RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING AND TECHNOLOGY

MOBILE SECURITY

LECTURE -1

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- What is mobile security?
- Popularity of Mobile Devices
- Insecurity of Mobile Devices
- Mobile Network Architecture
- Native Code
- OS Access
- Internet Access
- Risk Model
- MCQ
- References

INTRODUCTION TO MOBILE RISKS & SECURITY

What is mobile security?

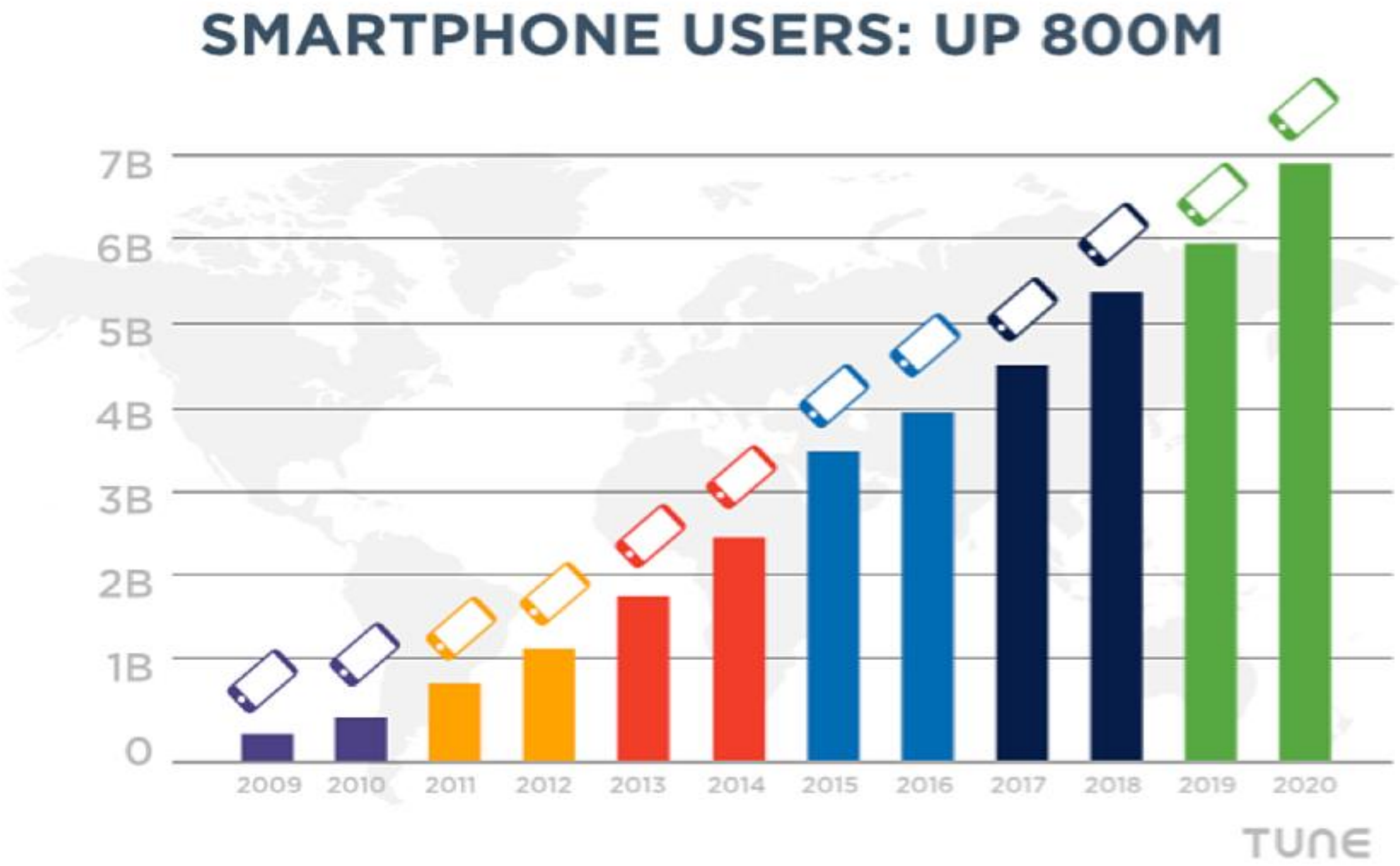
❑Mobile security is the protection of smart phones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

❑Mobile security is also known as wireless security.

❑Securing mobile devices has become increasingly important in recent years as the numbers of the devices in operation and the uses to which they are put have expanded dramatically.

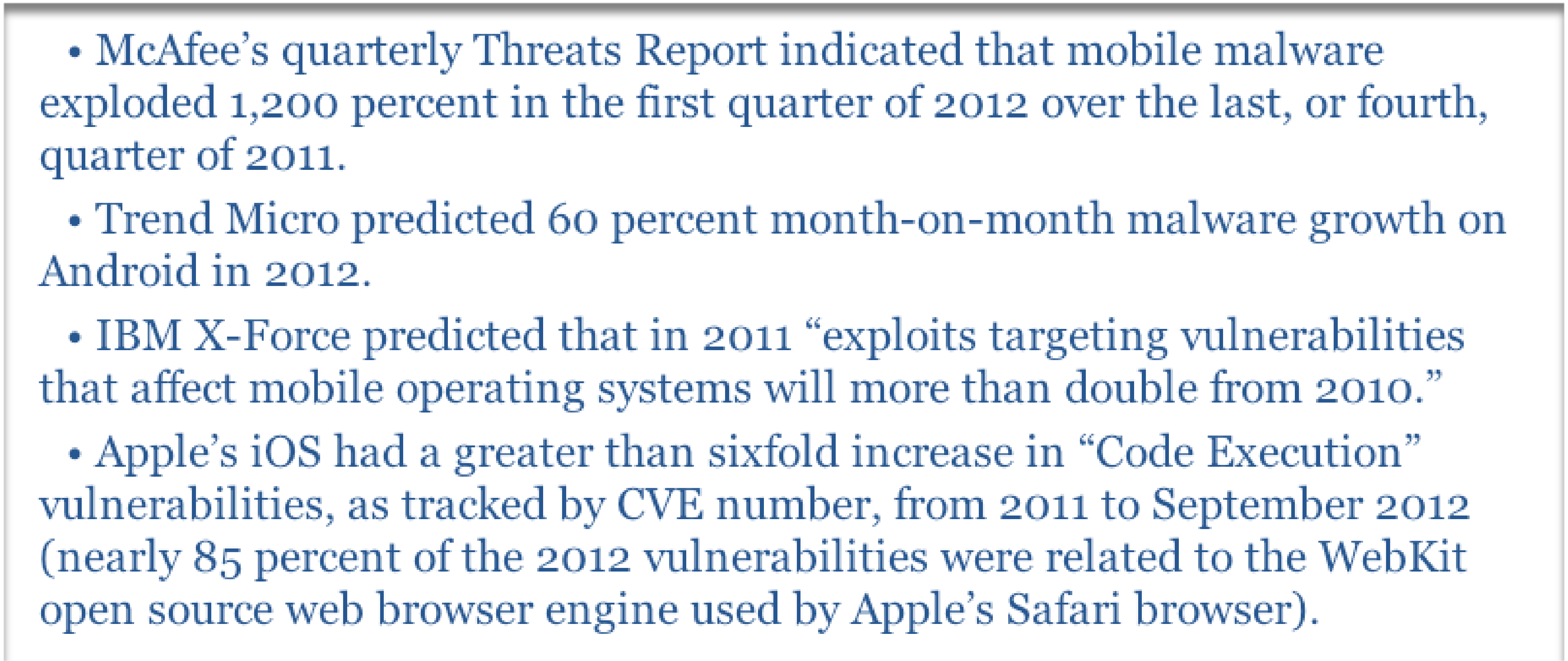
POPULARITY OF MOBILE DEVICE

Popularity of Mobile Devices



INSECURITY OF MOBILE DEVICES

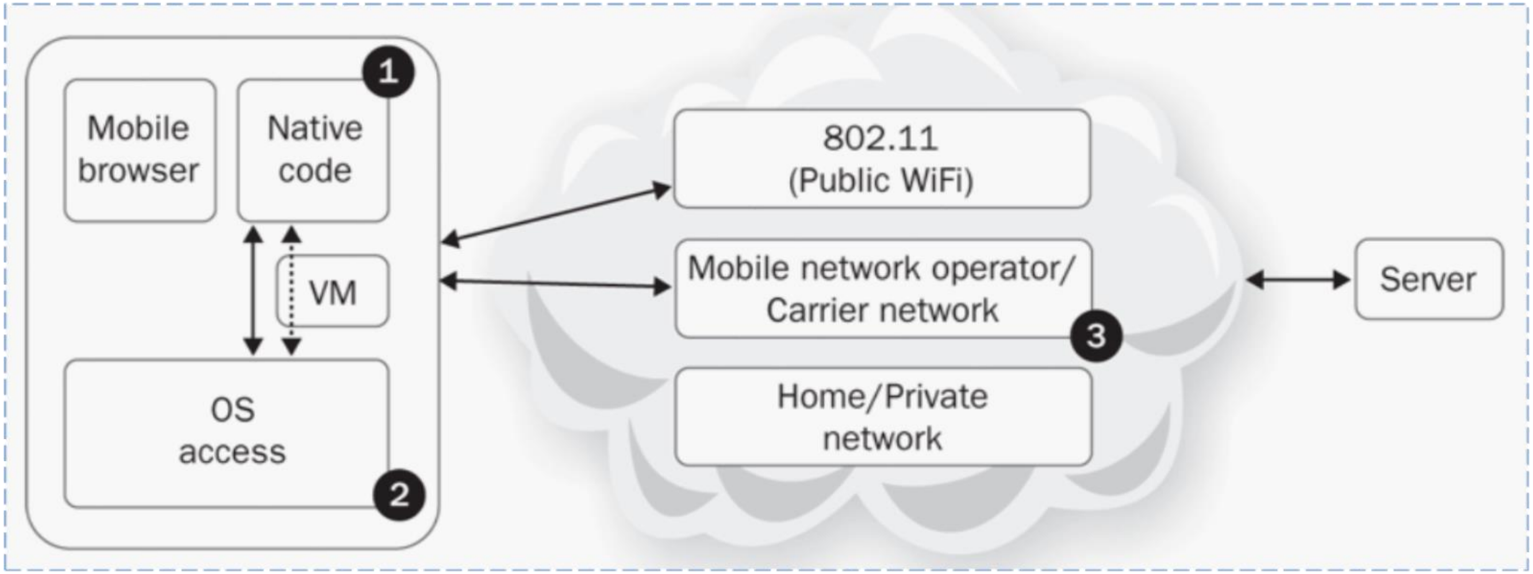
Insecurity of Mobile Devices



- McAfee’s quarterly Threats Report indicated that mobile malware exploded 1,200 percent in the first quarter of 2012 over the last, or fourth, quarter of 2011.
- Trend Micro predicted 60 percent month-on-month malware growth on Android in 2012.
- IBM X-Force predicted that in 2011 “exploits targeting vulnerabilities that affect mobile operating systems will more than double from 2010.”
- Apple’s iOS had a greater than sixfold increase in “Code Execution” vulnerabilities, as tracked by CVE number, from 2011 to September 2012 (nearly 85 percent of the 2012 vulnerabilities were related to the WebKit open source web browser engine used by Apple’s Safari browser).

THE MOBILE RISK MODEL

Mobile Network Architecture



THE MOBILE RISK MODEL

1. Native Code

❑Some languages like Java operate in a virtual machine

  ❑Run in a sandbox

  ❑Limited access to resources

❑Other languages like Objective-C run directly on the OS

  ❑More access to resources

  ❑Less safe

2. OS Access

Software running in a browser has limited access to the OS

❑Libraries

❑File system access

❑Interposes communications

❑System calls

THE MOBILE RISK MODEL

3. Internet Access

Mobile devices commonly use the mobile carrier's network and public Wi-Fi networks to connect to the Internet

Increased opportunity for Man-in-the-Middle (MiTM) attacks

Most mobile threats are variations on MiTM

MiTB (Man in the Browser)

MiTOS (Man in the OS)

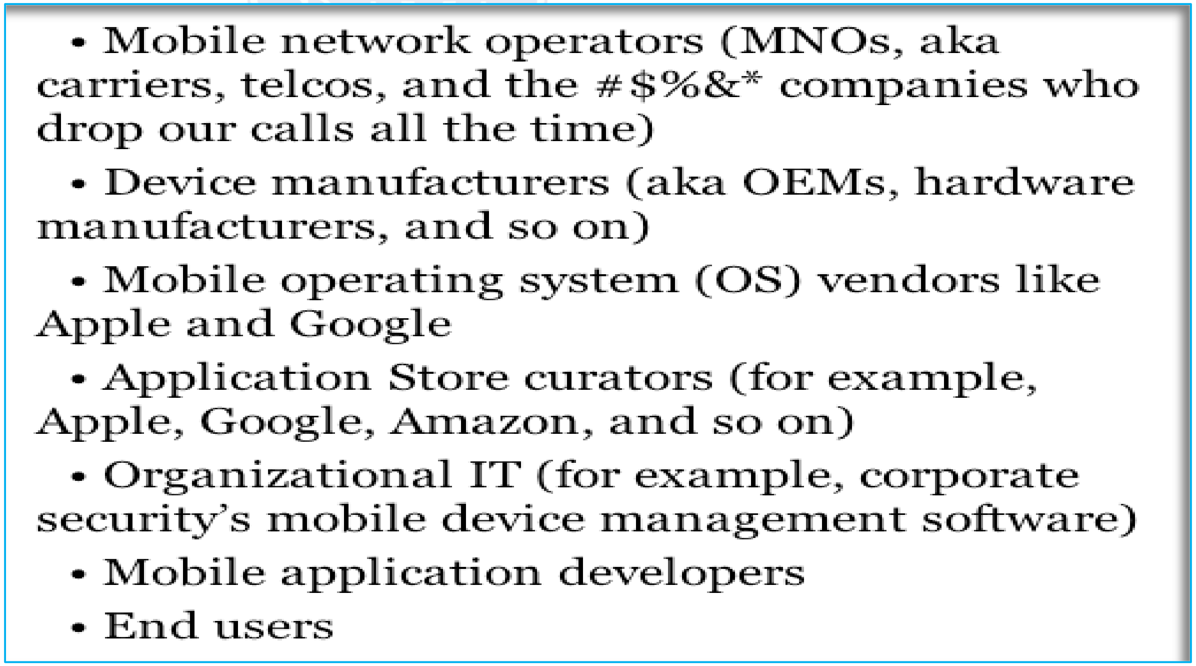
THE MOBILE RISK MODEL

Risk Model

There are three type of risk model

1. Identify stakeholders
2. Enumerate assets
3. Find relevant risks

Identification of Stakeholders



- Mobile network operators (MNOs, aka carriers, telcos, and the #$%&* companies who drop our calls all the time)
- Device manufacturers (aka OEMs, hardware manufacturers, and so on)
- Mobile operating system (OS) vendors like Apple and Google
- Application Store curators (for example, Apple, Google, Amazon, and so on)
- Organizational IT (for example, corporate security's mobile device management software)
- Mobile application developers
- End users

THE MOBILE RISK MODEL

Assets

- ❑ OS manufacturer values phone as a source of revenue
    - ❑ Threats include
        - ❑ Apps that may crash the OS
        - ❑ Users who may jailbreak the phone
- ❑ Users value their privacy
    - ❑ Threats include
        - ❑ The OS which may send data back to the carrier for "statistical purposes"
        - ❑ Apps preloaded by the MNO which might send data out

THE MOBILE RISK MODEL

Assets

- OS manufacturer values phone as a source of revenue
  - Threats include
    - Apps that may crash the OS
    - Users who may jailbreak the phone
- Users value their privacy
  - Threats include
    - The OS which may send data back to the carrier for "statistical purposes"
    - Apps preloaded by the MNO which might send data out

MCQ

1. 1. Which of the following is not an appropriate way of targeting a mobile phone for hacking?

a) Target mobile hardware vulnerabilities

b) Target apps’ vulnerabilities

c) Setup Keyloggers and spyware in smart-phones

d) Snatch the phone

2. Which of the following is not an OS for mobile?

a) Palm

b) Windows

c) Mango

d) Android

3. Mobile Phone OS contains open APIs that may be _____________ attack.

a) useful for

b) vulnerable to

c) easy to

d) meant for

4. ____________ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones.

a) Worms

b) Antivirus

c) Malware

d) Multimedia files

5. ____________ is the protection of smart-phones, phablets, tablets, and other portable tech-devices, & the networks to which they connect to, from threats & bugs.

a) OS Security

b) Database security

c) Cloud security

d) Mobile security

REFERENCES

- https://www.slideshare.net/SamBowne/cnit-128-ch-1-the-mobile-risk-ecosystem?from_action=save