Mobile Devices Vulnerabilities and Attacks (2)

Lecture 7

Security of Mobile Devices

2023

Outline

Side Channel Attacks

- What are they?
  - unconventional methods
  - attack the implementation and indirect / physical effects of that implementation
- Classification
  - active vs passive
  - physical properties vs logical properties
  - local vs vicinity vs remote attackers

Local Passive Side Channel Attacks

- Power analysis attack
  - analyse power consumption
  - deduce cryptographic operations
  - deduce secret key of DES
- Electromagnetic analysis attack
  - analyse electromagnetic energy
  - deduce keys of AES, RSA, ECC, ECDSA

Local Passive Side Channel Attacks

- Smudge attack
  - dust & dirt
  - specific marks for unlock pattern
- Shoulder surfing and reflections
  - reflections in sunglasses/windows
- Hand and device movements
  - movement of the user's hands
  - infer PIN/password

Local Active Side Channel Attacks

- Clock and power glitching
  - device connected to a power source
  - changes processing frequency & power consumption
  - underclocking
    - low processing frequency, low power consumption
  - overclocking
    - high processing frequency, high power consumption

Local Active Side Channel Attacks

- Electromagnetic fault injection
  - EM pulses affect state of memory cells
  - change values in memory
- Laser and optical faults
  - laser beams can flip bits in memory cells

Local Active Side Channel Attacks

- Temperature variation
  - Very high temperature
    - can lead to faults in memory cells or bit errors
  - Very low temperature
    - can lead to remanence effect of RAM
    - after reset RAM is not empty, values reman a period of time
    - cold-boot attack

Vicinity Passive Side Channel Attacks

- Network traffic analysis
  - Wireshark or tcpdump to inspect packets
- USB power analysis
  - USB charging stations can detect power traces
  - infer visited sites

Vicinity Passive Side Channel Attacks

- WiFi signal monitoring
  - Channel State Information (CSI)
    - how signal propagates
    - signal influenced by shadowing, fading, scattering, attenuation
  - keystrokes can affect the CSI
  - infer unlock PIN/pattern

Remote Passive Side Channel Attacks

- Linux inherited procfs leaks
  - /proc/[pid]/status
  - infer browsing behavior using the memory footprint
  - shared memory size to detect activity transitions
  - context switches and interrupts to detect keystroke pattern
- Data-usage statistics
  - infer browsing behavior

Remote Passive Side Channel Attacks

- Page deduplication
  - identical physical pages from different processes merged into one
  - copy-on-write fault when a process wants to write in that area
  - infer browsing behavior (images)
- Speech recognition
  - acoustic signals can influence gyroscope measurements
  - deduce what the user is saying

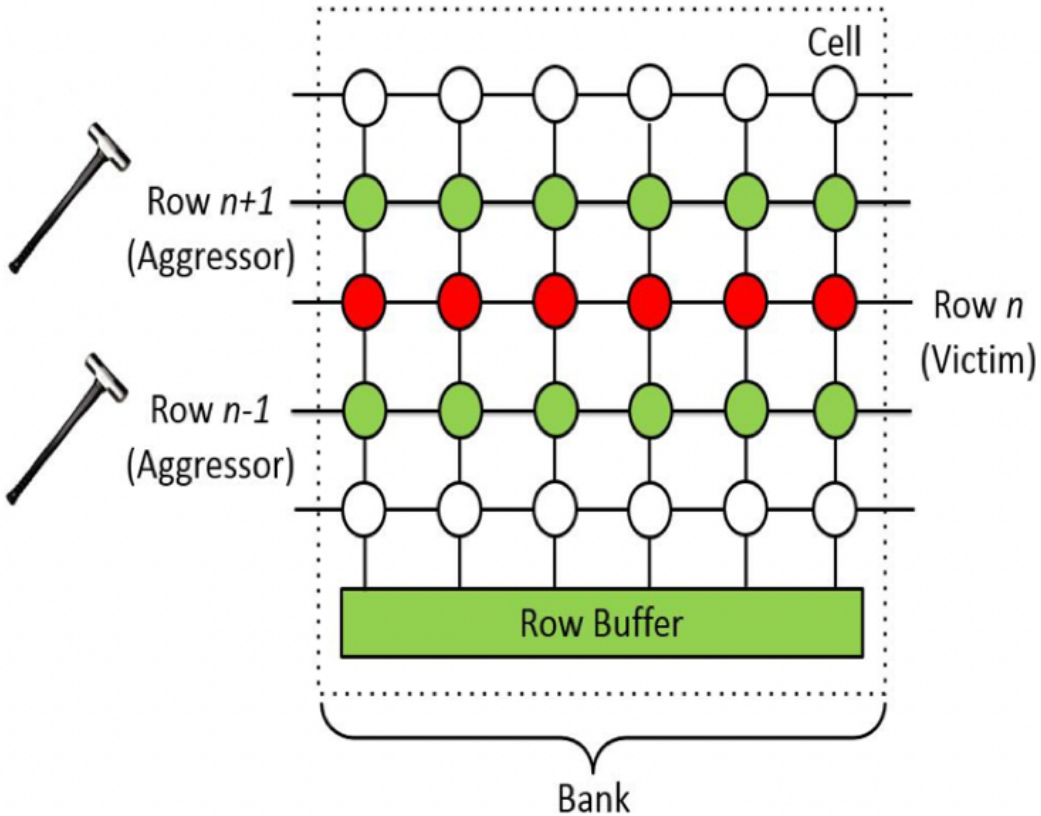
Remote Passive Side Channel Attacks

- Microarchitectural attacks
  - execution & access times to cache, RAM, disk
  - branch prediction units
  - cache-timing attacks against AES
- Location inference
  - accelerometer, gyroscope
  - speaker status information offered by Android API
  - speech length for each direction of travel
  - infer driver's route

Remote Active Side Channel Attacks

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

Rowhammer Bit Flip Attack



Source: `https://medium.com/baiduxlab/pc-security-facing-another-heavy-hammer-baidu-security-discovers-a-new-rowhammer-attack-be3dce8d1e92`

Outline

Malware

- Adware
- Backdoor
- File infector
- Potentially unwanted application (PUA)
- Ransomware
- Riskware
- Scareware
- Spyware
- Trojan, trojan-sms, trojan-spy, trojan-banker, trojan-dropper

Adware

- Display unwanted advertisements
- Lure the user to click on them
- May collect private information from the device
- May use the camera to take photos
- May install other malware
- May encrypt the data on the device
- Families: gexin, batmobi, ewind, shedun, pandaad, appad, etc.

Backdoor

- Gateway to the device
- Bypass authentication and security mechanisms
- Embedded into legitimate apps
- Collect private info, send / receive messages, make phone calls
- Extract the call history and the list of installed apps
- Installed when the user clicks on an adware
- Families: mobby, kapuser, hiddad, dendroid, levida, fobus, etc.

File Infector

- Attaches to APK packages
- Affect QoE, slow down device, consume battery
- Steal private information
- Access and modify files & device settings
- Use, block, delete other apps
- Root the device
- Families: leech, tachi, commplat, gudex, aqplay, etc.

Potentially Unwanted Applications (PUAs)

- Bundle with legitimate applications
- May behave as adware, spyware or hijackers
- May steal sensitive information
- May slow down the device
- May access the location through GPS
- Usually don't have destructive effect
- Families: apptrack, secapk, wiyun, youmi, scamapp, utchi, etc.

Ransomware

- Encrypts user files and directories
- Requests a ransom in exchange for the encryption key
- Paying does not guarantee the getting back the data
- Pose as legitimate apps
- Send/receive SMS, lock SIM card, lock device
- Steal credentials, communicate with remote server
- Families: congur, masnu, fusob, jisut, koler, lockscreen, etc.

Riskware

- Legitimate application
- Poses potential risks to device vulnerabilities
- May steal private information, may redirect to malicious websites
- May connect to malicious servers, receive/send SMS
- May steal network information and credetials
- May show advertisements, modify system files and settings
- Families: badpac, mobilepay, wificrack, triada, skymobi, etc.

Scareware

- Induce fear to convince the user to install malicious apps
- Fake alerts about malicious software detected on the device
- Convinces the user to install a fake security app that pretends to protect the device
- Collect device info, GPS location, install malicious apps
- Families: avpass, mobwin, fakeapp, etc.

Spyware

- Collect private information
- Sold to advertisers or external agencies
- Obtains access to location, phone information, camera
- Send/receive SMS, steal WiFi information
- Access and modify system settings & files
- Families: spynote, qqspy, spydealer, smsthief, spyagent, etc.

Trojans

- Behavior of legitimate applications
- Hide in the background
- Steal private information
- Delete/block/modify/copy data to disrupt functionality
- Sub-categories: trojan-banker, trojan-dropper, trojan-sms, trojan-spy
- Families: gluper, lotoor, rootnik, guerrilla, gugi, hqwar, etc.

Malware Detection

- Signature based techniques
  - Signature database
  - Static technique
  - Easily fooled by changing the executable
- Machine learning based techniques
  - Neural networks, deep learning
  - 2 steps: training, testing
  - Data required for the training stage

ML-based Malware Detection

- Static Analysis
  - Analyses app package contents
  - App is not executed
- Dynamic Analysis
  - Performed at runtime
  - User event and input emulator - feed input to app
  - Virtual machine detection -> avoid malicious operations
- Hybrid Analysis

Feature Extraction Methods

Analysis Type	Feature Extraction Method	Features Extracted
Static	Manifest analysis	Package name, Permissions, Intents, Activities, Services, Providers
	Code analysis	API calls, Information flow, Taint tracking, Opcodes, Native code, Cleartext analysis
Dynamic	Network traffic analysis	URLs, IPs, Network Protocols, Certificates, Non-encrypted data
	Code instrumentation	Java classes, intents, network traffic
	System calls analysis	System calls
	System resources analysis	CPU, Memory, and Battery usage, Process reports, Network usage
	User interaction analysis	Buttons, Icons, Actions/Events

Source: A Comprehensive Survey on Machine Learning Techniques for Android Malware Detection

Outline

Google Play Protect - On-device Protection

- Verify Apps service
  - Scans Android devices daily
  - Remove PHAs & block future installs
  - Contact server only when PHA is suspected
  - On demand & offline scanning
  - Remove or disable PHAs

Google Play Protect - Cloud-based Protection

- Powerful machine-learning algorithms
- Learn behavior of malicious & legitimate apps
- Suspicious behavior:
  - interact with other apps in unexpected ways
  - access or share personal data
  - install other apps
  - access suspicious websites
  - bypass security mechanisms

Google Play Protect - Cloud-based Protection

- Static analysis
- Dynamic analysis
- Heuristic and similarity analysis
- SafetyNet
- Signatures
- Security reports
- Developer relationships

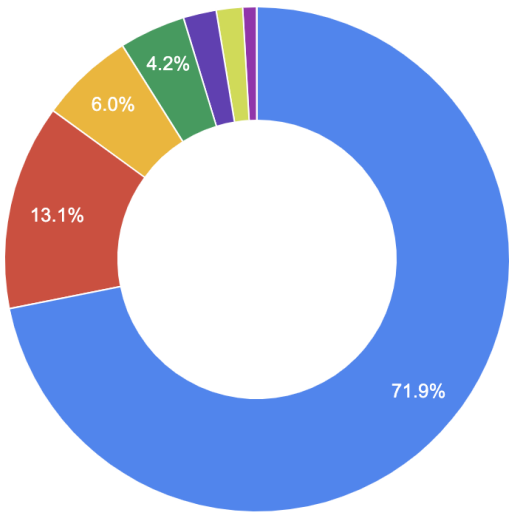
Google Play Protect - Cloud-based Protection

- Classifies apps on a scale from safe to harmful
- Safe apps are accepted on Google Play
- Harmful apps are blocked
- Potentially harmful apps
- Developers of harmful apps are banned

PHAs Detected by Google Play Protect

Oct 2022 – Dec 2022

Google Play



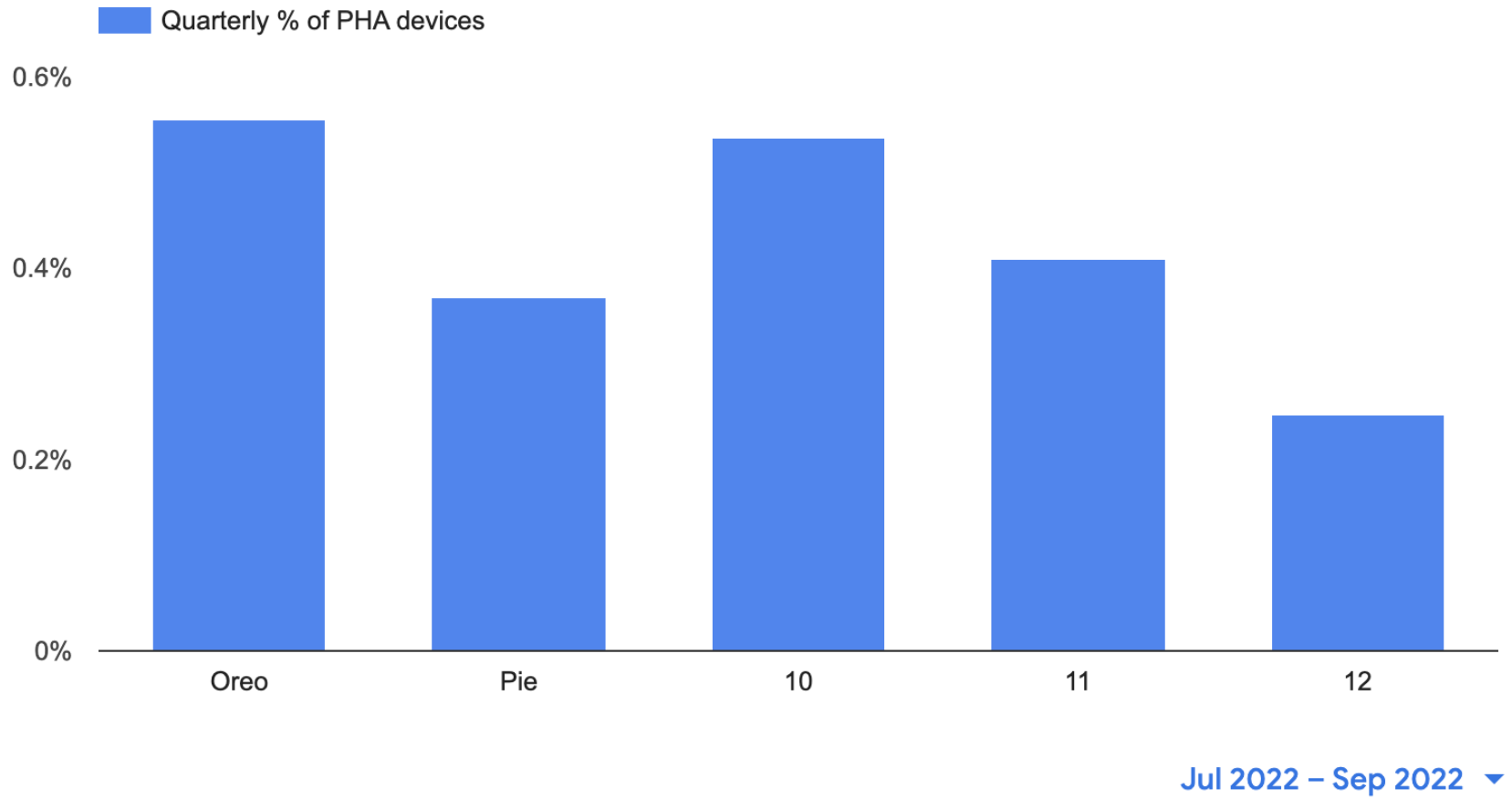
Category	PHA Install Rate
Privilege escalation	0.13383834%
Spyware	0.024477617%
Trojan	0.011214234%
Toll fraud	0.0078993064%
Hostile downloader	0.0039487582%
Phishing	0.0031301624%
Backdoor	0.001621958%
Commercial spyware	0.0000640906%
Rooting	0.0000035802%
DOS	0.0000028758%
Ransomware	0.0000018402%
SMS fraud	0.0000014107%
Spam	0.0000006751%
Windows malware	0.0000000631%
Call fraud	0.0000000228%

Source: `https://transparencyreport.google.com/android-security/store-app-safety?hl=en`

Preventive Measures

- User education
- Install apps from trusted sources
- Avoid clicking on advertisements
- Pay attention to permissions
- Wireless network security (no free WiFi)
- Prevent rooting/jailbreaking
- Keep OS up to date

Percentage of Devices with PHA by Android Version



Source: `https://transparencyreport.google.com/android-security/device-platform-safety?hl=en`

Outline

Bibliography

- Systematic Classification of Side-channel Attacks: A Case Study for Mobile Devices, Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak and Stefan Mangard
- https://www.itworldcanada.com/blog/understanding-android-malware-families-uamf-the-founda 441562
- A Comprehensive Survey on Machine Learning Techniques for Android Malware Detection https://www.mdpi.com/2078-2489/12/5/185
- https://transparencyreport.google.com/android-security/device-platform-safety?hl=en
- https://transparencyreport.google.com/android-security/store-app-safety?hl=en

Keywords

- Side channel attacks
- Malware
- adware
- backdoor
- file infector
- PUA
- ransomware
- riskware
- scareware
- spyware
- trojan
- static analysis
- dynamic analysis
- Verify Apps
- Google Play Protect
- PHA