Hardware Root of Trust

Unsecured mobile devices pose a great threat to the safety of personal or enterprise data. Fortunately, Knox provides software to protect against hackers who want to access your sensitive data.

But, software can be replaced or modified, so how can Knox be trusted? The foundation of Knox security is something called *Hardware Root of Trust*. This means that the security checks are *rooted in*, or *begin with* hardware checks. Hardware checks are very reliable and can't be attacked in the way software can. Upon device startup, Samsung uses hardware as a basis for checking all software components. The software performs a check on each Knox feature before allowing it to run. Since this *chain of security checks* begins with the very first hardware check, each feature is protected by hardware root of trust. No matter which link in the chain an attacker targets, one of the security checks will detect it.

When a security check detects an unapproved software change, either the boot process stops or the Knox warranty-fuse is blown. The Knox warranty-fuse, which is built into the device hardware, permanently blocks access to the Knox KeyStore when blown. This prevents any encrypted corporate data on the compromised device from ever being decrypted and revealed. It also means that the device can't be used to encrypt and store enterprise data in the future. The device still runs, but won't be allowed to use most Knox security features since detected modifications have broken our chain of trust.

Hardware Roots of Trust

The following sections describe the hardware components that are the foundation of Samsung Knox's trusted environment.

Device-Unique Hardware Key (DUHK) – The DUHK is a device-unique symmetric key that is set in hardware at manufacture time in the Samsung factory. The DUHK provides a way to bind data to a particular device as follows. The DUHK is only accessible to a hardware cryptography module and is not directly exposed to any software. However, software can request for data to be encrypted and decrypted by the DUHK. Data encrypted by the DUHK becomes bound to the device, because it cannot be decrypted on any other device. The DUHK is typically used to encrypt other cryptographic keys.

Samsung Secure Boot Key (SSBK) – The SSBK is an asymmetric key pair used to sign Samsung-approved executables of boot components. The private part the SSBK is used by Samsung to sign the secondary and application bootloaders. The public part of the SSBK is stored in hardware one-time programmable fuses at manufacture time in the Samsung factory. The Secure Boot process uses this public key to verify whether each boot component it loads is approved.

Rollback Prevention Fuses (RP Fuses) – The RP fuses are hardware fuses that encode the minimum acceptable version of Samsung-approved bootloaders. Old software may contain known vulnerabilities that can be exploited. The rollback prevention feature prevents approved, but out-of-date versions of bootloaders from being loaded. The version number in the RP fuses is set when system software is first installed and later during updates. RP fuses are one-time programmable. Thus, the minimum acceptable version can only be incremented but not decremented.

Knox Warranty Fuse – The Knox warranty bit is a one-time programmable fuse that signifies whether the device has ever been booted into an unapproved state. If the Trusted Boot process detects that non-approved components are used, or if certain critical security features such as SELinux are disabled, it sets the fuse. Thereafter, the device can never run Samsung Knox, access to the DUHK and DRK in the TrustZone Secure World is revoked, and the enterprise's data on the device cannot be recovered.

ARM TrustZone Secure World – The Secure World is a hardware-isolated environment in which highly sensitive software executes. The ARM® TrustZone® hardware enforces that memory and devices that are marked secure can only be accessed in the Secure World. Most of the system as we know it, including the kernel and middleware, as well as all apps, execute in what is called the Normal World. Normal World software can never access the data used by Secure World software. The Secure World software, on the other hand, is more privileged, and can access both Secure and Normal World resources. Knox makes extensive use of the Secure World both for cryptographic operations, and for monitoring Normal World security.

Bootloader ROM – The primary bootloader (PBL) is the first piece of code to run during the boot process. The PBL is trusted to start the measurement and verification of the boot chain. To prevent tampering, the PBL is kept in secure hardware Read Only Memory (ROM). The device hardware loads and runs the PBL from ROM at boot, and the PBL starts the Secure and Trusted Boot processes.

Device Root Key (DRK) – The DRK is a device-unique asymmetric key pair that is signed by Samsung's root key through an X.509 certificate. This certificate proves that the DRK was produced by Samsung. The DRK is generated at manufacture time in the Samsung factory and is stored on the device encrypted by the DUHK, thus binding it to the device. The DRK is only accessible from within the TrustZone Secure World.

Because the DRK is device-unique, it can be used to tie data to a device through cryptographic signatures. The DRK is not used directly to sign data; instead, signing keys are derived from the DRK. As an example, the TIMA attestation data, which proves the device is in a trusted state, is signed using the Attestation Key, which is itself signed by the DRK. The DRK signature proves that the attestation data originated from the TrustZone Secure World on a Samsung device. Note that while the DRK is not stored directly in hardware, it is an important part of the root of trust as it derives other signing keys, and is protected by both the DUHK and TrustZone Secure World.