# **CRYPTOME**

16 January 2011

## **Siemens Process Control System 7 Security**

Extracted from full Siemens Process Control System 7 Specifications:

http://cryptome.org/0003/siemens-pcs7.pdf

Related New York Times report on the Stuxnet virus today:

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

# 17 Industrial / Cyber Security

In order to protect the process automation system from the danger of hacker attacks, viruses etc., the vendor / system shall provide comprehensive industrial / cyber security capabilities consisting of products and procedures (best practices).

### 17.1 Use of "Defense in Depth" Architectures

The system shall support the use of a "Defense in Depth" strategy as recommended by the US Dept of Homeland Security. "Defense in Depth" advocates the creation of a nested security architecture by division of the plant into secure and closed security cells / segments with clearly defined and monitored access points.

## 17.2 Rules for Creation of Security Cells and Segments

The following rules shall be followed to ensure the creation of secure and fully functional security cells and segments:

- Each segment must form a self-sufficient "zone" that can be operated for a certain amount of time without connection to other segments; thus a segment must be capable of operating autonomously for a period of time.
- All components contained in a segment and involved in its function should be connected to one another (not through leased lines)
- Units that cause high network and computer load when connected from the outside via a complex security mechanism should be integrated directly in the segment
- Access to a security cell should take place only after the user's identity has been verified and logged and only under supervision of authorized persons, for example, physical access by operators.
- All connections to the Control System LAN should be routed through a firewall, with no connections circumventing it.

# 17.3 Securing network access points

The system shall allow clear demarcation between the protected internal network (control system LAN) and unprotected or untrusted external networks.

#### **Use of Firewalls**

The system shall support the use of firewalls to block selective (filter) traffic between network zones (subnets) or from a network to a device. To provide maximum protection, firewalls must allow for rules to be created which allow only necessary access by employing one or more of the following techniques:

- Packet filtering
- Circuit level gateways
- Proxy gateways
- Stateful inspection

#### Supported Firewalls

The following firewalls shall be supported at a minimum:

- Windows XP Personal Firewall
- Microsoft ISA Server 2004

#### **Security Modules for Industrial Environments**

The vendor shall supply rugged, industrial-rated security modules as required, meeting the following characteristics:

- Integrated firewall capable of Filtering on IP-, MAC addresses and ports
- Capable of providing the following additional functions: NAT, DHCP Server, Data encryption
- IP 30 Protection
- Operating Temperature Range: 0℃ to +60℃
- Capable of accepting Redundant Power input
- Can be configured / setup without expert security knowledge

#### **Creation of Demilitarized Zones (DMZ)**

The system shall support the ability to segment the network by use of demilitarized zones (DMZ). DMZs shall be used to provide a secure access point for the following types of control system connections:

- Data Historian (when it communicates outside the control network)
- Web servers
- Security servers
- SUS Servers

# 17.4 User Management and Access Control

#### **Central User Management**

The system shall provide the capability of the central management of users within domains or workgroups providing the following specific capabilities:

- Create, delete, lock-out users
- Ensure IDs are unique
- Two-level ID (username + password) or Login Device (e.g. Card Reader)

#### **Password Security**

To ensure the security of the passwords used for accessing the system, the following capabilities shall be available:

- Specification of password properties (min. length ...)
- Limited time for password validity
- Expired passwords excluded for the next "n" generations
- Forced password change after first Log-On
- Auto log-off after "n" minutes of inactivity
- Lock-out of users after "n" failed attempts to log-in.

#### **Role-based Access Control (RBAC)**

The system shall provide for user accounts with configurable access and permissions associated with the defined user role. The system shall support the implementation of the principle of minimal rights whereby users and computers can be configured with the minimum set of access rights necessary to perform their function.

#### Single Sign On

The system shall provide the ability for Single Sign On (SSO) authentication whereby a single login / password allows a user to have access to all programs (PC / Desktop Access, Engineering Tools, HMI, Batch Management) without requiring re-authentication for each application. The Single Sign on capability shall be capable of being used with Role-based Access Control (RBAC)

# 17.5 Software Security Patch Management & Testing

Continuous and immediate testing of new software security patches is critical to maintaining a secure network infrastructure.

#### Support for Immediate Installation of Microsoft Security Patches

If deemed necessary by the user, it shall be permissible to load the following new MS Security Patches on the system as soon as they are released from Microsoft:

- Windows operating system
- Internet Explorer
- SQL Server

#### **Testing of Microsoft Security Patches**

To ensure that the latest Microsoft Security patches have been tested for compatibility with the system, the vendor shall test new Microsoft security patches immediately upon their release. Results of the testing shall be communicated to end users so that they can choose when / if to update.

#### **Software Update Service**

The system shall support the use of the Windows Software Update Service (SUS) from Microsoft as a means to quickly and effectively implement automatic deployment of software updates and security patches on all PCs connected to the control network. The SUS Server shall allow viewing of all available updates so that they can be released as required in a procedure determined by the end user.

#### 17.6 Use of Virus Scanners & Malware Detection

The system shall support the installation of Virus Scanners on all PCs attached to the control network. The following Virus Scanners shall be supported at minimum:

- Trend Micro Office Scan
- Symantec Norton Antivirus
- McAfee Virusscan

#### **Minimizing Impact on System Performance**

To ensure that virus scanners do not have a negative impact on system performance, the vendor shall provide guidance on malware detection settings for use with their system based on the results of system compatibility testing.

#### **Updates and Testing of New Signature Files**

To ensure that virus scanners are able to be continuously updated to prevent new malware threats, the vendor shall test new virus signature files immediately upon their release. Results of the testing shall be communicated to end users so that they can choose when / if to update.

#### **Installation and Operation of Virus Scanners**

The Installation and Operation of Virus Scanners shall comply with the following:

- Engineering Stations and all other PCs where engineered data can be introduced to the Control System Network: Virus scanners shall be operated in a real-time mode with continuous scanning of all incoming traffic and shall support manual and periodic scans while offline (Runtime and Engineering)
- Operator Stations: Virus scanners shall be operated in real-time mode with continuous scanning of all incoming traffic (Runtime)

## 17.7 Auto Configuration of System Security Settings

To minimize the chance of error during the configuration of security settings, the system shall support the automatic configuration of Windows firewalls and registry entries.

# 17.8 Securing Access for Remote Maintenance / Troubleshooting

The system shall be capable of providing a secure connection for remote maintenance and troubleshooting. This access point shall be securable through use of local firewalls and virus scanning software at a minimum. The following methods shall be supported:

- Authentication and Encryption with IP Security (IPsec)
- Authentication and Encryption with Secure Sockets Layer (ssl and https)
- Use of VPN (Virtual Private Network) tunneling and Network Access Quarantine Control for Secure Support Access

# 17.9 Testing for Security Vulnerabilities

The system shall support the end user or designate testing for vulnerabilities using the Microsoft Baseline Security Analyzer (MBSA) or equivalent. Testing shall be able to identify the following conditions at a minimum:

- · Open ports and protocols in use
- Missing Microsoft security patches