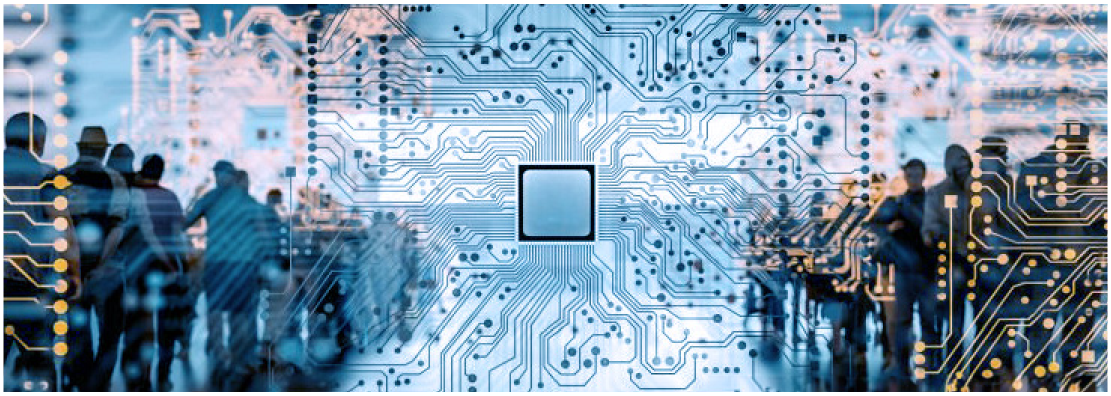
# Making your phone invisible to tracking is harder than you think

If you're at all familiar with action movies or TV shows, you've probably encountered a scene involving a character – perhaps a special agent or a fugitive on the run – removing the batteries from their burner phone or even snapping their device in half to avoid tracking. Simple as it may seem in films, real-world smartphones lack a foolproof method to disable tracking. Given this gap, we set out to design a solution to ensure our devices keep our lives private.

## "Off" doesn't always mean off

Tucked into every smartphone are radios that enable the device to access the internet, communicate with other devices, know its exact location and more. Four key radios – cellular, WiFi, Bluetooth, and GPS – power essential location-based features like mapping.

Unfortunately, the software-based nature of current smartphone radio controls exposes them to exploitation by threat actors armed with spyware. Software vulnerabilities allow attackers three key avenues for covert tracking: leveraging unexpectedly active radios, mimicking airplane mode and faking device power-down.



## UNEXPECTED RADIO BEHAVIOR

Numerous cases show that phone radios can remain active even in airplane mode or when powered off, and just one active radio – whether cellular, WiFi, Bluetooth, or GPS – can let an adversary locate your device.

On recent iPhone models, for example, Low Power Mode activates when the device is either switched off or the battery runs low. In this state, tracking features like the Find My service used to locate an iPhone continue to operate. In 2022, researchers from TU Darmstadt showed[1] that Bluetooth, NFC and Ultra-wideband radios remain active in this state, opening the door to stealthy tracking by an attacker with system-level access to the phone or the ability to externally find and track these radios.

## SIMULATED AIRPLANE MODE

With spyware on the phone, attackers can potentially show inaccurate device status on the screen to make it appear that the radios are turned off. Since the radios and the information displayed to the user are both controlled by the operating system, OS vulnerabilities can be exploited to mislead the user and silently track their location.

Researchers from Jamf Threat Labs recently highlighted[2] how airplane mode can be faked by manipulating the code governing airplane mode in iOS 16. In this case, the researchers, with total control of a phone, swapped in dummy code to the underlying network interface, inserted code to dim specific buttons and changed a single database parameter controlling cellular and WiFi access to feign no connection in the Safari web-browsing app. As such, the user is misled into thinking their radios are disabled, when in fact, they are still active.

## SIMULATED POWER-DOWN

Another trick that spyware can pull is simulating a power-down of the phone when the phone is indeed powered on.

One such technique, discovered[3] by researchers from ZecOps, allows an attacker to hijack and prevent any shutdown process that a user initiates, simulating a power-off while allowing spyware to remain active in the background. To achieve this, the researchers injected code into three background processes, including the one responsible for user interactions during the shutdown process. From the user's perspective, the phone looks and feels as if it is not powered on, and yet it remains awake and connected to the internet.

## A tragic scenario

Now that we know how adversaries can stealthily activate the radios inside our phones, let's examine some potential real-world consequences.

Here, our heroine is a well-known journalist working at a newspaper critical of an authoritarian regime. Drawing from published reports like the Pegasus Project and interactions with colleagues, she is well aware that her phone can be invisibly targeted with spyware capable of tracking her location, capturing sensitive conversations through the device's microphones and much more.

Before heading to a meeting with a valuable source, the journalist turns on airplane mode to turn off her phone's radios, assuming this will thwart any tracking attempts. She's unaware her phone has been infected with spyware, which silently uses radios to both determine her real-time location data and then to transmit the data to her attacker.

After the meeting, the attackers use other means – possibly leveraging data from a broker – to identify a list of phones that pinged simultaneously near their meeting location. After narrowing down the likely identity of the source, the attackers harass and physically assault him, ultimately forcing him to recant his comments to the journalist out of fear for his personal safety.

## Waiting for a patch

The grim reality is that, even with perfect digital hygiene or using features like Apple's Lockdown Mode, there's no guaranteed protection against the most advanced forms of spyware and the tracking they enable. Traditionally, a user's best bet has been to rely on vendors identifying and promptly patching vulnerabilities before attackers can exploit them with spyware in the wild.

Even vendors known for timely updates have had their share of security lapses. Apple's recently introduced Rapid Security Responses, for example, still depend on finding the problem before attackers do. In one extreme example, researchers from ZecOps discovered[4] in 2020 a critical bug that had affected iPhones and iPads for eight years. There's no guarantee that "the good guys" will spot a vulnerability before it's exploited by malicious parties. Relying on this is an expensive gamble.

## Enter strong-assurance radio controls

To stop stealth tracking, Privoro and Samsung have partnered to develop a hardware-to-hardware integration providing strong assurance that the radios in a user's Galaxy phone are completely disabled. The unique integration utilizes two separate systems: Privoro's SafeCase ONX™ (Onyx), a smart security case with special-purpose computing, and Samsung's Hardware Device Manager (HDM), a Samsung-exclusive security layer built into their latest smartphones.

**SAFECASE ONX™ S23**

AVAILABLE Q2 2024

Both SafeCase and HDM are independent from the phone's OS, and both utilize hardware-based security to provide immunity against spyware and other advanced attacks.
In addition, each radio disconnection (or reconnection) request undergoes

cryptographic verification, ensuring only actions by the true user via buttons on SafeCase are ever activated by Samsung's hardware. Preventing even the OS from changing the radio and sensor state safeguards the user from any spyware that may be on the device. Recognizing that no phone is impervious to software bugs, the two-system architecture fortifies against such inevitable vulnerabilities, providing a hardware safeguard that prevents these weaknesses from being exploited altogether.

In fact, an attacker who has successfully implanted spyware on the phone can't even interact with SafeCase to attack it. SafeCase doesn't support running external code, which means there are no apps and no chance for malware. So, to override the user's selections for radio states, an adversary would need to not only hack Android, but independently synchronize physical attacks on Samsung HDM hardware controls *and* the physically separate system on SafeCase itself.

## A tragic scenario, revisited

Let's go back to the journalist with the spyware-infected phone. Now armed with SafeCase and HDM, she securely disables her phone's radios before meeting with a source. After pressing a button on SafeCase to disable the phone's radios, SafeCase creates a new policy update, then pushes the update to her phone, where HDM ultimately verifies the integrity of the radio request and disconnects the radios. Attackers monitoring her are left in the dark, unable to see why they're not receiving location data and unable to determine where she is. Any future attempts to use spyware on her phone also fail; the spyware can't stealthily turn on radios that she has explicitly disabled using SafeCase. To the phone and its operating system, these radios and sensors effectively no longer exist.

She now can meet with and protect the confidentiality of her source, preventing their exposure and allowing her to successfully publish her exposé on the authoritarian regime.

While fully aware of the persistent threat of spyware and her status as a high-value target, the journalist now rests a bit easier. She has a secret weapon that gives her the confidence to know she's effectively untraceable.

**SOURCES**

1. Kovacs, Eduard, "Hackers Can Abuse Low-Power Mode to Run Malware on Powered-Off iPhones," SecurityWeek, May 16, 2022.
2. Nelson, Nate, "Researchers Trick an iPhone Into Faking Airplane Mode," Dark Reading, August 17, 2023.
3. Seals, Tara, "Apple iPhone Malware Tactic Causes Fake Shutdowns to Enable Spying," Threatpost, January 6, 2022.
4. Goodin, Dan. "A critical iPhone and iPad bug that lurked for 8 years may be under active attack," Ars Technica, April 22, 2020.