T31 – Improving Industrial Security and Robustness for Industrial Control Systems (ICS)

Mike Bush, Technology Manager
Clark Case, Technology Manager
Agenda

How did we get here?

What can we do to protect our systems?

Logix Security

FactoryTalk Security

Keeping Appraised
How did we get here?

Stuxnet Introduces the First Known Rootkit for Industrial Control Systems

As we’ve explained in our recent W32.Stuxnet blog series, Stuxnet infects Windows systems in its search for industrial control systems, often generically (but incorrectly) known as SCADA systems. Industrial control
How did we get here?

Italian Researcher Publishes 34 ICS Vulnerabilities

Dale G Peterson

Luigi Auriemma, an Italian researcher from Milan, set a new record today publishing 34 ICS vulnerabilities all at once. In his words from bugtraq, the vulnerabilities

News

Researcher discloses zero-day flaws in SCADA systems

Flaws disclosed in products from Rockwell, five other vendors

By Jaikumar Vijayan

September 16, 2011 05:01 PM ET

Computerworld - An Italian security researcher this week disclosed details of several zero-day vulnerabilities he discovered in Supervisory Control and Data
How did we get here?

Hacker Apparently Triggers Illinois Water Pump Burnout

Attack illustrates the extent to which industrial control systems are Internet-connected, yet lack basic password checks or access controls.

By Mathew J. Schwartz InformationWeek
November 21, 2011 11:45 AM

Federal authorities are investigating a hack that resulted in the burnout of a water pump at the Curran-Gardner Township Public Water District in Illinois. Located west of Springfield, Ill., the utility serves about

Exclusive: Comedy of Errors Led to False ‘Water-Pump Hack’ Report

By Kim Zetter November 30, 2011 | 5:54 pm | Categories: Cybersecurity, Hacks and Cracks

Follow @KimZetter
How did we get here?

DHS Issued False ‘Water Pump Hack’ Report; Called It a ‘Success’

BY KIM ZETTER  10.02.12  10:00 PM

When an Illinois fusion center distributed a report last year stating that hackers from Russia had broken into a water district’s SCADA system and sabotaged a water pump, the Department of Homeland Security stepped in publicly to denounce the report as false, blaming the regional fusion center for spreading unsubstantiated claims and sowing panic in the industrial control system community.

But while DHS was busy pointing a finger at the fusion center, its own Office of Intelligence and Analysis had been irresponsibly spreading the same false information privately in a report to Congress and the intelligence community, according to a Senate subcommittee investigation released late Tuesday. The DHS report was issued five days after the fusion center report was issued.
How did we get here?

A Valentine's Day present for SCADA companies: new exploit tools

By Sean Gallagher | Published 4 days ago

There's good news for people who love bad news about the security of industrial control systems. At the
How did we get here?

**Back from the brink**
AMSC tries to rebound after disastrous software theft

**DEVENS** — Last year, the unthinkable happened to American Superconductor Corp. An employee sold its secrets to the Chinese.

The company's proprietary software ended up in the hands of its biggest customer, Sinovel Wind Group Co. American Superconductor, or AMSC, makes the controls that make wind turbines work; it had been
Agenda

How did we get here?

What can we do to protect our systems?

Logix Security

FactoryTalk Security

Keeping Appraised
What can we do to protect our systems?

- Implement a good network design
- Use tools offered by Rockwell Automation and our partners
- Keep apprised
Good Network Design

- Comprehensive Network Security Model for Defense-in-Depth
- Industrial Security Policy
- Implement DMZ
Network & Security Services at a Glance

**ASSESS**
- Assess the current state of the security program, design, policy
- Assess the current state of the network design, implementation

**DESIGN/PLAN**
- Design and plan a network infrastructure
- Design and plan security program, policy, infrastructure, business continuity plan

**IMPLEMENT**
- Installation and configuration of a network
- Implementation of a security program, infrastructure design, policy training

**AUDIT**
- Audit current architecture compared to governing body (ODVA, CNI, IEEE, TIA/EIA)
- Audit security program compared to governing body (NERC CIP, ISA SP-99, NIST 800-53, NIST 800-82)

**MANAGE/MONITOR**
- Manage, maintain and monitor uptime and issues on the network
- Managed Security Services (Incident response, disaster recovery, monitoring)
Products from Encompass Partners…
Agenda

How did we get here?

What can we do to protect our systems?

**Logix Security**

FactoryTalk Security

Keeping Appraised
Controller Security Tools

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

- Users can assign External Access settings of Read/Write, Read Only, or None to tags
  - Useful to control which tags can be modified from an HMI or other external application
- A cryptographically licensed trusted connection is established between RSLogix™ 5000 and the Logix controller
  - Ensures the “External Access” attribute can only be changed by RSLogix 5000
  - “Who” can use RSLogix 5000 to change this attribute controlled by FactoryTalk® Security
- Users can also define tags as Constants
  - Constants can not be modified by controller logic

Improves security of tags especially when used in conjunction with FactoryTalk® Security
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
New in Logix v20 – 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 RSLogix 5000, in other software applications and in other controllers via Message instruction

- The set of events that causes the Audit Value to change can be configured
New in Logix v20 – Controller Change Detection

- The Audit Value is stored in every Controller Log entry
- FactoryTalk® AssetCentre (in version 4.1), will be able to monitor the Audit Value and read in the Controller Log

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Date</th>
<th>User Name</th>
<th>Change State Value</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>Record Number</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Record Time</td>
<td>1:21:07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Project download</td>
<td></td>
<td>NA\clark [ Daniel W. Clark ]</td>
<td>16#FD60_CB89_029F_3500</td>
</tr>
<tr>
<td>9</td>
<td>Change Log entry added</td>
<td></td>
<td>NA\clark [ Daniel W. Clark ]</td>
<td>16#FD60_CB89_029F_3521</td>
</tr>
<tr>
<td>10</td>
<td>CCUID Configuration update</td>
<td></td>
<td>None</td>
<td>16#FD60_CB89_029F_3566</td>
</tr>
<tr>
<td>11</td>
<td>Change Log entry added</td>
<td></td>
<td>None</td>
<td>16#FD60_CB89_029F_358F</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>
Agenda

- How did we get here?
- What can we do to protect our systems?
- Logix Security
- **FactoryTalk Security**
- Keeping Appraised
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 group)
FactoryTalk Security Configuration

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)
FactoryTalk Security
Disconnected Operation – Cached Credentials

- FactoryTalk® Directory provides a central storage repository (yellow pages) for:
  - Security configuration information (Users, roles, controllers, permissions…)
  - Every time a client connects to the Directory, it is updated with the latest security information…
  - … and that information is cached locally when disconnected from the Directory
Disconnected operation is supported by caching the Directory’s security credentials on the client computer.

- This new Policy defines how long those credential are valid while disconnected.

Directory cache expiration

Determine how long the cache files remain available after the client computer is disconnected from the server. Once this time elapses, reconnect to the directory server to access the latest data files.

- Minimum: 0 hours
- Maximum: 9999 hours
- Default: 0 hours before expiration
Coming in v2.51 / Logix v21(SR5.1)
FactoryTalk Security - Cache Expiration - Override by Computer

- Allow modification of the Directory Cache setting by:
  - Computer Group
  - Or Computer
New in Logix v20 (SR5)
Security Authority Identifier

- With FactoryTalk Services Platform SR5 and Logix V20
  - Configures Logix Controllers to **require** that all users be authenticated from a **specific instance** of the FactoryTalk Directory before they can access the controller (Security Authority Identifier)
  - Security Authority Identifier gets stored in the project (“project binding”) – secures the offline file

Anyone working on a project (on-line or off-line) with the “Security Authority ID required” box checked...

Is first required to “Log On” ....

... using the FactoryTalk Directory used to secure the project
New in Logix v20
Security Authority Identifier

- Using the FactoryTalk Administration Console, the **Security Authority Identifier** can be...
  - Viewed or changed (without changing the FTDirectory contents)
  - Encrypted with a passphrase or password to allow for secure backup copies (disaster recovery)
  - Enable secure duplication and distribution to allow multiple FTDirectories to share the same ID!
    - Can be used to replace the CPU Lock functionality that was deprecated in v20
Security Authority Identifier
Best Practices

- Backup the Directory and Encrypt it
  - There are no backdoors so keep it in a safe place

- Backup your projects
  - Offline projects are also secured
  - Option: save a secured and unsecured offline project
FactoryTalk Security is installed by Logix 5000 (automatically) starting with v20

With v20, security is always on but effectively “disabled” to allow out-of-box default access during installation;

- If you are a Windows “Administrator” on your local computer;
- You automatically become a FactoryTalk “Administrator” and
- Automatically get “Logged In” as “FTAdministrator” by just launching Logix 5000

With v21, we are adding “Authenticated Users” group to the out-of-box default access

- If you are a Windows “Standard User” on your local computer;
- You automatically become a “FactoryTalk User” and
- Automatically get “Logged In” by just launching Logix 5000
- Eliminates the “Log On to FactoryTalk” pop-up dialog
**Application Authorization**

- Acts like an application white listing service to “accept” or “deny” Directory Access from software applications ("no Yellow Pages for you")
  - Manage access by; App Name, Version, Computer and Publisher (Rockwell Automation)
    - Publisher column displays the digital signature that verifies the authenticity of the software
  - Diagnostic Log contains a record of “accept” and “deny”
Log on to FactoryTalk using an administrator account

To secure your FactoryTalk system, you must log on to that directory using a user account that has administrative access to the directory:

- If you installed FactoryTalk Services Platform, version 2.10 (CPR 6) or later on a new computer, you can access the:
  - Network Directory using any Windows user account that is a member of the Windows Administrators group or your local computer
  - Local Directory using any Windows user account

- If you upgraded from FactoryTalk Automation Platform version 2.00 (CPR 7), you can log on using any FactoryTalk or Windows-linked account that is a member of the FactoryTalk Administrators group. If the FactoryTalk administrator account is locked or has expired, you can enable it using the FactoryTalk Directory Configuration Wizard.

See **Log on to FactoryTalk**. You must log on to, and configure security settings for, each directory separately.

**Tips:**

- If the administrator account is a locked or expired Windows-linked account, enable the account in Windows.
- If the administrator account is a locked or expired FactoryTalk user account, run the **FactoryTalk Directory Configuration Wizard** to enable the account.

**IMPORTANT!** Keep your administrator user name and password in a safe place. To enable the administrator account, you must have both the original user name and password to the account. If either is lost, the account cannot be enabled.
New in Logix v20 – Trusted Slot Designation

Controller Properties - Security Hardening

Security Authority: FactoryTalk Security (\SERVERURI\rest_of_the...)

Require Matching Security Authority ID for Authentication and Authorization

Restrict Communication Except Through Selected Slots

Select Slots:

Communication Restricted Through Controller Ports
1756-EN2TSC Secure Communication Module

Remote Workstation

Optional Cisco VPN Appliance (ASA)

Maintenance Port

Site operations

Remote 1756-EN2TSC

- Secure Communications between a CLX controller and plant level systems (ie. MES, Site operations, peer to peer with other systems, user workstations, etc.)
- Users or Systems must authenticate themselves to this module before gaining access to modules on the local 1756 Backplane
Agenda

How did we get here?

What can we do to protect our systems?

Logix Security

FactoryTalk Security

Keeping Appraised
Keeping Apprised – ICS CERT

http://www.us-cert.gov/control_systems/ics-cert/

Control Systems Security Program (CSSP)

Industrial Control Systems Cyber Emergency Response Team
Keeping Apprised
SCADASEC Mailing List

[SCADASEC] Grant opportunity- Trust/Identity ... (Cross posted) - Good thoughts, Joe, but allow me to point
[SCADASEC] Five Tactical Security Metrics To Watch - Essentially, there are five (5) primary metrics which
[SCADASEC] Google's Chrome no longer checking SSL revocation - We're talking about smartgrid stuff, right?
[SCADASEC] What fuels our thought-base...? Is it education, is it experience, ...both, ... - Robert Mathews
[SCADASEC] Smart Grid Network in the Cloud - I'd like to hear more about how the agility/Convergence sol
[SCADASEC] UPDATE - Analysis Shows Design Flaw, Not Vulnerability Sunk Siemens - Two examples can
[SCADASEC] RNADIARECEIVER vulnerability - Kevin Lackey wrote: > eliminate external connectivity and
[SCADASEC] More exposure to "SCADA" devices through Shodan... - On 1/22/12 8:55 PM, Bob Radvanyo
[SCADASEC] iPad & iPhone & Android SCADA and HMI app security analysis? -
[SCADASEC] Disclosure behavior at the S4 Conference - Moderator note: Found the
[SCADASEC] Cloud ICS inquiry - Thank you all for your insightful responses. I real
[SCADASEC] Project basecamp presentation at S4 - and more news stories: http
[SCADASEC] SLUB, SLAB, and SLOB - Moderator note: * The following post seems
[SCADASEC] Anonymous publishes claimed Israeli SCADA systems passwords
Keeping Apprised

http://rockwellautomation.com/security

Assessment Services

Security Technology

Security FAQ

Security Services

Leadership & Standards

secure@ra.rockwell.com

Pretty Good Privacy (PGP) Public Key

Copyright © 2011 Rockwell Automation, Inc. All rights reserved.
Keeping Apprised - Microsoft Patch Qualification

Whitepaper
Computer System Security Updates: Why patch your computers?

Knowledgebase Article #: 35530*

Microsoft Patch Qualification for Rockwell Automation software products

http://rockwellautomation.custhelp.com/app/answers/detail/a_id/35530
# Keeping Apprised - Microsoft Patch Qualification

![Microsoft Patch Qualification](http://www.rockwellautomation.com/)

## MS Patch Qualifications

- Home
- What's New this Month
- CPEs
- OS's
- Limited Qualifications

Download to Excel ![Download](http://www.rockwellautomation.com/)

## What's New this Month

<table>
<thead>
<tr>
<th>MS KnowledgeBase</th>
<th>MS Security Bulletin</th>
<th>Date Released</th>
<th>Qualification Status</th>
<th>Recommendation</th>
<th>CPR</th>
<th>Date Published</th>
<th>Details</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB953300</td>
<td>MS08-061</td>
<td>10/13/2009</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>9</td>
<td>2/18/2010</td>
<td>XPSP2, 2003R2SP2</td>
<td></td>
</tr>
<tr>
<td>KB953300</td>
<td>MS08-061</td>
<td>10/13/2009</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>7</td>
<td>2/18/2010</td>
<td>XPSP2, 2003R2SP2</td>
<td></td>
</tr>
<tr>
<td>KB953300</td>
<td>MS08-061</td>
<td>10/13/2009</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-008</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>7</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2, 2003R2SP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-008</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-008</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-006</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>7</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-006</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-006</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-005</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>7</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-005</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>6</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
<tr>
<td>KB978262</td>
<td>MS10-005</td>
<td>2/9/2010</td>
<td>Published</td>
<td>Fully Qualified</td>
<td>7</td>
<td>2/18/2010</td>
<td>2KAdvSP4, XPSP2</td>
<td></td>
</tr>
</tbody>
</table>

Last Updated: 2/19/2010
Industrial security continues to rapidly become an essential consideration in the design and operation of contemporary control systems. Rockwell Automation recognizes the importance of security for industrial control applications. Employing good security measures in a control system can help protect against other things, such as personal safety, critical assets, intellectual property, and key proprietary data. It remains an integral aspect to the Rockwell Automation control philosophy to deliver and evolve comprehensive security solutions that meet customer needs while also providing an appropriate level of support and services that help fulfill our customer's security goals and requirements.

This Industrial Security Advisory Index contains direct pointers to specific industrial security content held in Rockwell Automation's Knowledgebase and public website. The materials contained herein and hereby referenced are intended to inform, educate, and assist our customers about industrial security as it relates to Rockwell Automation products and systems.

Rockwell Automation Security Notices & Alerts:

- **54103 - Firmware Upgrade Security Notice: Comment on DHS Communication (Control Systems Vulnerability)**
- **57729 - Potential Security Vulnerabilities in ControlLogix 1756-ENBT/A EtherNet/IP Bridge**
- **58984 - ControlLogix 1756-ENBT/A EtherNet/IP Bridge Firmware Upgrade Process**
- **65980 - Password Security Vulnerability in MicroLogix™ Controllers**
- **65982 - Client Software Authentication Security Vulnerability in MicroLogix™ Controllers**
- **66678 - Password Security Vulnerability in PLC-5® and SLC™ 5/0x Controllers**
- **66684 - Client Software Authentication Security Vulnerability in PLC-5® and SLC™ 5/0x Controllers**
- **69735 - Open UDP Port in 1756-ENBT EtherNet/IP™ Communication Interface**
- **70020 - Rockwell Automation recommended mitigations for Zero day vulnerability (W32.stuxnet)
To make sure you get the news you can use...

http://rockwellautomation.com/security
Questions?
Backup Slides:
CPU Lock using FactoryTalk Security and SAID
OEM “CPU Lock” of Logix Controller

Both OEM users need to lock and unlock the controller.
Bob “Locks” the Controller

Bob’s Computer
(Local FTDirectory)

Step 1: Bind the controller project to Bob’s FactoryTalk Directory and download to “lock” the project (Note: Bob’s Security Authority ID is:

Current Identifier: 42CBE60F-6657-49E1-A047-83630813CA65)

Step 2: Open Admin Console and select “backup” the FTDirectory

Step 3: Enter a “passphrase” to encrypt the file (= “Welcome1”) And add file name (“CPU Lock file”)

Step 4: Email the “CPU Lock file” to Tom, call Tom and give him the secret “passphrase”
Tom “Unlocks” the Controller

Step 1: Extract the file from Bob’s email

Step 2: Open Admin Console and select “restore” the Directory (select the “CPU Lock File”)

Step 3: Enter the “passphrase” that Bob gave Tom (=> “Welcome1”)

Step 4: Select “restore security authority identifier only” (Note: the ID is now the same as the one on Bob’s computer)

Open Logix 5000 and connect to the controller!