Setting Hardware Root-of-Trust from Edge to Cloud, and How to Use it

Computer & Electronics Security Application Rendez-vous, 2022

Florent Chabaud
Chief Product Security Officer
16/11/2022
Trust is not Security
Years of debates: should you trust cryptography?

- Clipper Chip (1993)
- Trusted Computing Platform Alliance (1999)
- Trusted Platform Module (2009)
- E. Snowden and other Leaks (2013-)
Root-of-Trust
An application of Kerckhoffs’ second principle

• Minimize the data to protect from threats

• Everything can be public but secret keys
  • Same for private keys

• Everything can be changed but public keys

• Hardware makes sense to protect confidentiality and integrity (e.g. smart card)
Attestation Mechanism

Trusted Computing Base

• How can I trust hardware for protecting keys?
• Is it really “my” hardware?
• Attestation Mechanism principle allows a device to authenticate itself to a verifier

• Each device must have a Unique Device Secret (UDS) which characterizes the attester device.

• A private authentication key unique to each device.
  • The key is immutable and certified by the provisioner.
• A private signature key unique to each device.
  • The key is updated and certified by the device owner.
What is a device?
Why firmware is important?

- Typical host architecture
  - A bus to interconnect devices
  - A high speed interconnection for memory
- Two Memory Access modes
  - Indirect through CPUs
  - Direct through DMA

- For instance, NIC devices make extensive use of DMA
- What if their firmware is trapped or tainted?
What firmware?
Dozens of firmware!

- Business context: Enterprise/EDGE Servers + HPC
  - Hardware is managed by a Baseboard Management Controller (BMC), Racks by RMC, Power by PMC, Hydro by HMC, etc.

- BMC firmware
  - U-boot
  - BMC OS
- BMC Recovery firmware
- UEFI BIOS
- OS
- CPUs
  - Microcode
  - GPUs
- Devices
  - NIC
  - Disk
- FPGA/CPLD
  - 1, 2?... 9!

<table>
<thead>
<tr>
<th>Sl#</th>
<th>Device Name</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MAIN FPGA</td>
<td>FPGA</td>
</tr>
<tr>
<td>2</td>
<td>IO FPGA</td>
<td>FPGA</td>
</tr>
<tr>
<td>3</td>
<td>PCPLD</td>
<td>CPLD</td>
</tr>
<tr>
<td>4</td>
<td>PFR CPLD</td>
<td>CPLD</td>
</tr>
<tr>
<td>5</td>
<td>MSM FPGA</td>
<td>FPGA</td>
</tr>
<tr>
<td>6</td>
<td>GPU CPLD0</td>
<td>CPLD</td>
</tr>
<tr>
<td>7</td>
<td>GPU CPLD1</td>
<td>CPLD</td>
</tr>
<tr>
<td>8</td>
<td>EDSFF CPLD 0</td>
<td>CPLD</td>
</tr>
<tr>
<td>9</td>
<td>EDSFF CPLD 1</td>
<td>CPLD</td>
</tr>
</tbody>
</table>
Open Compute Project
ARM, Meta, IBM, Intel, Nokia, Google, Microsoft, Dell, Hewlett Packard Enterprise, NVIDIA, Cisco, Lenovo and al...
The HPC challenge
Finding room for trust

• BullSequana X2410
  • 3 Compute nodes
  • 2 AMD Epyc Processors per node

• BullSequana XH2000
  • 32 blades per cabinet = 96 compute nodes
  • 30 cabinets = 5760 CPU
  • + management nodes, storage nodes, etc.
# BullSequana Root-of-Trust Design

## Why ATOS made a different choice

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sovereignty</strong></td>
<td>Unknown hardware is difficult to trust.</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Need to address all kind of hardware (Edge to HPC) with different physical constraints</td>
</tr>
<tr>
<td><strong>Agility</strong></td>
<td>Ability to add rapidly additional security features</td>
</tr>
<tr>
<td><strong>Agnostic</strong></td>
<td>All our products to benefit of the same recoverability features whatever their CPU / GPU / HW</td>
</tr>
<tr>
<td><strong>Hardware security level</strong></td>
<td>Leverage existing security hardware features to anchor security</td>
</tr>
</tbody>
</table>

- Use well-known hardware
- No additional hardware
- Software based security
- BMC is the RoT
- Use ARM TrustZone
Components for BullSequana Trusted Computing Base
Certifiable at high level

• **ARM OTP mechanism**
  - Well-known security feature to anchor keys and secure configuration of the SoC ARM core

• **ARM TrustZone**
  - Simple and robust technology used in cell phones for years

• **Secure OS (ProvenCore)**
  - µOS whose security has been mathematically proven
  - Evaluation Assurance Level (EAL) 7 is the highest level of evaluation for Common Criteria
  - It means that the security properties are immune to ANY input presented to the OS
Platform Firmware Resiliency

Initial level of PFR

- **Chain-of-Trust for Detection - CTD (Secure boot)**
  - BMC FW boot / BIOS/OS boot
  - ARM CPU OTP provides HW Root of Trust
  - ProvenCore is launched as a second stage for boot. It stores keys securely.
  - ProvenCore double checks the initial boot stage of the host OS

- **Chain-of-Trust for Upgrade – CTU (Firmware Update)**
  - ProvenCore is the Root of Trust for any FW component update (BMC, CPLD, FPGA, BIOS)
Chain-of-Trust for Detection
Complements the Intel CPU native hardware security features

INTEL CPU
OS Loader
Secure Boot image (PEI)
TeaCore in Trusted Zone
Initial Boot Block
Launch validated image

ARM CPU
Secure Boot ROM code
Secure Boot image U-Boot-spl
U-Boot
TeaCore in Trusted Zone
OpenBMC
FIT image
OpenBMC
TeaCore in Trusted Zone
Verify image signature

OS Loader image
OEM Boot Block
INTEL CPU
INTEL CPU
INTEL CPU

Intel TXT

Flash Memory Area
Storage Area
Root-of-Trust overall scheme
Chain of trust for detection and upgrade

SOC

BMC Firmware Payload

First stage

BMC boot

OS Firmware Payload

OS boot

RT

HSM

CTD

CTU
# Certified HSM appliance

*Trustway Proteccio by Atos*

## Keys

<table>
<thead>
<tr>
<th>Keys</th>
<th>Backup Shamir Scheme</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV</td>
<td>1 out of 3</td>
<td>Automated</td>
</tr>
<tr>
<td>PROD CoT</td>
<td>3 out of 6 on 2 sites</td>
<td>Automated</td>
</tr>
<tr>
<td>PROD RoT</td>
<td>3 out of 6 on 2 sites</td>
<td>CIK: 1 out of 3</td>
</tr>
<tr>
<td>SPARE RoT</td>
<td>3 out of 6 on 2 sites</td>
<td>From backup only</td>
</tr>
</tbody>
</table>
Addressing the HPC challenge
Using Trusted Execution Architecture (TEA) in each BMC

- All 2000+ nodes have a BMC with TEA
- We have the eggs; we can build the chicken!
- We can build a shared secret known to the TEAs
- And use it to protect internal communications
Conclusion
And envisioned next steps

• Next generation of BullSequana servers from Edge to Cloud and HPC will embed a Trusted Execution Architecture

• Trust in Atos' TEA is founded on:
  2. Private keys protected by an RGS certified Atos Trustway Proteccio HSM.
  3. The well-known ARM TrustZone technology embedded in the existing BMC component of our platforms.
  4. The hardened operating system TeaCore developed by ProvenRun on Atos specification and based on their formally proven and EAL7 certified operating system ProvenCore

• Initial security features implemented:
  1. Secure Boot (Chain-of-Trust for Detection)
  2. Firmware update (Chain-of-Trust for Upgrade)

• Envisioned next steps
  • Internal and third-party security assessment
  • Leverage the benefit from a Trusted Execution Environment to develop additional security features (e.g., TPMfw)
  • Adapt CTD to other CPUs such as EPI's chips
  • Take in account hybrid architectures mixing devices from different vendors
Thank you!

For more information please contact:
M +33 675 084 850
florent.chabaud@atos.net