In order to ensure data and system integrity, assurances of a system’s state are needed. This can be provided through secure boot, a mechanism whereby the system is booted in stages and the boot is only allowed to continue if each stage is valid.

However, secure boot systems are not common in everyday systems for the following reasons:

• Many proposals require special hardware (e.g., AEGIS, IBM 4758) that can be expensive
• Encryption-based solutions require substantial key management and those keys are released after the boot

Storage is well-positioned to provide a solution for secure boot because it can ensure that information is not released until the boot is verified.

We design Firma, a system protecting on-disk storage by measuring the host system state from boot time until the OS kernel is loaded.

• While a single-user system can be supported by this architecture, we concentrate on a system running virtual machines.

We use integrity measurement to determine the state of the host system. A measurement is a hashed fingerprint of the code at a particular stage.

• Hardware support emanates from the core root of trust for measurement (CRTM), which is secured on the host.
• Subsequent steps are measured from the BIOS through the VMM up to the OS and applications.
• Attestation of the code on the disk is performed using a trusted platform module (TPM) on the host, which is a tamper-resistant, secure microcontroller found in most modern x86 systems.

The Quote operation on the TPM is performed and the results compared with values inside the TPM’s platform configuration registers (PCRs).

Our prototype shows that less than a second is added to the boot time and in our tests of supporting periodic runtime attestations, and the impact on throughput is negligible.

A full measurement of a virtual machine monitor the size of the VMWare ESX hypervisor takes approximately 9 seconds; we perform this is an error has occurred. These costs can be brought down through lazy attestation, hiding the computational costs in seek times for the disk.