OCP Security Project Overview

Speaker: Nate Klein (Google)
OCP Security Project Goals

• Improve security across the entire computing industry through open standards
  - Security is a base requirement, not a differentiator
  - Reduce redundant effort
  - Security snowflakes are less secure
• Specifications for hardware and software security implementations
• Flexible solutions that will work across different types of IT equipment
• Use existing and emerging standards

Project Charter
Secure and Resilient

NIST SP 800-193 lists three pillars of resilient systems

1. Protection
2. Detection
3. Recovery

Goal: Enable all OCP Accepted and Inspired designs to comply with 800-193
Released Documents

White Papers

• Security Threats ([link](#))
  - Defining the threat landscape
• Attestation ([link](#))
  - Detection pillar
• Secure Boot ([link](#))
  - Protection pillar

Community Contributions

• Ownership and Control of Firmware ([link](#))
• Best Practices for Firmware Code Signing ([link](#))
Security Threats

• Defines the specific types of threats that we are mitigating
  - Bit rot
  - Misconfiguration
  - Remote/logical access to a system
  - Limited physical access to a system
• Defines what is out of scope
  - Runtime attacks
  - Firmware or hardware bugs
  - Supply chain attacks (mostly)
Attestation

- Defines the keys, seeds, and identities needed for each RoT
- Verify the identity of all roots of trust
  - Provisioning process creates a unique, unclonable, and immutable identity
- What to measure
  - Executable firmware
  - Configuration/Debug state
  - Other security state
- Securely transmit/receive attestation information
Secure Boot

• Firmware encryption is not sufficient
• Enforcement must be immutable
• Required algorithms and minimum key strengths
• Rules for dual-signing
• Key revocation, re-keying, and ownership transfer
• Secure boot failure must not render the device unrecoverable
Works in Progress

• Recovery
  - Third pillar of a resilient system
• Secure Platform Overview
  - Architecture of a secure system
  - Roots of trust for measurement, update, and recovery
• Ownership Transfer
  - Ensuring reusability without compromising security
• Cryptography
  - Bridging US and international standards
Security Checklist Changes

- Badges go away
  - Nobody wanted anything but gold
  - One size didn’t fit all
- Specifications define their security requirements
  - Security section is mandatory in specifications
  - Allows flexibility
  - Security requirements can be tailored to the use case

Developing a new product specification? Come talk to the security group!
Call to Action

• Join us! [https://www.opencompute.org/projects/security](https://www.opencompute.org/projects/security)
  - Weekly project meeting
  - Mailing list
• Create open-source reference implementations
  - Attestor and attestee firmware
  - Root of trust RTL
• Meet with the Security group
  - New OCP contributions talk to us early
• Discuss security with your vendors