SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

Setting the Security Standard for OCP Hardware

Andres Lagar-Cavilla

OCP Incubation Committee
Principal Engineer, Google

A SNIA Event

OCP Structure

Projects

- Server, Storage, Networking, etc
- Security is a top level project
- Project leads are Nate Klein (Google) and Bryan Kelly (Microsoft)
- Today’s presentation covers what the project does in depth

Incubation Committee

- Steer OCP strategy – each project has an IC seat
- Anoint new projects and subprojects, new strategic initiatives
- Andres Lagar-Cavilla (Google) represents Security

Foundation

- Staff (CEO, operations, etc) running the foundation business

Board

- Seven seats: 3 individual, 4 Platinum members (Meta, Microsoft, Google, Intel)

OCP Value

It is the only industry body where system architecture comes together

Examples

- DMTF: protocols (Redfish, SPDM)
- TCG: security specifications (TPM, Opal)
- NIST: standards (AES GCM, 800-193)
- NVMe: storage

All touch on security, directly or tangentially

But the system does not come together ← role of OCP is to fill this gap

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

OCP Security Message to SNIA

Make SSD security boring and consistent

Foundational

- Adopt internal RTM
- Follow NIST 800-193 for firmware resiliency
- Rely on board protection against denial of service

APIs

- Use SPDM 1.2+ for attestation, don’t reinvent the wheel
- Encap in Redfish for top level hardware management API surface

Directional (not yet sanctioned by OCP project)

- Align on MCTP sideband to facilitate SPDM (in addition to NVME-MI) …. i3c ….
- Role of PCI IDE and SPDM over DoE

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!
- Weekly meeting cadence (agenda)
- Time set apart to discuss contributions’ security sections

Call to Action

Join us! 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

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containin material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Please take a moment to rate this session.

Your feedback is important to us.