An Inherently Secure Computer

Dr. Hamed Okhravi
MIT Lincoln Laboratory
5 March 2018
Motivation

Cyber requirements for mission success:

• Reliable, timely response
• Secure communications over untrusted networks
• Secure backend computing infrastructure

Example problems: Industrial control systems, military, voting systems, etc.
Cybersecurity Challenges

- Prevalent use of COTS/GOTS components in DoD systems
- None of these components has security built in
- Cyber defenses are often patchwork with intangible benefits
- Protections are often limited to best practices (i.e., hygiene)
- Little protection against Tier III-VI adversaries

Tiers based on dollars invested by attackers

DSB Resilient Military Systems and the Advanced Cyber Threat, Jan 2013

- Deter: Creates vulnerabilities using full spectrum
- Mitigate: Discovers unknown vulnerabilities
- Defend: Exploits pre-existing known vulnerabilities

Existential

Nuisance
## Secure Systems Lay of the Land

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MULTICS, Project MAC</td>
<td>PDP-11</td>
<td>x86, Windows, Linux</td>
<td></td>
<td>Inherently Insecure Systems Add-on Defenses</td>
<td>Inherently Insecure Systems Built-in Defenses</td>
<td>Inherently Secure Systems</td>
</tr>
</tbody>
</table>

### Inherently Insecure Systems
- Add-on Defenses
- Built-in Defenses
- Inherently Secure Computer

### Inherently Secure Systems
- Resilient mission computer seeks to redesign hardware and software for security, fundamentally changing the paradigm of adding defenses to legacy systems

**Time-sharing operating system**
- Predecessor to modern processors and OSes; popularized C

**Most systems we use today**
- Intel Skylake, DARPA CRASH, and MRC

**Trend toward built-in defenses**
- Fundamental redesign for security

---

An Inherently Secure Computer - 4
HO 03/05/18

Lincoln Laboratory
Massachusetts Institute of Technology
Vision

• Vision
  Create the inherently secure computer system of the future

• Goals
  – Create an inherently secure processor design
  – Implement the processor and integrate with proper software stack
  – Demonstrate it for a use case
  – Expand to other use cases

• Impact
  – Novel rethinking of computer architecture with security as a central goal
  – Demonstration on a mission use case
  – Reshape the cybersecurity landscape
Problem Statement

- Missing Authentication
- Violating Spec
- Unsafe Defaults
- Memory Safety
- Race Condition
- Input Validation
- Privilege Confusion
- Side Channels

Design Vulnerabilities

Implementation Vulnerabilities

\[ a = b + c; \]
Vision for Processor and OS Components

Current Model with a Safe Language (e.g., Rust)

- Legacy Processor
- Unsafe Libraries
- Unsafe Code

Inherently Secure Computer Model with a Safe Language (e.g., Rust)

- Safe OS
- Semantically Matched Processor
**Broader Vision**

**Vision:** Create a secure-by-design system in which the mission can succeed regardless of attempted attacks

Commercial legacy compute stacks and trends drive increased cyber vulnerability

**Resilience for duration of the mission**

Clean-slate “minimalist” stack built to guarantee resilience

**Resilient Mission Computer**

- Authenticated User and Monitored Program
- Inherently Safe HLL to Minimize Attack Surface
- Validated Secure OS Developed in HLL
- Semantically Matched Secure Processor
  - Hardware directly implements HLL semantics to remove vulnerabilities
  - Checking built into the hardware to guarantee secure execution
  - Anti-tamper for CPI protection

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MULTICS, Project MAC</td>
<td>PDP-11</td>
<td>x86, Windows, Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

New computer architecture provides inherent security and guarantees mission success
### Technology Enablers for Inherently Secure Computer

<table>
<thead>
<tr>
<th>Validated, Secure OS</th>
<th>Semantically Matched Secure Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Preventing large classes of attacks using safe languages</td>
<td>• Semantically rich processor aware of security requirements</td>
</tr>
<tr>
<td>• Security enforced among all software layers</td>
<td>• Assured enforcement of security checks in the processor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitored Program</th>
<th>Authenticated User</th>
<th>Anti-Tamper</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Monitoring mission requirements</td>
<td>• Strong continuous authentication</td>
<td>• Cyber seals to detect tampering</td>
</tr>
<tr>
<td>• Detecting hard-to-prevent attacks</td>
<td>• Proper attribution of actions</td>
<td>• Side channels to detect supply chain attacks</td>
</tr>
</tbody>
</table>

An Inherently Secure Computer - 9
HO 03/05/18
An Inherently Secure Computer

Time Horizons for Technology Enablers

Initial Proof of Concept
- Validated, Secure OS
- Semantically Matched Secure Processor

Extension and Expansion
- Monitored Program

Full Vision
- Authenticated User
- Anti-Tamper

TIME
- 2020
- 2023
- 2026
Current Campus Collaboration and Opportunities

• Current Collaboration:
  – Dr. Howie Shrobe (HW Security)

• Opportunities:
  – Operating Systems
  – Programming Languages
  – Compilers
  – Formal Methods
  – Architectures
  – Secure Enclaves
  – AI
  – Cryptography
Summary

• Large classes of attacks are possible because of legacy design choices
• Inherently Secure Computer envisions a rethinking of computer architecture with ‘security’ as its central goal
• A combination of hardware and software innovations aim to prevent attacks by design
• It aims to provide a more even playing field for defenders
• Focus is on ‘mission success’ rather than general notions of security
• We are looking for new collaboration opportunities