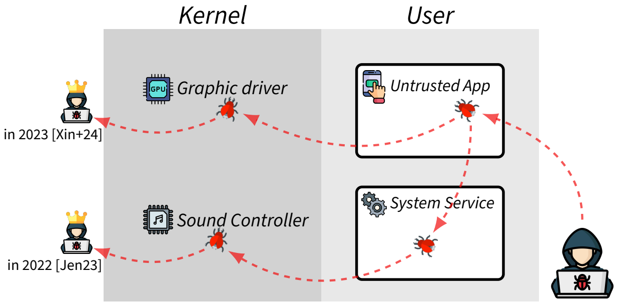
The Doom of Device Drivers:

Your Android Device (Most Likely) has N-Day Kernel Vulnerabilities

Lukas Maar[1] Florian Draschbacher[1,2] Lorenz Schumm[1] Ernesto Martínez García[1]
Stefan Mangard[1]

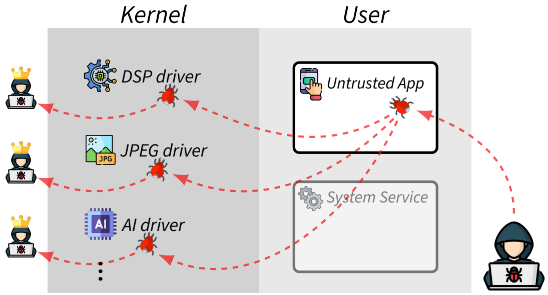
SCIENCE
PASSION
TECHNOLOGY

Prior End-to-End Device Compromises



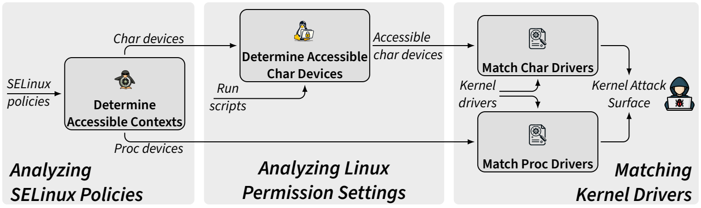
Prior Android device compromises typically began by exploiting vulns in user-facing apps, e.g., messengers. They then chained vulns to escalate privileges, typically pivoting to system before attacking the kernel [Jen23]. Others targeted the minimal kernel attack surface, mainly GPU drivers [Xin+24]; 4 of 5 in 2023 exploited GPU bugs [SSS24].

High-Level Overview



We analyze alternative kernel drivers as equally—if not more—critical exploit targets than from GPUs. We set the following criteria:
(C1) Accessibility: Accessible from untrusted security contexts.
(C2) Broad Impact: Affect a wide range of Android devices.
(C3) Susceptibility: Contains exploitable vulnerabilities.
Crucially, concurrent work [Int24; Int25; Jen24] demonstrated that the DSP driver has been exploited in the wild.

Attack Surface Analysis of Android Kernels



To satisfy **(C1)**, we analyze device firmwares, finding kernel drivers accessible to the untrusted security context.

Analysis of N-Day Driver Vulnerabilities

```
commit 29cbad25d9bf36341131dcc7dfff75b4255d2111
Author: Abhishek Singh <quic_abhishes@quicinc.com>
Date:   Fri Jun 21 16:04:09 2024 +0530

    dsp-kernel: Do not search the global map in the process-specific list

    If a user makes the ioctl call for the fastrpc_internal_mmap with the
    global map flag, fd, and va corresponding to some map already present
    in the process-specific list, then this map present in the process-
    specific list could be added to the global list. Because global maps
    are also searched in the process-specific list. If a map gets removed
    from the global list and another concurrent thread is using the same
    map for a process-specific use case, it could lead to a use-after-free.
    Avoid searching the global map in the process-specific list.
```

To satisfy **(C2)**, we use public data (e.g., git history or bug reports) to identify n-day vulns in these drivers and show they impact many devices.

Detecting N-Day Patches in Kernel Drivers

OEM	All Devices Analyzed		Devices with Target Drivers	
	Crit Vuln	Any Vuln	Crit Vuln	Any Vuln
	%	%	%	%
Samsung	45.5	45.5	74.1	74.1
Xiaomi	67.3	71.4	75.0	79.5
Asus	75.0	100.0	75.0	100.0
Realme	56.2	62.5	56.2	62.5
Vivo	40.0	40.0	40.0	40.0
Oppo	42.9	42.9	42.9	42.9
OnePlus	85.7	85.7	85.7	85.7

To satisfy **(C3)**, we perform a patch inclusion analysis and show that 59.1 % of recent Android devices are affected by unpatched, highly critical n-day driver vulns (i.e., UAF and OOB write), with 61.4 % affected by vulns of any severity (including OOB read and DOS).

Key Findings

(1) Clustering: Devices vulnerable to 1 n-day vuln are often vulnerable to many.
(2) Replacement: Vulns are often fixed via new device models than updates.
(3) Delay: Patch times can exceed a year, varying by OEM, ODM, and vuln type.
(4) Reuse: PoCs for ODM driver vulns work across OEMs and timeframes.
(5) Exploit: Malicious actors can weaponize n-day vulns, avoiding costly zero-days.

Contact

Lukas Maar
lukas.maar@tugraz.at
https://lukasmaar.github.io
https://github.com/lukasmaar

Bibliography

[Int24] Amnesty International. **"A Digital Prison": Surveillance and the suppression of civil society in Serbia**. 2024.

[Int25] Amnesty International. **Cellebrite zero-day exploit used to target phone of Serbian student activist**. 2025.

[Jen23] Seth Jenkins. **Analyzing a Modern In-the-wild Android Exploit**. 2023.

[Jen24] Seth Jenkins. **The Qualcomm DSP Driver - Unexpectedly Excavating an Exploit**. 2024.

[SSS24] Maddie Stone, Jared Semrau, and James Sadowski. **We're All in this Together: A Year in Review of Zero-Days Exploited In-the-Wild in 2023**. 2024.

[Xin+24] Xuan Xing et al. **Google & Arm - Raising The Bar on GPU Security**. 2024.

[1] Graz University of Technology [2] A-SIT Austria