Information Security Practices for Industrial Control Systems

Kevin Sullivan
Microsoft
kevsull@microsoft.com

Abstract

Industrial control systems have some unique operational requirements but the computing technology has much in common with general purpose IT systems. Information security practices that have been developed first for IT systems have application to industrial control systems as well. This paper proposes five such practices be applied to industrial control systems.

1. Introduction

Critical infrastructures such as energy, water and chemical extensively use IT systems to manage production processes and ultimately deliver services such as electric power and drinking water to customers. These systems include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems, collectively referred to here as Industrial Control Systems (ICS). Today's ICS employ much of the same technology that is used in business information systems. The systems are generally built on operating systems such as Microsoft Windows® or a commercial distribution of Linux. This commonality extends up to the database and systems management layers as well. Communication between control systems has historically relied on proprietary protocols but is now starting to make use of TCP/IP, the standard protocol of internet communications.

Industrial Control Systems are no longer niche systems using propriety software and hidden behind locked doors. They are making using of the same technology as PCs and sometimes connected to public networks. Many of the security practices used for IT systems apply to ICS and can be used to efficiently secure these systems with minimal additional development.

2. Attack surface reduction

A system's attack surface refers to the system's exposure to attack resulting from functionality including installed programs, ports and services. One of the most practical means to reduce a systems attack surface is to configure the system to the minimum level of functionality required for a task. Reducing a system's attack surface has the potential to reduce hardware requirements, increase performance, alleviate compliance concerns and remove avenues for attack. There are several IT practices that will help to reduce the attack surface of ICS.

Configuration management, the process of selecting, deploying and maintaining the configuration items of a given IT system, allows administrators to reduce the attack surface across multiple assets in a systematic way. A simple way to accomplish this is through the use of configuration templates. Configuration templates are a representation of desired settings that can be applied to and maintained on an asset. More advanced organizations may employ a configuration management data base (CMDB) to manage the entire configuration lifecycle from planning through verification. The North American Electric Reliability Corporation's cyber security standards require unnecessary ports and services to be disabled or removed to reduce the attack surface of critical cyber assets. [1] A configuration management process would help the organization to manage these ports and services in a repeatable and documentable fashion.

Any effort to secure industrial control systems must address legacy systems. These systems typically have a lifecycle much longer than that of traditional IT systems. Software and devices are often deployed beyond their supported lifespan and lack protections against threats that did not exist when they were initially designed. Like IT systems, ICS must plan for both intended and unintended applications to evolve over the useful lifespan of the system. While upgradability is most desirable to keep pace with technological development and protect against

evolving threats other interim solutions may be appropriate for use in cyber physical systems, such as virtualization.

Virtualization allows for a single computing device to host multiple instances of an operating system or an application. In the case of ICS, virtualization could allow a legacy operating system or application to be hosted by a more recent host operating system providing protection against current threats as well as the ability to run on up to date hardware. This reduces the attack surface as the modern host operating system can better limit access to the system and provide additional protections.

3. Network segmentation

Physical separation of computers and networks, once considered the ultimate security measure, has fallen to business and technology pressures. Many of today's systems derive their power and utility from connections to multiple systems including sensors and databases. Efforts to reduce cost and increase visibility have resulted in highly connected systems within and between enterprises. While this connectivity does present security concerns there are promising technologies and security controls that can help to mitigate these threats.

Network controls can be most effective when the administrators can define the acceptable traffic patterns of the system. In most corporate IT environments this is not feasible due to the wide variety of business tasks and the loss of revenue or productivity if legitimate network traffic is inadvertently blocked. The limited set of functionality and network traffic used by control systems offers an opportunity for administrators to create a white list of acceptable traffic patterns and block all others.

While physical network segmentation remains available, consider the viable options for policy based segmentation and protection of network communications. Policy based network segmentation allows an organization to set policies to control how systems communicate over the network without additional network devices. The use of policy based controls on a single network reduces cost and complexity while restricting unauthorized access and protecting systems from attack.

A common technology used to achieve this segmentation is Internet Protocol Security (IPSec). IPSec authenticates and optionally encrypts the traffic between hosts or gateways. Encryption can be a concern for ICS because of the performance impacts on a real time system. It is important to note that with IPSec encryption is optional. Integrity and authentication can be provided without encrypting the network traffic. Network access protection (NAP) provides the ability to segment or restrict network access based on a set of requirements placed upon the system. NAP can be used to limit the network access of a system that is not compliant with a particular policy or is infected with malware. These policy based tools allow ICS to be networked together with great management capabilities and reduced risk of exposure or attack.

4. Authentication and access control

As systems become more connected and subject to greater regulations it is critical to control who is able to access the system. Authentication is generally performed with a user name and password, or less in some legacy systems. Passwords suffer from several vulnerabilities including interception and cracking. Once an adversary has access to a user or system password they can act as that user or system. This problem has been mitigated by two-factor authentication in which a user is required to provide something they have (a smart card or similar device) and something they know (a PIN). Caution should be taken in applying this to cyber physical systems without appropriate consideration of human factors. When two-factor authentication cannot be used, the system should require complex passwords that are changed on a regular basis.

Excessive privileges assigned to users, programs, or other systems can leave a system in a vulnerable state. The seminal paper by Saltzer and Schroeder makes the case for least privilege stating that "Every program and every user of the system should operate using the least set of privileges necessary to complete the job." [2] This is an important concept to be carried into cyber physical systems which may provide multiple functions and allow many users to access the system. The configuration and access control functions should restrict the program or user to the minimal set of privileges required. This can be accomplished through role based access control to facilitate provisioning. In a critical cyber physical system this can be valuable in allowing a user to quickly gain proper system access for the role they are performing, especially in the case of an emergency. New developments in identity management allow for the use of claims to represent attributes of a user or system for identity and access decisions. [3] These claims are separate from the authentication mechanisms allowing for federation between systems and organizations.

5. Secure development

Operating systems, once the main target of attackers, have benefited from large investments in secure development. The attackers, however, have not relented and shifted their focus to the application layer where a diverse set of programs offer an uneven security terrain with new possibilities for attack. Over the second half of 2008, operating system vulnerabilities represented just 8.8% of all disclosed vulnerabilities. The remainder consisted of browser and other application vulnerabilities. [4]

Secure development practices are a critical requirement of cyber physical systems due to the potential impact on national and economic security and public safety. Organizations developing software for cyber physical systems need to implement a process for designing, developing and delivering quality software with minimal vulnerabilities. These processes go beyond engineering activities to include design, training and accountability.

A key component of secure development is threat modeling. Threat modeling is the process of assessing and documenting the security risks associated with an application, system, or network. [5] This process is not limited to IT assets; the process can be used to examine the threats to a physical infrastructure as well. By examining the cyber and physical assets and their relationships, one can understand potential weaknesses or avenues for attack and use this data to plan for mitigations.

Throughout the development phase there are many generally accepted practices used by leading software companies to reduce the number and severity of vulnerabilities in a product. Attack surface reduction, mentioned above in the system context, can also be applied to secure development. Limiting code that runs by default and restricting access to code help to reduce the likelihood of a severe vulnerability. [6] Other practices include minimizing the use of unsafe functions, using code analysis tools and validation of input and output. [7] These development practices, combined with threat modeling and training provide the foundation for secure development processes in any organization.

6. Security response and updating

Secure development practices have reduced the number and severity of vulnerabilities but not eliminated them. For the simple fact that new threats will be discovered after a product's release, there will always be a need to respond to vulnerabilities in software. Software vendors must plan for the inevitability of responding to a vulnerability and providing an update to customers. Customers must also prepare to receive, evaluate and deploy these updates.

A vendor's vulnerability response process begins by being prepared to receive and acknowledge vulnerability reports. Each report should be investigated to determine the impact and full scope including other products and similar vulnerabilities. Once the scope and impact is understood, the vendor produces a comprehensive update followed by rigorous testing to ensure the vulnerability is fully addressed and there are no unintended effects on the functionality of the system. At this point, the vendor communicates authoritatively to the affected customers with information regarding the scope and severity of the issue, potential mitigations and workarounds and the availability of the update.

Upon receiving notification of an available update the customer should assess the applicability of the update to their environment and plan to deploy the update in accordance with their risk management program. The work to reduce the attack surface of the system helps to reduce the number of updates that need to be deployed. The time between the availability of an update and an exploit continues to decrease necessitating rapid evaluation and deployment of updates to reduce risk to the infrastructure. [4]

The security updates released by Microsoft each month represent just a fraction of the total effort required for update management. However it is important not to overlook network devices, databases and applications. [8] The Slammer worm of 2003 demonstrated the importance of software inventory and holistic updating. Slammer exploited a vulnerability in SQL server that had been patched 6 months earlier. [9] The reason that the worm spread so quickly was that many computers had portions of the Microsoft SQL Server® product installed without being aware. An examination of the system's attack surface and effective configuration management would have revealed the installed programs and informed the update management process.

Vendors and operators of ICS must react swiftly to reports of vulnerabilities in their products. Sound response processes by the vendor will help to ensure that the issue is fully eradicated and comprehensively tested. Operators should plan to evaluate and deploy updates as part of an overall risk management program, taking into account the other practices indicated in this paper which provide defense in depth.

7. Conclusion

With technological advances such as the smart grid, ICS continue to evolve into full IT systems with all the benefits and risks. This evolution provides an

opportunity to standardize security practices across environments. Owners and operators of ICS can employ attack surface reduction and network segmentation with the systems they already own. Authentication and access control are as much about process and policy as about technology. Secure development and response are a cooperative process between vendors and operators in which they set requirements, build response processes and manage risk throughout the environment.

The security practices outlined above have been effectively used by IT systems to manage risk to an acceptable level. Undoubtedly, cyber physical systems have unique operating requirements that must be taken into account, however these practices should not be ignored nor should security controls be reinvented for ICS.

8. References

[1] North American Electric Reliability Corporation (NERC). CIP Standard. [Online]. http://www.nerc.com/files/CIP-007-2.pdf

[2] J.H. Saltzer and M.D. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, vol. 63, no. 9, September 1975.

[3] Kim Cameron. (2005, May) Identity Weblog. [Online]. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[4] Microsoft Corporation. (Microsoft Security Intelligence Report volume 6 (July - December 2008), April) Security Intelligence Report. [Online]. http://www.microsoft.com/sir

[5] Frank Swidersky and Window Snyder, *Threat Modeling*. Redmond, USA: Microsoft Press, 2004.

[6] Michael Howard. (2004, November) Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users. [Online]. http://msdn.microsoft.com/en-us/magazine/cc163882.aspx

[7] SAFECode. (2008, April) Fundemental Practices for Secure Software Development. [Online]. http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf

[8] Dennis Brandl, "'DONA' forget about security," *Control Engineering*, December 2008.

[9] Microsoft. (2002, July) Microsoft Security Bulletin MS02-039: Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875). [Online]. http://www.microsoft.com/technet/security/bulletin/MS02-039.mspx