What specific technical vulnerabilities in US consumer tech allow for unauthorized tracker removal by government?

April 19, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

Unauthorized tracker removal in US consumer technology is primarily enabled by deep-seated technical vulnerabilities, including intentional hardware manipulations during manufacturing, firmware backdoors, and processor-level exploits. These vulnerabilities, often introduced through supply chain interdiction, create persistent and difficult-to-detect access points that allow for remote system control, data removal, and the termination of security agents. While security frameworks like FIPS 140-3 and Secure Boot offer protections, they are often insufficient against sophisticated physical and kernel-level attacks, leaving millions of existing devices vulnerable.

Key Findings

Hardware-Level Vulnerabilities and Supply Chain Interdiction

Hardware-level manipulations and Trojans provide a permanent and difficult-to-detect mechanism for unauthorized data removal because they are "baked into the physical silicon" and often require physical component replacement for remediation [2]. Intentional microchip manipulations during manufacturing allow for remote access to remove data or shut down systems [2]. This includes hardware Trojans in printed circuit boards (PCBs) introduced through the supply chain or manual methods like soldering [2]. Supply chain interdiction, which involves pre-delivery modification of hardware components or firmware, is considered a more unmitigable threat than "in-the-field" attacks due to the physical permanence of these modifications [2].

Processor-Level and Firmware Exploits

Vulnerabilities in modern microarchitectures, such as the "Orc attack" on RISC-V and the "Sinkhole" vulnerability in AMD processors, enable the installation of persistent malware

and unauthorized memory access [3, 11]. Speculative execution flaws like Spectre and Meltdown also allow unauthorized memory access [3, 12]. Firmware backdoors, often introduced via shared manufacturer code in IoT and embedded devices, provide persistent access [2]. Additionally, bootkits like BlackLotus can bypass Secure Boot to provide nearly undetectable system control [6].

Kernel-Level Control and Attestation Bypass

Achieving kernel-level privileges is a critical step for unauthorized tracker removal, as it allows attackers to terminate security monitoring processes and software [15, 16, 17]. The "Bring Your Own Vulnerable Driver" (BYOVD) technique exploits this by loading cryptographically valid, digitally signed, but vulnerable or revoked drivers into the kernel [18]. For example, in a 2026 incident, attackers used the `EnPortv.sys` EnCase forensic driver, which had a certificate revoked in 2010, to gain kernel-mode execution [18]. The Windows kernel does not check Certificate Revocation Lists (CRLs) during the driver load process, enabling this bypass [18]. This driver utilized an IOCTL function, `KillProc` (0x223078), to terminate processes with `PROCESS_TERMINATE` access, bypassing user-mode protections like Protected Process Light (PPL) that shield security agents [18].

Runtime manipulation tools like Magisk or Frida can bypass hardware-backed attestation APIs, such as Apple's App Attest and Google's Play Integrity, by altering device states after the boot process [15, 16, 17]. Specific vulnerabilities, such as CVE-2023-42824, serve as tools to bypass these attestation mechanisms [15, 16, 17]. Kernel-mode execution, potentially achieved through GPU driver exploitation, can also facilitate bypassing the isolation boundaries of Trusted Execution Environments (TEEs) like ARM TrustZone [13, 15, 17]. Furthermore, "elastic kernel object" vulnerabilities can bypass Kernel Address Space Layout Randomization (KASLR) and heap cookie protectors, providing arbitrary kernel read capabilities [2, 8, 13, 16].

Limitations of Current Security Frameworks

Existing security frameworks struggle to prevent unauthorized government access due to the inherent difficulty in patching hardware and firmware vulnerabilities [2]. The FCC's "Covered List" targets new, high-risk foreign-made communication equipment, but it leaves millions of existing, unsecured, foreign-produced routers and IoT devices unaddressed [2, 4, 10]. These legacy devices represent a high risk as they can serve as

entry points for unauthorized network access and espionage [2, 4, 10].

While security certifications like FIPS 140-3 provide a framework for protecting cryptographic modules, they may have a scope gap regarding certain hardware-level modifications [4, 11, 13, 14]. FIPS 140-3 Level 4 offers robust environmental protection and the ability to destroy private keys if an attack is detected [9, 14, 17]. However, even highly secure processors can remain vulnerable to sophisticated physical exploits like side-channel attacks (e.g., electromagnetic analysis, voltage glitching, laser exposure) that bypass internal security measures [4, 9, 11, 13]. Detecting tampering at the circuit board level remains challenging due to supply chain complexity [2, 5].

Secure Boot and Trusted Platform Module (TPM)-based platform integrity verification, while designed to prevent unauthorized software execution and verify platform integrity during boot, are not entirely sufficient to detect all unauthorized hardware modifications [1, 7, 16]. Modern supply chains are inherently vulnerable to the insertion of counterfeit components and unauthorized modifications [1, 2, 5, 16]. While SBOM and HBOM frameworks increase transparency, they do not inherently detect unauthorized structural or component tampering [2, 5].

Implications

The prevalence of hardware-level vulnerabilities, firmware backdoors, and kernel-mode exploits means that US consumer technology faces a persistent and evolving threat of unauthorized tracker removal by government actors. The deep integration of these vulnerabilities, often at the manufacturing stage or through sophisticated supply chain interdiction, renders many traditional software-based security measures ineffective. The inherent difficulty in patching hardware flaws, which frequently require physical component replacement, creates long-term access points that are challenging to remediate.

Current regulatory efforts, such as the FCC's "Covered List," primarily address new equipment, leaving a significant installed base of legacy devices vulnerable to exploitation. This gap allows for continued unauthorized access to millions of consumer devices, particularly unsecured routers and IoT products. Furthermore, even advanced security certifications like FIPS 140-3 and hardware-backed attestation mechanisms can be bypassed by sophisticated physical attacks, side-channel exploits, or kernel-level

runtime manipulations. The ability of attackers to load vulnerable, signed drivers to gain kernel-mode control, even when certificates are revoked, highlights a fundamental weakness in OS-level protections. This implies that a multi-layered defense strategy must extend beyond software and cryptographic modules to include rigorous physical security, continuous monitoring for microarchitectural anomalies, and a comprehensive approach to supply chain integrity that accounts for both pre-delivery and post-deployment threats.

Limitations and Caveats

This report synthesizes findings from the provided research, which offers a snapshot of technical vulnerabilities. It does not provide specific cost-benefit projections or implementation timelines for integrating advanced verification methods like HBOM into CI/CD pipelines. The research also does not explicitly identify which manufacturer-specific hardware features (e.g., Apple's Secure Enclave, Google's Titan M2) are "most" susceptible to "in-the-field" attacks, beyond general statements that hardware can be compromised post-deployment. Additionally, the report does not detail specific industry-standard testing methodologies that should be mandated alongside FIPS 140-3 certification to verify tamper-resistance against state-level actors, nor does it mention specific Common Criteria Security Profiles for high-assurance components. The quantitative impact of "Attestation of Origin" protocols like IETF RATS on reducing undetected component tampering was also not covered.

Sources

[1] Irs Sets Tracking Device Policy House Oversight Report Says - taxnotes.com - https://www.taxnotes.com/research/federal/legislative-documents/congressional-committee-reports/irs-sets-tracking-device-policy-house-oversight-report-says/gc3b

[2] [peer-reviewed] Article - sciencedirect.com - AUTHORS UNAVAILABLE - https://www.sciencedirect.com/science/article/pii/S2542660523002111

[3] 91 Of Americans Concerned About Backdoor Data Access - thepaypers.com - https://thepaypers.com/fraud-and-fincrime/news/91-of-americans-concerned-about-backdoor-data-access

[4] Study Notes - cliffsnotes.com - https://www.cliffsnotes.com/study-notes/20329693

[5] Item - news.ycombinator.com - https://news.ycombinator.com/item?id=39244254

[6] [blog] Lhardware Vulnerabilities The 88 Surge In Physical Device Ex - medium.com - https://medium.com/@instatunnel/lhardware-vulnerabilities-the-88-surge-in-physical-device-exploits-271d936d6370

[7] Hardware Attacks - searchinform.com - https://searchinform.com/articles/cybersecurity/cyber-threats/cyber-attacks/hardware-attacks/

[8] [peer-reviewed] A Review of IoT Firmware Vulnerabilities and Auditing Techniques - Authors: Taimur Bakhshi; Bogdan Ghita; Ievgeniia Kuzminykh - Journal: Sensors (Basel, Switzerland) -

https://pmc.ncbi.nlm.nih.gov/articles/PMC10821153/

[9] [edu] Supply Chain Interdiction The Mysterious Case Of Exploding P - scm.ncsu.edu - https://scm.ncsu.edu/scm-articles/article/supply-chain-interdiction-the-mysterious-case-of-exploding-pagers

[10] [edu] PdfCoverPage - verso.uidaho.edu - https://verso.uidaho.edu/view/pdfCoverPage?instCode=01ALLIANCE_UID&filePid=13308673780001851&download=true

[11] Introduction To Trusted Execution Environment And Arms Trust - embeddedbits.org - https://embeddedbits.org/introduction-to-trusted-execution-environment-and-arms-trustzone-embeddedbits/

[12] Techniques - attack.mitre.org - https://attack.mitre.org/techniques/T1474/002/

[13] [edu] Tamper - cl.cam.ac.uk - https://www.cl.cam.ac.uk/archive/rja14/tamper.html

[14] [preprint] Html - arxiv.org - AUTHORS UNAVAILABLE - https://arxiv.org/html/2501.04394v1

[15] Reports - rand.org - https://www.rand.org/pubs/reports/R609-1.html

[16] [blog] Security Mitigations - tuxcare.com - https://tuxcare.com/blog/security-mitigations/

[17] Why Is Common Criteria Security Certification Useful And Wha - embeddedcomputing.com - https://embeddedcomputing.com/technology/security/why-is-common-criteria-security-certification-useful-and-what-do-the-eal-levels-mean

[18] [edu] STUDY OF PRIVILEGE ESCALATION ATTACK ON ANDROID AND ITS COUN - academia.edu - https://www.academia.edu/4354312/STUDY_OF_PRIVILEGE_ESCALATION_ATTACK_ON_ANDROID_AND_ITS_COUNTERMEASURES