Using the TPM Specifications

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.

What are the Specifications?

- TPM Main Part 1: Design Principles
- TPM Main Part 2: Structures
- TPM Main Part 3: Commands

Also potentially useful:

- PC Client TPM Specification
  - Defines requirements for real-world TPM chips
  - Which commands must be supported, what PCRs and localities mean, minimum sizes...
- TCG Softare Stack (TSS) Specification
  - If programming with the TSS

Part 1: Design Principles

- High-level context, such as architecture and goals
- Charts of how various commands and structures relate to each other
- Look here for:
  - High-level overviews
  - Architectural requirements (e.g., which components must be present)
  - Manufacturing requirements (e.g., how good RNG must be)
  - Behavioral requirements (e.g., dictionary attack prevention, when PCRs are checked)
- Rarely contains comprehensive detail.

Part 2: Structures

- Data structure definitions, both internal to the TPM and passed to the TPM.
- Usually used in conjunction with Commands spec.
- **More important than it sounds.**
  - Often, TPM commands will call for one meaningful argument that is a structure
  - That structure may contain many pieces of critical information
  - **You cannot understand TPM commands without looking up all of the data structures involved!**
  - (Note: Many of them are multi-layered.)

Part 3: Commands

- API definition for TPM
- The most useful spec for people designing TPM applications
  - But keep in mind, you'll need Structures handy.
- Generally well-grouped by command purpose; always read the informative comments!
- Most commands have common overhead for authorization sessions

Example