Mobile Devices Vulnerabilities

Lecture 7

Security of Mobile Devices

2020

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

Outline

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

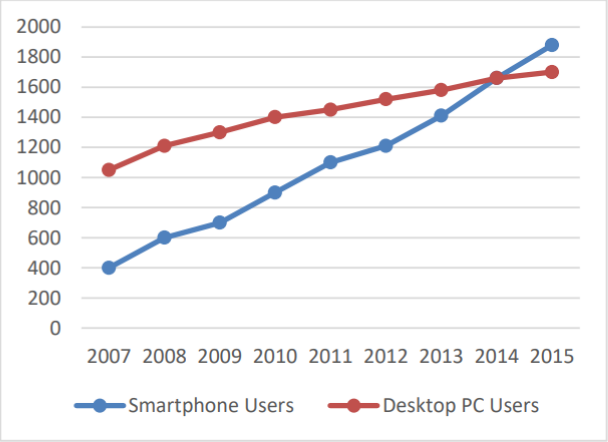
Side channel attacks

Gaining root access

Bibliography

- Vulnerabilities
- What can you gain?
- Causes

Mobile vs Desktop



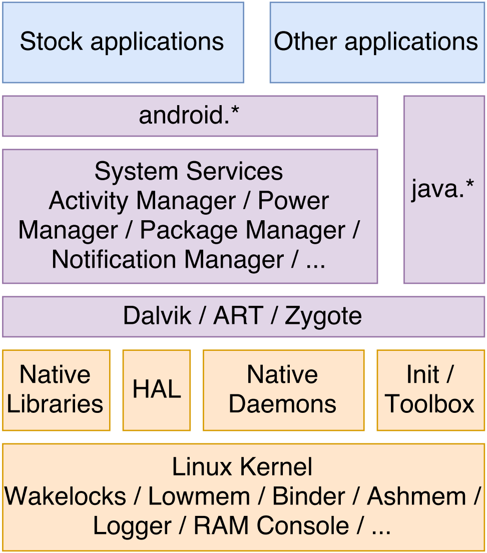
Number of internet users (millions)

Attack surface

- Attack vector
- Attack surface
- Castle analogy

Attack surface

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 / ...

Attack surface classification

- Remote
- Local
- Physical

Outline

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

Android application attack surface

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

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

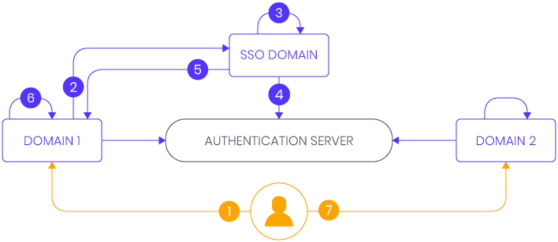
- information leakage through logs
  - excessive, very verbose logging
  - Firefox - browsing activity, session identifiers
- insecure transmission of sensitive data
- Unsecured IPC endpoints
  - who can access whom?
  - activities - UI redressing attacks (clickjacking) - Cloak and Dagger
  - bounded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

Malware

- virus
- spyware
- botnet
- trojan
- rootkit

- Google Single Sign On (SSO)

THE SSO AUTHENTICATION PROCESS



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

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

- Why do we still have malicious apps with the Google Play Protect check?

Google Play Protect

- Evading Google Play Protect
  - 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

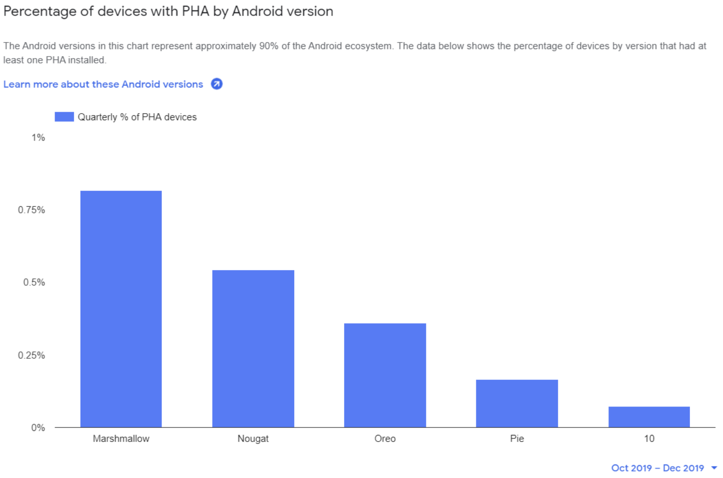
Malware detection

- signature based techniques
- machine learning based techniques

Malware countermeasures

- user education
- install apps from trusted sources
- wireless network security (no free WiFi)
- prevent rooting/jailbreaking
- keep OS up to date

Malware countermeasures



Percentage of devices with PHA by Android version

The Android versions in this chart represent approximately 90% of the Android ecosystem. The data below shows the percentage of devices by version that had at least one PHA installed.

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

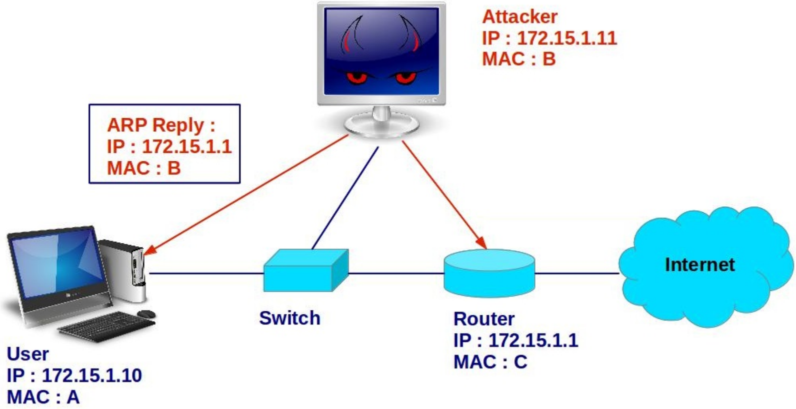
Gaining root access

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



Mobile network attacks

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

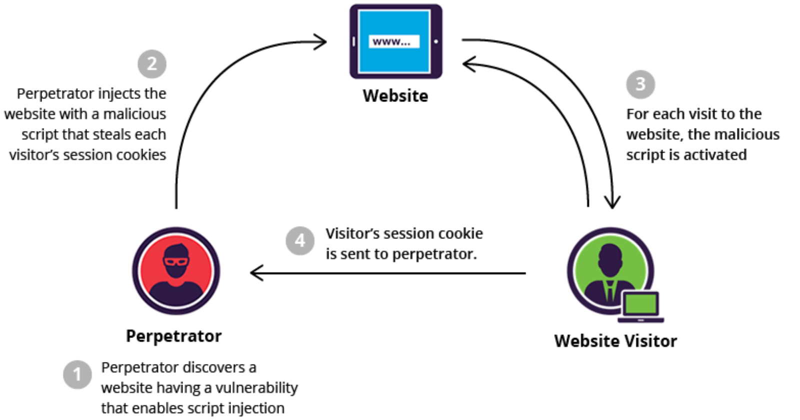
- Dialer attack
  - tel://URI received through SMS, Twitter post
  - USSD code for factory reset
  - USSD code for reseting PUK - after 10 times, SIM card is destroyed

- 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

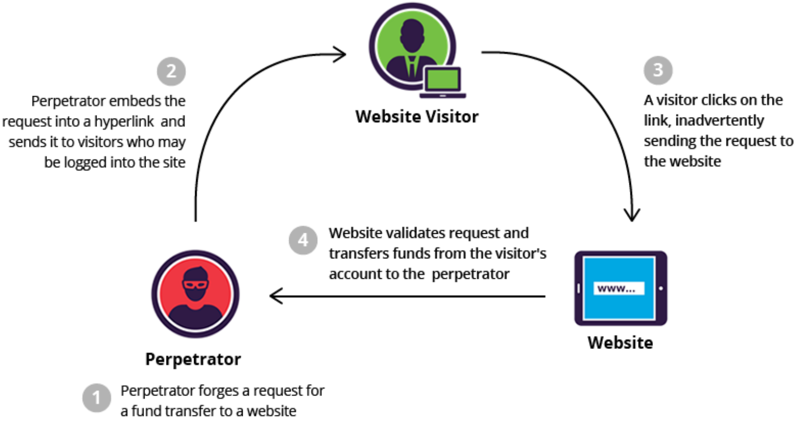
- Client applications
- Browser attacks
  - Plethora of technologies: HTTP(S)/FTP, HTML, JavaScript
  - rogue URL
  - cross-site scripting (XSS)
  - cross-site request forgery (CSRF)

Cross-site scripting



www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Cross-site request forgery



1 Perpetrator forges a request for a fund transfer to a website

2 Perpetrator embeds the request into a hyperlink and sends it to visitors who may be logged into the site

3 A visitor clicks on the link, inadvertently sending the request to the website

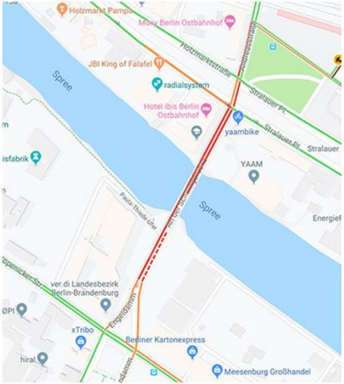
4 Website validates request and transfers funds from the visitor's account to the perpetrator

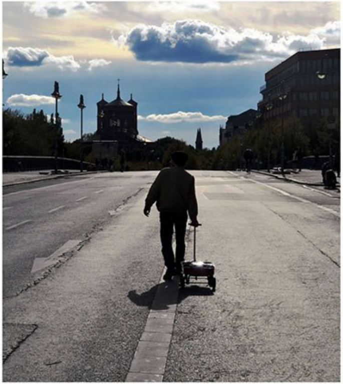
Client-side attack surface

- 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

Wireless communication attacks

- GPS
  - no known attacks to compromise a device
  - GPS spoofing





Wireless communication attacks

- Baseband (GSM, HSPA, LTE)
  - emulate a base station (cell tower) - specialized equipment
  - RIL (Radio Interface Layer) - AT commands through USB or Bluetooth (attention commands that can read/write messages, downgrade OS, charge the user)

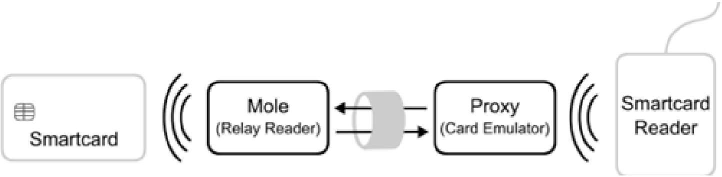
Wireless communication attacks

- Bluetooth
  - weaknesses related to pairing and encryption in the Android Bluetooth stack (BlueDroid)
  - Bluejacking - send unsolicited messages to the target
  - Bluesnarfing - access unrestricted data from the target
  - BlueBorne - unrestricted access to a remote device. Heap overflow generated by sending multiple Bluetooth discovery packets.
  - BlueFrag - allows remote code execution through a specially crafted Bluetooth packet. Bluetooth address can be deduced from MAC address.

- WiFi
  - WEP, WPA, WPA2, WPA3
  - rogue AP (access point)
  - Krack - Key Reinstallation Attack

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

Wireless communication attacks



Outline

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

Local attack surfaces

- file system - files, pipes, character and block devices
  - F2FS (Flash Friendly File System) vulnerabilities
  - memory corruption → boundary checks → integer overflows
- TCP/IP stack
  - CVE-2014-0100
  - IPv4 fragmentation
  - race condition - fragment deleted before being added to a LRU list
  - use-after-free issue
  - internal denial of service

Local attack surfaces

- binder
  - use-after-free issue caused by race conditions between binder ioctl calls
- shared memory
  - KillingInTheNameOf jailbreak
  - remaps the system properties address space to be writable
  - ro.secure = 0
  - root access through ADB

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

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

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

- 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 - unlock lock screen
- shoulder surfing and reflections - reflections on sunglasses can be used to capture what the user is writing/pressing
- hand and device movements - infer PIN input

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 (cold-boot attack)

Vicinity pasive side channel attacks

- network traffic analysis
- USB power analysis
  - USB charging stations can detect power traces
  - infer visited sites
- WiFi signal monitoring
  - keystrokes can affect the WiFi signal - Channel State Information (CSI)
  - infer unlock patterns

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 different processes
  - copy-on-write fault when another process wants to write in that area
  - infer browsing behavior

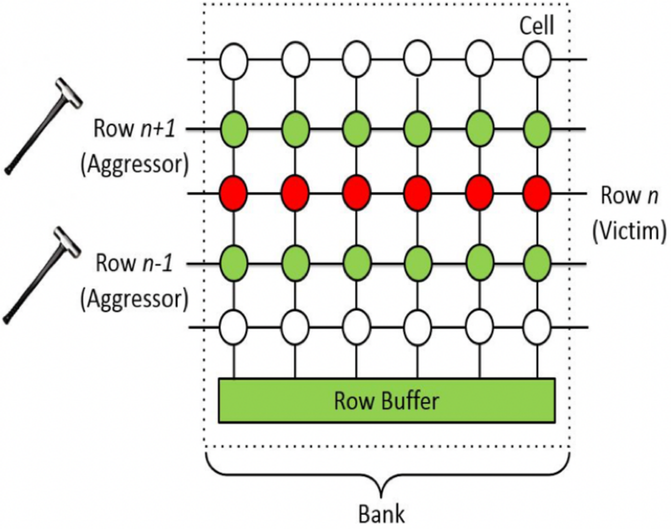
Remote pasive side channel attacks

- 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
  - DDR3 or DDR4 SDRAM cells
  - high cell density in DRAM
  - cells leak their electrical charge to other cells
  - bypass isolation between DRAM memory cells
  - RAMpage attack - gain root privileges

Rowhammer


Cell
Row n+1
(Aggressor)
Row n
(Victim)
Row n-1
(Aggressor)
Row Buffer
Bank

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

RageAgainstTheCage jailbreak

```
/* Code intended to run with elevated privileges */
do_stuff_as_privileged();

/* Drop privileges to unprivileged user */
setuid(uid);

/* Code intended to run with lower privileges */
do_stuff_as_unprivileged();
```

RageAgainstTheCage jailbreak

```
/* Code intended to run with elevated privileges */
do_stuff_as_privileged();

/* Drop privileges to unprivileged user */
setuid(uid);

/* Code intended to run with lower privileges */
do_stuff_as_unprivileged();
```

```
ERRORS
     EAGAIN The uid does not match the current
            uid and uid brings process over its
            RLIMIT_NPROC resource limit.
```

RageAgainstTheCage jailbreak

```
/* Code intended to run with elevated privileges */
do_stuff_as_privileged();

/* Drop privileges to unprivileged user */
setuid(uid);

/* Code intended to run with lower privileges */
do_stuff_as_unprivileged();
```

```
ERRORS
    EAGAIN The uid does not match the current
           uid and uid brings process over its
           RLIMIT_NPROC resource limit.
```

```
RLIMIT_NPROC
    The maximum number of processes (or, more
    precisely on Linux, threads) that can be
    created for the real user ID of the calling
    process. Upon encountering this limit, fork(2)
    fails with the error EAGAIN.
```

RageAgainstTheCage jailbreak

- too many processes → setuid will fail → privileges will not be dropped
- Who can we target for this? Answer: ADB

```
/* then switch user and group to "shell" */
setgid(AID_SHELL);
setuid(AID_SHELL);
```

RageAgainstTheCage jailbreak

- fork() up to RLIMIT_NPROC for shell user
- kill adb process, fork() again
- setuid() fails for adb
- adb shell is now a root shell

- Goto Don’t root robots presentation

Outline

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Side channel attacks

Gaining root access

Bibliography

- Android Hacker's Handbook, Joshua J. Drake, 2014
- Systematic Classification of Side-channel Attacks: A Case Study for Mobile Devices, Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak and Stefan Mangard
- A Survery on Smartphones Security: Software Vulnerabilities, Malware and Attacks

Keywords

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

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