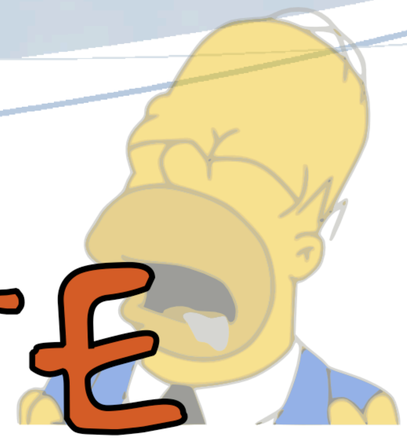
CERIAS



SALIVATE

Secure Architecture for Loading, Initializing, and Verifying A Trusted Environment

Trusted Entities

BIOS CD-ROM

BIOS CD-ROM

BIOS CD-ROM

Network BIOS CD-ROM

Network BIOS CD-ROM

Network BIOS CD-ROM

Hard Drive Network BIOS CD-ROM

Secure Boot Process

Computer begins boot process after reboot or power-on.

GRUB (GRand Unified Bootloader) initialized from trusted, read-only media (CD-ROM).

ATTACK VECTOR!
An attacker modifies the BIOS to boot compromised media instead of the trusted CD-ROM

DEFENDED!
Trusted BIOS provided by Intel Trusted Platform Module (TPM) and assumed physical security

GRUB requests a signed timestamp from administration server

ATTACK VECTOR!
A malicious server attempts forgery, replay, or denial of service of timestamp responses

DEFENDED!
Three-tiered protocol detects and mitigates all three attacks

A challenge nonce is generated from received timestamp

Challenge nonce is used to request a known-secure digest of hard drive partitions

ATTACK VECTOR!
Malicious response is sent from rogue server either as a replay attack, with a bad nonce, or with a bad signature

DEFENDED!
Public key signatures and challenge nonce are used to verify response integrity

Hard drive integrity is verified against provided digests

ATTACK VECTOR!
Hard drive contents have been altered by a previous attack

DEFENDED!
Imaging software is loaded and partitions are restored to a known-secure state

Do hard drive partition digests match?

Yes

No

Re-Imaging operating system boots

Known-secure partitions are streamed from the administration server to the application server

Application server reboots and begins secure boot process again

Secure boot process is completed and verified operating system is booted

Re-Imaging Process

Team Members

MICHAEL ARMBRUST
JAY GENGELBACH
GREGORY OSE
PARKER FATH

Project Description

In a networked environment, it is unreasonable to assume that any system is completely impervious to attack. When a system is compromised, however, system administrators would like to restore it to a trusted state. By utilizing a guaranteed boot sequence, the problem of restoring a compromised system is reduced to the simple task of rebooting the machine.

This project presents a flexible architecture for a secure boot and imaging process that ensures a server always boots into a trusted state, without making any assumptions about its previous condition.

Part of the poly 2 architecture

http://projects.cerias.purdue.edu/poly2

NSF Award: 0523243-CNS

PURDUE UNIVERSITY

PURDUE HOMELAND SECURITY INSTITUTE

CERIAS

REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING

Discovery Park e-Enterprise Center