U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

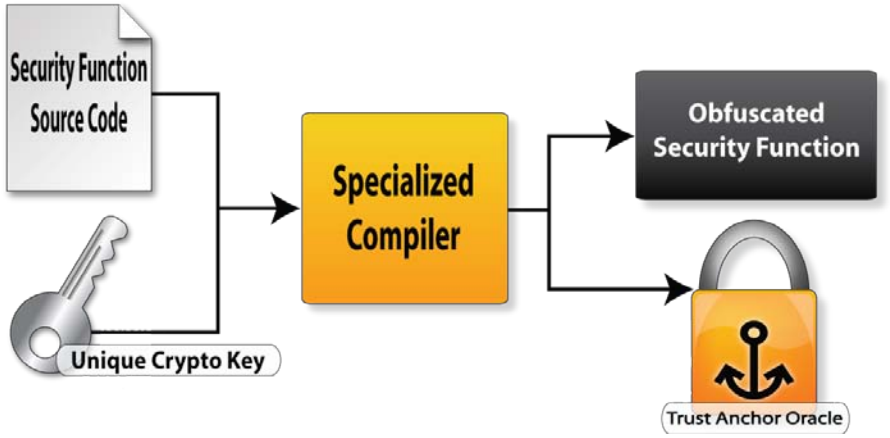
Adrian R Chavez

Sandia National Laboratories

Protecting PCS against Lifecycle Attacks Using Trust Anchors

Summary Slide: Trust Anchors / Code Seal

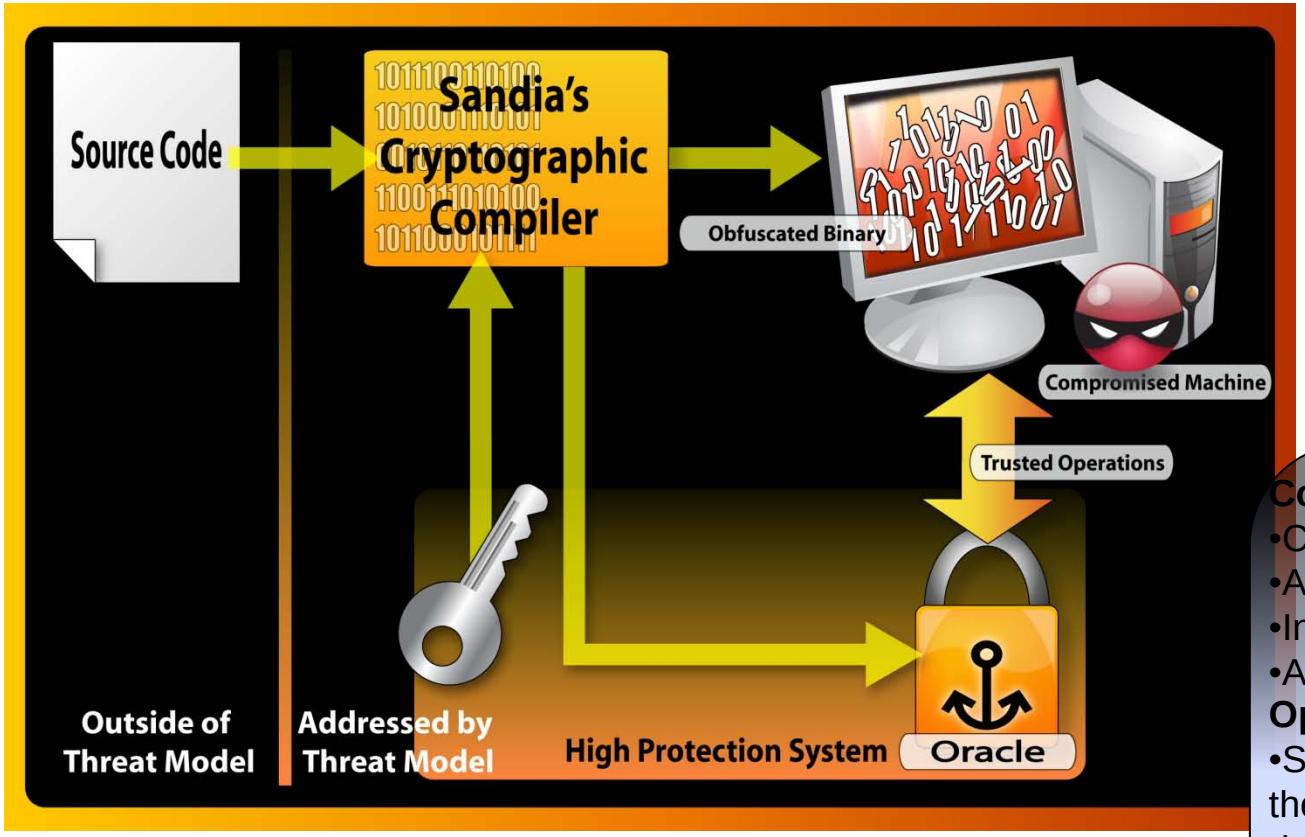
- **Outcomes:** Trust Anchor technology enables new security strategies addressing lifecycle attacks for which there are currently no relevant defenses



- **Roadmap Challenge:** Develop and Integrate Protective Measures
- **Major Successes:** Implemented and improved performance of trust anchor algorithms and implementation

- **Schedule:** Implement Trust Anchors 3/10; Performance Testing/Prototype 8/10; Scenario Development 1/11; Vulnerability Assessment 3/11
- **Level of Effort:** $400K
- **Funds Remaining:** $257K
- **Performers:** SNL
- **Partners:** Exploring industry opportunities to commercialize technology

CodeSeal



CodeSeal Features

- Cryptographic strength
- Assured authorization of execution
- Integrity of execution
- Anti-Reverse Engineering

Operational Requirements

- Secure communication between the Oracle and Obfuscated Binary during operations
- System-High protection of both the Oracle and the Key

Approach and Execution

- **Approach**
  - Implement Trust Anchors in Software
    - Advanced from State Machines -> Turing Machines
    - C++, Java, OCaml
  - Test, Validate, and Improve Trust Anchors
    - Show Any Algorithm Can be Secured by Trust Anchors
    - Improved Performance significantly ($O(n^2)$ reduction)
  - Apply Technology
    - Process Control System Applications
    - Smart Grid Applications

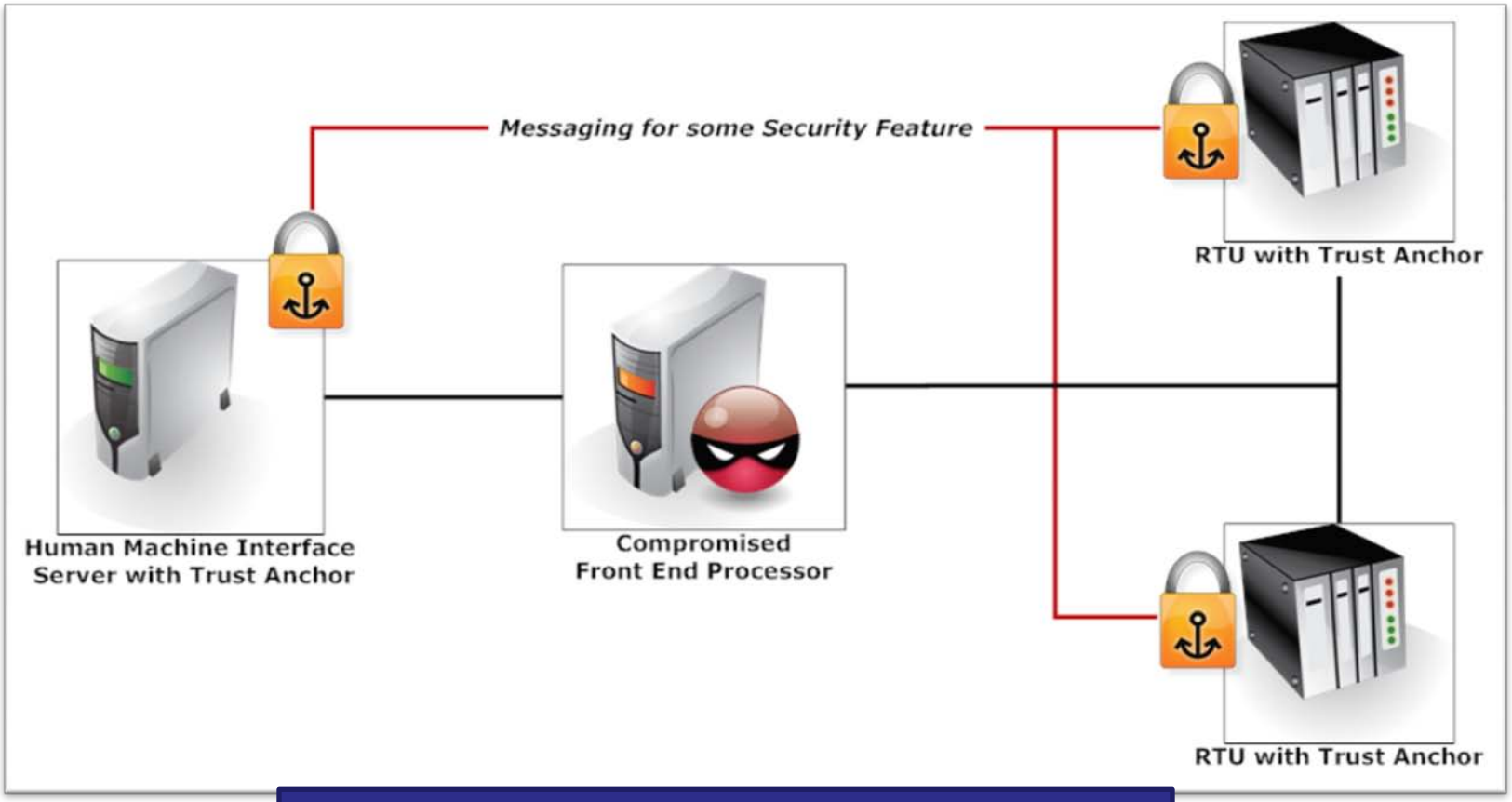
Approach and Execution

- **Metrics for Success**
  - Acceptable Performance of Trust Anchors
    - Prototype implementation complete
  - Position for Commercialization
    - Currently in early negotiations with industry
  - Progress in Addressing Lifecycle Threats
    - Use trust anchors as independent monitor
    - Use trust anchors to protect/trust code

Technical Accomplishments, Quality, and Productivity

- **Challenges to Success**
  - Convert State Machine Algorithms to Turing Machines
    - Modify Algorithms to include “memory”
  - Develop Meaningful Use Cases
- **Technical Achievements to Date**
  - Applied Trust Anchors to mitigate lifecycle attacks on a Front End Processor in a Mod/Sim Environment
  - Implemented Trust Anchors capable of securing any algorithm
  - Significantly improved performance

Trust Anchors in Process Control Systems Proof of Concept



Obfuscate authentication and validate critical control messages to remote

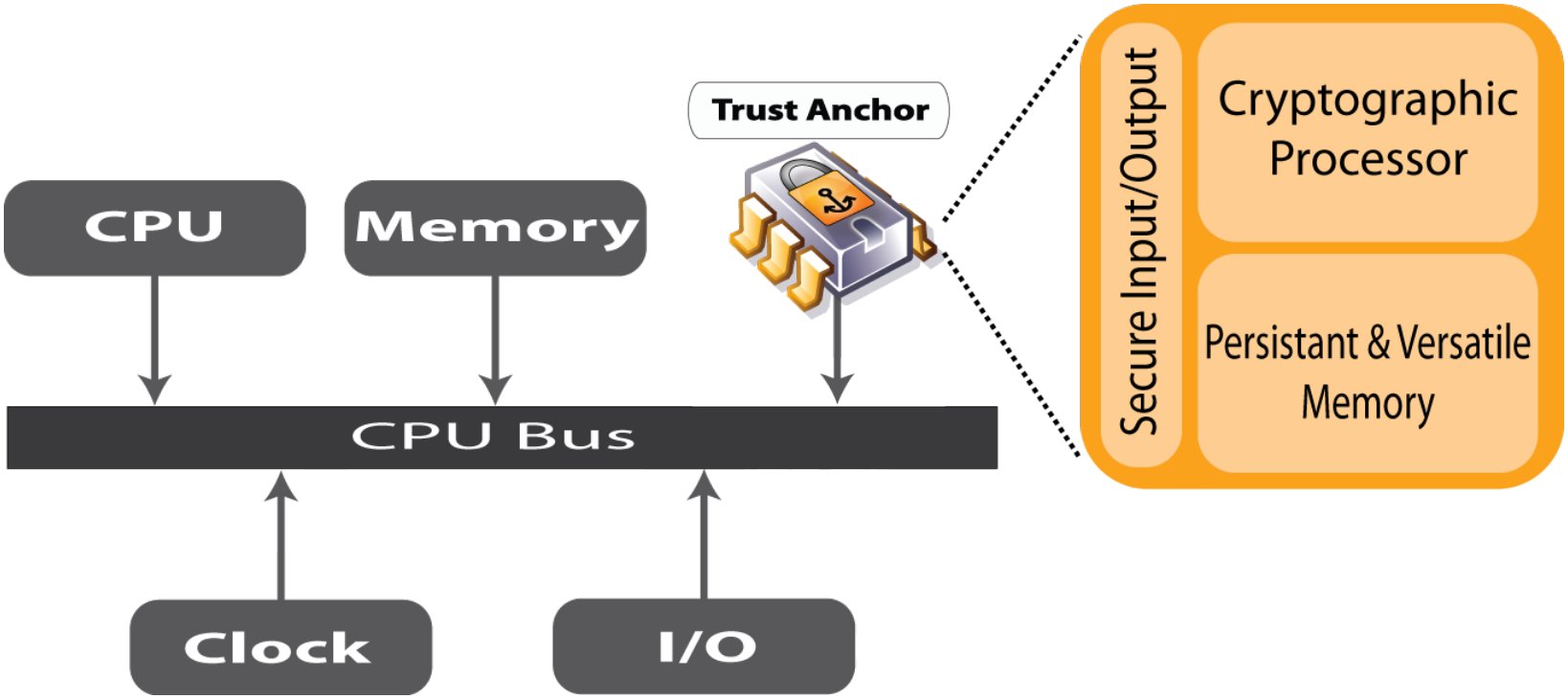
Technology Transfer, Collaborations, and Partnerships

- **Plans to gain industry input**
  - Currently in negotiations with industry to commercialize technology
  - Receiving feedback on how to apply technology
- **Plans to transfer technology/knowledge to end user**
  - Open publication of algorithms to help protect against lifecycle attacks
  - Continue educating and openly publishing research findings
  - Prototype tested in a virtual modeling and simulation tool to protect vulnerable Programmable Logic Controller and Front End Processor

Next Steps

- **Approach For Next Year**
  - Develop hardware implementation
  - Investigate operational requirements
  - Collaborate and incorporate feedback from Industry
- **Describe potential follow-on work, if any**
  - Feed R&D into industry to commercialize and validate technology
  - Potential use in smart grid/AMI applications

Next Steps: Trust Anchor Hardware Integration



Questions?