Secure Boot and Measured Boot in UEFI Systems

Secure Boot and Measured Boot are two critical components in the UEFI (Unified Extensible Firmware Interface) specification that enhance the integrity and trustworthiness of a system during the boot process. While both aim to protect against rootkits and bootkits, they operate with different mechanisms and goals.

📏 Measured Boot

Objective: Record and report the integrity of the boot process, allowing detection of unauthorized modifications.

How It Works:

1. **TPM (Trusted Platform Module):** Each stage of the boot process calculates a hash of the next stage and stores it in TPM Platform Configuration Registers (PCRs).
2. **Measurements:** Include UEFI firmware, bootloaders, kernel, and critical configuration files.
3. **Remote Attestation:** A remote system (e.g., enterprise attestation server) can request a quote of the TPM PCR values to verify boot integrity.
4. **Integrity Validation:** Based on known-good hashes (golden measurements), an enterprise system can determine if the boot process was tampered with.

Benefits:

- Detects unauthorized changes even if Secure Boot was bypassed.
- Enables remote auditing and policy enforcement (e.g., deny network access to tampered systems).

Limitations:

- Requires TPM hardware and proper attestation infrastructure.
- Doesn’t block execution; it only records for later analysis.

🆘 Real-World Example

Secure Boot in Action: On a Windows 11 machine, the bootloader and kernel are signed by Microsoft. If a rootkit modifies the bootloader, the signature won’t match, and the firmware blocks it.

Measured Boot in Action: In an enterprise network, the TPM records boot measurements. During login, the enterprise server checks the TPM quote. If bootloader hashes don’t match the golden image, access is denied or flagged.

By combining Secure Boot and Measured Boot, modern systems gain both **protection** and **visibility**—one prevents threats at the source, the other detects them when prevention fails.