Galaxy-SafeCase is the ultimate Zero Trust endpoint

Introducing next-level damage containment via off-device hardware isolation

To meet ambitious goals for realizing Zero Trust (ZT), Federal organizations require new endpoint capabilities for limiting damage in the event of device compromise. A powerful new hardware-to-hardware approach between Samsung's Galaxy phones and Privoro's SafeCase security devices represents a path forward for achieving ZT at the endpoint level. By using two separate systems, both of which are effectively independent from the phone's operating system (OS) and based in hardware, key security functions are isolated from the commercial OS and therefore are out of reach of an assumed compromise. A key use case of this approach is the ability to mitigate the active espionage risk of mobile devices.

A "two-man rule" for mitigating active espionage

Imagine that an adversary wants access to the US military's nuclear arsenal. First, the adversary will need to gain illicit entry into a launch control center by getting past physical security, the "gates, guards and guns" protecting the building. This will be no small feat, but once achieved, the adversary will not be able to simply walk up and press a big red "Launch" button – more authorization is needed. Part of this Zero Trust approach is the "two-man rule," whereby two separate keys must be engaged simultaneously by two different people for a launch to take place. So even if the adversaries achieve access to the launch control center, they will still need to find the two keys in two separate locations to engage the weapons.

A similar ZT logic drives the Galaxy-SafeCase solution.

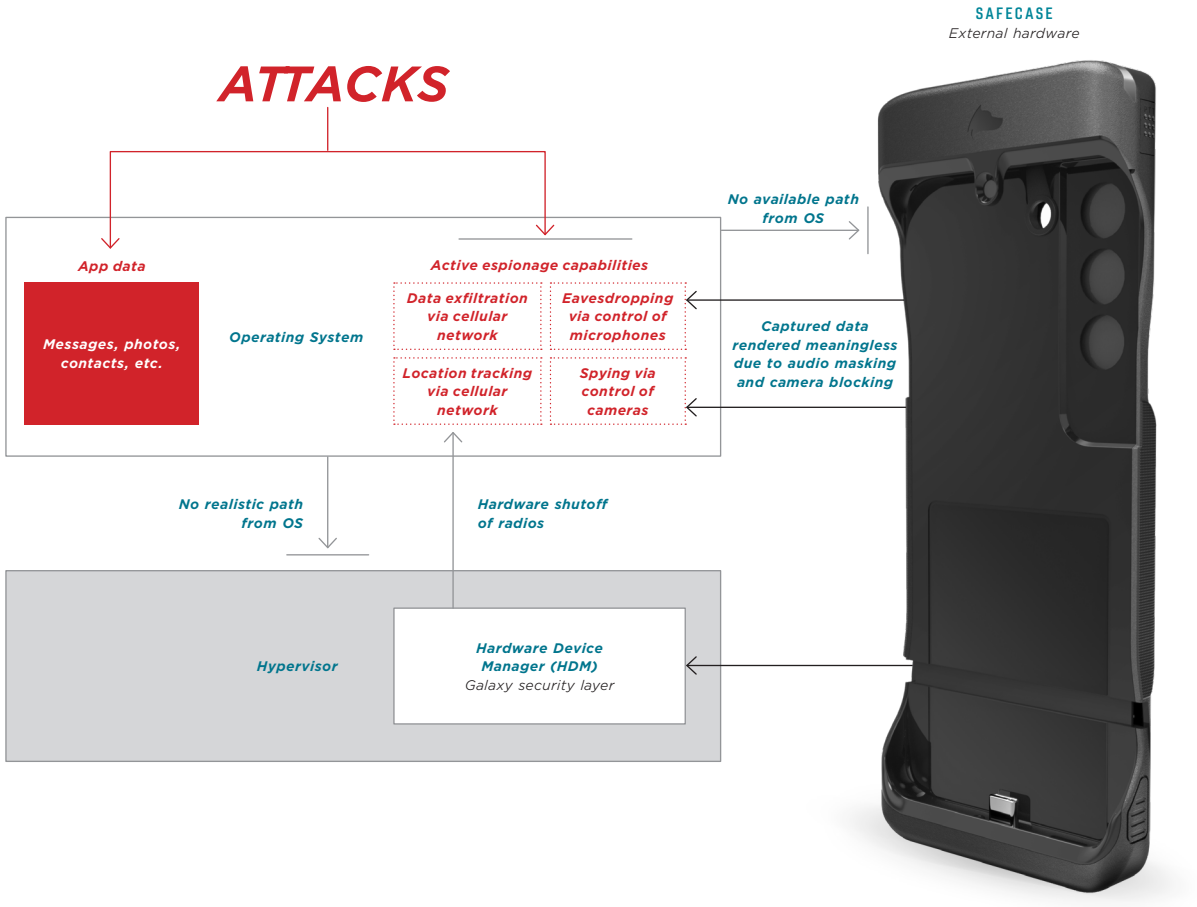
An attacker looking to leverage a targeted mobile device for active espionage first needs to compromise the phone to gain access to the device. To achieve this access, adversarial nation-states and other well-resourced attackers employ spyware and similar advanced attacks that exploit vulnerabilities in the OS or in the firmware of a specific component, such as the cellular radio. New capabilities for compromising smartphones are regularly devised, with many sophisticated attacks available for purchase to almost anyone with adequate funds.

SAMSUNG | PRIVORO®

As it stands today, a threat actor who has compromised the OS has full control over the device's hardware components, overriding the user's selections within OS controls or the organization's peripheral policies enforced via mobile device management (MDM) software. Crucially, the device's cameras and microphones can be hijacked to look in on and listen to a targeted individual's environment, while the wireless radios can be leveraged for data exfiltration.

The Galaxy-SafeCase solution acknowledges the vulnerability in software-only controls, employing hardware isolation to reduce the potential damage of security incidents. In the event that the phone's OS is compromised, an attacker doesn't have any visibility into the other two systems needed to perform active espionage. One of these systems, Samsung's Hardware Device Manager (HDM), is on the device but "under" the OS (i.e., with a higher privilege level than the OS). The other system, Privoro's SafeCase, is outside the device entirely. In effect, there isn't a feasible way to punch from the compromised OS down to HDM or out to SafeCase.

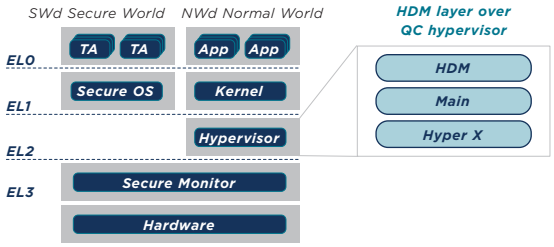
This means that an attacker looking to perform active espionage would need to independently compromise HDM and SafeCase, exponentially increasing the difficulty of attack. And because there are two separate hardware manufacturers involved, there is no overlap between codebases or system architectures that would facilitate compromise of one system in the unlikely event that the other system is compromised.



The two-system approach

The two-system approach between Galaxy and SafeCase effectively marries consumer and government technology, resulting in a system that is both highly capable and highly secure. Galaxy provides the third-party architecture hosting powerful apps, while SafeCase provides the necessary data protections against a nation-state threat model.

SafeCase is a first-of-its-kind security device for mobile devices that's designed to be functionally independent of the regulated phone. It provides two main capabilities: anti-surveillance and special-purpose computing. To combat surveillance, SafeCase blocks the phone's cameras and masks ambient audio before it reaches the phone's speakers, in effect rendering meaningless any captured audio and video. The special-purpose computing system enables unique security functions, one of which is the ability to cryptographically sign peripheral policy updates and pass them to Galaxy's HDM.



HDM is a Samsung-exclusive security layer running in hardware, below the OS. It gates access to physical sensors (cameras and microphones), communication chips (cellular, WiFi, Bluetooth and NFC) and other peripherals (USB, speaker and GPS). HDM leverages cryptographic controls to verify that signed policy updates are authentic before implementing them via the hypervisor. It can even trigger automatic physical lockout of peripherals upon detection of device compromise or device rooting (i.e., the gaining of full privileges).

SafeCase maximizes the effectiveness of HDM by placing the policy decision point outside of the commercial device and its OS. Because mobile policy decisions and signing originate in SafeCase and then effectively bypass the phone's OS via HDM, they are protected from manipulation via any spyware that may be on the device. And even if the attacker were able to somehow manipulate a policy update, it would not pass HDM's cryptographic verification.

SafeCase only interfaces with Galaxy via an Android app on the phone and a Bluetooth Low Energy (BLE) connection to the app. However, because the ZT security model assumes that the phone's OS is compromised, these elements are not used for trusted purposes. The app piggybacks on the phone's untrusted data channel by creating a secure tunnel through it, enabling reporting and monitoring via the cloud. The BLE connection provides user interface functions, letting users view SafeCase connection status and battery level through the app. The HDM integration also uses this channel for passing signed, encrypted policy updates from SafeCase to HDM.

GALAXY S22®
AVAILABLE NOW

Hardware-based security

In addition to their independence from the phone's OS, both SafeCase and HDM utilize hardware-based security to provide immunity against spyware and other advanced attacks, strengthening the ZT model.

SafeCase has its own hardware root of trust – an unalterable, cryptographically secure foundation for the services built on top of it, including the initiation of policy updates. Unlike a traditional computing device, which is designed to run third-party code, SafeCase has a closed system that only runs firmware that has been developed and cryptographically signed by Privoro. Other measures, like strict supply chain controls and manufacturing within a protected facility in the United States, strengthen the device's security posture. The result is a small attack surface providing minimal opportunities for exploitation.

Samsung's HDM runs in a security-enhanced hardware area. It saves policies in secure storage, ensuring that a policy cannot be modified anywhere other than HDM. HDM also uses its own unique, hardware-backed key to prove its identity, creating a cryptographic foundation for all policy processing. Importantly, HDM is loaded before the kernel (the critical security center of the OS) in the secure boot process, which is the chain of trust that begins when the phone is powered on and ensures that each component is cryptographically validated before being loaded. As such, policy updates are enforced before the OS even loads, meaning that a compromised OS cannot override the policy.

A future-focused foundation

In addition to providing trusted control over hardware components, Galaxy and SafeCase both support other capabilities driving Zero Trust.

Galaxy, through its Samsung Knox platform, supports the key principles of ZT endpoint security, including the evaluation and protection of user and device contexts and regulated access to enterprise resources. It does so by enabling features like continuous multifactor authentication (CMFA), continuous monitoring of endpoint security, context-based access and fine-grained access control.

Similarly, the special-purpose computing system of SafeCase can support off-device hardware isolation for additional security-critical processes, such as identity/authentication, private key storage and related services.

Importantly, continuous monitoring employed by both two systems provides a redundancy critical to ZT, whereby device state is checked by both systems. This redundancy provides high assurance that the device is being used in accordance with defined policy – for example, that a user cannot turn on their phone's cellular radio while in a secure space.

The result is a strong foundation for incorporating current and future ZT capabilities into the enterprise.

SafeCase trials are underway across the Federal government.
Let's create a custom game plan for driving your organization forward.

Learn more **privoro.com**
Initiate a trial **sales@privoro.com**