Cyber Security Model for Manufacturing

Nancy Cam-Winget
Distinguished Engineer
Cisco Systems

Xuechen Yang
Senior Engineering Director
SolarWinds

Presented at the ODVA
2015 Industry Conference & 17th Annual Meeting
October 13-15, 2015
Frisco, Texas, USA

Abstract
Industrial Control Systems (ICS), especially Manufacturing Systems, is becoming a primary Cybersecurity target. With the increased number of reported threats, ODVA is in the process of adopting security measures. This paper will present an Industrial Control System Cybersecurity framework and further describe its mapping to Manufacturing. In particular, we will put focus on how ODVA's effort fits into the larger framework and how it can continue to influence and strengthen on the ICS Cybersecurity framework.

Keywords

Cybersecurity, Role-Based Access Control (RBAC), Network Visibility, trustworthiness, machine-2-machine (M2M), IDS/IPS, SIEM, SDL, root of trust, RNG

Definition of terms (optional)

IDS/IPS: Intrusion Detection Systems is a monitoring tool to provide the visibility of network traffics and report any suspicious patterns that could indicate a network or system attack; and Intrusion Protection Systems is a deeper inspection tool that also includes policies and rules for alerting and providing remediating actions to an administrator.
Network Visibility: the means to have awareness of who (humans and devices), what (applications) and how the communications are traversing through the network.

RNG: Random Number Generator.

SDL: Security Design Lifecycle defines the phases and tasks to ensure a robust and secure system.

SIEM: Security Information and Event Management is a type of technology for managing security events. Such products attempt to provide a more holistic view beyond network traffic and improve on the efficacy of security event reporting.

Trustworthiness: in the context of Cybersecurity, it is the ability for a device, application or human to attest to its authenticity.

Introduction

The "ICS-Cert Year in Review" reports [1][2][3] show a growing trend of reported incidents with the latest 2014 report demonstrating a growing trend in manufacturing where reported incidents went up from 38 incidents constituting 15% of the total reported ICS incidents in 2013 to 65 in 2014, constituting 27% of the reported incidents. With the growing trend in threats and reported incidents, the need to secure Manufacturing deployments strengthens ODVA's initiative to provide security in the protocols and interfaces.

The National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) continue to address the security issues and of late are focused on Industrial Control Systems as they pertain to the nation's critical infrastructure. In particular, NIST currently has an active public working group focused on this topic in the Cyber Physical Security Working Group. It is a public forum (http://www.nist.gov/cps/cpspwg.cfm) with different focus groups where defining a reference architecture and cybersecurity are two of its main areas of focus. A general framework for an ICS Cybersecurity was also published on February 2014 [4] enumerating the set of functions and activities required to achieve specific cybersecurity outcomes; the table is also summarized in Figure 1 below.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS,MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 1 Critical Infrastructure Core Structure and Functions

With ODVA's focus on defining the Industrial Automation standards for vendors and suppliers to interoperate, it is well aligned to address the Asset Management, Access Control, Data Security, Protective Technologies and general Communication categories identified in Figure 1. This paper will focus on outlining a cybersecurity framework and design lifecycle focused on these specific categories relevant to ODVA.

A Cybersecurity Model for ODVA

With the specific functions and categories as defined by NIST in Figure 1, we can map them into specific Cybersecurity features and functions and align them to the ICS Purdue model as shown in Figure 2.

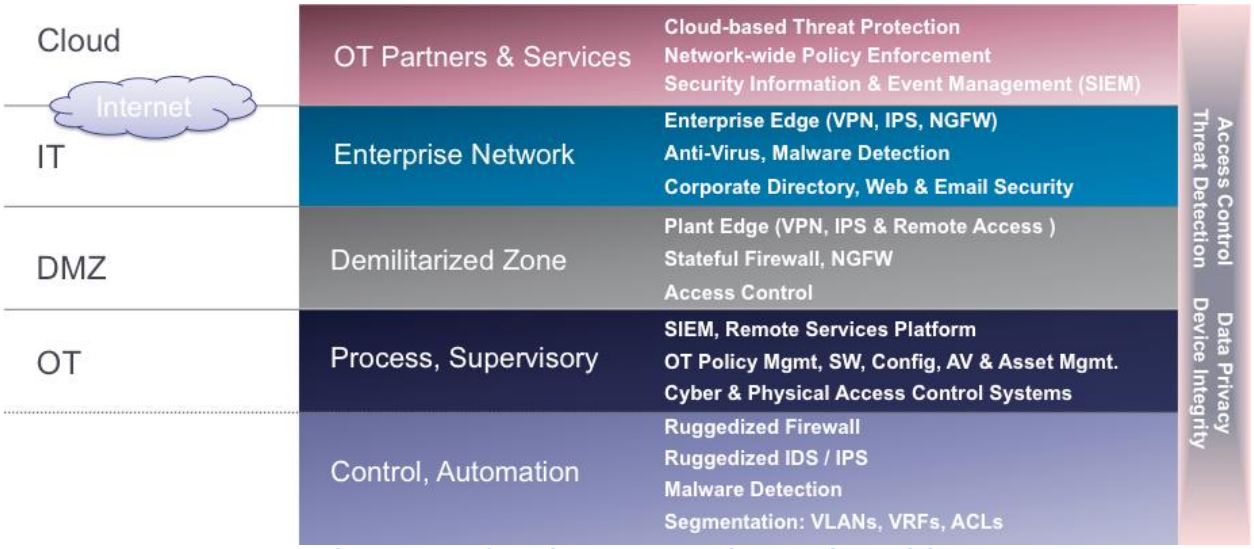

Figure 2 Manufacturing Systems Cybersecurity Model

The Manufacturing Cybersecurity model maps the access control functions across the span of the entire deployment, from the Purdue Level 0 and Level 1 devices through the enterprise and cloud services in Level 5 (and above). Similarly, the Threat Detection mechanisms must accumulate the information for analysis across the entire infrastructure to enable the detection and protection mechanisms provided through IDS/IPS, SIEM and other vulnerability and malware assessment tools. These technologies rely on secure communications across every link and communication paths between all devices and applications. As these security services are now mapped into the common Industrial Automation and in particular, the Manufacturing Systems model, we can now focus on ODVA's alignment and proposed evolution in designing and defining the next generation technologies to address cybersecurity.

A Security Framework for ODVA

To ensure the overall security and integrity of an Industrial Automation ecosystem, Figure 2 demonstrates that all devices, whether a M2M device, a network device, a host or a data server must be secure. The requirements of building a trusted ecosystem implies that all devices, beyond securing its communications, must be robust and secure (e.g. trustworthy). To ensure such trustworthiness, different security components must be provided in the device; these components are shown in Figure 3 and can serve as ODVA's security framework.

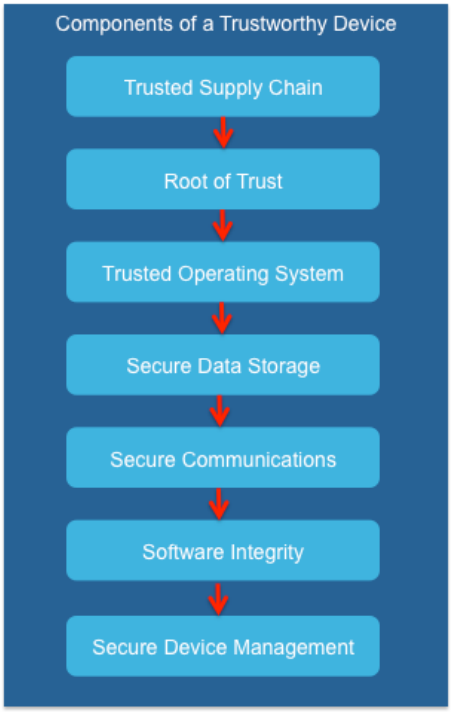

Figure 3 Trustworthy Device Components

The components are summarized as follows:

Trusted Supply Chain: To build a trustworthy ecosystem, we must first ensure that all components of the ecosystem can be trusted; e.g. the supply chain must also be trusted. While this component is not in ODVA's scope to define fully, it merits mention as failure to consign trusted vendors, suppliers and processes for the componentry (whether it is for the Industrial Automation ecosystem or for the particular device being built) breaks the trustworthiness of the system. The ISO 28000 series provide a set of specifications for addressing and building a trusted/secure supply chain.

Root of Trust: A root of trust is a set of functions that are inherently trusted; these functions could be either hardware or software functions that perform measurements or verification of software, perform authentication and protect cryptographic keys. One such specification and implementation is the Trusted Protected Module (TPM) [7] defined by the Trusted Computing Group. Most systems offering root of trust implement hardware assisted components, such as a TPM as the hardware implementation offers best protection of the key storage and its supply chain can be better controlled. Without a root of trust, any outgoing information from the device could be deemed untrusted.

Trusted Operating System: A trusted operating system is one that provides a secure operating environment. Compliance or criteria for a "secure operating environment" have been defined by some organizations such as the ISO/IEC 15408. Some of the functions defined include providing memory and file protection, I/O device access controls, user authentication, access controls and be able to detect some attacks. A function to help provide one security level of assurance that the operating environment is trustworthy is secure boot. An untrusted operating system could allow malware and other attacks.

Secure Data storage: Beyond the protective measures to ensure the system software is protected, applications and data stored on the device must also be protected. This component's goal is to ensure that data stored on the device is only accessed by authorized users and processes as well as providing mechanisms to ensure the data cannot be infected, tampered or corrupted.

Secure Communications: communications involves providing the network services to facilitate communications with other devices securely. This function must provide the appropriate cryptographic

tools to allow the communications to be secure, e.g. providing confidentiality, integrity and replay protection where appropriate. It is understood that not all communication needs confidentiality, but at minimum, communicating peers must be able to authenticate and ensure the information has not been forged, replayed or corrupted.

Software Integrity: Along with a trusted operating system, applications running on the device must be protected from tampering or infection. Software Integrity is the component that defines the functions, processes and tools that help in the detection and protection of software applications running on the device.

Secure Device Management: While each of the components described are functions that help secure a device, these functions and modules must also be managed and managed securely. In particular, the device's security lifecycle must be carefully managed to ensure its identity, credentials and overall health remains secure. Similarly, the configurations and software used to protect the device must also be securely managed. With trends shifting towards outsourcing management or facilitating device management at a larger scale through a cloud based computing system, it becomes more imperative that the management component includes secure communications between the device and the management system. Note that the device, as a whole, may also be managed by different software applications and as such, protective measures such as authentication and authorization of these management applications apply.

Implementing a Trustworthy Device

With a general framework and components defined to design a Trustworthy Device (shown in Figure 3), different levels of security and trustworthiness can be achieved based on implementation. Thus, there are implementation considerations to determine what needs to be included to provide different levels of security.

As ODVA defines how to provide security, it is well poised to define both the protocols to allow products to be built and provide security at any of the levels defined while maintaining interoperability. Additionally, with the levels defined CIP secure specifications may also define best security practices based on these levels.

As shown in Figure 4, different security levels can be achieved based on the type of functionality provided on the device. Spanning from no security (Level 0) to the "golden standard", e.g. Level 4. The list below provides a high-level overview for each level:

- **Level 0** – While at minimum, any component should follow a Trusted Supply chain process; this level offers no security. This level is not recommended for any industrial system.

- **Level 1** – Level 1 security devices have limited security functionalities, which are all software-based. It provides minimum functionality to secure protected (network) communications through the use of username/password techniques and minimal key management. It's suitable for low-cost connected devices that are not part of mission-critical operations. The security features include:
    - Limited core security implementation in software (e.g. no key generation, no OS hardening, no software obfuscation)
    - Software based cryptographic tools to establish secure communications

- **Level 2** – For legacy devices, retrofitting hardware-based security technology is not practical; in which case, software-based security anchor technology can be leveraged. While it may not be as secure and trustworthy, with the right implementation, software-based anchor performs reasonably well and is a viable means to provide security when a hardware-based option is not feasible. Various Level 2 devices are available on the market today, including the smart home automation devices. The security features encompass:

- Software-based security anchor
- All the features defined in Level 1

- **Level 3** – Similar to Level 2 but with the added hardware (vs. software) security anchor to enable a true root of trust. Recommended for adoption by all Industrial machines and devices are part of critical operations, for example, an industrial robot. The features encompass:
  - Hardware security anchor (e.g. TPM or similar functional technology)
  - All features as defined in Level 2

- **Level 4** – Best recommended practice for adoption by all Industrial management and control stations that need to manage operation and file manipulation. For example, any full-featured Industrial HMI System must support level 4 security. The security features encompass:
  - Application and file security
  - Secure device (lifecycle) management
  - Anti-tampering protection of the "root of trust" component
  - All features as defined in Level 3

Figure 4 Implementing different Security levels of Trustworthy Device

Theoretically, vendors may choose to build a secure device in a number of different ways as long as it is bolstered by a security anchor (either hardware or software based) and meets all security requirements. However, as we all know that a poorly designed architecture or implementation can introduce security holes and vulnerabilities into a system, regardless of the encryption key length or encryption algorithm strength. There needs to be a reference architecture that guides the design and implementation of such Trustworthy devices. Another important note is to recognize that the protocols and interfaces designed, but include the agility and flexibility to allow for new cryptographic algorithms and key lengths to "future" proof when an algorithm has been proven to be weakened or compromised.

Figure 5 shows the reference architecture of enabling Trustworthy device and systems. It's a layered design with each layer modularized to allow for each of the modules to be independently implemented and standard APIs defined between the layers.

- **Trustworthy Services** – This is where the root-of-trust is established, identities and anchors stored and maintained. The security of all other layers hinges on the integrity of the security anchor. If the security anchor is compromised, the entire system can no longer be trusted. The set of trustworthy services can be implemented in either hardware or software, and includes following functionalities:

    - Key Generation and RNG; while RNGs can be pseudo-random good sources of entropy are required to ensure randomness. NIST's recommendations [8] and approved methods should be used.
    - Cryptographic Acceleration. At minimum, cryptographic algorithms must be supported, whether in pure software, firmware or fully accelerated in hardware.
    - Integrity and Anti-Tampering. Integrity of at minimum, the operating system software and the trusted modules (and anti-tampering techniques against these modules) must be provided.
    - Secure Boot and Secure Firmware Upgrade
    - Secure Storage
- **Security Core** Services– This software-based layer encapsulates functions provided by the trustworthy services and present them to the rest of the system via standard APIs. It may perform other security functions as well, for example, OS software hardening, and system-level software attestation.
- **Device Security Management Services** – This layer embodies the set of security functions and features that are essential to secure software operations and the overall security health throughout a device's lifecycle. For example, this layer shall support some form of 802.1AR certificate enrollment (e.g. EST or SCEP) and certificate management functions, and bind the secure device identity to the certificate and private key. Typical services include:
    - Certificate Enrollment and Secure ID Management
    - Secure Connectivity Agent (e.g. 802.1X)
    - Secure Logging and Auditing
    - Application and File Inspection and Attestation
- **Vendor-specific Software Apps** – Different vendors can build various security applications on top of the underlying security layers and tailor the system for potentially different levels of security to ensure interoperability across different network and operations. For example, ODVA members can easily implement Secure CIP application by leveraging the security APIs provided by the underlying layers.

Figure 5 Reference Architecture of Trustworthy Device

As shown in Figure 5, there are numerous options that can be used as the baseline for each layer. For example, multiple chipset vendors including Intel and ARM have already provided TPM functionality in their offerings. In addition, Cisco Systems offers both hardware and software-based security anchor products. It is up to the device manufacturers to choose the right platform, services and security levels to from which to build their devices. Since each layer can be built independently ,as long as it conforms to the standard interface, this architecture enables the freedom and flexibility for building security features to comprise a trustworthy device.

ODVA's role

ODVA is well positioned to drive the standardization of a security solution for an industrial automation network. ODVA is actively working on defining the next generation secure CIP protocol along with provisions on how to enroll and manage secure identities. ODVA should consider expanding their scope to also include:

- Continue current activity of evolving secure CIP protocol, for example,
  - Better integration secure CIP with Certificate Enrollment and Secure Identity Management process
  - Protect legacy CIP devices with a secure CIP gateway or proxy
- Define security levels and profiles for industrial endpoint, including
  - Functional requirement for each security level
  - Deployment use cases and threat modeling for each security level
  - Guidelines to manufacturers on the security levels required for different industrial operations, and how to map these requirements to purchase decisions

    - Recommendation to customers on how to install and deploy industrial devices/machines with different security levels
- Define and standardize the reference architecture of secure industrial endpoint, including
    - Functional requirement for each security layer
    - APIs and data flow between different layers
- Define guidelines on network infrastructure and networking devices, including
    - Network-based attack vector and threat modeling
    - Network setup and topologies for securing industrial network
    - Recommendation on how to install and deploy network-based security solutions
- Define compliance standards and inter-operability requirements, including
    - Compliance requirements for each security level
    - Compliance requirements for different deployment use cases
    - Testing procedures for compliance tests

References (optional)

[1] U.S. CERT, ICS-CERT Year in Review 2014 Report, https://ics-cert.us-cert.gov/Year-Review-2014
[2] U.S. CERT, ICS-CERT Year in Review 2013 Report, https://ics-cert.us-cert.gov/ICS-CERT-Year-Review-2013
[3] U.S. CERT, ICS-CERT Year in Review 2012 Report, https://ics-cert.us-cert.gov/ICS-CERT-Year-Review-2012
[4] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, February 2014, http://nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[5] Sanjay B. Joshi, Jeffrey S. Smith (1994) *Computer Control of Flexible Manufacturing Systems*. p. 7
[6] NIST, NIST SP 800-64 revision 2, October 2008, http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
[7] Trusted Computing Group, TPM 2.0, http://www.trustedcomputinggroup.org/developers/trusted_platform_module
[8] NIST, NIST SP 800-90A, January 2012, http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf