Case Study: Industrial Controls

Winning Against the "Indefensible Attack"

Introduction

The next 'Pearl Harbor attack' will include attacks on private sector functions, including those supporting our daily lives. Attacks on industrial systems are adversely effecting production processes in critical infrastructure environments at an increasing rate. And a vast majority of industries still lack adequate cyber security controls.

Against this backdrop, providers of Industrial Control Systems (ICS) software recognize the need to increase security measures on solutions that power much of the country's critical infrastructure. In an environment where nation-states are investing heavily in building out cyber warfare capabilities, the pressure continues to mount.

Background of Customer Application

Virsec has been working with a leading global provider of ICS Supervisory Control & Data Acquisition (SCADA) software and solutions to protect control system software from memory-based, binary attacks. The legacy solution for protecting ICS applications has been Application Control (file whitelisting), but this leaves these critical systems exposed to a significant class of "indefensible" attacks—fileless, memory-based.

The following constraints and concerns were paramount for this organization and its global customers:

1. Increasing operational technology (OT) and IT convergence over the past decade for operational efficiency of industrial control systems has increased the risk of malware infections and malicious activity at OT systems are no longer "air-gapped" from the internet.
2. Safety and reliability are paramount for critical SCADA systems like the power grid, with which often require 100% uptime. This makes patching software and updating signatures in security products difficult and expensive.
3. Much of the SCADA world is run on legacy Windows platforms that are end-of-life at this point. These systems are often compiled for 32-bit operation as opposed to newer 64-bit architecture. Given the relentless focus on uptime, availability and costs, getting more life out of existing and legacy solutions is important.
4. Relying on IT organizations for the security of control systems is a major deterrent to adoption of new solutions. Security must be seamlessly integrated into OT systems and easily accessible to control system engineers. Even the legacy Application Control solution which did not rely on an Internet connection, was more cumbersome to implement than expected.

System Architecture and POC Environment

The customer was primarily concerned about a class of attack their security experts were finding to be "indefensible"—memory-based attacks on known or unknown, zero-day vulnerabilities that could bypass an Application Control whitelist or Anti-Malware products and take malicious action. For example, the Stuxnet malware took advantage of over 20 zero-day vulnerabilities and caused systems to report erroneous data back to control system engineers.

Figure 1 shows a typical ICS system. Tier 0 includes I/O devices such as sensors, actuators, Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs).

Tier 1 is the Supervisory SCADA layer, which includes functional components like a Central Object Repository, Application Servers, Tier 1 Historian, Human Machine Interface (HMI), Engineering Workstation, etc. They configure, monitor and control the elements in Tier 0 while feeding information to the upper tiers. These components reside on Windows-based servers that aggregate information or perform specific functions in the solution such as logging live data (alarms and events) received from Application Engines, the HMI or the operator station, and being the repositories holding factory configuration information.

Tier 2 is Web-facing and generally segregated from Tier 1 by a firewall. Here information is aggregated and made available to analysts connecting from a corporate location through an Intranet. At this tier, vital servers such as a Tier 2 Historian can aggregate information from various Tier 1 Historians and an Information Server acts as web portal to visualize information from factory systems. In addition, the Microsoft SQL Server typically provides the persistent data repository and is also susceptible to attack.

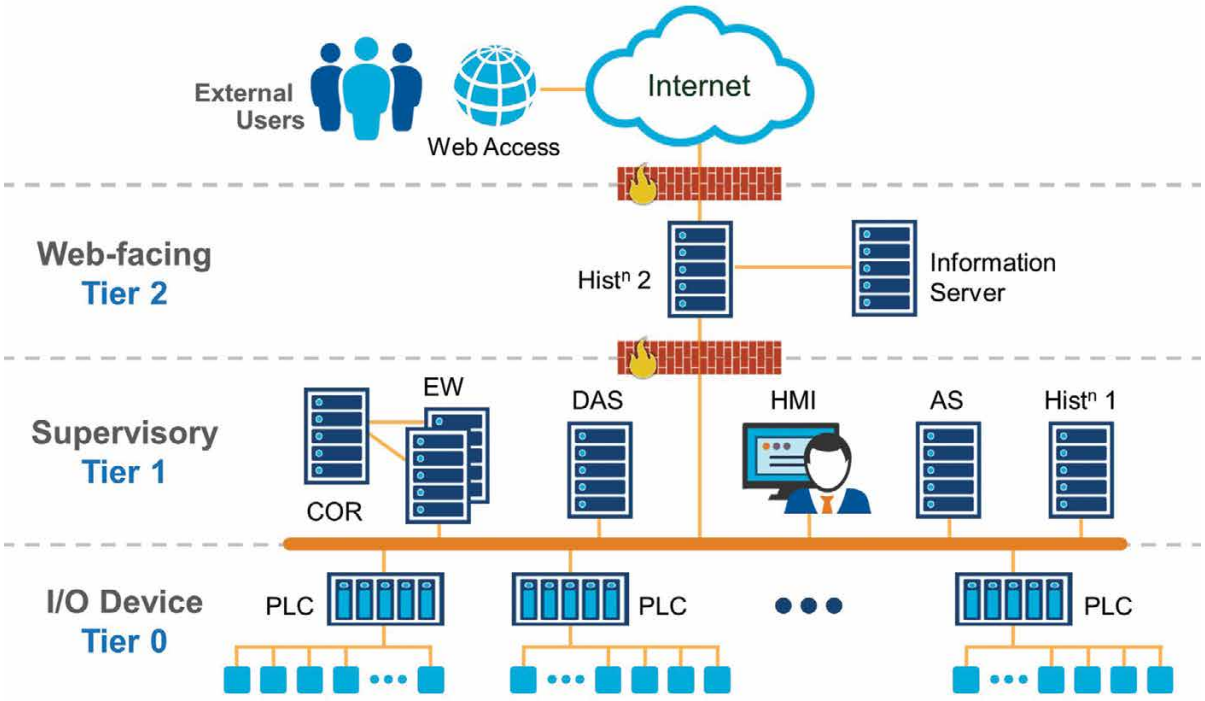

Figure 1: General ICS-SCADA Representative Architecture

Vulnerability and Attack Concerns

The customer was particularly concerned about DLL Hijacking and memory-based attacks such as Library Injection. For example, with DLL Hijacking, an attacker might swap a language support DLL (for internationalization) with a compromised DLL which could open a reverse shell in addition to performing all the expected localization functions.

In addition, zero-day attacks on unpatched Microsoft components, like SQL Server, were also a concern. In these environments, automatic software patching generally turned off due to uptime constraints.

Figure 2 shows the ICS-SCADA environment used for the tests of the Virsec Security Platform (TM). The primary OS was Windows Server 2012 running on VMware ESX VMs on off-the-shelf servers.

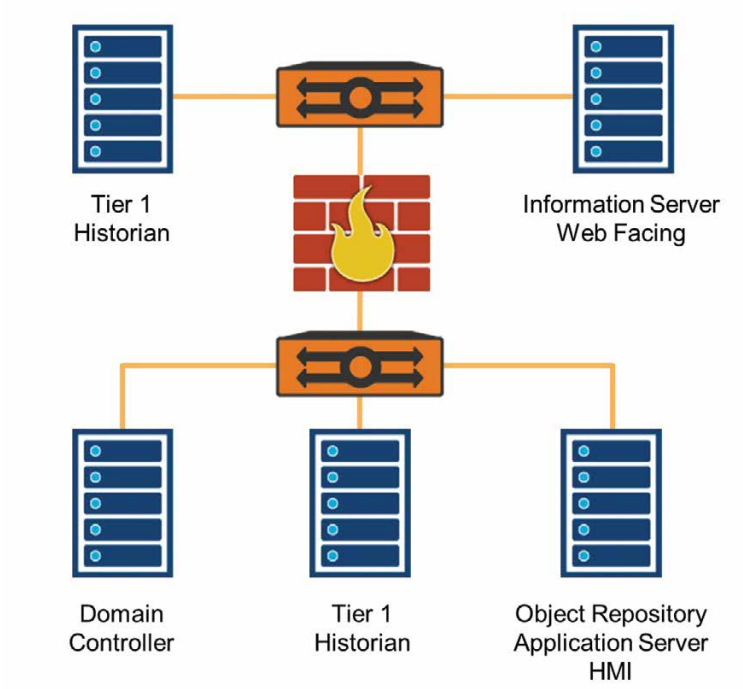

Figure 2: POC Deployment Architecture

The customer's Chief Security Architect tested capabilities for detecting "indefensible" memory-based attacks like library injection and buffer overflow exploits using its Trusted Execution® approach. They also evaluated how Virsec could extend or improve existing Application Control options for the ICS-SCADA solution.

Results

In order to validate the solution, the customer uses the Virsec Application Integrity Protection, to protect Windows application components from memory-based attacks.

The key performance metrics were:

1. Efficacy of attack detection
2. Performance impact

Specifically, the customer tested Virsec's claims of near perfect accuracy and performance impact of less than 5% additional CPU utilization.

A key aspect of protection Virsec provides was the ability to protect both 32-bit and 64-bit Windows applications, particularly during complex mixed-mode initiation paths where child processes of ancestor processes might change in mode support. Given the use of legacy Windows and application types in ICS-SCADA, this was a key requirement for a runtime execution protection product. To measure the performance impact, measurements were taken both with and without Virsec.

To measure accuracy, a DLL injection attack was staged on every component of a protected application, along with a proprietary exploit on a buffer error vulnerability that the customer had recently encountered.

DLL Injection Attack Detection

Runtime Execution Integrity. The system was subjected to a simulated DLL Injection attacks by using the "Syringe" utility, which can be used by hackers to inject malicious code into running applications.

In all cases, regardless of where in the application sub-process chain the attack took place, Virsec detected the malicious event immediately. Virsec's memory corruption and memory-based attack protection is deterministic and detects even non-malware, fileless memory attacks the moment the normal execution path is subverted.

File Integrity Monitoring, which uses checksum and disk location checks of application components to detect potential attacks. For example, threat or attack alerts can be raised when unknown or tampered-with application libraries are discovered when being loaded into memory, or when a malicious DLL that violates file integrity is dropped into the application's home directory. It also flags changes to file system attributes like file modification timestamps, ownerships, etc.

Average Performance Impact

Given reliability and uptime requirements for ICS-SCADA systems, ensuring a low performance impact on the protected application components was a key requirement for the customer.

Measurements were taken over long periods of time, ranging from 90 minutes to several hours to determine the average CPU impact of the Virsec solution on the customer's ICS software. In all cases, Virsec protection added less than 5% to the CPU load.

Conclusion

Virsec Security Platform with Trusted Execution technology delivers breakthrough ICS-SCADA security designed to meet stringent critical infrastructure requirements.

Requirement	Virsec Requirement	Virsec Security Protection
100% ICS system uptime without reboots of OS servers	No OS reboot required. Does not depend on signatures packages being delivered	Detects zero-day, or fileless attacks in microseconds
Windows patches installed infrequently	Does not depend on the latest application patch being applied	Detects zero-day attacks against any application including unpatched binaries
Support for legacy Windows versions including 32 and 64-bit application processes	Binary protection supports legacy Windows versions and any 32-bit and 64-bit applications	Protects runtime execution integrity of all 32-bit or 64-bit applications and all sub-processes.
Seamless enablement of security within ICS-SCADA	Exposes attack alerts via RESTful API for integration	Seamless integration of ICS security protection into control system interfaces

Virsec Security Platform successfully demonstrated protection from "indefensible," fileless, memory-based attacks which easily bypass Application Control whitelists or Anti-Malware products. The solution detected DLL Injection and buffer error vulnerability attacks 100% of the time, with CPU performance impacts well under 5% under various load conditions.