RT-180: The Feasibility of Enhancing the Security of Complex Systems Through Disaggregation of Security Components To Asymmetric Multi-Processors

SYSTEMS ENGINEERING RESEARCH CENTER

Dr. David J. Coe (PI), Dr. Jeffrey H. Kulick, and Dr. Aleksandar Milenkovic

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Research Task / Overview

If they can't see it, they can't attack it…

- Investigate disaggregation of critical security algorithms into Asymmetric Multi-Processor System on a Chip (ASMP SoC)
- Determine ASMP SoC requirements
- Identify COTS ASMP SoC board(s) for proof-of-concept demonstration
- Develop research roadmap for future work

Goals & Objectives

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

Analysis of Prior Art

Coprocessors have historically been used to improve performance

- Examples: I/O, floating-point, graphics, and cryptographic coprocessors
  - Ryan Cowart, David Coe, Jeffrey Kulick, and Aleksandar Milenkovic, "An Implementation and Experimental Evaluation of Hardware Accelerated Ciphers in All-Programmable SoCs" in ACM SE '17: SouthEast Conference

Coprocessors are now employed to secure systems

- Trusted Platform Module (TPM) for secure generation/storage of cryptographic keys
  - Trusted Computing Group, https://trustedcomputingroup.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," Microsemi SoC , 1/8/2015.
- 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
  - Participants required to use RISC-V soft-core processor
  - Restrictions on area and performance impacts increase by phase

Phase	Chip Area	Performance	Power
1	< 50%	< 20%	0%
2	< 40%	< 15%	0%
3	< 30%	< 10%	0%

Observations

- You can't bolt on security
- DARPA, Altera, & Microsemi SoC are trying to build security in from the ground up

Methodology

- 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 algorithm to execute unimpeded by attacks launched against the protected system

Future Research

Phase	Approach	Threat Mitigated
1	Passive memory inspection by ASMP	Memory corruption, code injection
2	Control-flow verification	Return-oriented programming
3	Introduction of trusted zones	Threats against OS-level abstractions
4	Hypervisor assisted ASMP	Threats against system-level abstractions

Contacts/References

Dr. David J. Coe (coed@uah.edu)
Dr. Jeffrey H. Kulick (kulickj@uah.edu)
Dr. Aleksandar Milenkovic (milenka@uah.edu)

- Reece Johnston, Sun-il Kim, David J. Coe, Letha Etzkorn, Jeffrey H. Kulick, and Aleksandar Milenkovic, "Xen Network Flow Analysis for Intrusion Detection," 11th Cyber and Information Security Research Conference, Oak Ridge, Tennessee, April 5-7, 2016.
- David J. Coe, Jeffrey H. Kulick, Aleksandar Milenkovic, Sun-il Kim, and Letha Etzkorn, "An Approach to Securing Cloud and Internet of Things Applications, 2016 National Cyber Summit, June 7-9, 2016.
- Amrish K. Tewar, Albert R. Myers, Aleksandar Milenković, "mcfTRaptor: Toward unobtrusive on-the-fly control-flow tracing in multicores," Journal of Systems Architecture, Vol. 61, No. 10, November 2015, pp. 601-614, doi: 10.1016/j.sysarc.2015.07.005.
- Vladimir Uzelac, Aleksandar Milenković, Milena Milenković, Martin Burtscher, "Using Branch Predictors and Variable Encoding for On-the-fly Program Tracing," IEEE Transactions on Computers, Vol. 63, No. 4, April 2014, pp. 1008-1020, doi: 10.1109/TC.2012.267.
- Austin Rogers, Aleksandar Milenković, "Security extensions for integrity and confidentiality in embedded processors," *Microprocessors and Microsystems*, Vol. 33, Issues 5-6, pp. 398-414 (August 2009).