Motivation

Mobile Security 2023

Florian Draschbacher
florian.draschbacher@iaik.tugraz.at

Some slides based on material by **Johannes Feichtner**

Smartphones – History

Once upon a time...

- PDA combined with a phone (starting in the late 90ies)
- IBM Simon (1994)
  - Touch Screen, Phone, Fax, E-Mail
- Nokia Communicator (1996)
  - Internet, Calendar, E-Mail, Business Apps
- Windows Mobile (2000)

Image: GR8Ausar / CC-BY-SA

Early Smartphones

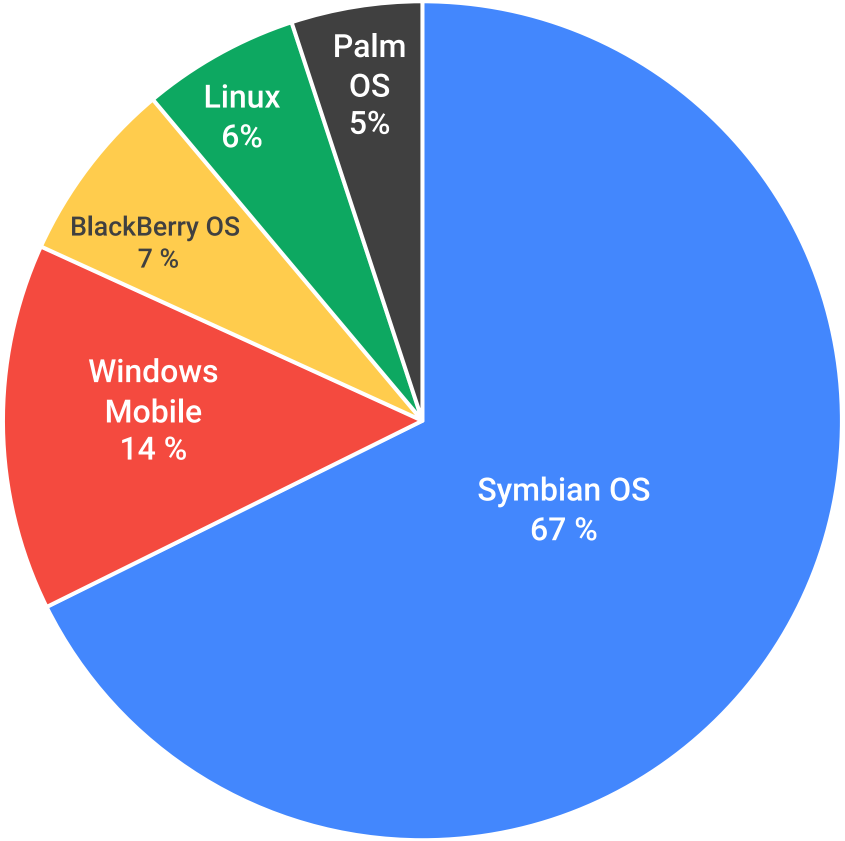
- Niche products for business use
  - Expensive
  - Impractical
  - Limited set of 3rd-party applications

- Very limited security
  - Hardware and OS often lacked basic security functionality
  - IBM Simon: No virtual memory
  - Windows Mobile: No file permissions, no real process isolation

Smartphone Trends By 2006

- Code Signing and User-grantable Permissions
  - Symbian OS, BlackBerry OS
- Linux kernel and custom Java VM
  - Nokia Maemo platform
  - Motorola EZX platform
- Smartphones try to enter consumer market

Market Share by OS



Source: canalys.com

IAIK TU Graz

2007: The iPhone

- First smartphone fully targeted at consumer market
- Novel capacitive touchscreen UI
  - Pencil-free on-screen keyboard
- ”Full-featured” web browser
- Key to emergence of app industry
  - Only web apps in iPhone 1.0
  - Only code-signed native apps later

Image: Flickr: Partyzan_XXI / CC-BY-SA

2008: First Android-based smartphone

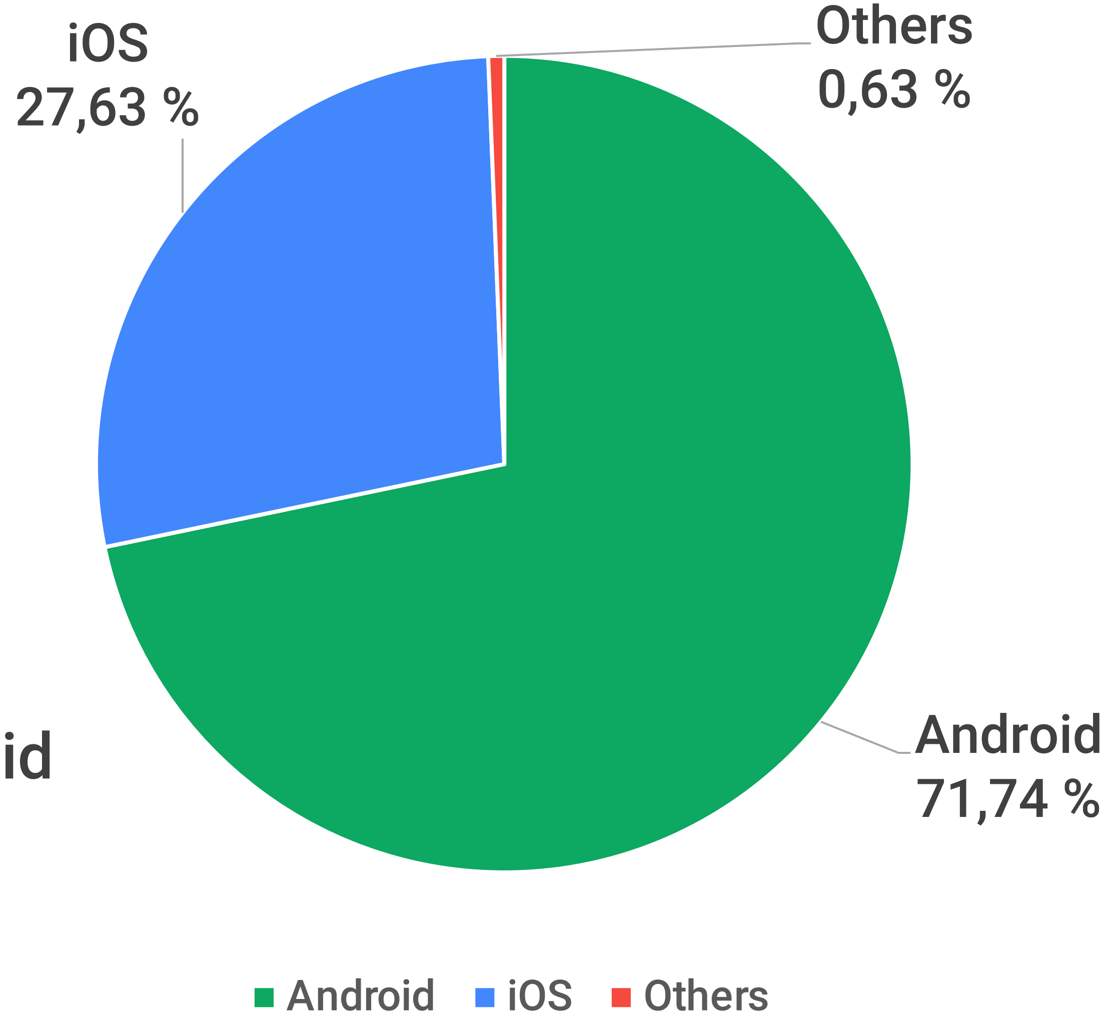
- Startup founded in 2003
  - Goal: Develop OS for smarter mobile devices
  - Competitor to Symbian and Windows Mobile
- 2005: Sold to Google
  - Shipped on devices of Open Handset Alliance
- 2007: Radical shift after introduction of iPhone
  - Focus on touchscreen devices

ANDROID

Image: Flickr: Michael Oryl/ CC-BY-SA

Today

- Android most popular OS
  - Even when compared to desktops
- Smartphones used by 6.6B people
  - More than 80% of world's population!
- Account for 59% of Internet traffic
- More than 4 million apps for iOS & Android
  - 255B downloads per year
  - Industry of hundreds of billions of $



Sources: statcounter.com; statista.com; Data from 2022,

Applications

- Social networks: Twitter, Facebook, Instagram, Snapchat, …
  - Contact data, Internet, Camera, Location (Network + GPS)
- Games: Online, multi-player, huge market
  - Internet, advertisements (Internet, Location, IDs), accelerometers, gyroscope
- Navigation: Hiking, biking, cities, maritime, aviation
  - Your location, „where are my friends?“

Applications

- Business: e-mail, calendar, container apps
  - Access to critical data, e-mails (!), company infrastructure

- Augmented reality: Navigation, games, peaks, …
  - Camera, Compass, Orientation, Internet

- Banking: Online Banking, Mobile Payment
  - PIN / TAN entry, access to Secure Elements
  - Two-factor authentication tends to happen on one device…

Applications

- Security software: Virus scanners, remote wipe / access
  - Access everything, sometimes rooted (Android) or with jail-break (iOS)

- Shopping: Amazon, Willhaben, AliExpress
  - Account information, credit card data, purchase history

- Personal data manager: Google Keep, Photos → Cloud, Password Managers
  - Handling sensitive data
  - User does not know / understand what happens behind the scenes

Everything turns smart

- iOS was the first in a family of related mobile OSs
  - watchOS, tvOS, audioOS
- Android is everywhere
  - Android TV, Wear OS, Home appliances, …
- Emerging market of embedded, connected, smart devices
  - Similarities to smartphones
  - Internet of Things

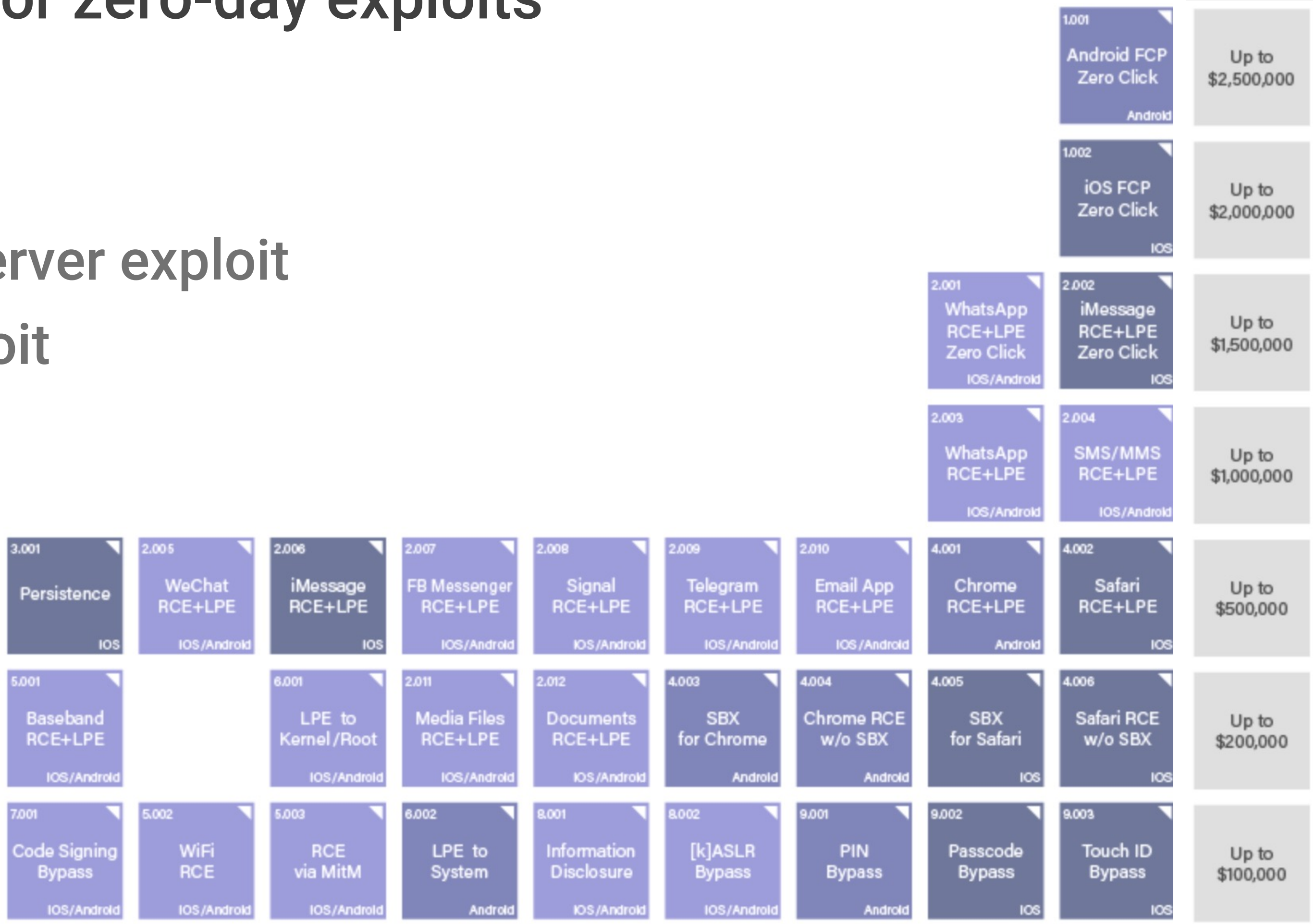
Image: Screenshot, apple.com

Image: lametric.com

Threats

Mobile Devices Attract Attackers

- There is an industry and market for zero-day exploits
- Zerodium:
  - Up to $1,000,000 for desktop / server exploit
  - Up to $2,500,000 for mobile exploit
- Apple:
  - Up to $2,000,000 Source: apple.com
- Google:
  - Up to $1,000,000 Source: google.com
- Microsoft:
  - Up to $200,000 Source: microsoft.com



								1.001 Android FCP Zero Click Android	Up to $2,500,000
								1.002 iOS FCP Zero Click iOS	Up to $2,000,000
							2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS	Up to $1,500,000
							2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android	Up to $1,000,000
3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS	Up to $500,000
5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS	Up to $200,000
7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS	Up to $100,000

Source: zerodium.com

Why Are Mobile Devices Interesting to Attackers?

- High density of sensitive data
  - “Many valuable assets”
- High degree of connectedness
  - “Large attack surface”
- Unique challenges
  - Security vs. Usability
  - Security vs. Innovation
  - Security vs. Customization

Pictures: Google / Apache 2.0

Assets on Mobile Devices

Attackers are aiming at…

- Data (Confidentiality)
  - Personal Data: Pictures, Messages, Files, Browsing History, …
  - Sensor Data: GPS, Microphone, Camera, Accelerometer, …
  - Authentication Data: Passwords, Credentials, Bank Accounts, Car Keys, …
- Availability
  - What if you cannot call emergency when you need it
- Device Resources
  - CPU power, Display space, Network access, …

Attack Surface: Cellular

- Many standards: GPRS/GSM has many security problems
  - A5/0: broken (and partly banned)
  - A5/1: broken using rainbow tables in 2009
  - A5/2: export version, broken in 1999
  - A5/3: Backport of Kasumi UMTS cipher

https://gsmmap.org

- Security is deployed on higher levels (VPNs, HTTPS, etc)

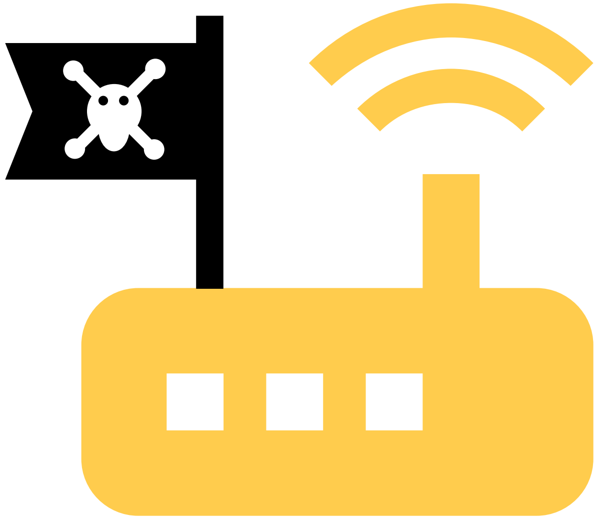
- However:
  - 2G still widely available, particularly in Europe
  - Telephone, SMS, MMS services integrated as apps into phone
  - MMS with Malware, e.g. „Stagefright“ on Android

Attack Surface: WiFi

- Huge problem: Open WiFi access points

- Old problems re-emerge:
  - ARP Poisoning
  - Sniffing unencrypted traffic
  - Phishing
  - Faking DNS entries
  - Faking TLS certificates (MITM → HTTPS)

Tools:
- Intercepter-NG
- Aircrack-ng
- …



Picture: Google / Apache 2.0

Attack Surface: WiFi

- Problems also in the protocol itself
  - Design and Implementation

- 2017: KRACK
  - Key Reinstallation Attack effectively allowed bypassing WPA2 encryption

- 2019: KR00K
  - Newer variation of KRACK

- 2021: FragAttacks
  - Inject WiFi frames into WPA3 protected network
  - Allows e.g. to enforce malicious DNS server

Attack Surface: WiFi

- Interesting demo by Ian Beer of Google's Project Zero
  - AWDL Proximity exploit

- AWDL: Apple Wireless Direct Link
  - Ad-hoc WiFi protocol underlying AirDrop, AirPlay, CarPlay, Handoff, Quickstart, …

- iOS kernel driver contained double-free in frame parsing
  - Can be exploited over the air!

- Enables kernel read and write, which allows infiltrating any app process

Attack Surface: WiFi

AWDL Proximity exploit

Source:
https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html

Attack Surface: Bluetooth

Problems by design

- Visibility
- Pairing

Problems by implementation

- BrakTooth (2021): DoS or code execution on 1400 chipsets Source: asset-group.github.io
  - Family of vulnerabilities in Bluetooth Classic Controllers
  - All running the same vulnerable firmware
- SweynTooth (2020): DoS, code execution or security bypass Source: asset-group.github.io
  - Family of vulnerabilities in Bluetooth LE SDKs of multiple SoC vendors
- Attackers just need to be in radio range
- Highlight flaws in the Bluetooth Stack Certification Process

Attack Surface: NFC

- Near Field Communication (NFC)
  - Short range (freq. 13.56 MHz) → some kind of security
  - Payments, Social Networking, Access tokens, …

Picture: mirrorsnake / CC BY-SA

- Devices can act as both reader and tag

- 2022: MitM attack against Apple Pay Source: practical_emv.gitlab.io
  - Payments without user authorization

- 2019: Flaw in Android Beam Source: trendmicro.com
  - Allows installing apps through NFC (install dialog has to be confirmed though)

Attack Surface: USB

- Most modern smartphones can act as USB host and client / accessory

- iOS
  - Proprietary protocols for Network, Audio, Screen Sharing via USB (Largely undocumented)
  - iOS Accessory Protocol (Licensable)
  - Debugging and management via ***usbmuxd*** and ***lockdownd*** (Reverse-Engineered by libimobiledevice)

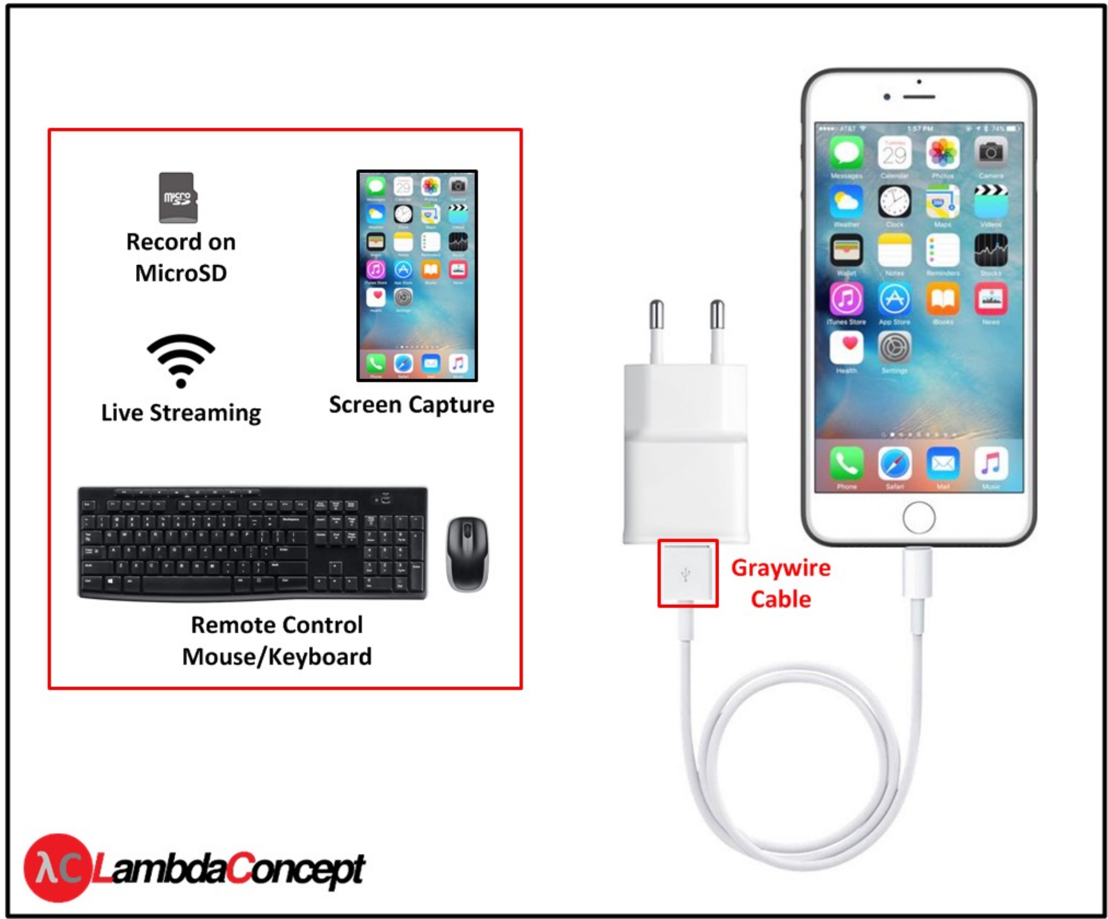
- Android
  - Class-compliant Network, Audio implementations
  - Open Accessory Protocols for Audio and custom functionality
  - Debugging and socket muxing via ***Android Debug Bridge*** (ADB)

Attack Surface: USB

- Juice-jacking attacks
  - Seemingly harmless charging cable
  - Actually acts as an accessory or computer to the smartphone

- Early attacks:
  - Extract files from the device
  - Install apps

- Still partly possible on modern OS:
  - Record screen contents
  - Intercept Internet connection
  - Extract Wifi credentials



Source: http://blog.lambdaconcept.com/post/2019-09/graywire/

Attack Surface: USB

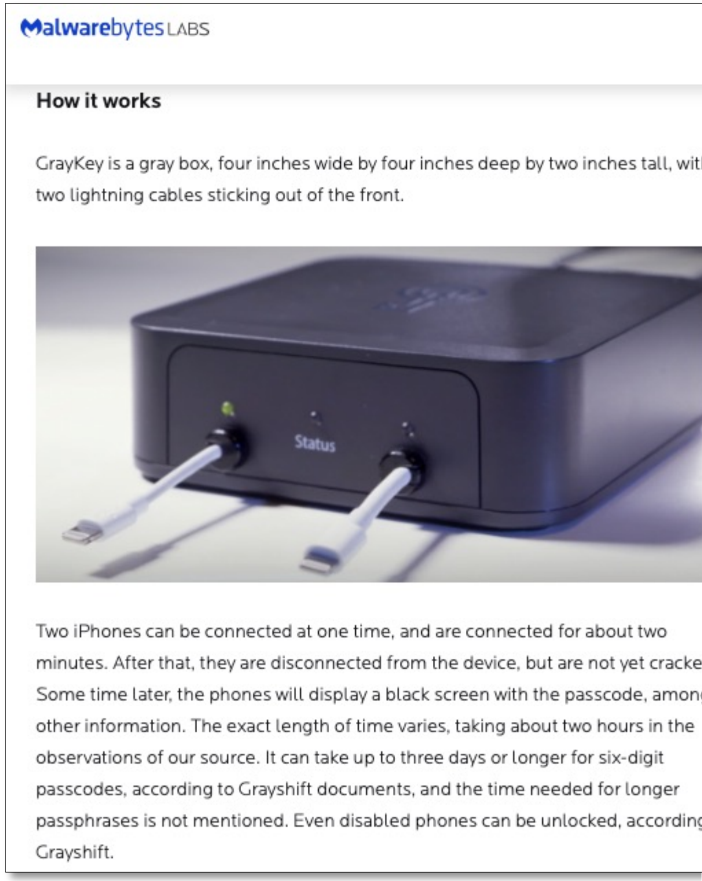
- USB Debugging Interfaces pose Security Risk: *“JuiceJacking”*

- 2012/2013: Android 4.2.2 / iOS 7 add user consent for debug connection Sources: cs.android.com / theta44.org

- 2017: GrayKey Box
  - Brute-force pin and extract data from locked iOS device

- 2018: iOS 12 locks USB 1 hour after screen lock

- Today: O.MG Cable
  - Computer hidden in charging cable
  - Keystroke injection via WiFi connection



Malwarebytes LABS

How it works

GrayKey is a gray box, four inches wide by four inches deep by two inches tall, wit two lightning cables sticking out of the front.

Two iPhones can be connected at one time, and are connected for about two minutes. After that, they are disconnected from the device, but are not yet cracke Some time later, the phones will display a black screen with the passcode, amon other information. The exact length of time varies, taking about two hours in the observations of our source. It can take up to three days or longer for six-digit passcodes, according to Grayshift documents, and the time needed for longer passphrases is not mentioned. Even disabled phones can be unlocked, according Grayshift.

Source: malwarebytes.com

Attack Surface: USB

- Multiple iOS Jailbreaks were made possible by exploits of USB vulnerabilities

- Checkrain jailbreak / Checkm8 exploit (2019):
  - Use-after-free in USB code Source: habr.com
  - Same code in iOS and BootROM

- evasi0n jailbreak (2013):
  - Insufficient pointer validation in `IOUSBDeviceFamily` driver Source: azimuthsecurity.com

Attack Surface: Internet Connection

- A considerable portion of apps misconfigure TLS
  - Trust any server certificate
  - Don’t check certificate subject

- Consequence:
  - MITM attacks may extract e.g. credentials, credit card data, …

- Additionally: Most apps do not use certificate pinning
  - State-scale actors may still intercept traffic!

Attack Surface: Location

Finding a GPS fix can take a long time…

→ *Solution: Assisted GPS (A-GPS)*

- Send coarse location + IMSI to SUPL server
  - *„Secure User Plane Location Protocol“*
- SUPL server depends on device

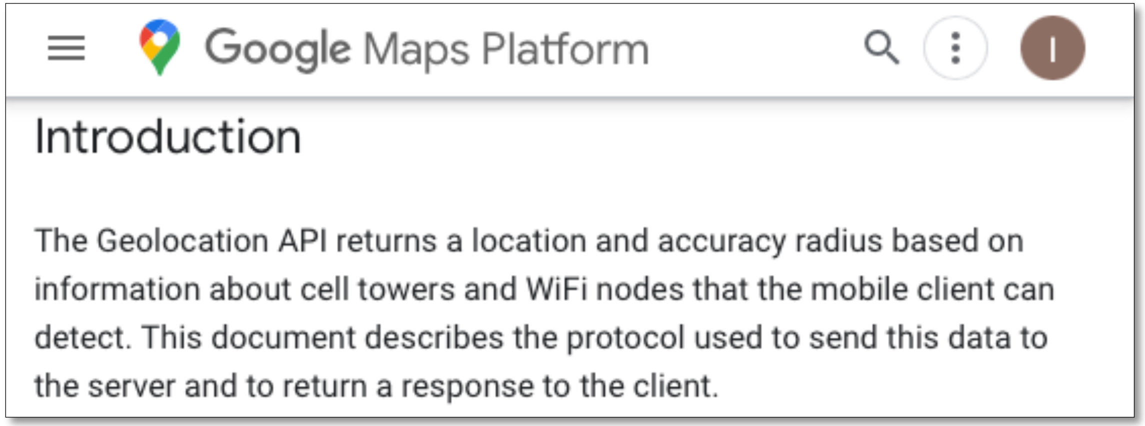
```
cat /etc/system/gps.conf | grep SUPL_HOST (or /vendor/etc/gps.conf)
SUPL_HOST=supl.google.com # Google
SUPL_HOST=supl.sonyericsson.com # Sony
SUPL_HOST=supl.qxwz.com # China(?)
...
```

Good: TLS is used to protect transfer

Bad: The certificate's validity is not checked on some devices! Source: wirelessmoves.com

Attack Surface: Location

Google and others can locate you from connected WiFi nodes and cell towers



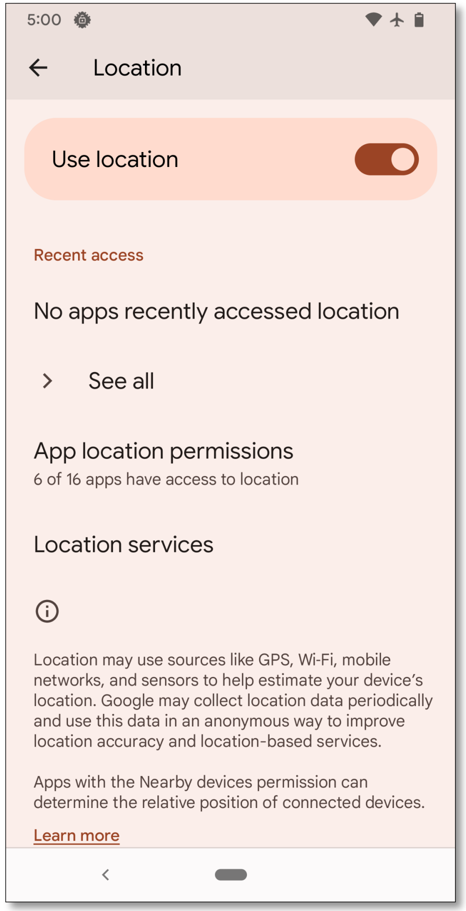
Introduction

The Geolocation API returns a location and accuracy radius based on information about cell towers and WiFi nodes that the mobile client can detect. This document describes the protocol used to send this data to the server and to return a response to the client.

Source: developers.google.com

How do they learn this mapping?

> “Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services”



Use location

Recent access

No apps recently accessed location

See all

App location permissions

6 of 16 apps have access to location

Location services

Location may use sources like GPS, Wi-Fi, mobile networks, and sensors to help estimate your device’s location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Apps with the Nearby devices permission can determine the relative position of connected devices.

Learn more

Attack Surface: Apps

Potentially malicious developers can get code execution and escalate from there

- Psychic Papers
  - iOS apps could get arbitrary entitlements due to XML parser bugs
- DirtyCOW
  - Linux race condition in COW that allows to gain temporary root access
- macDirtyCOW
  - Similar more recent vulnerability allows temporary system modification on iOS
- Cloak and Dagger
  - Android apps could control complete UI feedback loop to take over device

Additional Challenges

Smartphone - Threats

- Companies know much about PC security
  → *Can we apply this mobile devices / smartphones?*

Only in a very limited way!

- Many parts of Android and iOS were implemented specifically for them

- Only a handful of security experts on teams
  - No chance to ***review*** every single code line!
  - Help ***design*** features with security in mind

Smartphone - Challenges

- New technologies in combination with old ones
  - E.g. Linux as basis + key storage in hardware
- Mixed private / business use cases
  - How to separate these two spheres?
  - Limited administrative access to devices
- Legacy security strategies are ineffective
  - Innovation outpaces security practices
- Smartphones are every-day companions
  - Mobility poses risks

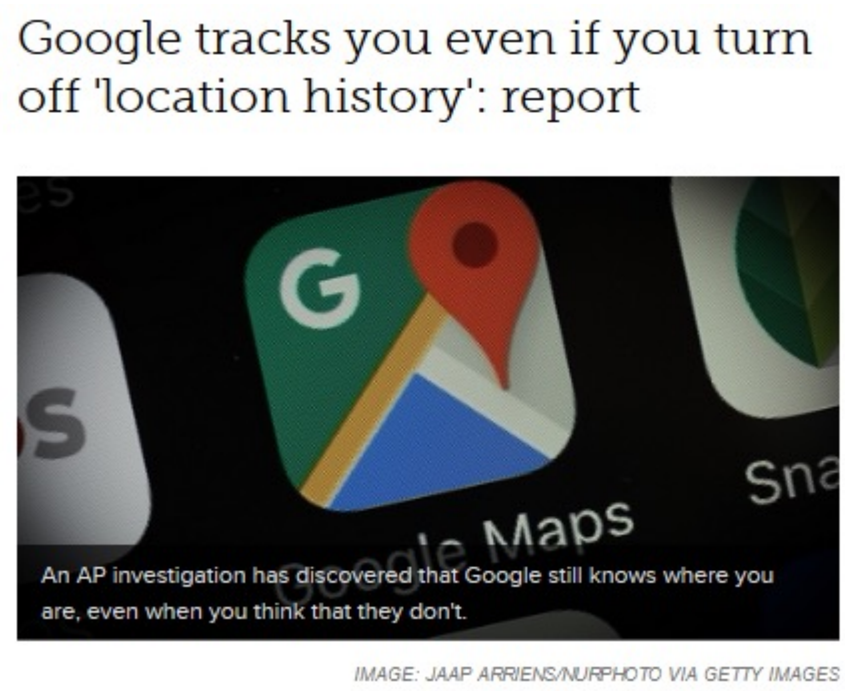
Data & Sensors

- Smartphone is taken everywhere
  - Collecting data even while not actively used

- Location
  - Network Cell ID (coarse)
  - GPS (fine)
    - Usually used with A-GPS for faster 3D fix

- Microphone, Motion Data, …
  - Ads may collect sensor data that leaks credit card info

    Source: Diamantaris et al., 2021



Google tracks you even if you turn off 'location history': report

An AP investigation has discovered that Google still knows where you are, even when you think that they don't.

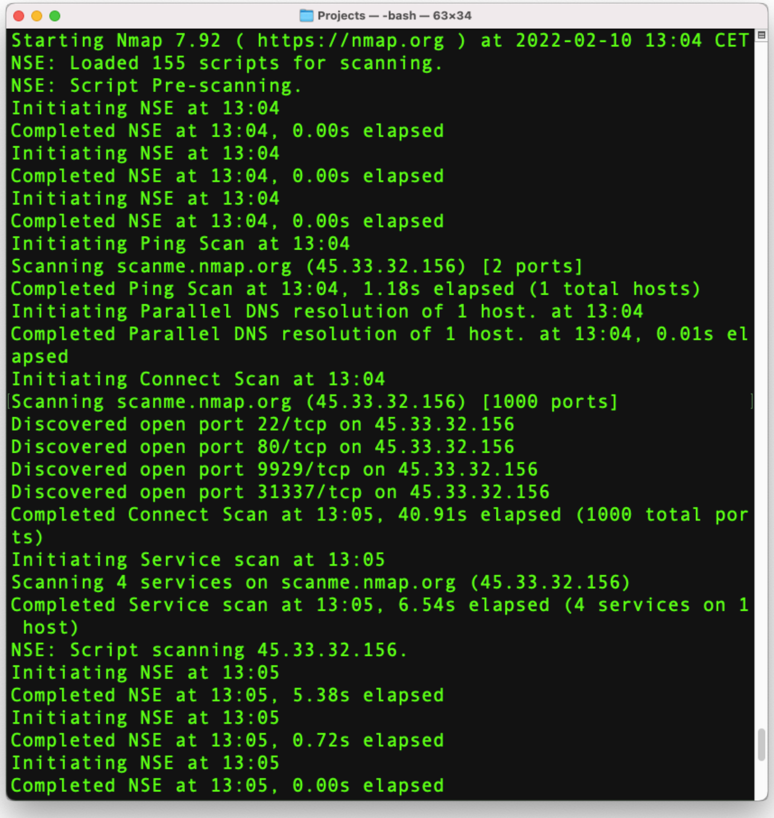
IMAGE: JAAP ARRIENS/NURPHOTO VIA GETTY IMAGES

Source: mashable.com

Mobility

- Install malware on smartphone on-the-fly
  - Steal it from a jacket, take it from a table, …

- Use it for attacks
  - Spy with its microphone, camera
  - Do ARP Spoofing / MITM in WiFis
  - Scan networks
  - Open a rogue access point



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-10 13:04 CET
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating Ping Scan at 13:04
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 13:04, 1.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.01s el
apsed
Initiating Connect Scan at 13:04
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 13:05, 40.91s elapsed (1000 total por
ts)
Initiating Service scan at 13:05
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:05, 6.54s elapsed (4 services on 1
 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 13:05
Completed NSE at 13:05, 5.38s elapsed
Initiating NSE at 13:05
Completed NSE at 13:05, 0.72s elapsed
Initiating NSE at 13:05
Completed NSE at 13:05, 0.00s elapsed
```

Business vs. Private Use

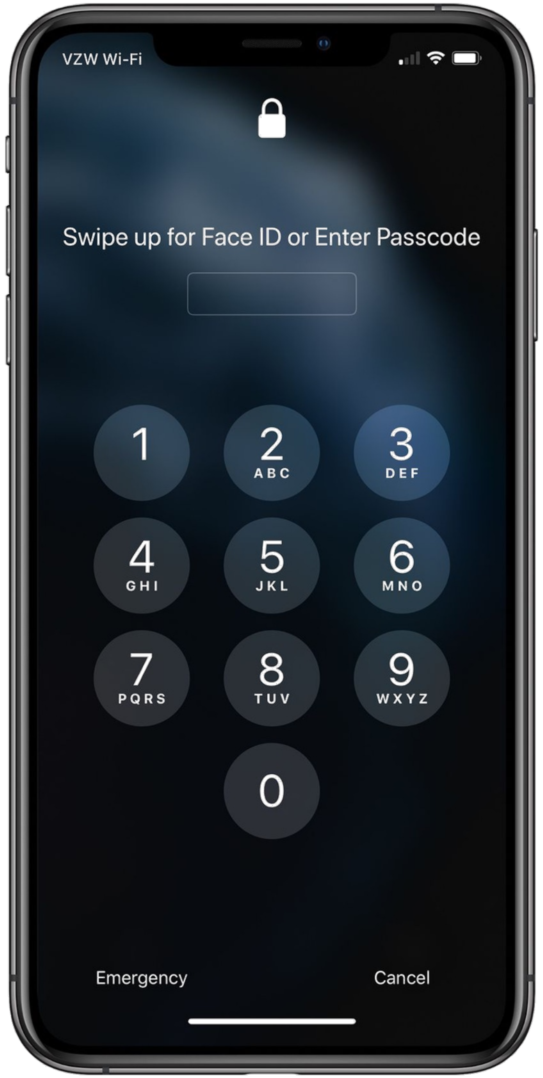
- Complete mixture of two areas
- Usually strict security policy for corporate apps
- No security policy for private apps on same device
  - Still effects on device‘s security
- BYOD – Bring your own device
  - Corporate apps on potentially insecure system

Pictures: Google / Apache 2.0

Security vs. Usability

Smart phones need to be easily approachable!

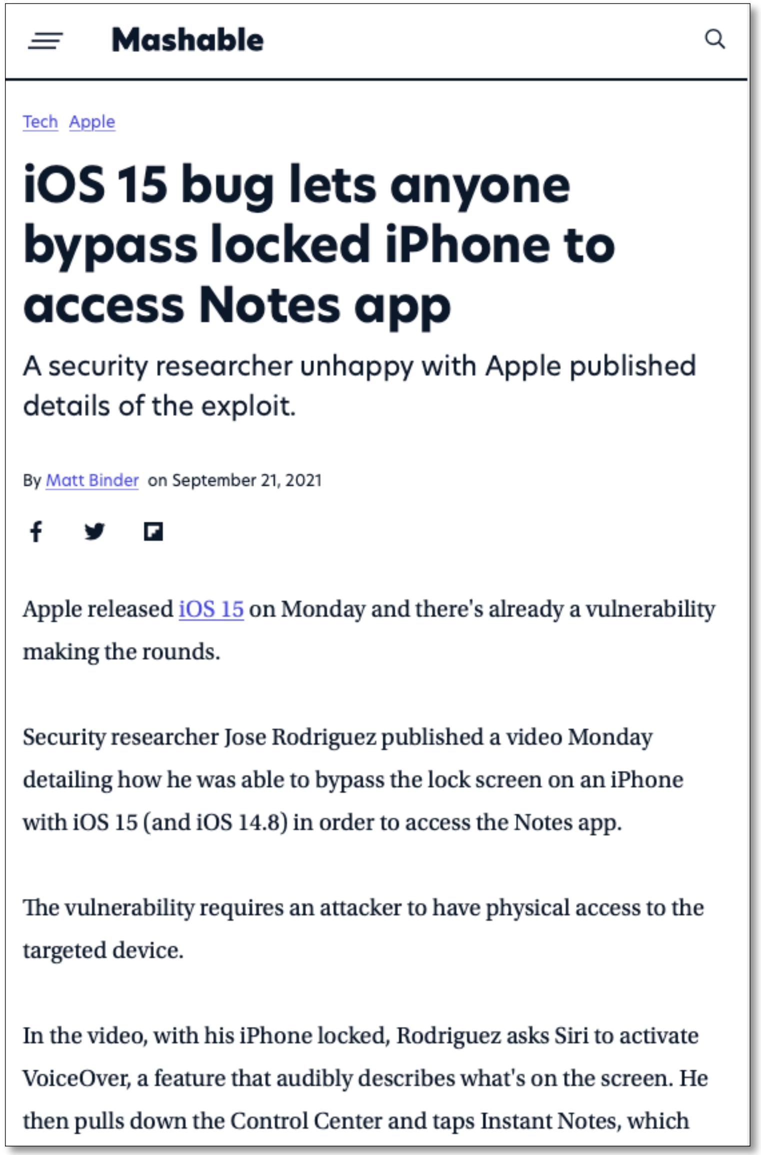
- PIN codes, short passwords, screen unlock patterns
- Two-Factor-Authentication on one device
- Take pictures without unlocking the device



Access Protection – PINs / Passwords

- PIN: Typically 4 digits, quite low entropy
- Passwords: No limits but usability?
- Patterns (Android):
  Nice but entropy? Looking over shoulder…
- Face ID / Unlock: Circumvent with photo?
- Fingerprints: TouchID with iOS 8, Android 6.0

Access Protection – PINs / Passwords



Mashable

Tech Apple

iOS 15 bug lets anyone bypass locked iPhone to access Notes app

A security researcher unhappy with Apple published details of the exploit.

By Matt Binder on September 21, 2021

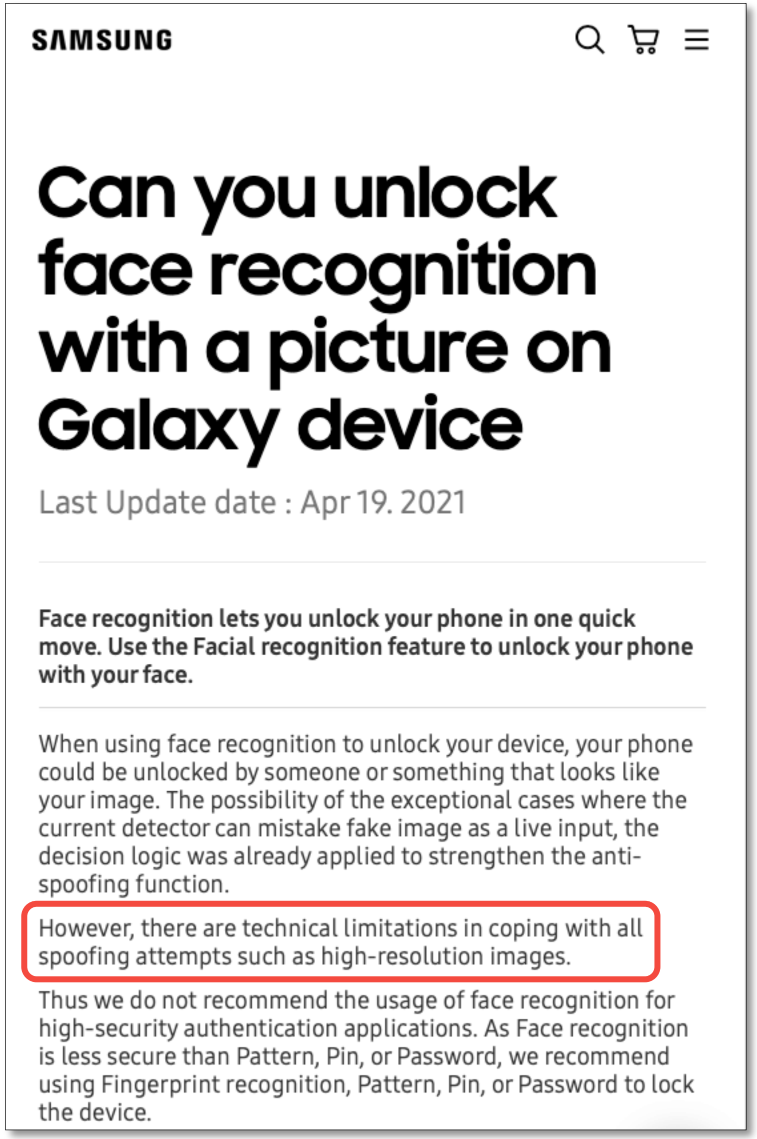
Apple released iOS 15 on Monday and there's already a vulnerability making the rounds.

Security researcher Jose Rodriguez published a video Monday detailing how he was able to bypass the lock screen on an iPhone with iOS 15 (and iOS 14.8) in order to access the Notes app.

The vulnerability requires an attacker to have physical access to the targeted device.

In the video, with his iPhone locked, Rodriguez asks Siri to activate VoiceOver, a feature that audibly describes what's on the screen. He then pulls down the Control Center and taps Instant Notes, which

Source: mashable.com



SAMSUNG

Can you unlock face recognition with a picture on Galaxy device

Last Update date : Apr 19. 2021

Face recognition lets you unlock your phone in one quick move. Use the Facial recognition feature to unlock your phone with your face.

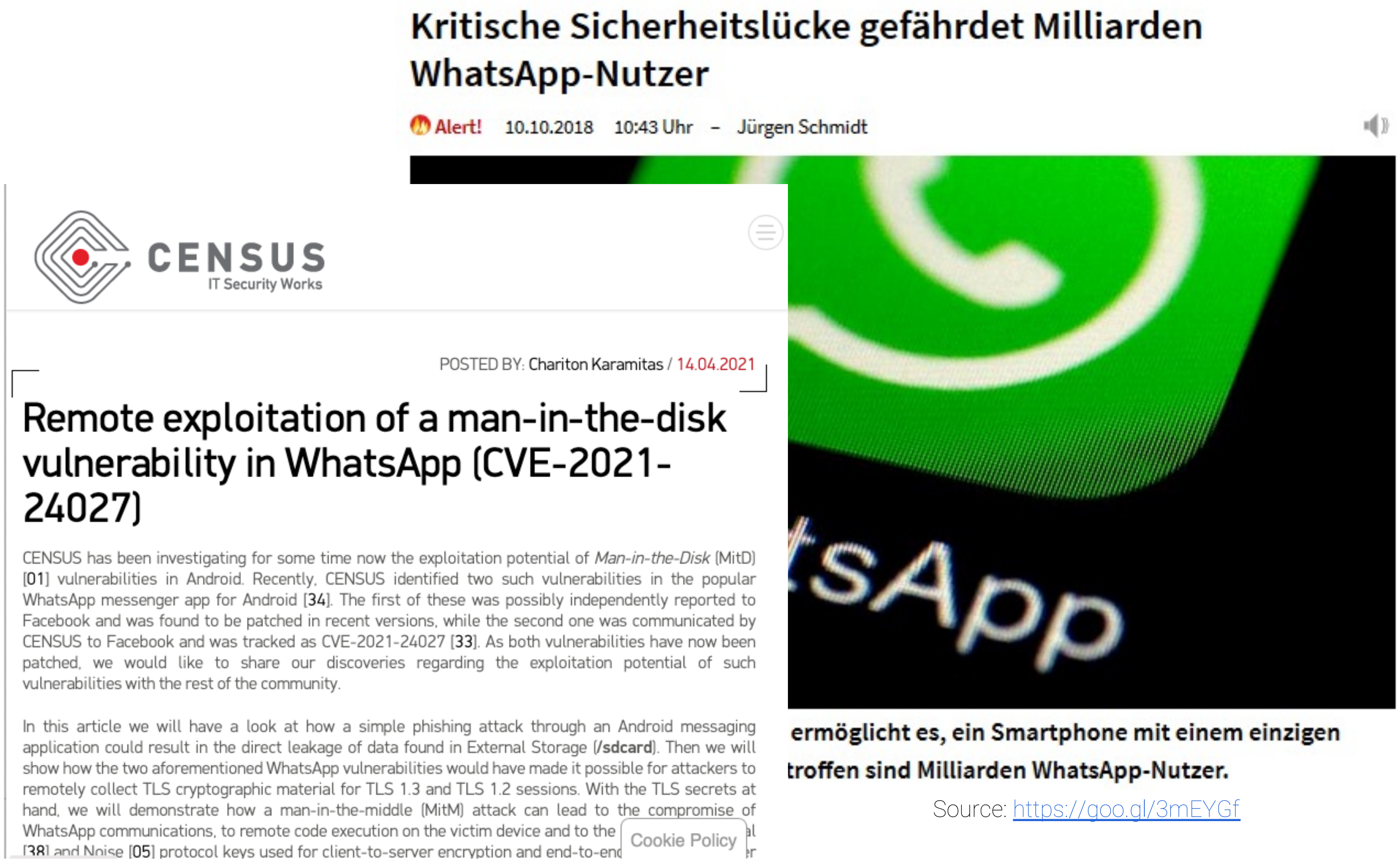
When using face recognition to unlock your device, your phone could be unlocked by someone or something that looks like your image. The possibility of the exceptional cases where the current detector can mistake fake image as a live input, the decision logic was already applied to strengthen the anti-spoofing function.

However, there are technical limitations in coping with all spoofing attempts such as high-resolution images.

Thus we do not recommend the usage of face recognition for high-security authentication applications. As Face recognition is less secure than Pattern, Pin, or Password, we recommend using Fingerprint recognition, Pattern, Pin, or Password to lock the device.

Source: samsung.com

Security vs. Efficiency



Kritische Sicherheitslücke gefährdet Milliarden WhatsApp-Nutzer

Alert! 10.10.2018 10:43 Uhr – Jürgen Schmidt

ermöglicht es, ein Smartphone mit einem einzigen
troffen sind Milliarden WhatsApp-Nutzer.

CENSUS
IT Security Works

POSTED BY: Chariton Karamitas / 14.04.2021

Remote exploitation of a man-in-the-disk vulnerability in WhatsApp (CVE-2021-24027)

CENSUS has been investigating for some time now the exploitation potential of *Man-in-the-Disk* (MitD) [01] vulnerabilities in Android. Recently, CENSUS identified two such vulnerabilities in the popular WhatsApp messenger app for Android [34]. The first of these was possibly independently reported to Facebook and was found to be patched in recent versions, while the second one was communicated by CENSUS to Facebook and was tracked as CVE-2021-24027 [33]. As both vulnerabilities have now been patched, we would like to share our discoveries regarding the exploitation potential of such vulnerabilities with the rest of the community.

In this article we will have a look at how a simple phishing attack through an Android messaging application could result in the direct leakage of data found in External Storage (**/sdcard**). Then we will show how the two aforementioned WhatsApp vulnerabilities would have made it possible for attackers to remotely collect TLS cryptographic material for TLS 1.3 and TLS 1.2 sessions. With the TLS secrets at hand, we will demonstrate how a man-in-the-middle (MitM) attack can lead to the compromise of WhatsApp communications, to remote code execution on the victim device and to the al [38] and Noise [05] protocol keys used for client-to-server encryption and end-to-end r

Cookie Policy

Source: census-labs.com

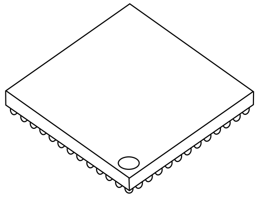
Source: https://goo.gl/3mEYGf

Security vs. Performance

Protecting data using encryption

→ Which scope? Whole storage or just certain data?

- Performance issue
  - Symmetric keys, often protected with asymmetric ones
- Where to store the keys?
  - **Nowhere!** → Derived from PIN / password!
  - Isolated Area → Device storage or Secure Element



Picture: ZyMOS / CC BY-SA

Mobile Device Management (MDM)

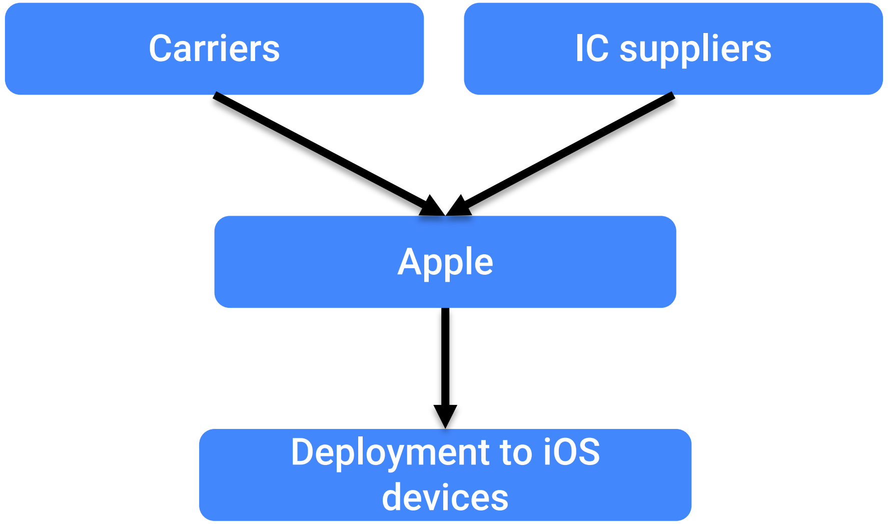
- **Deploy security policies that the user cannot change**
  - Password strength, encryption, applications, proxy, VPN, etc.
  - Forbid installation / removal of apps, limit bluetooth functionality, …
- **Get information from device**
  - Location, Call logs, SMS, Backups, …
- **Remote Actions**
  - OS Updates, Device Wipe, enforce device encryption, …

Challenge: Bring-your-own-device!

Updates

- Security updates are vital, especially in business environments

- Android: Slow update adoption
  - Improvements: Project Treble

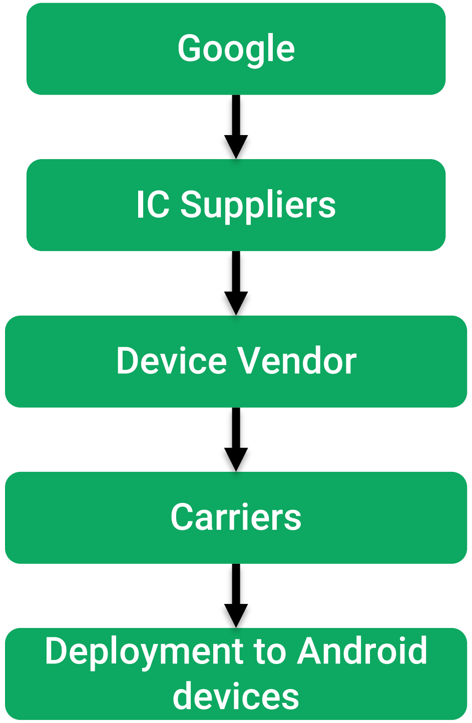


Carriers

IC suppliers

Apple

Deployment to iOS devices



Google

IC Suppliers

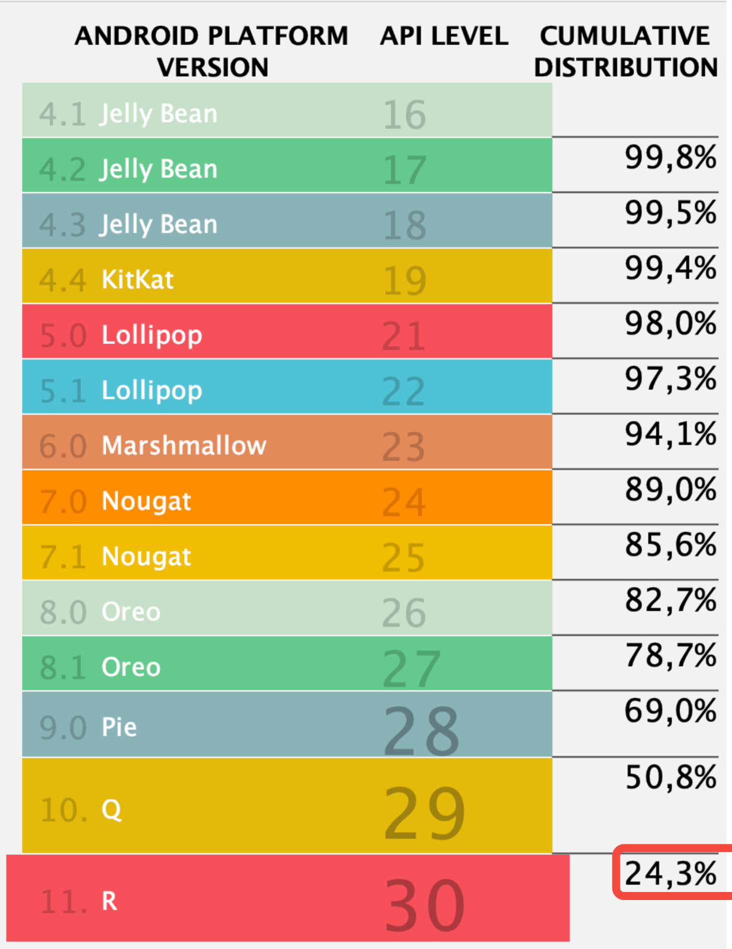
Device Vendor

Carriers

Deployment to Android devices

Source: googleblog.com

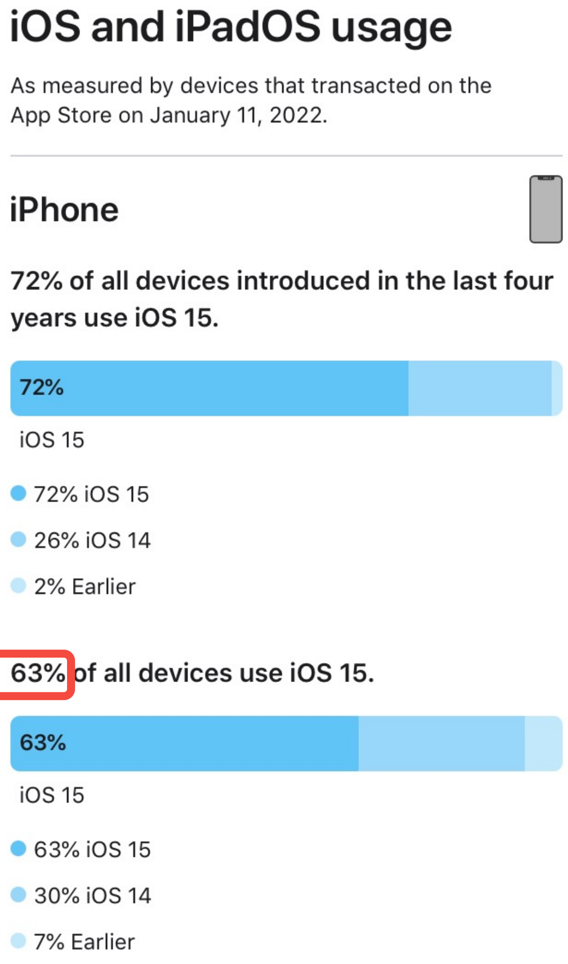
Version Distributions (Q1/2022)



ANDROID PLATFORM VERSION		API LEVEL	CUMULATIVE DISTRIBUTION
4.1	Jelly Bean	16	
4.2	Jelly Bean	17	99,8%
4.3	Jelly Bean	18	99,5%
4.4	KitKat	19	99,4%
5.0	Lollipop	21	98,0%
5.1	Lollipop	22	97,3%
6.0	Marshmallow	23	94,1%
7.0	Nougat	24	89,0%
7.1	Nougat	25	85,6%
8.0	Oreo	26	82,7%
8.1	Oreo	27	78,7%
9.0	Pie	28	69,0%
10.	Q	29	50,8%
11.	R	30	24,3%

Source: Android Studio

VS



iOS and iPadOS usage

As measured by devices that transacted on the App Store on January 11, 2022.

iPhone

72% of all devices introduced in the last four years use iOS 15.

- ● 72% iOS 15
- ● 26% iOS 14
- ● 2% Earlier

63% of all devices use iOS 15.

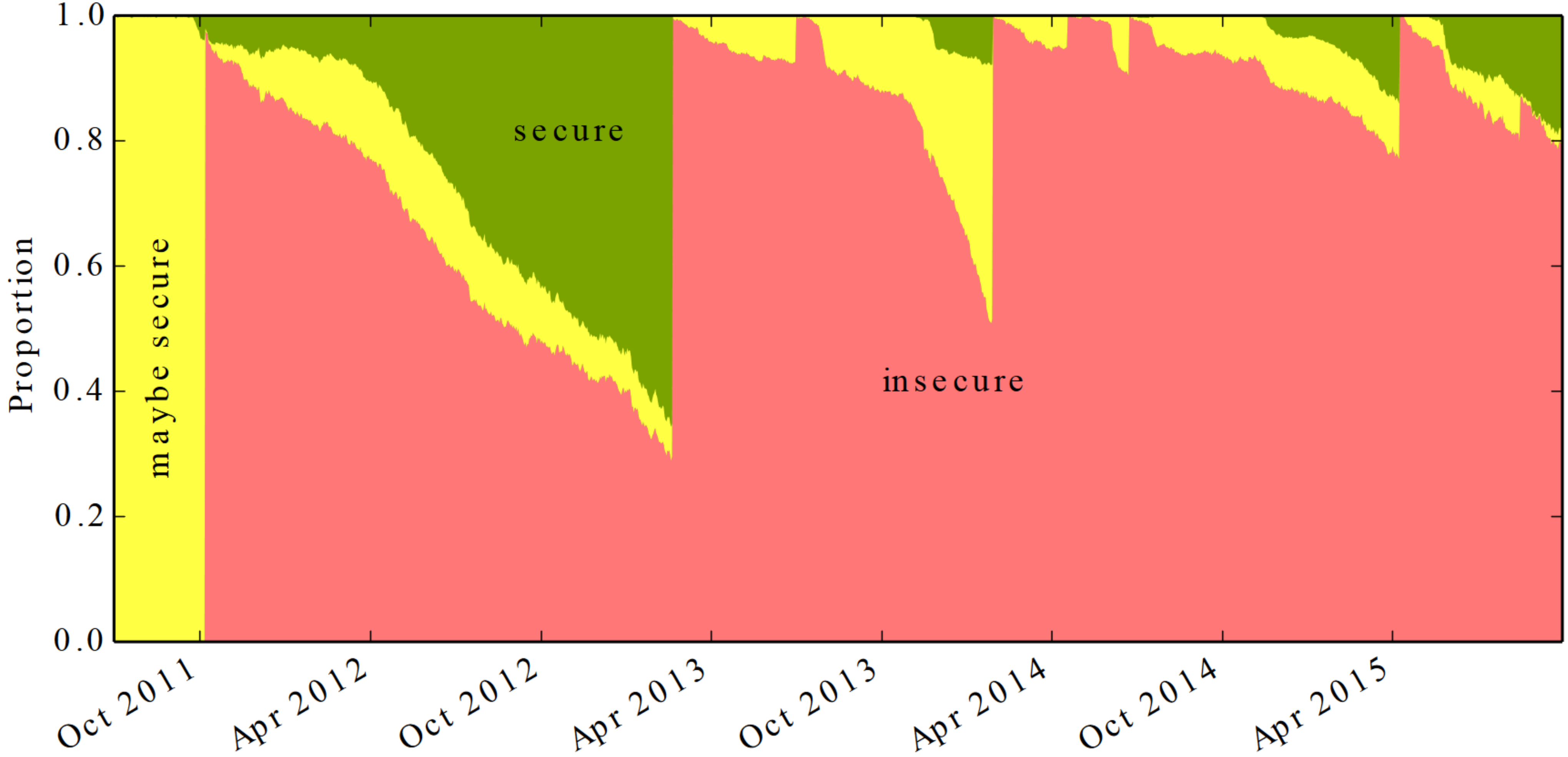
- ● 63% iOS 15
- ● 30% iOS 14
- ● 7% Earlier

Source: apple.com

Android 11: Released in September 2020

iOS 15: Released in September 2021

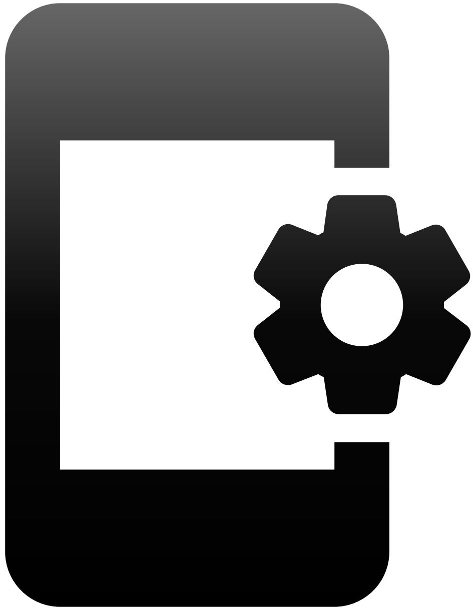
Vulnerable Android Devices



Source: androidvulnerabilities.org

Applications – OS Integration

- Access to APIs, Sensors, other Apps
  - Inter-Process Communication (IPC)
  - Android Permissions
  - How does the user know what a permission serves for?
- Protection of application data?
  - Disk encryption vs. App-specific storage
- How deep can apps integrate with the system?
- Rooted / jailbroken vs. normal use cases



Picture: Google / Apache 2.0

Access Protection – User Credentials

- How are credentials stored?
  - Hardware / Software?

- Complex passwords will be stored…
  - VPN to infrastructure

- WiFi, VPN, website passwords, etc.

- Are they encrypted, protected via PIN / password?

- How can they be accessed?

Outlook

Topics Mobile Security 2023

- Key & Data Storage on Mobile
  - Generation, Exchange, Attestation, …
- iOS Platform Security
  - iBoot, SEP, Data Protection, Jailbreak
- iOS Application Security
  - Components, Permissions, Crypto, …
  - Sandbox, Signing, Malware, …
- Android Platform Security
  - Verified Boot, FBE, SELinux, Root, …
- Android Application Security I & II
  - Components, Permissions, Crypto, …
  - Sandbox, Signing, SafetyNet, …
- Mobile Hardware Security
  - IoT, Embedded, Interfaces, FW
- Mobile Network Security
  - GMS, 3G, 4G, Attacks
- Mobile Security Research
  - Approach, Bounties, Laws, News

Outlook

- 24.03.2023
  - Key & Data Storage on Mobile Devices

- 31.03.2023
  - iOS Platform Security