OPEN

Compute Project

Security Project Charter

Revision 1.0

Author: Nate Klein (nxk@google.com)

Date: February 6, 2018

Table of Contents

Overview

The Security Project creates designs and specifications to enable software security for all IT gear through collaboration with the wider Open Compute community. This project provides a foundation for securing all IT gear that is designed in other Open Compute projects. Successful projects delivered by this project will:

- Remove redundant effort required by other projects to create their own security solutions
- Provide standard hardware and software security implementations
- Provide flexible solutions that will work across different types of IT equipment
- Standardize components required for hardware based software security
- Improve security across the entire cloud computing industry through open standards
- Use existing and emerging standards where appropriate

In-Scope Activities

The Security Project will focus on the following:

- Standard hardware interface and protocols for ensuring boot code integrity
- Open-source firmware for dedicated security hardware
- Security firmware APIs and protocols
- Change of ownership of the IT gear (e.g. resale)
- Firmware Security provisioning methodologies
- Secure boot of firmware and operating system
- Recovery from a compromised or untrusted state
- Securing and verifying all mutable storage (flash for BIOS, BMC, microcontroller(s), CPLD, etc)
- Secure updates to mutable storage with versatile rollback-protection options
- Conformance to standards developed in this project

Out of Scope Activities

The following areas will be out of scope of the Security Project:

- IT gear physical security countermeasures and anti-tamper
- Application level secure coding practices
- Software/hardware penetration testing
- New Encryption/Compression algorithms