CYBERCRIME: MOBILE & WIRELESS DEVICES

Quick Exam Notes
*Brought to you by **ZenYukti***

1. Introduction — Mobile & Wireless Devices

- **Mobile Device:** Portable computing device — smartphones, tablets, PDAs, laptops
- **Wireless Device:** Communicates without physical cables — uses Wi-Fi, Bluetooth, NFC, cellular
- Mobile computing = perform computing tasks anywhere using wireless networks
- Rapid growth → massive attack surface for cybercriminals
- Mobile devices now store: contacts, emails, banking apps, photos, location data — goldmine for attackers

⚠ *More data on mobiles = more attractive target than desktop PCs*

2. Proliferation of Mobile & Wireless Devices

- **Proliferation:** Rapid increase and spread of mobile devices worldwide
- Factors driving proliferation:
  - Affordable smartphones — billions of users globally
  - Cheap mobile internet (4G/5G) — always connected
  - BYOD (Bring Your Own Device) trend in workplaces
  - Mobile banking, e-commerce, social media — all on phone
  - IoT devices — smart TVs, smart watches, smart home devices
- Result: More devices = more entry points for attackers
- India: 2nd largest smartphone market globally → huge cybercrime risk

3. Trends in Mobility

Trend	Description	Security Risk
BYOD	Employees use personal devices for work	Mix of personal & corporate data
COPE	Company-Owned, Personally Enabled devices	Difficult to control personal use
5G Networks	Ultra-fast, low latency connectivity	More devices connected, larger attack surface
IoT Integration	Smart devices connected to internet	Weak security in IoT devices
Mobile Payments	UPI, NFC payments, digital wallets	Transaction interception, fraud
Mobile Cloud	Data stored on cloud, accessed via mobile	Data breaches, account hijacking
MDM Solutions	Mobile Device Management for enterprises	If MDM hacked, all devices compromised
Wearables	Smartwatches, fitness bands	Constant biometric data collection — privacy risk

4. Credit Card Frauds in Mobile & Wireless Computing Era

- **Credit Card Fraud:** Unauthorized use of someone's card/card details for financial gain

Types of Credit Card Fraud

- **Skimming:** Hardware device placed on ATM/POS terminal to copy card data
- **Phishing/Vishing:** Fake calls/SMS/emails tricking user into sharing card details
- **SIM Swapping:** Attacker convinces telecom to transfer victim's number to attacker's SIM → bypass OTP
- **Man-in-the-Browser:** Malware intercepts transactions inside the browser
- **Fake Mobile Apps:** Counterfeit banking apps steal credentials
- **Public Wi-Fi Sniffing:** Intercept unencrypted card transactions on open networks
- **Card Not Present (CNP) Fraud:** Using stolen card details for online purchases (no physical card needed)
- **Contactless/NFC Fraud:** Reading card data wirelessly using NFC readers in crowded places

Prevention

- Enable transaction alerts (SMS/email) for every transaction
- Use virtual cards for online shopping
- Never share OTP — banks NEVER ask for it
- Use official banking apps only (verify developer in app store)
- Avoid saving card details on websites

⚠ *SIM swap is the most dangerous — attacker can bypass all OTP-based 2FA*

5. Security Challenges Posed by Mobile Devices

Challenge	Explanation
Loss / Theft	Physical device loss exposes all stored data immediately
Unsecured Wi-Fi	Connecting to open/public Wi-Fi — easy interception
Malware & Spyware	Malicious apps from unofficial stores infect devices
Bluetooth Attacks	Bluejacking, Bluesnarfing via open Bluetooth connections
Outdated OS	Unpatched vulnerabilities exploited by attackers
Weak Passwords/PINs	Easy-to-guess lock screen = easy access
Excessive App Permissions	Apps accessing camera, mic, contacts beyond necessity
Jailbreaking/Rooting	Removes OS security restrictions — highly vulnerable
No Encryption	Data stored unencrypted — readable if device accessed
Synchronization Risk	Auto-sync with cloud/PC can spread malware across devices
SMS-based OTP	SIM swap or SS7 attacks can intercept OTPs
GPS Tracking	Location data leaked through apps — stalking, profiling

6. Registry Settings for Mobile Devices

- **Registry:** Database storing configuration settings for OS and applications on a device
- On Windows Mobile/CE devices: similar to Windows Desktop registry (HKLM, HKCU keys)
- Registry settings control: network access, app permissions, security policies, device behavior

Important Security-Related Registry Settings

- **Device Lock Settings:** Enforce PIN/password, set auto-lock timeout
- **Remote Wipe:** Registry key to enable remote deletion of device data if lost
- **Encryption Policies:** Force storage and SD card encryption
- **VPN Configuration:** Enforce VPN use for corporate network access
- **Application Whitelist:** Allow only approved apps to run
- **Bluetooth/Wi-Fi Policies:** Disable Bluetooth/Wi-Fi when not in use via registry
- In Android/iOS: managed via MDM profiles instead of traditional registry

⚠ *Incorrect registry modification can brick/destabilize the device*

7. Authentication Service Security

- **Authentication:** Verifying the identity of a user before granting access

Authentication Methods on Mobile

Method	Description	Security Level

PIN / Password	Numeric or alphanumeric code	Low–Medium
Biometrics (Fingerprint)	Fingerprint scan	High
Face Recognition	Facial mapping for unlock	Medium–High
Pattern Lock	Draw pattern on screen	Low (easily guessed/smudged)
OTP (One-Time Password)	Sent via SMS or authenticator app	Medium (vulnerable to SIM swap)
Push Notification Auth	Approve login via app notification	High
Authenticator App (TOTP)	Time-based code (Google Auth, Authy)	High
Certificate-based Auth	Digital certificates for enterprise	Very High
Multi-Factor Auth (MFA)	Combine 2+ methods	Very High

- **Single Sign-On (SSO):** One login credential for multiple services — convenient but single point of failure
- **Zero Trust:** Never trust any device by default — verify every access request

Always use MFA — if one factor is compromised, second layer protects you

8. Attacks on Mobile / Cell Phones

Network-Based Attacks

- **Eavesdropping:** Intercepting calls/data over unsecured networks
- **Man-in-the-Middle (MitM):** Attacker sits between phone and network, intercepts traffic
- **SS7 Attack:** Exploit Signaling System 7 (telecom protocol) — intercept calls/SMS globally
- **Rogue Access Point:** Fake Wi-Fi hotspot — users connect thinking it's legitimate

Bluetooth-Based Attacks

- **Bluejacking:** Sending unsolicited messages to Bluetooth-enabled devices
- **Bluesnarfing:** Unauthorized access to device data (contacts, emails) via Bluetooth
- **Bluebugging:** Full control over phone (calls, SMS, internet) via Bluetooth bug
- **BlueBorne:** Critical Bluetooth vulnerability — spreads like worm, no pairing needed

Malware-Based Attacks

- **Mobile Virus/Worm:** Self-replicating malware spreading via SMS, MMS, Bluetooth
- **Trojan Horse:** Malicious app disguised as legitimate (e.g., fake game/utility)
- **Spyware:** Silently monitors activity, keystrokes, location, messages
- **Ransomware:** Locks device/encrypts files, demands payment
- **Adware:** Displays unwanted ads, may redirect browser

Social/Other Attacks

- **Smishing:** Phishing via SMS — fake bank/delivery messages with malicious links
- **Vishing:** Voice call fraud — fake customer support steals credentials
- **SIM Cloning:** Duplicate SIM card to intercept calls and OTPs
- **GPS Spoofing:** Feed false GPS coordinates to device
- **Juice Jacking:** Malware installed via infected USB charging stations

Juice Jacking: NEVER use public USB charging ports — use your own charger/power bank

9. Mobile Devices: Security Implications for Organizations

- Employees using mobiles for work creates risks:
  - Corporate emails, documents, VPN access on personal/mobile devices
  - If device lost/stolen → confidential data exposed
  - Malware on personal phone can spread to corporate network via sync
  - Employees bypass security policies using personal devices

Implication	Risk
Data Leakage	Sensitive corporate data stored/transmitted on unsecured device
Unauthorized Access	Former employees retaining access via old devices
Network Intrusion	Infected mobile device connects to corporate Wi-Fi → spreads malware
Compliance Issues	GDPR, HIPAA etc. violated if data on uncontrolled mobile devices
Shadow IT	Employees use unapproved apps for work — IT team unaware
Insider Threat	Employee intentionally copies data to personal phone
Phishing Gateway	Work emails on mobile — easier to click phishing links on small screen

⚠ *BYOD = highest risk — organization has least control over personal devices*

10. Organizational Measures for Handling Mobile Devices

Technical Measures

- **MDM (Mobile Device Management):** Centrally manage, monitor, and secure all mobile devices
  - Enforce policies, remote wipe, app management, encryption
- **MAM (Mobile Application Management):** Control specific apps rather than entire device
- **MTD (Mobile Threat Defense):** Real-time threat detection on mobile devices
- **Containerization:** Separate work apps/data from personal apps in secure container
- **VPN Enforcement:** All corporate traffic routed through VPN
- **Device Encryption:** Mandate full-device and SD card encryption
- **Remote Wipe:** IT can erase device data if lost/stolen
- **App Whitelisting:** Only approved apps allowed on work devices

Administrative Measures

- Conduct regular mobile security audits
- Enforce least privilege — apps/users get minimum required access
- Maintain inventory of all devices accessing corporate resources
- Immediate deprovisioning when employee leaves organization
- Regular security awareness training for employees
- Incident response plan specifically for mobile device breaches

11. Organizational Security Policies in Mobile Computing Era

Key Policies Organizations Must Have

- **BYOD Policy:** Rules for personal devices used for work — acceptable use, required security settings
- **Acceptable Use Policy (AUP):** What employees can/cannot do on company devices
- **Password Policy:** Minimum password strength, expiry, no reuse rules
- **Data Classification Policy:** Define what data can/cannot be stored on mobile devices
- **Remote Access Policy:** VPN requirements, approved methods for accessing corporate resources
- **Lost/Stolen Device Policy:** Immediate reporting procedure + remote wipe protocol
- **App Installation Policy:** Only approved/vetted apps on work devices
- **Encryption Policy:** Mandatory encryption of device storage and communications
- **Network Access Policy:** No connecting to public Wi-Fi without VPN
- **Social Media Policy:** Restrictions on sharing corporate info via personal social media

Policy Implementation Framework

Phase	Action
1. Assess	Inventory all devices, identify risks, classify data sensitivity

2. Design	Create policies based on risk assessment and compliance needs
3. Deploy	Implement MDM, configure devices, enforce encryption
4. Train	Educate employees on policies, threats, and safe practices
5. Monitor	Continuous monitoring, threat detection, audit logs
6. Review	Regularly update policies for new threats and technology changes

12. QUICK RECAP — KEY TERMS

Term	One-Line Definition
BYOD	Bring Your Own Device — personal device for work use
MDM	Mobile Device Management — centrally manage/secure devices
SIM Swapping	Transfer victim's phone number to attacker's SIM — bypass OTP
Bluejacking	Send unsolicited Bluetooth messages (no data stolen)
Bluesnarfing	Steal data via Bluetooth (contacts, emails)
Bluebugging	Full phone control via Bluetooth exploit
Juice Jacking	Malware via public USB charging ports
SS7 Attack	Exploit telecom protocol to intercept calls/SMS
Rogue Access Point	Fake Wi-Fi hotspot to intercept traffic
Smishing	Phishing via SMS messages
MitM	Attacker intercepts communication between two parties
Containerization	Isolate work apps from personal apps on same device
Remote Wipe	Erase device data remotely when lost/stolen
Skimming	Hardware device clones card data at ATM/POS
CNP Fraud	Card Not Present — online fraud using stolen card details
Jailbreaking/Rooting	Bypass OS restrictions — removes security protections
MAM	Mobile Application Management — manage specific apps, not full device
MTD	Mobile Threat Defense — real-time mobile threat detection
Spyware	Silently monitors device activity without user knowledge

END OF NOTES

ZenYukti

Quick Exam Notes

zenyukti.in

Other Unit Notes

All subject notes on GitHub — free to access & star

github.com/ZenYukti/MyNotes

Join ZenYukti Discord

Free workspace — internship & hackathon updates, tech discussions

go.zenyukti.in/discord

FIND US ON

Made with care by **ZenYukti** · Share freely, learn together

Quick Exam Notes | Exam Ready | Free Resource