CIP Security and IEC-62443-4-2

Jack Visoky
Rockwell Automation

Joakim Wiberg
HMS Networks

March 4, 2020
Introduction

- CIP Security is the ODVA standard for securing CIP and EtherNet/IP
- How does CIP Security fit in with IEC 62443?
  - First, some background on IEC 62443
  - Then some background on CIP Security Profiles
  - Discussion on how CIP Security meets some 62443 requirements
• International standard that is gaining a lot of traction within the industry
• Focus is on security of industrial automation systems
• Many parts, covers a wide variety of areas
• Focus for us is on component requirements
• For a component, IEC 62443-4-1 defines how a product is developed
  – Important, but out of the scope of the paper
• IEC 62443-4-2 defines functional requirements for a component
  – Here a component could be a device, software, product, etc…
• IEC 62443 contains levels of security, one through four
  – SL 1 – Focused on actors who unintentionally cause security events
  – SL 2 – Focused on attackers with basic skills and resources
  – SL 3 – Focused on advanced attackers with moderate resources
  – SL 4 – Focused on the highest level of attackers with significant skills and resources
• IEC 62443 defines *what you have to do, not how you have to do it*
IEC 62443-4-2 – Component Requirements

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability
CIP Security as an answer for IEC 62443

• CIP Security can be used to meet a number of the IEC 62443 requirements
• What is meant by CIP Security? Well, we have to make some assumptions
  – Assume a simple device, one Ethernet port, implements CIP Security EtherNet/IP Confidentiality Profile and CIP Security User Authentication Profile
  – Let’s draw the trust boundary like shown
    • Data coming in-going out the Ethernet port is crossing a trust boundary
  – Small changes in product structure can have a big effect on the security case, take note that careful, individual analysis is needed
CIP Security: EtherNet/IP Confidentiality Profile

- Built on IETF standard technologies, ubiquitous in communication sec
  – Secure communications via TLS (messaging) and DTLS (I/O)
  – Certificate management via CIP and EST

- Security Properties:
  – Authentication of the endpoints – ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.
  – Message integrity and authentication – ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS message authentication code (HMAC).
  – Message encryption – optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS handshake.
CIP Security User Authentication Profile

• Again, built on standard technologies
  – OAuth 2.0, JWTs, and OpenID Connect
• Authentication and Authorization of humans, devices, and software processes
• Central identity management for integration with IT system, local identity management for simple OT systems
• Supports multifactor authentication and various workflows via OpenID Connect
• With these two profiles, many items are covered
  – Nearly 50% of the total requirements are either fully met or partially met
  – Many items out of scope cannot be covered by a communications protocol
Wait, so CIP Security is less than 50% Coverage?

• Although we are showing requirements coverage, not all requirements are “equal work items”
  – A given requirement might be very complex or fairly straightforward
  – Many requirements are in disparate areas (e.g. internal structure of the hardware versus integration with software tools)

• It would not be realistic to expect a communication protocol to cover all 62443 requirements
  – Despite this, CIP Security provides significant coverage
  – CIP Security provides a strong solution for relevant requirements
Some Examples

- Given the number of requirements, we can’t go through all of them in the allotted time
- However, we have chosen a few that we felt were illustrative and/or interesting for the audience
- You can always read our paper if you want to know about a specific requirement or all the requirements 😊
CR 1.1 – Human user identification and authentication

- Requirement deals with identification of humans using industrial equipment
- Met via CIP Security User Authentication Profile
  - Authentication for humans and non-humans via tokens (JWT)
- Two Requirement Enhancements:
  - Unique identification and authentication
    - With User Authentication Profile, each user has a unique identity via the ‘sub’ claim of the JWT
  - Multifactor authentication on all interfaces
    - Integrating with an OpenID Connect system provides for multifactor authentication
CR 1.3 – Account management

- Accounts can be managed centrally or locally with CIP Security User Authentication Profile
  - Locally involves just the device managing the accounts
  - Centrally involves integrating into a 3rd party identity management system
CR 1.8 – Public Key Infrastructure and Certificates

- Certificates can be managed over CIP, or via EST
- EST allows native integration with IT certificate management
- Certificates are standard X.509, used for TLS and DTLS, furthering the IT/OT integration
- CIP Security fully integrates into a PKI for certificate management
CR 2.1 – Authorization enforcement

• CIP Security User Authentication Profile implements access policy via standard roles
  – These can be extended with general “claims” within the JWT
  – Standard roles can also be extended if necessary
  – Groups for policy enforcement also supported (via ‘aud’ claim)

• Two Requirement Enhancements
  – Authorization enforcement for all users
    • Once User Authentication is set up it is enforced for all users
  – Permission mapping to role
    • Specification gives mandatory permissions and suggested permissions for roles
      – Spec would not be able to mandate access to all attributes and services for all products, given the wide range of CIP products
CR 3.1 – Communication integrity

• TLS and DTLS cipher suites use Message Authentication Code via SHA-2 HMACs for protection of the data

• One requirement enhancement
  – Communication authentication
    • Same reasoning, HMACs from TLS and DTLS protect the authenticity of the data

• SHA-2 suite is widely recognized as a best-in-class algorithm for data protection
CR 3.12 – Provisioning product supplier roots of trust

• CIP Security provides the option of including a “Vendor Certificate”, that is, a unique cryptographic identity signed by the vendor with the associated root of trust for the signing CA
  – This is an 802.1AR IDevID

• This partially meets the CR 3.12 requirement
  – It is up to the vendor to store this securely within the product, ODVA does not “conformance test” hardware secure key storage
  – It is up to the vendor to use the Vendor Certificate and root of trust for enabling security functions beyond just CIP Security (e.g. secure updates)
CR 4.1 – Information confidentiality

• Confidentiality of information in transit over EtherNet/IP is covered by CIP Security EtherNet/IP Confidentiality Profile
  – TLS and DTLS provide the option to encrypt the data
  – Mandatory to support cipher suites for CIP Security use AES CBC for data protection

• However, CIP Security only covers the data while in transit
  – While at rest the data may also need to have confidentiality applied, this aspect is outside the scope of CIP Security
CR 4.3 – Use of cryptography

- CIP Security is built on open, well-used, and well-vetted standards like TLS, DTLS, EST, OAuth 2.0, OpenID Connect.
- Cryptography from these technologies includes algorithms recognized by international standards bodies and best-in-class:
  - AES
  - SHA
  - ECC
  - RSA
Out of Scope

• What are some of the things that are out of scope?
  – Logging is a big item; there are a number of requirements around logging
  – EtherNet/IP System Architecture SIG has discussed possible standardization of Syslog
    • This would be in line with the strategy to use well-known, well-vetted technologies
    • With the addition of Syslog support several other requirements would also be covered
    • SIG will be investigating this in the coming year

• Internal product structure
  – E.g. Secure Boot, Secure Storage, Physical Interface Management, etc.)
  – These items are not possible for a communications standard to cover

• DoS protections
  – This deals with internal product structure and communications layers below CIP and EtherNet/IP (e.g. IP Storm)
Summary of mappings

- CIP Security uses best in class security technology to meet a number of IEC 62443 requirements
- Our hope is that this paper is an aid to ODVA members wanting to certify to IEC 62443 products/systems that implement CIP Security

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Met by CIP Security</td>
<td>29</td>
</tr>
<tr>
<td>Partially Met by CIP</td>
<td>3</td>
</tr>
<tr>
<td>Out of scope for CIP Security</td>
<td>42</td>
</tr>
</tbody>
</table>
Questions?

- Are there any questions or further discussion?
- You can contact us later if questions arise, through the SIG forum or other means
  - If you are a vendor interested in security, consider joining the EtherNet/IP System Architecture SIG and the CIP Security Working Group

THANK YOU!!!