PMCA605L : Cyber Security

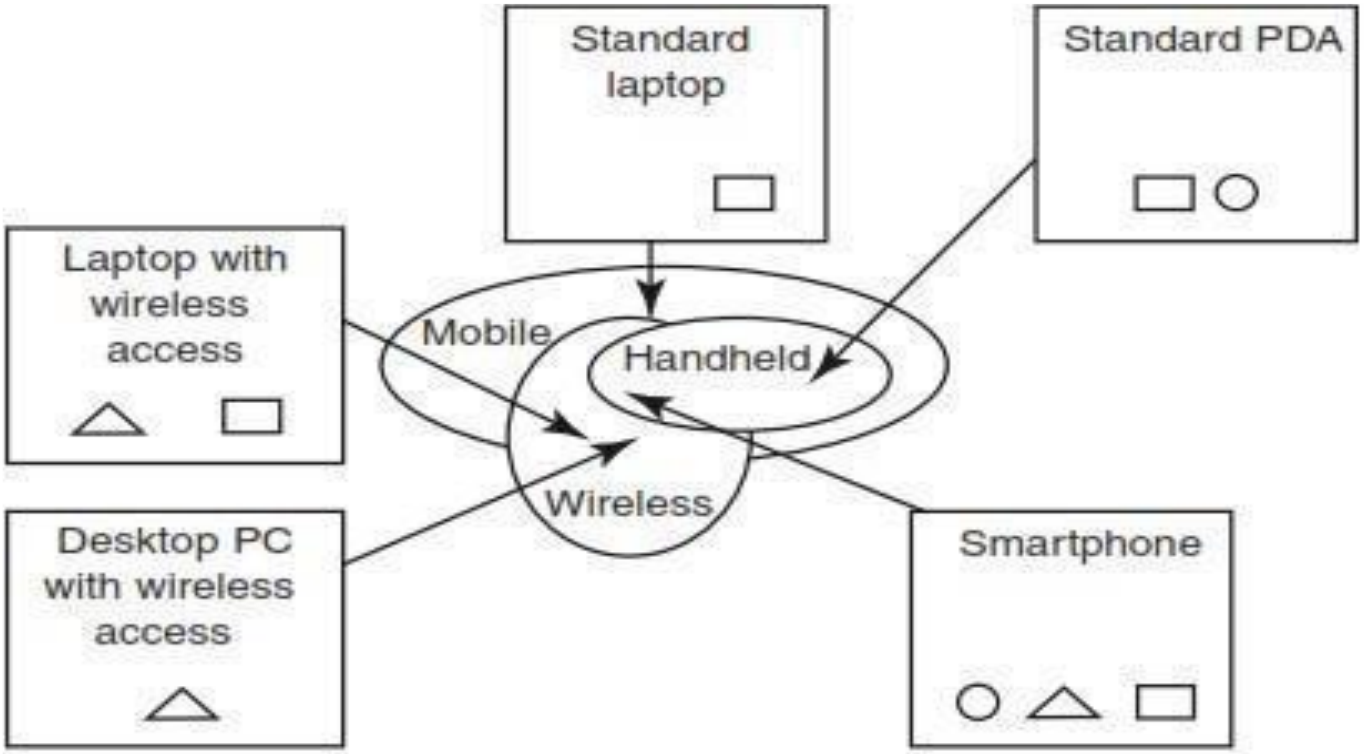
Module 2 : Cyber Crime

Courtesy: Nina Godbole, Sunit Belapure *& Other Sources of Internet*

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Dr. R. K. Nadesh

Mobile, Wireless Devices and Hand-held devices



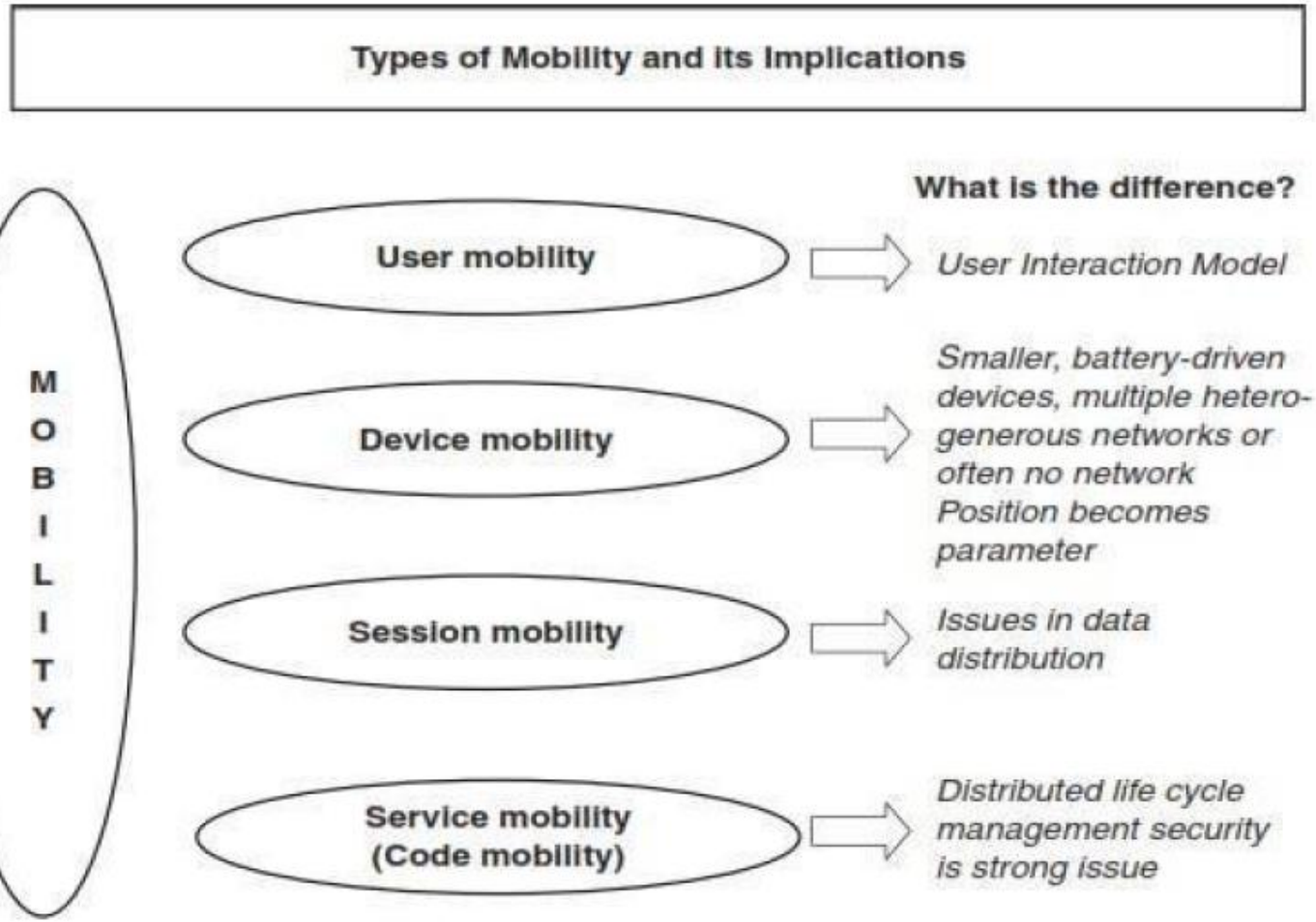
PDA – Personal digital assistant

□ – Mobile device

△ – Wireless device

○ – Handheld device

Mobility types and implications



Trends in Mobility

- ✓ **Wireless** refers to transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection.

- ✓ **Smart hand-held** are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network and can have software installed on them.

- ➢ The larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data, and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity.

BYOD

Trends in Mobility : 3G, 4G, and 5G networks

- 3G/4G/5G promises greater variety in applications, highly improved usability, and speedier networking.
- This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
- There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors.
- One is from outside the mobile network – public Internet, private networks and other operator's networks
- The other is within the mobile networks – devices such as data-capable handsets and Smartphones, notebook computers, or even desktop computers connected to the 3G/4G network.

Popular types of attacks against 3G mobile networks

1. Malware, viruses, and worms
2. Denial-of-service (DoS)
3. Overbilling attack
4. Spoofed policy development process (PDP)
5. Signaling-level attacks

Common Attacks on 3G, 4G, and 5G Networks

- **Man-in-the-Middle (MITM) Attacks:** Intercepting communication between the user device and the network, attackers can eavesdrop, alter, or steal sensitive data.

- **Denial of Service (DoS) and Distributed DoS (DDoS):** Overloading network resources with excessive traffic can disrupt services, affecting legitimate users.

Common Attacks on 3G, 4G, and 5G Networks

- **IMSI Catchers (Stingray Attacks) :** Devices impersonate legitimate cell towers to capture IMSI (International Mobile Subscriber Identity) numbers.

  - Often used in 3G and 4G due to weaker mutual authentication.

  - 5G introduces stronger protections against such attacks, but improperly configured networks remain vulnerable.

Common Attacks on 3G, 4G, and 5G Networks

- **SMS Spoofing and Phishing:** Attackers send fraudulent SMS messages to trick users into revealing sensitive information or downloading malware.

- **Rogue Base Stations**: Fake base stations are set up to lure mobile devices, allowing attackers to intercept or manipulate data.

- **Network Sniffing**: Using tools to monitor and capture unencrypted traffic between the device and the network.

4G-Specific Attacks

- **LTE Jamming:** Interference with LTE signals prevents devices from connecting to the network, causing denial of service.

- **Downgrade Attacks**: Forcing a device to switch from 4G to less secure 2G or 3G networks allows attackers to exploit vulnerabilities in those networks.

- **Control Plane Signaling Attacks:** Overloading the signaling plane of an LTE network can lead to service degradation or outages.

- **VoLTE (Voice over LTE) Attacks:** Exploiting vulnerabilities in VoLTE implementations can lead to call interception or manipulation.

5G-Specific Attacks

- **Edge Computing Threats:** Mobile Edge Computing (MEC) nodes in 5G networks can become targets for attackers seeking to compromise localized data processing and services.

- **Virtualization Vulnerabilities:** 5G networks heavily use software-defined networking (SDN) and network function virtualization (NFV), which may have exploitable vulnerabilities if not properly secured.

- **IoT Device Exploitation:** With 5G's support for massive IoT connectivity, poorly secured IoT devices become entry points for attackers to compromise the network.

Credit Card Frauds in the Mobile and Wireless Computing Era

- Wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere.

- It allows businesses to quickly, efficiently, and professionally process transactions from mobile locations.

- Some upscale restaurants are using wireless processing equipment to secure their credit card-paying customers.

Credit Card

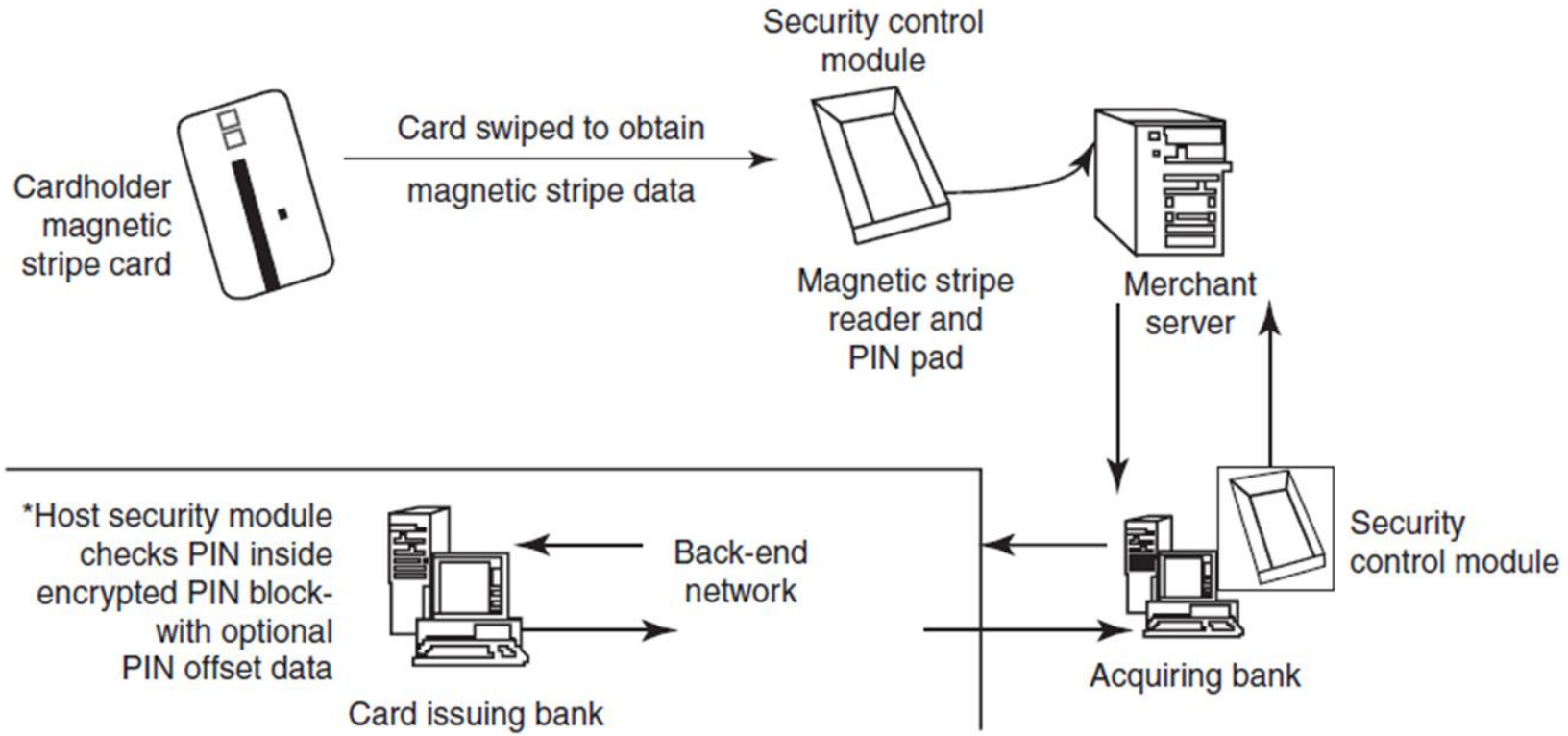


Figure 1 Online environment for credit card transactions.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Key Components in Credit Card Architecture

- **Cardholder:** The individual using the credit card to make a purchase.
- **Merchant:**The business or vendor that accepts credit card payments.
- **Point of Sale (POS) System or Payment Gateway**: The terminal or online interface where the card details are captured.
- **Acquiring Bank (Merchant's Bank):** The bank that processes transactions for the merchant and sends the payment request to the card network.

Key Components in Credit Card Architecture

- **Card Network:** Networks like Visa, Mastercard, or American Express act as intermediaries to facilitate communication between the acquiring and issuing banks.

- **Issuing Bank:** The bank or financial institution that issued the credit card to the cardholder.

- **Payment Processor:** A third-party service provider that handles transaction processing between the merchant and the card network.

Steps in Credit Card Transaction Processing

- **Cardholder Action**: The cardholder initiates a payment by swiping, tapping, inserting their card, or entering card details online.
- **Merchant Action:** The POS or payment gateway sends the transaction details to the acquiring bank.
- **Acquirer Action:** The acquiring bank forwards the request to the card network.
- **Card Network Action:** The card network communicates with the issuing bank to validate the card details, available credit, and transaction legitimacy.
- **Issuer Action**: The issuing bank approves or declines the transaction and sends the response back through the network to the acquirer, and then to the merchant.

Types and Techniques of Credit Card Frauds

- *Traditional Techniques*

➢ Paper-based 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*
- **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.

Card-Present Fraud (Physical Fraud)

- Fraudsters steal or clone the physical credit card to make unauthorized transactions.

Common methods:

- Lost or Stolen Cards: Using cards obtained from theft or loss.
- Card Skimming: Capturing card details using a skimming device at ATMs or point-of-sale (POS) terminals.

Techniques of Credit Card Frauds

- **Skimming:**

✓ A device is attached to ATMs or POS terminals to capture card information during legitimate transactions.

✓ Often paired with hidden cameras to capture PINs.

- **Data Breaches**

✓ Hacking into databases of companies to steal large volumes of cardholder information.

✓ Commonly seen in large-scale cyberattacks.

Techniques of Credit Card Frauds

- **Eavesdropping and Shoulder Surfing:** Physically observing or listening to users entering their card details or PINs.
- **Malware and Keyloggers :** Fraudsters infect devices with malware to capture keystrokes or screenshots during online transactions. Common in unprotected or public systems.
- **Man-in-the-Middle (MITM) Attacks :** Intercepting communication between a user and a website during online transactions to steal card data. Often occurs on insecure or public Wi-Fi networks.

Techniques of Credit Card Frauds

- **SIM Swap Fraud:** Fraudsters trick telecom operators into issuing a new SIM card with the victim's number, intercepting OTPs and other security codes.

- **Fake Websites:** Fraudsters create fake replicas of legitimate websites to trick users into entering their card details.

- **Social Engineering:** Manipulating individuals into revealing card details via psychological tricks or impersonation.

Modern Techniques

- Skimming to commit fraud: 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.

- Site cloning and false merchant sites on the Internet - designed to get people to hand over their credit card details. (Triangulation)

- Use Credit Card Generators (Software)

Security Challenges Posed by Mobile Devices

- *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.*

Managing the registry settings and configurations.

- Microsoft ActiveSync acts as the gateway between a Windows-powered PC and a Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos, and applications from a user's desktop to his/her device.

- It can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs.

- Establishing trusted groups through appropriate registry settings becomes crucial.

- One of the most prevalent areas where this attention to security is applicable is within "group policy."

- New mobile applications are constantly being provided to help protect against Spyware, viruses, worms, malware, and other Malicious Codes that run through the networks and the Internet.

- The core problem of many mobile security issues on a Windows platform is that the baseline security is not configured properly.

Registry Settings for Mobile Devices

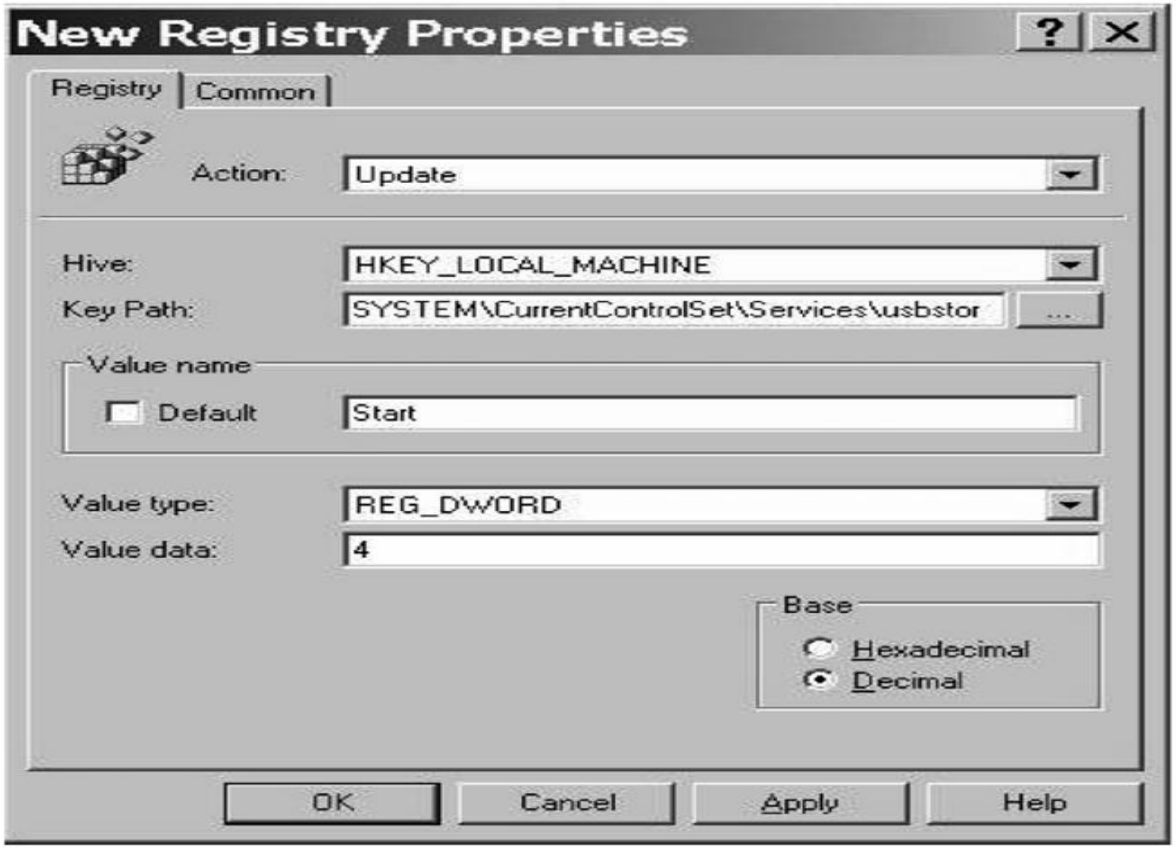


Figure 2 Registry value browsing.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Authentication Service Security

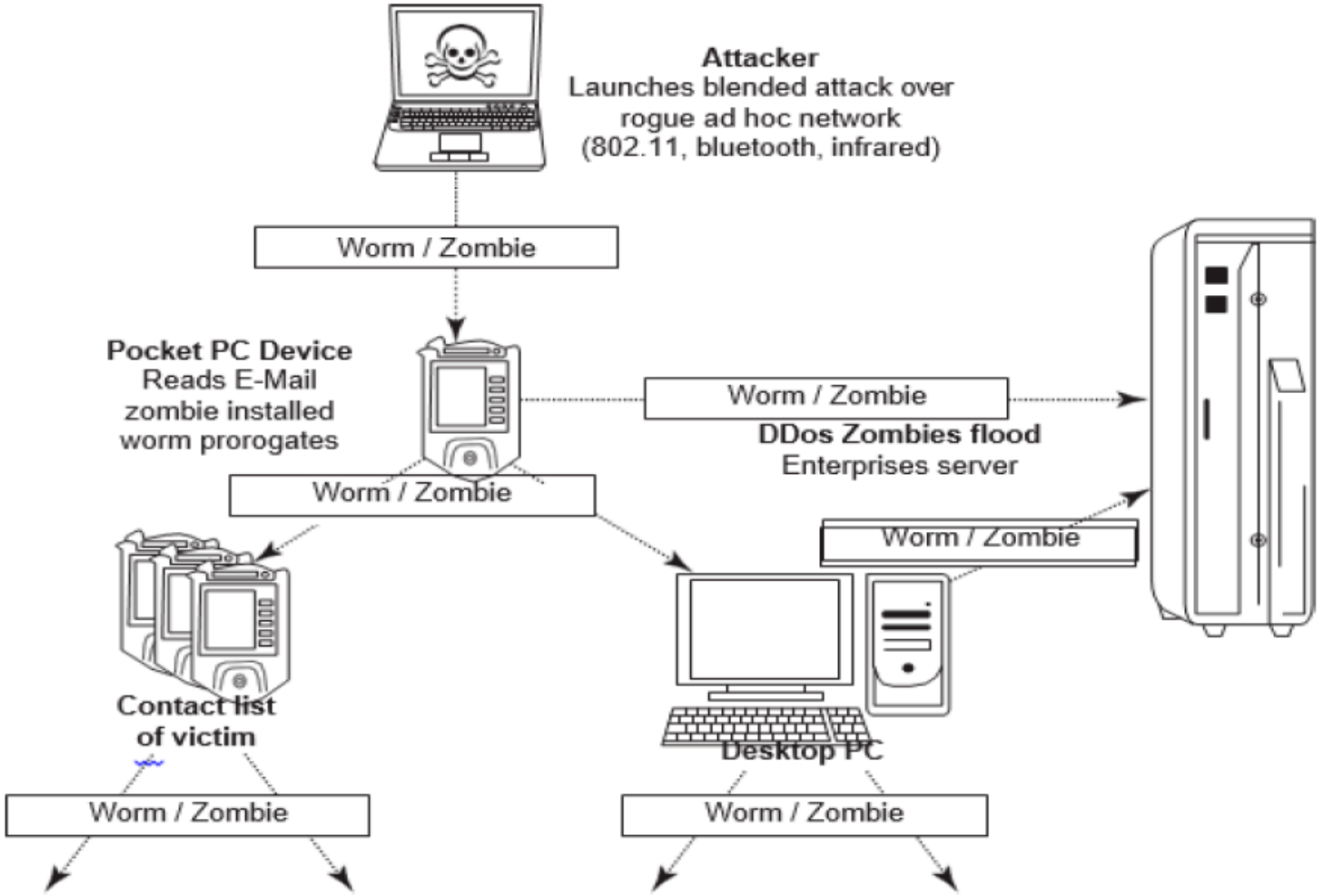
- There are two components of security in mobile computing
  - *security of devices*
  - *security in networks*

- A secure network access involves mutual authentication between the device and the base stations or Web servers.

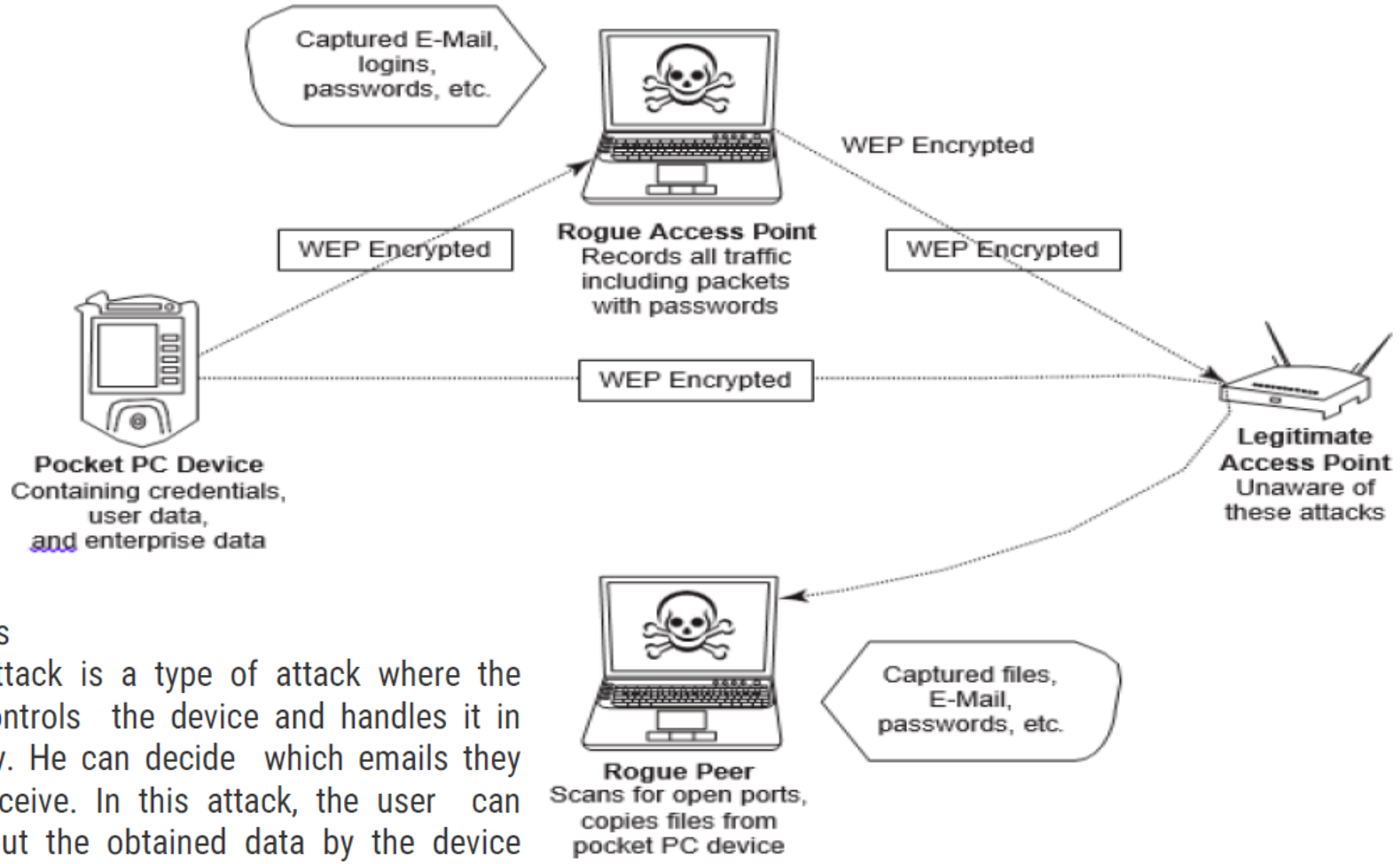
- Authentication services security is important given the typical attacks on mobile devices through wireless networks: DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks, and session hijacking.

  - Security measures in this scenario come from *Wireless Application Protocols* (WAPs), use of *VPNs*, *media access control* (*MAC*) *address filtering* and development in 802.xx standards.

Push attack on mobile devices



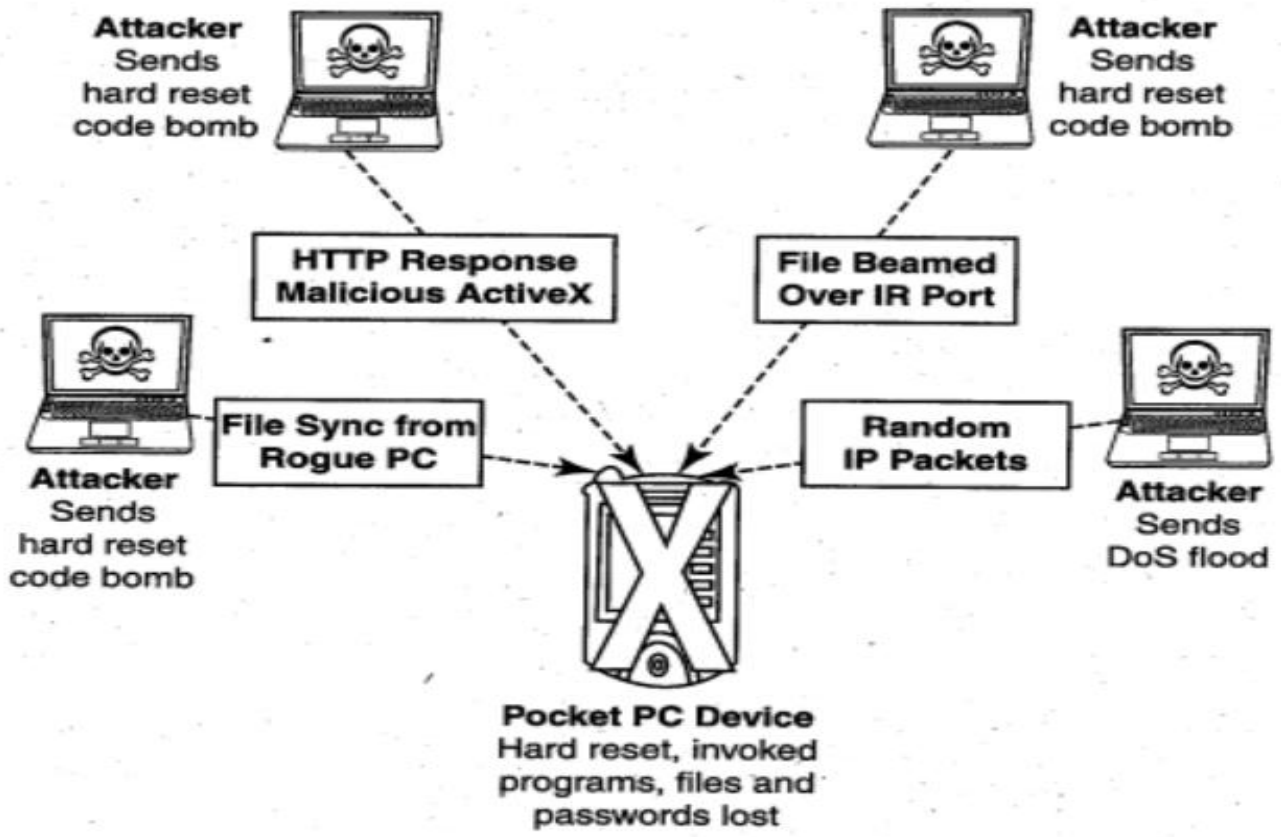
Pull attack on mobile devices



Pull Attacks

The pull attack is a type of attack where the attacker controls the device and handles it in his/her way. He can decide which emails they want to receive. In this attack, the user can decide about the obtained data by the device itself.

Crash Attack on Mobile Device



Cryptographic Security for Mobile Devices

- *Cryptographically generated addresses* (CGA) is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.

- The address the owner uses is the corresponding private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure.

- Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices.

LDAP 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.

- It is a light weight version of Directory Access Protocol (DAP) because it does not include security features in its initial version.

Media Player Control Security

- Media player can turn out to be a source of threat to information held on mobile devices.

- 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.

- In the registry, there are some keys which control the behavior of the Windows Media Player control. Microsoft, through its developer network MSDN, describes details of registry value settings on the mobile devices.

Networking API Security for Mobile Computing Applications

- ✓With *E-Commerce* and *M-Commerce,* online payments are becoming a common phenomenon with the *payment gateways* accessed remotely and possibly wirelessly.

- ✓With *Web services* and their use in mobile computing applications, the API becomes an important consideration.

RAS Security for Mobile Devices

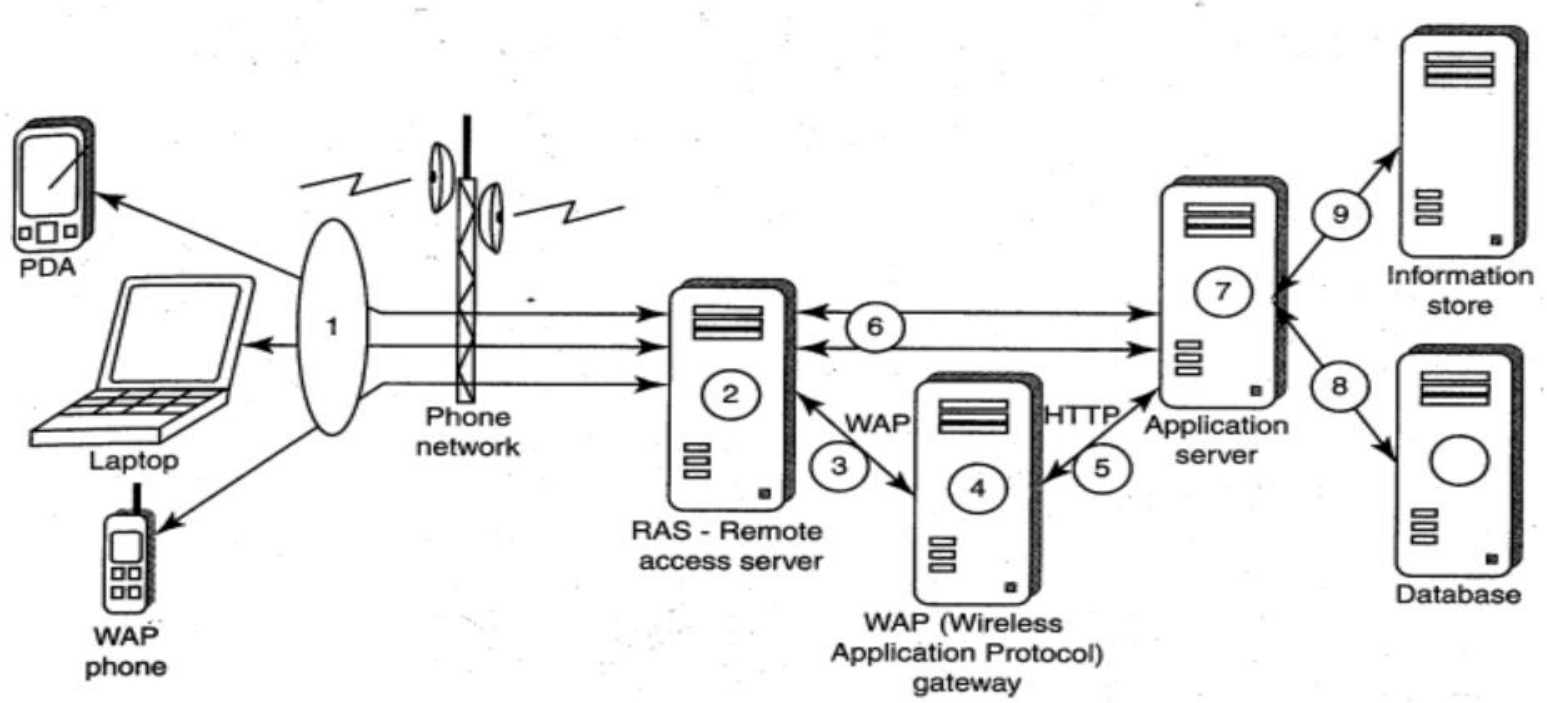
RAS is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices.

- *Impersonating* or *masquerading* - By using a mobile device to appear as a registered user to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

- *Port scanning* - First, attackers use a domain name system (DNS) server to locate the *IP address* of a connected computer. 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.

- 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.

Remote Access Server (RAS) security.



Attacks on Mobile Phone

- Mobile phones are increasingly targeted by cyberattacks due to their widespread usage, storage of sensitive data, and connection to the internet.

- Bluetooth and MMS (Multimedia Messaging Service) are two communication protocols that have historically been exploited to spread mobile viruses

Mobile Viruses

- 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.

How to Protect from Mobile Malwares Attacks?

1. Download or accept programs and content 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

- Definition: A specific type of phishing that uses malicious apps or malware on mobile devices to steal information.
- Medium: Mobile applications or malicious software installed on smartphones.
- Example: Downloading a fake app that secretly tracks your keystrokes or accesses personal data.

Phishing

- Definition: A broad term for scams involving deceptive communication designed to trick victims into revealing sensitive information, such as usernames, passwords, or financial data.
- Medium: Primarily email but can also include fake websites or instant messaging.
- Example: Receiving an email that appears to be from your bank, asking you to click on a link and update your account information.

Vishing (Voice Phishing)

- Definition: Phishing conducted via phone calls where attackers impersonate legitimate organizations to extract information or money.
- Medium: Telephone or voice communication.
- Example: A scammer pretending to be a tax official and threatening legal action unless you provide personal details or make a payment over the phone.

Smishing (SMS Phishing)

- Definition: Phishing via text messages (SMS), luring victims to click malicious links or provide sensitive information.
- Medium: SMS or text messages.
- Example: Receiving a text claiming you've won a prize and need to click a link to claim it, which then leads to a fraudulent website.

Summary

Type	Medium	Example
Phishing	Email, websites, instant messages	Fake email from a bank asking for login credentials.
Mishing	Mobile apps, malware	Malicious app that steals data from your phone.
Vishing	Phone calls	Caller pretending to be tech support asking for login details.
Smishing	SMS/Text messages	Text claiming you've won a prize with a link to a fake site.

To protect yourself, always verify communication sources, avoid clicking unknown links, and refrain from sharing sensitive information without proper validation.

Hacking Bluetooth

- Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication.

- An attacker installs special software on a laptop and then installs a Bluetooth antenna that constantly scans the nearby surroundings for active Bluetooth connections.

- Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls, and much more.

Common Attacks -Bluetooth

- **Bluejacking** - Sending unsolicited messages to nearby Bluetooth-enabled devices.

- **Bluesnarfing** - Unauthorized access to data on a Bluetooth-enabled device. (An attacker accesses your phone's contacts without your knowledge)

- **Bluebugging** - Gaining control over a Bluetooth-enabled device without the owner's consent. (A hacker takes control of your phone and uses it to send messages or make calls.)

Common Attacks -Bluetooth

- **Bluesmack** - A Denial-of-Service (DoS) attack that overwhelms a device with Bluetooth requests, causing it to crash or become unresponsive.

- **Blueborne** - Exploiting vulnerabilities in Bluetooth protocols to execute malicious actions on a device. (The attacker can install malware, steal data, or take control of the device.)

- **CarWhispering** - Exploiting weaknesses in Bluetooth-enabled car systems to eavesdrop or send audio messages.

- **Bluetooth Impersonation Attack (BIAS)** - Exploiting flaws in the Bluetooth authentication process to impersonate a trusted device. (An attacker pretends to be a previously paired device to connect automatically.)

Protection Against Bluetooth Attacks

- **Turn Off Bluetooth**: Disable Bluetooth when not in use.
- **Avoid Unknown Pairing Requests**: Reject pairing requests from unknown devices.
- **Update Firmware**: Keep your device's firmware and software updated to patch vulnerabilities.
- **Use Strong Pairing Codes**: Avoid default or easily guessable PINs.
- **Limit Visibility**: Set your device's Bluetooth to "non-discoverable" mode when not pairing.
- **Install Security Software**: Use trusted antivirus or security apps that monitor Bluetooth activity.

Bluetooth Hacking Tools

- **Scanning and Discovery Tools** -Scans for Bluetooth devices and retrieves details like MAC addresses and device names. **(Bluescanner)**
- **Sniffing Tools** - Sniffing tools intercept and analyze Bluetooth communication. **(BlueSniff)**
- **Exploitation -** Tools exploit vulnerabilities in Bluetooth implementations**. (BTCrack, Bluebugger)**
- **Jamming and DoS Tools –**

Bluetooth Jammer: Blocks Bluetooth communication in a specified range by sending interference signals.

Bluesmack: Sends malformed packets to crash or freeze Bluetooth devices.

Bluetooth Hacking Tools

Bluelog: A simple Bluetooth scanner designed to create a log of discoverable devices.

Bluepot: A Bluetooth honeypot used to detect and log attacks on Bluetooth networks.

Bluediving is a penetration testing tool designed for Bluetooth security auditing. It includes various modules to exploit vulnerabilities in Bluetooth devices, primarily targeting older or improperly secured implementations.

Organizational Policy for Mobile Hand-Held Device Use

- This policy applies to all employees, contractors, and third parties using mobile hand-held devices to access the organization's network, systems, or sensitive data.

- To ensure the appropriate, secure, and responsible use of mobile hand-held devices (e.g., smartphones, tablets) in the organization, maintaining productivity, security, and compliance with legal standards.

Policy Guidelines

- **Acceptable Use:** Mobile devices may only be used for tasks directly related to job responsibilities.

- **Device Security:**

✓ All devices must be password-protected, with strong passcodes that comply with organizational standards.

✓ Devices must have installed up-to-date antivirus software and the latest operating system updates.

✓ Remote wipe capability must be enabled to prevent unauthorized access in case of loss or theft.

Policy Guidelines

Data Protection :

- ✓ Sensitive organizational data must not be stored locally on mobile devices unless authorized.
- ✓ Data transmitted over public Wi-Fi must use a Virtual Private Network (VPN).
- ✓ Cloud synchronization for work data must only occur through approved platforms.

Policy Guidelines

App Usage :

- ✓ Only approved applications may be downloaded and used for work-related activities.
- ✓ Employees must refrain from downloading apps from unofficial sources that could compromise security.

Policy Guidelines

Bring Your Own Device (BYOD)

- Employees using personal devices must enroll in the organization's Mobile Device Management (MDM) system.

- BYOD users must adhere to the same security and acceptable-use guidelines as company-provided devices.

Policy Guidelines

Lost or Stolen Devices

- Any lost or stolen device must be reported to the IT department immediately.
- The organization may remotely disable or wipe the device to prevent data breaches.

Policy Guidelines

Monitoring and Privacy

- The organization reserves the right to monitor usage of company-provided devices and apps for compliance with policies.

- Personal data on employee-owned devices remains private, except in cases involving security incidents or policy violations.

Policy Guidelines

Prohibited Activities

- Usage of mobile devices while driving or in restricted work areas (e.g., labs) unless hands-free is allowed and safe.

- Accessing, sharing, or storing inappropriate or illegal content.

Disciplinary Actions

- Violations of this policy may result in disciplinary action, up to and including termination, depending on the severity.

Policy Guidelines

Compliance and Accountability

- **Regular Training**:
  - Conduct workshops and refresher courses on mobile security.
- **Enforcement**:
  - Enforce strict consequences for non-compliance with security guidelines.
- **Feedback Mechanism**:
  - Encourage reporting of issues and suggestions to improve security practices.

Including Mobile Devices in Security Strategy

A few things that enterprises can use are:

1. 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.

2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.

3. Develop a system of more frequent and thorough security audits for mobile devices.

4. Incorporate security awareness into your mobile training and support programs.

5. Notify the appropriate law-enforcement agency and change passwords.

Identity and Access Management (IAM)

- Identity management, often referred to as Identity and Access Management (IAM), is a set of processes, policies, and technologies that organizations use to manage and secure digital identities.

- To enable the **right individuals** to access the **right resources** at the **right times** for the right reasons by **authentication** and **authorisation** of identities and access.

- One of the most common ways to control access to computer systems is to identify who is at the keyboard (and prove that identity), and then decide what they are allowed to do.

- **Single Sign-On (SSO):** Allowing users to log in once and gain access to multiple systems or applications without the need to re-authenticate for each one.

Authentication & Authorization

- Authentication is the means of verifying who a **person** (or process) is, while authorization determines what they're **allowed to do**.

- This should always be done in accordance with the principle of least privilege—giving each person only the amount of access they require to be effective in their job function, and no more.

Authentication

- Two parts: a public statement of identity (usually in the form of a *username*)
- Combined with a private response to a challenge (such as a *password*). ***single-factor authentication***
- The secret response to the authentication challenge can be based on **one or more factors**—(***secret word, number, or passphrase, smartcard, ID tag, or code generator, biometric factor like a fingerprint or retinal print***)

Multifactor authentication

- Two or more methods of check-in
- Something you know (a password or PIN code)
- Something you have (such as a card or token)
- Something you are (a unique physical characteristic) identity

Access Control

- **Who should have access to what resource?**

  (Assignment of entitlements to users)

- **Why should the user have access to the resource?**

  (Assignment of entitlements based on the user's job functions and responsibilities)

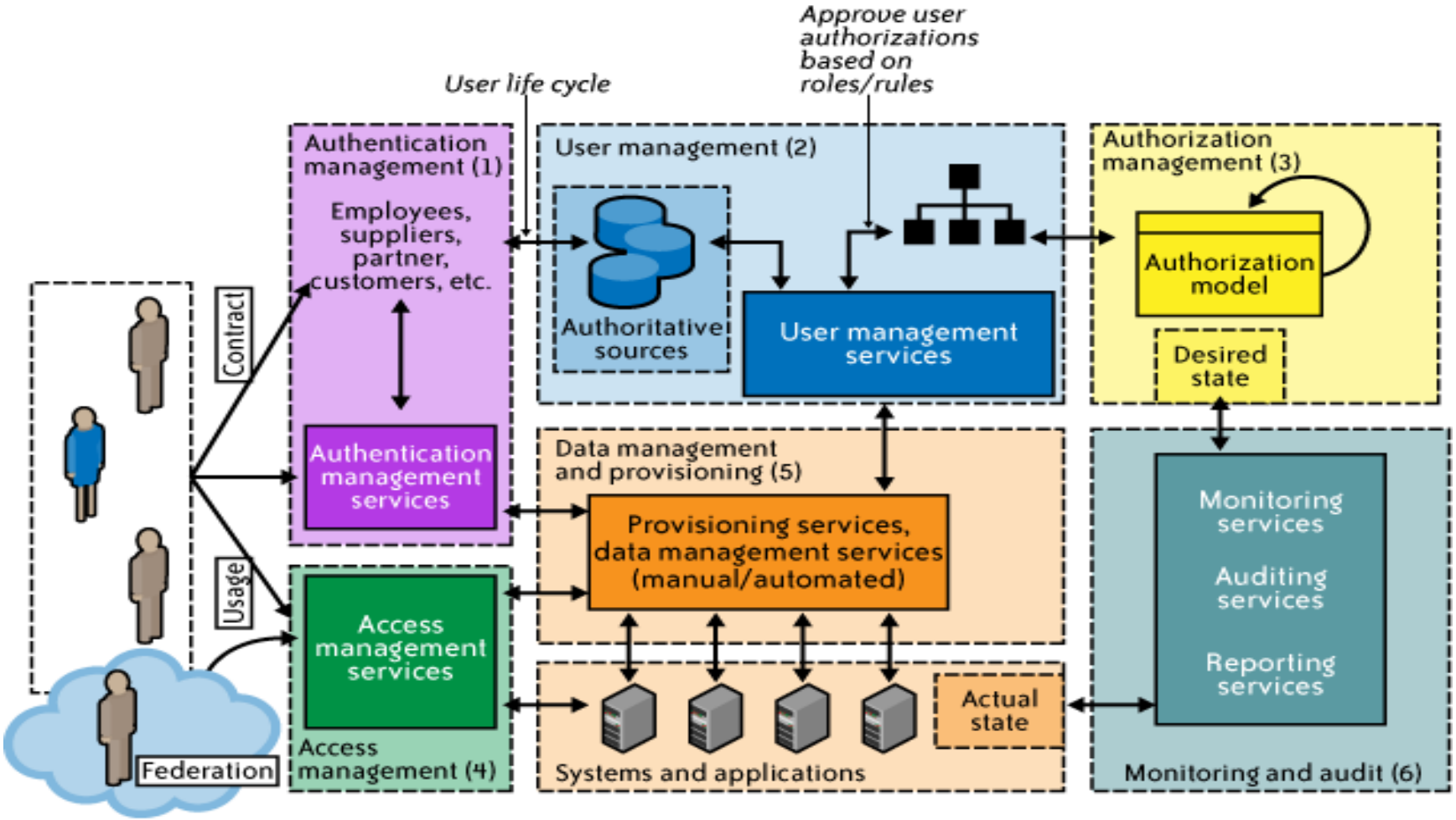
- **How should the user access the resource?**

  (What authentication method and strength are required prior to granting access to the resource)

- **Who has access to what resource?**

  (Auditing and reporting to verify entitlement assignments)

IAM Architecture



IAM Architecture

- **User Management:-** It consists of activities for the control and management over the identity life cycles.
- **Authentication Management:-** It consists of activities for effectively controlling and managing the processes for determining which user is trying to access the services and whether those services are relevant to him or not.
- **Authorization Management:-** It consists of activities for effectively controlling and managing the processes for determining which services are allowed to access according to the policies made by the administrator of the organization.
- **Access Management:-** It is used in response to a request made by the user wanting to access the resources with the organization.

IAM Architecture

- **Operational Activities of IAM:-** In this process, onboard the new users on the organization's system and application and provide them with necessary access to the services and data. Deprovisioning works completely opposite in that we delete or deactivate the identity of the user and de-relinquish all the privileges of the user.

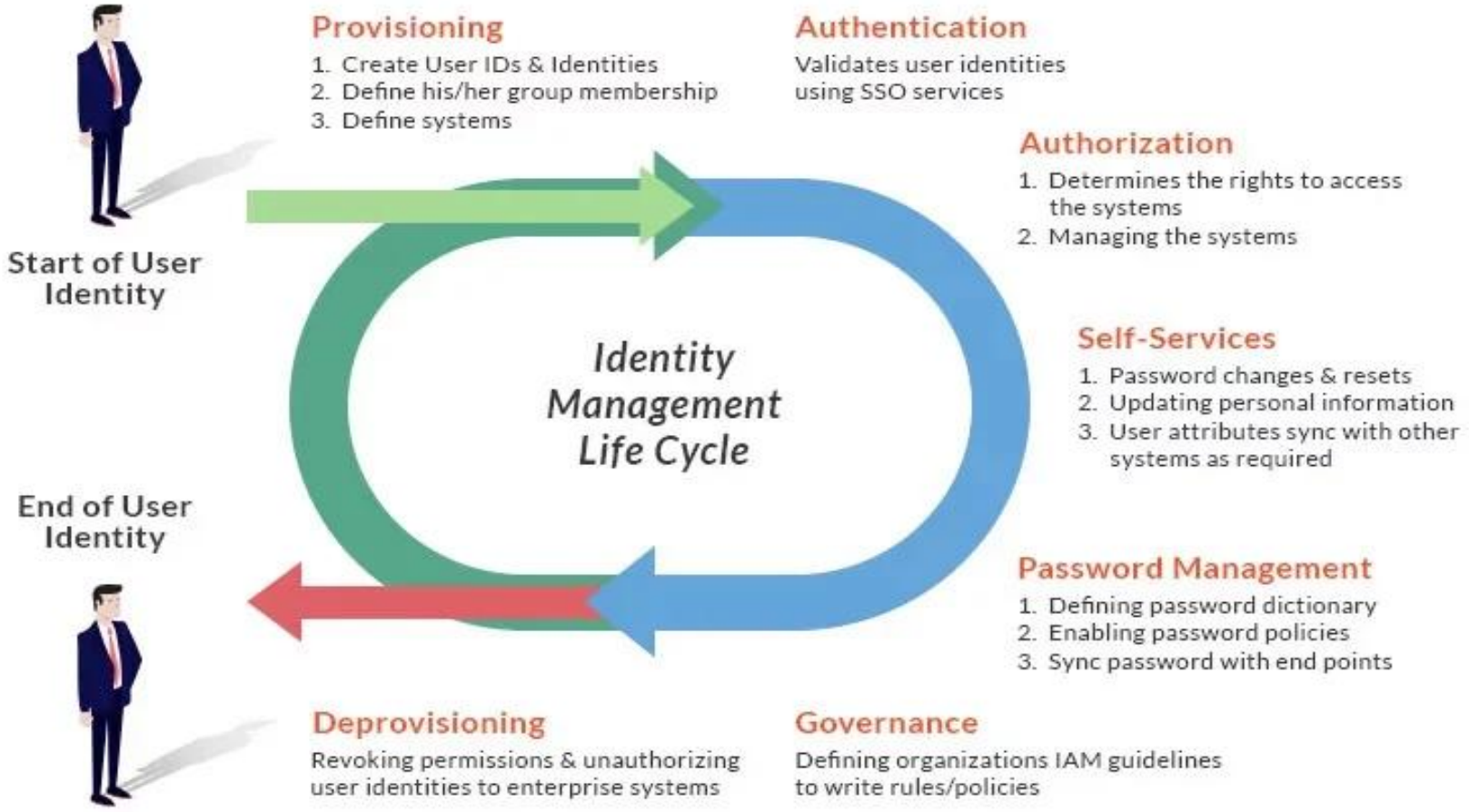
- **Credential and Attribute Management:-** Credentials are bound to an individual user and are verified during the authentication process. These processes generally include allotment of username, static or dynamic password, handling the password expiration, encryption management, and access policies of the user.

IAM Architecture

- **Entitlement Management:-** These are also known as authorization policies in which we address the provisioning and de-provisioning of the privileges provided to the user for accessing the databases, applications, and systems. We provide only the required privileges to the users according to their roles. It can also be used for security purposes.

- **Identity Federation Management:-** In this process, we manage the relationships beyond the internal networks of the organization that is among the different organizations. The federations are the associates of the organization that came together to exchange information about the user's resources to enable collaboration and transactions.

Identity Management Life Cycle



Identity and Access Management Standards

- Identity and access management standards are critical for ensuring system security, data confidentiality, and integrity in an era where many organizations rely on cloud services, Internet of Things (IoT) connectivity, Artificial Intelligence (AI), and machine learning.

Key IAM Standards

1. Authentication Standards

- **OAuth 2.0**: Open standard for access delegation, allowing third-party applications to request limited access to user accounts. Commonly used for API security and user consent workflows.

- **OpenID Connect (OIDC)**

✓ Authentication layer built on top of OAuth 2.0.
✓ Enables user authentication and retrieval of basic profile information.
✓ Widely used for Single Sign-On (SSO).

- **SAML (Security Assertion Markup Language)**

✓ Commonly used for federated identity and SSO.
✓ XML-based protocol for exchanging authentication and authorization data between parties.

- **Kerberos**

✓ Protocol for secure authentication in distributed networks using tickets.
✓ Commonly used in enterprise environments, such as Microsoft Active Directory.

IAM Standards

2. Access Control Standards

- **RBAC (Role-Based Access Control)**
  - Assigns permissions to roles rather than individual users, simplifying management.
  - Standardized in ANSI INCITS 359-2004.
- **ABAC (Attribute-Based Access Control)**
  - Access control decisions are based on attributes (e.g., user roles, location, or device type).
  - Provides more granular and dynamic access control.
- **PBAC (Policy-Based Access Control)**
  - Leverages policies and logical rules to define access permissions.
  - Often integrated with ABAC for fine-grained control.

IAM Standards

3. Identity Federation Standards

- **Federated Identity Management (FIM)**
  - Allows users to access multiple systems across organizational boundaries with a single identity.
  - Protocols include SAML, OIDC, and WS-Federation.
- **SCIM (System for Cross-domain Identity Management)**
  - Open standard for automating user provisioning and deprovisioning across multiple systems.
  - Ensures consistent identity information across platforms.

IAM Standards

4. Credential Management Standards

- FIDO2
  - Authentication standard that enables passwordless login using hardware tokens, biometrics, or PINs.
  - Supported by the Fast Identity Online (FIDO) Alliance.
- X.509
  - Standard for digital certificates used in public key infrastructure (PKI) to verify identity.

IAM Standards

5. Regulatory and Compliance Standards

- **ISO/IEC 27001**
  - International standard for information security management systems, including IAM practices.
  - Helps organizations protect sensitive information.
- **NIST SP 800-63**
  - U.S. federal guidelines for digital identity management, covering identity proofing, authentication, and federation.
- **GDPR (General Data Protection Regulation)**
  - European regulation requiring strong data protection measures, including identity and access control mechanisms.
- **HIPAA (Health Insurance Portability and Accountability Act)**
  - U.S. regulation enforcing secure access to healthcare information.

IAM Standards

6. Privileged Access Management (PAM) Standards

- ISO/IEC 27002
  - Provides guidelines for managing privileged access.
  - Emphasizes the principle of least privilege and logging privileged activities.

IAM Standards

7. Interoperability Standards

- **LDAP (Lightweight Directory Access Protocol)**
  - Standard protocol for accessing and managing directory information.
  - Used by systems like Active Directory for storing user identities.
- **WS-Federation**
  - Web services standard for federated identity management.
  - Allows single sign-on across different domains and platforms.

Key Principles in IAM Standards

1. **Single Sign-On (SSO)**
    - Centralized authentication enabling users to log in once and access multiple systems.
2. **Multi-Factor Authentication (MFA)**
    - Requires two or more authentication factors to verify user identity.
3. **Zero Trust Security**
    - Assumes no implicit trust; requires continuous verification for all access requests.
4. **Access Governance**
    - Regularly reviews access rights to ensure compliance with policies and minimize risks.
5. **Identity Federation**
    - Integrates identities across multiple systems, organizations, or domains.

Benefits of IAM Standards

- **Enhanced Security:** Protect against unauthorized access and data breaches.
- **Interoperability:** Enable systems and services to work seamlessly together.
- **Regulatory Compliance:** Meet legal and industry-specific security requirements.
- **Operational Efficiency:** Reduce administrative overhead through automation and centralization.

Summary

- Mobile and Wireless Devices.
- Credit Card Fraud in mobile and wireless computing.
- Attacks on Mobile Phone.
- Organizational Security Policies.
- Identity and Access Management.

References: Nina Godbole, Sunit Belapure, “Cyber Security - Understanding Cybercrimes, Computer Forensics and Legal Perspectives”, 2018, 1st Edition, Wiley.