a few

Reviewing Attacks on Android

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, a full list of references is provided on the last slide.

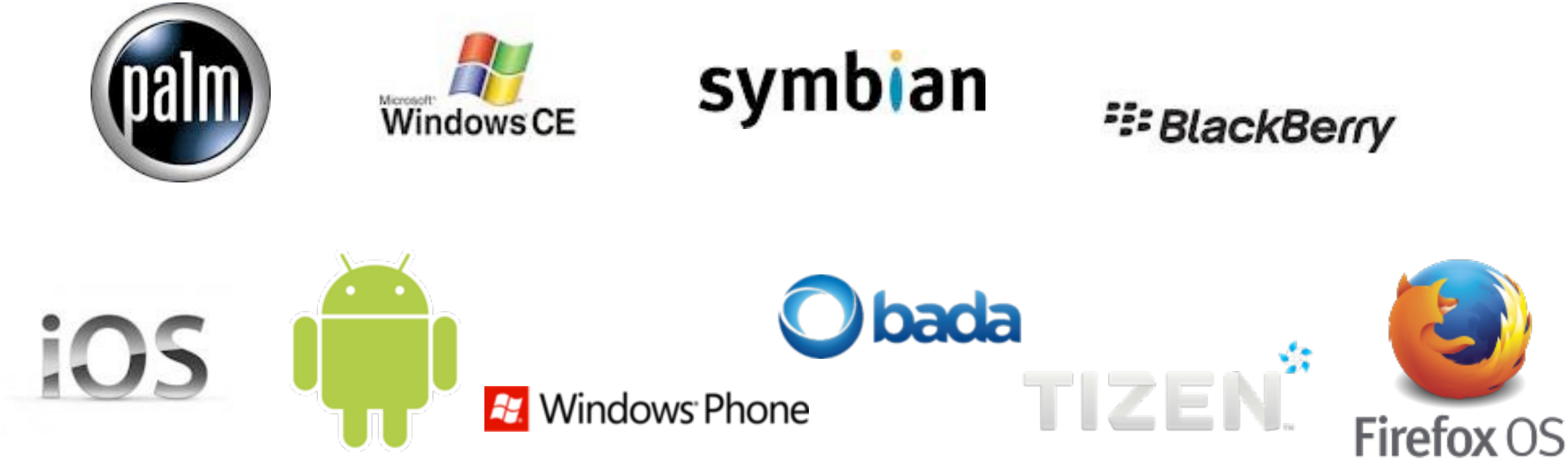
History

- First commercial hand held cell phone 1983 (1362)
  - used embedded systems

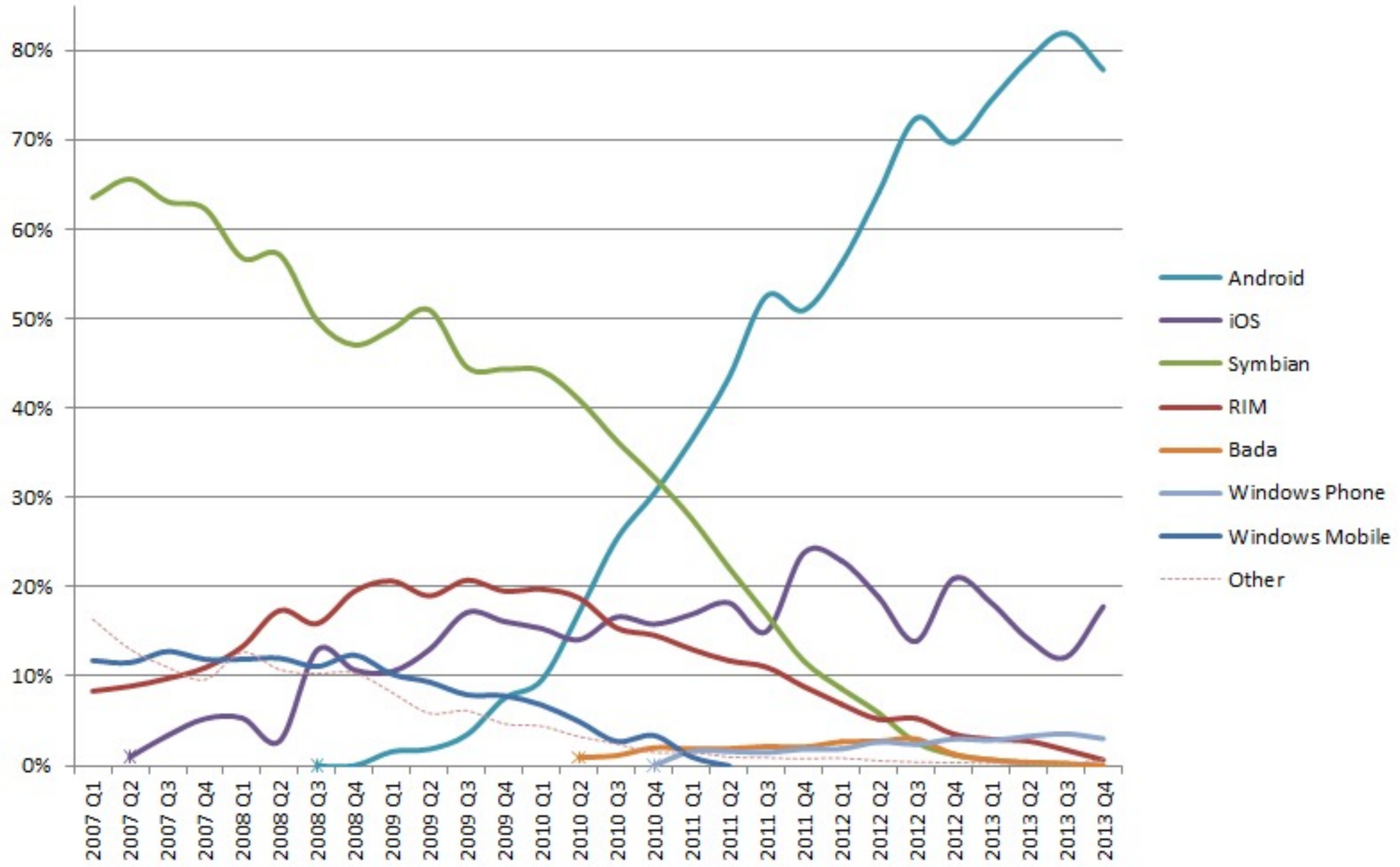
The first smartphone

- IBM Simon 1993 (1372)
  - touchscreen, email
  - Based on ROM-DOS

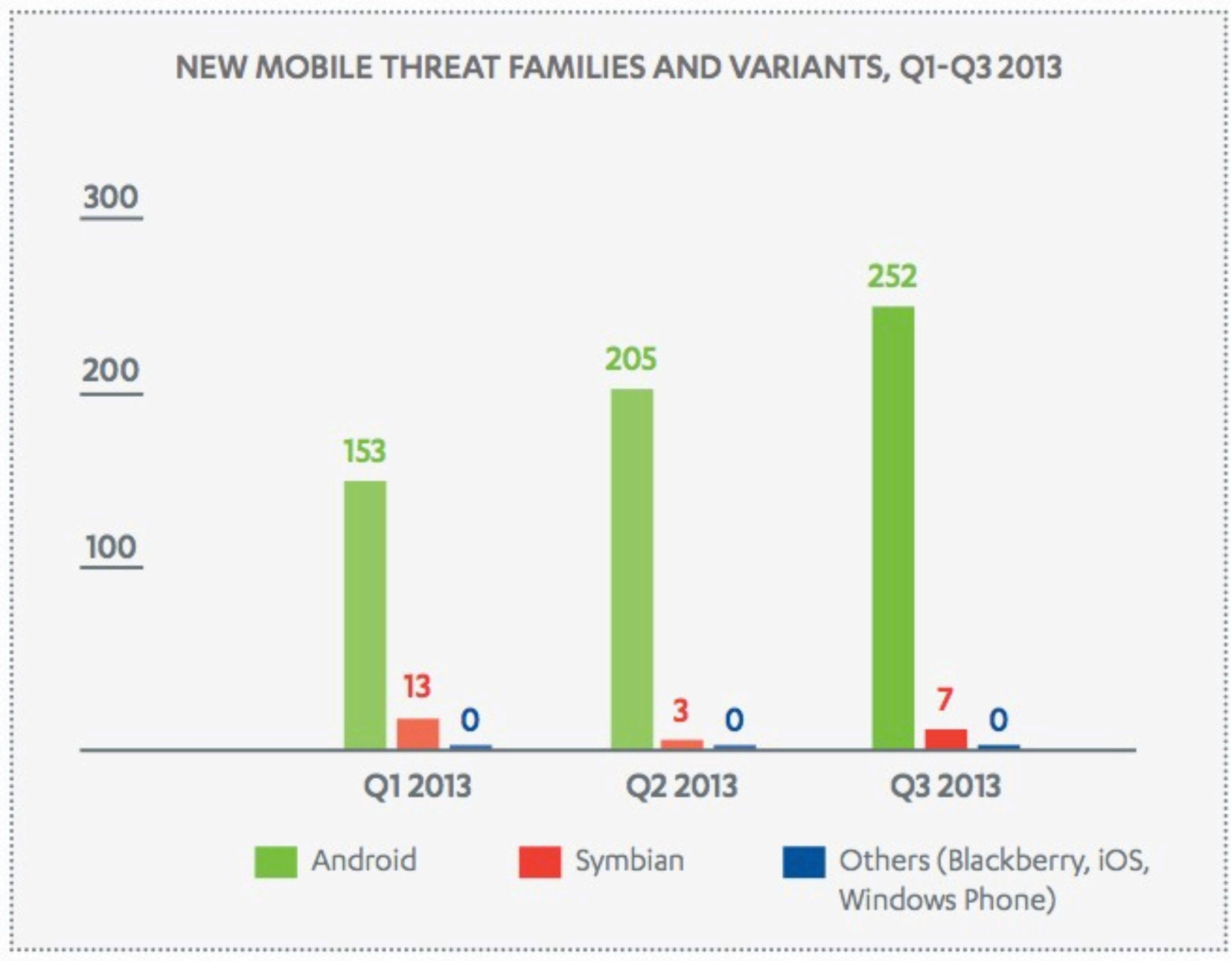
- After ROM-DOS



World-Wide Smartphone Sales (%)



[Wikipedia_MobileOS]


NEW MOBILE THREAT FAMILIES AND VARIANTS, Q1-Q3 2013
300
200
100
153
13
0
205
3
0
252
7
0
Q1 2013
Q2 2013
Q3 2013
Android
Symbian
Others (Blackberry, iOS, Windows Phone)

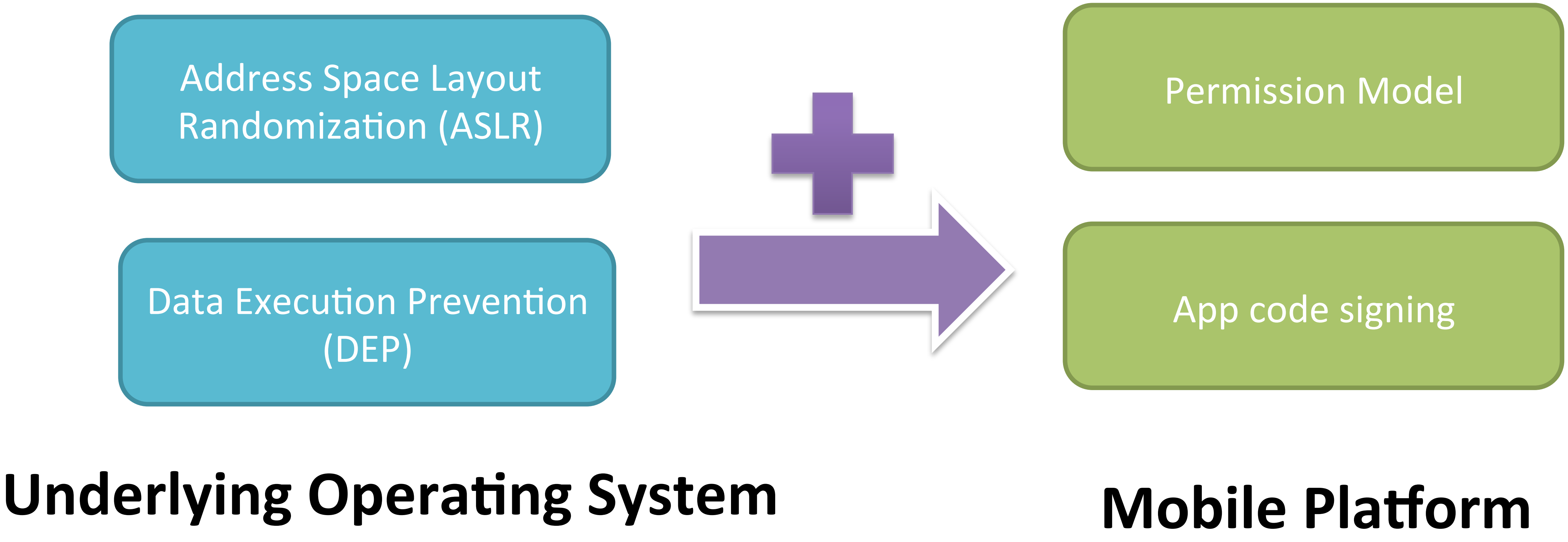
[f-secure]

Questions we investigate

- **People at google are smart, latest security measures are being used, could there be any problems?**
- Wouldn’t upgrading my android definitely improve my security?
- No microphone permission, so would there be any risk of eavesdropping?
- I have no private info on my smartphone, would there be any privacy risks?

From Zygote to Morula: Fortifying Weakened ASLR on Android, B. Lee, L. Lu, T. Wang, T. Kim, and W. Lee, IEEE Symposium on Security and Privacy, 2014.

Security Hardening on Android



Address Space Layout Randomization (ASLR)

Data Execution Prevention (DEP)

Underlying Operating System

Permission Model

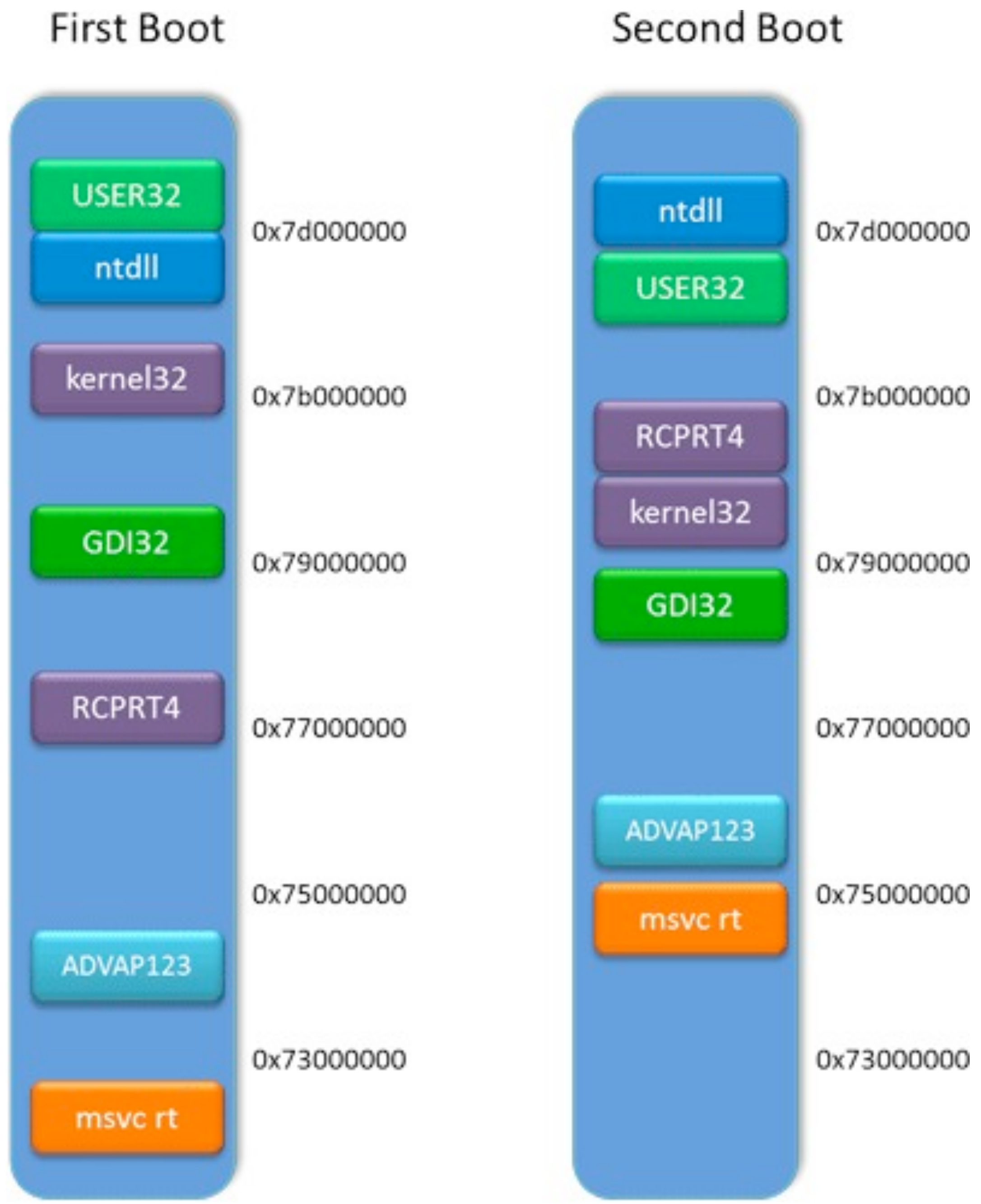
App code signing

Mobile Platform

[Lee2014]

ASLR (Address Space Layout Randomization)

- To implement many of the attacks, location of loaded codes in the memory should be known
- ASLR randomized the layout for each process
- Implemented in many OSes
  - Linux
    - Android 4.1 implements ASLR
  - Mac OS
  - Windows
  - . . . . . .

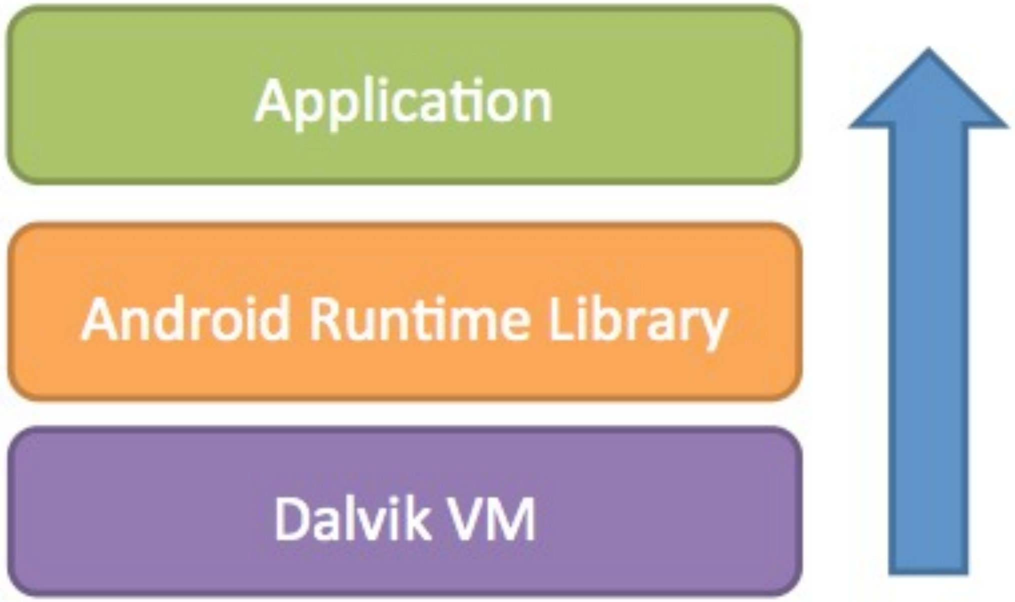


[PcInpact]

Performance Prioritized Designs of Android

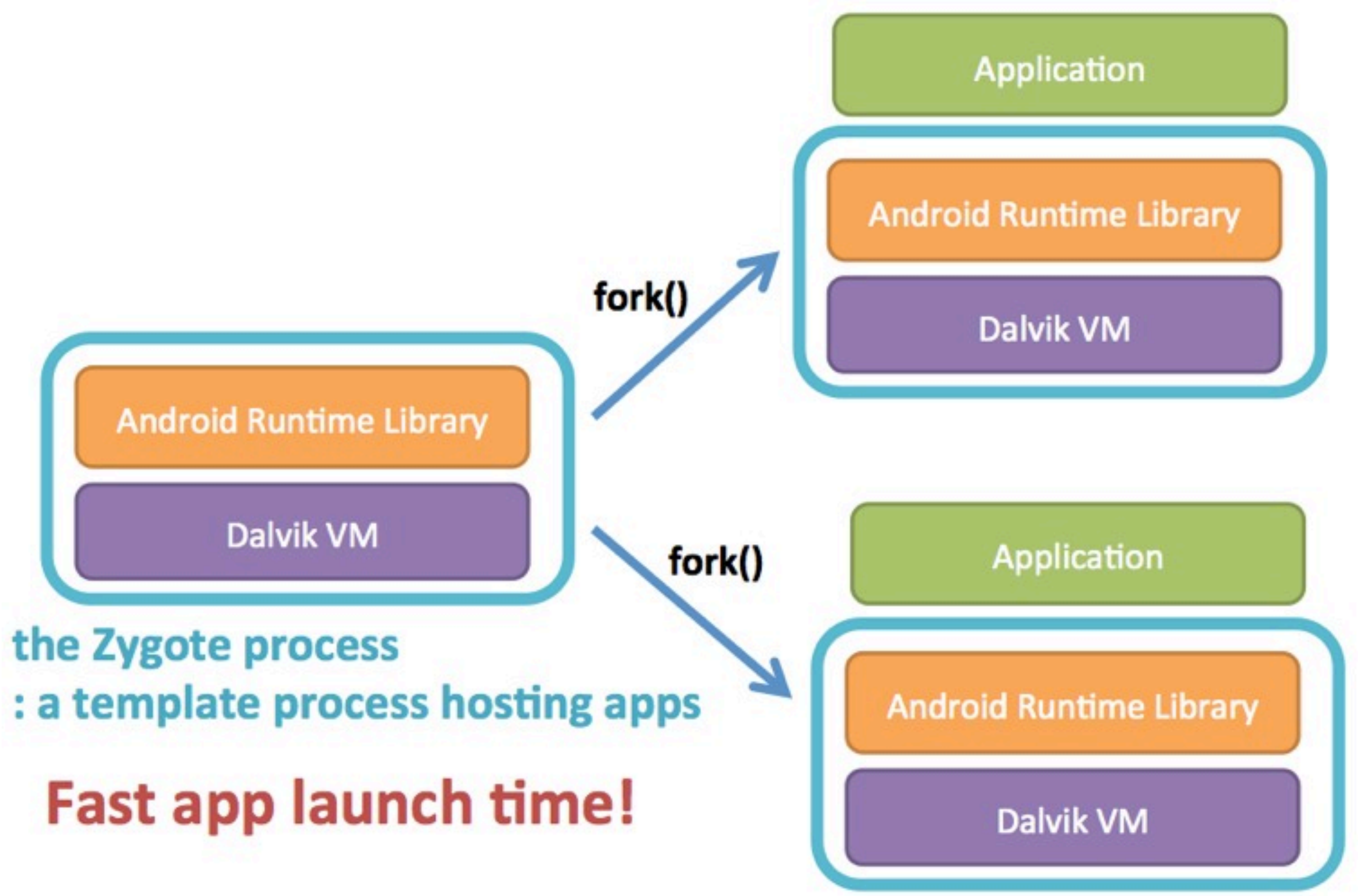
- Multi---layered architectures
  - Android Applications run on Dalvik VM
  - with additional runtime libraries

- --> Slow app launch time



[Lee2014]

Process creation module

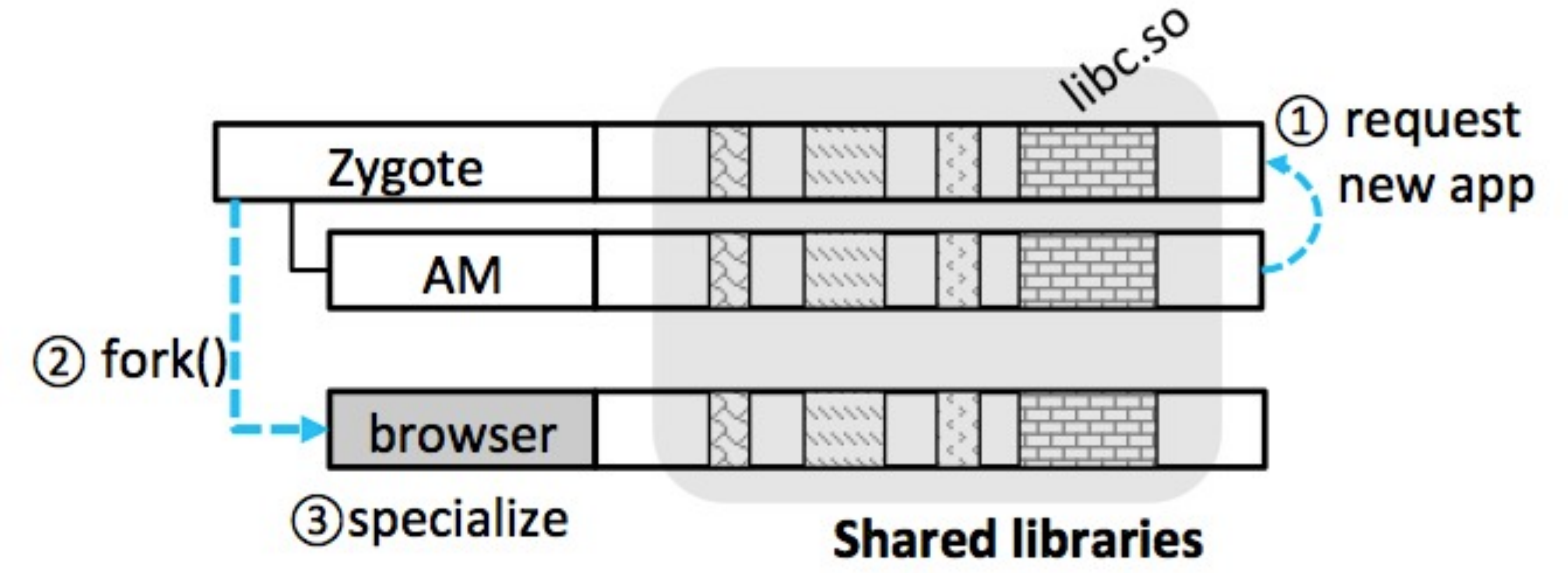


the Zygote process
: a template process hosting apps

Fast app launch time!

[Lee2014]

Weakened ASLR effectiveness

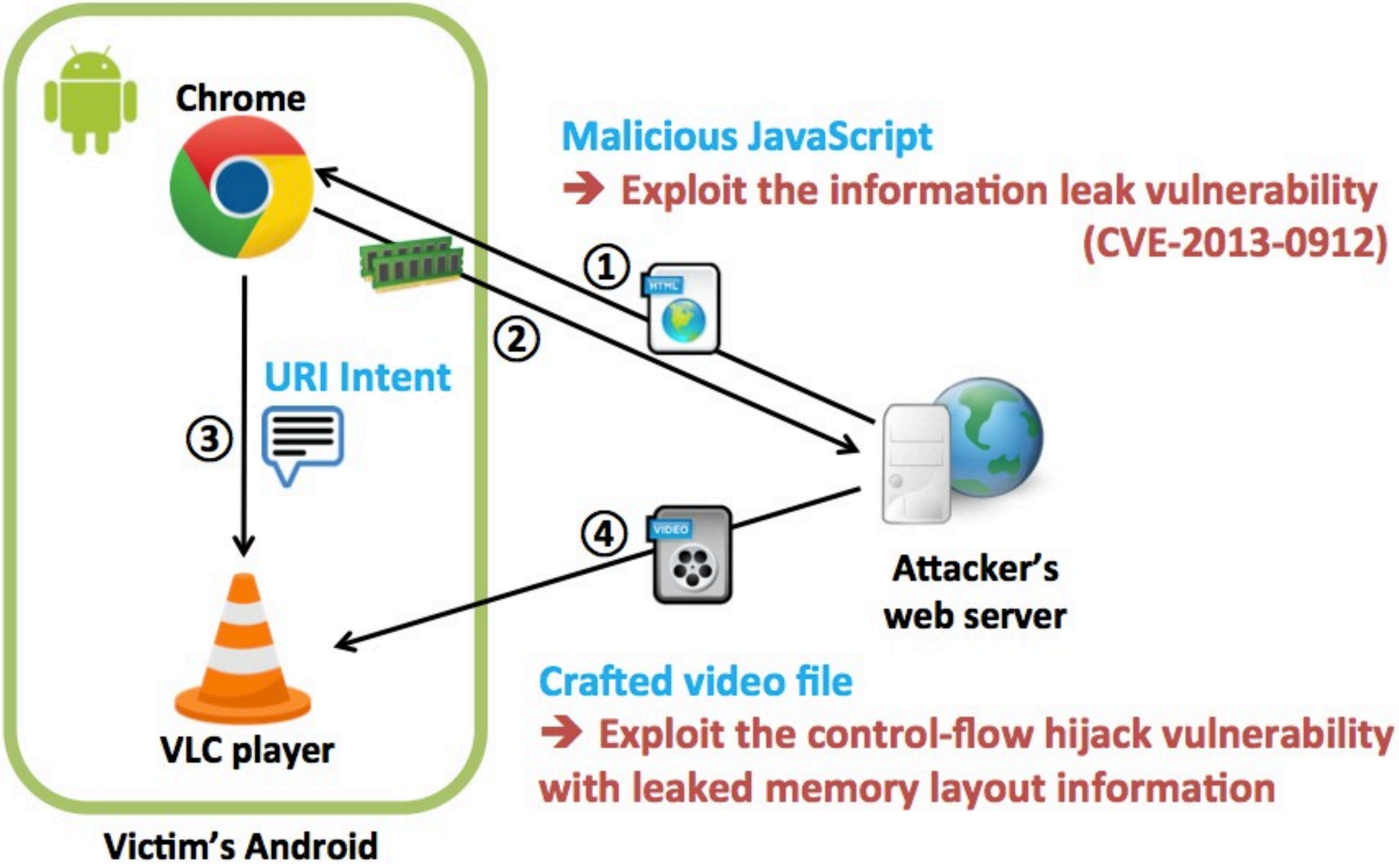


- All apps have the same memory layouts
    - For shared libraries loaded by the Zygote process

Weakens Android ASLR security

[Lee2014]

Attacking weakened ASLR: Remote Coordination Attack



Malicious JavaScript

➔ Exploit the information leak vulnerability (CVE-2013-0912)

Crafted video file

➔ Exploit the control-flow hijack vulnerability with leaked memory layout information

[Lee2014]

Attacking weakened ASLR: Local Trojan Attack

- Zero---permission trojan app
  - Asks (almost) no permissions to the system
  - Scanning memory spaces using the native code
  - Layout information can be exported
    - Intent
    - Internet
- Once the trojan app is installed, ASLR can be easily bypassed

[Lee2014]

Questions we investigate

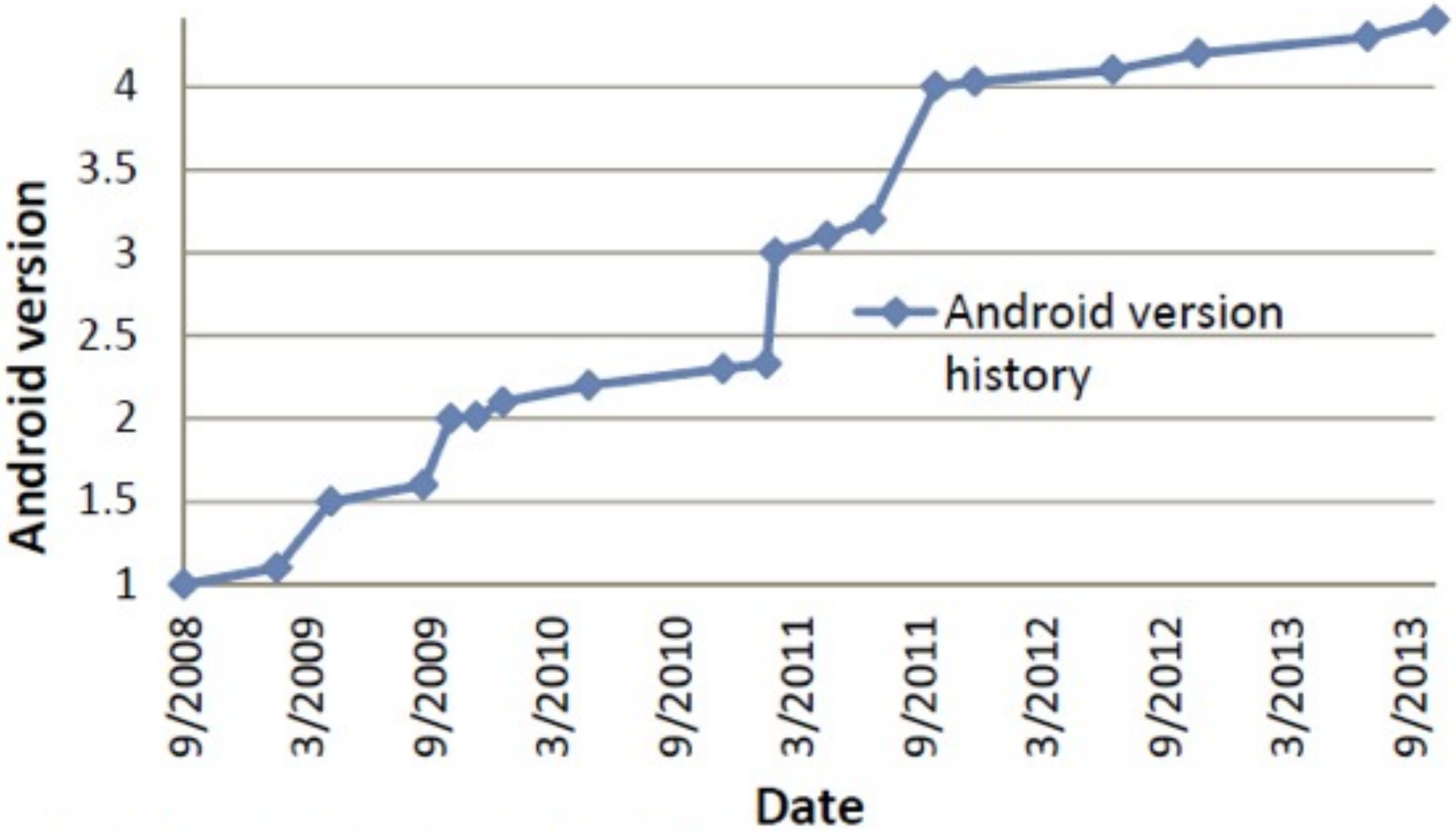
- People at google are smart, latest security measures are being used, could there be any problems?
- **Wouldn’t upgrading my android definitely improve my security?**
- No microphone permission, so would there be any risk of eavesdropping?
- I have no private info on my smartphone, would there be any privacy risks?

Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating,

L. Xing, X. Pan, R. Wang, K. Yuan, and X. Wang, IEEE Symposium on Security and Privacy, 2014.

Mobile OS Updating (Android)

- More complex
  - Sandboxed apps
  - Lots of sensitive user data
  - Updating live system
- More often
- More files
  - 15,525 files from
  - 4.0.4 to 4.1.2
- Less steps (for user)
  - Press one button



[Xing2014]

Android Updating

- Download upgrading image through OTA (Over the Air)
- Reboot to recovery mode
- Replace some system files, such as bootloader, Package Manager Service (PMS), and APKs under `/system` directory
- Reboot to the new OS
- Update other components

[Xing2014]

What PMS does when upgrading Android OS

- Install or reinstall all system apps under `/system`, and then 3rd-party apps under `/data/app`
- Register an app's permissions, shared UID, activities, intent filters, ……
- Decide what to do when a conflict occurs (duplicated attr. or prop.)
  - Build a structure `mSettings` for existing apps, and include:
    - `mPackages`
    - `mUserIds`
    - `mSharedUsers`
    - `mPermissions`
    - etc.
  - Check the `mSettings` when installing a new system package
  - If having conflicts, decide case by case.

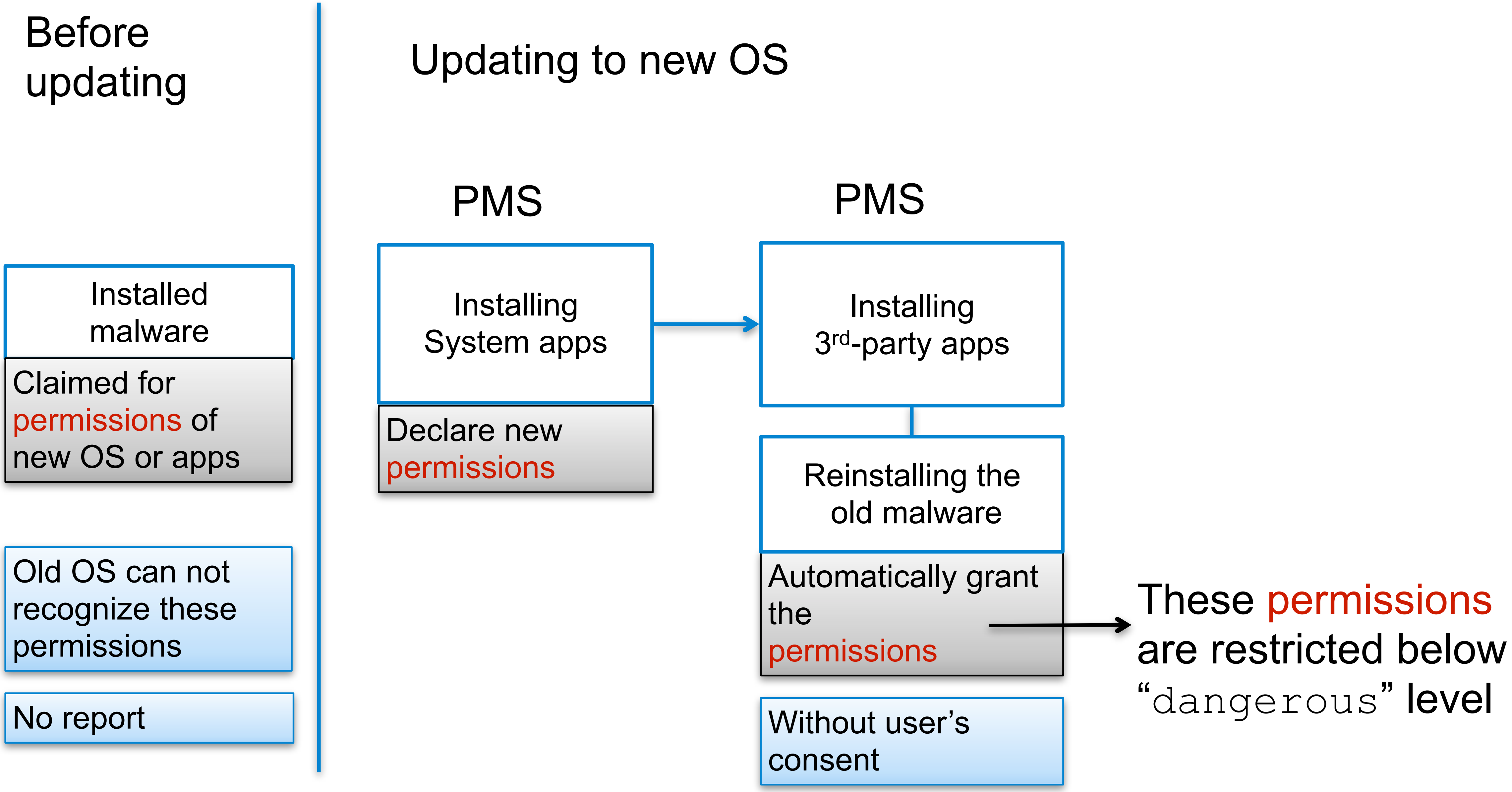
[Xing2014]

Pileup Exploits

- Assume that an attacker has a malicious app installed through google play or 3rd part market
- App requests permission not available in current version
- Possible exploits:
    - Permission Harvesting and Preempting
    - Shared UID Grabbing
    - Data Contamination
    - Denial of Services

[Xing2014]

Pileup Exploits – Permission Harvesting and Preempting



Before updating

Installed malware

Claimed for permissions of new OS or apps

Old OS can not recognize these permissions

No report

Updating to new OS

PMS

Installing System apps

Declare new permissions

PMS

Installing 3rd-party apps

Reinstalling the old malware

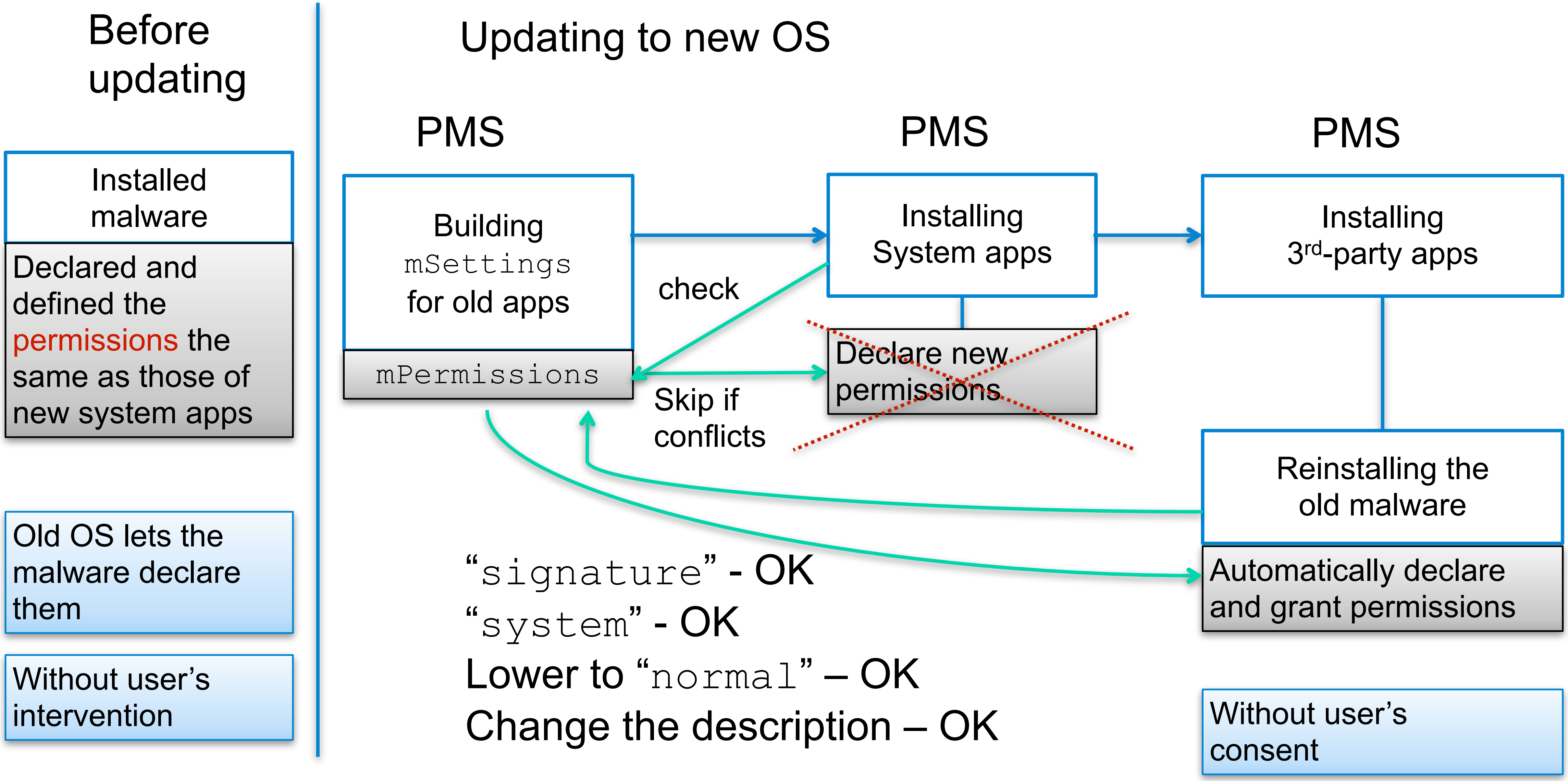
Automatically grant the permissions

Without user's consent

These permissions are restricted below "`dangerous`" level

[Xing2014]

Pileup Exploits – Permission Harvesting and Preempting



Before updating

Installed malware

Declared and defined the permissions the same as those of new system apps

Old OS lets the malware declare them

Without user's intervention

Updating to new OS

PMS

Building `mSettings` for old apps

`mPermissions`

check

Skip if conflicts

PMS

Installing System apps

~~Declare new permissions~~

PMS

Installing 3rd-party apps

Reinstalling the old malware

Automatically declare and grant permissions

Without user's consent

"`signature`" - OK

"`system`" - OK

Lower to "`normal`" – OK

Change the description – OK

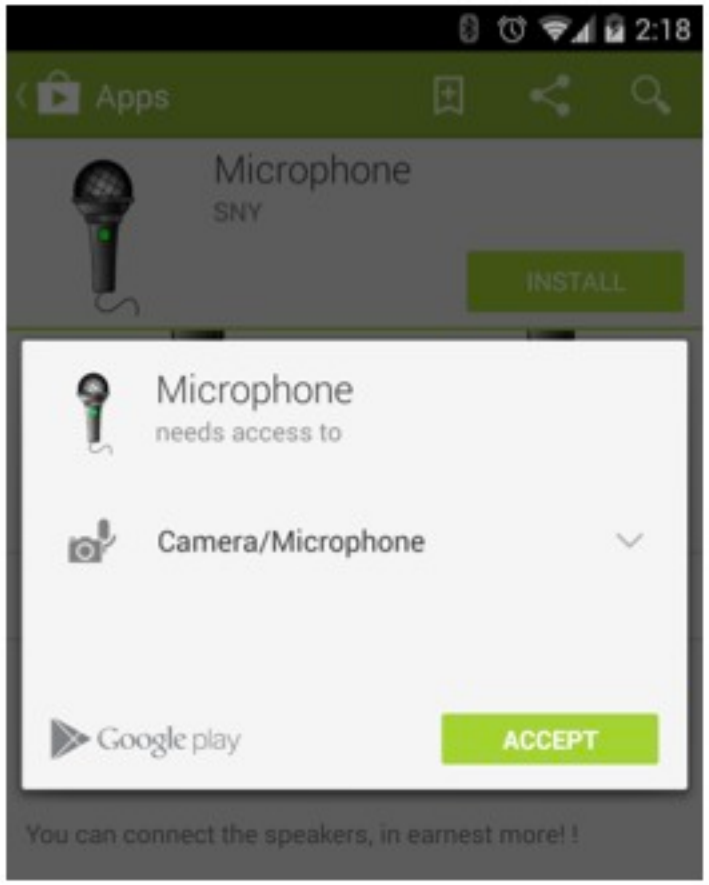
[Xing2014]

Questions we investigate

- People at google are smart, latest security measures are being used, could there be any problems?
- Wouldn’t upgrading my android definitely improve my security?
- **No microphone permission, so would there be any risk of eavesdropping?**
- I have no private info on my smartphone, would there be any privacy risks?

Gyrophone: Recognizing Speech from Gyroscope Signals, Y. Michalevsky, D. Boneh, G. Nakibly, Usenix Security 2014.

MICROPHONE ACCESS



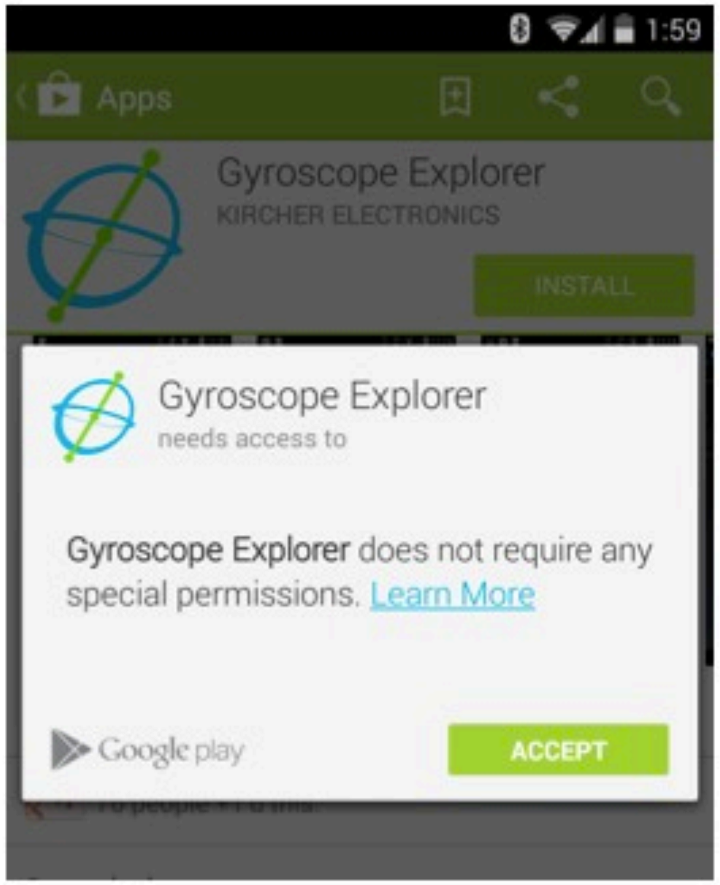
Microphone
needs access to

Camera/Microphone

You can connect the speakers, in earnest more! !

REQUIRES PERMISSIONS

GYROSCOPE ACCESS



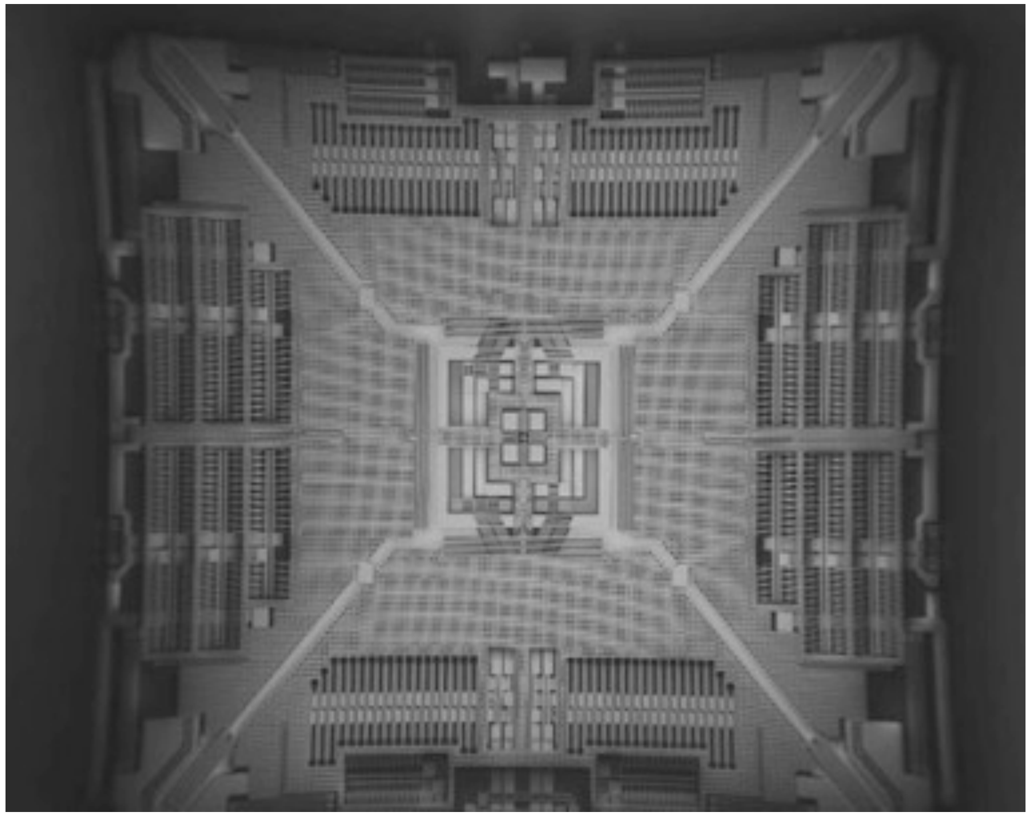
Gyroscope Explorer
needs access to

Gyroscope Explorer does not require any special permissions. Learn More

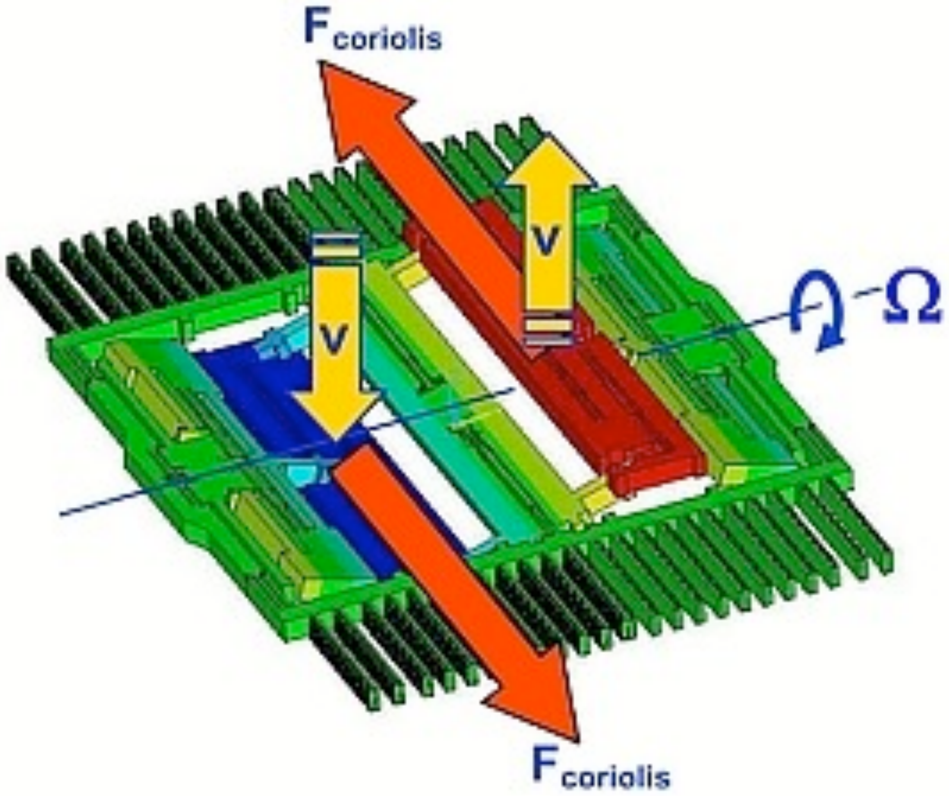
DOES NOT REQUIRE PERMISSIONS

[Michalevsky2014]

Gyroscopes



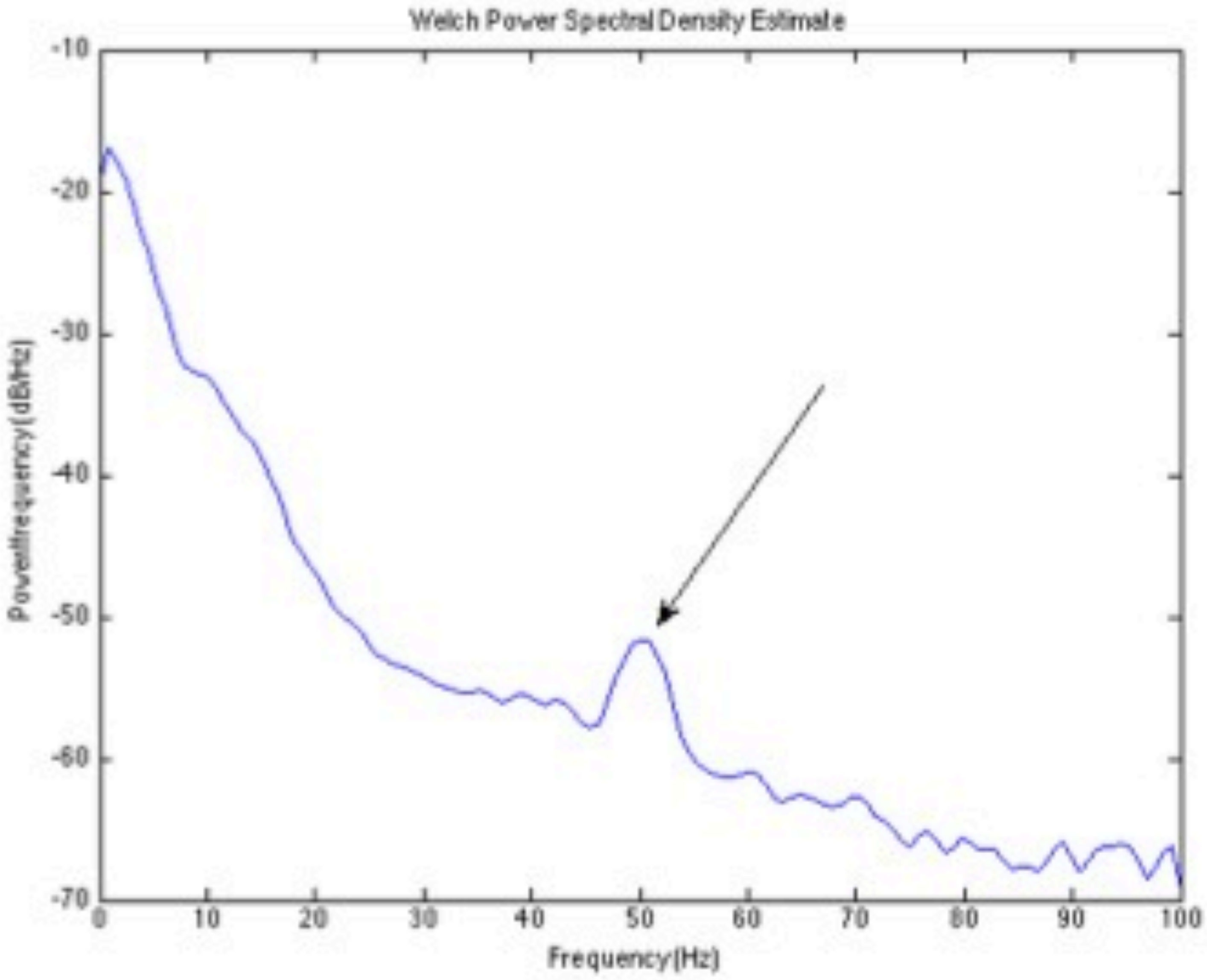
STM Microelectronics
Samsung Galaxy



InvenSense
Google Nexus

[Michalevsky2014]

Gyroscopes are susceptible to sound



50 HZ TONE POWER SPECTRAL DENSITY

[Michalevsky2014]

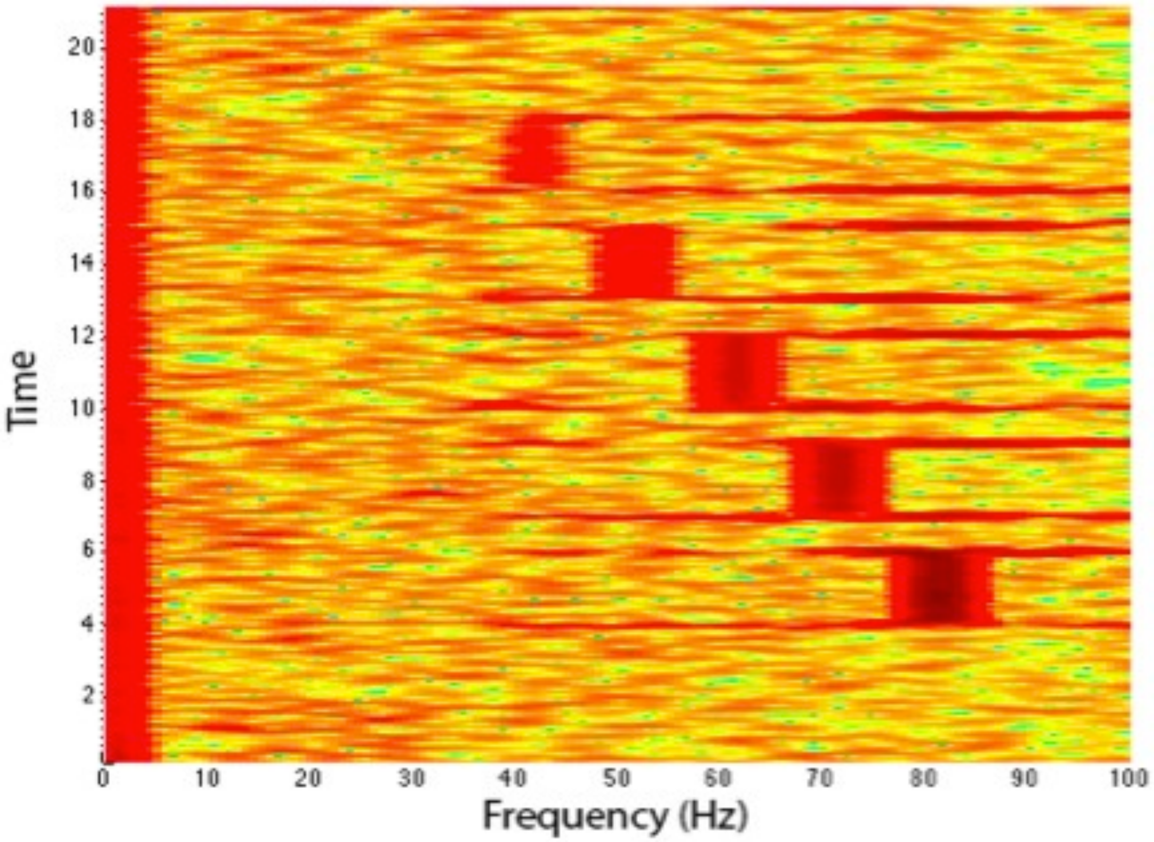
Gyroscopes are (lousy, but still) microphones

- Hardware sampling frequency:
  - InvenSense: up to 8000 Hz
  - STM Microelectronics: 800 Hz
- Software sampling frequency:
  - Android: 200 Hz
  - iOS: 100 Hz
- Very low SNR (Signal-to-Noise Ratio)
  - Acoustic sensitivity threshold: ~70 dB
    - Comparable to a loud conversation.

[Michalevsky2014]

How do we look into higher frequencies?

- Speech range:
  - Adult male 85-180 HZ
  - Adult female 165 - 255 HZ
- Make use of aliasing

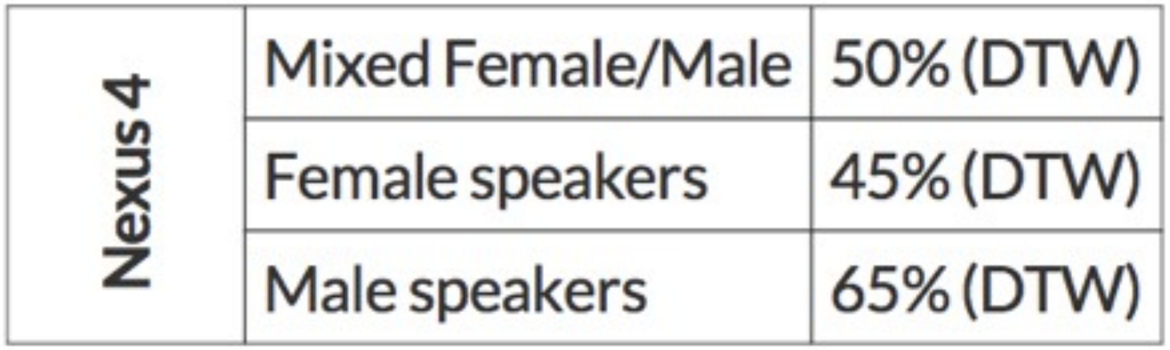


THE RESULT OF RECORDING TONES BETWEEN 120 AND 160 HZ ON A NEXUS 7 DEVICE

[Michalevsky2014]

Accuracy

- Gender identification
  - Nexus 4 84%
  - Galaxy S III 82%
  - Random guess probability 50%
- Speaker identification



Nexus 4	Mixed Female/Male	50% (DTW)
	Female speakers	45% (DTW)
	Male speakers	65% (DTW)

  - Random guess probability is 20% for one gender and 10% for a mixed set
- Isolated word recognition (speaker dependent)
  - 65% (random guessprobability 9%)

[Michalevsky2014]

What if OS is patched?

- Hardware sampling frequency:
  - InvenSense: up to 8000 Hz
  - STM Microelectronics: 800 Hz
- Software sampling frequency:
  - Android: 200 Hz
  - iOS: 100 Hz

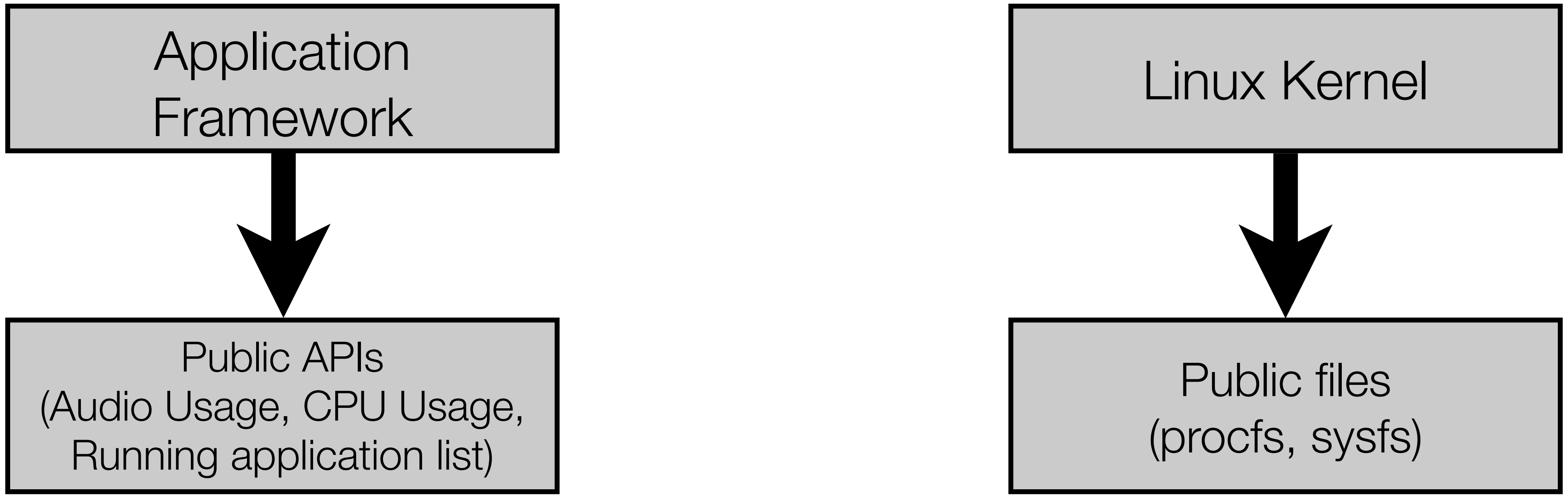
[Michalevsky2014]

Questions we investigate

- People at google are smart, latest security measures are being used, could there be any problems?
- Wouldn’t upgrading my android definitely improve my security?
- No microphone permission, so would there be any risk of eavesdropping?
- **I have no private info on my smartphone, would there be any privacy risks?**

Identity, location, disease and more: inferring your secrets from android public resources, X. Zhou, S. Demetriou, D. He, M. Naveed, X. Pan, X. Wang, C. Gunter, K. CCS 2013.

Android Public Resources


Application Framework
Public APIs (Audio Usage, CPU Usage, Running application list)
Linux Kernel
Public files (procfs, sysfs)

[Zhou2013]

Location inference

- /proc/net/arp contains Address Resolution Protocol (ARP) information!
- /proc/net/arp contains BSSID (i.e. MAC address of the wireless interface) of the access point phone is connected to
  - ARP information wasn’t considered sensitive in original Linux design
- Databases such as Navizon collest MAC to GPS locations
- zero permission app could collect MAC information from /proc/net/arp

[Zhou2013]

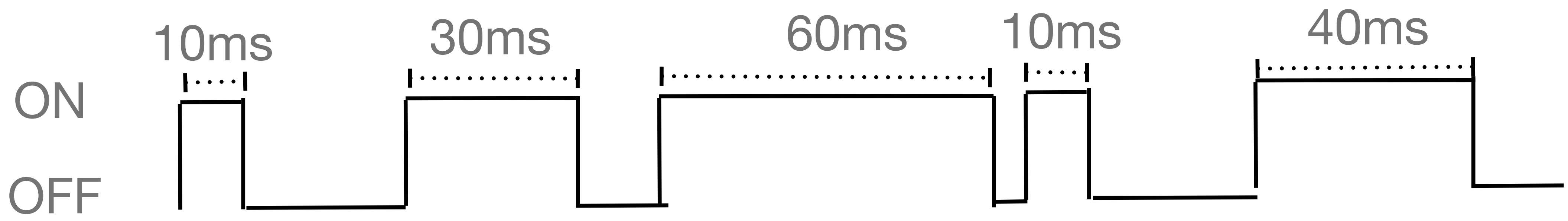
Transmitting out information

- Using URI ACTION_VIEW an app could transmit a GET request through the browser
  - A payload could be transmitted with the GET request
- User will observe this on the screen
  - When screen is off, the browser will be “paused”
- Therefore, an app will continuously check the lcd status indicator (/lcd_power)
  - When indicator becomes zero, the screen dims out
  - the app will submit the request to the browser at that point
  - after transmission, it redirect the browser to google to cover its tracks

[Zhou2013]

Driving route interference

- Speaker status (i.e. On/Off), could be check by AudioManager.isMusicActive



- Segment 1: Turn left onto N Goodwin Ave
- Segment 2: Head west on W Clark St toward N Busey Ave

Driving route interference

- Check if GPS navigation app is running
- Collect speaker on/off periods
- Create Fingerprint
  - 10 | 30 | 60 | 10 | 40
- Find the matching fingerprint in the database

[Zhou2013]

Questions we investigated

- People at google are smart, latest security measures are being used, could there be any problems?
- Wouldn’t upgrading my android definitely improve my security?
- No microphone permission, so would there be any risk of eavesdropping?
- I have no private info on my smartphone, would there be any privacy risks?

Acknowledgments/References

- [Wikipedia_MobileOS] http://en.wikipedia.org/wiki/Mobile_operating_system
- [f-secure] Mobile Threat Report, F-Secure, Q3-2013. http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
- [Lee2014] From Zygote to Morula: Fortifying Weakened ASLR on Android, B. Lee, L. Lu, T. Wang, T. Kim, and W. Lee, IEEE Symposium on Security and Privacy, 2014.
- [Xing2014] Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating, L. Xing, X. Pan, R. Wang, K. Yuan, and X. Wang, IEEE Symposium on Security and Privacy, 2014.
- [Michalevsky2014] Gyrophone: Recognizing Speech from Gyroscope Signals, Y. Michalevsky, D. Boneh, G. Nakibly, Usenix Security 2014.
- [Zhou2013] Identity, location, disease and more: inferring your secrets from android public resources, X. Zhou, S. Demetriou, D. He, M. Naveed, X. Pan, X. Wang, C. Gunter, K. CCS 2013.