Mobile Forensics and Challenges: Perspective of Indian Investigators

Saurabh Kumar
Senior Research Scholar
IIT Kanpur

Images Source: Google images

DIGITAL FORENSICS & INVESTIGATION

Terms and Definitions

- **Mobile Forensics:** The science of recovering digital evidence from mobile phone under forensically sound conditions using accepted methods. (NIST)

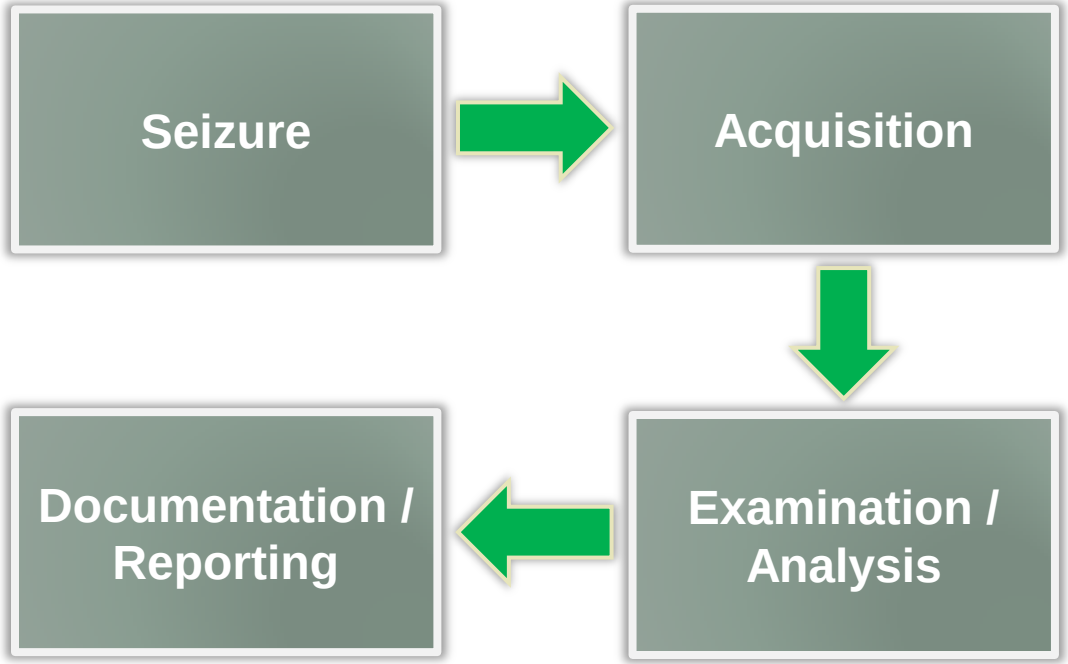
- **Penetration Test:** A method of evaluating the security of a computer system or network by simulating an attack from malicious **outsider/insider**. (Wikipedia)

- **Vulnerability Assessment:** A process of identifying, quantifying and prioritizing the vulnerabilities in a system.

Forensics Overview

- Potential scenarios, not specific to Mobile
- Evidence gathering for legal proceedings
- Corporate investigations
  - Intellectual property or data theft
  - Employment-related investigations including discrimination, sexual harassment
  - Security audit
- Family matters
  - Estate disputes
  - Divorce
- Government security and operations
  - Cyber Threats
  - Stopping cyber attacks
  - Intelligence / Counter-intelligence gathering

Investigation Process



Forensics Considerations

- Important items to consider during investigations
  - Chain of custody
  - Detailed notes and complete report
- Validation of investigations results using tools or other investigators

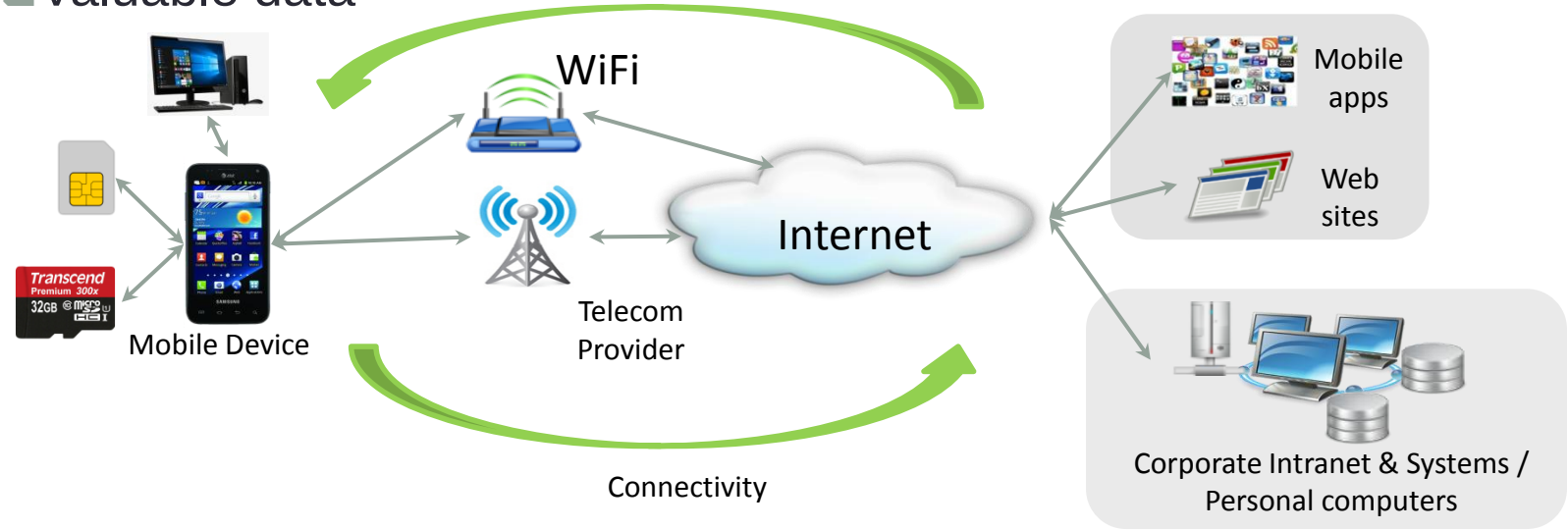
Legalities

- Possibility of a mobile device being involved in crimes
- Easily cross geographical boundaries; multi-jurisdiction issues
- Investigator should be well aware of regional laws
- Data may be altered during collections, causing legal challenges

MOBILE FORENSICS

Why Mobile Forensics

- Technology improvements
- User activity
- Valuable data
- Always on
- Multiple Communication Entity



Type of Evidence from Mobile

- Physical
- Electronic

Physical Evidence from Mobile

- DNA
- Fingerprints

Electronic Evidence

- Can be use to establish **LAB**
- **L**ocation
- **A**ssociation
- **B**ehavior
- Some Information
  - Call history
  - Contacts
  - SMSs
  - Calendar
  - Location
  - Images
  - Audio/Video
  - Many more…

Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Network Service Provider

- Can provide
  - Subscriber details
  - Call History – Call Details Record (CDR)
  - List of accessed web services – IP Details Record (IPDR)
  - Geographic location – Tower locations through which a phone is connected for communication
  - Cell Tower Logs (Tower Dump)

Call Details Record (CDR)

- Looks like

Info abut associated Mobile Device

Info about user's location

Calling No.	Called No.	REC TYPE	TRANS_DT	Duration	IMEI	CELL ID
94XXXXX093	94XXXXX032	MOC	20130101113117	63	35789004232353	405-54-902-2
94XXXXX534	94XXXXX093	MTC	20130101132532	40	35789004232353	405-54-576-1
94XXXXX997	94XXXXX093	SMT	20130101165754	1	35789004232353	405-54-576-3
94XXXXX093	94XXXXX109	MOC	20130101165937	247	35789004232353	405-54-576-2

Calling No.	Called No.	REC TYPE	Date	Time	Duration	IMEI	FIRST_CELL ID (Origin)
94XXXXX093	94XXXXX032	OUT	01/01/2013	11:31:17	63	35789004232353	405-54-902-2
94XXXXX534	94XXXXX093	IN	01/01/2013	13:25:32	40	35789004232353	405-54-576-1
94XXXXX997	94XXXXX093	S_IN	01/01/2013	16:57:54	1	35789004232353	405-54-576-3
94XXXXX093	94XXXXX109	OUT	01/01/2013	16:59:37	247	35789004232353	405-54-576-2

Cell ID

- Cell ID is used to uniquely identify BTS (base transceiver station)
- Comprises of four components
  - Mobile Country Code (MCC): first 2-3 digit
  - Mobile Network Code (MNC): next 2-3 digit
  - Location Area Code (LAC): variable length
  - Sector ID (SID): last digit
- Device is always associated with a BTS

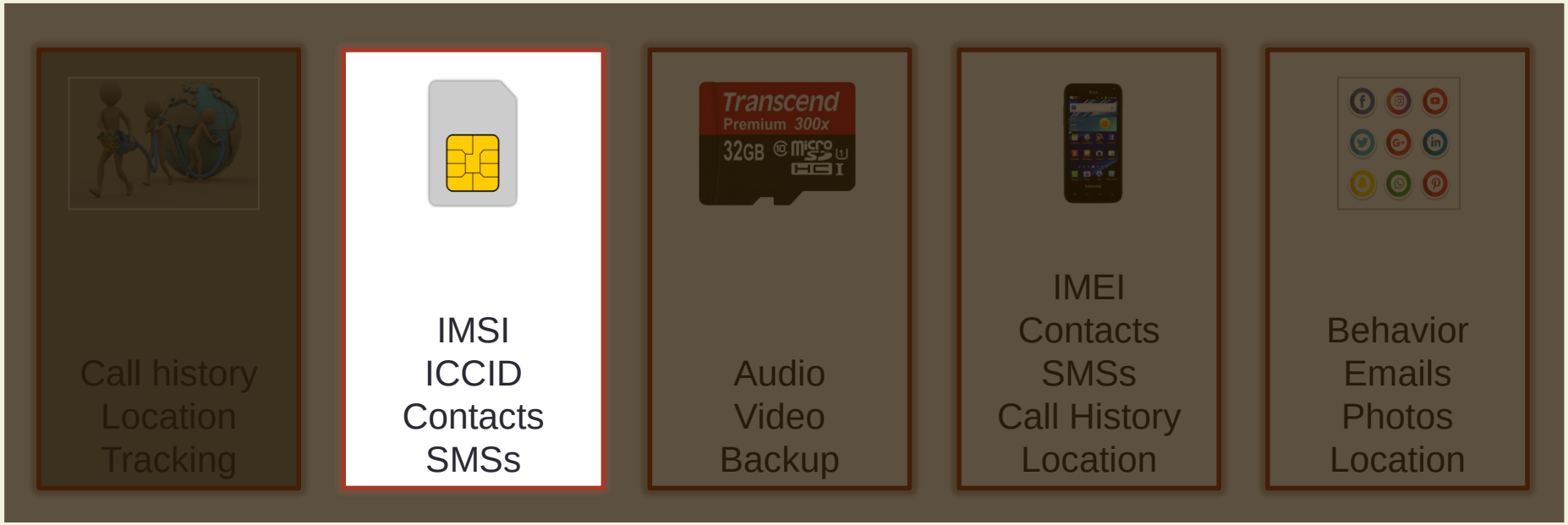
Tower Dump

SUBS NO	OTHER PRTY NO	Date	TIME	Dur	CELLID FIRST	CELLID LAST	REC TYPE	SUBS IMEI	SUBS IMSI	SUBSCRIPTION TYPE	SMS CENTER NO	MSCID
9197XXXXX772	9177XXXXX344	8/20/2013	05:01:51	25	11971-20/8	11971-20/8	MOC	359326022655600	405804191782627	PRE	?	919762099002
9181XXXXX996	9183XXXXX714	8/20/2013	05:10:29	1	13311-20/8	13311-20/8	SMMT	358650031107530	405804191482793	PRE	919823000040	919762099002
9197XXXXX131	9198XXXXX217	8/20/2013	05:38:48	94	13311-20/8	13311-20/8	MTC	359351043644880	405804170433460	POST	?	919762099002
9187XXXXX730	9187XXXXX108	8/20/2013	05:53:03	1	13311-20/8	13311-20/8	SMMO	355672050976690	405804181584703	PRE	919716099155	919762099002

Challenges with Mobile Networks

- No uniformity between CDR format
- Correlation among multiple CDR
- Difficulty in analyzing tower dump
  - Huge amount of data
  - Difficulty in extraction of useful information
- Non availability of live tower data

Sources of Information



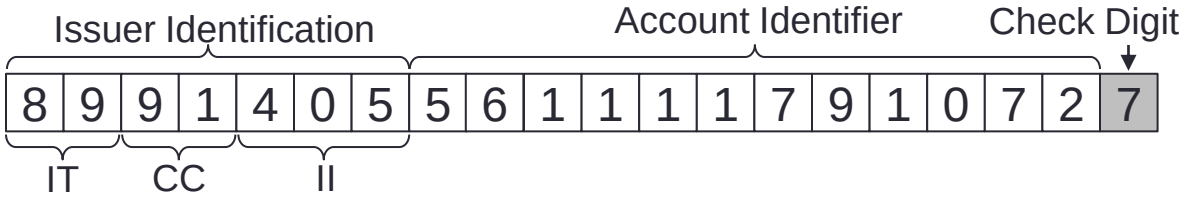
Subscriber Identity Module (SIM)

- Identifies/authenticates a subscriber to the network
- Two Unique Identity
  - ICCID
  - IMSI – (Programmable)
- Storage for contacts, SMSs, etc…

Integrated Circuit Card ID (ICCID)

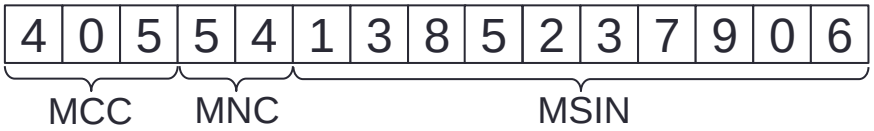
- It is SIM serial number
- 19 or 20 digit length
- Service provider can identify phone number from ICCID
- Reveals country of origin, Industry Type, and network
  - Issuer Identification Number: composed of industry type (first 2 digit), country code (next 2-3 digit), and issuer identifier (next 1-4 digit)
  - Individual account identification: Variable length
  - Check digit – Last digit of ICCID

IT: Industry Type
CC: Country Code
II: Issuer Identifier



International Mobile Subscriber Identity (IMSI)

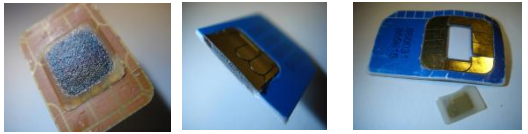
- Used by the network to identify subscriber
- 15 digit number
- Stored on the SIM card (programmed by the network provider)
- Reveals name and country of issuing service provider
  - Mobile Country Code (MCC): first 2-3 digit
  - Mobile Network Code (MNC): next 2-3 digit
  - Mobile Subscriber Identification Number (MSIN): remaining digits



Challenges with SIM

- Issue with ICCID
  - Partial ID is printed on SIM card
  - No printed information about ICCID

- Damaged SIM card



- eSIM

Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

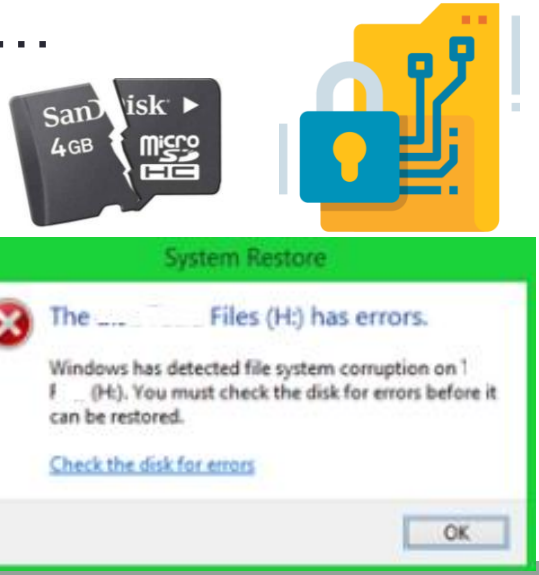
IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Memory Card

- Serves as secondary storage for mobile
- Use file system to store information mostly FAT
- Stores Audio, video, photos, backup, etc…

- Challenge:
  - Damaged memory card
  - Corrupted file system
  - Encryption



Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Mobile Handset

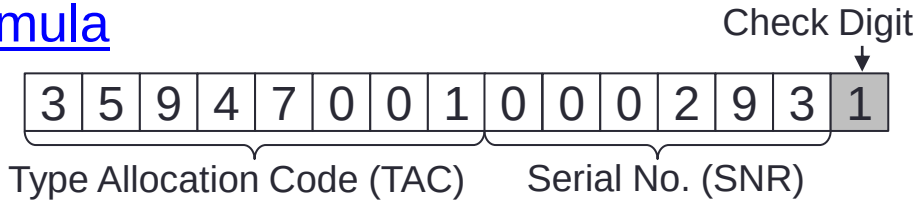
- Just Looking
  - Make / Model
  - Condition
  - Age
  - Capabilities
  - Network type 2G, 3G, 4G, Others
- Rich source of information
  - Contacts, images, videos, call logs, SMSs, etc..
- Uniquely identified by using IMEI






International Mobile Equipment Identifier (IMEI)

- Kind of serial number of the handset, (15 digit long)
- Intended to be unique
  - Can be reprogrammed with specialized equipment (illegal)
- Can reveal (First eight digits, TAC)
  - Make, mode, date and country of origin
- Serial Number (next six digits)
- Check digit (last digit)
- Can be validated by using Luhn formula



Information of Interest

Basic Information	• IMEI • H/W and S/W information • Network Information
Event Logs	• Incoming, outgoing missed call history • SMS history • Session logs – Wi-if, GPRS/3G/4G
Calendar Events	• Meetings, reminders • Last modification
Tasks	• Description • Deadline, priority • Completion date & time
Messaging System	• Text and multimedia messages • BIO messages: vCard, configurations, and others • Beamed messages: file sent via Bluetooth, IT or USB

Information of Interest cont..

GPS Navigation	• Last fixed GPS coordinates • Search and Routes history • Saved maps, favorite places
Location Tagger	• GPS coordinates in camera snapshots • Cell tower coordinates in camera snapshots • Cell tower coordinates for SMS, calls
IM Clients	• IP, Login (UID, email) and password* • Contact list, • Chat and call history
Contact Info	• Caller groups • Speed dials
Apps	• Multiple Apps with there storage capacity • Like social media activities, emails, web history, etc..

Challenges with Mobile Device

- Multiple smartphone vendors and OS(es)
- Mobile platform security features
- Generic state of the device
- Anti-forensic techniques
- Dynamic nature of evidence
- Accidental reset
- Device alteration
- Phone lock
- Malicious Programs
- Multiple communication point
- Legal issues

Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Applications (Apps)

- Can be used to analyze behavior/state of person
  - Social gathering, health condition, etc..
- App stores local data in SQLite database
- Application analysis can give type of information and metadata about an App

- Challenge:
  - Different architecture for different Apps
  - Dynamic nature – behave differently in different environment
  - Use of encryption to store data
  - Correlations between Apps

ANDROID

Why Android?

Android Ecosystem

1. Almost completely open source

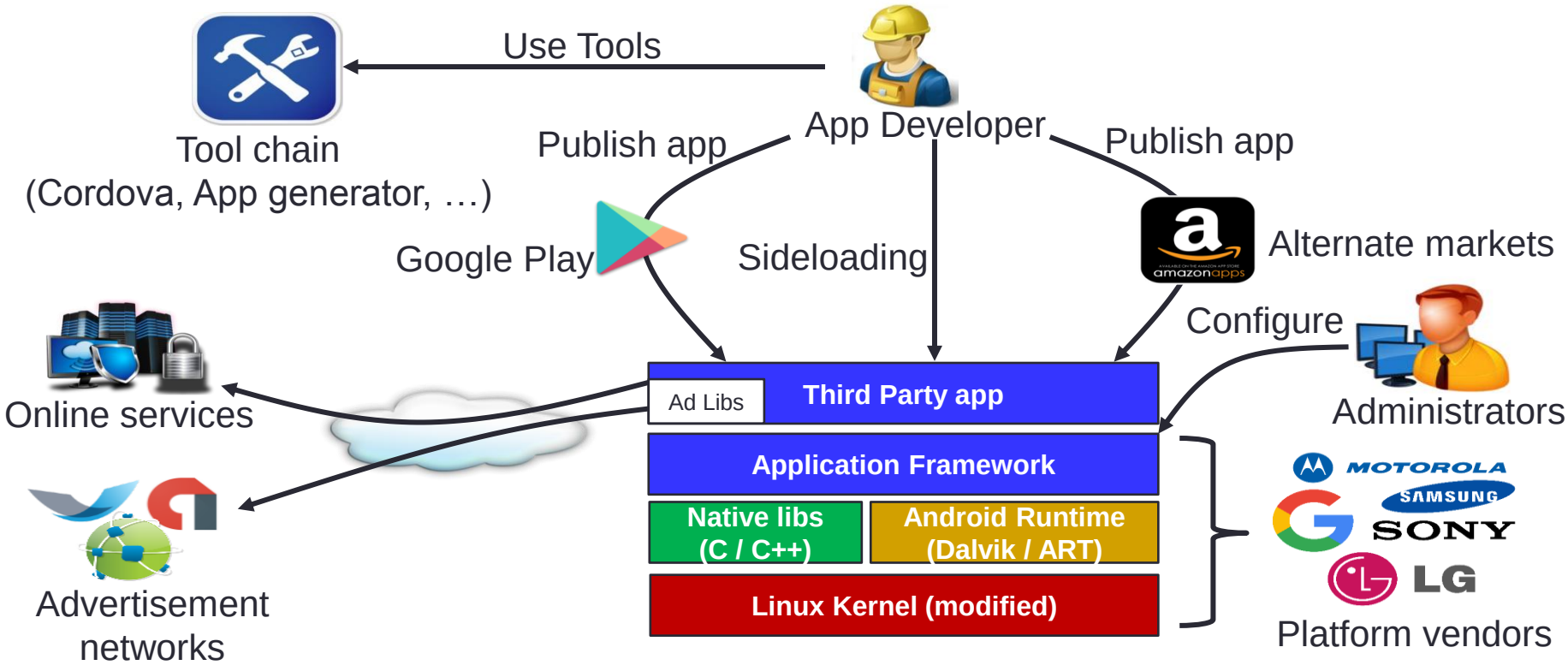
Source: https://giphy.com/gifs/southparkgifs-3o6ZtqprcPDOkDru5W

2. Global Smartphone Market Trends

Period	Android	iOS	Windows	Others
Q1 2016	83.4%	15.4%	0.8%	0.4%
Q2 2016	87.6%	11.7%	0.4%	0.3%
Q3 2016	86.6%	12.5%	0.3%	0.4%
Q4 2016	81.4%	18.2%	0.2%	0.2%
Q1 2017	85%	14.7%	0.1%	0.1%

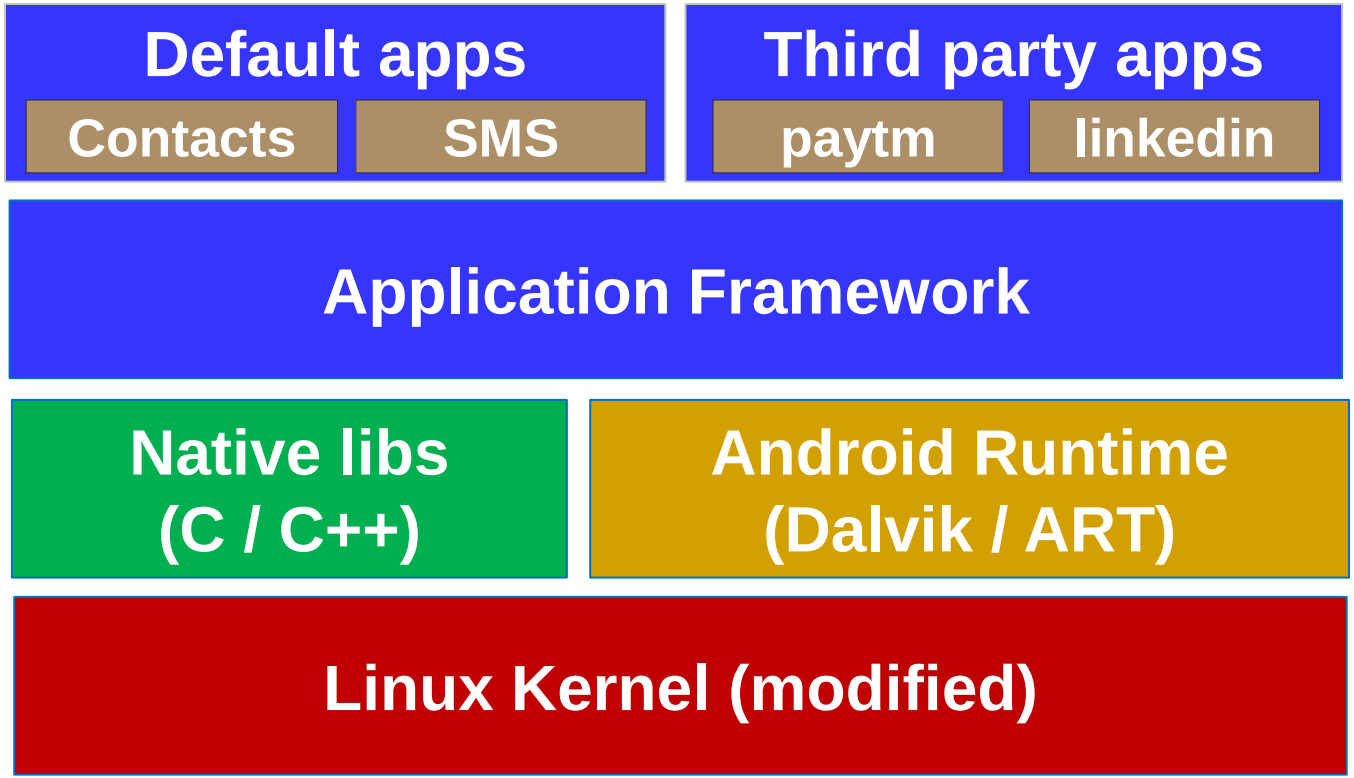
Source: International Data Corporation (IDC), May 2017

Actors in the Android Ecosystem



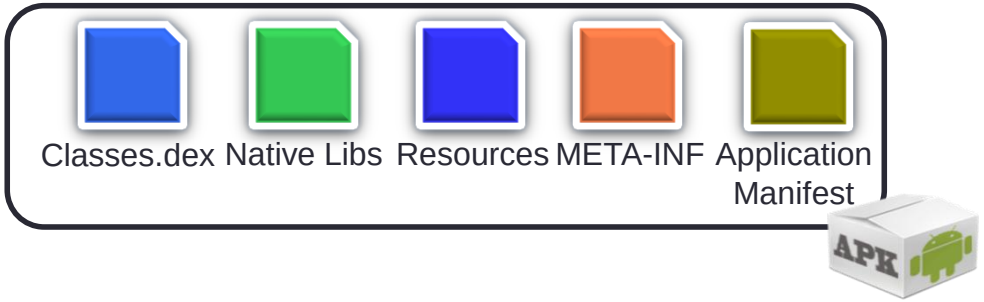
ANDROID APPLICATIONS

Android Software Stack



Application Packages (APK)

- APK is simply a packaging format like **JAR**, ZIP and TAR
- Component of Application
  - Activity
  - Content Provider
  - Services
  - Broadcast Receiver
- Native Code (C/C++ shared libraries)
- Resources
- META-INF
- Application Manifest

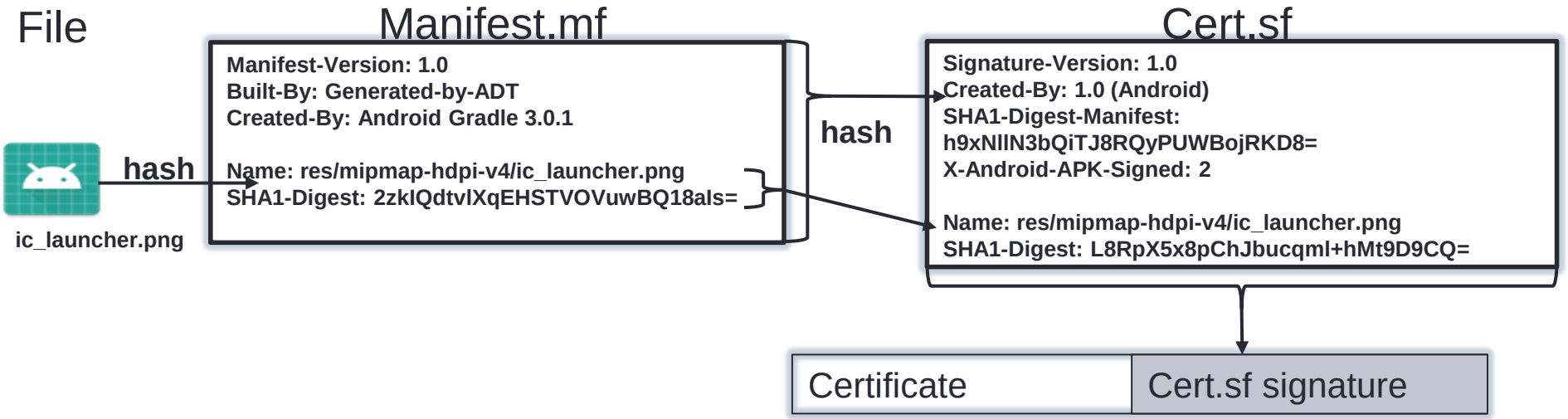


ANDROID SECURITY ARCHITECTURE

- Package Integrity
- Sandboxing
- Permission and Least Privilege

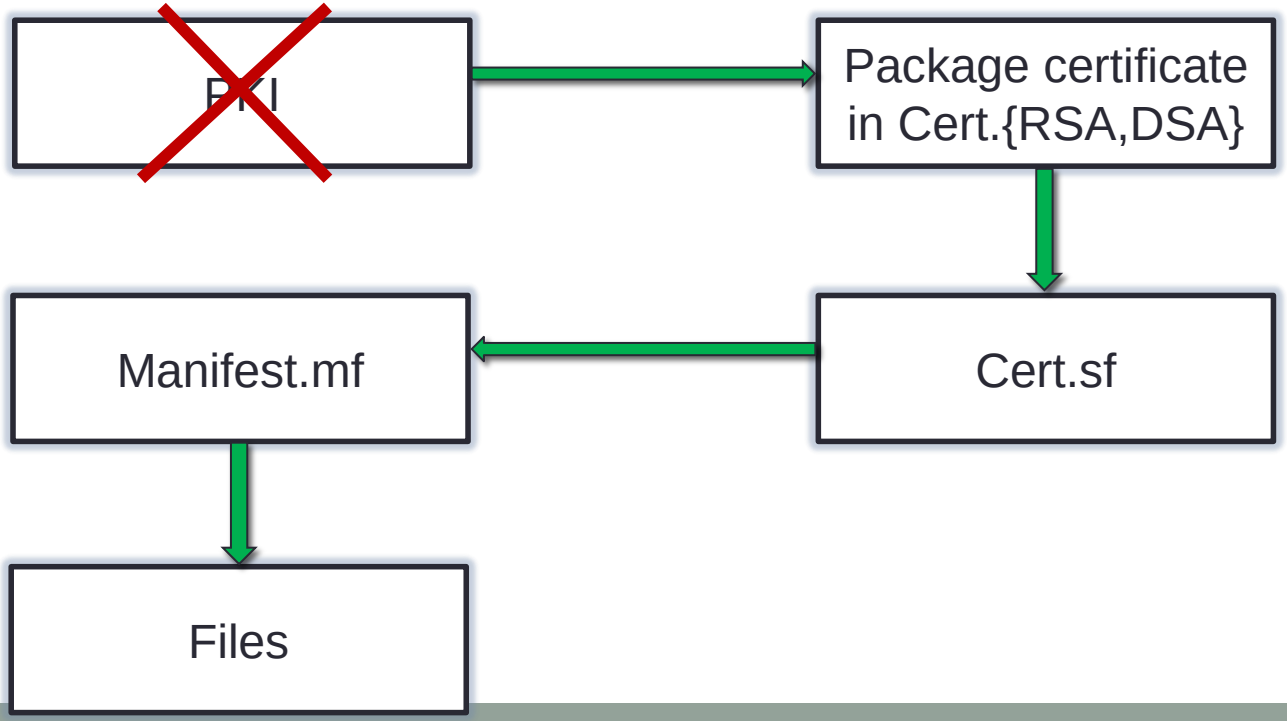
Package Integrity: Package Manifest

- Created with **jarsigner**
- META-INF
  - Manifest.mf, Cert.sf, Cert.{RSA,DSA}



Verifying of package manifest

Chain of trust:

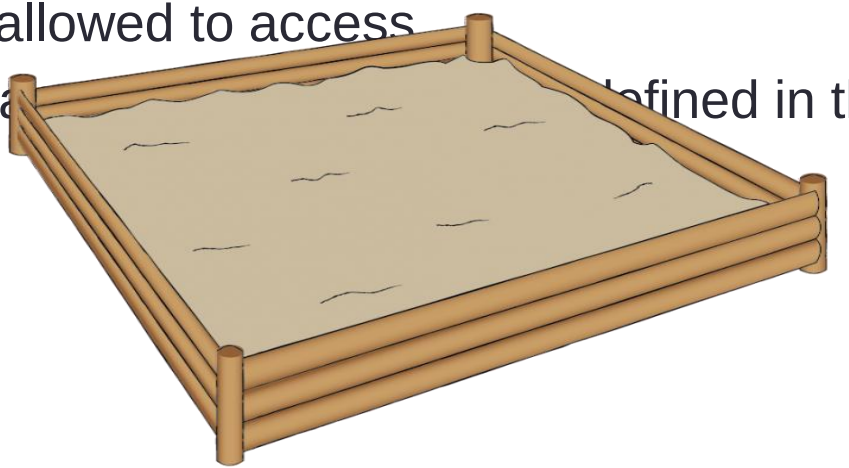


Android Security Architecture

- Package Integrity
- Sandboxing
- Permission and Least Privilege

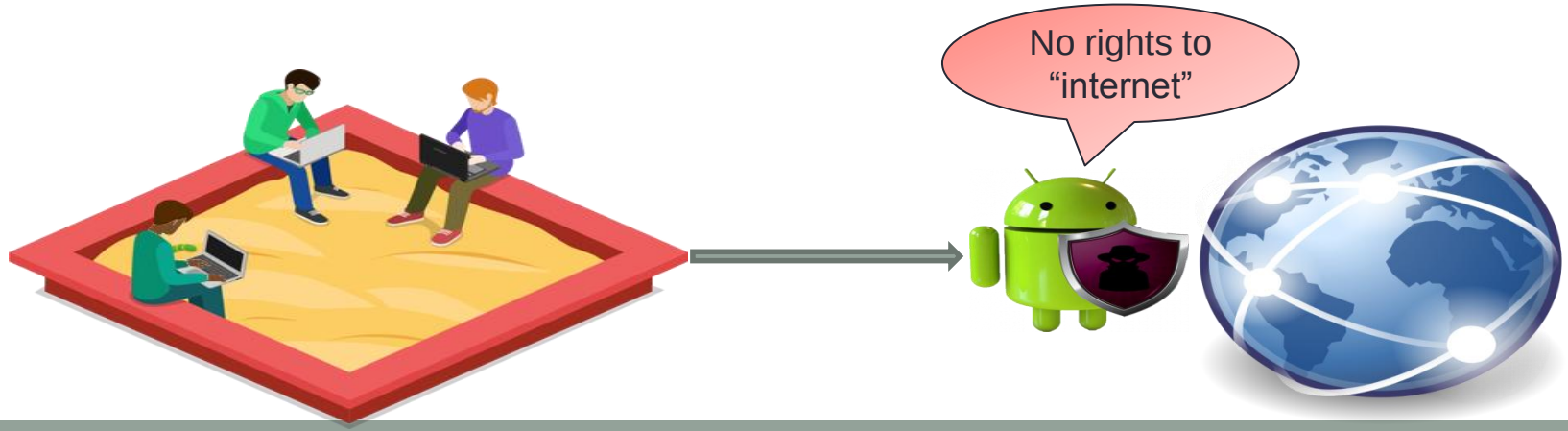
Sandboxing

- The application sandbox **specifies** which system **resources** the application is allowed to access
- An **attacker** ca[illegible]efined in the sandbox



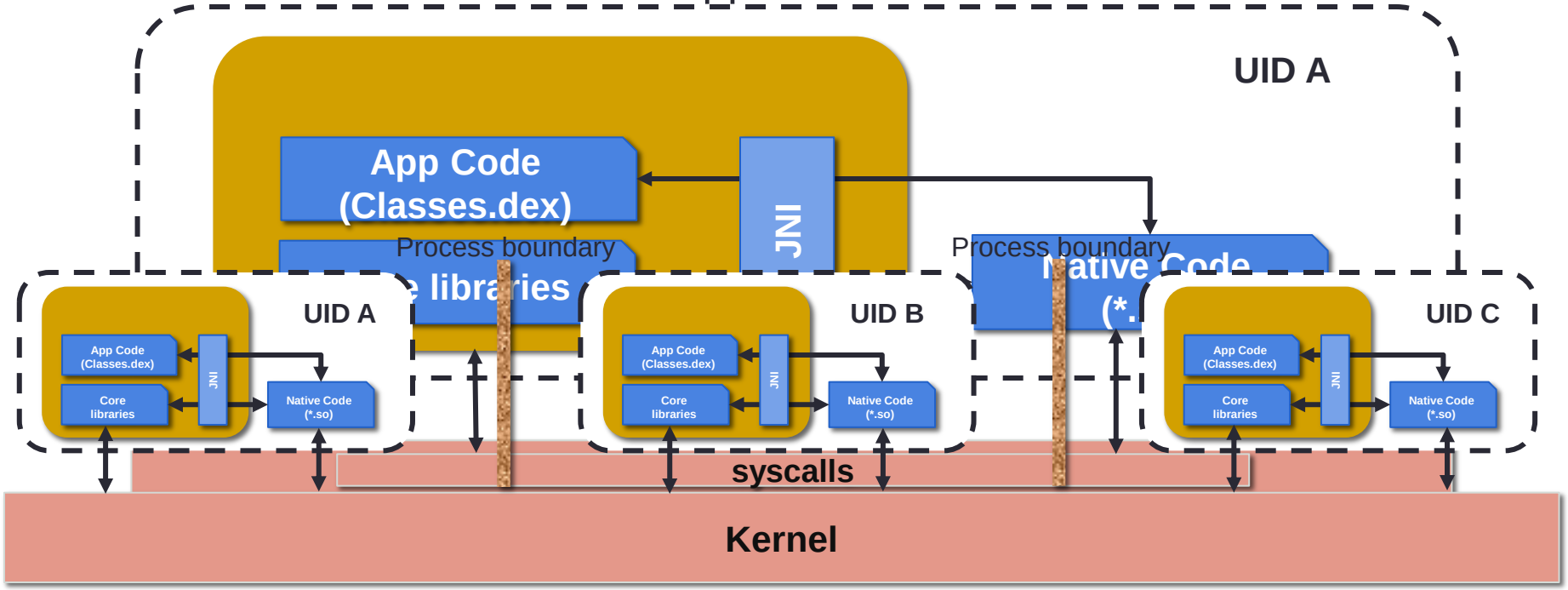
Application Isolation by Sandboxing

- Each Application is **isolated** in its own **environment**
  - **Applications** can access only its **own resources**
  - Access to **sensitive resources** depends on the **application's rights**
- **Sandboxing** is enforced by **Linux**



Application sandbox

- Isolation: Each installed App has



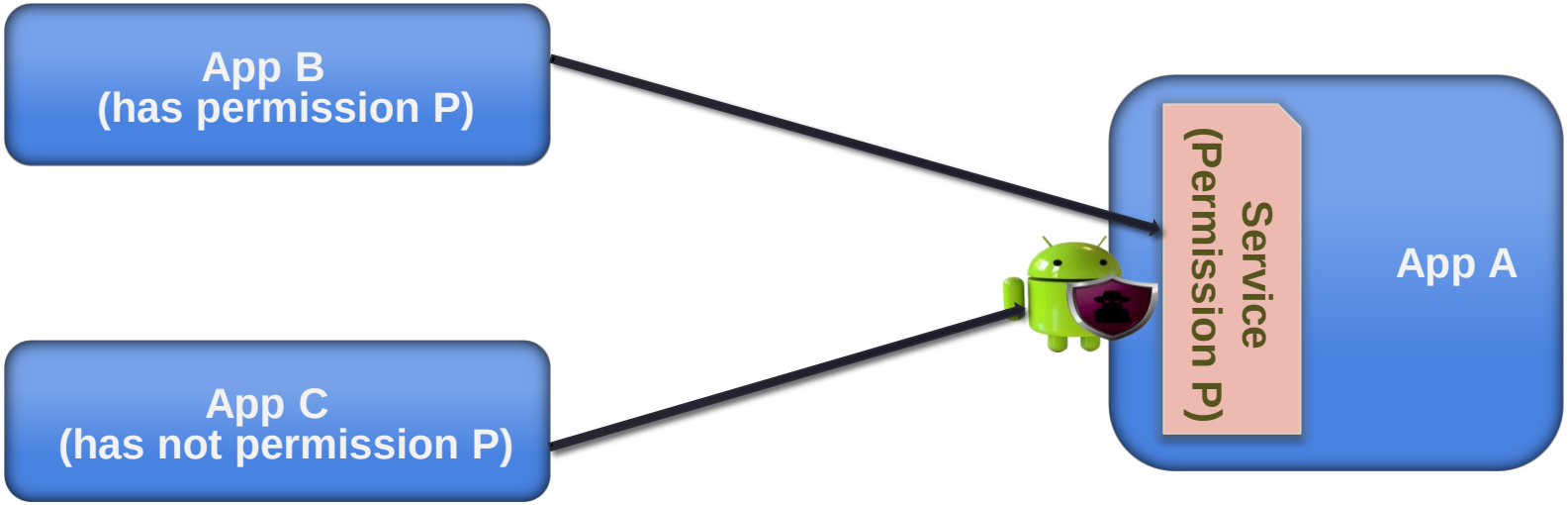
Android Security Architecture

- Package Integrity
- Sandboxing
- Permission and Least Privilege

Android Permission System

- **Access rights** in Android's application framework
  - Permissions are required to **gain** access to
    - System interfaces (Internet, send SMS, etc.)
    - System resources (logs, battery, etc.)
    - Sensitive data (SMS, contacts, etc.)
  - Currently more than 140 default permissions defined in Android
- Permissions are **assigned** to sandbox
- Application developers can also **define** their **own** permissions

Android Permission: Example

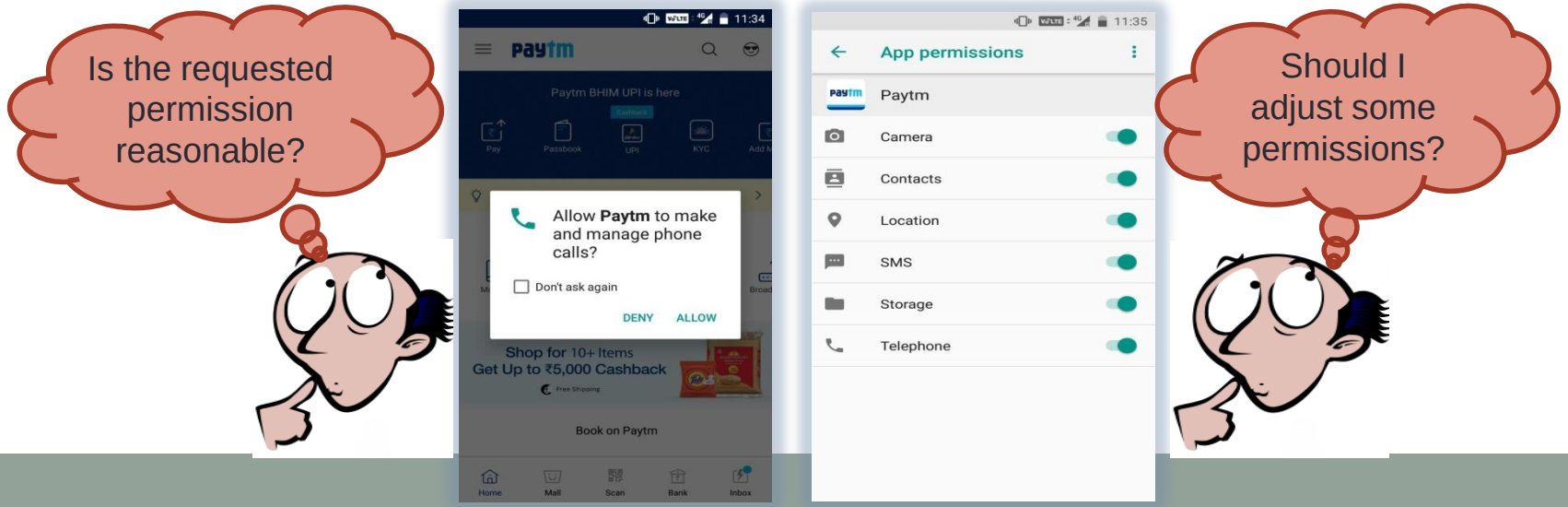


Permissions' Protection Level

- Normal
- Dangerous
- Signature
- SignatureOrSystem

Dynamic Permissions (≥ Android 6.0)

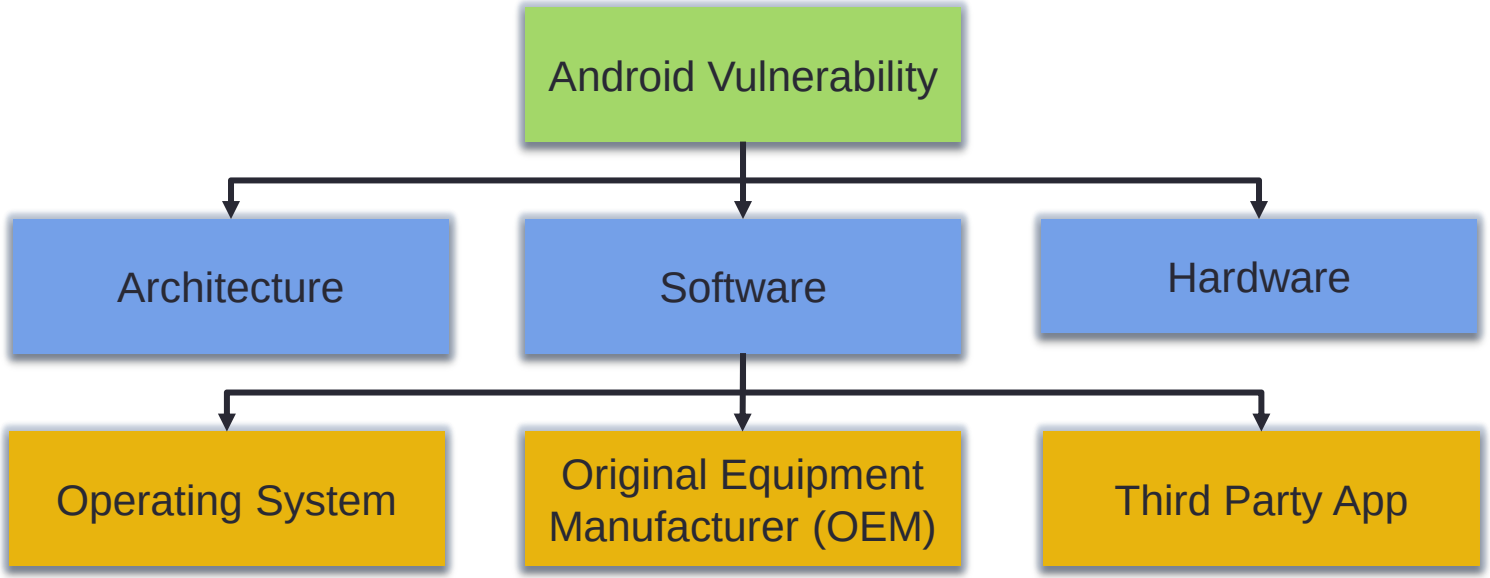
- App developers must **check** if their apps hold required **dangerous** permission, otherwise request them at runtime
- User can **grant** permissions at runtime and also **revoke** once granted permissions again



ANDROID VULNERABILITIES

- Architecture Based
- Software Based
- Hardware Based

Vulnerability Classification



ANDROID VULNERABILITIES

- Architecture Based
- Software Based
- Hardware Based

Application-Level Privilege Escalation Attacks

Malicious App

Confused Deputy App

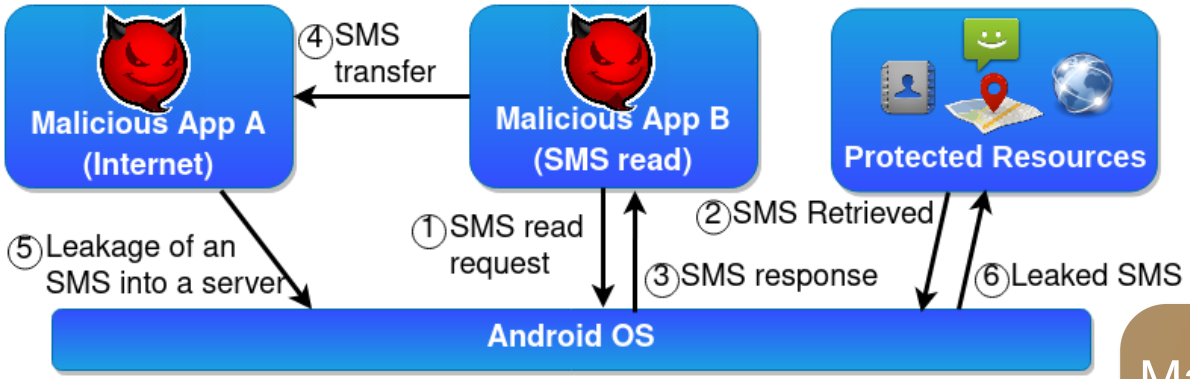
Confused Deputy Attack

Malicious App

Malicious App

Collusion Attack

Collusion Attack



Malicious apps **collude** in order to **merge** their respective **permissions**

- Variants:
  - Apps communicate directly
  - Apps communicate via covert channels in Android

ANDROID VULNERABILITIES

- Architecture Based
- Software Based
- Hardware Based

Dirty COW

- Existed in the Linux Kernel for **9 years**
- A **local** Privilege Escalation Vulnerability
- Exploits a race condition in the implementation of the **copy-on-write** mechanism
- Turns a **read-only** mapping of a file into a writable mapping


Android malware ZNIU exploits DirtyCOW vulnerability

29 SEP 2017 0

Android, Google, Malware, SophosLabs, Vulnerability

Source: https://nakedsecurity.sophos.com/2017/09/29/android-malware-zniu-exploits-dirtycow-vulnerability/

Media Projection Service Issue

Vulnerabilities

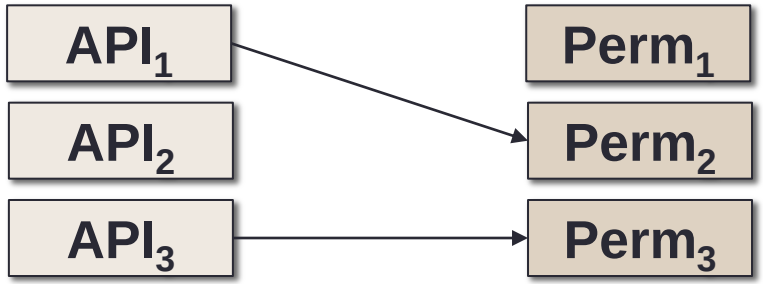
Android issue allows attackers to capture screen and record audio on 77% of all devices

November 20, 2017 Eslam Medhat 14 Views 0 Comments android, MediaProjection

Source: https://latesthackingnews.com/2017/11/20/android-issue-allows-attackers-to-capture-screen-and-record-audio-on-77-of-all-devices/

Over-privileged Apps

- Many apps request permissions that their **functionality** does not **require**
- Suspected root cause: API **documentation/naming** convention
  - Solution: API Permissions Maps
    - **Can be integrated into lint tools**



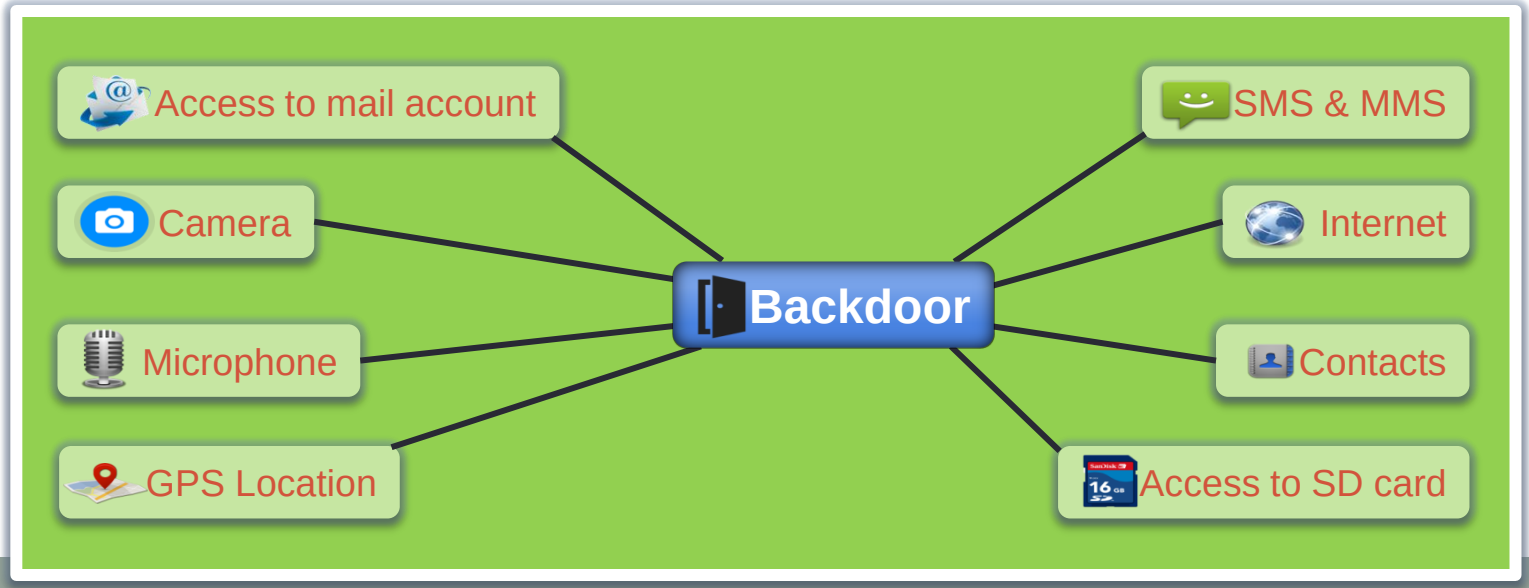
Confused Deputy Attack

- A privileged app is fooled into **misusing** its privileges on behalf of another (malicious) **unprivileged app**[1]

- Example:
  - **Unauthorized** phone calls[2]
  - Various confused deputies in **system apps**[3]

Confused Deputy Introduce by OEMs

- Several **confused deputies** found in Samsung devices' **firmware**
  - One deputy running with system privileges provided **root shell service** to any app



ANDROID VULNERABILITIES

- Architecture Based
- Software Based
- Hardware Based

Broadcom Wi-Fi SoC Flaw

BIZ & IT —

Android devices can be fatally hacked by malicious Wi-Fi networks

Broadcom chips allow rogue Wi-Fi signals to execute code of attacker's choosing.

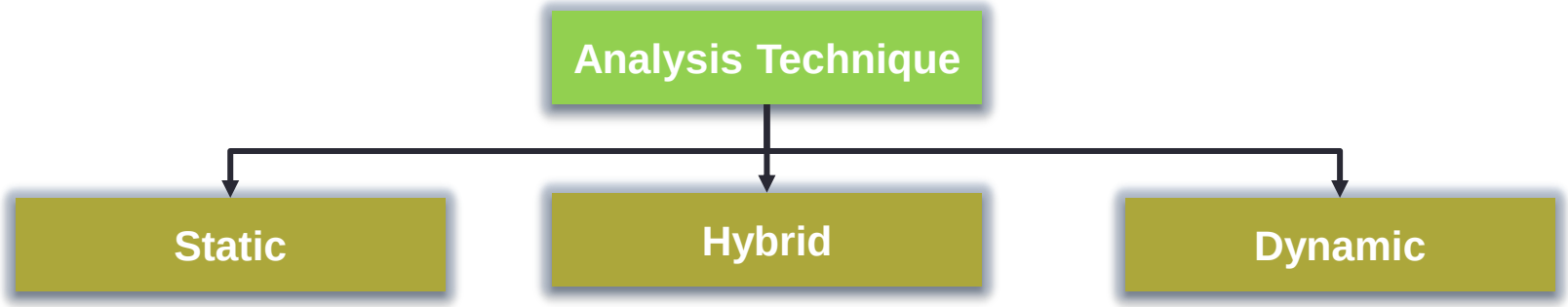
DAN GOODIN - 4/6/2017, 1:16 AM

Source: https://arstechnica.com/information-technology/2017/04/wide-range-of-android-phones-vulnerable-to-device-hijacks-over-wi-fi/

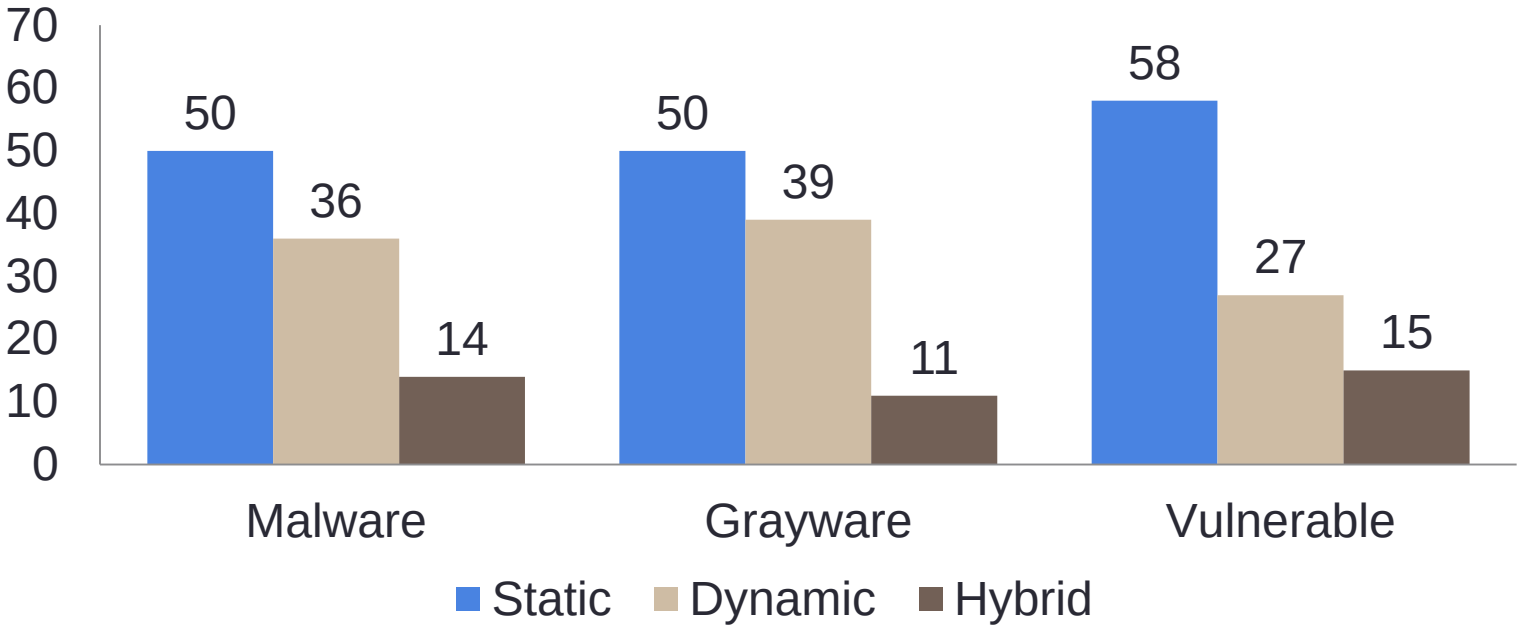
APPLICATION ANALYSIS

- Analysis Techniques and its Limitations

Analysis Techniques



Analysis Techniques used in Different Area



Static Analysis

- Analyze application without executing
- Profiling an App is faster
- Can be bypassed through
  - code obfuscation, dynamic code loading, packed code
- Tools:
  - Dex2Jar
  - APKTool
  - Androguard
  - FlowDroid

Dynamic Analysis

- Run applications on an Emulator
- Observe the behavior of an App
- Challenge:
  - Platform sensing App can evade dynamic analysis

Android Emulator

- A virtual mobile device
- Use Case:
  - Prototype, develop and test an application
  - Dynamic Analysis of malware
    - Used by security companies

Emulation-Detection

Detection Categories	Description
Unique device information (basic)	Detection by observing unrealistic device information values (e.g., IMEI value is 00000)
Unique device information (smart)	Detection based on fixed reading of unique device information (e.g., IMEI value is constant)
Sensors reading	Absence of sensor or observing static values from fluctuating sensors
GPS information	No change on GPS location data or fake location change
Device State information	No change to the device state w.r.t. telephony signal, battery power.
Distributed detection	Observing identical unique information for multiple devices in a network.

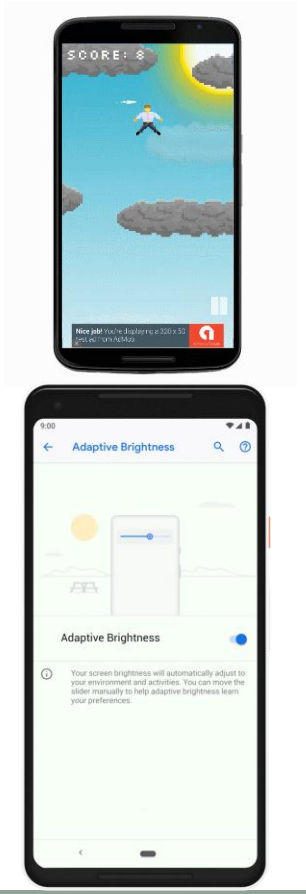
Unique Device Information

- Basic
  - Unrealistic/null value for IMEI, Phone No. etc.
- Smart
  - Realistic but fixed values

	IMEI	Phone No.	ICCID
	123456789012347	90139442364	89914105611117910720
	null/00000000000	15555215554	89014103211118510720
cuckoo DROiD	351451208401216	97259916243	89963040082067415160
cuckoo DROiD	351451208401216	97259916243	89963040082067415160

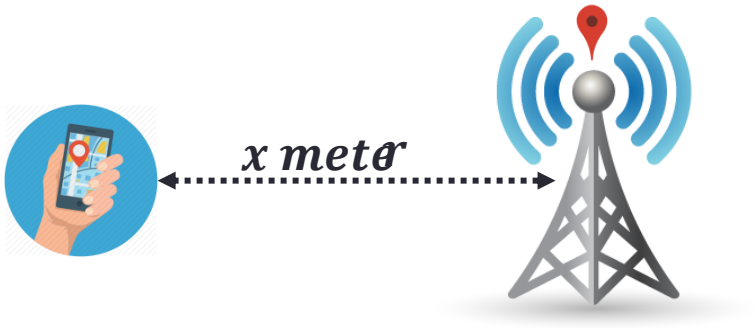
Sensors

- Different sensors in a smart phone
  - Motion Sensors: accelerometer, gyroscope
  - Environmental Sensors: illumination (light), humidity
- Detection:
  - Count: At least 6-7 or more sensors in a smartphone
  - Reading: No change in sensors reading



GPS Information

- No change in GPS location
- Use of mock location API to provide fake location
- No correlation with BTS geo-location



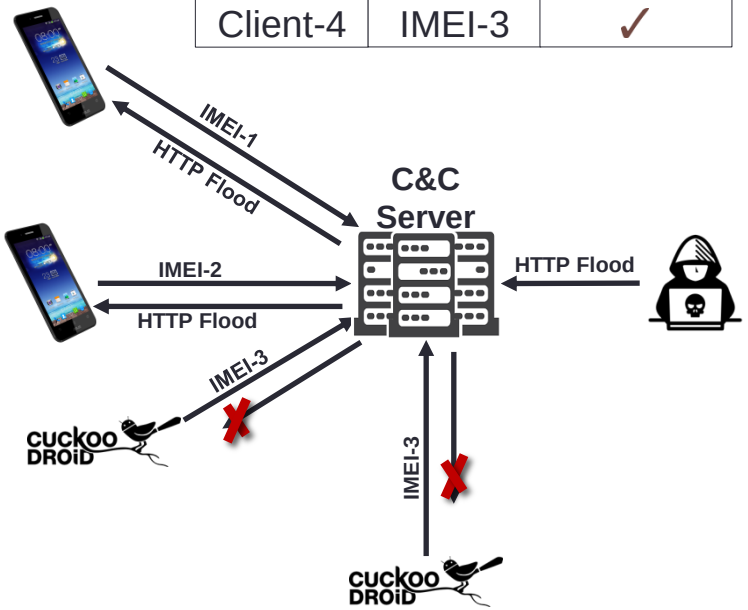
Device State Information

- Smartphone state may change due to:
  - Battery power
  - Signal Strength
  - SMS
  - Call
- No state change in emulated platform

Distributed Detection

- Detection on server
  - App communicates with server
  - Observing identical information for multiple device like IMEI
- Example:
  - Botnet analysis

Client No.	IMEI	Emulated?
Client-1	IMEI-1	✗
Client-2	IMEI-2	✗
Client-3	IMEI-3	✗
Client-4	IMEI-3	✓



Existing Frameworks Evaluation

Detection Type	Sub-type	Emulator	DroidBox	CuckooDroid	MobSF
Unique Device Information	Basic	✓	✗	✗	✗
	Smart	✓	✓	✓	✓
Sensors	Count	✗	✗	✗	✓
	Reading	✓	✓	✓	✓
Device State	--	✓	✓	✓	✓
GPS	Cond (i) (Normal)	✓	✓	✓	✓
	Cond (i) (Fake)	✗	✗	✗	✗
	Cond (i) & (ii)	✓	✓	✓	✓
	Cond (i) & (iii)	✓	✓	✓	✓
Distributed (Server config)	No Emulation	✗	✗	✗	✗
	W/- Emulation	✓	✓	✓	✓

Summary: Emulation Detection

- Existing framework fails to defend against detection method:
  - Smart unique device information
  - Sensors and GPS information
  - Device state
  - Distributed detection

- Need a robust anti-emulation-detection system:
  - Hides underline emulated platform
  - Remain undetected when attack is performed from any layer

https://github.com/skmtr1/FDP-Mobile-Forensics

Questions..

Thank You