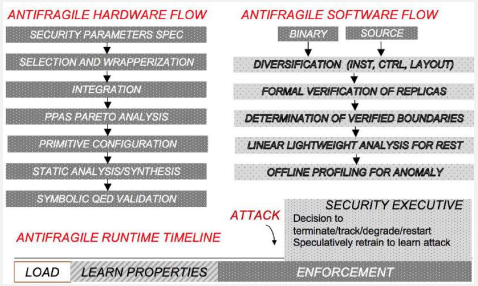
SSITH: TA1 (Hardware) Performers

Driving Applications: System Security Integrated Through Hardware and Firmware

Columbia University
Low-overhead, Anti-fragile architecture that can detect and track the provenance of an attack and can be retrofitted into legacy systems.



Source: Columbia University

Charles Stark Draper Lab
Implements security through tagging, policy management and security interlocks

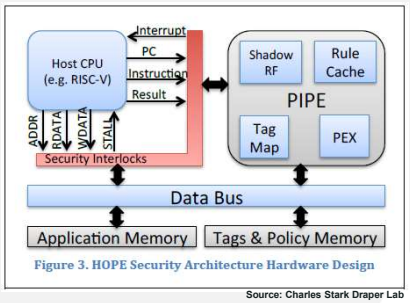
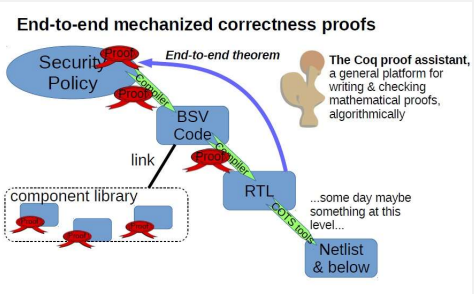


Figure 3. HOPE Security Architecture Hardware Design

Source: Charles Stark Draper Lab

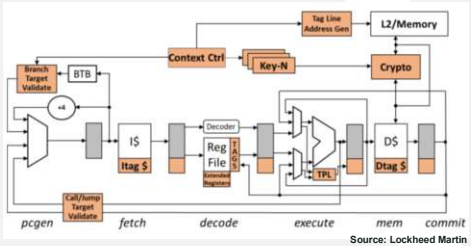
Team	Technical Area	PI	Collaborators
Columbia	1	Dr. Simha Sethumadhavan	Brown University, Stanford University
Charles Draper Laboratories	1	Mr. Christopher Lockett	Dorner Works Ltd., Dover Microsystems, University of Pennsylvania, MIT, Portland State University
MIT	1	Dr. Adam Chlipala	Accelerated Technology Inc.
Cornell	1	Dr. Edward Suh	
Lockheed Martin Rotary and Mission Systems	1	Mr. Brian Whipp	Binghamton University (SUNY), Lockheed Martin Advanced Technology Lab
SRI International	1	Dr. Peter Neumann	University of Cambridge, ARM Ltd., Ararat River Consulting LLC
University of Michigan	1	Dr. Todd Austin	Princeton University, The University of Texas at Austin
University of California, San Diego	1	Dr. Dean M. Tullsen	George Mason University

Massachusetts Institute of Technology
Extends and integrates three promising hardware security technologies: Bluespec, Kami and Samntum.



Source: Massachusetts Institute of Technology

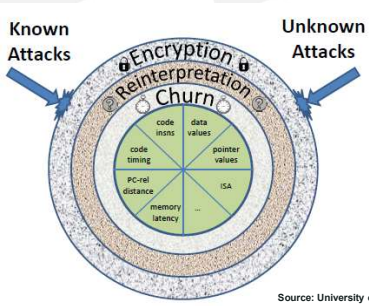
Lockheed Martin Rotary and Mission Systems
Will implement an architecture which consists of data and instruction word tagging, automatic bounds checking, and lightweight isolation protection domains.



Source: Lockheed Martin

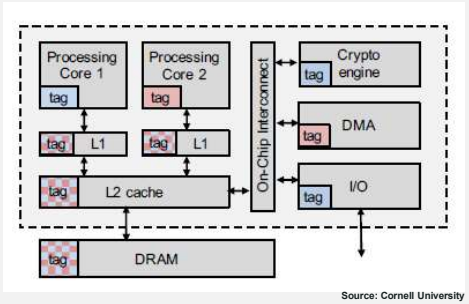
RISC-V Rocket Pipeline with HARD Extensions (in Orange.)

University of Michigan
Will build an architectures which protects information assets by using Ensembles of Moving Target Defenses (EMTDs) whereby Assets are encrypted or reinterpreted and undergo periodic churn, changing their encryption or interpretation keys.



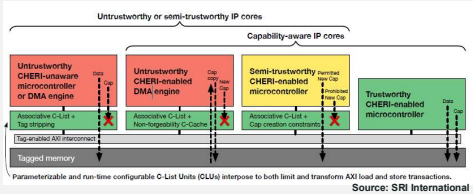
Source: University of Michigan

Cornell University
Implements a Tagged Information Flow control approach based on a tagged architecture where every 64-bytes of memory has two tags, an 8-bit confidentiality tag an 8-bit integrity tag.



Source: Cornell University

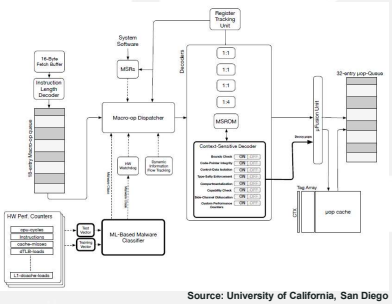
SRI International
Builds upon successful CHERI technology developed within the DARPA I2O CRASH program which mitigates memory-based exploits by strictly enforcing integrity, provenance validity, monotonicity, bounds, permissions, and encapsulation on C/C++ pointers.



Parameterizable and run-time configurable C-List Units (CLUs) interpose to both limit and transform AXI load and store transactions.

Source: SRI International

University of California, San Diego
Context-sensitive decoding for selective translation of instructions to micro-ops to allow for adaptation to constantly changing security levels. Machine-learning (in hardware) will identify and predict malware threats, appropriately set the threat level, and enable adaptive coverage of most likely threats.



Source: University of California, San Diego

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S.

Distribution Statement A – Approved for Public Release, Distribution Unlimited

THE ELECTRONICS RESURGENCE INITIATIVE