John Mulder

# Sandia National Laboratories Projects

## Cybersecurity for Energy Delivery Systems Peer Review

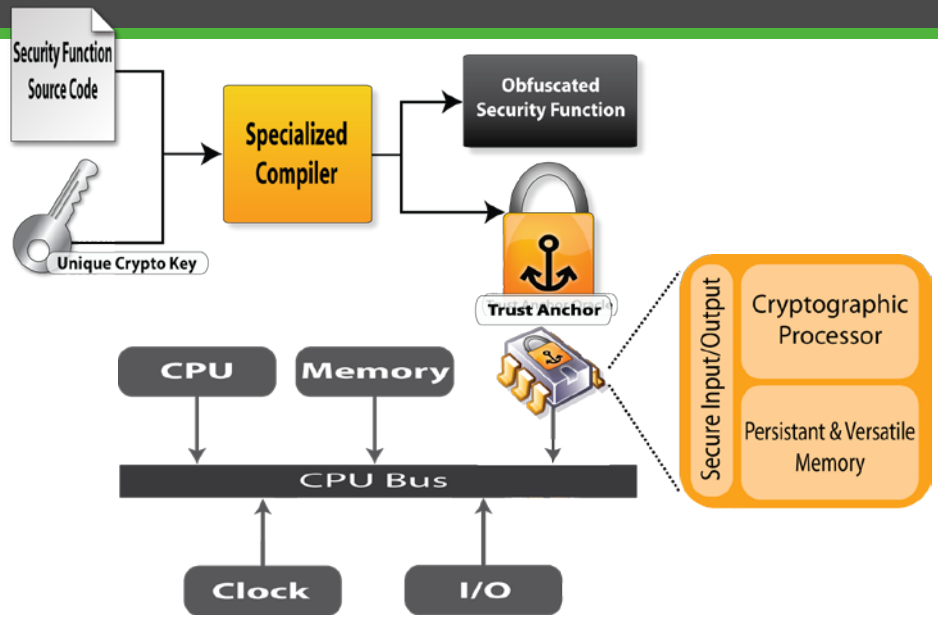
July 24-26, 2012

# Project Summaries

- **Trust Anchors / Code Seal**
  - Technology to obfuscate critical security functions.
- **PLC Integrity Checking**
  - Technology to download firmware from embedded field devices and issue alerts when modifications have occurred.
- **Formal Methods for PLC Logic Verification**
  - Application of formal proofs to verify security properties of PLC logic.
- **AMI ZigBee HAN Gateway Assessment**
  - Assessment of the security features in an implementation of a SEP 1.1 HAN in a residential smart meter.

# Summary: Trust Anchors

- **Objective**
  - Trust anchor technology enables new security strategies addressing lifecycle threats for which there are currently no relevant defenses.
- **Technical Approach**
  - Obscure monitoring and/or critical security functions so they cannot be reverse engineered
  - Trusted Platform Module (TPM) chip leveraged as a trust anchor
  - Demonstrate obfuscated software executing on a representative control system




- **Schedule**
  - Fully integrated TPM chip 5/12; Demonstrate TPM usage 7/12; Final report 8/12
- **Performers:** Sandia National Laboratories
- **Partners:** None

# Technical Approach and Feasibility

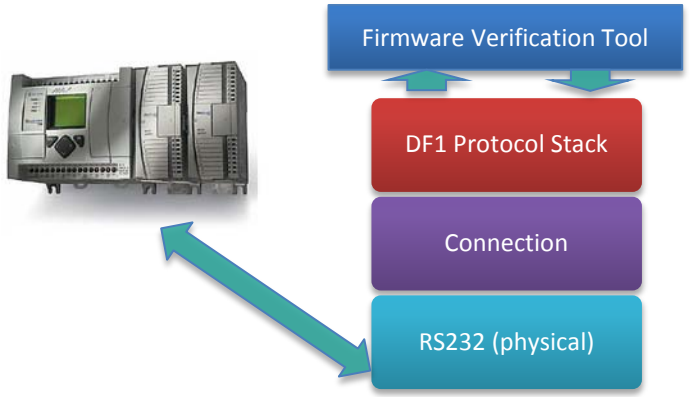
- **Approach**
  - Our systems are too complex to reliably analyze
  - CodeSeal can validate/implement and protect critical software functions
  - Integrate a trust anchor, TPM, into a system to enable trusted operations on untrusted systems
  - Software can execute with confidentiality and integrity with the aid of a resource limited trust anchor
- **Challenges to Success**
  - Performance
    - Increase resources on trust anchor
    - Leverage TPM chip for cryptographic key storage/generation
    - 97% increase in performance

# Collaboration/Technology Transfer

- **Major Accomplishments:**
  - Ported trust anchor to use TPM chip as a key generator/storage
  - Enhanced performance - ~97% increase in speed
- **Actual Progress (technical, $, and time) vs Planned Progress**
  - On schedule and budget to complete all project deliverables one month ahead of schedule
- **Plans to transfer technology/knowledge to end user**
  - Worked with industry to transfer early prototype
  - Performance enhancements make technology more viable for commercialization
  - Technology can be used to protect critical infrastructure system against lifecycle attacks and malware
    - Obfuscate a whitelist of approved executables, configurations, firmware
    - Obfuscate monitoring functions
  - Trust anchor can be expanded to tie a piece of software to execute on a specific piece of hardware
- **Combining Trust anchors and Physically Unclonable Functions (PUFs)**
  - Derive trust anchor key based on unique physical variations in the fabrication of a piece of hardware
  - 2 year effort to develop PUF and integrate with trust anchor
  - Effort to perform R&D, test, demonstrate, and perform outreach

# Summary: PLC Integrity Checking

- **Objective**
  - Produce a tool that alerts when the firmware on an embedded device is modified. This is a new capability that will detect a category of attacks that no current technology addresses.
- **Technical Approach**
  - Analyze the firmware update process
  - Develop tool to download firmware from the device over a network and compare to previous versions




- **Status**

  June 2012: Working prototype of system complete
- **Performers:** Sandia National Laboratories

# Technical Approach and Feasibility

- **Approach**
  - No systems currently exist for detecting when a device's firmware has been modified.
  - This technology can be used to detect next-generation attacks that modify field device firmware with little/no overhead/work.
- **Challenges to Success**
  - Firmware access techniques are undocumented and vary between vendors
    - Firmware update processes can be studied by building listeners/parsers
- **Status**
  - Prototype system supporting one PLC model is complete
- **Technology Transfer**
  - We are currently hoping to work with the device vendor to get the validation program into the hands of customers.

# Summary: Formal Methods for PLC Logic Verification

- **Objective**
  - PLC logic is typically designed by an engineer for a particular PLC installation, it rarely goes through rigorous security reviews.
  - Formal methods can affect long-term technological solutions to help remove known classes of defects from software components.
- **Technical Approach**
  - Evaluate formal verification techniques to reason about security properties of PLC logic.
  - Demonstrate that formal methods can be used to improve security properties of PLC logic.
- **Schedule**

  July 2012: Formal Methods feasibility report

  December 2012: Demonstration of a system using variations of PLC logic with different security properties

  January 2013: Technical report detailing the techniques and the results of their application.
- **Performers:** Sandia National Laboratories

# Technical Approach and Feasibility

- **Approach**
  - PLC logic is rigorously tested for safety concerns, but logic reviews for security issues are rare.
  - Academics have applied formal methods to PLC logic with reasonable success, but their approaches have not been adopted by industry.
  - We hope to apply formal verification and static analysis techniques to this problem in a way that can be easily used by industry.
- **Challenges to Success**
  - Most formal methods research is highly theoretical and difficult to apply to real systems.
    - We are approaching the problem with a very narrow scope.
    - Examining the use of static analysis techniques that are less comprehensive than formal proofs, but much easier to apply to real programs.
- **Status**
  - Project is in early stages, but approach seems viable and work is progressing.

# Additional Slides:
# SEP 1.1 Home Area Network Assessment

- **Objective**
  - Assess the security features of an implementation of a SEP 1.1 HAN provided by a residential smart meter to help the utilities and vendor better understand any vulnerabilities in their system.
- **Technical Approach**
  - Used the standards reviews done by NESCOR and SGIP-CSWG
  - Our own research into the ZigBee SEP.
  - Open ZigBee assessment frameworks such as KillerBee.

- **Status**
  - Final report of findings issued to utilities and AMI vendor June 2012
- **Performers:** Sandia National Laboratories
- **Partners:** Two electrical distribution utilities, and an AMI system vendor