Supply Chain Integration For Integrity

Policy and architecture for built-in supply chain integrity of trusted components for Electric Delivery Systems (EDS)

Frederick T. Sheldon, Ph.D.
Kaylee Justice and
Elijah Fetzer
David Manz, Ph.D.

Summer 2013
Current Needs of EDS

Supply Chain Integration For Integrity


• Plan provides a supporting framework of goals and milestones for protecting control systems for the foreseeable future (10 years)
  
  – By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
  
  – Sector needs a reference architecture that demonstrates how to ensure supply chain integrity
The Future: Smart Grid

Supply Chain Integration For Integrity

1. Renewable Energy
2. Synchrophasors, Volt regulation, DC transmission lines
3. Photovoltaics, Microturbines & Fuel cells
4. Hybrid base-load plants that combine energy sources
5. Grid automation, Machine-to-machine communication
6. Demand response (DR) pricing, Distributed energy storage
7. Large-scale energy storage of intermittent resources, Dispatchable DR & efficient virtual power plants, Planning for efficiency
8. Smart meters, Advanced Metering Infrastructure, Neighborhood- and campus-scale microgrids
9. Increased end-use energy efficiency to reduce total electricity demand

Figure from: Bracken Hendricks and Adam Shepard James, “The Networked Energy Web The Convergence of Energy Efficiency, Smart Grid, and Distributed Power Generation as the Next Frontier of the ICT Revolution” The Center for American Progress, www.americanprogress.org, Aug. 2012
Introduction

Supply Chain Integration For Integrity

• SCI-FI Challenge:
  – New capabilities are vital to detecting the presence of undesired functionality in the supply-chain with the intent to compromise the integrity and availability of energy delivery system (EDS) components.

• Goals:
  – Establish the business case for vendors/asset owners and get their involvement early on,
  – Develop a strategy for commercializing/implementing solutions throughout the energy sector,
  – Develop continuous detection capability for use during operation at the energy asset end-user installation,
  – Demonstrate at end-user site to validate clear industry acceptance.
Introduction (cont.)

Supply Chain Integration For Integrity

• Fundamental requirement:
  - Innovative solutions should be interoperable, scalable, cost-effective advanced technologies that implement common methods and best practices

• A multi-laboratory collaboration involving vendors and asset owners:
  - Demonstrate how the identified research comprehensively addresses the Supply Chain Challenge
  - Prototypes an existing technology gap
  - The approach is divided into three prongs as follows,…
SCI-FI Approach

Supply Chain Integration For Integrity

Interdisciplinary Approach

Divided into three prongs:

1. Hardware reverse-engineering to assure no unintended functionality.

2. Analyze software and firmware to assure no unintended functionality (Malware-Free)

3. Evaluate policy and architecture
SCI-FI Approach
Supply Chain Integration For Integrity

Need
Methods to ensure the integrity and providence of critical un-vetted power grid components. There is a lack of a highly trusted chain-of-custody.

Approach
Create an integrated system which enables us to evaluate/ensure the integrity of the hardware and software that comprise power grid components.

Benefit
High confidence that no hidden functionality exists in the hardware, firmware, or software. Post-deployment confidence that EDS will remain resilient and secure against cyber attack.

LLNL
Developing analysis capabilities for embedded field device firmware & energy management system application SW.

PNNL Project Lead
Developing tools and techniques to reverse engineer, identify and attribute components of the IC state machines to ensure accuracy and integrity of the hardware.

ORNL
Developing policy and architecture needed to implement tools and techniques created by PNNL and LLNL.

Funded by DOE/DEDS 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
Benefit

✓ High confidence that no hidden functionality exists in the hardware, firmware, or software.

✓ Post-deployment confidence that EDS will remain resilient and secure against cyber attack.
SCI-FI Approach

Supply Chain Integration For Integrity

Developing policy and architecture needed to implement tools and techniques created by PNNL and LLNL.
**ORNL Policy Approach**

**Supply Chain Integration For Integrity**

- Static and Dynamic supply chain protection strategy supported by a *Trusted Computing Base (TCB)* approach
  - **Static**: discovering a compromise of EDS digital assets after manufacturing but *before commissioning*
  - **Dynamic**: sensing compromise of EDS digital assets *post deployment*

- The TCB supports the *security policies* as the basis for implementing a *Transitive Root of Trust (TRoT)* in complex systems
Security Policy & Enforcement

Supply Chain Integration For Integrity

• Two approaches to achieving security policy enforcement:
  
  – *Typically, various security measures are applied to a system that is discovered to be insufficient post-deployment*
  
  – *An improved posture would be to articulate the security policy and then construct a system sufficient to enforce it to some level of confidence*

• Types of policies:
  
  – *Least Privilege*
  
  – *Role-based Access Control*
  
  – *Integrity*
  
  – *Availability*
  
  – *Separation*
  
  – *Confidentiality*
1. Least Privilege Policy

- No entity within a system should be accorded privileges greater than those required to carry out its tasks

- Users are assigned *roles* (collections of various job functions)

- A user’s role can change as his/her responsibilities evolve

- Mitigated failure scenarios:
  - Authorized employee issues an invalid mass remote disconnect
  - Authorized employee manipulates Meter Data Management System data to over-/under-charge customer
Policy Analysis, Specification and Mitigation

Supply Chain Integration For Integrity

2. Integrity Policy

- Protects the reliability or criticality of information
- Prevents messages from being modified or inserted
- Mitigated failure scenarios:
  - Compromises/leaks customers’ protected PII (packet insertion attack)
  - False meter alarms overwhelm AMI & masking real alarms (replay attack)

3. Availability Policy

- Ensuring that each component of a system has its required dependencies
- Protects system efficiency
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

4. Separation Policy
   - **Isolates processes from one another**
   - **Protects the integrity of separate processes**
   - **Mitigated failure scenarios:**
     - Breaching of a cellular provider's network exposing AMI access
     - A breach in one network affects the integrity of another network

5. Confidentiality Policy
   - **Protects information from unauthorized disclosure**
   - **Applies to requirements for secrecy and privacy**
   - **Mitigated failure scenarios:**
     - Leaked employees/customers Personally Identifiable Information (PII)
Policy Enforcement with TCB

Supply Chain Integration For Integrity

• Trusted Computing Base (TCB): *The portion of the system that is relied on to enforce the security policy of the platform.*

• Cyber-Physical Device (CPD) TCB requirements:
  – Must be properly established
  – Must enforce policy
  – Must isolate sensitive code from ALL other software
  – Must be minimal in size (small security perimeter)
  – Must verify and attest to system integrity with NO downtime
  – Must provide meaningful attestation of executed code
  – Must be carefully designed and implemented
A Reference Architecture Using TCB/TRoT

Supply Chain Integration For Integrity

• Need:
  - **Implement & Enforce Policy Specifications**

• Solution:
  - **Transitive trust chain**
  - **Chain begins with a hardware Root of Trust (RoT)**
  - **Verifies Trust in all necessary software components**
    • This process measures each component before it is executed
Establishing the TCB

Supply Chain Integration For Integrity

• How can we ensure that our Trusted Computing Base is Trustworthy?

• Let’s start with a hardware-based Root of Trust

• Transfer trust from *known* Trusted hardware (PNNL) ONLY to Trusted software/firmware (LLNL)

• Hmm… Transferring trust? How does that work?

Well, I’m glad you asked!
Transitive Root of Trust (TRoT)

Supply Chain Integration For Integrity

Scenario 1:

People: Alice and Bob

1. Alice is known to be **Trusted**

2. Bob is unknown and therefore **NOT Trusted**

3. Alice verifies that Bob is **Trusted**

4. Bob is now **Trusted**

Alice transferred **Trust** to Bob
Transitive Root of Trust (TRoT)

Supply Chain Integration For Integrity

Scenario 2:

People: Alice and Bob; Casey and Daniel

1. Alice → Bob = Trusted
2. Daniel → Casey = Trusted
3. Casey tells Bob “EDS whitelist is genuine.”

Bob can now trust that “EDS whitelist is genuine.”
Leveraging Existing Trusted Computing Components
Supplementary Chain Integration For Integrity

• Assumptions:
  – Most CPUs and OSs support some form of trusted computing architecture (DoD-driven market)
  – Leverage existing trusted computing components on the market to provide reliable post-deployment security and system integrity for CPDs in EDS

• Trusted computing premise:
  – HW-based Root of Trust (RoT) / Trust Anchor (TA)
  – Such components are assumed to always behave in the expected manner (immutable) *-* / *+*
Trusted Platform Module (TPM)

Supply Chain Integration For Integrity

• The Trusted Platform Module (TPM) is a Trust Anchor (TA) designed and standardized by the Trusted Computing Group and currently in wide production.

• Trusted capabilities
  – Protected registers
  – Core Root of Trust Measurement (CRTM)
  – etc.

• Forms the Trust Anchor of the Transitive Root of Trust (TRoT) chain.
Flicker: A Secure Execution Architecture

Supply Chain Integration For Integrity

• Uses the TPM and common secure virtualization hardware support with a secure execution architecture to form a secure TCB

• Flicker allows security-sensitive code to execute in complete isolation from all other software
  
  – Holds functional integrity even if BIOS, OS, etc. are all malicious
  
  – Enables meaningful software attestation and facilitates formal security analysis of the software remaining in the TCB
  
  – Minimizes TCB,... contains fewer than 250 lines of code
  
  – Secure virtualization hardware: AMD’s Secure Virtual Machine (SVM) architecture or Intel’s Trusted Execution Technology (TXT)
Digital Management, Inc. (DMI)

Supply Chain Integration For Integrity

- DMI will work with ORNL to support two key task areas in the SCI-FI project
  - Built-in Supply Chain Integrity Trust model (TM) for verifying the integrity of the components/subsystems in the electric power industry supply chain

- Supply Chain Architecture and Policy Analysis
  - Define a reference architecture (with industry support) for trust anchor (TA) interactions across the supply chain and develop a schema and best practices for verifying the integrity of supply-chain components
  - Support for assembling an Industry Advisory Board
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

**ORNL + DMI Phase I Tasking**

**Supply Chain Integration For Integrity**

- **Main tasks for ORNL/DMI (2.1.1 or 2.1.2):**
  - Completion of a specification (report) on policies that are enforceable via Transitive Root of Trust (i.e., TCB Energy Delivery Systems)
  - In other words, must show that (in principle) the TRoT is scalable to a multi-nodal system and that TCB policies are enforceable.
  - **Note:** identify the main policies that are EDS practical, relevant and scalable
  - **This must be achieved by the end of CY13 (Dec 2013).**
  - **Note:** master schedule from PNNL does not have this milestone showing
ORNL + DMI Phase II Tasking

Supply Chain Integration For Integrity

• Prototype of TRoT for a Cyber-Physical Device and within a Trusted Network of N Devices such that:
  – TRoT is scalable to a multi-nodal system and that TCB policies are enforceable
  – Must identify canonical test case(s) that demonstrate how to verify that disparate trusted anchor implementations are measurably trustworthy.

• Due November 2014.
Conclusions

**Supply Chain Integration For Integrity**

- **AIM**: Policy and architecture for built-in supply chain integrity of trusted components for EDS

  - Develop an EDS-specific Trust Anchor architecture embodied by a set of policies leveraging the Trust Model, Trust Anchor, and TRoT concepts that can be applied to the electric power industry supply chain

  - Demonstrate how a Trust Model represents appropriate EDS network architectures as a basis for establishing EDS supply chain integrity best practices

  - Identify/capture EDS-specific best practices for ensuring supply chain security, integrity and interoperability
Consequently,...

Supply Chain Integration For Integrity

• Empower asset owners to demand enhanced technology capabilities to ensure SCI-FI

• Establish a chain of trust and integrity of purchased products

— Cradle-to-grave (technology based) chain of custody that augments SCRM in such a way that allows the conveying of relevant integrity information from one end of the supply chain (manufacturing) to the other (consumer)!
SCI-FI Benefits and Takeaways

Supply Chain Integration For Integrity

• Reference architecture for trusted computing and policy specification

• Demonstrate that Transitive Root of Trust is scalable to a multi-nodal system, and that appropriate TCB policies are enforceable

• A trust schema is being planned that may be used in an appropriate interoperable Energy Delivery System (EDS) network architecture as a basis for establishing EDS supply chain integrity best practices

• The tools and technologies developed will be made available for asset owners and vendors (one caveat)
Milestones

Supply Chain Integration For Integrity

• Create integrity schemas

• Instantiate an EDS specific platform trust services (PTS) specification

• Specify a PTS communications scheme via TNC

• Specify integrity information submission and publication interfaces
Deliverables

Supply Chain Integration For Integrity

• Develop policy/architecture spec for EDS specific TRoT

• Develop a trust schema appropriate for EDS network architecture
  – Requirements spec to enable TRoT for a CPD
  – Requirements spec to enable a trusted network for TRoT for “n” CPDs
Deliverables

Supply Chain Integration For Integrity

• Identify EDS specific best practices for ensuring supply chain security, integrity and interoperability

  — Demonstrate/simulate a prototype trusted networked TRoT with actual CPDs

  — Work with PG&E and TVA to understand the specifications for a value-added tool for PG&E and other utilities
Inside our work space in the DECC lab (above). Protective Relays SEL-451 Relays (right).
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
Supply Chain Risk Management Challenges

Supply Chain Integration For Integrity

- Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world not always with the knowledge of the acquirer.

- Abundant opportunities exist for malicious actors to tamper with and sabotage products ultimately compromising system integrity, reliability, and safety.

- Organizations acquiring hardware, software, and services are not able to fully understand and appropriately manage the security risks associated with the use of these products and services.
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Supply Chain Risk Management Challenges

Supply Chain Integration For Integrity

- Challenges range from insufficient acquirer practices to lack of transparency into the supply chain
  - A substantial number of organizations or people can “touch” an ICT product without being identified
  - Standardized methodology and lexicon for managing ICT supply chain risks is just emerging
  - Inconsistent ICT products and services acquisition practices contribute to acquirers’ lack of understanding what is happening in their supply chain
  - Counterfeit hardware and software proliferate
  - Acquirers do not have a framework to help enforce security and assurance compliance for vendors
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
Resistance is futile

Supply Chain Integration For Integrity

- The ICT supply chain is unavoidably global
- Pedigree and provenance are often untraceable, even by suppliers themselves
- Basing risk assessment on national origins is impractical and not appropriate

National Origins of Components Used in Leading Personal Computer

<table>
<thead>
<tr>
<th></th>
<th>Dell</th>
<th>HP</th>
<th>Lenovo</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System design</strong></td>
<td>China, India, Singapore, Taiwan, US</td>
<td>India, US</td>
<td>China, Japan, Taiwan, US</td>
</tr>
<tr>
<td><strong>Motherboard</strong></td>
<td>China</td>
<td>China</td>
<td>China</td>
</tr>
<tr>
<td><strong>assembly</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Brazil, China, Ireland, Malaysia, US</td>
<td>Australia, Canada, China, Czech Republic, India, US</td>
<td>Brazil, China, Czech Republic, Hungary, India, Japan, Mexico</td>
</tr>
<tr>
<td><strong>assembly</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BIOS design</strong></td>
<td>China, India, US</td>
<td>China, India, US</td>
<td>China, Japan, US</td>
</tr>
</tbody>
</table>
What does this have to do with Smart Grid?

Supply Chain Integration For Integrity

- Smart Grid consists of ICT products
- These products are purchased by acquirers from suppliers
- These suppliers have supply chains of their own

How many acquirers have asked their Smart Grid vendors questions about security and other practices exercised by the vendors’ upstream suppliers?
# ICT SCRM vs. Traditional Supply Chain Risk Management

## Supply Chain Integration For Integrity

<table>
<thead>
<tr>
<th>Traditional Supply Chain Risk Management</th>
<th>ICT Supply Chain Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will my physical product get to me on time?</td>
<td>Will my product (physical or logical) get to me as it was shipped and as I ordered?</td>
</tr>
<tr>
<td>Is my supply chain resilient and will it continue delivering what I need in case of disaster?</td>
<td>Is my supply chain infiltrated by someone who is inserting extra features into my hardware and software to exploit my systems and get to my information now or later?</td>
</tr>
<tr>
<td>What is the risk <strong>TO</strong> my supply chain that delivers critical products and services that I need to mitigate?</td>
<td>What is the risk <strong>FROM</strong> my supply chain to my business and mission that I need to mitigate?</td>
</tr>
</tbody>
</table>

ICT SCRM = Information Communication Technology Supply Chain Risk Management
What are the risks?

Supply Chain Integration For Integrity

• Intentional insertion of malicious functionality

• Counterfeit electronics

• Poor practices upstream
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.