T03 - New Security Features Help Reduce Risk in Your Industrial Control System
**ICS Security in the News**

**BBC** Hack attack causes 'massive damage' at steel works

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI).

It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.

This led to parts of the plant failing and meant a blast furnace could not be shut down as normal.

The unscheduled shutdown of the furnace caused the damage, said the report.

In its report, BSI said the attackers were very skilled and used both targeted emails and social engineering techniques to infiltrate the plant. In particular, said BSI, the attackers used a "spear phishing" campaign aimed at particular individuals in the company to trick people into opening messages that sought and grabbed login names and passwords.
Secure Automation and Information
Defending the Digital Architecture

Secure Network Infrastructure
Control Access to the network, and Detect unwanted access and activity

Access Control & Policy Management
Control Who, What, Where & When access is allowed, to which application & device

Content Protection
Protect viewing, editing, and use of specific pieces of control system content

Tamper Detection
Detect & Record unwanted Activity & Modifications to the application

INDUSTRIAL SECURITY
MUST BE IMPLEMENTED AS A SYSTEM
Secure Automation and Information
Capability Overview

**Tamper Detection**
Detect & Record unwanted Activity & Modifications to the application
- Firmware Digital Signatures
- Auditing with FactoryTalk® AssetCentre
- Change Detection and Logging for Controllers
- High Integrity Add-On Instructions (AOIs)

**Secure Network Infrastructure**
Control Access to the network, and Detect unwanted access and activity
- Validated Architectures
- Stratix® Portfolio
- Network and Security Services
- Stratix® 5950
- 1756-EN2TSC/B

**Content Protection**
Protect viewing, editing, and use of specific pieces of control system content

**Access Control and Policy Management**
Control Who, What, Where & When access is allowed, to which application & device
- Logix Source Protection
- Data Access Control
- FactoryTalk® Security
- Firmware Digital Signatures
- Auditing with FactoryTalk® AssetCentre
- Change Detection and Logging for Controllers
- High Integrity Add-On Instructions (AOIs)

**Partnerships**
- Tripwire Partnership
- Owl CTI Partnership
- Tempered Networks Partnership
- Symantec Partnership
Sources of Risk

Which control system components do you consider at greatest risk for compromise?

Rank the top three, with “1” indicating the component at greatest risk.

Source: The State of Security in Control Systems Today, SANS Institute
Holistic Approach

A secure application depends on multiple layers of protection and industrial security must be implemented as a system.

- **Defense in Depth**
  Shield targets behind multiple levels of security countermeasures to help reduce risk

- **Openness**
  Consideration for participation of a variety of vendors in our security solutions

- **Flexibility**
  Able to accommodate a customer’s needs, including policies & procedures

- **Consistency**
  Solutions that align with Government directives and Standards Bodies
Vendors must build security into products with a focus on security throughout the products lifecycle...

- **Product Security Office**
- **Secure Development Lifecycle**
FactoryTalk® AssetCentre 7.0
Asset Inventory Crawler

• Scheduled scan of RSLinx® Driver; report on all automation assets
• Scan engineering workstations for installed software
• Create/update/compare assets
• Output PDF of Asset Inventory Report

Discover and maintain an inventory of devices in the plant and help customers manage their automation investment effectively!
Incident Audit and Response
FactoryTalk® AssetCentre

Archive & Disaster Recovery
• Centrally manage versions of electronic files & folders
• Automatic (scheduled) Backup & Compare of operating asset configurations

Audit
• Track user actions – Who did What, When, Where?
• Searching and reporting on log files (scheduled or ad hoc)

Security
• Restrict viewing of artifacts
• Prevent unauthorized access to make changes

Extensibility
• Ability to extend and add support for 3rd party devices
• Easy to scale asset management to meet your needs

Process Device Configuration & Calibration
• Support for Process Device Configuration using FDT-DTM technology
• Paperless management of instrument calibration data
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.
FactoryTalk® Temporary Users
New in Version 28

- Use FactoryTalk® Temporary Users to temporarily give someone access to privileges of a different user group
Permission Sets for Securing Projects
New in Version 28

- Secure a project file with a Permission Set to use the same policies for many controllers
Permission Sets for Securing Objects
New in Version 28

- Apply Permission Sets to Routines, AOIs and Tags to have different policies for different components
Guest User Access
New in Version 28

- With Guest Users, grant limited permissions to users who aren't members of your FactoryTalk® Directory.
Guest Users can further limit access to a project file with a Secondary Security Authority.
Tamper Detection: Controller Change Detection

- Every Logix Controller exposes a Change Detection Audit Value
- When something happens that can affect 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
Tamper Detection:
Controller Change Detection

- The Audit Value is stored in every Controller Log entry
- FactoryTalk® AssetCentre (in version 4.1), can 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>remark</td>
<td>TSV-Controller-Log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remark</td>
<td>Date = Jun-02-2011 15:21:20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remark</td>
<td>Controller = 1756-L71/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remark</td>
<td>Serial-Number = 16#0067_D1CF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remark</td>
<td>Revision = 20.02</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Record Number</td>
<td>Time</td>
<td>Entry Description</td>
<td>User Name</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td></td>
<td>Project download</td>
<td>NA\clark \ Daniel W. Clark</td>
</tr>
<tr>
<td>8</td>
<td>1 Jun-02-2011 15:21:07</td>
<td></td>
<td>Change Log entry added</td>
<td>NA\clark \ Daniel W. Clark</td>
</tr>
<tr>
<td>9</td>
<td>2 Jun-02-2011 15:21:07</td>
<td></td>
<td>Change Log entry added</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>3 Jun-02-2011 15:21:38</td>
<td></td>
<td>CCUID Configuration update</td>
<td>None</td>
</tr>
<tr>
<td>11</td>
<td>4 Jun-02-2011 15:21:38</td>
<td></td>
<td>Change Log entry added</td>
<td>None</td>
</tr>
</tbody>
</table>
Content Protection
License Based Source Protection

- Access to selected Routines and AOIs can be controlled using Licenses
- Licenses are managed by the content owner using a web based application, and reside on secure USB devices
Content Protection
Execution Protection

- Content owners can help prevent overuse by requiring a license to be present in the controller to allow protected routines and AOIs to execute
Stratix® 5950 Security Appliance

Now Released

Strategic collaboration between Cisco and Rockwell Automation

- Based on recognized and proven technologies
  - Adaptive Security Appliance for Firewall and VPN
  - FirePOWER™ Technology for Inspection and detection
  - Enhanced with OT context of protocols, behaviors, and features

- Key Features:
  - Deep Packet Inspection for ICS protocols
  - Threat & Application Update Service
  - DIN rail mount
  - Connectivity Options:
    - (4) 1Gig Copper
    - (2) 1Gig Copper and (2) SFP
  - Industrially-hardened
Stratix® 5950 Security Appliance

Applications

The Stratix® 5950 is ideal for resolution of the following challenges:

Lacking visibility and control to help prevent erroneous activity and to maintain integrity of operations on the plant floor, for ex., prevention of tampered with firmware being downloaded to a Controller by confirming only an authorized user can conduct the download.

Stratix® 5950 offers Intrusion Prevention capability and detailed network visibility which enhances traditional firewall functionality to allow for informed decision making through the use of Deep Packet Inspection technology.

Threat control for vulnerable industrial control systems (ICS) devices, and/or legacy equipment, and protection against communications from ICS components at risk of compromise.

Stratix® 5950 allows for vulnerability identification and mitigation through configuration of policies to block actions, like CIP Reads, Writes, Download to provide protections for communications with ICS devices like HMI, and Computer Workstations.

Stratix® 5950 addresses the challenge for Industrial Automation professionals to maintain operations integrity while making data more available from the ICS.
Firewalls and Deep Packet Inspection

- **Typical IT firewalls are capable of inspecting**
  - Source or Destination MAC or IP address
  - Source or Destination TCP or UDP Ports, or
  - Protocol elements of a packet

- **Deep Packet Inspection extends upon these firewalls’ capabilities**
  - Provides granular protection per protocol (ex. CIP, Modbus, DNP3) in the Industrial Zone
  - Gives the visibility and control to help prevent erroneous or malicious activity down to the Cell / Area zone level

- **Intrusion Prevention System (IPS) and Intrusion Detection Systems (IPS) uses DPI.** What you want to do after you have inspected the packet?
  1.) After inspecting the packet using DPI, achieve granular control through security rules that act on matched network traffic – do we want to drop the packet after inspection?
  2.) Do we allow this application or command, or is this a known threat?
For Centralized Management (as an alternative to an on-box management interface for each Stratix 5950):
- FireSIGHT® Management Center
- Cisco Security Manager

Industrial Demilitarized Zone (IDMZ)

Industrial Zone
Levels 0 - 3
(Plant-wide Network)
ControlLogix® Secure Communications
Released - 1756-EN2TSC/B

Enforce network access control at the 1756 chassis

- Authentication and Access Control through IPsec or L2TP (Up-to 8 Tunnels)
- Compatible with and connects to:
  - Windows Servers, Workstations, and Mobile devices
  - Security Appliances (Stratix® 5900, Stratix® 5950, Cisco ASA)
  - Other 1756-EN2TSC Modules
- Configuration through embedded HTTPS interface

Non-SECURE Mode (Out of the Box)
- Does not support Motion
  - DOES support CIP Sync™ (the use of time in the network)
- Does not support Redundancy

SECURE Mode (when enabled)
- Disable the USB port and IP address switches (for users concerned about risks associated with physical access to the module)
- Configure authorized username and password credentials for the module
- Secure Backup and restore functions for configuration
ControlLogix® Secure Communications

Applications

The 1756-EN2TSC/B module is ideal for the following applications:

- Controllers leveraging multiple network cards with dedicated cards for “upward” connectivity.
  - Replace the “upward” facing card with this module to add access control going up to plant servers/site operations, other production cells, or programming terminals across the plant network.

- Looking for network based access control at the local controller to prevent unauthorized access from the plant network.
  - Authentication to this module required to access the Controller or any other modules in the local 1756 backplane over the Ethernet network.

- Looking to encrypt data coming to and from the controller over the network to production servers.
  - Encrypt sensitive production data going across the plant network.
Secure Network Infrastructure
New Tested and Validated Architectures

Achieve infrastructure security through a common, tested and validated system architecture leveraging the Stratix® portfolio and Cisco security solutions.

Converged Plantwide Ethernet (CPwE):
• Segmentation Methods within the Cell/Area Zone (2013)
• Securely Traversing IACS Data Across the industrial demilitarized zone (2015)
  • ENET-WP038A-EN-P; ENET-TD009A-EN-P
• Deploying Identity Services within a Converged Plantwide Ethernet Architecture (2015)
  • ENET-WP037A-EN-P; ENET-TD008A-EN-P
• Site-to-site VPN to a Converged Plantwide Ethernet Architecture (2016)
  • ENET-TD012A-EN-P
• Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture (2016)
  • ENET-WP011A-EN-P, ENET-TD002A-EN-P

Download these and more at:
Series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

Applies to those responsible for designing, manufacturing, implementing, or managing industrial control systems:

- End-users (that is, asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors
Encompass™ Partner - Tripwire

- Tripwire CCM
  - Audit industrial automation networks and controllers for secure and approved configurations
  - Identify unauthorized changes, configuration hardening errors and security vulnerabilities
  - Layer on top of a standard implementation of FactoryTalk® AssetCentre for greater visibility into industrial automation applications
Symantec Embedded Security: Critical System Protection

- Great for helping to protect PCs that cannot be frequently updated
- Completely policy driven – no signatures
- Features include:
  - Application Whitelisting
  - Sandboxing
  - Host Firewall
  - File Protection
  - Monitoring, and more…
Network segmentation using private overlay networks on top of untrusted infrastructure

- Private networks can be mapped to users and/or devices
- Requires no changes to existing infrastructure
- Leverages HIPswitches and a centralized HIPConductor
- Data Diodes for secure one-way data transfer
- Enables data to move out of control system networks without allowing any data in, for...
  - View-only OPC
  - View-only screen sharing
  - Historian Replication
  - Backups
- Allow tightly controlled movement of data into control system networks for needed files, patches and software updates
Network and Security Services
Full lifecycle service offering with global capability

We can help, from assessment to on-site security control deployment...

- Converged skill set of operational technology (OT) and information technology (IT)
- Experience across industrial control applications and networks
- Unlike large IT vendors and resellers, we offer a comprehensive and tailored solution that balances both strategic and tactical needs of your company.

Because infrastructure matters...
Thank you! Questions?