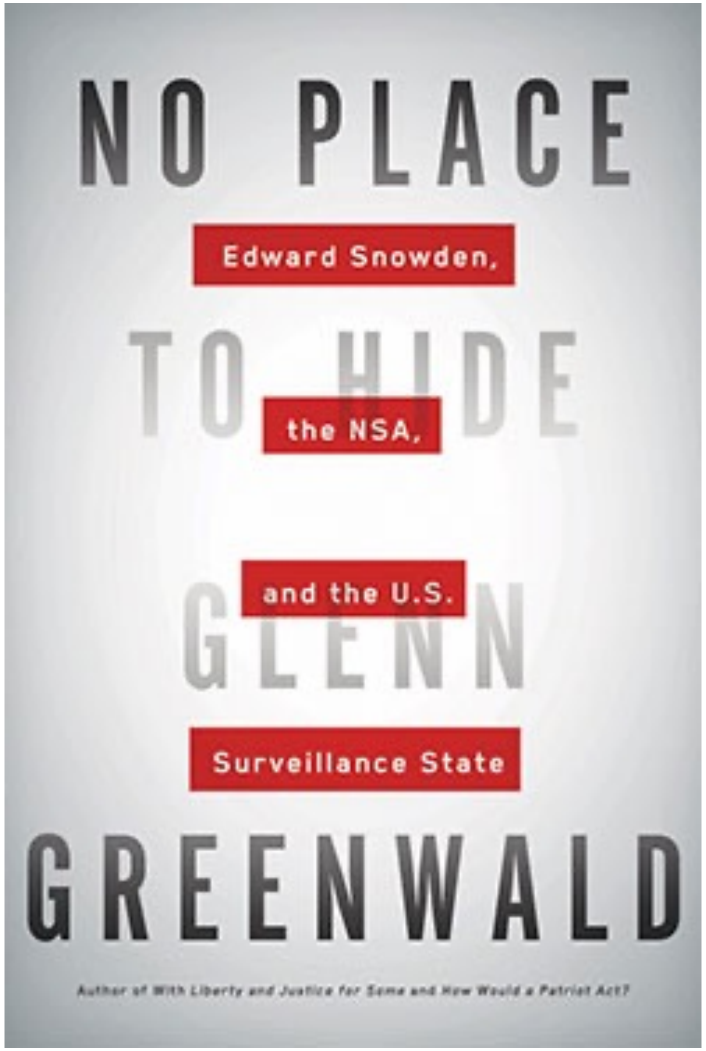
Security Engineering

Ecosystems Security: App stores, incentives, markets. Windows and Azure; supply-chain attacks. Accessory control.

Supply Chain Attacks: Operation Gunman

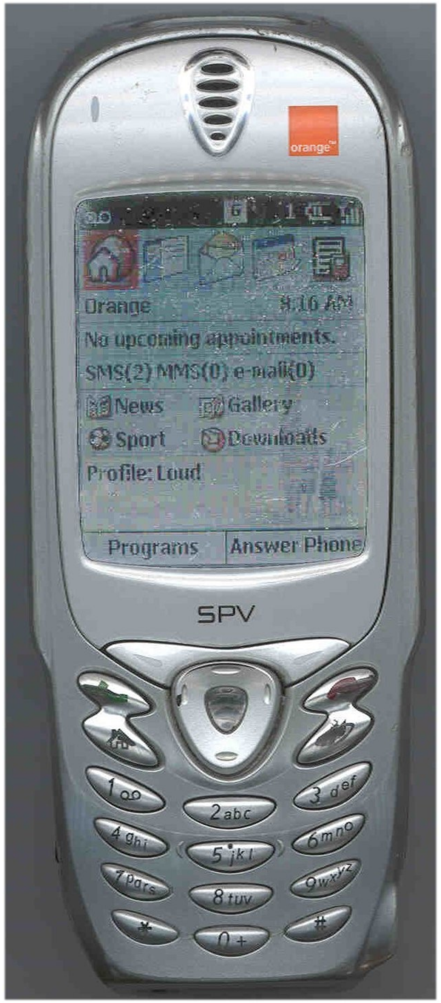
Supply Chain Attacks (2): Cisco Routers



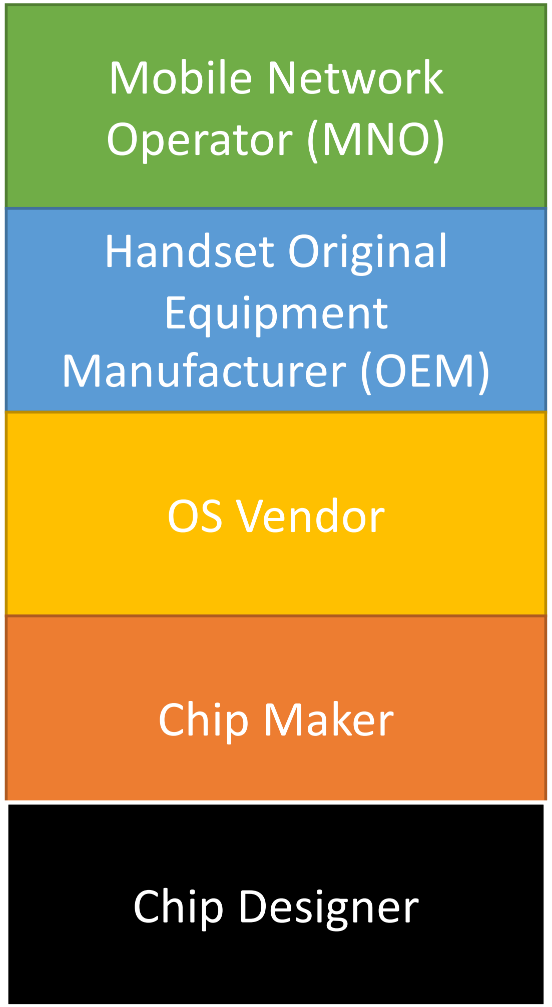
Supply Chain Attacks (3): Supermicro Motherboards

- Chip implanted into the motherboard to “phone home”
- Implant not placed in Supermicro’s design, but altered at manufacture time!
- Is this easier than bugging the software? Or the BIOS (also hacked in this instance)?
- Who along the supply chain could get you? It’s not always the easiest targets, but the most accessible.

Platform Security



Who is in charge?



Mobile Network Operator (MNO)

Handset Original Equipment Manufacturer (OEM)

OS Vendor

Chip Maker

Chip Designer

Platform Security: Android

Mobile Network Operator (MNO)	EE
Handset Original Equipment Manufacturer (OEM)	HTC
OS Vendor	Google
Chip Maker	TSMC
Chip Designer	Qualcomm & ARM

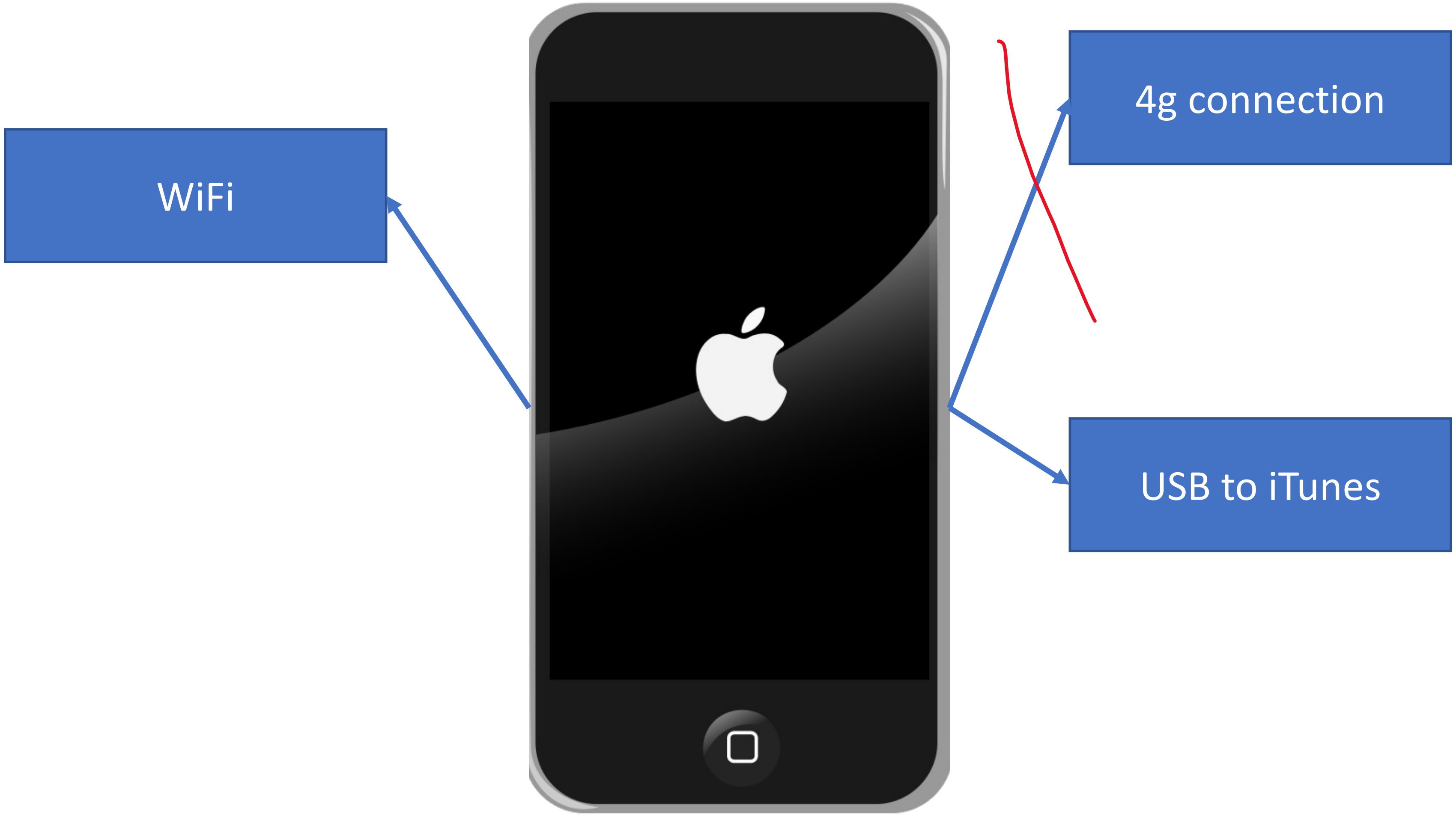
How do updates **Propagate?**

Why is Android Free?

Platform Security: Apple

Mobile Network Operator (MNO)	EE
Handset Original Equipment Manufacturer (OEM)	Apple
OS Vendor	Apple
Chip Maker	TSMC/Samsung
Chip Designer	Apple & ARM

Platform Security: Apple



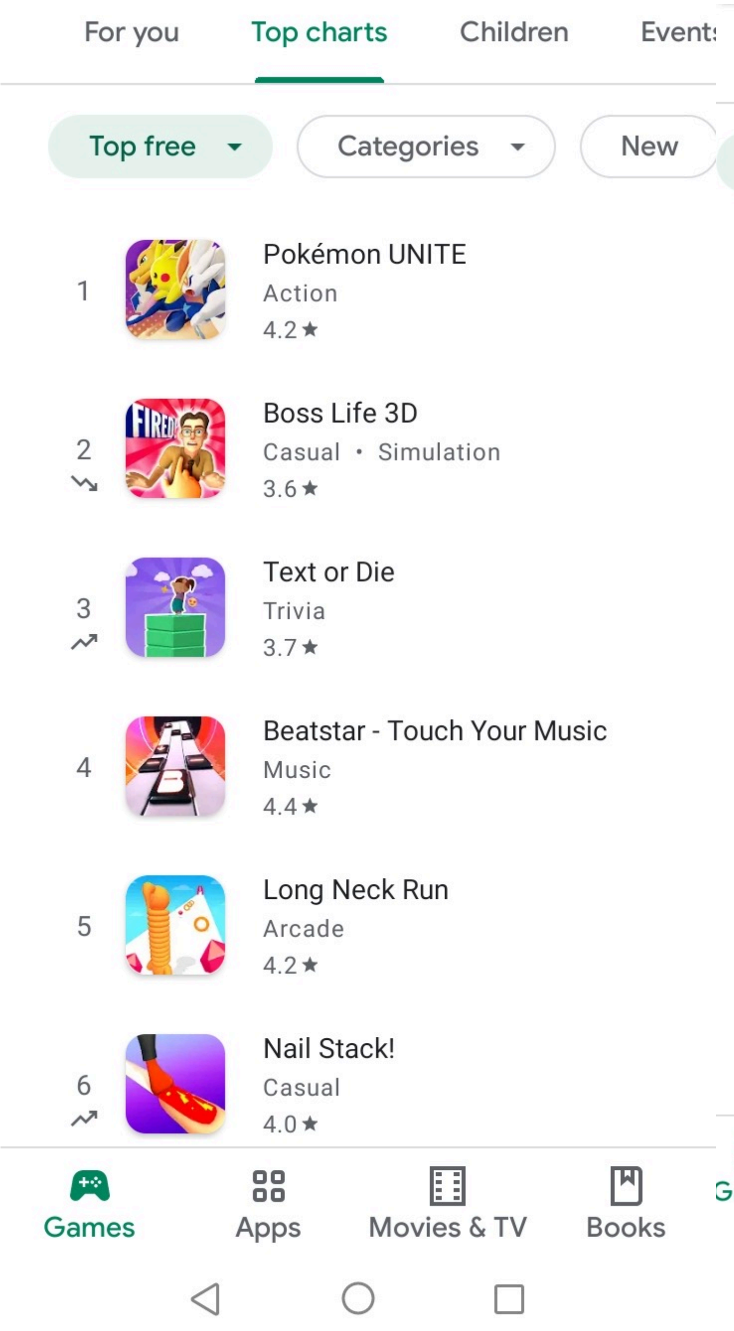
WiFi

4g connection

USB to iTunes

App Store Ecosystems

App Store Ecosystems



1 Pokémon UNITE
Action
4.2★

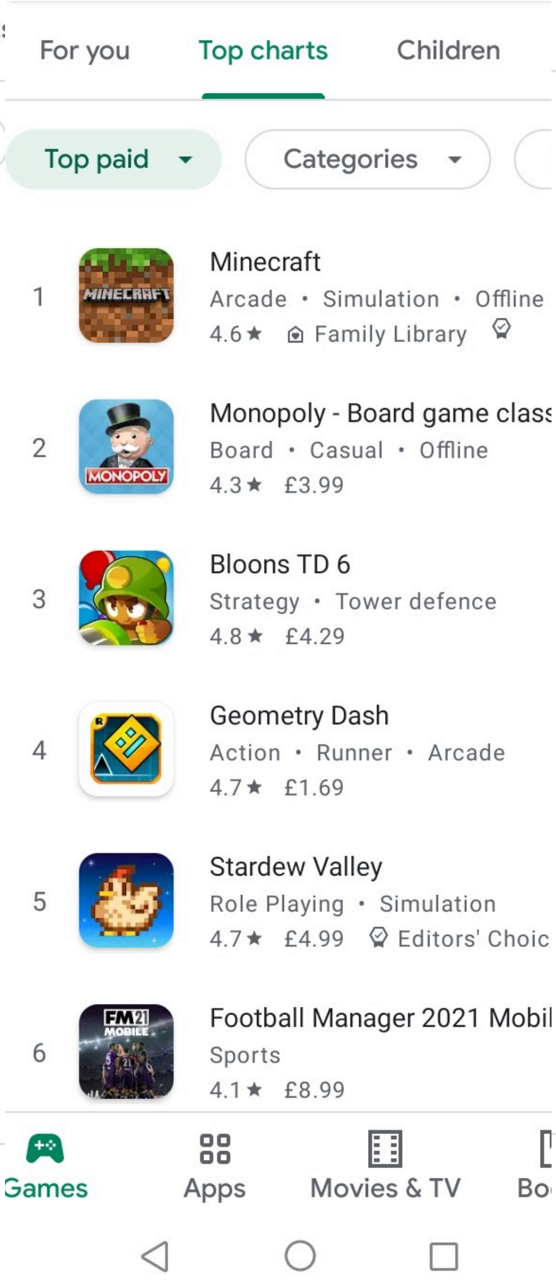
2 Boss Life 3D
Casual • Simulation
3.6★

3 Text or Die
Trivia
3.7★

4 Beatstar - Touch Your Music
Music
4.4★

5 Long Neck Run
Arcade
4.2★

6 Nail Stack!
Casual
4.0★



1 Minecraft
Arcade • Simulation • Offline
4.6★ Family Library

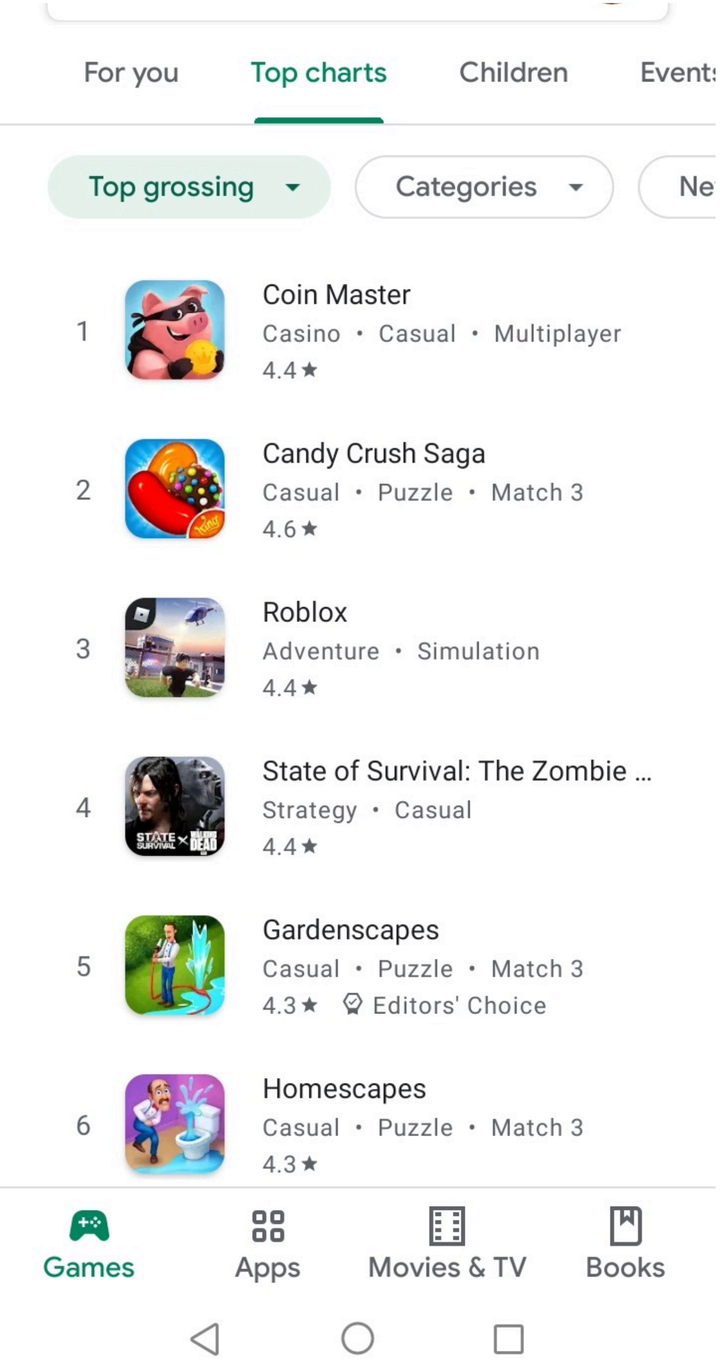
2 Monopoly - Board game class
Board • Casual • Offline
4.3★ £3.99

3 Bloons TD 6
Strategy • Tower defence
4.8★ £4.29

4 Geometry Dash
Action • Runner • Arcade
4.7★ £1.69

5 Stardew Valley
Role Playing • Simulation
4.7★ £4.99 Editors' Choic

6 Football Manager 2021 Mobil
Sports
4.1★ £8.99



1 Coin Master
Casino • Casual • Multiplayer
4.4★

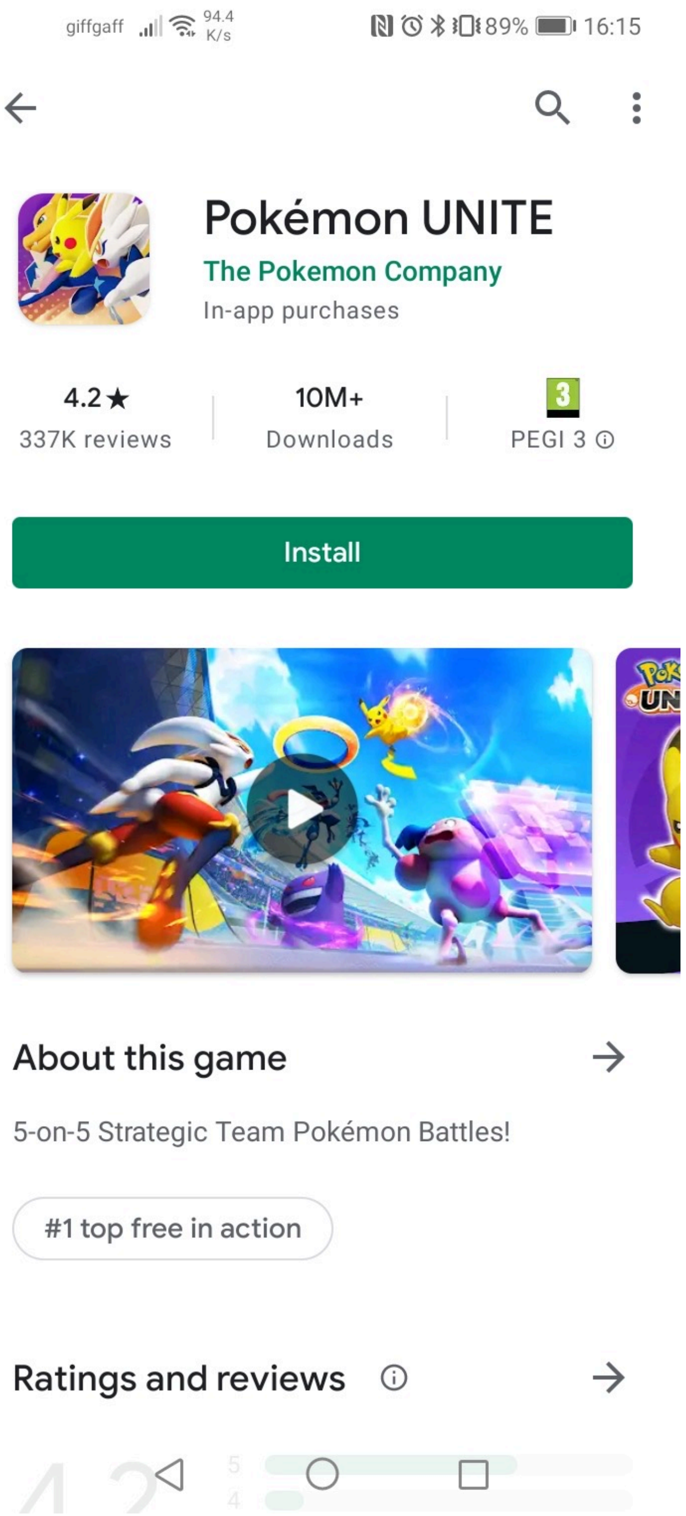
2 Candy Crush Saga
Casual • Puzzle • Match 3
4.6★

3 Roblox
Adventure • Simulation
4.4★

4 State of Survival: The Zombie ...
Strategy • Casual
4.4★

5 Gardenscapes
Casual • Puzzle • Match 3
4.3★ Editors' Choice

6 Homescapes
Casual • Puzzle • Match 3
4.3★



Pokémon UNITE

The Pokemon Company

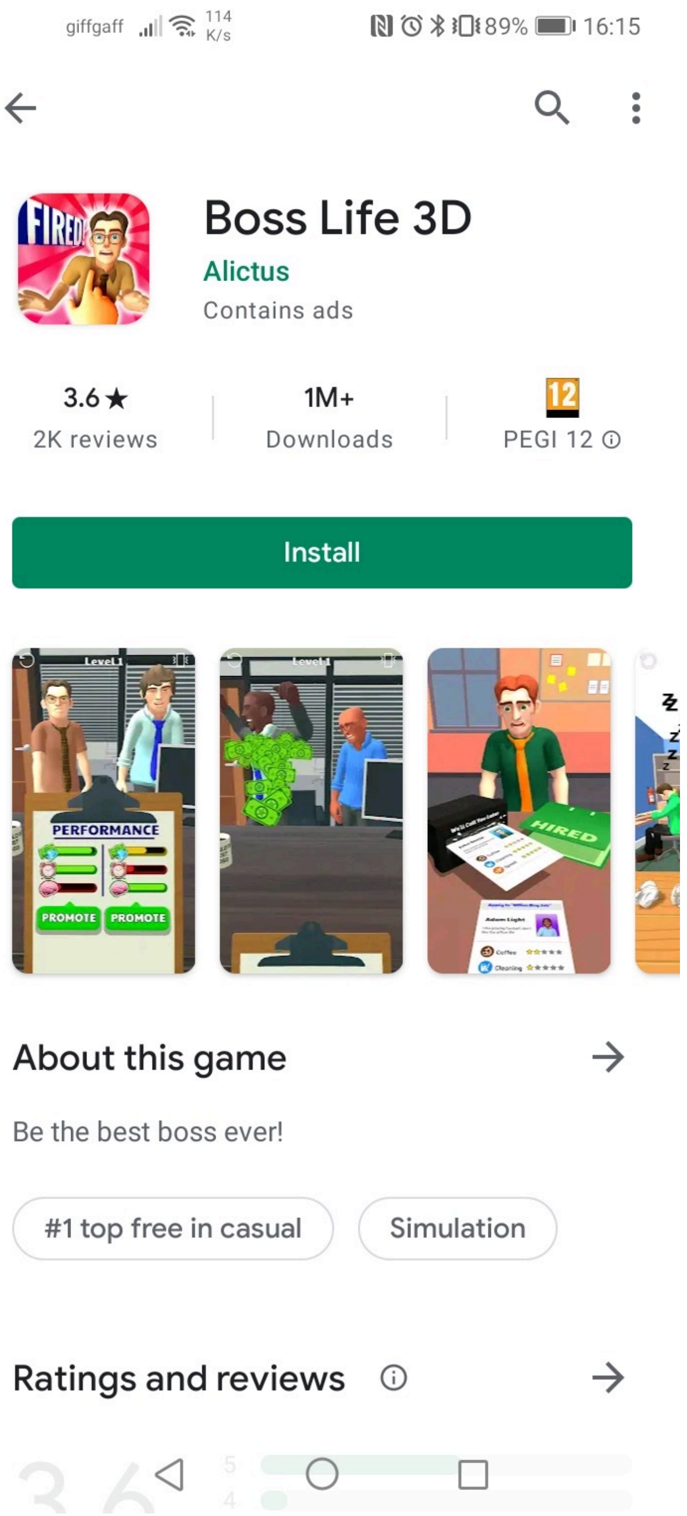
In-app purchases

4.2★ 337K reviews | 10M+ Downloads | 3 PEGI 3 ⓘ

About this game →

5-on-5 Strategic Team Pokémon Battles!

Ratings and reviews ⓘ →



Boss Life 3D

Alictus

Contains ads

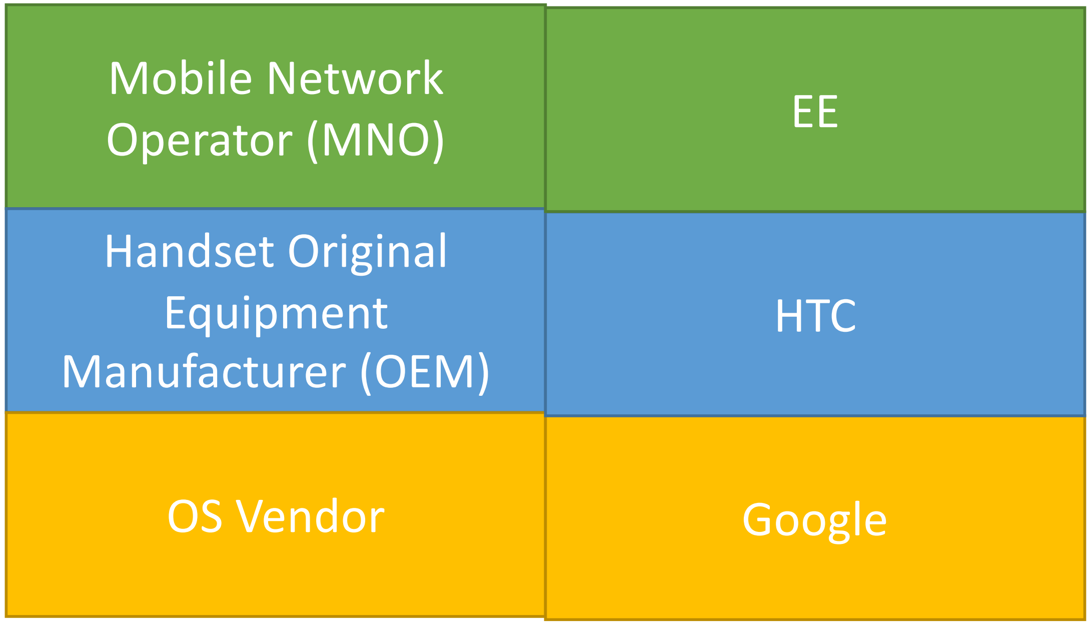
3.6★ 2K reviews | 1M+ Downloads | 12 PEGI 12 ⓘ

About this game →

Be the best boss ever!

Ratings and reviews ⓘ →

App Store Ecosystems



Mobile Network Operator (MNO)

EE

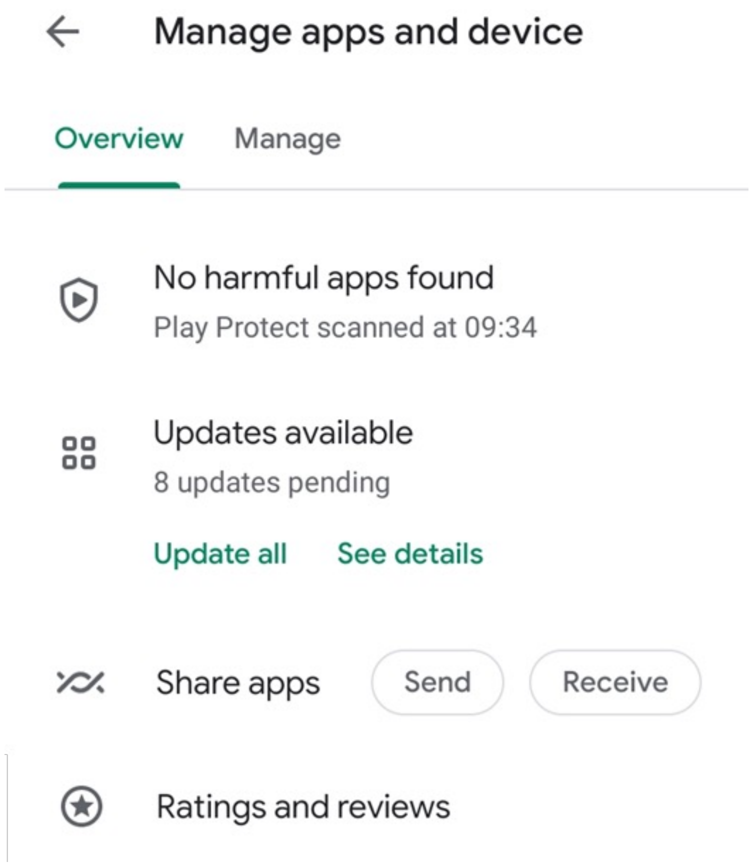
Handset Original Equipment Manufacturer (OEM)

HTC

OS Vendor

Google

Google Play



← Manage apps and device

Overview Manage

No harmful apps found

Play Protect scanned at 09:34

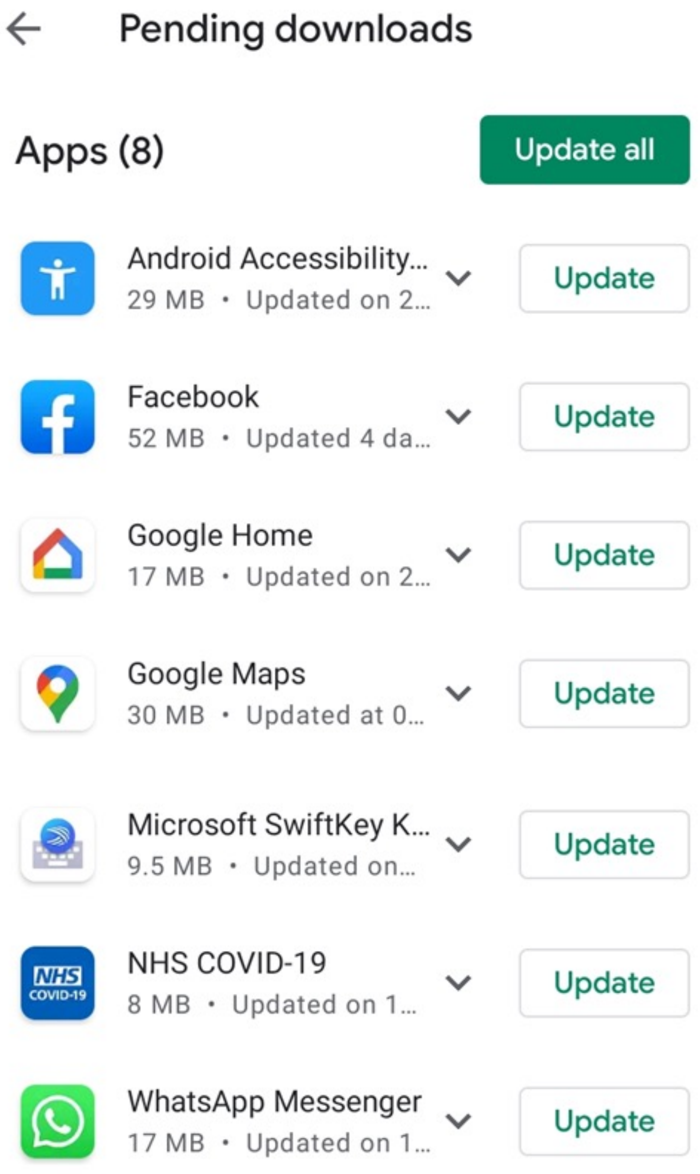
Updates available

8 updates pending

Update all See details

Share apps Send Receive

Ratings and reviews



← Pending downloads

Apps (8) Update all

Android Accessibility... 29 MB • Updated on 2... Update

Facebook 52 MB • Updated 4 da... Update

Google Home 17 MB • Updated on 2... Update

Google Maps 30 MB • Updated at 0... Update

Microsoft SwiftKey K... 9.5 MB • Updated on... Update

NHS COVID-19 8 MB • Updated on 1... Update

WhatsApp Messenger 17 MB • Updated on 1... Update

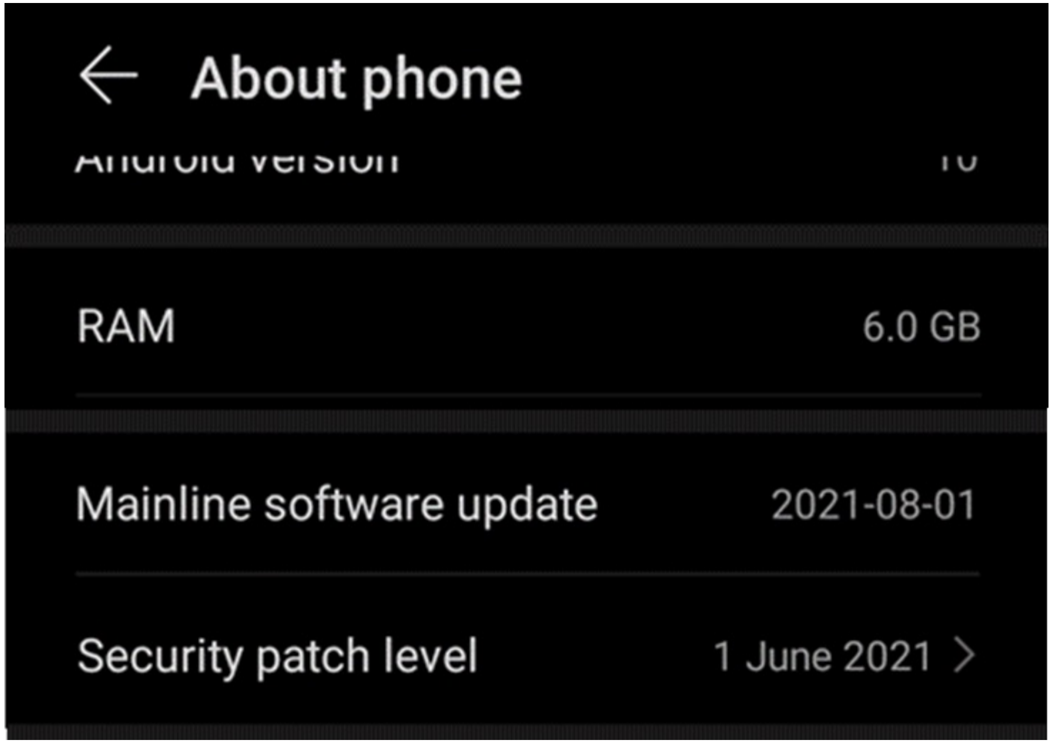
Google Play (2)

- Self-signed applications (unlike iOS)
- Default with no “Install Apps from External Sources” – security and lock-in
- App Security Improvement Program

Google App Security

- Suite of Sanitizers and Mitigators for User Code: BoundsSan, AddrSan, IntSan, Shadow Stacks, Scudo Hardened Allocator
- Not just about protecting Android the OS: if you extract rent from an ecosystem, you need to protect the 3rd party code too!

Android Security Updates



About phone

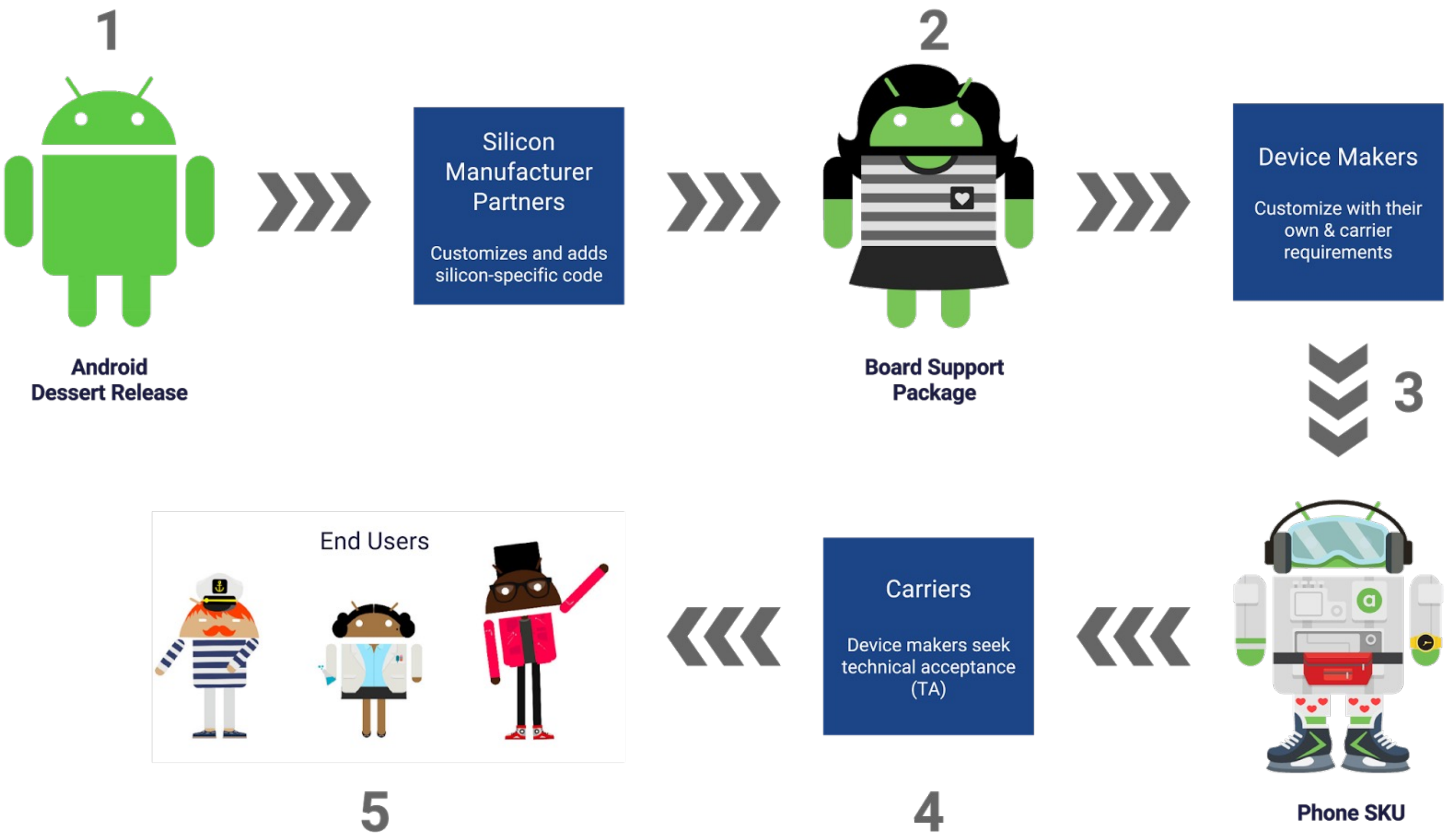
Android version 10

RAM 6.0 GB

Mainline software update 2021-08-01

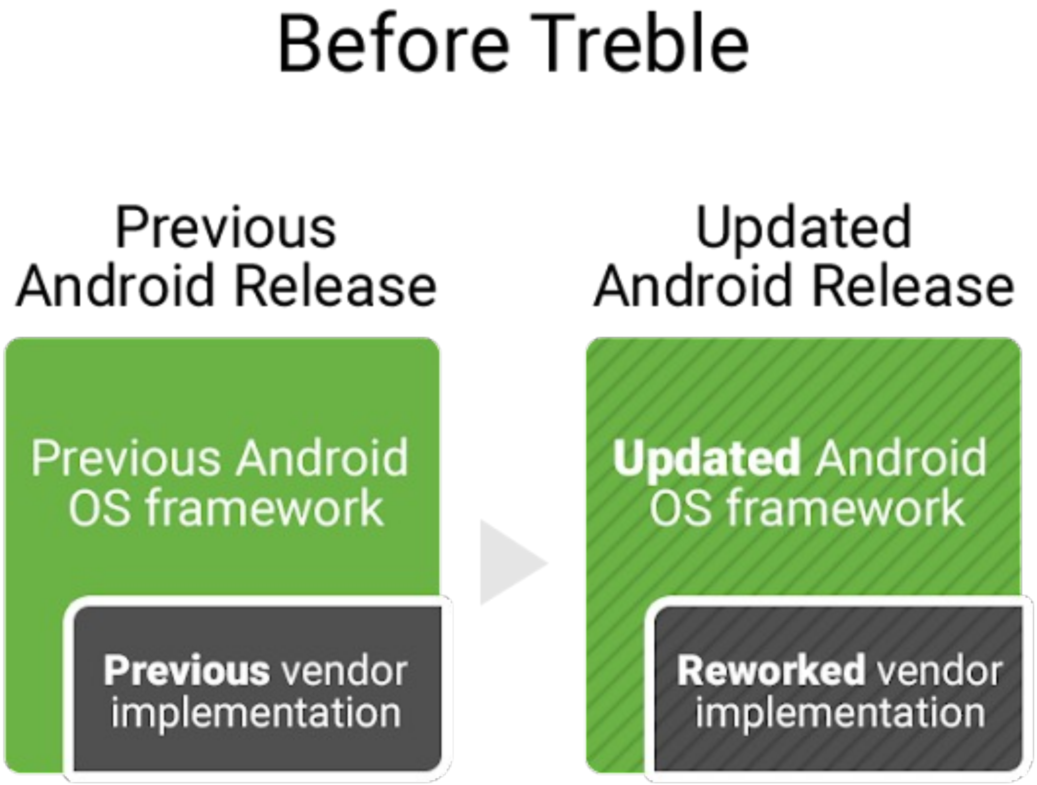
Security patch level 1 June 2021

Android Update Lifecycle


1
Android
Dessert Release
Silicon
Manufacturer
Partners
Customizes and adds silicon-specific code
2
Board Support
Package
Device Makers
Customize with their own & carrier requirements
3
Phone SKU
4
Carriers
Device makers seek technical acceptance (TA)
5
End Users

https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html

Android Update Lifecycle



Before Treble

Previous Android Release

Previous Android OS framework

Previous vendor implementation

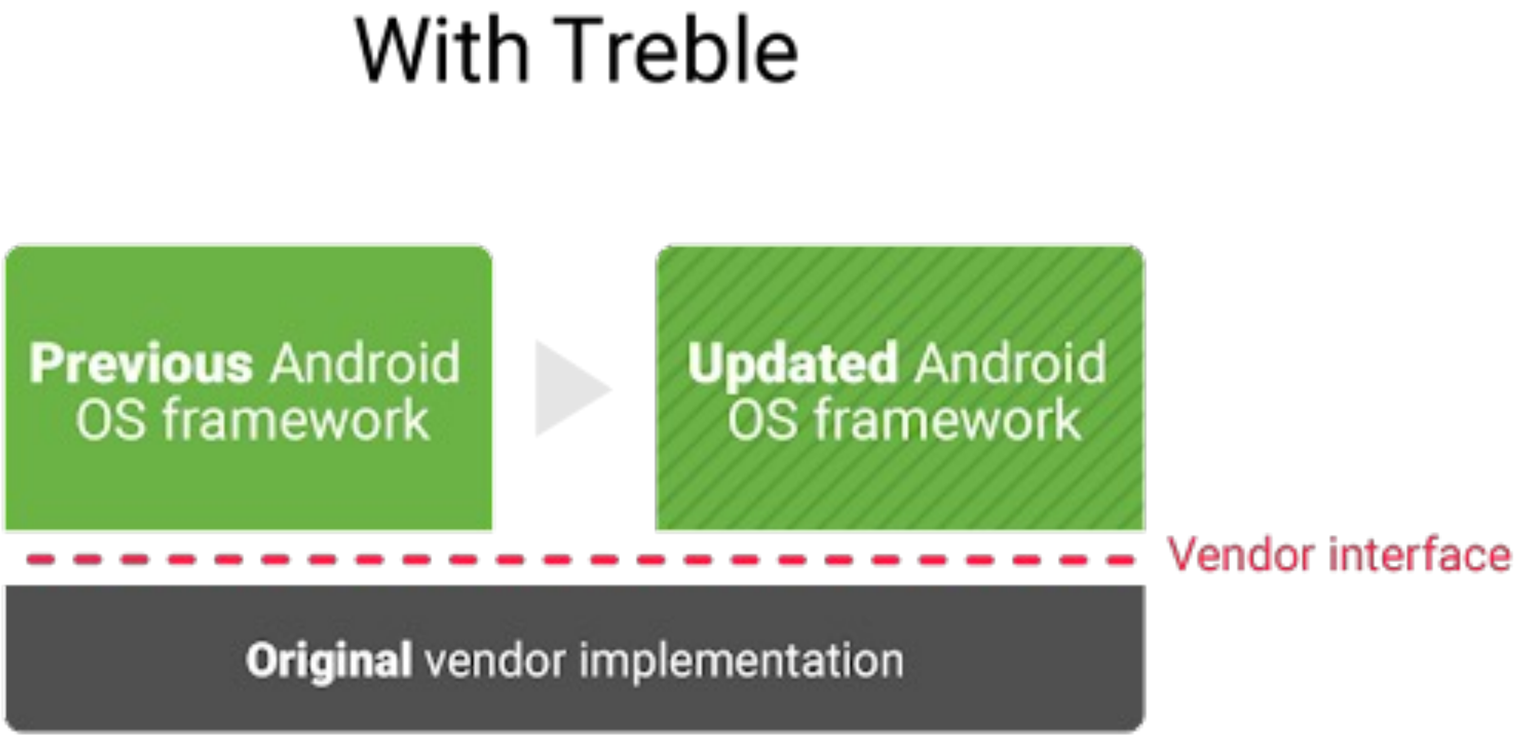
Updated Android Release

Updated Android OS framework

Reworked vendor implementation

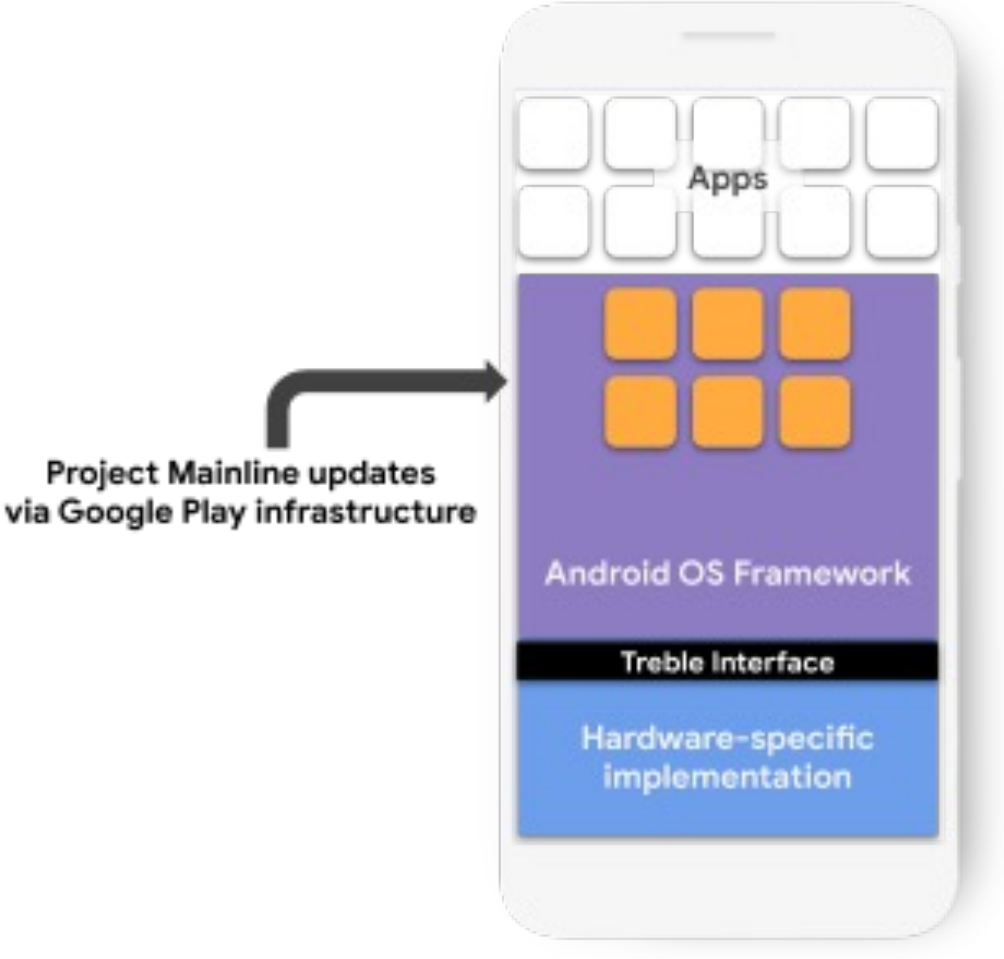
https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html

Android Update Lifecycle


With Treble
Previous Android OS framework
Updated Android OS framework
Vendor interface
Original vendor implementation

https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html

Android Update Lifecycle: Project Mainline


Apps
Project Mainline updates via Google Play infrastructure
Android OS Framework
Treble Interface
Hardware-specific implementation

https://android-developers.googleblog.com/2019/05/fresher-os-with-projects-treble-and-mainline.html

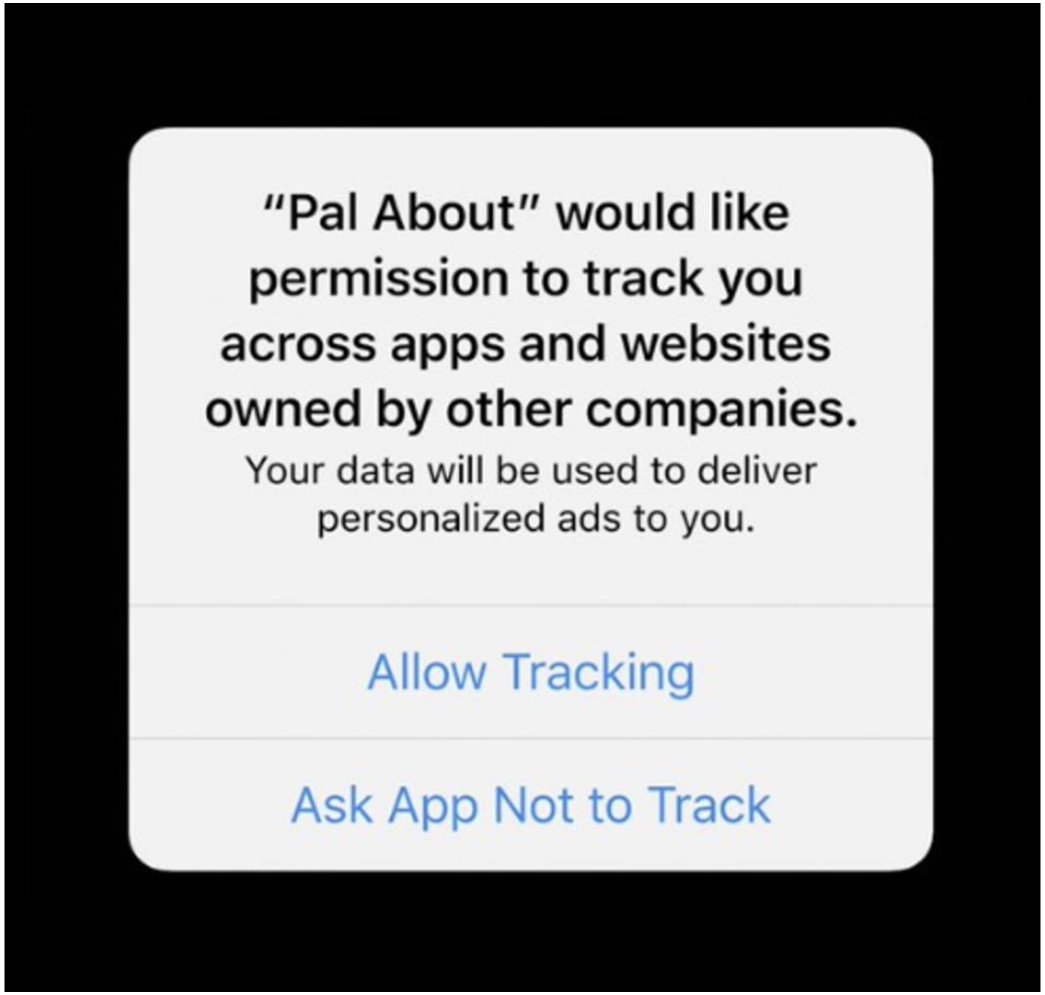
Other Android App Security Mechanisms

- From the Chip Vendor: TrustZone.
- Obfuscation: mandatory in banking.
- Android KeyStore
- SIM locking: device in the custody of the attacker!

Apple

- (Semi)-closed ecosystem.
- 30% commission on products sold through App Store, incl. IAPs – antitrust issues e.g. Epic Games Lawsuit
- Patches for 5ish years – why does Apple have more incentive here?
- Largely closed source – there is obscurity, but is it part of the security?

Apple IDFA



“Pal About” would like permission to track you across apps and websites owned by other companies.

Your data will be used to deliver personalized ads to you.

App Ecosystem (Continued)

- Apps can be/go bad for many reasons.
- “We Purchase Apps” – ad fraud.
- Tussles around trust in Ad Networks even in reputable apps: e.g. CamScanner started dropping Trojans on phones!
- Google: Apps assumed bad and contained. Windows: global visibility, with Antivirus to do the heavy lifting.
- Google Play Store still has trouble with “Repackaging”: adding “Riders” to “Carrier” apps.

“Why is Windows so Insecure?”

- Medical and defence can build dependable systems, so why was Win95/98 totally defenceless?
- “Ship it Tuesday and get it right by Version 3”.
- Competition *for* the market: rational to get as much (poorly written) software as quickly as possible.
- Initial vs Sustained Velocity, and Technical Debt
- “Bargains then Ripoffs” – not just poor security, but dumping costs on users also rational behaviour.

Microsoft “turned their s*** around”

- *“I would always make a point of asking hackers, ‘I know you hate the vendors, but of all of them, who do you hate least?’ The answer was always the same.* ***‘Microsoft,’ they would tell me. ‘They turned their s*** around.’****” **–** Nicole Perlroth*
- From XP Onwards: free security tools, secure coding training for all staff, patching.
- BUT – more effort went into protecting premium video than credit card numbers!

Maturing your Ecosystem

- What might a patch to fix a bug break, in the Windows Software ***Ecosystem***?
- …With legacy code that likely assumes it's running as admin?
- Sustained Velocity bites…
- Can you change your Ecosystem to make it more secure? Microsoft tried and failed with the Windows App Store, Universal Windows Apps, and Windows 10S.
- Is this all Microsoft's fault? Why target OSX when Windows has 5x the users…

Azure

- Microsoft moving to a new ecosystem… the CLOUD.
- Not just about using Microsoft’s Server Hardware – also about using their software ecosystem.
- Azure Security Centre: Compliance reporting, threat modelling, crypto standards, managing risks of 3rd-party components, pen testing.
- “Bargains then Ripoffs”

Azure - Encryption

- HSMs now maintained by Azure or Amazon, not the bank!
- Double Encryption DRM
- Cloud Key vault

Code Supply Chain

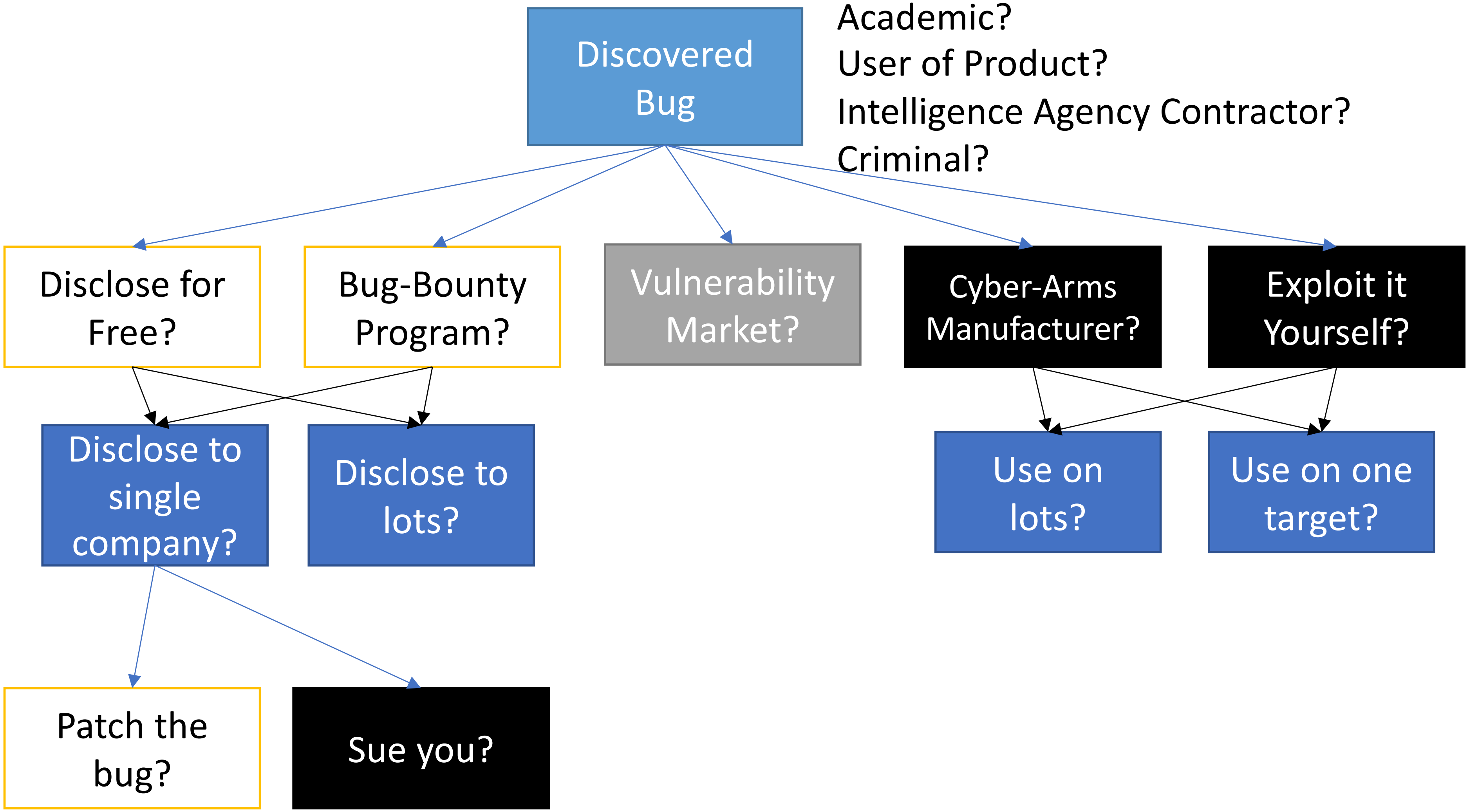
- Can insiders (un)intentionally get bad code committed to release?
- Who is an “insider” for the software running in your device? Think about your OS kernel, libraries…
- Code reviews are a form of multi-party authorisation, but be careful to avoid rubberstamping…
- In this scenario, bugs aren’t random – they’re introduced to open-source projects with wide use!

Code Supply Chain (2)

- Who makes the decision to integrate patches into your products?
- Third-party code review: keep an internal version and review upstream patches as they appear.
- The Compiler is part of your TCB!
- Code signing can help you work out provenance, but watch out for your keys leaking, and beware of who has signing keys…

Vulnerability Market Ecosystems

Customer?
Academic?
User of Product?
Intelligence Agency Contractor?
Criminal?



Discovered Bug

Disclose for Free?

Bug-Bounty Program?

Vulnerability Market?

Cyber-Arms Manufacturer?

Exploit it Yourself?

Disclose to single company?

Disclose to lots?

Use on lots?

Use on one target?

Patch the bug?

Sue you?

Whose Fault is it Anyway?

- Incentives are to blame shift – both to partners in your ecosystem, and even within teams in the same company.
- Your hardware teams will blame your software teams: who should actually fix it?
- BIDI attacks: Compiler? Editor? Build environment? Repository code-smell checking? The easiest deployment may not be the cheapest or most comprehensive…

Accessory Control

Razors and Blades Model

- Two-part pricing.
- Lexmark vs SCC 2004: free market for cryptologists!

The New Improved Gillette SAFETY RAZOR

PATENTED JAN.13.1920

NEW STANDARD
Genuine Leather Covered Case,
Purple Velvet and Satin Lined.
New Standard. Triple Silver Plated New Improved Gillette Safety Razor. Metal Blade Box
Set below contains 24 shaving edges
(12 double-edged Gillette Blades).
Article No. 1054 300 Certificates

TUCKAWAY
A Small Compact Set.
Metal Case, Purple Velvet and Satin Lined.
Tuckaway. Triple Silver Plated New Improved Gillette Safety Razor. Triple Silver Plated Case; Metal Blade Box.
Above set contains 24 shaving edges
(12 double-edged Gillette Blades).
Article No. 1054 300 Certificates

GILLETTE BLADES
24 Shaving Edges (12 double-edged Gillette Blades).
Article No. 336 65 Certificates

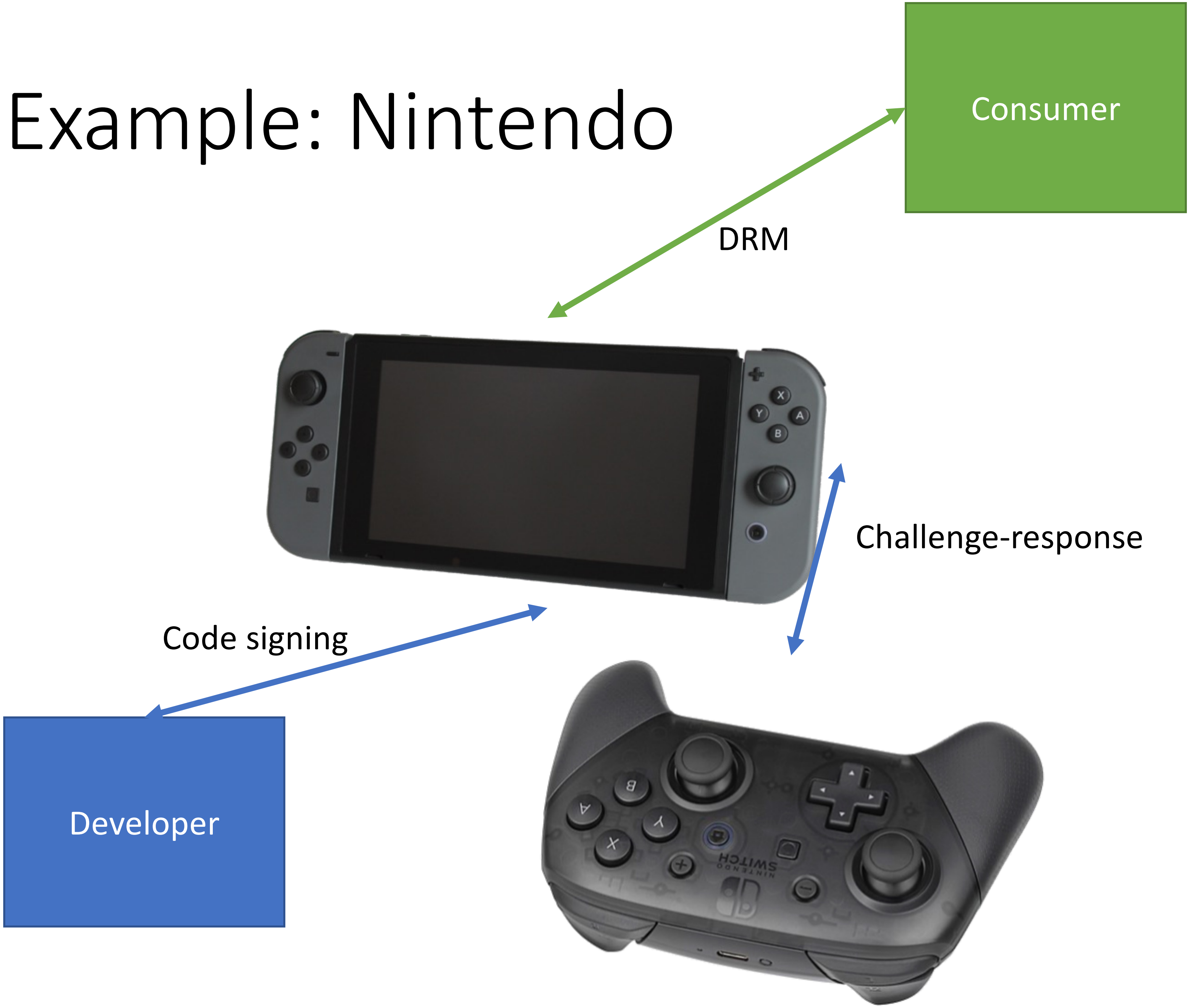
GILLETTE BROWNIE
(Old Type)
Imitation Leather Covered Metal Case.
Gillette Brownie. Nickle Plated, Old Type Gillette Safety Razor, 6 Shaving Edges (3 double-edged Gillette Blades) in sealed packet.
Article No. 1055 65 Certificates

GILLETTE SAFETY RAZOR COMPANY, BOSTON

MADE IN U.S.A. Gillette KNOWN THE WORLD OVER
TUCKAWAY
OVERHANGING CAP
CHANNELED GUARD
ADJUSTABLE SHORT FLEXURE
FULCRUM SHOULDER
NEW STANDARD
MADE IN U.S.A. TRADE Gillette MARK KNOWN THE WORLD OVER
MADE IN U.S.A. Gillette KNOWN THE WORLD OVER
NO STROPPING 207 NO HONING
Gillette

HEWLETT PACKARD
hp
HP Officejet
Ink Cartridge
Cyan
89

Example: Nintendo



Consumer

DRM

Challenge-response

Code signing

Developer

Example: Overrun Prevention

- Accessory Control gets complicated with complex supply chains
- E.g. you’re an IP vendor selling a circuit design to be run on cameras at $2 per camera.
- You sell licenses for 100k cameras, and find 200k appear on the market.
- IP Vendor -> Camera Company -> Factory. Who has incentives to cheat?

Is Accessory Control Objectionable?

- Depends how competitive the markets are.
- BUT – tech entrenches and causes monopolies…
- Right-to-Repair Laws – a common battleground.
- Sustainability: accessory control usually lowers lifetimes.