System Security Integration Through Hardware and Firmware (SSITH)

PM: Linton Salmon DARPA/MTO

Design & Security

SSITH Performers

Prime	POC
Charles Stark Draper Laboratory	Arun Thomas arun@draper.com
Lockheed Martin RMS	Jim Eiche james.eiche@lmco.com
MIT	Adam Chlipala adamc@csail.mit.edu
SRI International	Robert Watson robert.watson@cl.cam.ac.uk
UC San Diego	Dean M. Tullsen tullsen@cs.ucsd.edu
University of Michigan	Todd Austin austin@umich.edu
Galois, Inc.	Joe Kiniry kiniry@galois.com

Background

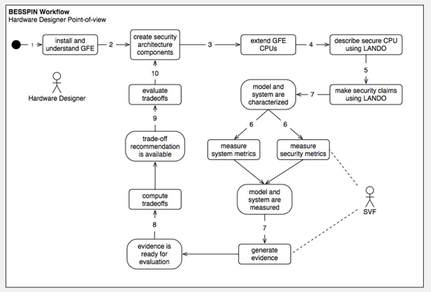
Eliminate hardware vulnerabilities

- Many cyber attacks are software exploiting hardware vulnerabilities
- SSITH closes hardware loopholes by restricting system to allowed states
- Verified using formal methods

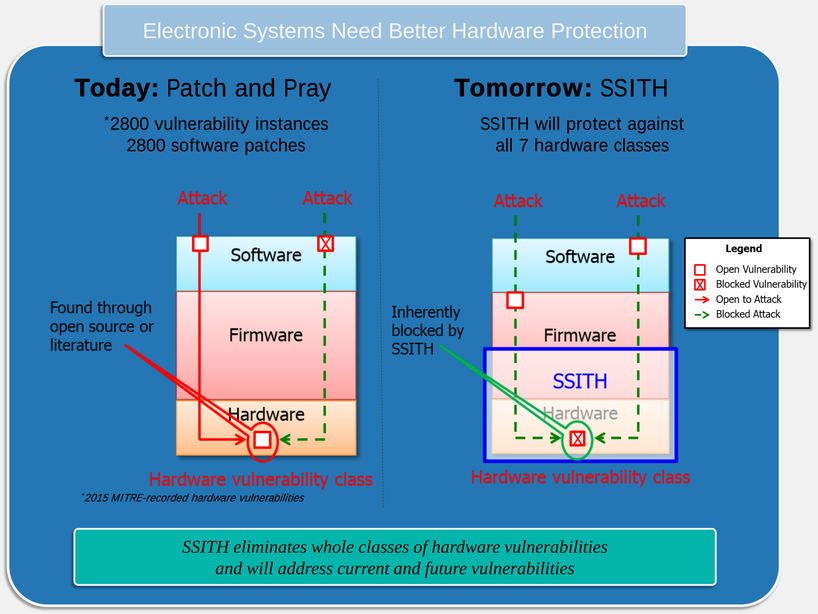
Galois, Inc.

Technical Approach

Automated system security metrics framework and tools; objective analysis; uses formal methods; GFE IP development and support: RISC-V baseline for evaluation.



SSITH Technical Approach



Charles Stark Draper Lab

Technical Approach

Every word has metadata + every instruction is checked based on flexible security micro-policies defined in software (DSL); compartmentalization; PPASS workbench.

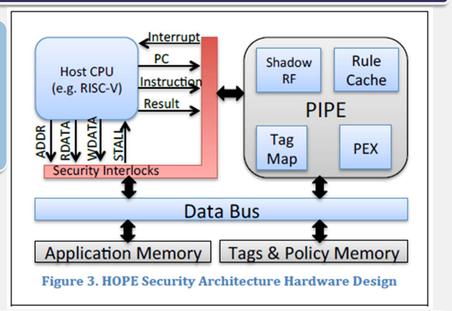
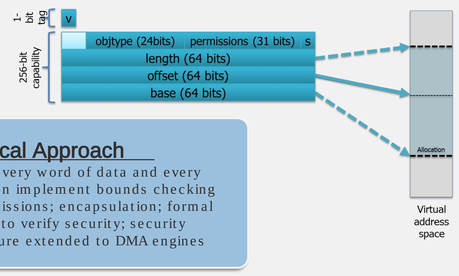


Figure 3. HOPE Security Architecture Hardware Design

SRI International



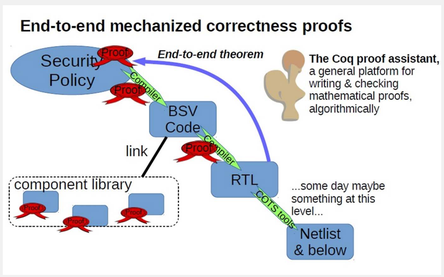
Technical Approach

Tags on every word of data and every instruction implement bounds checking and permissions; encapsulation; formal methods to verify security; security architecture extended to DMA engines

Massachusetts Institute of Technology

Technical Approach

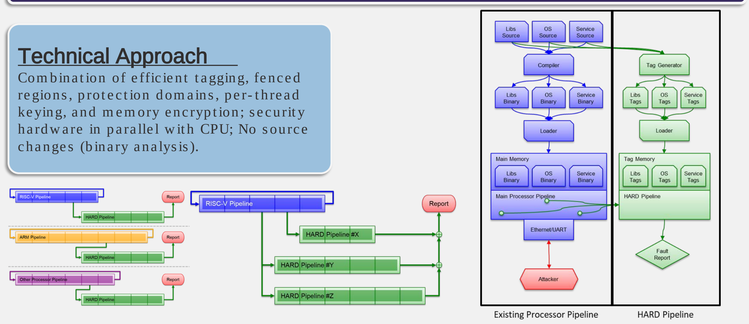
Hardware security compiler with end-to-end formal verification; generic support for tagging policies; compartmentalized secure enclaves.



Lockheed Martin RMS

Technical Approach

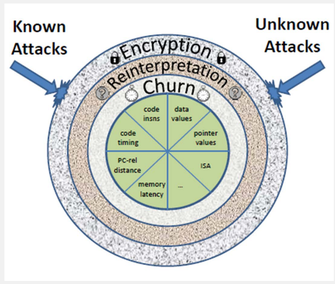
Combination of efficient tagging, fenced regions, protection domains, per-thread keying, and memory encryption; security hardware in parallel with CPU; No source changes (binary analysis).



University of Michigan

Technical Approach

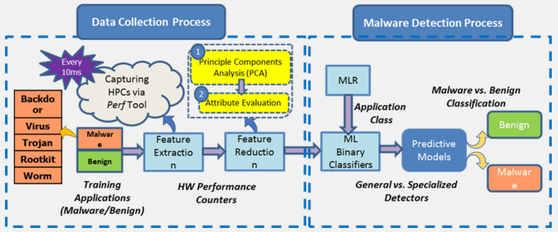
High entropy (hard to hack) plus rapid churning (no time to exploit) to mediate "undefined semantics"; tagging; encryption; relocation of memory areas.



University of California, San Diego

Technical Approach

Anti-fragility approach learns from attacks; machine learning based on Hardware Performance Registers; efficient X86 implementation leveraging micro-ops.



www.darpa.mil

THE ELECTRONICS RESURGENCE INITIATIVE