Titanium Technology Protection

Titanium Secure Boot

Star Lab's Titanium Secure Boot provides the strongest level of boot-time authentication/trust on Intel chipsets, with a simple provisioning process and support for secure software updates.

Titanium Secure Boot goes a step beyond the typical static root/chain of trust measurements used by other Secure Boot capabilities, additionally building a dynamic chain of trust leveraging Intel's Trusted eXecution Technology (TXT). This dynamic component significantly reduces the level of inherent trust placed in the early firmware components involved in the measurement process while also reducing the impact of runtime exploitation of boot-time components (a significant threat). Titanium Secure Boot also leverages the Trusted Platform Module (TPM) for all cryptographic key storage, providing both a hardware root of security and a very straightforward provisioning process for both diskless and diskfull systems.

Additionally, because Titanium Secure Boot measures the initial RAM disk/filesystem and the Linux kernel command line parameters; an attacker cannot subvert or interpose late-load security components by modifying software within the initramfs, disable important security features, or enable system debugging capabilities. With Titanium Secure Boot, measurements (stored in the TPM Platform Configuration Registers or PCRs) are combined to unlock/unseal non-extractable cryptographic key material in the TPM. The unlock/unseal attempt succeeds only if the sequence of measurements exactly match a prior trusted state.

Titanium Secure Boot verifies the authenticity of boot-time components with both static and dynamic chain of trust measurements and leverages the host TPM to both store and seal cryptographic key material to a known good system state.

Titanium Secure Boot has been through pre-evaluation with participation from Navy, Army, and MDA Anti-Tamper Evaluation Teams.

LEARN MORE

Titanium Technology Protection

Titanium Secure Boot

Intel Secure Boot Process:

STATIC/DYNAMIC
Trust Measurements

DELIVER
Boot Keys

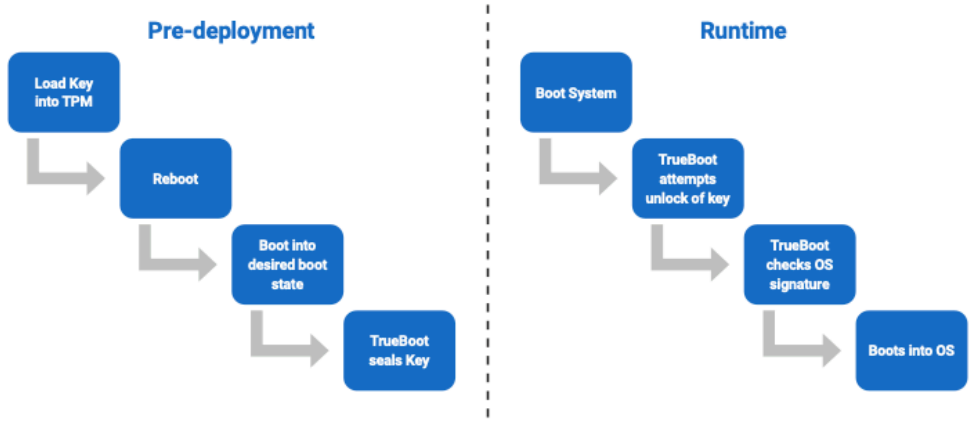
VERIFY
Boot Components

START
OS/Hypervisor

Since Titanium Secure Boot is independent from the kernel or other boot components, it works with most any distribution of Linux including Wind River Linux, RedHat Linux, RedHawk, etc. on a host using either legacy BIOS or UEFI boot and supports both network and disk-based booting.

Using the Titanium Secure Boot tooling, the Linux Kernel and initial RAM disk/filesystem are protected and authenticated by customer-controlled key material sealed within the TPM, meaning that they can be updated remotely by trusted parties without requiring the TPM to be re-provisioned.

Titanium Secure Boot Process:



Contact us if you are interested in learning how Titanium Security Suite can quickly and easily meet your security requirements and protect your system against the full spectrum of reverse engineering and cyber-attacks.

1325 Pennsylvania Ave. NW Suite #700, Washington, D.C. 20004
(202) 706-7027
https://starlab.io