Samsung KNOX boot-time protections

Secure Boot and Trusted Boot

When a device is first turned on, the user's apps are not immediately available. First, a chain of software components is started, with each component starting the next one in the chain. Once the hardware is powered on, it first runs a program called a bootloader, which in turn runs the operating system's kernel, a highly privileged component that starts applications and can access storage and network devices directly.

Many device vendors support a process known as Secure Boot, and Samsung KNOX devices are no exception. In a Secure Boot process, each component in the boot chain (bootloader, kernel, etc.) checks the integrity of the next component through signature verification. If the signature verification fails, the boot process is stopped.

Secure Boot is limited because it cannot distinguish between different *approved* versions. For example, Secure Boot cannot tell the difference between a bootloader with a known vulnerability and a later patched version, since both versions have valid signatures. To address this limitation, Samsung KNOX adopts Trusted Boot in addition to Secure Boot. In the Trusted Boot process, each software component in the chain measures and securely stores the cryptographic hash of the next component in TrustZone Secure World memory before loading it. Storing these measurements allows a third-party to identify the exact versions of software loaded on the device through the process of attestation. For example, this can be used to verify that only the latest patched versions of software are run, complementing the *Rollback Prevention feature that ensures patched software is not downgraded to a vulnerable version.*

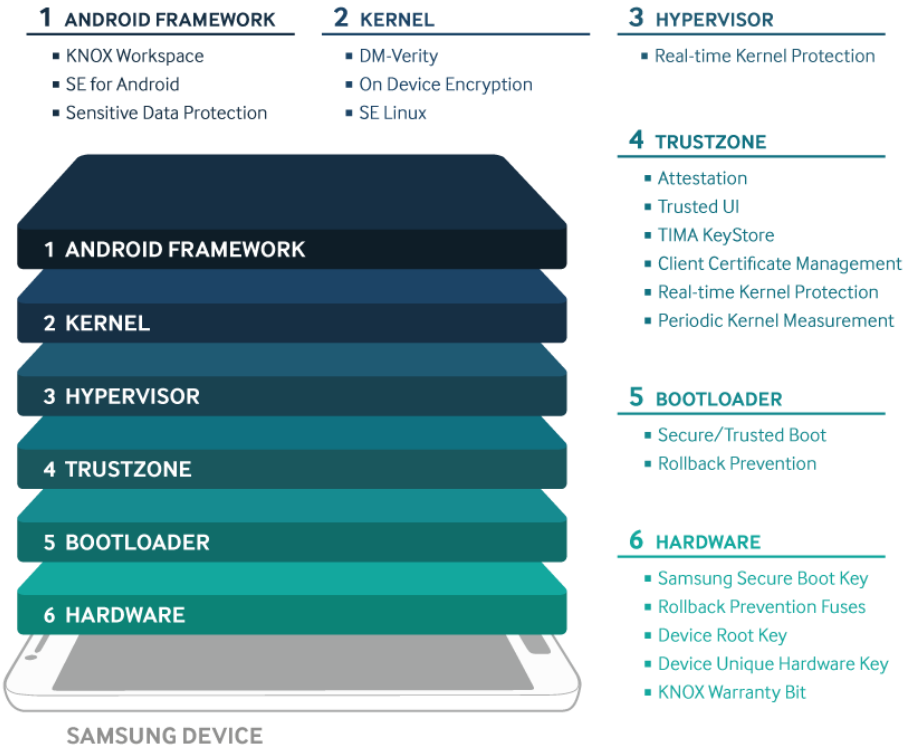
If signature verification fails, KNOX either records the tampering by blowing a one-time fuse, called the KNOX warranty fuse, or by preventing further booting, depending on the configuration. Devices that have the fuse set cannot run certain KNOX features such as the KNOX Workspace thereafter.

Both Secure Boot and Trusted Boot have their trust rooted in hardware. The first piece of software loaded is the primary boot loader, which is kept in hardware-protected Read-Only Memory (ROM). In addition, the cryptographic key used to verify signatures is the Samsung Secure Boot Key, also stored in hardware fuses.

Rollback Prevention (RP)

Rollback Prevention blocks the device from loading or flashing an approved but old version of boot components. **Old versions of software may contain known vulnerabilities that attackers can exploit.** Rollback prevention checks the version of the bootloader and kernel during both boot and updates, and blocks these processes from continuing if versions are unacceptably old. The lowest acceptable version of the bootloader is stored in secure hardware fuses when the device is flashed, and the lowest acceptable version of the kernel is stored in the bootloader itself. Whenever a vendor-applied update occurs, the lowest acceptable version can be incremented in the fuses. Because this value is kept in fuses, it cannot be decremented even through physical tampering.

Rollback Prevention fuses are set at manufacturing time in the Samsung factory to prevent old firmware versions from overwriting newer ones.



Samsung KNOX Architecture Overview