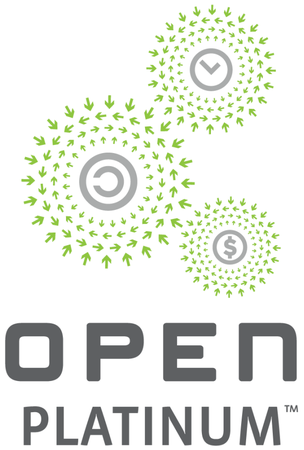

Open. Together.
OCP
SUMMIT

CHIPSEC on Non-UEFI Platforms

Stephano Cetola
CHIPSEC Community Manager
Intel Corporation



CHIPSEC History

SECURITY

- CHIPSEC is a framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components.
- Originally developed by Yuriy Bulygin (@c7zero)
- First version of CHIPSEC was released in March 2014 at CanSecWest
- Currently used by firmware developers, system validation and system integrators

https://github.com/chipsec/chipsec.git

Current CHIPSEC Assumptions

SECURITY

- Runs on an Intel based platform
- Firmware has a threat model compatible with UEFI
- All platforms require the same level of security

Threat Model Assumptions

SECURITY

- **Configuration Settings**
  - Program and lock registers when possible
  - Minimize the use of non-volatile data that is updatable from OS
- **Flash Access**
  - Ensure the Serial Peripheral Interface (SPI) flash can be updated in runtime
  - Use the System Management Mode (SMM) or Protected Range (PRx) register to protect SPI flash
  - Verify flash programming matches guidance from Intel
- **Others…**

So What's the Problem?

SECURITY

- **Different methods to secure the platform exist**
  - Read Only (RO) backup firmware with forced recovery
  - Physical presence for update
  - RO firmware
- **Platforms have different security requirements**
  - Open Development System (cannot be locked down)
  - High Assurance Critical System (very, very locked down)
- **CHIPSEC modules do not comprehend different platforms requirements**
  - This means security engineers may find 'false positive' issues
  - if your threat model is not well understood and documented.

Processing Results

SECURITY

- **Know your platform**
  Understand the security assumptions of your platform
- **Know your security requirements**
  Is physical attack part of your model?
  Are you developing or deploying custom firmware?
- **Understand why you may skip certain modules**

CHIPSEC Example

SECURITY

- **CHIPSEC run on Chromebook in developer mode**
  - Legacy Boot to Linux*
  - Skylake Y processor
- **Results Summary**
  - Failure in **`bios_wp`**
  - Warnings in expected locations
  - UEFI tests skipped as expected
  - All others passed

Thanks to John Loucaides from Eclypsium for the log file.

False Positive Example in `bios_wp`

SECURITY

```
[x][ ============================================================
[x][ Module: BIOS Region Write Protection
[x][ ============================================================
[*] BC = 0x0000008D << BIOS Control (b:d.f 00:31.5 + 0xDC)
    [00] BIOSWE           = 1 << BIOS Write Enable
    [01] BLE              = 0 << BIOS Lock Enable
    [02] SRC              = 3 << SPI Read Configuration
    [04] TSS              = 0 << Top Swap Status
    [05] SMM_BWP          = 0 << SMM BIOS Write Protection
    [06] BBS              = 0 << Boot BIOS Strap
    [07] BILD             = 1 << BIOS Interface Lock Down
[-] BIOS region write protection is disabled!
```

- **Failure due to different security model being used**
  - SMM based protections disabled
  - Configuration locked (good)
- **User needs to understand that this is not a real failure**

What Can the OCP Community Do?

SECURITY

- **Require Published Threat Models for OCP Accepted Hardware**
- **Discuss updates to CHIPSEC to support different threat models**
  - Open issues on GitHub if you find problems
  - Looking for community guidance on implementation
- **Create or update modules to support multiple threat models**
- **Submit issues and pull requests on GitHub**

https://github.com/chipsec/chipsec

Get Involved Today

Project: https://github.com/chipsec/chipsec

Follow: @CHIPSEC

Training: UEFI and CHIPSEC Development for Security Researchers

Contact: chipsec@intel.com

Legal Notice

No computer system can be absolutely secure.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel, the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others


Open. Together.
OCP Global Summit | March 14–15, 2019
OCP
SUMMIT