D3B3sh>5!>>o

SOFTPROM | ACALVIO

Acalvio ShadowPlex in OT/ICS Environments

Unifying Risk Management for IT/OT Convergence

Table of Contents

1. Introduction – The Risk Management Challenge in OT Environments 2
2. Background – The OT Environment & Purdue Model 2
3. MITRE ATT&CK for ICS 4
4. Deception-Based Risk-Management for OT/ICS and MITRE Shield 4
5. Acalvio ShadowPlex: Solution Strategy 5
6. Acalvio ShadowPlex: Solution Capabilities 5
6.1. Low interaction ports on decoys 5
6.2. Custom web decoys 6
6.3. Golden image virtualized decoys 6
6.4. Breadcrumbs 7
7. ShadowPlex OT/ICS Deployment Model 7
8. Summary 8

List of Figures

Figure 1. The Purdue reference model 3
Figure 2. Decoys are easily customized to match ICS device port characteristics 6
Figure 3. Custom decoy for Honeywell Niagara supervisor, created using golden image upload 6

1. Introduction – The Risk Management Challenge in OT Environments

Enterprises and regulated industries are well aware that their risk management strategy must include cybersecurity for OT (Operational Technology) environments. These organizations know that the combination of high potential impact to safety and core operations and limited focus on IT security in industrial environments translates into substantial risk. Unfortunately, implementing security controls in such facilities is difficult for a number of reasons, including but not limited to:

- Concerns that security controls will impact production availability.
- Lack of understanding of OT systems and protocols by IT Security staff
- Onerous change management restrictions
- The inability to deploy many types of security solutions on OT systems.

This application note will describe how Acalvio ShadowPlex can be used for threat detection and visibility to effectively manage risk in OT environments.

2. Background – The OT Environment & Purdue Model

OT networks (also known as Industrial Control System or ICS networks) are dedicated to monitoring and controlling physical plant equipment, for both operational and safety purposes. As such, they are populated with dedicated hardware for specific tasks (e.g. Controllers/PLCs, Engineering workstations and HMI terminals) from specialized vendors (e.g. Rockwell, Siemens, Honeywell). The controllers are in turn connected to the physical sensors, actuators, etc. within the plant. Following a multi-decade transition, these networks are largely IP-based, but make heavy use of proprietary protocols above the IP layer.

OT networks should always be segmented from enterprise networks via firewalls. The OT devices on the network tend to be left in place for years or even decades. The age and proprietary nature of such devices means that equipment that can't be patched and may fail even if simply scanned by a benign analysis tool. Documentation of the OT environment may also be lacking, and in some cases a level of indifference to security by plant operations has resulted in a "Better if we just don't touch it." mindset.

In an attempt to promote better, more consistent OT security, a university-industry partnership created the Purdue Reference Model. The model is a structured approach for organizing and segmenting OT networks and defines five network layers (numbered 0 to 4) into which OT devices should be placed:

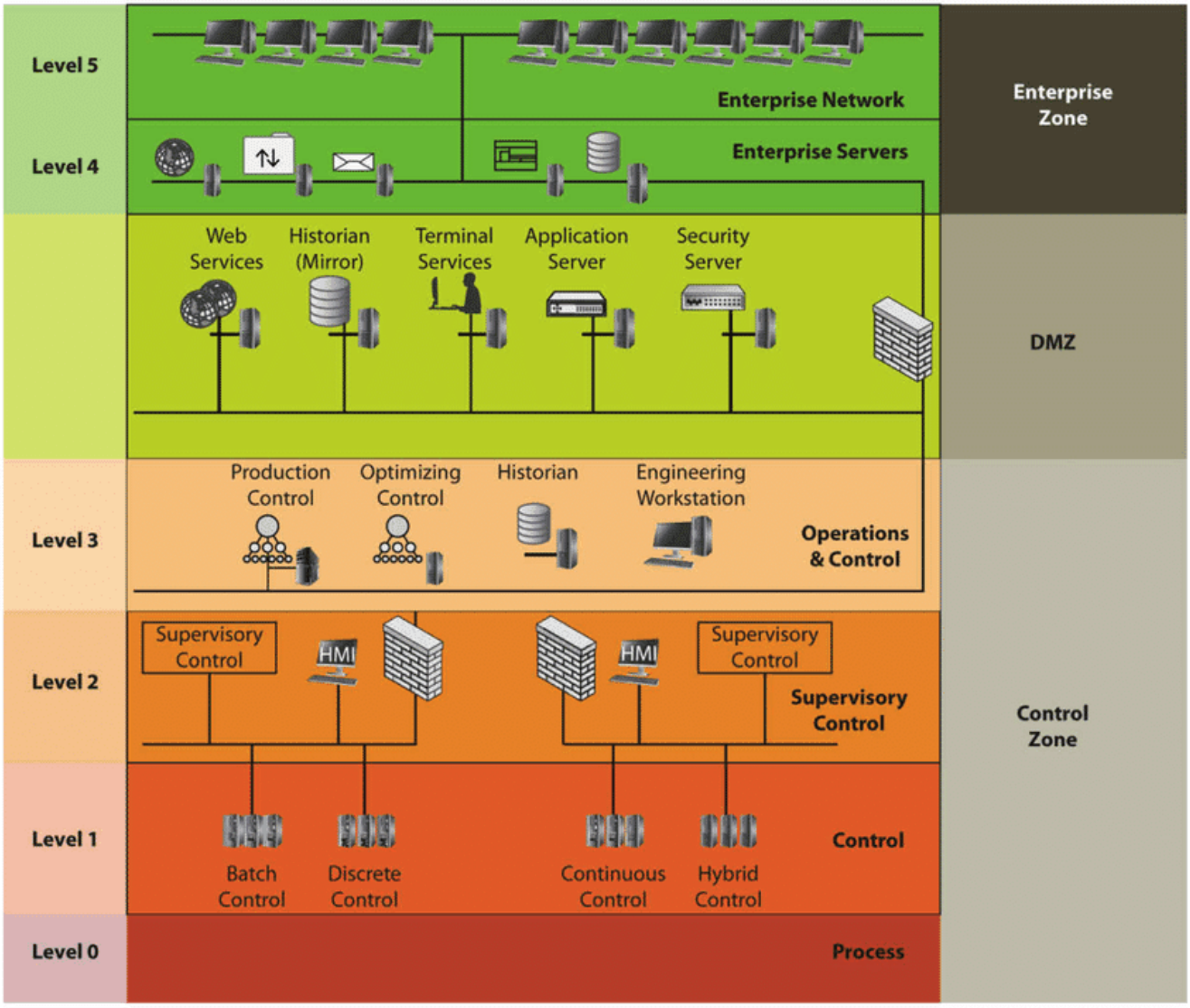

Figure 1. The Purdue reference model

The Purdue model is nothing like a detailed IT security control framework such as PCI-DSS or NIST 800-53. It is simply a model for network segmentation. However, a key principle of the model is that direct connections between the OT (Layers 0-3) and enterprise (Layer 4) networks is prohibited. This is why a Layer 3.5 is typically established as a DMZ between enterprise and OT networks. The DMZ is particularly important, as real-world experience has shown that most OT attacks start in the Enterprise IT domain and then propagate into the OT network across the IT/OT network boundary.

OT/ICS equipment is differentiated from IoT devices in that OT is dedicated to plant operations and safety. IoT devices such as security cameras or building environmental control are deployed more broadly, and are often placed on networks under the control of enterprise IT. This whitepaper will focus on OT risk management.

3. MITRE ATT&CK for ICS

IT Security professionals will be familiar with the MITRE ATT&CK for Enterprise framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. However, actual attacks have shown that OT environments are vulnerable and exploited in ways not covered by the enterprise framework. Therefore, in 2020 MITRE released a supplementary document specific to industrial control systems. "ATT&CK for Industrial Control Systems" adds tactics, techniques, and adversarial groups relevant to OT environments and equipment. Since OT networks contain a mix of IT (Windows or Linux based) and OT devices, both the Enterprise and ICS ATT&CK frameworks must be considered when planning risk-management strategies in the OT space.

> *"ATT&CK for ICS focuses on adversaries who have a primary goal of disrupting an industrial control process, destroying property or causing temporary or permanent harm or death to humans by attacking industrial control systems."*
> MITRE, 2020

4. Deception-Based Risk-Management for OT/ICS and MITRE Shield

As noted previously, IT Security staff have a difficult challenge in reducing risk in OT environments. Fortunately, Deception solutions are particularly well-suited to meeting this challenge. This is because they have a number of attributes that make them more palatable and less risky than alternative technologies.

Deception Attribute	Benefit
Independence	Ease of Deployment: Solution independent of production systems with no agents or in-line devices.
No production impact	Low Risk: No possible production impact from active scanning
Coverage	Supports IT and OT environments; bridges IT / ICS cross-domain gap
Visibility	Provides detailed network intelligence, and investigative forensics

The value of deception-based active defense has been recognized by MITRE, as manifested in their Shield knowledge base, which was released in mid-2020. Unlike ATT&CK for Enterprise and ICS, MITRE Shield focuses on the strategies of defenders, not attackers. Based on MITRE's own adversary engagement operations spanning over a decade, Shield is organized into defensive principles (Tactics) and more specific Techniques and Procedures and supports a cross-mapping to the ATT&CK framework.

> *"Carefully constructed deception systems are often indistinguishable from production systems and can serve as high-fidelity detection systems. Shield techniques can include deceptions for detection, deterrence, or other desired effect." MITRE, An Introduction to MITRE Shield, 2020*

Shield makes heavy use of Deception, appearing in all eight of the techniques in the matrix. For example, five of the twenty techniques in the crucial "Detect"

tactic leverage decoys. Overall, Deception is by far the most common solution suggested in MITRE Shield, and therefore is the natural choice for OT network security.

5. Acalvio ShadowPlex: Solution Strategy

Acalvio's strategy for OT/ICS environments is to provide a flexible, multi-layer toolkit for deception based on the reality that such networks are extremely heterogeneous. The strategy recognizes that most OT attacks originate on the IT side, though a minority leverage other vectors such as poorly secured remote access. The Acalvio platform was specifically designed with the customization necessary to deploy credible Deception in most any situation, including OT networks. This is the natural approach given the heterogeneous nature of ICS environments: The endless combinations of vendors, devices, and age of equipment necessitates a level of customization to be credible. It also accommodates the reality of the limitations found in OT environments not seen on the IT side:

- Purdue model recommendations & OT segmentation policies
- Stringent change control procedures
- Deployment, physical access, and WAN bandwidth limitations

Each organization has different policies; what is allowed in a manufacturing plant may not be allowed in a nuclear power plant or off-shore oil rig. And these policies are changing as the OT market moves to more connected systems and governance becomes influenced by IT, a process known as "IT/OT convergence".

6. Acalvio ShadowPlex: Solution Capabilities

ShadowPlex provides built-in PLC decoys (Modbus over TCP, BACnet, Siemens S7, Rockwell Ethernet-IP) from multiple vendors. For Honeywell customers, ShadowPlex also provides decoys for Niagara AX, Enterprise Buildings Integrator (EBI TCWS, EBI Easy Mobile)), Digital Video Manager (DVM) and Network Video Recorder (NVR).

In addition, ShadowPlex supports a number of Deception customization options to support OT/ICS deployments, which are detailed below, in order of desired engagement level:

6.1. Low interaction ports on decoys

ShadowPlex allows customizing a decoy template by opening specific ports. The decoys listen on those ports and alert on any access. This approach can be used to mimic PLCs and RTUs, which are not covered by the built-in decoy types.

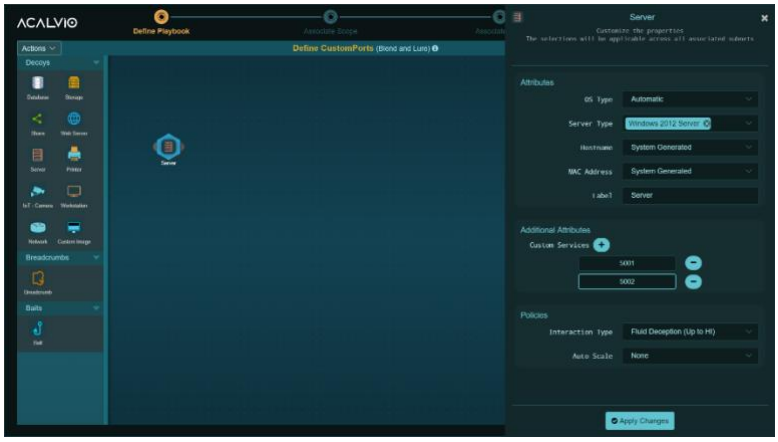

Figure 2. Decoys are easily customized to match ICS device port characteristics

6.2. Custom web decoys

ShadowPlex supports uploading custom web content onto web-server decoys in the bespoke deception palate. Many HMIs, remote terminals and OPC servers have a web-based GUI interface. The GUI interface from these devices can be uploaded as custom web content and ShadowPlex automatically creates corresponding decoys with the same web interface.

6.3. Golden image virtualized decoys

More sophisticated, higher interaction decoys can be created based on gold images of OT hosts. The Acalvio platform can create thousands of decoys from the gold image automatically and deploy them across the distributed network. By leveraging patented Fluid Deception™ technology, the resource and license overheads for these authentic decoys are kept to a minimum.

HMIs and other IT-based ICS elements can be recreated using gold image replication and virtualization. The following screenshot shows an example where an authentic decoy of a Honeywell Niagara Supervisor was created from an uploaded golden image.

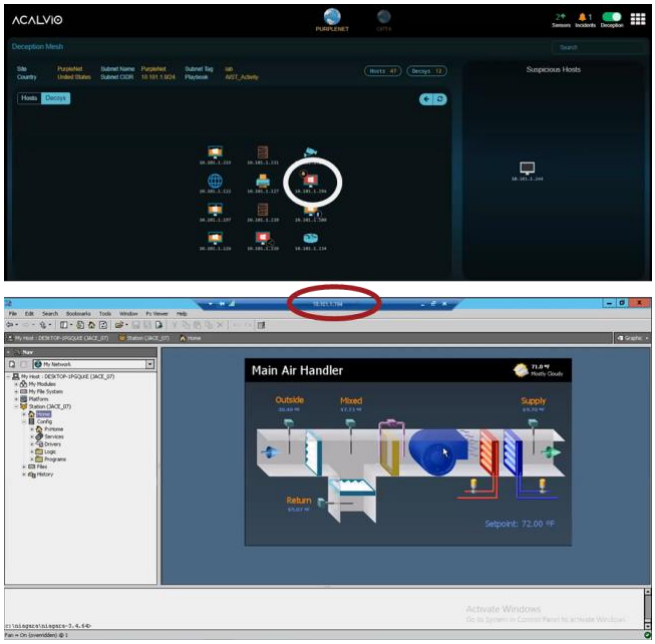

Figure 3. Custom decoy for Honeywell Niagara supervisor, created using golden image upload

6.4. Breadcrumbs

ShadowPlex increases the effectiveness of decoys by allowing creation of corresponding breadcrumbs for those decoys. Such breadcrumbs direct the attacks towards the decoys and can be deployed automatically by the ShadowPlex platform. ShadowPlex simplifies this process by modeling the attributes of the host for the breadcrumb and crafting the breadcrumb for credibility in the environment.

ShadowPlex breadcrumb deployment architecture is agentless. This avoids the compatibility and security challenges associated with the deployment of an additional agent.

7. ShadowPlex OT/ICS Deployment Model

Acalvio recommends a three-stage deployment model for ShadowPlex within an OT environment. First, relevant OT production assets are modeled, and custom or semi-custom decoys are created. For the increasing number of OT assets that are based on IT (Windows/Linux) platforms, the turnkey ShadowPlex deception palette is used. These decoys are deployed within the OT environment in Layers 1 through 3.5 of the Purdue model, the exact placement being dependent on the network architecture and DMZ locations. The decoys are projected by a ShadowPlex Sensor. The communication from the sensor to the ADC is “outbound only”, eliminating the need for riskier “OT inbound” firewall policies.

Next breadcrumbs that point to the decoys are crafted. Acalvio tooling automates this process without the use of agents. Placement of breadcrumbs is flexible and depends on the on the risk management strategy of the organization. For example, some teams may place breadcrumbs on IT network devices that access the OT network, reasoning that the path is open anyway and they want to know if it’s being misused. Others may decide to limit breadcrumb placement within the OT network, on devices that can accept them. These would typically be deployed in Layers 2 to 3.5.

The Acalvio Deception Center (ADC) is the ShadowPlex control and management node. This may be placed either within the IT or OT environment, depending on the corporate security policy and the operational model. Some organization delegate OT Security Operations to dedicated teams, while others centralize operations. Furthermore, more risk-averse organizations may prohibit direct connections of any kind across the IT/OT boundary unless they terminate in the DMZ. In this case the ADC should be placed in the DMZ, and solution operators can be granted access as required.

To streamline the process, Acalvio customers can rely on the assistance or our Customer Success organization, which has the tools and experience to aid in modeling OT devices to create deception assets. They also assist in determining the best deployment architecture given the organization’s security policies and operational model.

8. Summary

Risk management and security in OT/ICS environments is challenging, in particular because of the limited scope for implementing more invasive solutions commonly seen in enterprise networks. However, Deception is well-suited for such environments, because of its low-risk nature. Acalvio's strategy is to support flexible deployment models, and customization of assets to mimic OT/ICS assets. This makes ShadowPlex an operationally viable option for OT governance and risk management, across the wide variety of industries in which such mission-critical networks are present.