presented by

Updated TCG TPM 2.0 Specs

UEFI US Fall Plugfest – September 20 - 22, 2016

Richard “Dick” Wilkins, Ph.D.
Phoenix Technologies Ltd.

Agenda

- Introduction
- The Specs
- This stuff is new
- What has changed
- Call to Action
- Questions?

Previous presentations

- Summerfest 2013 @ Microsoft
  - I talked about the TPM 2.0 hardware and the physical interfaces
  - No usage spec was available
- Plugfest March 2016 in Taipei
  - I spoke about the recently published TCG specs and what was new
- Today…
  - New pending specs and what significant changes they include
  - Not yet published but out for public review in the next few weeks

Applicable TCG Specs

- PC Client Platform Firmware Profile Specification, Rev .21
  Published, (New version pending, October?)
- EFI Protocol Specification, Rev .13
  Published, with errata available
- PC Client Platform Physical Presence Interface Specification V1.30 Rev .52
  Published, with errata available

http://www.trustedcomputinggroup.org/resources/specifications_in_public_review
http://www.trustedcomputinggroup.org/resource-directory/

Not in EDK II

- All the stuff I'm talking about here is new
- It is unlikely that the changes are included in the Tianocore open-source code base yet
- That will need to happen ASAP

- See Microsoft's slides about the TrEE (Trusted Execution Environment) protocol in the TCG EFI Protocol spec

TPM Event Log back in ACPI

- In earlier versions of the TCG TPM2 PFP spec, the event log had been removed from the ACPI tables
- It is back!
- The TPM2 ACPI table must have a pointer to non-reclaimable memory, minimum 64KB in length, that contains the event log
- Still accessible from the EFI protocol as well
- An OS may add to the log at runtime
- See Section 8.2 and Table 11

Tagged Events are back

- Tagged (custom) events were deprecated for TPM 2.0
- The were returned due to attestation needs for OSes and applications
- Only the event type and structure are standardized. The content is user defined
- See Section 9.4.2

Support for UEFI 2.5 added

- The secure boot related variables are normally measured into PCR[7]
  - Many measurement details have been changed
- DeployedMode and AuditMode variable support has been added
- If these variables change during boot,
  - the system must be restarted OR
  - The variables must be re-measured into PCR[1]
- See Section 2.3.4

TPM Disabled or Hidden

- Clarified the definitions and requirements for platform firmware when the TPM is disabled and when the TPM is hidden (by end user or by platform OEM)
- See Section 8 and numerous other places

Other

- Clarified a great deal of event logging information based on implementer feedback
- Clarified and fixed error condition definitions and requirements for platform firmware to handle these cases
- Fixed more errata since the last published Errata spec
- Made a number of general clarifications in non-normative text

Call to Action

- All IBVs, OEMs and OSVs need to make themselves aware of these required changes
- They may matter to IHVs as well, particularly those with option ROMs
- Code changes are needed for Tianocore/EDKII, can you help?
- The TPM 2.0 is mandatory on most platforms. So these code changes are now mandatory as well

Closing remarks

Questions?

Thanks for attending the UEFI US Fall Plugfest 2016

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by