Using the NOVA Microhypervisor for Trusted Computing at Scale

Udo Steinberg
Agenda

❖ NOVA Microhypervisor Overview
  ➢ Architecture, Scalability
  ➢ Innovation Timeline

❖ Trusted Computing
  ➢ Verified vs. Measured Boot / SRTM vs. DRTM
  ➢ Intel Trusted Execution Technology (TXT)
  ➢ Trusted Platform Module (TPM)
  ➢ Integrity Measurement of NOVA and Root-PD

❖ Q & A
BedRock Ultravisor Architecture

VM (Linux) | VM (Windows) | VM (Appliance) | VM (RTOS) | VM (Unikernel)

VMM | VMM | VMM | VMM | VMM

UART Multiplexer | VirtIO Socket Multiplexer | Network Multiplexer (Virtual Switch) | UART Driver | Storage Driver | Platform Manager | Session Manager | Network Driver | Host Applications

Master Controller (Root Protection Domain)

NOVA Microhypervisor (ARMv8-A or Intel x86-64)

Ultravisor™

Formal Verification of Bare Metal Property™
Scaling NOVA from Embedded to Cloud Servers

All trademarks and brand names are the property of their respective owners. All company and product names used in these slides are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.
Both using UEFI firmware with ACPI support
NOVA / Server: 3rd Gen Intel Xeon-SP (c6i.metal)
NOVA Microhypervisor: Innovation Timeline

NOVA release cadence is ~2 months
What Problem Does Trusted Computing Solve?

- Once you have a formally verified software stack
  - and a compiler that produced a qualified set of binaries for the target architecture
- How do you ensure that some computer is running those binaries
  - and not some other (malicious) software instead
  - before you entrust that computer with your data or secrets
- In other words, how can you
  - either restrict the software that a computer will launch
  - or determine what software has been launched on a computer
Verified Boot: Static Root of Trust

- Boot policies are enforced during the boot process
- Starting with the Core Root of Trust for Verification, the currently executing module verifies the integrity of the next module against a boot policy (e.g. UEFI db/dbx) ⇒ Chain of Trust
- Integrity measurement is a cryptographic hash ⇒ unique + indicative to changes in the module
Integrity measurements are extended into TPM PCRs during the boot process.

Starting with the Core Root of Trust for Measurement, the currently executing module extends the launch integrity measurement for the next module into the TPM.
DRTM Flow lets system boot into an untrustworthy state (initially)

- Measured Launch later “resets” system into a trustworthy safe state
- Takes control of all CPUs and forces them down a protected and measured code path
Intel Trusted Execution Technology (TXT / CBnT)

❖ Provides a Dynamic Root of Trust (DRTM)

❖ Prerequisites
  ➢ CPU support (SMX features)
  ➢ TXT-capable chipset (DMA protection)
  ➢ TPM 2.0 (preferably) or 1.2
  ➢ SINIT Authenticated Code Module (ACM)

❖ Use Cases
  ➢ Remote Attestation (via TPM Quote)
  ➢ Local Attestation (via Launch Control Policy)
GETSEC[SENTER] Late Launch Sequence

Design Decision
NOVA late-launches itself (~650 LOC)

Unrecoverable failure causes TXT Shutdown

GETSEC[SENTER] Late Launch Sequence Diagram:

- **ILP**
  - Load ACM
  - Load MLE
  - Launch (DRTM)

- **RLPs**
  - SENTER Event broadcast
  - Each CPU sends ACK

- **SENTER Event**
  - All CPUs in secure environment

- **Measured Launch Environment (NOVA)**
  - SINIT launches MLE
  - ILP launches SINIT ACM

- **GETSEC[WAKEUP] for RLPs**

ILP broadcasts SENTER message
Each CPU responds to SENTER event
Each CPU issues ACK
ILP continues once all ACKs received

NOVA Microhypervisor
Udo Steinberg - FOSDEM 2024
A verifier can use the crypto agile event log to recompute/validate the composite value in each PCR.
Integrity Measurement (NOVA)

What (not) to include in integrity measurement requires careful consideration:

- Sensitive to: modifications in NOVA measured region, command-line parameters
- Insensitive to: hardware platform, memory map, multiboot modules, code self-patching

Build system prints reference integrity measurements for NOVA
Extending the Chain of Trust into User-Mode

❖ Compute the Root-PD launch integrity measurement
  ➢ Define the attestable region to measure
  ➢ Compute the integrity measurement of that region
    ■ Either using TPM Hash/Event Sequence (maximum crypto agility)
    ■ Or using a SW implementation in NOVA (maximum performance)
❖ Drive the Trusted Platform Module
  ➢ Different MMIO Interfaces
  ➢ Different TPM Families
❖ Append integrity measurement to the TPM event log

Time for measuring a 2 MiB image into a PCR

<table>
<thead>
<tr>
<th></th>
<th>NOVA (perf)</th>
<th>TPM2 (agility)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>15 + 2 ms</td>
<td>13700 ms</td>
</tr>
</tbody>
</table>
Integrity Measurement (Root Protection Domain)

- NOVA must measure Root-PD **before** launching it
  - Attestable region must be conveyed to NOVA without any invocations from Root-PD
  - Using ELF PHDRs (first non-writable PT_LOAD segment)

- Hash Computation
  - Digests computed by NOVA in C++ (for all supported hash algorithms)
  - Subsequently extended into PCR 19 (for all PCR banks)

- NOVA implements the FIPS 180-4 Secure Hash Standard (~130 LOC)
  - SHA1: -160
  - SHA2: -224, -256, -384, -512
Trusted Platform Module Infrastructure in NOVA

- Supports all TPM interface types (FIFO and CRB) (~250 LOC)
- Supports relevant command subset (Family 1.2 and 2.0) (~500 LOC)
  - Determine TPM capabilities (PCRs, Algorithms, …)
  - Perform PCR operations
- TPM localities control PCR access
  - Loc 2 belongs to NOVA Microhypervisor
  - Loc 1 belongs to User-Mode Environment
  - Loc 0 is for Legacy Use

<table>
<thead>
<tr>
<th>Locality</th>
<th>Usage</th>
<th>Can Extend</th>
<th>Can Reset</th>
<th>Next Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>CRTM</td>
<td>0-18, 23</td>
<td>17-22</td>
<td>PCR 17</td>
</tr>
<tr>
<td>3</td>
<td>SINIT ACM</td>
<td>0-20, 23</td>
<td>16, 20-23</td>
<td>PCR 17</td>
</tr>
<tr>
<td>2</td>
<td>NOVA</td>
<td>0-23</td>
<td>16, 20-23</td>
<td>PCR 19</td>
</tr>
<tr>
<td>1</td>
<td>Root PD</td>
<td>0-16, 20, 23</td>
<td>16, 23</td>
<td>PCR 20</td>
</tr>
</tbody>
</table>
Confidential & Trusted Computing Building Blocks

❖ Availability
➢ Cache & Memory Bandwidth Allocation Technology (CAT/CDP/MBA) - since 22.26

❖ Integrity
➢ Control-Flow Enforcement Technology (CET IBT+SSS) - since 22.17

❖ Confidentiality
➢ Total Memory Encryption with Multiple Keys (TME-MK) - since 22.52

❖ Measured Launch & Attestation
➢ Trusted Execution Technology (TXT/CBnT) - since 23.26

NOVA Microhypervisor
Udo Steinberg - FOSDEM 2024
Questions and Discussion

The NOVA microhypervisor is licensed under GPLv2

Releases: https://github.com/udosteinberg/NOVA/tags

More Information: bedrocksystems.com and hypervisor.org