Securing The Hardware Platform in the Cloud: Cerberus Present And Future

Badriddine Khessib
Senior Director
Azure Hardware Infrastructure
Azure Hardware | Project Olympus

100% inhouse design by Microsoft
Contract manufactured by ODMs

Open Source Development Model
Develop hardware at cloud speed, jointly with community and industry

Industry Ecosystem
Vibrant ecosystem for next generation datacenter hardware
Open Source Hardware deployed in Azure Datacenters

Flexible and Modular design to handle wide variety of public cloud workloads

**Compute**
- Intel, AMD, ARM64 CPUs
- High density GPU expansion for HPC/AI
- NVM (DRAM+battery) and 3DXP for low-latency

**Storage**
- High density HDD and Flash expansion
- Microsoft custom designed SSDs

**Networking**
- 50 Gbps networking
- Accelerated VMs using FPGAs
Rethinking system security at cloud-scale

**LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group**

ESET researchers have shown that the Sednit operators used different components of the LoJax malware to target a few government organizations in the Balkans as well as in Central and Eastern Europe.

**Vulnerabilities in modern computers leak passwords and sensitive data.**

**Microcode Updates for the USENIX 2017 paper: Reverse Engineering x86 Processor Microcode**

**SGX side-channel attacks**

Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing

**Bloomberg Businessweek**

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

**Meltdown**  **Spectre**
Hardware Security Threats

### Firmware Vulnerabilities

- BIOS
- BMC
- NIC
- FPGA
- SSD
- Option ROMs
- GPU’s
- HBA’s
- Etc...

**LoJax**: First UEFI rootkit found in the wild, courtesy of the Sednit group

- Higher Likelihood, medium sophistication
- Can be mitigated with engineering investments

### Hardware Tampering

- Very sophisticated, nation-state level
- Risk mitigated mostly via supply chain controls
NIST 800-193: Protect, Detect, Recover

- Authenticate integrity of all firmware updates
- Root(s) of trust & chain(s) of trust across the platform

- Detect unauthorized access or corruption
- Generate traces & events to help detect anomalies

- Restore firmware to state of integrity
- Automatic, Automatable and manual recovery scenarios

What is Cerberus

1. A set of **platform requirements**
   - E.g. Power sequencing while establishing trust

2. A set of **requirements** for ensuring **firmware integrity**
   - E.g. how to verify firmware integrity at boot
   - E.g. how to verify firmware signatures during updates

3. A **chip** that helps you implement the requirements
Project Cerberus – Hardware Root of Trust

Hierarchical topology provides scalable attestation

Prevents unauthorized access pre-boot, boot-time, run-time

Platform Secure Boot Policy enforcement
## Project Cerberus Controller

**Dedicated security microprocessor**
- Internal secure SRAM, secure Flash.

**Contains crypto acceleration blocks**
- SHA / AES / TRNG / PKA

**One Time Programmable (OTP) memory for Key persistence**

**Hardware Physically Unclonable Function (PUF)**

**Device Identifier Composition Engine (DICE)**

**SPI/QSPI bit-stream filter interface**

**Deployed on Project Olympus platforms**

<table>
<thead>
<tr>
<th>Micro Processor</th>
<th>AES-256</th>
<th>TRNG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power &amp; Clock Unit</td>
<td>PKA</td>
<td>SHA2</td>
</tr>
<tr>
<td>POR, OCS, PLL, Clock Out</td>
<td>SRAM PUF</td>
<td>OTP</td>
</tr>
<tr>
<td></td>
<td>Flash</td>
<td>I2C</td>
</tr>
<tr>
<td></td>
<td>ADC</td>
<td>Temp Sensor</td>
</tr>
<tr>
<td></td>
<td>SPIFI</td>
<td>SPI/QSPI Filter</td>
</tr>
<tr>
<td></td>
<td>SRAM</td>
<td>ROM</td>
</tr>
</tbody>
</table>
Why Cerberus Next?

- Standardize secure boot for peripheral devices
  - Some implementations are not so secure!
- Harden against physical intrusion scenarios
  - Man-in-the-middle attack
- Secure key/measurement storage
- Advanced key management
- Supply chain security
  - DeviceID an ManufacturerID authentication and signing
Cerberus Continued Integration

Silicon Integrated RoT
Compatible with Cerberus Discrete
Enhanced Features:
- Secure key/measurement storage
- Advanced key Management
Open Design
- Open Firmware
- Open RTL
Call To Action

Participate in OCP Security Project

Complete Cerberus V1 Spec

Start the Cerberus Next Silicon Definition

Visit MS and partner booths to see Cerberus in action
DNN Architecture and Benchmarks

THANK YOU

Marc Tremblay
DE Azure CSI