Towards measured boot out of the box

Matthew Garrett

@mjg59 | mjg59@coreos.com | coreos.com

CoreOS

Security of the boot chain is vital

CoreOS

UEFI Secure Boot

CoreOS

Various embedded solutions

CoreOS

Rely on security of firmware

CoreOS

No way to prove verification happened

CoreOS

Why does this matter?

CoreOS

Compromised servers

CoreOS

Modified laptops

CoreOS

Can’t protect against hardware attacks

CoreOS

…but we can cover most others

CoreOS

Trusted Platform Module

CoreOS

Small chip

CoreOS

Platform Configuration Registers

CoreOS

Measurement

$$PCR_{new} = hash(PCR_{old} | hash(data))$$

CoreOS

Associated log

CoreOS

Trusted GRUB

CoreOS

(old and busted)

Core OS

Rohde & Schwarz

(no UEFI support, not TPM2 support)

CoreOS

https://github.com/coreos/grub

What do we measure?

CoreOS

Traditional approach

CoreOS

Most components in separate PCRs

CoreOS

Need to re-use PCRs

CoreOS

Order of loading matters

CoreOS

Unimportant configuration changes alter values

CoreOS

Suboptimal

Use the logfile

CoreOS

Replay log to ensure it’s valid

CoreOS

Look at individual log entries

CoreOS

Two choices

CoreOS

Log entry contains description of binary and hash of binary

CoreOS

Log entry contains text and hash of text

CoreOS

Policy describes each binary

CoreOS

Policy describes regular expressions

CoreOS

Where does the policy come from?

CoreOS builds policy automatically on OS release

CoreOS

Problems:

CoreOS

Initramfs varies across systems

CoreOS

Reproducible initramfs builds

CoreOS

Generic initramfs

CoreOS

Where do we store boot data?

CoreOS

Use UEFI variables

CoreOS

Use TPM

CoreOS

Things to use the TPM for:

CoreOS

TPMTOTP

CoreOS

Disk encryption keys

CoreOS

SSH keys

CoreOS

Unseal/reseal

Doesn’t TXT make all of this easier?

CoreOS

(ha ha ha)

CoreOS

No secure boot support

CoreOS

Incompatible with runtime UEFI

CoreOS

Summary:

Core OS

Ship bootloader support
Ship known-good measurements
Integration with firmware updates
Deterministic initramfs generation