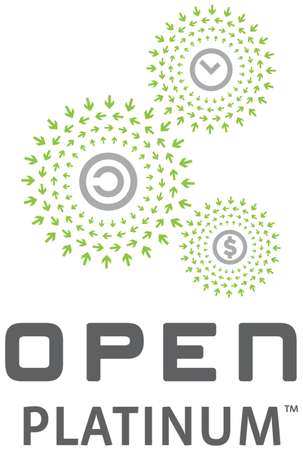
Open. Together.

OCP
REGIONAL
SUMMIT

Secure-Boot on OCP NIC

Prevent Supply-Chain and Cloning Attacks

Yuval Itkin – Distinguished Architect
Elad Wind – Director, Solutions Engineer



NICs Are A Target for Attacks

- Hardware attacks are part of the datacenters security threat landscape
  1. Tampering with supply chain elements
  2. Cloning devices
- **Secure Boot** addresses supply chain attacks – but not cloning
- NICs must combine **Secure Boot** with **Cloning Protection** to prevent both attack methods

SECURITY

WHITE PAPERS
(IN PROCESS)

Secure Boot

- **NIST** Special Publication **SP800-193**
  “Platform Firmware Resiliency Guidelines”
- Using Secure-boot assures that only properly **signed firmware images** can be loaded into a device
- Devices can only **authenticate** the signature using a **pre-provisioned public key**

Cloning Protection

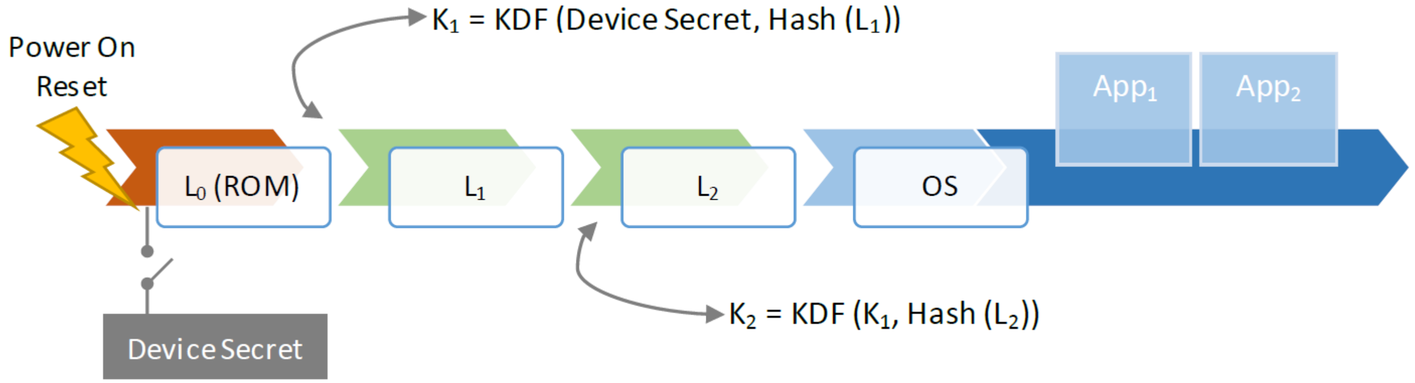
- Datacenters may provision different rights per device-ID
- Vendors may enable capabilities using firmware image
- Cloning Protection prevents hardware replicas
- Cloning Protection mandates using an embedded device-unique key

2 Methods to Prevent Cloning

1. Attestation protocol
2. Device-based cloning protection during secure boot

1. Attestation Based Cloning Protection

- Devices are individually provisioned to the systems installed in using its Device-Secret and firmware image
- Device provides firmware measurements based on its Device Secret



* See more information in RIoT Paper

2. HW RoT Based Cloning Protection

- The device-unique key is inaccessible and invisible to the external world
- Hardware RoT verifies the firmware using a **runtime-calculated device-specific signature** against an off-chip stored signature

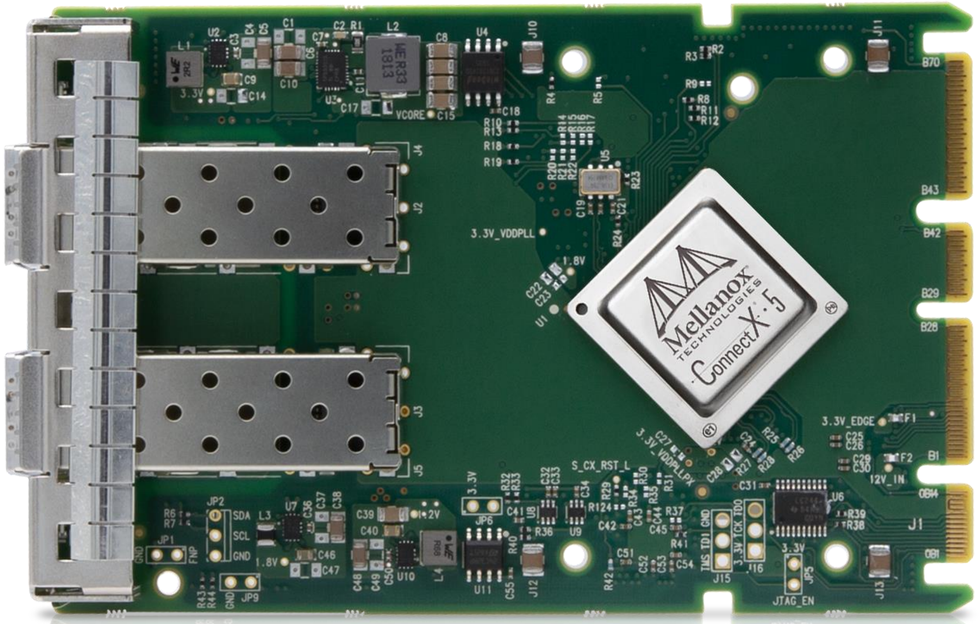
- Note: this method mandates devices to embed the cloning-protection signature during firmware update

Mellanox OCP NIC 3.0 Cards

OPEN INSPIRED™

ConnectX®-6 Dx

ConnectX®-5



Mellanox OCP NICs

OCP NIC 3.0 specifications
***opencompute.org**/wiki/Server/Mezz*

Mellanox OCP Products
mellanox.com/ocp

Mellanox OCP-inspired
opencompute.org/products?query=mellanox

Call To Action

Choose NICs combining Secure Boot with Cloning Protection

- Secure Boot alone doesn’t solve hardware attacks
- Cloning Protection using attestation protocol requires keeping a log of device-secrets
- Prefer Device-based Cloning Protection

Project Specification: opencompute.org/wiki/Security

OCP REGIONAL SUMMIT

Open. Together.

OCP Regional Summit

26–27, September, 2019