacking Bluetooth

Bluetooth hacking tools

1. **BlueScanner:** This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2. **BlueSniff:** This is a GUI-based utility for fi nding discoverable and hidden Bluetooth enabled devices.
3. **BlueBugger:** The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4. **Bluesnarfer:** If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5. **BlueDiving:** Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

Hacking Bluetooth

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

1. **Bluejacking:** It means Bluetooth + Jacking where Jacking is short name for hijack – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.
2. **Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

Hacking Bluetooth

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

3. Bluebugging: It allows attackers to remotely access a user's phone and use its features without user's attention.
4. Car Whisperer: It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

- Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking.
- These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

Hacking Bluetooth

"Bluetooth and Bluetooth Security" is a separate subject in itself. Readers may visit the following websites to explore more on this topic:

- https://www.bluetooth.org/apps/content/
- http://www.bluetooth.com/English/Pages/default.aspx
- http://www.bluetoothhack.info/