Hardware Rooted Trust for Industrial Control Systems

Dr. John Ross Wallrabenstein

Sypris Research

©Sypris Electronics, LLC 2016, All Rights Reserved
Focus of Talk

Common Cybersecurity Vulnerabilities in ICS [DHS 2011]

1. **Input Validation**

2. **Access Controls, Credential Management, Security Configuration**
   - Credential Protection
   - Firewall Rules
   - Network Configuration

3. **Authentication**
   - Password Strength
   - Identity Spoofing
Focus of Talk

Common Cybersecurity Vulnerabilities in ICS [DHS 2011]

1. **Input Validation**
2. **Access Controls, Credential Management, Security Configuration**
   - Credential Protection
   - Firewall Rules
   - Network Configuration
3. **Authentication**
   - Password Strength
   - Identity Spoofing
<table>
<thead>
<tr>
<th>Vendor Mitigations:</th>
<th>Asset Owners Mitigations:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Educate/train developers in secure coding</td>
<td>• Redesign network layouts to take full advantage of firewalls, VPNs, etc.</td>
</tr>
<tr>
<td>- Lack of input validation, authentication, and integrity checks</td>
<td>• Implement a layered network topology (critical communications in secure and reliable layer)</td>
</tr>
<tr>
<td>• Expeditiously test and provide security patches to affected customers</td>
<td>• Restrict physical access to the ICS network and devices</td>
</tr>
<tr>
<td>• <strong>Implement and test strong authentication and encryption mechanisms</strong></td>
<td>• Deploy timely security patches after testing</td>
</tr>
<tr>
<td>• Increase the robustness of network parsing code</td>
<td>• Customize IDSs for the ICS hosts and networks</td>
</tr>
<tr>
<td>• Develop network traffic firewall and IDS rule sets</td>
<td>• Restrict ICS user privileges (i.e., establishing role-based access control)</td>
</tr>
<tr>
<td>- Create custom protocol parsers for common IDS</td>
<td>• Develop a password management plan (strong passwords)</td>
</tr>
<tr>
<td>• Conduct third party security source code audits</td>
<td>• Change all default passwords</td>
</tr>
<tr>
<td>• Redesign network protocols with security</td>
<td></td>
</tr>
<tr>
<td>• Develop advanced cyber test suites for security issue in product lines</td>
<td></td>
</tr>
<tr>
<td>• <strong>Develop encryption and/or cryptographic hashes to ICS data storage and communications</strong></td>
<td></td>
</tr>
</tbody>
</table>
Division of System

User Control Stations
1. Issues Commands to System
2. Required to Authenticate User
3. Enforces Access Control Policies

Nodes & Programmable Logic Controllers
1. Unmonitored
2. Physically Unsecured
3. Resource-Constrained
Controller
Control
Server
Satellite
Phone Line
Radio

Non-IP Network
Programmable Logic Controllers
Critical Assets

Security by Obscurity
Tampering
Geographic Isolation
Unverified Data Origin
Multiple Vendors
Limited Bandwidth
Proprietary Protocols

Electrical
Nuclear
Water

Shared Keys
External Access
Man in the Middle

User Authentication

© Sypris Electronics, LLC 2016, All Rights Reserved
Goals for ICS Nodes

- **Hardware Root-of-Trust**
  - Extract identity from unique physical characteristics of silicon

- **Tamper Sensitivity**
  - Hardware tampering modifies physical characteristics
  - Modified physical characteristics changes extracted identity

- **Reduce/Eliminate Private Key Exposure**
  - Never *(generate, reconstruct, or) store* private key
Identity: Traditional Cryptographic Systems

- Symmetric Private Key **Stored** on Drive
Identity: Traditional Cryptographic Systems

- Asymmetric Private Key **Stored** on Drive
Identity: Traditional Approach Limitations

- Identity is Stored
Secure Hardware Solutions

- Secure Hardware
  - Rugged Enclosure
  - Tamper Resistance
  - Epoxy Coating
  - Battery Hold-Up

- Limitations
  - Size & Weight
  - $$$

© Sypris Electronics, LLC 2016, All Rights Reserved
Core Concept: Ideal Hardware Identity Source based on Complex Physical Interaction
Ideal Hardware Identity Properties

Definition

Ideal Properties of Hardware Identity Sources

- **Entropy**: The output is computationally indistinguishable from a random string

- **Clonability**
  - **Physical**: Impossible to create a physical clone
  - **Mathematical**: Impossible to create a mathematical model

- **Variance**
  - **Inter-Device**: Two devices queried on the same challenge have responses with $\approx 50\%$ differing bits
  - **Intra-Device**: The extracted hardware identity should be $t$-close to a fixed value $r$ when queried on the same challenge

- **Tamper Sensitivity**: Short-term fluctuations induce at most $t$ errors, while malicious tampering induces greater than $t$ errors
Physical Unclonable Functions

*Physical unclonable functions* (PUFs) can be used to extract hardware identity:

- Physical properties of the PUF prevent manufacturer from generating two identical PUFs
- A PUF is input a challenge, and outputs a response
- Two different PUFs will return different responses for the same challenge
- Example PUF constructions include Arbiter, Ring Oscillator, and SRAM
PUF-Based Identity Management

Identity is **Dynamically Regenerated** As Needed
Core Concept: Identically manufactured devices have different hardware identities
Core Concept: Hardware tampering fundamentally changes hardware identity
Private Key Exposure Reduction/Elimination

Keyed System: A cryptographic system where the private key must be continuously protected
Near-Keyless System: A cryptographic system where the private key exists for a brief time $\epsilon$
Keyless System: A cryptographic system where the private key never exists
# Standard PKI vs. Hardware Rooted Identity

<table>
<thead>
<tr>
<th>Feature</th>
<th>PKI</th>
<th>Hardware Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Private Information Storage</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Intrinsic Hardware Identity</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Intrinsic Tamper Protection</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Robust to Hardware Failure</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scalable Processing</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Plug-and-Play (FIDO/PKCS#11)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>384-bit Elliptic Curve Cryptography</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Discussion

Questions

Trusted Solutions... From Thought to Finish

Providing Trusted Solutions that Secure our Customers’ Interests Globally