OPTIMIZATION OF INDUSTRIAL CYBERSECURITY
Update on ODVA’s Technical Approach

David Doggett, Schneider Electric
Cliff Whitehead, Rockwell Automation

October 15, 2015
Increasing need for security is common knowledge. Are we delivering?

- Oct 2012 Presentation to the members and whitepaper.
  - Harden Devices
  - Protect CIP
  - Secure CIP

- Cybersecurity a subgroup of the Systems and Architecture SIG.
  - New Volume 8 of the CIP Networks Library addresses security.
ODVA’s Role in Security

• Environment:
  – Cybersecurity weaknesses will always exist.
  – The future is a convergence of production and other systems.
  – Secure Protocols form a key element of a Defense in Depth strategy.

• Assumptions:
  – The networks should be considered to have very limited trust.
  – All entities on the network should be considered untrusted until they can be authenticated.
  – Access to a device should not be allowed until authorized by the device itself.
  – Physical access to a device will be limited to only trusted individuals.

• A secure device should:
  • Reject data that has been altered in any way (data integrity)
  • Reject messages sent by unknown/untrusted people or devices (authenticity).
  • Reject messages that request actions that are not allowed (authorization)
ODVA’s Role in Security

- ODVAs Role:
  - Secure protocol on which secure devices and systems can be built.
  - Recommendations for implementation of a secure system.
Elements of CIP Security

- **Secure CIP**
- **Protect CIP**
- **Harden Devices**

### 2014-2017 Timeline

- **2014**
  - Protected Mode

- **2015**
  - Device Authentication
  - Message Integrity
  - Message Confidentiality

- **2016**
  - User Authentication
  - Authorization (CIP object)

- **2017**
  - Device Robustness
  - Default Services and Settings
Harden Devices

- Protection Mode
  - Attribute of the Identity Object.
  - Rejects disruptive CIP services when attribute is set.

- Network Robustness
  - Further analysis being done of how ODVA will interact with existing standards/certifications.

- Recommended/Required Security Settings
  - More work to be done to ensure a secure by default installation.
## Protect and Secure CIP ™ Based on Threats, using Proven Technologies

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Threat Description</th>
<th>Security Property</th>
<th>Volume 8: CIP Security™</th>
<th>Future enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spooﬁng identity</td>
<td>E.g. illegally accessing and then using another user’s or devices authentication information, such as username and password.</td>
<td>Device authorization</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User authorization</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Tampering with data</td>
<td>The malicious modiﬁcation of data, including unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it ﬂows between two computers over an open network, such as the Internet.</td>
<td>Message integrity (Ethernet)</td>
<td>x (CIP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data integrity (at rest)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Repudiation</td>
<td>Threats associated with users or devices who deny performing an action without other parties having any way to prove otherwise. Nonrepudiation refers to the ability of a system to counter repudiation threats. E.g., a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.</td>
<td>Non-repudiation (audit of events)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Exposure of information to individuals who are not supposed to have access to it. E.g., the ability of users to read a ﬁle that they were not granted access to, or the ability of an intruder to read data in transit between two computers.</td>
<td>Message conﬁdentiality</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Denial of service</td>
<td>Denying service to valid users, e.g., for example, by making a Web server temporarily unavailable or unusable. Certain types of DoS threats must be protected against to improve system availability and reliability.</td>
<td>Message integrity</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Elevation of privilege</td>
<td>An unprivileged user gaining privileged, and thereby sufﬁcient, access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.</td>
<td>Authorization</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Device Authorization
- Preshared Keys.
- Device Certificates.
- TLS/DTLS with Mutual Authentication.

Message Integrity/Confidentiality
- TLS/DTLS (with encryption).
- Null Cipher for speed / HMAC

Performance, will vary but initial test is
- 400ms connection times (from 100ms)
- Minimal impact on data exchange (Null Cipher).
Device Authentication

- Group of trusted devices (IEC62443 security zone) based on sharing common keys or Certificates signed by a trusted end user CA.

- Pre shared key
  - Simple implementation for users of smaller systems.

- Certificate Based
  - Proven cryptographic identity per device (X509 Cert)
  - More robust and secure for large systems.
  - Certificate Handling covered as part of specification.
    - Default certificate (vendor installed or device self signed) available on startup.
    - Local PKI support for installing end user certificates to ensure uniqueness of devices at a end user site.
      - Push mode for end user device certificates defined in 2015 specification.
      - Pull mode (EST/SCEP) to be defined later but can be implemented now.
- UCMM and Class 3 - EtherNet/IP over TLS (Port 2221/tcp)
- Class 0/1 – EtherNet/IP over DTLS (Port 2221/udp)
  - Forward_Open and Forward_Close moved to DTLS/UDP.
- Identity and Integrity of communications in all use cases.
  - Confidentiality of communications optional.
- Authorization based on possession of preshared key or trusted certificate.
  - CIP object security to be covered in 2017+
### Elements of CIP Security

#### Secure CIP
- Device Authentication (x509 Cert)
- Message Integrity (TLS/DTLS)
- Message Confidentiality (TLS/DTLS)
- Certificate Handling (EST/SCEP, CSP/OCSP)

#### Protect CIP
- User Authentication Authorization (CIP object)

#### Harden Devices
- Protected Mode
- Device Robustness
- Default Services and Settings

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2015 ODVA, Inc. All rights reserved.
THANK YOU