JULY 11-13, 2017
BUDAPEST, HUNGARY

Xen Project

DEVELOPER AND DESIGN SUMMIT

Xen Project
DEVELOPER AND DESIGN SUMMIT

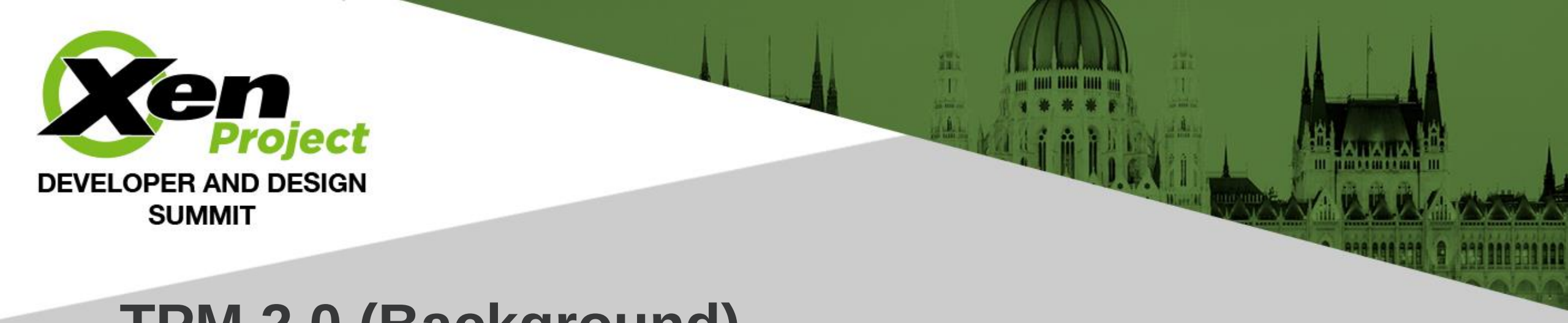
JULY 11-13, 2017
BUDAPEST, HUNGARY

Supporting TPM 2.0 In The DRTM on OpenXT

Chris Rogers, Research Software Engineer, *AIS*

Agenda

- ***Background***
- TPM 2.0 Development
- Future Work



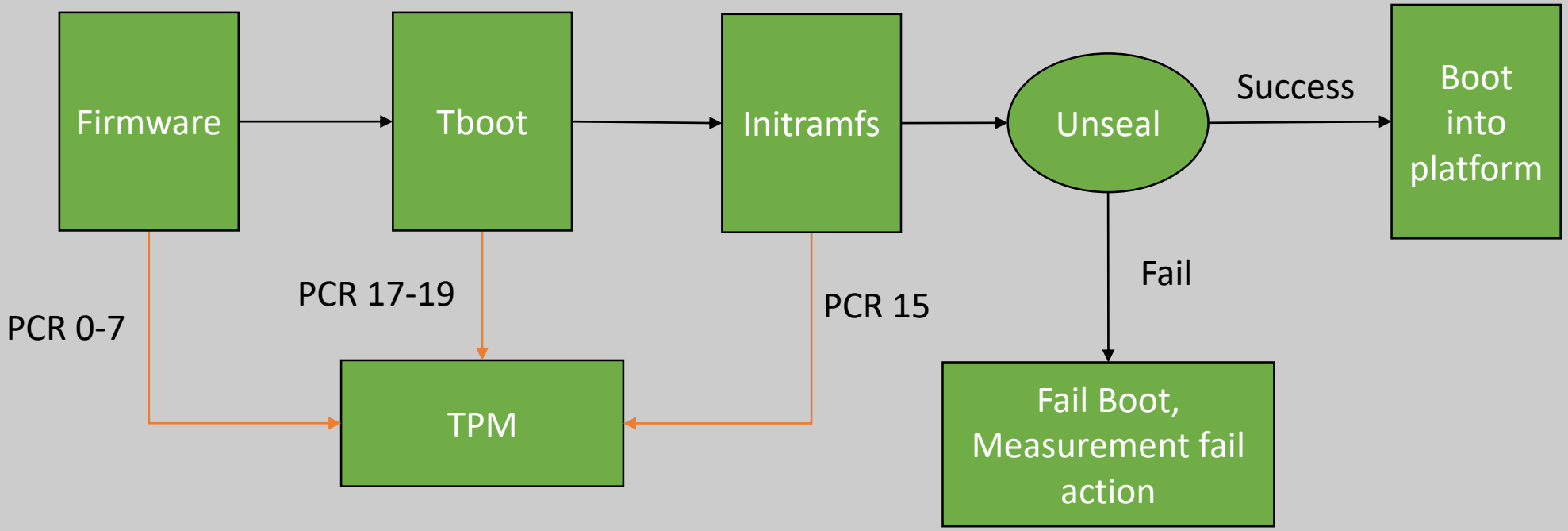
TPM 2.0 (Background)

- Secure cryptoprocessor standard
- Discrete hardware
- Used to establish a “root of trust”

OpenXT (Background)

- Xen-based client virtualization platform
- Intel TXT, Tboot, TPM for DRTM

OpenXT – Measured Launch (Background)



Agenda

- Background
- ***TPM 2.0 Development***
- Future Work

Why? (TPM 2.0)

- TPM 1.2 is outdated
  - SHA-1 has known collisions
  - Limited options for encryption algs (RSA, optional AES)
    - Prime factorization's days are numbered
  - Unable to adapt to changing security landscape
- TrouSerS
  - OpenXT's TSS for 1.2, no plans to support 2.0

Focus Areas (TPM 2.0)

- Tboot
- TSS/Toolstack
- Dom0 management scripts

Tboot (TPM 2.0)

- Tb_polgen, policy generation tool
  - Verified Launch Policy tells tboot which PCR num and bank for extend
  - Hardcoded to use SHA-1 for hashing ops
  - Patched to make hash alg configurable

Tboot (TPM 2.0)

- First up, last down
  - Tboot needs to perform an “Orderly shutdown”
    - On reboot, halt, or S4
    - S3 is a special case
  - See TCG Spec: Part 1, Section 19.8.6
  - Hardware solution to specific Dictionary Attack vector
  - Once in lockout, authenticated ops fail
    - Either tpm_clear, reset lockout with hierarchy, wait for TPM_PT_LOCKOUT_COUNTER

TSS/Toolstack (TPM 2.0)

- Currently using Intel's TPM 2.0 projects
  - TPM2.0-TSS (https://github.com/01org/tpm2.0-tss.git)
  - tpm2.0-tools (https://github.com/01org/tpm2.0-tools.git) v2.0.0
- Several patches against tpm2.0-tools
  - Tpm2_extendpcr, tpm2_sealdata, tpm2_unsealdata
  - Various lib modifications

TSS/Toolstack (TPM 2.0)

- Tpm2_extendpcr
  - Basic tool to extend pcr values
  - Dom0 extends PCR-15 with hash of rootfs
- Tpm2_sealdata
  - Builds PCR policy, creates sealed data blob against provided set of PCRs.
- Tpm2_unsealdata
  - Builds PCR policy, loads sealed blob into TPM with (tpm2_load) and unseals with tpm2_unseal.

TSS/Toolstack (TPM 2.0)

- Current implementation doesn’t use resource manager
  - Use Tss2_Sys_FlushContext() to manage loaded handles.
  - Avoid limit of max transient handles with simple operations.

Dom0 (TPM 2.0)

- New Selinux rules
- Measured Launch scripts
  - Support new hash algs, new tools syntax
  - Implement framework for “layered sealing”
  - Logic changes to handle 2.0 vs 1.2 (we support both, TPM version determined at runtime)
- https://github.com/openxt

Agenda

- Background
- TPM 2.0 Development
- ***Future Work***

Layered Sealing (Future Work)

- Manufacturers sometimes have inconsistencies with TPM hardware.
  - Certain bios measurements are inconsistent
  - When hash bank is disabled, PCRs are still extended
- Solve this problem in software with Layered Sealing

Layered Sealing (Future Work)

- Normally, we seal against a single bank.
  - *seal_sha256*(priv_key)
- With a layered approach, we can protect the key *and* verify platform integrity.
- For all available PCR banks, layer the seal operations
  - *seal_sha512*(*seal_sha384*(*seal_sha256*(*seal_sha1*(priv_key))))
  - Unseal in the opposite direction to retrieve key.

Layered Sealing (Future Work)

- Implementation challenges:
  - Max private data size is 128 bytes (MAX_SYM_DATA)
  - Output of single seal operation is a TPM2B_Private struct, much larger than 128 bytes.
- Read and seal 128 byte segments
- Seal ops are cheap, though input/output files will become large after 2+ seals.
- In progress, targeted for next OpenXT release

Future Work

- OpenXT uses TPM for specific use case, but TPM 2.0 has many new features.
- Remote attestation
  - Use TPM to assure remote management server that platform integrity is sound
- Crypto
- Dedicated Key Storage

Questions?