Firmware security’s a thing.
Current State of Things

- Fragmented at best
  - Each chip vendor has their own integrated secure boot solution
  - Proprietary solutions are black boxes
- Lowest common denominator: no security at all
Security Project Goals

- Improve security across the entire computing industry through open standards
  - Security is a base requirement, not a differentiator
  - Reduce redundant effort
  - Building your own security snowflake is bad
- Specifications for hardware and software security implementations
- Flexible solutions that will work across different types of IT equipment
- Use existing and emerging standards
Focal Points

● Securing and verifying all mutable storage (flash for BIOS, BMC, uC, CPLD, etc)
  ○ Firmware provisioning
  ○ Secure updates & roll-backs
  ○ Recovery
  ○ Attestation
● Standardizing interfaces
  ○ Software APIs
  ○ Hardware/electrical
● Changing ownership
  ○ Key rotation
  ○ Used gear should be secure too
What’s out of our scope?

- Physical security countermeasures and anti-tamper
  - Disabling debug interfaces is in scope, screwdriver based attacks are not
  - No thermite :-(
- Application level secure coding practices
- Software/hardware penetration testing
- New encryption or compression algorithms
We’re making some progress

- Threats we want to defend against
  - Common Security Threats
- Drafts in progress of two large specification sections
  - Secure Boot
  - Attestation
Join Us!

https://www.opencompute.org/projects/security

- Mailing list
- Weekly meeting