Securing Control System Network with CIP Security

June 23rd, 2020
Introductions

Brandon Singh
Presenter
Network Specialist
The Reynolds Company
– Dallas / Fort Worth

Mike Masterson
Panelist
Automation / Network Specialist
The Reynolds Company
– Houston

Joe Belaschky
Panelist
Automation / Network Specialist
The Reynolds Company
– Houston

Mark McGinnis
Panelist
Automation Specialist
The Reynolds Company
– Dallas / Fort Worth
2020 Online Events - Register to receive a calendar invite

User Group

Thursday, July 16th
My Rockwell Automation & Software Portal
10:00 am

Tech Talks

Wednesday, June 24th
931 Intrinsic Safety Barriers
10:00 am

Wednesday, July 1st
Automatic Device Configuration with PowerFlex Drives
10:00 am

Podcast

Friday, June 26th
Network Series Part 4 – The IT Episode

https://www.reynoldsonline.com/eventsUnit.action
CIP Security™ Protocol
Defense in Depth Security
Agenda

1. Why do we care?
2. What are we doing?
3. How are we doing it?
4. Phase approach
5. Questions
Why do we care?

- Historically, Industrial Control Systems (ICS) network protocols lack the security properties necessary to allow a device to “defend itself” against a network/communications attack
  - Lack of authenticity (security), integrity, and confidentiality
  - Ethernet/IP™ network protocol, PROFINET, Modbus, etc. all have the same issues
- Secure communications are required for certification to IEC62443, and are identified as a critical capability in most all other publications, standards and frameworks.
Attacker
What happens when someone gets into the network?

Direct Connect

Original Connection

Man-in-The Middle (MitM)

Monitoring Data
Secure communications

CIP Security™ protocol helps provide a secure transport for an EtherNet/IP™ network

- Enables an EtherNet/IP™ connected device to help protect itself from malicious communications
  - Reject messages sent by untrusted people or untrusted devices (authenticity)
  - Reject data that has been altered (integrity)
  - Helps prevent viewing of EtherNet/IP™ data by unauthorized parties (confidentiality)

- Reinforces defense in depth
  - Multiple layers of security are more resilient to attack
  - Each layer adds to the one above it
  - This does not replace the need for firewalls or other infrastructure.
<table>
<thead>
<tr>
<th>Security property</th>
<th>Volume 8: CIP Security™ Technical Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device identity</td>
<td>X.509v3 digital certificates used to provide cryptographically secure identifies to devices</td>
</tr>
<tr>
<td>Device authentication</td>
<td>TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) cryptographic protocols used to help provide secure transport of EtherNet/IP™ traffic</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authenticity to EtherNet/IP™ traffic</td>
</tr>
<tr>
<td>Data confidentiality</td>
<td>Data encryption as a means of encoding messages or information to help prevent reading or viewing of EtherNet/IP™ data by unauthorized parties</td>
</tr>
</tbody>
</table>
Leveraging proven technology
Identity, authentication, integrity and confidentiality
CIP Security™ protocol overview
Secure communications with EtherNet/IP™ network protocol

- **Identity, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data
- **Initial products, CIP™ securable products**

![Diagram showing secure communications with CIP Security™ protocol]
CIP Security™ protocol overview
Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data
CIP Security™ protocol overview
Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data

FactoryTalk® Linx

Hacker is able to send commands to the controller

MiTM

1756-EN4TR
Integrity
HMAC keyed-hash message authentication code

- An HMAC is attached to every message as a means to validate integrity and authenticity
- The message is first “hashed” to provide integrity
  - A mathematical function that maps a message of arbitrary size to a message of fixed size (like a checksum or CRC)
  - It is easy to compute the hash value for any given message
  - It is infeasible to generate a message from its hash (i.e., one way)
  - It is infeasible to modify a message without changing the hash
  - It is infeasible to find two different messages with the same hash
- A secret key is also added to the message before it is “hashed” to provide authenticity
  - You can’t validate the message unless you know the secret
- HMAC is fast and efficient with only a minor performance impact
CIP Security™ protocol overview
Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Help prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data

FactoryTalk® Linx

Now, hacker is not able to modify data, however, can still view it

1756-EN4TR
Data confidentially

- Encryption can be used as a means of encoding messages or information to help prevent reading or viewing of EtherNet/IP™ data by unauthorized parties (eavesdropping on the wire)
- The encryption method is negotiated as part of the TLS/DTLS “handshake” process
- It is optional
  - Not all ICS traffic contains “secrets” that need to be safeguarded (data integrity and authenticity is typically the goal)
  - The added encryption will impact data throughput performance
CIP Security™ protocol overview
Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data
So what exactly am I securing with CIP Security™ protocol?

- The EtherNet/IP™ port itself
- Dual IP ports can contain different security configurations
CIP Security™ protocol overview

Secure communications with EtherNet/IP™ network protocol

- **Authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data

Notable features:

- **System management**
  - Easily create and deploy security policies to many devices, all at once
- **Micro-segmentation**
  - Segment your automation application into smaller cell/zones.
- **Device-based firewall**
  - Enable/disable available ports/protocols of devices (ie./ HTTP/HTTPS)
- **Initial key products**
  - FactoryTalk® Linx software, ControlLogix® 5580 controllers, 1756-EN4TR ControlLogix® communication module, and Kinetix® 5700 and PowerFlex® 755T drives
- **Legacy Systems Support**
  - Trusted IP – authorize specific communications based on IP address
  - Retrofit 1756 based systems with the new 1756-EN4TR
Configuration

FactoryTalk® Policy Manager software
Modeling tool concepts
• Devices
• Zones
• Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.
Configuration

FactoryTalk® Policy Manager software
Modeling tool concepts
• Devices
• Zones
• Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.
Deployed model

FactoryTalk® Policy Manager software
Modeling tool concepts
- Devices
- Zones
- Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.

Legend
- Trusted Device
- Integrity
- Encrypted
- Trusted IP list
- Certificate

Zone 1
Deployed model

Once the model has been deployed, **FactoryTalk® Policy Manager** software and the **FactoryTalk® System Services** platform are no longer required. They are only required if additional changes need to be deployed.
Sample deployment

FactoryTalk® Policy Manager software
FactoryTalk® System Services platform

FactoryTalk® View software

Studio 5000® software
Sample deployment
Things to be aware of
Initial Constraints in 2019 (FT Services 6.11.00) Release

- Does not support CIP™ protocol bridging
  - Can't configure CIP Security™ protocol through a CIP™ bridge
- Does not support high availability
- Does not support Network Address Translation (NAT)
  - Unless the NAT is mapped to a public IP address
- Does not support Automatic Device Replacement (ADR)
- Supports only one NIC if multiple NICs are available in FactoryTalk® Linx software
Use case scenario (Phase I)

- Secure configuration to the controller: computers to controller
- Secure the inbound connection via 1756-EN4TR module or the ControlLogix® 5580 controller itself
Use case scenario (Phase II)

- Extend the model: Add devices to Trusted IP list as appropriate
- Remove devices from Trusted IP list as they become CIP™ securable
Release schedule

Available

- FactoryTalk® Policy Manager software (FactoryTalk® Services Platform version 6.11.00 or later)
- ControlLogix® 5580 controller (version 32 or later)
- 1756-EN4TR ControlLogix® communication module
- Kinetix® 5700 drive

Upcoming

- CIP Security™ proxy, target Q3 2020
- PowerFlex® 755T drive, target Q3 2020
References

- CIP Security with Rockwell Automation Products – Application Technique


- CIP Security within a Converged Plantwide Ethernet Architecture – White Paper

- FactoryTalk Policy Manager – Getting Results Guide
  https://literature.rockwellautomation.com/idc/groups/literature/documents/gr/ftalk-gr001_-en-e.pdf
Thank you for attending

TRC Tech Talks
Online Seminars