TPM Event Log

This document briefly describes what TPM log is and how it is handed over from the preboot firmware to the operating system.

Introduction

The preboot firmware maintains an event log that gets new entries every time something gets hashed by it to any of the PCR registers. The events are segregated by their type and contain the value of the hashed PCR register. Typically, the preboot firmware will hash the components to who execution is to be handed over or actions relevant to the boot process.

The main application for this is remote attestation and the reason why it is useful is nicely put in the very first section of [1]:

"Attestation is used to provide information about the platformâ€™s state to a challenger. However, PCR contents are difficult to interpret; therefore, attestation is typically more useful when the PCR contents are accompanied by a measurement log. While not trusted on their own, the measurement log contains a richer set of information than do the PCR contents. The PCR contents are used to provide the validation of the measurement log."

UEFI event log

UEFI provided event log has a few somewhat weird quirks.

Before calling ExitBootServices() Linux EFI stub copies the event log to a custom configuration table defined by the stub itself. Unfortunately, the events generated by ExitBootServices() don't end up in the table.

The firmware provides so called final events configuration table to sort out this issue. Events gets mirrored to this table after the first time EFI_TCG2_PROTOCOL.GetEventLog() gets called.

This introduces another problem: nothing guarantees that it is not called before the Linux EFI stub gets to run. Thus, it needs to calculate and save the final events table size while the stub is still running to the custom configuration table so that the TPM driver can later on skip these events when concatenating two halves of the event log from the custom configuration table and the final events table.

References

- [1] https://trustedcomputinggroup.org/resource/pc-client-specific-platform-firmware-profile-specification/
- [2] The final concatenation is done in drivers/char/tpm/eventlog/efi.c