SYSTEMS ENGINEERING RESEARCH CENTER

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

The Feasibility of Enhancing the Security of Complex Systems Through the Disaggregation of Security Components to Asymmetric Multi-Processors

Sponsor: DASD(SE)

By

Dr. David J. Coe and Dr. Jeffrey H. Kulick

9th Annual SERC Sponsor Research Review

November 8, 2017

FHI 360 CONFERENCE CENTER

1825 Connecticut Avenue NW, 8th Floor

Washington, DC 20009

www.sercuarc.org

Outline

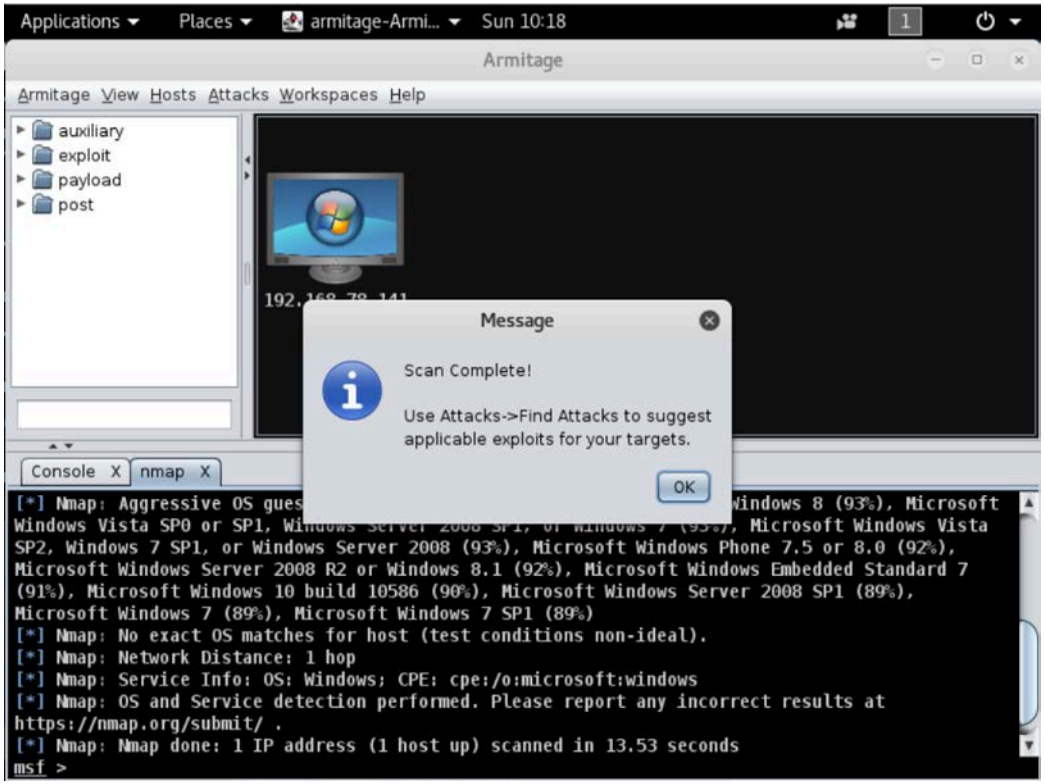
- Research Objectives
- Motivation
- Background
- Our Approach
- Advantages of Our Approach
- Research Plan
- Risks
- Questions

Research Objective

- Objective
  - Enhance the security of complex cyber-physical systems
- Our Strategy
  - Reduce the attack surface by deploying protection mechanisms into components that are not visible to the attacker
  - If they can't see it, they can't attack it…

Motivation - 1

- Cyber attack tools are now widely available and easy to use
  - An unskilled attacker can scan a targeted network, identify vulnerabilities in exposed systems, and select attacks that exploit those vulnerabilities
  - Tools include scripts to disable antivirus software and destroy forensic data



Armitage: a menu-driven cyber attack tool

Motivation - 2

- Fundamental issues
  - Security cannot be bolted on after system development
    - Security is an ***emergent property*** of the entire system including how the system is designed, implemented, deployed, used, and maintained
    - Security must be considered at the outset before development begins and addressed continuously through retirement of the system
  - The system under attack is untrustworthy since it is under attack
    - We cannot count on this system to protect itself on its own

- **We propose to transition to an inherently more *securable* computer system architecture**

Background: Security Coprocessors - 1

- Coprocessors have historically been used to improve performance (ex. I/O, floating-point, graphics, and cryptographic coprocessors)
- Trusted Platform Module (TPM) for secure generation/storage of cryptographic keys
  - Trusted Computing Group, https://trustedcomputinggroup.org/tpm-main-specification
- IBM 4758 crypto coprocessor added anti-tamper protections
  - "Extracting a 3DES key from an IBM 4758,", http://www.cl.cam.ac.uk/~rnc1/descrack/ibm4758.html
- Altera, Microsemi SoC Corp, and others investigated use of FPGAs to help secure the boot process
  - US Patent US 9600291 B1, "Secure boot using a field programmable gate array (FPGA), Altera Corporation, published March 21, 2017.
  - US Patent US 20150012737 A1, "Secure boot for unsecure processors," January 8, 2015.

Background: Security Coprocessors - 2

- DARPA System Security Integrated Through Hardware and Firmware Program (SSITH) seeks to mitigate common hardware vulnerabilities
  - Linton Salmon, "System Security Integrated Through Hardware and Firmware (SSITH)," DARPA Proposers Day Overview, April 21, 2017
  - 3+ year, $50M program
  - Vulnerability categories:
    - buffer errors, permissions/privileges/access control, resource management, code injection, information leakage/exposure, cryptographic errors, and numeric errors
  - Participants required to use RISC-V soft-core processor
  - Progressive restrictions on area and performance impacts
    - Chip area: < 50% ➔ < 30%
    - Performance: < 20% ➔ < 10%
    - Power impact: 0%

Our Approach

- Use an Asymmetric Multi-Processor System on a Chip (ASMP SoC) to create regions of isolated, trusted hardware
- Disaggregate the most critical security algorithms from the system under attack and deploy them to the isolated trusted hardware
- Allow these most critical security algorithms to execute unimpeded by attacks launched against the protected system

Advantages of Our Approach - 1

- Enhanced security through the use of ***SoC technology***
  - Integration of system components into a single packaged chip makes probing more challenging, especially as feature sizes decrease to nanometers
  - An attacker will need additional technical expertise and access to specialized hardware to successfully de-encapsulate and probe the SoC integrated circuit

- Enhanced security through ***encapsulation and information hiding***
  - Sequestering of the most critical security algorithms in the ASMP SoC but outside of the application processor makes them less visible to an attacker
  - An attacker who gains access to the application processor and examines the lists of running processes will see no information about those security algorithms

Advantages of Our Approach - 2

- Enhanced security through ***asymmetry***
  - As system designers, we control which which communication paths exist and their properties (read-only, write-only, or readable/writable)
  - Use this control to create ***asymmetry of exposure*** to isolate the hardware executing the most critical security algorithms
  - The use of an ASMP SoC which contains an FPGA allows us to exploit ***asymmetry of execution engines*** by deploying hardware implementations of security algorithms, which makes it more difficult for a remote attacker to alter or disable these algorithms without physical access
- Enhanced security through ***disaggregation***
  - A commonly employed technique which adds layers of software isolation to enhance the security of operating systems and hypervisors
  - We are proposing to add layers of hardware isolation via the ASMP SoC and disaggregate the security algorithms into trusted hardware

Research Plan - 1

- **Phase 1**
  - Threat mitigated: memory corruption/code injection
  - The embedded application processor is assumed to be untrustworthy
  - An ASMP soft-core processor will be provided memory layout information for the embedded application in advance
  - The ASMP processor will passively observe in real time the memory of the embedded application processor running on an RTOS
  - Deviations between the desired layout and the run-time memory contents will be annunciated to the operator through an independent communications channel

Research Plan - 2

- **Phase 1 - Plan of Work**
  - Projected Schedule: 12 months
  - Projected Budget: $300K

	Year 1			
	Q1	Q2	Q3	Q4
Phase 1				
Threat Modeling				
Prototyping				
Assessment				
Investigations				

- UAH Team Members
  - Dr. David J. Coe
    - Threat modeling/assessment, management tasks
  - Dr. Jeffrey H. Kulick
    - System architect
  - Dr. Aleksandar Milenkovic
    - Execution tracing, performance analysis
  - Engineering support staff
  - Graduate student researchers

Research Plan - 3

- **Phase 2**
  - Threat mitigated: return-oriented programming (ROP)
  - Real-time analysis of embedded application control flow graph
- **Phase 3**
  - Threat mitigated: attacks against Linux OS-level abstractions (scheduler, memory manager, etc.)
  - A trusted enclave is established in the otherwise untrusted application processor to provide information about OS-level abstractions to ASMP
- **Phase 4**
  - Threat mitigated: attacks against system-level correct behavior
  - Trusted enclave in untrusted application processor provides information about system-level abstractions to ASMP

Risks - 1

- **Risk #1 - Performance Impact on Real-Time Embedded Applications**
  - Mitigation - Use an asymmetric SoC which does not use resources required by the embedded application
- **Risk #2 - Insufficient Isolation Between ASMPs**
  - Mitigation - Use threat analysis to identify vulnerabilities and reduce attack surface

Risks - 2

- **Risk #3 - Obtaining Buy In and Adoption of New Secure Architectures by Developers**
  - —Mitigation - Hard evidence of enhanced security and education of next generation developers

- **Risk #4 - Evolving Technological Advances in Computing, Security, and Threats**
  - —Mitigation - Continuous analysis of evolving technologies and threats.

Thank you!

Questions?