Android Vulnerabilities

Lecture 11

Security of Mobile Devices

2019

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

Outline

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

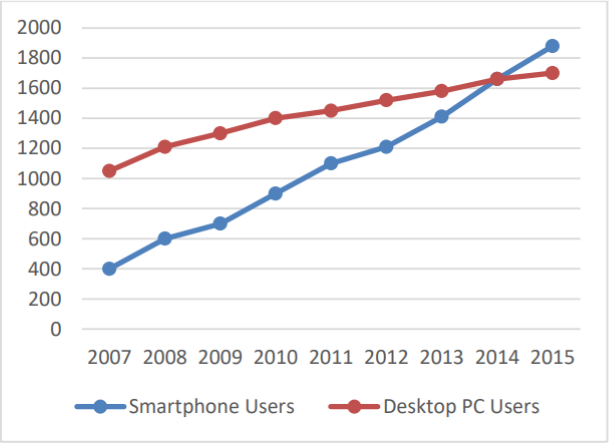
Side channel attacks

Gaining root access

Bibliography

- Vulnerabilities
- What can you gain?
- Causes

Mobile vs Desktop

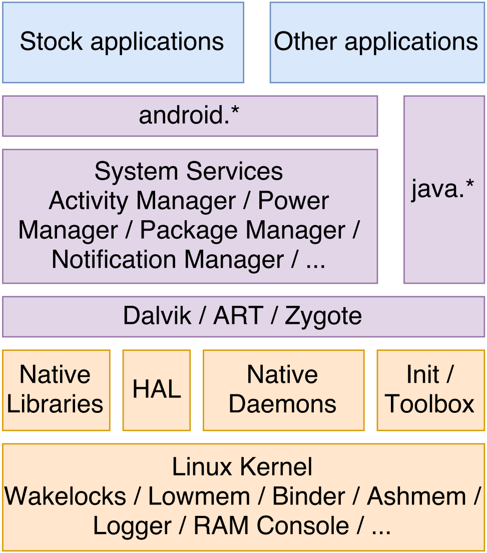


Number of internet users (millions)

Attack surface

- Attack vector
- Attack surface
- Castle analogy

Android system attack surface



Stock applications

Other applications

android.*

java.*

System Services
Activity Manager / Power Manager / Package Manager / Notification Manager / ...

Dalvik / ART / Zygote

Native Libraries

HAL

Native Daemons

Init / Toolbox

Linux Kernel
Wakelocks / Lowmem / Binder / Ashmem / Logger / RAM Console / ...

Android application attack surface

- Activities
- Services (exposed and bound services)
- Broadcast receivers
- Content providers

Attack surface classification

- Remote
- Local
- Physical

Outline

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

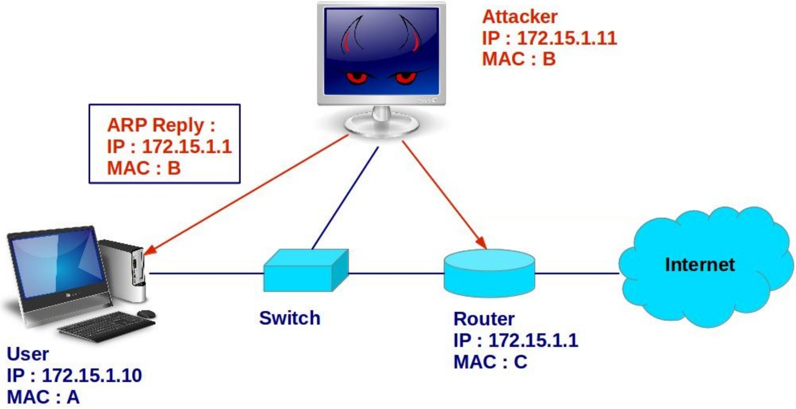
Gaining root access

Bibliography

Network attacks

- No network services available
- Susceptible to common network attacks
  - Spoofing attacks (ARP, DNS, DHCP)
  - Man in the middle attacks
  - TCP attacks (SYN flooding, RST attack, sequence prediction attack)
  - DoS attacks

ARP Spoofing



- Cellular communications - an addtional remote surface attack
- SMS, MMS
- WAP (Wireless Application Protocol)

- Dialer attack
  - tel://URI received through SMS, Twitter post
  - USSD code for factory reset
  - USSD code for reseting PUK - after 10 times, SIM card is destroyed

- Stagefright attack
  - Android native multimedia library
  - exploited through MMS, Hangouts, web browsers
  - integer overflow leads to heap overflow
  - shellcode with a reverse TCP connection callback

Client-side attack surface

- Client applications
- Browser attacks
  - Plethora of technologies: HTTP(S)/FTP, HTML, JavaScript
  - rogue URL
  - cross-site scripting (XSS)
  - cross-site request forgery (CSRF)

Client-side attack surface

- Web-Powered mobile applications - Twitter, Dropbox
- Authentication - SSL/TLS certificates
- Apps do not adequately validate the certificates
- 8% of the apps on Google Play Store exposed to MitM attacks

Google Infrastructure

- Google Single Sign On (SSO)
- Google Play Store
- Malicious applications
- Third-party applications

Google Infrastructure

- Google Single Sign On (SSO)
- Google Play Store
- Malicious applications
- Third-party applications
  - Top 100 Android Paid App list
  - hacked, modified, available on 3rd party distribution sites
  - over 500k downloads
  - Android.troj.mdk Trojan infected over 1 million Chinese Android devices - Temple Run, Fishing Joy

Google Infrastructure

- Verify Apps feature queries a Google database
- Bouncer
  - QEMU machine that runs the application in an isolated environment
  - dynamic runtime analysis tool
  - populates the environment dummy data (contacts, photos)

Bouncer

- Why do we still have malicious apps with the Bouncer check?

- Evading Bouncer
  - identifying the unique dummy data
  - identifying the unique fingerprint of the QEMU instance
  - use a command and control server that sends to the application malicious code

Wireless communication attacks

- GPS
  - no known attacks to compromise a device
  - GPS spoofing
- Baseband (GSM, HSPA, LTE)
  - emulate a base station (cell tower) - specialized equipment
  - RIL (Radio Interface Layer) - AT commands through USB

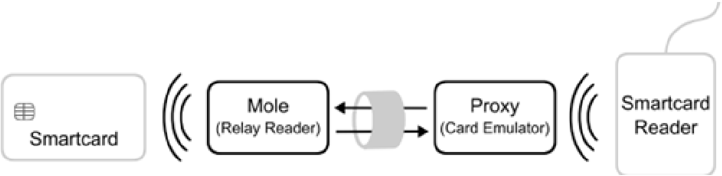
Wireless communication attacks

- Bluetooth
  - weaknesses related to pairing and encryption in the Android Bluetooth stack (BlueDroid)
  - Bluejacking, BlueBorne (heap overflow)
- WiFi
  - WEP, WPA, WPA2, WPA3
  - rogue AP (access point)
  - Krack - Key Reinstallation Attack

Wireless communication attacks

- NFC
  - lack of encryption and authentication
  - browser attack
  - NFC relay attack

Wireless communication attacks



Outline

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

Local attack surfaces

- file system - files, pipes, character and block devices
  - F2FS (Flash Friendly File System) vulnerabilities
  - boundary checks, integer overflows
- sockets
  - PF_INET
  - PF_UNIX
  - PF_NETLINK - Gingerbreak jailbreak
- binder
  - Use-After-Free issue caused by race conditions
- shared memory - KillingInTheNameOf jailbreak

Outline

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

Physical attack surfaces

- dismantling the device
- USB
  - send AT commands to the RIL - issue calls, alter the pin
  - vold vulnerability - allows to overwrite filesystems through USB

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

Application security

- application permission issues
  - Android documentation related to permissions does not correspond with what the Android middleware actually requires
  - undergranting or overgranting permissions
- insecure transmission of sensitive data
- insecure data storage
  - plaintext storage
  - no encryption
  - Skype - world-readable, world-writable permissions, no encryption

Application security

- information leakage through logs
  - excessive, very verbose logging
  - Firefox - browsing activity, session identifiers
- insecure transmission of sensitive data
- Unsecured IPC endpoints
  - who can access whom?
  - activities - UI redressing attacks (clickjacking) - Cloak and Dagger
  - bounded services - expose functionality
  - content providers - expose data, susceptible to SQLite injection
  - broadcast receivers - implicit intents

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

Side channel attacks

- What are they?
- Classification
  - Active vs Passive
  - Physical properties vs Logical properties
  - Local attackers vs Vicinity attackers vs Remote attackers

Local pasive side channel attacks

- power analysis attack - attacks on DES
- electromagnetic analysis attack - attacks on AES, RSA, ECC, ECDSA
- smudge attack
- shoulder surfing and reflections
- hand and device movements

Local active side channel attacks

- clock and power glitching
  - underclocking, overclocking
- electromagnetic fault injection
  - EM pulses affect state of memory cells
- laser and optical faults
  - laser beams can flip bits in memory cells
- temperature variation
  - heat up can lead to faults in memory cells
  - cooling down can lead to remanence effect of RAM

Vicinity pasive side channel attacks

- network traffic analysis
- USB power analysis
    - USB charging stations can detect power traces
- WiFi signal monitoring
    - keystrokes can affect the WiFi signal

Remote pasive side channel attacks

- Linux inherited procfs leaks
  - /proc/[pid]/status
  - infer browsing behavior using the memory footprint
  - shared memory size increase to detect activity transitions
  - number of context switches and interrupts to detect keystrokes pattern
- data-usage statistics
  - infer browsing behavior
- page deduplication
  - identical physical pages merged into one across differente processes
  - copy-on-write
  - infer browsing behavior

Remote pasive side channel attacks

- microarchitectural attacks
  - timing behavior of cryptographic system components
  - branch prediction units, CPU caches
  - cache-timing attacks against AES
- location inference
  - accelerometer, gyroscope
  - speaker status information offered by Android API
  - infer speech length (Turn right onto East Main Street)
- speech recognition
  - acoustic signals can influence gyroscope measurements

Remote active side channel attacks

- Rowhammer
  - high cell density in DRAM
  - cells leak their electrical charge to other cells
  - bypass isolation between DRAM memory cells
  - RAMpage attack - gain root privileges

Outline

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

- Goto Don't root robots presentation
- The don't root robots presentation is not required for the exam

General concepts

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Application security

Side channel attacks

Gaining root access

Bibliography

- Android Hacker's Handbook, Joshua J. Drake, 2014

Keywords

- Attack vector
- Attack surface
- Application security
- Side channel attacks
- Root access
- Cellular communications
- WiFi
- Bluetooth
- NFC

- Activities
- Services
- Content providers
- Broadcast receivers
- Bouncer