Using the TPM:
Other TPM Features

Ariel Segall
ariels@alum.mit.edu

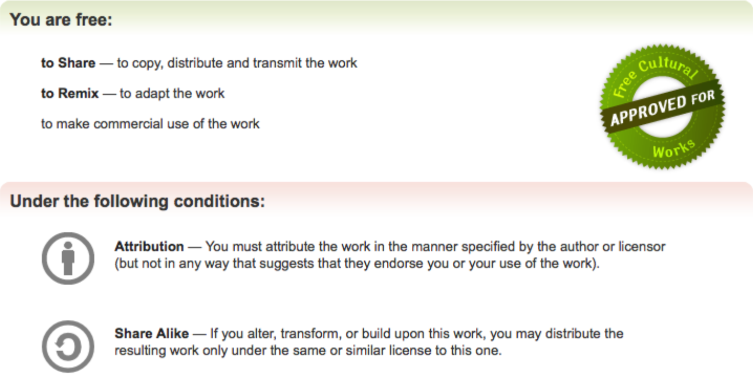
Day 2

Approved for Public Release: 12-2749.
Distribution unlimited

License

All materials are licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0



You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

to make commercial use of the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

The Smorgasbord

The TPM has a number of minor features worth discussing

- Not significant enough for 101
- Too small for own talks

We'll briefly touch on several, so you'll be familiar with the concepts

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

TPM Flags

- The TPM has a number of internal settings: “flags”
- Values (mostly) changeable by owner or set by TPM
- Most are not very relevant to enterprise, e.g.:
  - Ownership: determines whether an owner exists
  - ReadPubEK: determines if EK pubkey can be read; for privacy
- Some are potentially very important:
  - **FIPS: Many TPM commands will require minimum good security practices**
  - **nvLocked: Enables or disables all authorization checks on NVRAM**
- Others are useful in unusal corner cases, e.g:
  - CEKPUsed: Indicates if EK created by mfr process or TPM command
  - disableOwnerClear: Determines whether owner can clear TPM
- Full list in TPM Structures spec

Getting and Setting TPM Flags

- TPM_GetCapability: Retrieves current value of a TPM flag or other internal information, such as number of key slots available, size of NVRAM, etc.
- TPM_SetCapability: Owner-authorized command to change flag values.
- Full list of capabilities and subcapabilities (i.e., indexes to flags and other information) in Structures spec, under TPM_CAPABILITY_AREA.
  - What does that mean? We'll cover that this afternoon.
- Note: When programming using TSS, there are actually more commands that can be used to retrieve and set flags. We won't cover those today.

Some flags, including FIPS mode, are permanently set by the manufacturer.

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

Key Migration

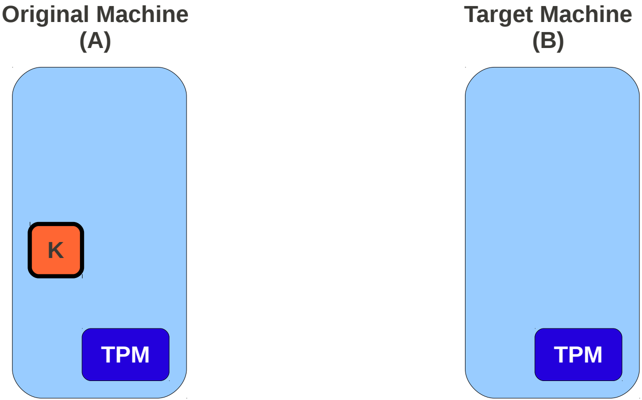
- In TPM keys talk, mentioned that keys could be migratable
- All other talks: use non-migratable keys!
- Key migration is a criticial feature for enterprise
  - Backup
  - System replacement

Migration in a Nutshell

- Create migratable key K on TPM A
- Create migration blob, reencrypting K to key on TPM B
    - Requires authorization of owner, or delegated auth
    - Note: B doesn't actually have to be a TPM, though designed to be
- B decrypts blob; K now available to B.

Note: K still usable on A! This is backup approach.

Migration: Starting State



Original Machine (A)

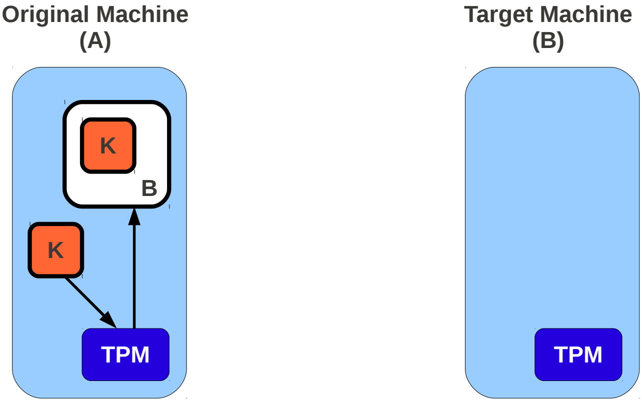
K

TPM

Target Machine (B)

TPM

Migration: Creating Migration Blob



Original Machine
(A)

K

B

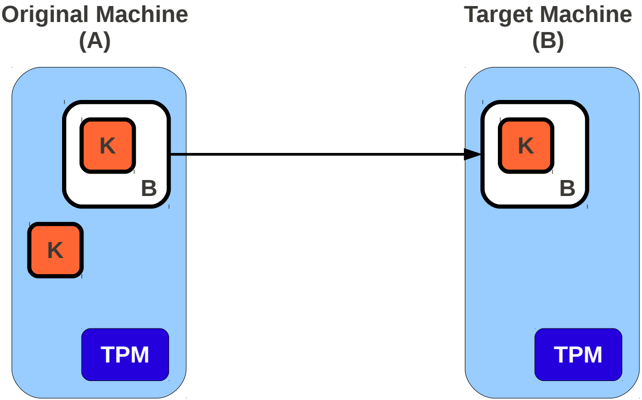
K

TPM

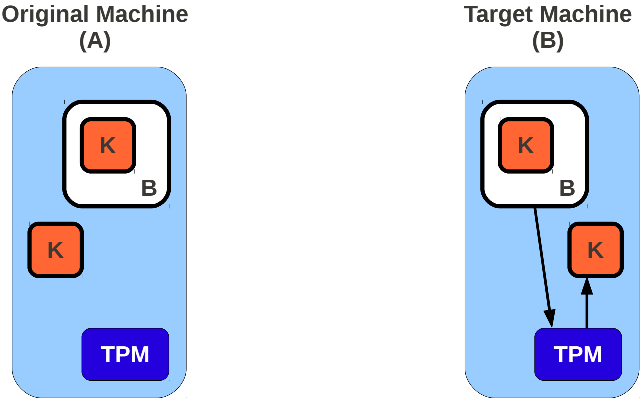
Target Machine
(B)

TPM

Migration: Transferring Migration Blob



Migration: Decrypting Migration Blob



Original Machine
(A)

Target Machine
(B)

Certified Migration Keys (CMKs)

- Normal migratable keys cannot be certified: could be migrated to non-TPM
- CMKs always migrate to migration authority, which verifies final destination
- Owner approves migration authorities for system
- Can be certified; cert includes authority info
- More complex than normal migration, but more assurance

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

Monotonic Counters

- TPMs provide monotonic counters
- Guaranteed to always increase over time
    - When deliberately incremented– not clocks
- Good for internal freshness checking!
    - Counter values cannot be signed for external verification
    - Can use to invalidate old saved data: include value, increment counter
- Unlike NVRAM, burnout due to too many updates extremely unlikely

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

Tick Counters

- TPM has no internal clock
- Closest equivalent: tick counters
- Count from start of last tick session
  - Usually last startup, but not guaranteed
- Combines counter with tick session nonce, allowing comparisons
  - TPM will sign tick stamps– use Identity!
  - Approximate clock per boot
- Surprisingly accurate!
  - Intended primarily for short-term, relative comparisons
  - Usable for timing-based attestation

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

Random Number Generation

- TPM can act as random number generator
  - Frequent question: how good?
  - Answer: Don't know, manufacturer dependent
  - Hardware entropy recommended, not required
- Bytes retrievable with `TPM_GetRandom` command
- Entropy can be added from outside with `TPM_StirRandom` command
  - RNG used to create TPM keys
  - Allows high-quality entropy to be imported for better key generation

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

OwnerEvict Keys

- We've previously said that loaded keys are unloaded on reboot, or when the TPM runs out of key storage space.
- There is an exception: OwnerEvict Keys
    - Currently loaded key; owner sets OwnerEvict flag on it.
    - Key must not have any parent PCR constraints. (Constraints on key itself fine.)
    - Key will never be unloaded until flag is changed by owner.
- Very useful; no need to track key on disk or load!
- *Very* limited; some TPMs have as few as 3 key slots.
- Use `TPM_KeyControlOwner` command to set.

Topics We'll Cover

- TPM Flags
- Key Migration
- Monotonic Counters
- Tick Counters
- Random Number Generation
- OwnerEvict Keys
- Clearing the TPM

Clearing the TPM

- What does an enterprise do with TPM when disposing of machine?
- *Clear* the TPM
- Two approaches:
  - Through BIOS (ForceClear must be enabled; can be disabled temporarily)
  - `TPM_OwnerClear` command (must be enabled; once disabled, stays until TPM cleared)
- Erases all non-permanent data from TPM
  - Owner erased, along with SRK
  - Key storage cleared (in FIPS mode, overwritten with 0)
  - Flags returned to default value
  - Non-manufacturer NVRAM deallocated
  - etc
- Some things remain: EK, monotonic counter
  - Also PCRs– cannot clear TPM to fake boot state

Questions?