Tying TPMs throughout the stack

Matthew Garrett
<mjg59@coreos.com>

Trusted Platform Modules

- Small
- Slow
- Can't DMA
- Can't force the OS to do anything

So what's the point?

Measured boot

Each component measures the next

Each measurement is pushed into the TPM

Each measurement extends the previous measurement

To get a specific value:

- Write the same sequence of values
- Break hash algorithm

What can you do with this?

Encrypt data

Hard drive decryption keys

TOTP data

github.com/mjg59/tpmtotp

But what about after boot?

SSH keys

github.com/ThomasHabets/simple-tpm-pk11

Random numbers

modprobe tpm_rng

Configuring TPMs

```
echo 14 >/sys/class/misc/tpm0/ppi/request
```

Check /sys/class/misc/tpm0/ppi/transition_action

tpm_takeownership -y -z

Boot logs

/sys/kernel/security/tpm0/

Bootloader support

github.com/mjg59/grub

TPM 2.0

Ugh

Brilliant future?

TSPI is awful

github.com/mjg59/python-tss

PKCS#11

Opencryptoki (boo)

Chaps (yay)

Reasonable TPM broker, or abstract TPM away?

github.com/mjg59/tpmtotp
github.com/ThomasHabets/simple-tpm-pk11
github.com/mjg59/grub
github.com/mjg59/python-tss