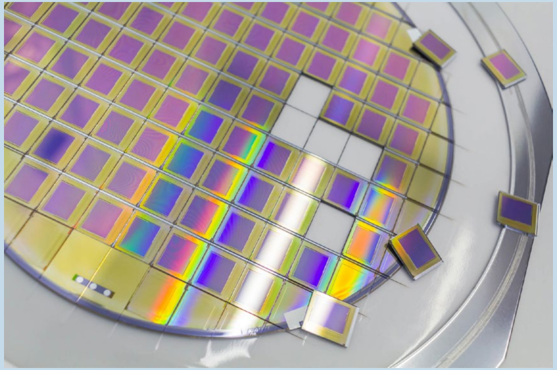
THE UNIVERSITY *of* EDINBURGH

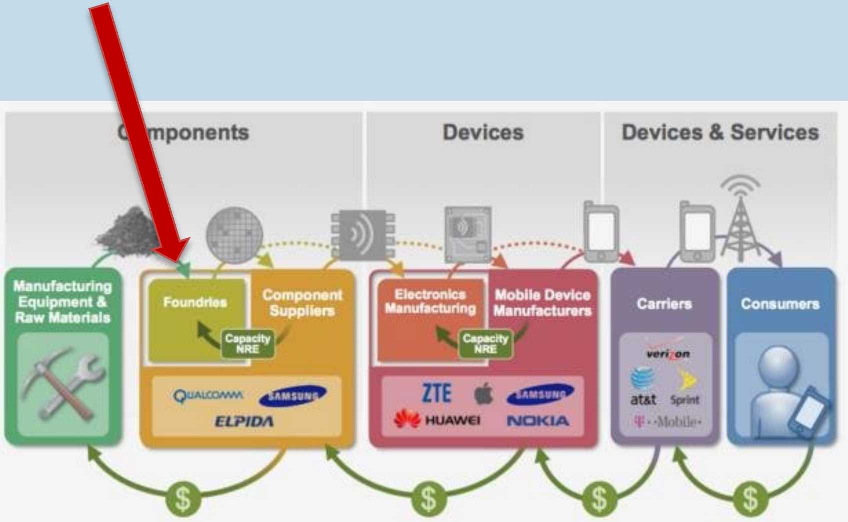
Ecosystems Security

Security Engineering (Spring 2026)

Lecturer: Jingjie Li & Daniel Woods

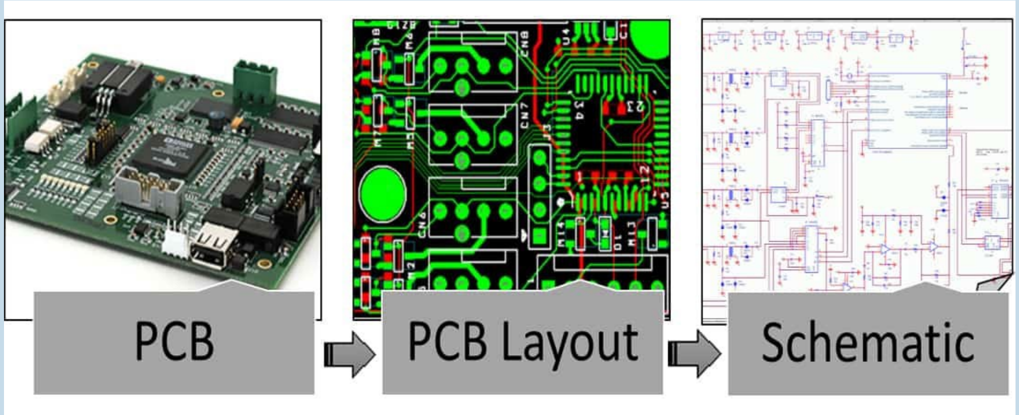
Extreme Ultraviolet Lithography (EUV) machines – why so important?

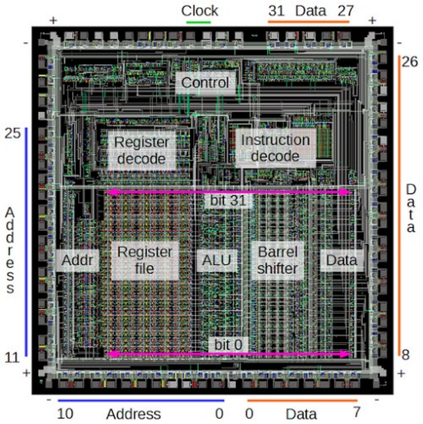




- Security is segmented in supply chain and ecosystems
- Original equipment manufacturer
- Things get complicated when attacker is really motivated and is capable
- Economics under building and governing a secure ecosystem

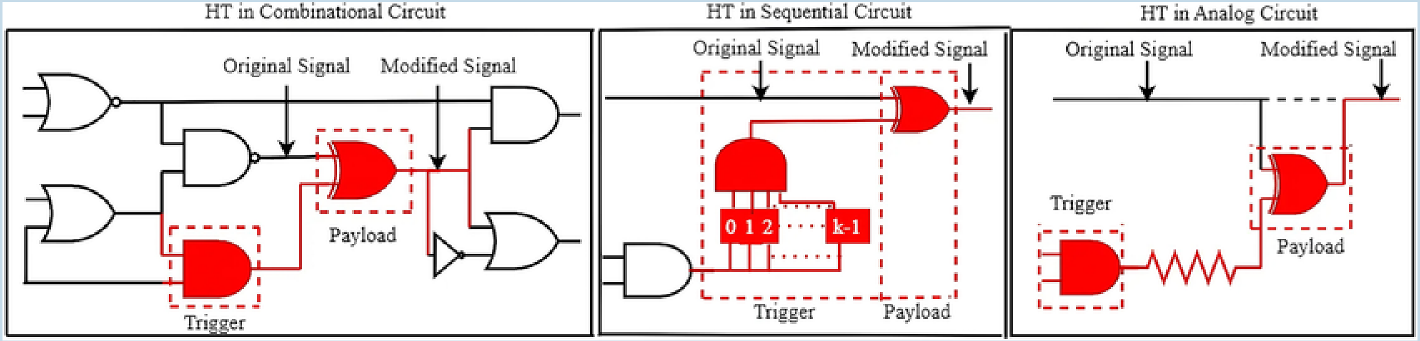
Hardware supplychain





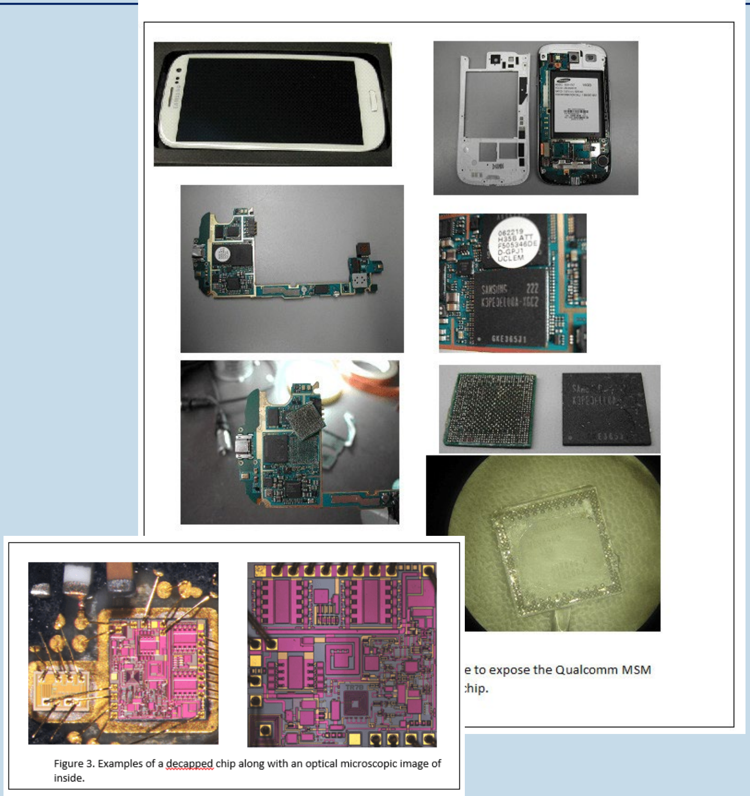
- Designers do not have full visibility into the manufacturing process
- Complexity of the hardware makes bugs and vulnerabilities even hard to find
- Designers/vendors even rely on reverse engineering to ensure IP/chip integrity

Hardware trojan



Hardware reverse engineering

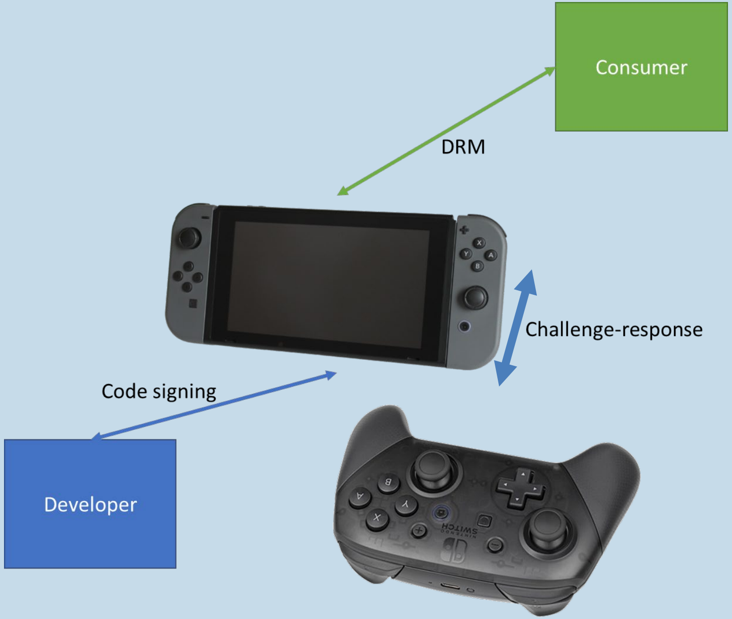
- Sample preparation
- SEM imaging
- Image processing
- Circuit extraction
- Circuit analysis…



e to expose the Qualcomm MSM
chip.

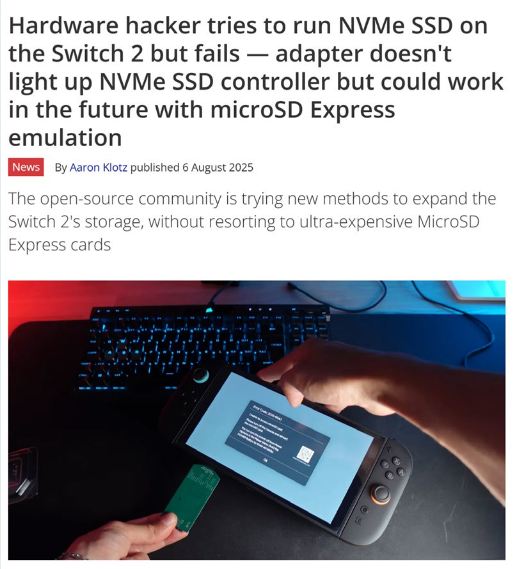
Figure 3. Examples of a decapped chip along with an optical microscopic image of inside.

Accessory control



- Locking users and developers through digital right management (DRM)
- DRM via security printing, obfuscation, temper-resistance, license check, etc.

Accessory control



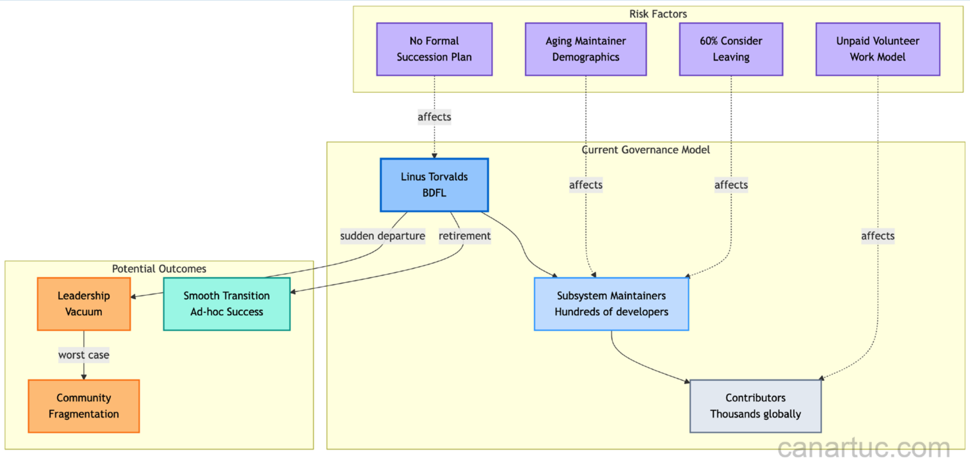
Hardware hacker tries to run NVMe SSD on the Switch 2 but fails — adapter doesn't light up NVMe SSD controller but could work in the future with microSD Express emulation

News By Aaron Klotz published 6 August 2025

The open-source community is trying new methods to expand the Switch 2's storage, without resorting to ultra-expensive MicroSD Express cards

- People are incentivized to cheat!
- 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?

Software and code supply chain



Risk Factors

No Formal Succession Plan

Aging Maintainer Demographics

60% Consider Leaving

Unpaid Volunteer Work Model

affects

Current Governance Model

Linus Torvalds BDFL

affects

affects

sudden departure

retirement

affects

Potential Outcomes

Leadership Vacuum

Smooth Transition Ad-hoc Success

Subsystem Maintainers Hundreds of developers

worst case

Community Fragmentation

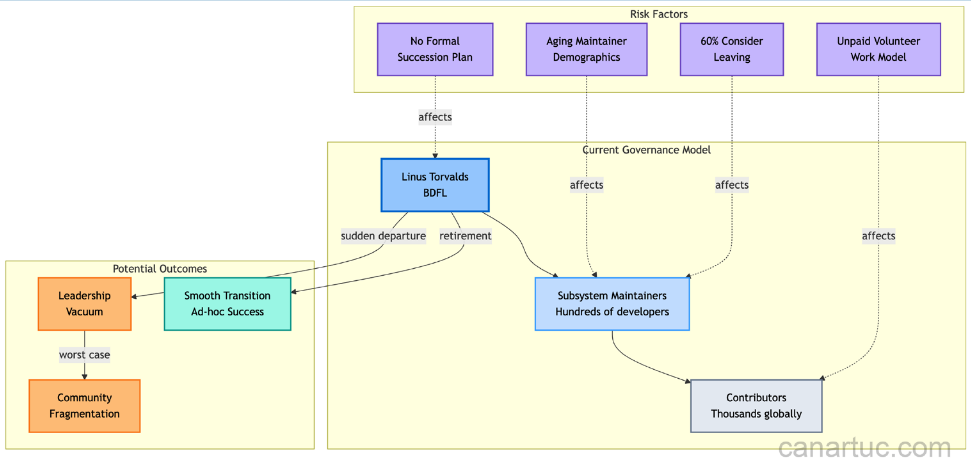
Contributors Thousands globally

canartuc.com

https://canartuc.medium.com/linux-kernel-maintainer-succession-the-crisis-hiding-in-plain-sight-295105d236b1

- 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!

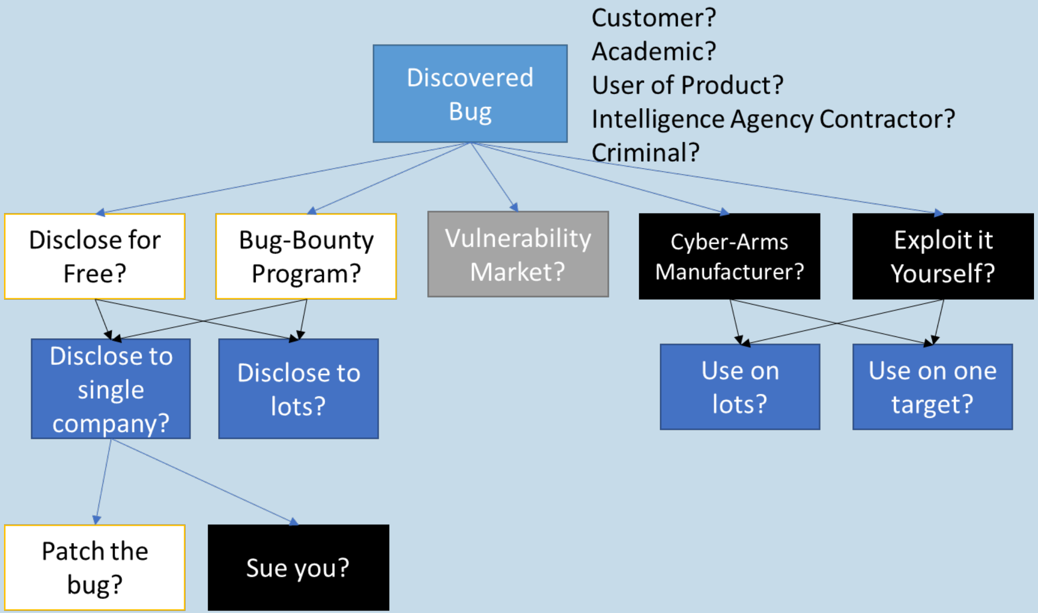
Software and code supply chain



https://canartuc.medium.com/linux-kernel-maintainer-succession-the-crisis-hiding-in-plain-sight-295105d236b1

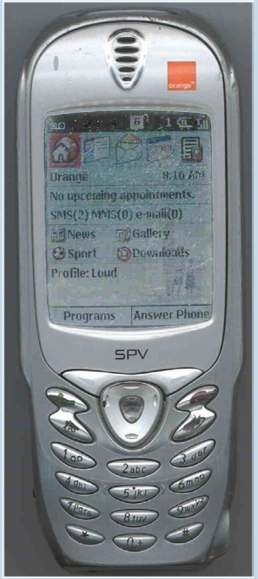
- Who makes the decision to integrate patches into your products?
- Third-party code review: keep an internal version and review upstream patches as they appear.
- The Compiler is part of your trust code base
- Code signing can help you work out provenance, but watch out for your keys leaking, and beware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

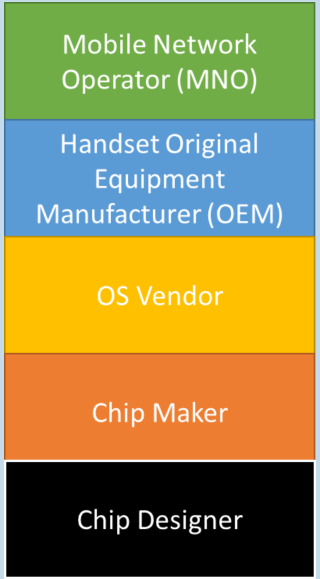
How to report vulnerability? Or should people even report?



- (Properly) reporting vulnerability is not easy, e.g., avoid zero days
- Risks on the reporters
- Misaligned incentives
- How people benefit from reporting?

Platform Security





Mobile Network Operator (MNO)

Handset Original Equipment Manufacturer (OEM)

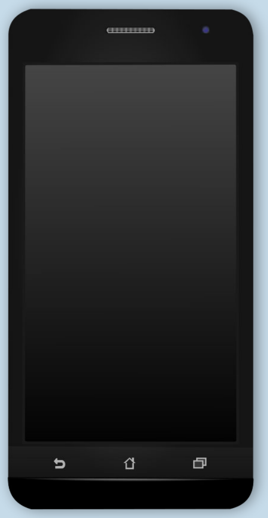
OS Vendor

Chip Maker

Chip Designer

- Security was fragmented along the supplychain
- Device platform design is not heterogeneous

Android platform



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

- Google taking control of the Android ecosystem, but still a lot of vendors!
- Updates propagates from bottom
- Who is incentivized to fix a bug? Most likely Google?

Why is Android free? Where do they make profit from?

Apple platform

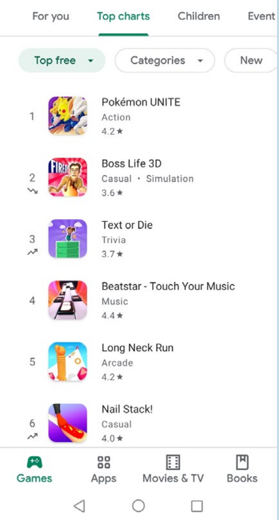
Mobile Network Operator (MNO)	EE
Handset Original Equipment Manufacturer (OEM)	Apple
OS Vendor	Apple
Chip Maker	TSMC/Samsung
Chip Designer	Apple & ARM

- More vertically integrated
- Semi-closed ecosystem
- Apple breaking dependencies on MNO for update
- Longer update coverage due to fewer tussles

Appstores

- ~30% of sales profit shared!
- Bundled and locked in entry point – leaving very few options for app developer
- Making apps more predatory (ad, paying, privacy / identity breach…)

Appstores



For you · Top charts · Children · Event

Top free ▾ · Categories ▾ · New

1 Pokémon UNITE
Action
4.2★

2 Boss Life 3D
Casual • Simulation
3.6★

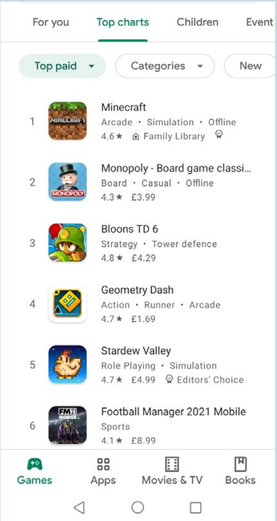
3 Text or Die
Trivia
3.7★

4 Beatstar - Touch Your Music
Music
4.4★

5 Long Neck Run
Arcade
4.2★

6 Nail Stack!
Casual
4.0★

Games · Apps · Movies & TV · Books



For you · Top charts · Children · Event

Top paid ▾ · Categories ▾ · New

1 Minecraft
Arcade • Simulation • Offline
4.6★ Family Library

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

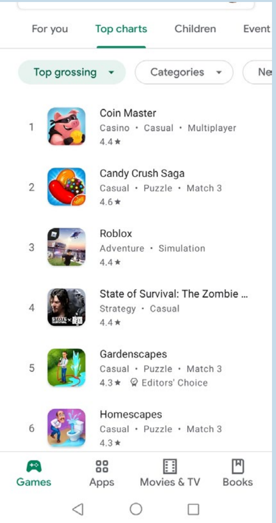
3 Bloons TD 6
Strategy • Tower defence
4.8★ £4.29

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

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

6 Football Manager 2021 Mobile
Sports
4.1★ £8.99

Games · Apps · Movies & TV · Books



For you · Top charts · Children · Event

Top grossing ▾ · Categories ▾ · Ne

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★

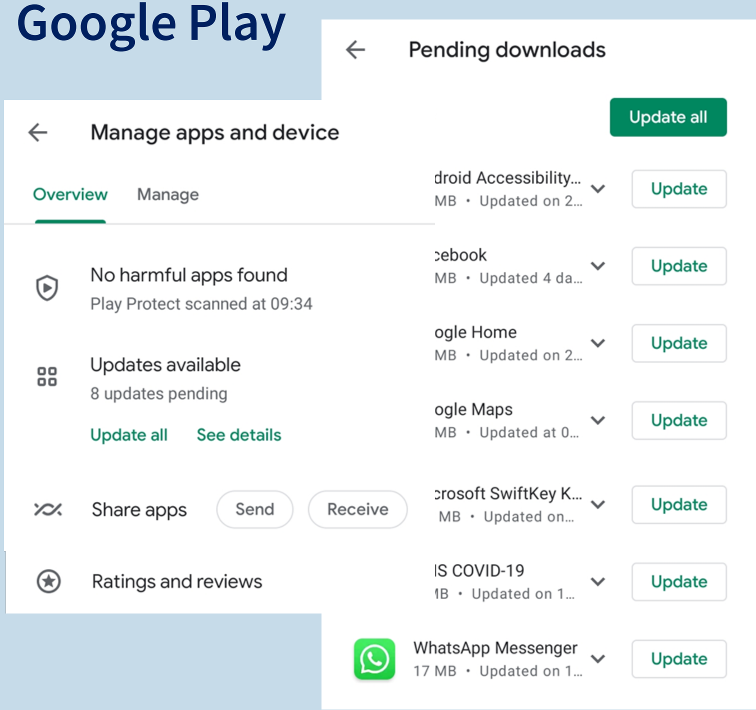
5 Gardenscapes
Casual • Puzzle • Match 3
4.3★ Editors' Choice

6 Homescapes
Casual • Puzzle • Match 3
4.3★

Games · Apps · Movies & TV · Books

- Free download + ad + data theft + microtransaction > paid preminum apps
- No internet access control in Android
- Ads making into the app sandbox, inheriting permissions

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

Update all

droid Accessibility… MB • Updated on 2… Update

cebook MB • Updated 4 da… Update

ogle Home MB • Updated on 2… Update

ogle Maps MB • Updated at 0… Update

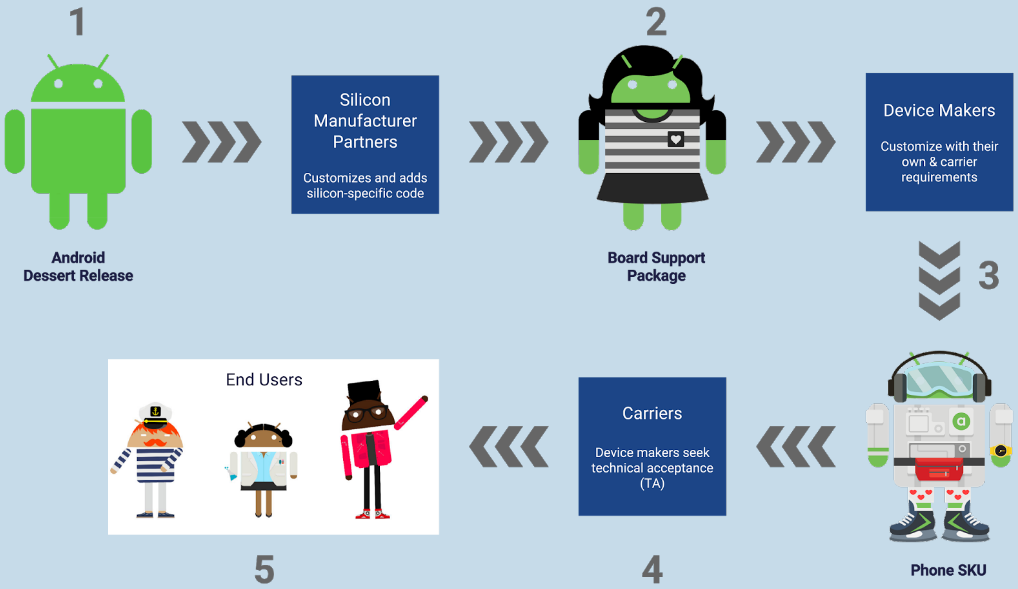
crosoft SwiftKey K… MB • Updated on… Update

IS COVID-19 1B • Updated on 1… Update

WhatsApp Messenger 17 MB • Updated on 1… Update

- Self-signed applications (unlike iOS)
- Default with no "Install Apps from External Sources" – security and lock-in
- App Security Improvement Program scanning whole store for harmful apps
- Suite of Sanitizers for User Code: BoundsSan, AddrSan, IntSan, Shadow Stack, Scudo
- Protecting third-party as well, why?

Android update



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

Carriers

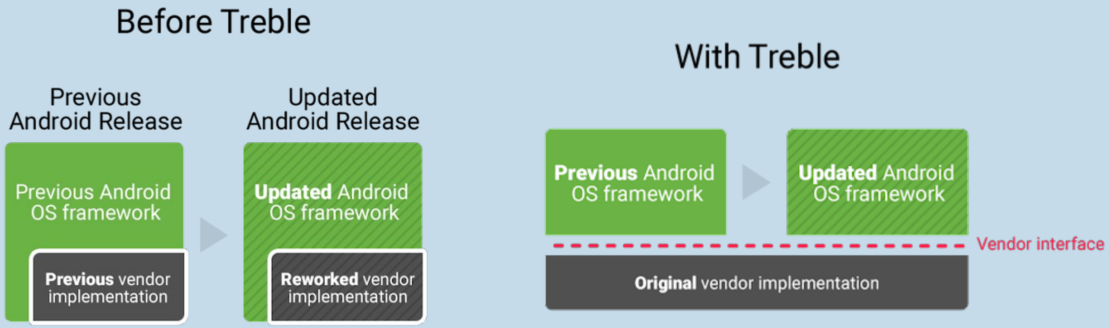
Device makers seek
technical acceptance
(TA)

4

End Users

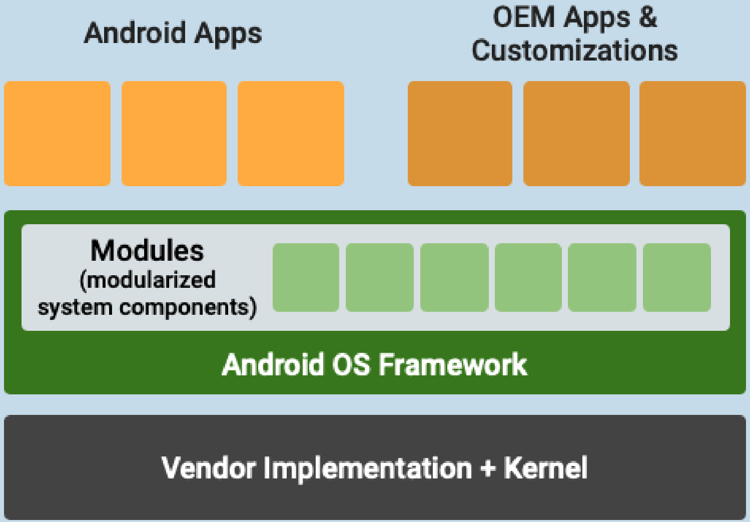
5

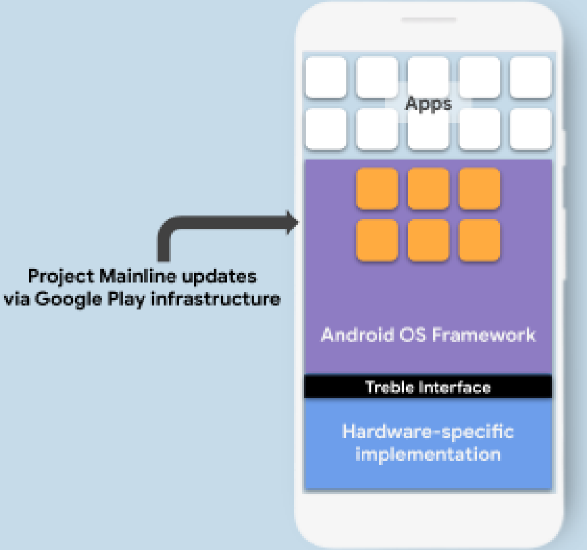
Android update


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

- Making OS implementation modular (isolated)
- Updates still need to push through (OEM) original equipment manufacturer……

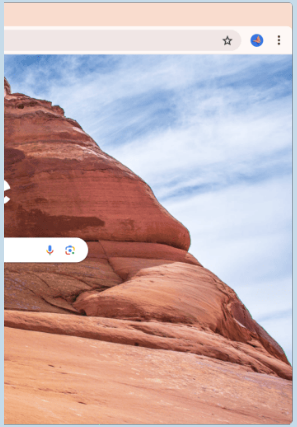
Android update: Mainline

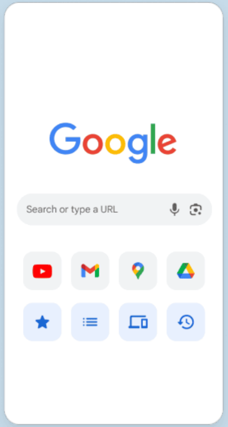

Android Apps
OEM Apps & Customizations
Modules
(modularized system components)
Android OS Framework
Vendor Implementation + Kernel


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

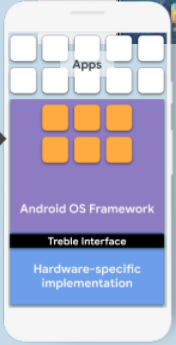
- Further modularization, delivering OS updates through Google Play infrastructure

Takeaway: vendors try to take back control, including security policy and exploits, from others

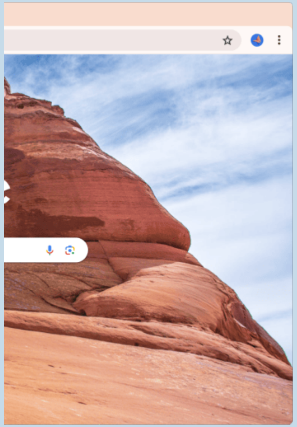


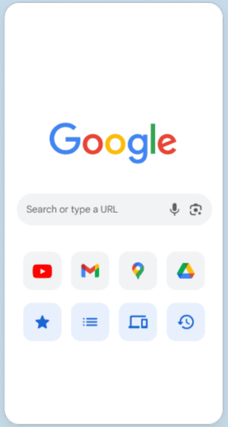


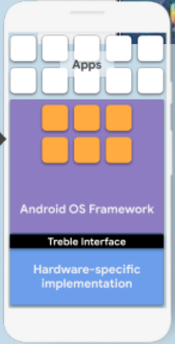
Project Mainline updates via Google Play infrastructure



Think: externalities and internalities for implementing lower-level security policies?

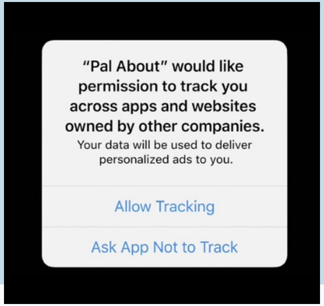






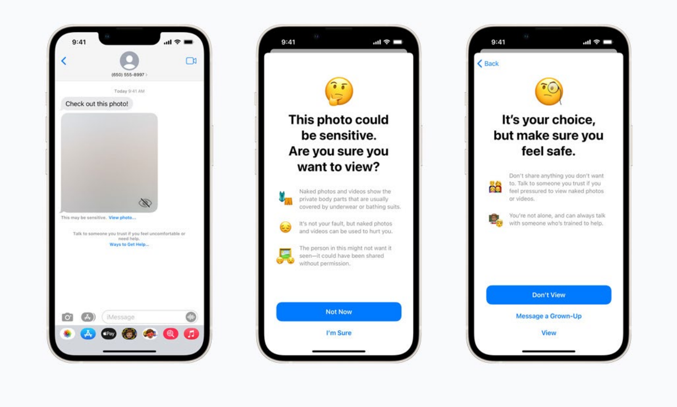
Project Mainline updates via Google Play infrastructure

Apple



"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.



Check out this photo!

This may be sensitive. View photo...

Talk to someone you trust if you feel uncomfortable or need help.

Ways to Get Help...

This photo could be sensitive. Are you sure you want to view?

Naked photos and videos show the private body parts that are usually covered by underwear or bathing suits.

It's not your fault, but naked photos and videos can be used to hurt you.

The person in this might not want it seen—it could have been shared without permission.

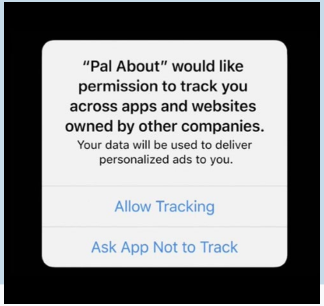
It's your choice, but make sure you feel safe.

Don't share anything you don't want to. Talk to someone you trust if you feel pressured to view naked photos or videos.

You're not alone, and can always talk with someone who's trained to help.

- (Semi)-closed ecosystem, apps signing by apple. Positioning as the company of privacy
- What is the incentive for Apple's third-party app opt out?
- Security claim vs reality?
- Largely closed source – there is obscurity, but is it part of the security?

Apple

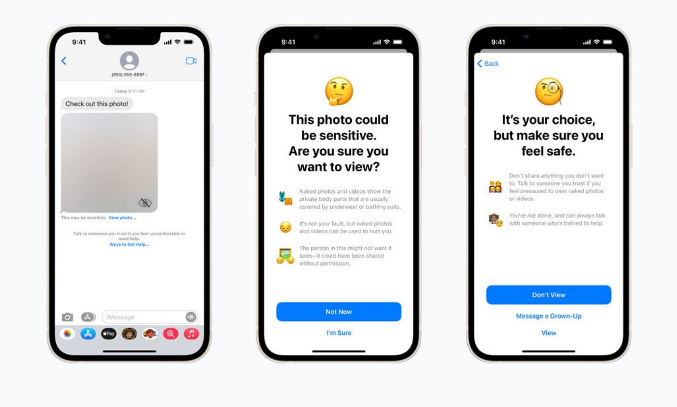


"Pal About" would like permission to track you across apps and websites owned by other companies.

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

Allow Tracking

Ask App Not to Track



Check out this photo!

This may be sensitive. View photo...

Talk to someone you trust if you feel uncomfortable or need help.

Ways to Get Help...

This photo could be sensitive. Are you sure you want to view?

Naked photos and videos show the private body parts that are usually covered by underwear or bathing suits.

It's not your fault, but naked photos and videos can be used to hurt you.

The person in this might not want it seen—it could have been shared without permission.

Not Now

I'm Sure

It's your choice, but make sure you feel safe.

Don't share anything you don't want to. Talk to someone you trust if you feel pressured to view naked photos or videos.

You're not alone, and can always talk with someone who's trained to help.

Don't View

Message a Grown-Up

View

- (Semi)-closed ecosystem, apps signing by apple. Positioning as the company of privacy
- What is the incentive for Apple's third-party app opt out?
- Security claim vs reality?
- Largely closed source – there is obscurity, but is it part of the security?
  - Incentivization of fixing things aligns due to vertical integration
  - Hard to vet though

Microsoft

- Compatibility slows things down, and Windows App market fails
- Start fresh with Azure Cloud (hardware + software)
- Azure Security Centre: Compliance reporting, threat modelling, crypto standards, managing risks of 3rd-party components, pen testing