Improving Industrial Security and Robustness for Industrial Control Systems (ICS)

Veysel Saylam – Commercial Engineer
Håkan Kallenberg – Solution Architect
Agenda

What can we do to protect our systems?

Logix Security

FactoryTalk Security
Security
Building a Security-oriented Architecture

Authenticated Access
Data Confidentiality
IP Protection
Product & Network Hardening
Tamper Prevention & Detection
Partnering & Supply Chain

Data Protection and Confidentiality
Remote Access
Network
IP Protection
Supply Chain
Role-based Security
Anti-Tamper and Detection
Partners
Level 1 Process Control
Field Devices!
Agenda

What can we do to protect our systems?

Logix Security

FactoryTalk Security
Controller Security Tools

- Turn the Key Switch
- Match The Project
- Protect the Source
- Embedded Change Log
- FactoryTalk Security
- Data Access Control
Firmware Digital Signatures

Purpose of digital signature
- Protect firmware from accidental and malicious corruption
- Ensure firmware was generated by Rockwell Automation

How they’re being introduced...
- New products have their firmware digitally signed from day 1 (L7x, Micro 800…)
- Digitally signed versions of existing products released as feasible (EN2T, DNB…)

How they work...
- Rockwell Automation digitally signs firmware kits with a private key when they are released
- Devices locally check the signature with a corresponding public key
- Any change to the firmware kit will cause the signature check to fail in device
Controller Change Detection

- Every Logix Controller exposes a Change Detection Audit Value
- When something happens that can impact the behavior of the controller, the value changes
- Audit Value is available in Studio5000 Logix Designer, in other software applications like FactoryTalk Asset Centre and in other controllers via the Message instruction

The set of events that causes the Audit Value to change can be configured
Controller Change Detection

- The Audit Value is stored in every Controller Log entry
- FactoryTalk® AssetCentre is able to monitor the Audit Value and read in the Controller Log

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>remark</td>
<td>TSV-Controller-Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>remark</td>
<td>Date = Jun-02-2011 15:21:20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>remark</td>
<td>Controller = 1756-L71/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>remark</td>
<td>Serial-Number = 16#0067_D1CF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>remark</td>
<td>Revision = 20.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Record Number Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>Jun-02-2011 15:21:07</td>
<td>Project download</td>
<td>NA\clark [ Daniel W. Clark ]</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>Jun-02-2011 15:21:07</td>
<td>Change Log entry added</td>
<td>NA\clark [ Daniel W. Clark ]</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>Jun-02-2011 15:21:38</td>
<td>CCUID Configuration update</td>
<td>None</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>Jun-02-2011 15:21:38</td>
<td>Change Log entry added</td>
<td>None</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trusted Slot Designation

Controller Properties - Security/Hardening

Security Authority: FactoryTalk Security (\SERVER\rest_of_the...

Require Matching Security Authority ID for Authentication and Authorization

Restrict Communication Except Through Selected Slots

Select Slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Communication Restricted Through Controller Ports

RSLogix5000 Configuration and Programming of the Logix 5000 family of controllers
Source Protection & AOI

- Source Protection to lock down Routines and Add-On Instructions (AOI)
- Viewing can be permitted if desired
- Source Key values are obfuscated in Studio 5000
- Source Keys are named. The name is displayed in place of the Source Key value
Agenda

- What can we do to protect our systems?
- Logix Security
- FactoryTalk Security
Use FactoryTalk Security to...

Manage the insider threat by authenticating the user and authorizing the use of Rockwell Automation software applications to access automation devices.

How does it work?

Provides a centralized authority to verify identity of each user and grants or deny user's requests to perform a particular set of actions on resources within the system.

- User Roles (FT groups or Windows groups)
- User Accounts (FT users or Windows users)
- Computers and Computer Groups
- System Policies (plant wide)
- Product Policies
- Controllers to be secured
- Secure Controllers by Area (resource groups)
The FactoryTalk Directory can be configured to secure system access based on:

- Secure Controllers by Area (resource groups)
- Product Policies
- System Policies (plant wide security)
- Computers and Computer Groups
- Controllers (to be secured)
- User 's (Windows or FactoryTalk Users)
- User Roles (Windows or FactoryTalk Groups)
Thank you for participating!