David Manz, PNNL, PM
Carl Miller, PNNL
Ken Masica, LLNL
Dan Quinlan, LLNL
John Munro, ORNL
Mark Pleszkoch, ORNL

Supply Chain Integration For Integrity (SCI-FI)

Cybersecurity for Energy Delivery Systems Peer Review

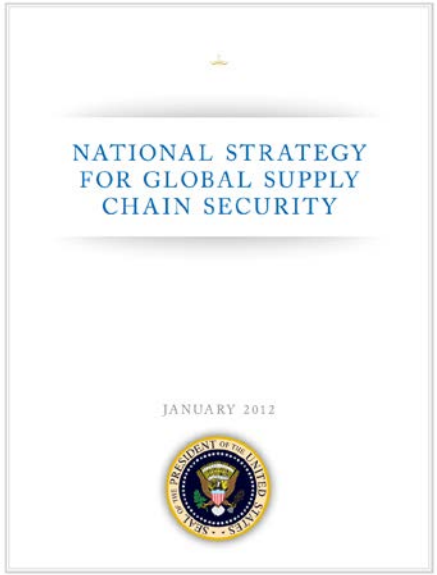
August 5-6, 2014

PNNL-SA-103976

Summary: Supply Chain Integration For Integrity

- **Objective**
  - The nation has identified **supply chain** security as a crucial part of securing **critical infrastructure**
  - Detect compromise of supply chain **integrity** for energy delivery systems

- **Schedule**
  - January 2013 – December 2015
  - November 2014: Proof of concept root of trust
  - January/Sept 2015: Mid-term/ final releases of software analysis into Rose
  - April 2015: Demonstration of hardware analysis performance
  - End: A suite of open source tools, demonstrations, and technology



- **Total Value of Award:** $3M
- **% Funds expended to date:** 56%
- **Performer:** PNNL
- **Partners:** ORNL, LLNL, PGE, vendors (including Itron)

Advancing the State of the Art (SOA)

- **An interdisciplinary approach addressing challenges of the supply chain in an integrated manner. The project is divided into three prongs:**
  - Evaluate **policy and architecture** for built-in supply chain integrity of trusted components
  - Analyze **software and firmware**
  - Address **hardware** supply chain concerns

Advancing the State of the Art (SOA)

- **Policy**
  - ORNL is *developing the policy* and processes needed to contextualize the hardware and software/firmware analysis tools and techniques created by PNNL and LLNL
- **Software/Firmware**
  - LLNL is *extending analysis capabilities* for both embedded field device firmware and energy management system application software
- **Hardware**
  - PNNL is *researching tools and techniques* needed to explore, identify, and attribute components of the state machines that integrated circuits are built upon to ensure accuracy and integrity of the hardware

Policy Scope

- **Use an experience-based threat model to understand and assess supply chain risks**
  - Vendor, parts supplier, third-party suppliers and services
  - Utility operations, renewable power sources, end-users
  - Organized crime, hostile governments, terrorist organizations
- **Identify segments of energy delivery system (EDS) supply chain amenable to implementing controls for trusted environment**
  - Use of certificates for hardware and software procurement
  - Use of keys and certificates for (limited) chain of custody tracking
- **Immediate supply chain concerns for hardware**
  - Secure boot
  - Work in trusted environment
- **Immediate supply chain concerns for software**
  - Initial procurement and installation
  - Maintenance and upgrades

Policy Approach: TPM Framework

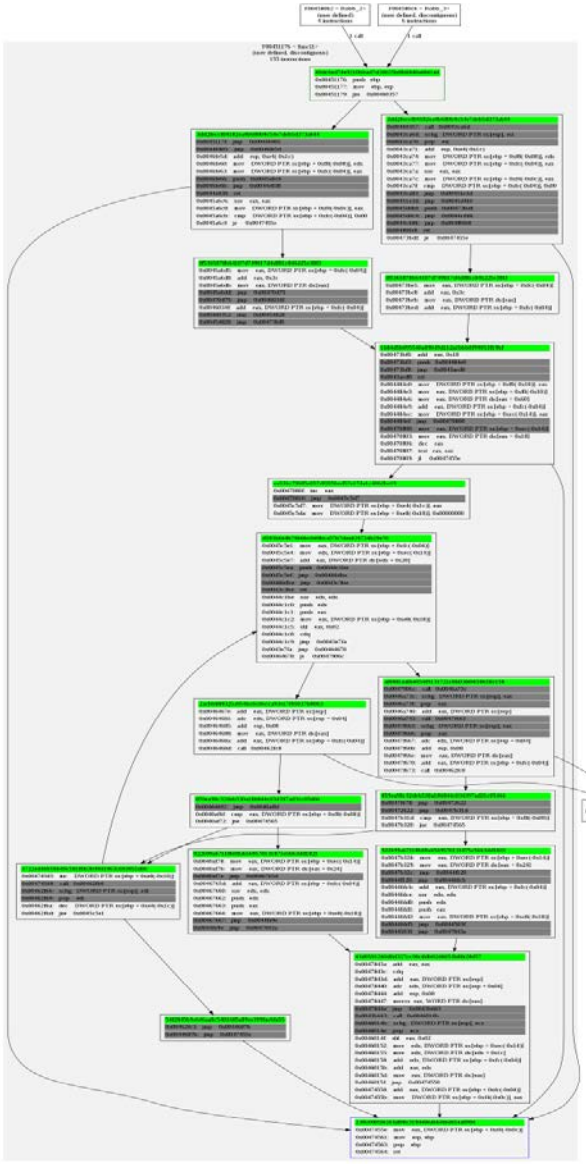
- **Concerns that can be addressed**
  - Secure boot
  - Authorization
  - Authentication
  - Remote attestation
  - Mechanisms for using keys and certificates to support supply chain integrity
  - Secure updates
  - Chain of custody
- **Framework can be implemented in hardware or software**
- **Use zones and conduits model to represent control, information, and ownership groupings in EDS of networked processors to implement Trusted Platform Module (TPM) framework**
  - Zones contain TPM components such as processors with their Trust Anchors and Trusted Computing Base
    - Greatest effort to establish and maintain trust must be expended in zones
    - An example: need separate zones for control centers for different functions/activities
      - Control
      - Engineering support
      - Business and administrative functions
  - Conduits handle transmission of encrypted data between zones

Software Scope

- **Security of the power grid must begin with the manufacturer of the components used to build and maintain the power grid**
  - Target detection of backdoors
  - Analysis of difference in firmware versions
  - Input/Output mapping and tainted flow analysis
  - Detection of anti-disassembly technology
  - Building analysis tool set for open distribution to utilities and vendors
  - Test suite of source code and binaries for evaluation of analysis technologies

Software Approach

- **Software Analysis**
  - Analysis of firmware (expect Advanced RISC Machine, but can also handle x86 and Power-PC)
  - Formal methods expertise to provide proof-based reasoning
  - Mixed concrete and symbolic interpretation to support static analysis
  - Abstract interpretation to support more efficient reasoning using abstract domains (state-of-the-art form of analysis for verification of safety properties)
  - Model checking to explore code paths (currently shared memory parallel)
  - Tools to support analysis of Trusted Computing implementations (work with ORNL)
  - Explore using high performance computing resources (distributed and shared memory parallel)

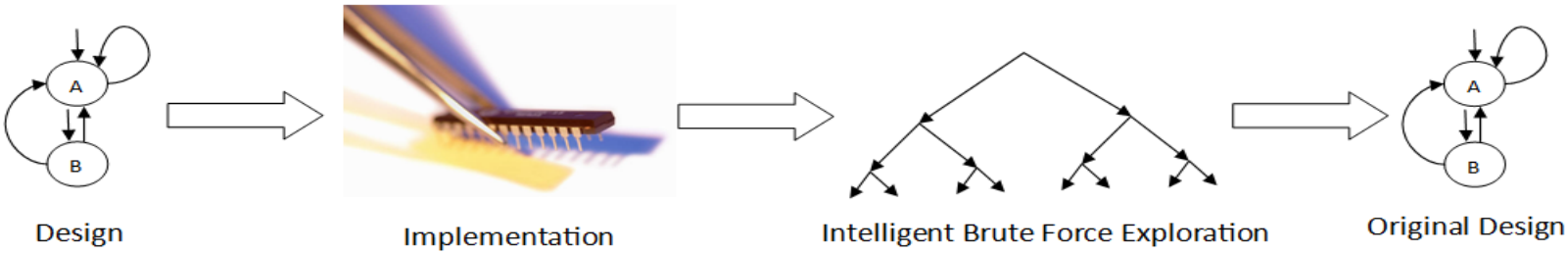


Hardware Scope

- **Integrated circuits (ICs)—that control our PCs, servers, SCADA systems, and the Smart Grid—are designed in the U.S. but put into silicon overseas**
  - The components that make up our national power grid and other critical systems are un-vetted and lack a trusted chain of custody
  - This supply chain gap puts systems that use these ICs at risk for modification or injection attacks
- **Performance of current non-destructive internal chip analysis methods are prohibitively time consuming**
  - Analysis could take thousands of years for a chip with just 70 states

Hardware Approach

- **By performing an *intelligent* brute force exploration of an integrated circuit, we can much more expeditiously build a picture of the state machine upon which the IC was designed – looking at the logic that drives the hardware rather than the physical hardware.**
  - We can then use that state machine to confirm the functions of the IC



  - After pin-profiling, actively interface with the I/O pins to some limited depth ("confidence level") to explore the inner workings of the IC
    - Use the recorded I/O values to create an initial state tree structure
  - Perform an initial exploration of the tree
    - Identify loops, terminators, and equivalent states which can significantly reduce the number of nodes with unexplored children
  - Obtain state information for unexplored leaf nodes, which are then treated as roots of new sub-trees and explored in a similar distributed fashion and recombined with initial, reduced tree, then reduced again

Challenges to Success

- **Appropriate validation**
  - Committee; utility feedback (BPA alliance, NIST framework, PGE); vendor engagement (Itron)
- **Chip scalability and functional identification**
  - Simulation demonstration
  - Iterative improvements to hardware demonstration
  - Library creation of sub-components
- **Extending software analysis to EDS domain**
  - Device firmware releases are packaged, compressed, and signed differently; SME was brought on to solve this issue in order to proceed with the primary software analysis goals of the project
- **Policy focus: vast area**
  - Survey landscape
  - Identify TPM, as applicable, with a specific focus for delivery

Progress to Date

- **ORNL**
  - Drafted report outlining the relevant information in support of SCI-FI policy recommendations
  - Proposed a Transitive Root of Trust (TRoT) model for the EDS using Trusted Computing Group TPM framework
- **LLNL**
  - Full representation of low level virtual machine (LLVM) code generation from binary executables
  - Demonstrated LLVM-based tools operating on binaries as part of technique to leverage third party program analysis tools that were not designed for binaries but work on binary executables
- **PNNL**
  - Identified and solicited industry vendor participation as part of the project team
  - Successfully performed pin profiling on a simple integrated circuit
  - Rediscovered a 50-state FSM on simulated integrated circuit with full correctness and completeness to a confidence level of 20 in under 5 minutes

Collaboration/Technology Transfer

- **Key partners identified in energy delivery domain**
  - Partners provide stakeholdership and advice early in the project
  - Partners are the key consumers and end users of the developing science and technology
- **Advisory Committee**
  - November 2013: Teleconference
  - January 2014: Teleconference follow-up with Itron
  - June 2014: Itron visit
- **Science and technology will be made widely available (open source) to ensure the broadest utilization and response possible**

Next Steps for this Project

- **Approach through the end of project**
  - Continue to engage vendor and industry stakeholders
    - Integration options
    - Demonstrations
    - Proofs of concept
  - Demonstrate a prototype trusted network TRoT
  - Demonstrate rediscovery of a medium sized IC and corresponding state machine
  - Final release of work into ROSE
  - Document results and transitions