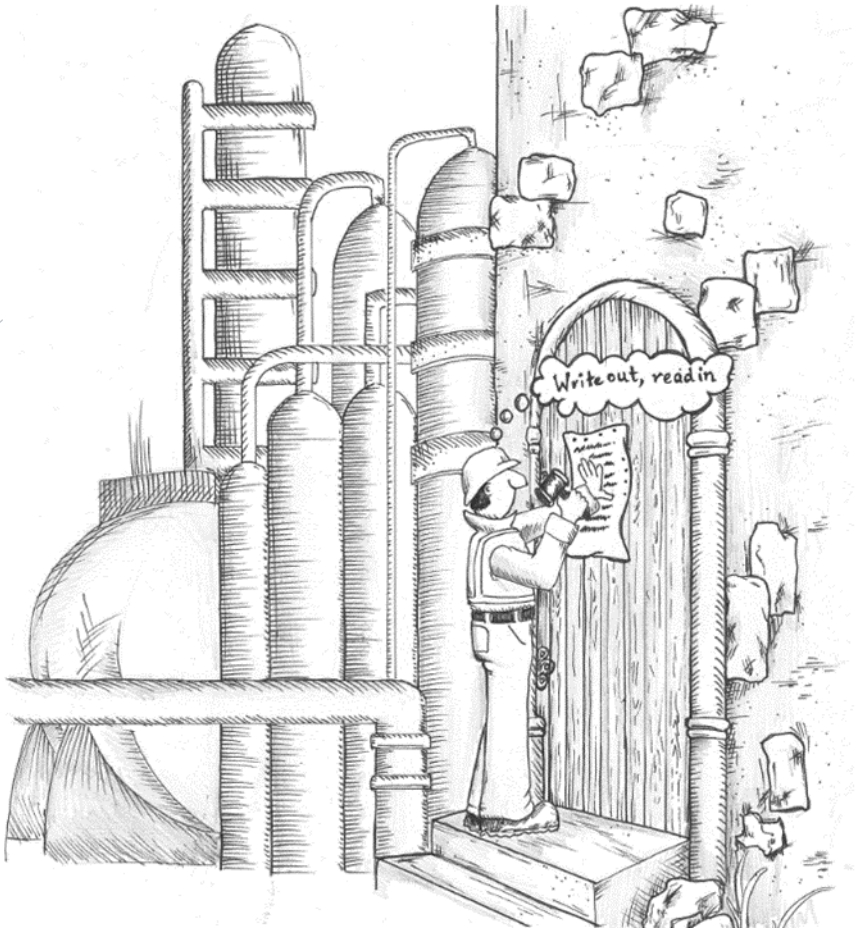
10/19/2020

Control Systems Segmentation

“Write Out, Read In” Security Model



Preface

A "Write Out, read in" security model is not a new concept; it is existentially the way we communicate; it is how we tell stories (writing out) and how we learn (reading in) applied to information systems. There are 2.5 million years of evolutionary history, and at least the same amount of empirical evidence of validating this model. Fundamentally, just like in life, we walk a thin line and narrow edge, trying to balance security and business need[1]. We are lucky when things are not degenerating into chaos or far too much order[1]. This position paper attempts to find that balance by modifying how information systems communicate by mimicking the natural way of communicating. The axioms outlined in this paper are the rules that help prevent the corruption of information when "written out or read in".

Problem Statement

Due to recent events, the current Purdue[2] model based segmentation model doesn't adequately address both network and application segmentation. Also, the current strategy focuses on process control systems as opposed to all industrial control devices. This creates potentially exploitable vulnerability paths into the various industrial systems. As such, one must modernize the segmentation model to address the dichotomy of meeting business needs and maintaining the security of industrial controls assets.

Strategy

The defense-in-depth cybersecurity strategy implements a risk-based approach for securing assets. Part of that strategy is to have continuous improvement. As the threat landscape changes, so must "we." The focus of this strategy is maintaining the integrity and availability of industrial control systems.

Tactics

Engage a working group of subject matter experts and key stakeholders to establish a framework that incorporates updated models, network designs, application data flows, current technology, and industry practices to define how control systems implement segmentation controls.

Guiding Principles

- Network segmentation should allow for safe and secure data exchange between the ICS network and business network or other partner networks.
- Compromise of one ICS network should not result in a consequential compromise of any other not directly connected ICS network
- Provide Zero-Day protection and resilience to viruses, worms, crimeware, and cryptoware outbreaks affecting corporate or other networks.

It is not

This document is not a comprehensive security strategy for ICS, nor an alternative to the Purdue model. Instead, it attempts to provide a secure method for advancing the network boundary controls between the ICS networks and the rest of the "universe" while offering better support for the new business needs born from Digital Transformation. Considerations for managing the introduction of portable media and external tools (ICS programming laptops) must be accounted for to reduce the likelihood that these controls are bypassed.

Focus

Foicus of this paper is to improve security of Industrial control networks by paying attention to how one enables communication patterns between Indutrial control netqworks and the rest of the world. That said the tenants expressed in this apaer are true and valid for any other environment.

---

[1] Jordan Petrerson "on breaking rules"

[2] **Purdue Enterprise Reference Architecture** (**PERA**) model by ISA-99 and used as a concept model for ICS network segmentation. It is an industry adopted reference model that shows the interconnections and interdependencies of all the main components of a typical ICS."

Tools and Techniques

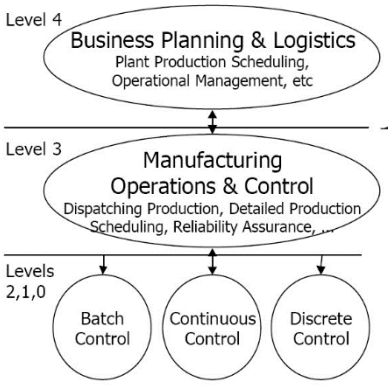
This strategy does not require the implementation of new tools; instead, it focuses on fortifying existing network segmentation by enforcing data flows as the data is written out and read in from the more security level and by scrutinizing these data flows to interrupt—potential command and control channels originating in lower security zones.

Last Stand Protocol

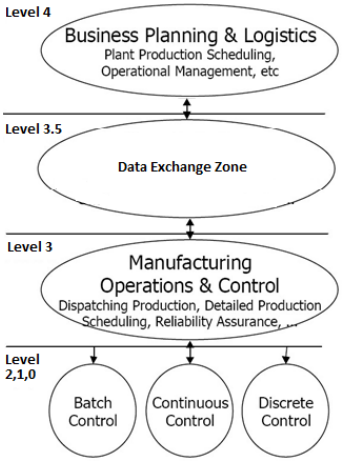
Following this strategy will ensure that while consuming services outside of the secure zone, safety, and reliable operation of this zone will be maintained even if the communication across the security zone boundary must be suspended.

Current architecture

Current ICS segmentation most commonly is based on a 20-year-old Purdue Enterprise architecture Reference model[3] This architecture reference model was focused on enterprise controls and process management. Its objective was to provide support for a reliable operating environment for industrial control networks[4]. Still, in time it became the de facto accepted security model for the modern ICS network architecture.

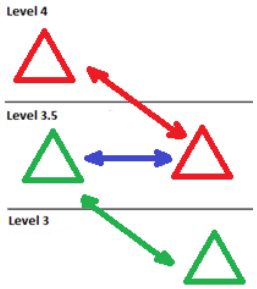


It might be useful to notice that the Purdue model's original release did not include Level 3.5. It is a later addition to the model as an additional security layer by using it as a communication intermediary between Level 3 and level 4 systems. This approach's effectiveness to protect against modern threats is low if the data is not inspected for malicious content by the intermediary or if the communication channel is not interrupted by protocol translation.



[3] The Purdue Enterprise Reference Architecture and Methodology
[4] Industry had to overcome limitations of the bus network

While this model is still relevant, arguably, it falls short in addressing changes to the threat landscape because:

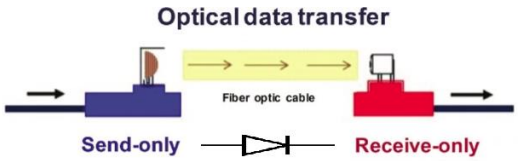


- It allows collocation of level 4 and level 3 system within Level 3.5
- It relies on authentication domain segmentation to maintain segmentation between the L4 and L3 systems
- It allows bidirectional communication paths for system management and functionality within the L3.5

This is resulting in an architectural weakness that could be misused by a nefarious actor or malicious agent to move laterally across security boundaries; especially if the hosts collocated in the level 3.5 zone are vulnerable to unauthenticated, remote code execution attacks (Zerologon, Bluekeep, EternalBlue, Petya, non-Petya…).

The challenge is that the Purdue model, while advancing security of the industrial control systems by managing communications paths between different security zones,[5] does not address the security of the communications themselves.[6]

Historically high-security environments resolved this architecture weakness by using data diodes that allowed data transfers only from a higher security level to a lower security level.

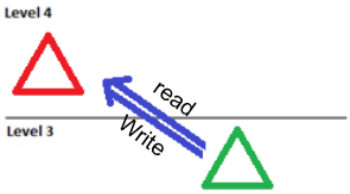


The Data Diode approach to allow communication between secure and insecure zones is a preferred communication method when it is essential to assure that malicious code will not propagate across the security zone boundaries. Unfortunately, this approach's weakness is that it only allows communication in one direction and is not well suited for the today's ICS network communication needs that require exchanging data between the business and ICS networks.

"Write Out, Read In" Model

The premise of "Write Out and Read In" is similar to the assumptions of both the Biba[7] security model and the Bell-LaPadua[8] models, which, while popular in the military, have been found unusable in the business space due to the very narrow focus of each model[9].

The notion that data can be "written out[10] and read in" could advance industrial control security if combined with the Purdue model to address vulnerabilities in the communication path while streamlining communications and reducing complexity by removing the need for a Level 3.5[11].



[5] by limiting communication path
[6] Defines plumbing but not what is in the pipes
[7] Biba Security Model
[8] Bell-LaPadula model
[9] data integrity or data confidentiality respectively
[10] NIST 800-82 p20
[11] Some conditions, such as third party B2B connection might need intermediary system in Level 3.5 to provide additional security

"Write Out and Read In" security model assumes that communication will always be initiated from a more secure zone (ICS) into lower security zone (business) and that the host in the high-security zone will act as the client to the server and that the used communication protocols (conduits) in are not vulnerable to attacks or compromise.

"WORI" axioms[12]

Data Flows & Protocol limitation

- All communications between a more secure zone and a less secure zone are initiated from the higher security zone.
- All communications across security boundaries must follow the least privileged principle with sources and destinations defined using IP addresses or Fully Qualified Domain Names and destination ports.
- The host in the higher security zone must act as the client[13] to the server in the lesser security zone.
- Communication protocols that support reverse shell/reverse management functions across security zones[14] are prohibited / not allowed.
- Out-of-band communication paths are recommended but are not required.
- VPN tunnels that bridge the same level security zones over a less secure zone is permitted. This is comparable to using metal conduits to protect physical cabling outside of the secure plant perimeter.
- Access to the Internet or other cloud services is not permitted for any protocols.
- Preference is given to secure protocols within and across security zones (i.e., Secure LDAP, SSH, SFTP).
- Vulnerable protocols and related traffic must not traverse security zones (e.g., NTML, RCP, SMB, NetBIOS, rSSH…)
- Protocols that do not require acknowledgment and protocol substitutions across the security zone boundary are encouraged (e.g., SMB > SFTP > SMB or OPC to MQTT).
- Be wary of the use of WebSockets as they could bypass your data flow (firewall) controls.
- Process control systems for plant operations must not rely on any external interfaces or systems to maintain safe and reliable real-time facility operations.
- Prevent protocol tunneling[15]. Protocol port numbers must not be trusted; confirm the communication requirements by validating protocols – do not assume port 23 is using the Telnet protocol.
- Consider using application-aware[16] firewall rules for additional protocol integrity checks.
- Introduce mechanisms to prevent or disrupt command and control mehanisms[17].

Intrusion Protection/Detection and Unified Threat Management Systems

Intrusion protection and detection systems are useful, but their capabilities are limited as network boundary controls. This is because the use of encrypted protocols and because many of the modern attacks by skilled advisories are not necessarily malicious in their appearance, but they are instead misuses or abuses of valid system functions. The use of IPS and IDS can be beneficial if they are in place to protect the boundary and their limitations are understood and mitigated by layers of controls.

Internet Isolation

The fundamental principle of the WORI model is that secure levels must be isolated from the Internet.

- Use jump boxes and remote desktop technology residing outside of the secure area for external access.
- Only allow ports, protocols, and IP addresses through the firewall that are explicitly required to perform a business function. Depreciated and/or insecure protocols are not allowed, for example SSL and early versions of TLS.

Level 3.5 DMZ

Historically, Level 3.5 DMZ has been used to exchange data between different security zones. Its value as a security control, while diminished, still exists, especially when data needs to be exchanged with external third-parties, assuming they are a bit

---

[12] Devil is in the details
[13] Client Server Architecture
[14] Reverse Shells Enable Attackers to Operate from Your Network Use web sockets to bypass Firewalls
[15] Detecting and Preventing Unauthorized Outbound Traffic
[16] What is application visibility and control?
[17] Disrupting the Cyber Kill Chain

more[18] than a data stop. For Level 3.5 DMZ to be a reasonable security control, it must interrupt command and control channels while allowing data flow. For example, use protocol "conversion," That is, going from SMB to FTP, or OPC to MQTT, or use immutable Linux [19] clients to fetch files from a MS-Windows platform.

- Data stops in Level 3.5 DMZ are not required unless data is inspected for malicious content, to complete protocol conversion, or support data leak detection and prevention (DLP).
- Cohabitation of systems across security zones or authentication zones within the same logical Level 3.5 DMZ is not permitted.

Leveraged Services

The placement of a management plane[20] for ICS infrastructure components was never a big issue, as it is always placed in the most secure zone. With digital transformation, cloud, and budgetary pressures to consolidate, leverage, and innovate ICS boundaries the management plane needs to be extended to encompass or include new components. For example, to leverage a single Antivirus Management Console across multiple distinctly separate ICS Level 3 environments, ensure that the Antivirus Management Console is secured to the same rigor as the most secure zone where AV agents report back. In an ideal world, ICS networks would be self-contained.

- If leveraged services are used, either on-prem or cloud, ensure that safe and reliable operation is maintained even if these leveraged services become unavailable.
- The use of leveraged infrastructure across multiple ICS networks is permitted, assuming the management plane is secured to the highest security zone it supports.
- System / Application management functions (management plane) must be protected in the same manner as the highest security zone they manage.
- If infrastructure components are provided via out-of-band networks, such as SANs, fiber channel storage, or virtual environments, those networks and associated management plane components must be secured at the same level as the systems they serve.

Name resolution

Domain Name System (DNS) is a ubiquitous service that is often overlooked as a potential conduit to the Internet from the ICS network. This is because its default setup is to forward domain name lookups to the Internet. This is not an issue if you block DNS (UDP/TCP 53) traffic at the firewall. But if you allowed it through your firewall, you have likely allowed it to perform Internet name lookups, thus opening a slow but effective command and control channel[21] from the ICS network to the worldwide Internet.

- When the resolution of external resources is needed, use conditional DNS forwarding or host files.
- When conditional DNS forwarding is used, configure the DNS forwarded to resolve the needed name.
- Do not allow unrestricted ICMP and DNS to the Internet as these can be misused for command and control or data exfiltration.
- The use of localhost files is permitted for name resolution.

Authentication and Data Security

Historically we have used authentication domainsas additional boundary control between two levels, and this allowed the colocation of assets belonging to two different Active Directory[22] domains. In the context of the ICS network, this is no longer acceptable due to numerous vulnerabilities that allowed unauthenticated code execution, creating a vulnerable operating environment.

- Authentication domains should be contained within their respective zone.

---

[18] NIST 800-52 p19

[19] My favorite superpower

[20] In computer networking, the management plane of a networking device is the element of a system that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system

[21] What is DNS tunneling?

[22] Active Directory

- Do not use Role Based Access Controls between security zones as a method to limit communications. Instead use RBAC to limit authorized access within an individual security zone.[23]
- Data security controls should be commensurate with the risk and should be secured according to the data impact, regardless of the security zones in which it resides.
- Applications must reside where they are consumed. Applications targeting business users should reside on the business network.
- The programming code that is being read must be validated if it can be executed (SQL, scripts, models, containers, VMs).

Remote Access

From a cybersecurity perspective, all-access outside of the ICS security zone should be considered remote access. All remote requires strong authentication that could consist of conditional access or multifactor authentication.

- Users accessing the ICS network remotely should be authenticated by the zone they are trying to access.
- The firewall should authenticate all remote access into ICS networks before the remote desktop, or remote shell protocols are exposed through the firewalls.[24] IE: Use client auth rules on the firewall that temporarily allow remote access connections as opposed to a static rule that would allow remote access at any time.
- Multi-factor[25] authentication is required for interactive remote access sessions.
- Use of HDMI to USB adapters and desktop sharing sessions for view only functions are permitted when supervised/observed.
- Hardened and properly patched (bastion) host[26] should be used as a jump station to reduce zero-day exploit[27] risks.
- Disable file sharing, drive mapping, and clipboard features in remote desktop accordingly Organizational risk apatite should drive these choices.

Industrial Internet of Things (IIoT)[28]

As the name implies, a fundamental feature of IIoT is the Internet. It is an essential component of a complex multilayer system[29] that fundamentally does not run without access to Internet-based resources. Thus, cybersecurity considerations will be complex.

- A new segmented (i.e., firewalled) IIoT network should be established for endpoint devices.
- Data produced by IIoT must not be elemental for safe and reliable plant operation.
- Consider the criticality of the data produced or function provided by IIoT and implement security controls that are commensurate with that criticality, across all layers[30] of IIoT architecture.
- Sensors designed to operate locally and forward data outside (i.e., outbound only) of the security zone can follow exiting standards.

Edge Computing[31]

It is a new moniker for processing data close to where it is produced, in near-real-time. It typically consists of a third-party managed computing device (e.g., industrial PC type hardware) deployed on the ICS network boundary with network connectivity provisioned by the vendor.

- Depending on the trust level associated with the service[32] (dedicated or shared), new segmented (firewalled) edge computing network might need to be established for edge devices
- The edge computing management plane should be configured in a manner consistent with the function of the service or function it provides.

---

[23] Access Control Implementation in ICS - Infosec Resources
[24] Wikipedia: Bluekeep
[25] Multi-factor authentication
[26] Wikipedia: Jump server
[27] Wikipedia: Zero day
[28] Wikipedia: IIoT
[29] The basics of IoT
[30] Evolving the Modular Layered Architecture in Digital Innovation
[31] Wikipedia: Edge Computing
[32] Secure Sockets Layer (SSL)

- When edge computing is used for plant operation, the solution should be capable of reliable and safe operation if disconnected from the management plane.

Containers[33]

Containers are an exciting but complex technology with a promise of transforming how to do IT[34]. A container is a virtual machine, with container host providing network translation, network filtering, and routing services. Some network security aspects to consider include:

- Every time a container is run, it will try to download an up-to-date version from the configured conatainer store, with the Internet as the default. The image of an existing container must be run to prevent this behavior or run a local container store .
- If container stores, orchestration, or management services are used, ensure that these are configured in a manner that is consistent with the security level they are running in.
- Depending on business security requirements, some attention might need to be given to these services' configuration.
- If containers are used for plant operation, they should be capable of reliable and safe operation if disconnected from the management plane.
- Promoting a new container into the ICS environment uses the same change control processes as when introducing a new device onto the network.

Security Event Monitoring

WORI model allows for the Security Event monitoring be simplified and streamlined on focusing on the outbound traffic and any remote access functions.

- Syslog protocol while in clear text it is a low risk protocol and it is is a preferred protocol to forward logs to log repository
- Use syslog forwarders to collect and forward logs when working with multiple hosts
- Focus monitoring on outbound traffic. High volume of paket denies at the firewall is a good indicator of a misconfiguration or malware attemting to “call home”.

Summary

A modern defense in depth strategy is required to safeguard industrial networks appropriately. A vital part of that strategy is a continuous improvement cycle of review and adapt. Recent events require the next cybersecurity iteration to adopt new tactics. Foundational to these new tactics is to adopt certain principles. The ‘Write Out, Read In’ model lays out these principals. By configuring the boundary between industrial control and external networks in the manner prescribed in this document, the overall cybersecurity posture of the industrial systems will increase; network and application complexity is reduced – thereby reducing the total cost of ownership; while improving the end-user experience.

WORI Benefits

With a recognition that this security model is departing from the traditional Purdue model by allowing direct, but restricted communication path from the Level 3 to Level 4 or cloud, it has the potential to:

- advance security for industrial control environments by:
    - enhancing isolation of control networks from *the business network*
    - simplifying firewall management and audit
    - preventing the potential of lateral propagation of threats from the less secure to the more secure zone
    - streamlining security event monitoring and cyber incident response
- improve the operational readiness through:
    - simplifying network and security architecture

[33] What are containers
[34] The spark for the container revolution

- reducing points of failure and establishing better recovery time objectives
- enhancing system performance through “fewer stops.”
- improving user experience
- reducing cross security boundary jumps
- data resides where the data is consumed
- reducing management overhead
- effecting a lower total cost of ownership (TCO).
- Enhancing support for IIoT and cloud technologies
- OT in full control over egress and ingress of data

Additional readings

- Building security to achieve engineering and business requirements
- Secure Architecture for Industrial Control Systems
- How threat actors are using SMB vulnerabilities
- Cyber-security in Industrial Control Systems
- The Untold Story of NotPetya
- Bell–LaPadula model
- Assuring Industrial Control System (ICS) Cyber Security by Joe Weiss PE
- Biba Model7