FIRSTCo.

Securing Industrial Control Systems on a Virtual Platform

How to Best Protect the Vital Virtual Business Assets

WHITE PAPER

Sajid Nazir and Mark Lazarides

sajid.nazir@firstco.uk.com
mark.lazarides@firstco.uk.com

9 Feb, 2016

Executive Summary

Industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) are used to monitor and control critical infrastructures, like transportation and power generation systems. Recent ICS are Internet-connected to exploit the benefits of remote connectivity and availability of mobile devices. The connection to the Internet however exposes the critical infrastructures relying on ICS to cyber security threats as evidenced by attacks such as Stuxnet [1].

The monitoring and control industry has been quick to appreciate the benefits of virtualisation and is keen to adopt it. Although, a virtual platform offers similar attack surface as physical hardware, some of its features can be leveraged to protect the hosted applications against security threats, and also to recover quickly from any disruption or disaster. Hardening is the process of protecting a system by reducing its vulnerability to attacks. Firstco Ltd. has established a VMware Virtual Development Environment (VDE) for developing, testing and simulating SCADA systems, and it maintains in-house security standards for ensuring a hardened system.

This paper covers the security hardening measures by combining the traditional best practices with the inherent features of a virtual infrastructure to yield a hardened ICS system.

What is Virtualisation?

Virtualisation defined

Virtualisation means creating a virtual (rather than physical) computing resource including CPU, storage, and network. It provides ease with which machines can be monitored, restored, deleted, and migrated. It is mature technology gradually finding its way into control and automation industry. A host operating system (OS) or hypervisor software (in case of bare metal system) are used to run guest OS or virtual machines (VMs) as shown in Figure 1.

The specifications describing VMs including the OS, storage, installed applications, and networking can be captured as a VM template [2]. This template can subsequently be used to create VMs to those specifications and can be kept updated with latest changes and updates.

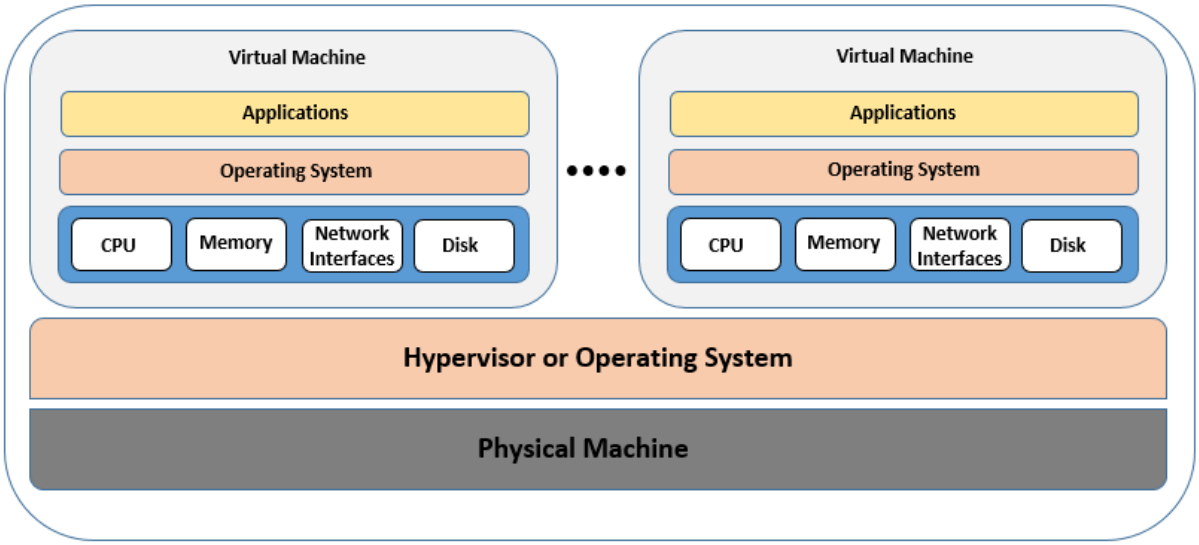

Figure 1: General configuration of a Virtual Platform.

Differences from Cloud Infrastructure

A cloud infrastructure can be defined as a platform which delivers services over the Internet. In contrast virtualization may or may not be cloud based. Depending on the needs and budget of a company it can opt for a totally in-house solution controlling everything within its administrative boundaries. Public infrastructures like Amazon Web Services (AWS) [3] allow creation of VM at their data centres. A hybrid configuration can be chosen to keep the mission critical elements in-house and stow away the backups and non-essential elements to a public infrastructure. The borders are blurred as a private infrastructure maintained by a company may be offered as a public offering to be used by another company.

Benefits of Virtualised Infrastructure

The benefits of virtualisation are better server utilisation, energy saving, and ease of deployment. The Vms are in fact just files which can be easily copied and shared. It is easy to change the resource allocation to meet the changing requirements. Virtualization platforms provide many features keeping downtime to a minimum. The higher return on investment is driving the industry towards migrating control and monitoring systems to virtual platforms.

Vulnerabilities of a Virtual Platform

Supervisory Control and Data Acquisition (SCADA) systems are used in industrial applications and are typically employed for control and monitoring of critical infrastructures, such as railways, airports, and power infrastructures. A compromised or failed system can thus have serious consequences for public safety, health or security.

Two recent attacks on the VMs are Cloudburst [4] and Crisis malware [5]. The attacks demonstrate how VMs can be targeted and thereafter the host itself could be attacked.

- **Similarities to Physical Systems**
  Despite many differences, a virtual machine is similar to a physical machine in terms of its vulnerabilities. A VM runs a commercial OS exposing it to all vulnerabilities of that OS.

- **Single Point of Entry and Failure**
  The virtual infrastructure can house thousands of machines running on host platforms which otherwise would have been servers dedicated to different business processes and with their own individual security measures. A compromised VM on a Virtual infrastructure could be disastrous as the infection can propagate to other VMs in the cluster. The biggest risk is of a VM attack leading to an attack on the host.

- **Host Platform**
  The host or hypervisor may itself be running a host OS such as Windows or Linux, which increases the attack surface and makes it only as secure as the guest OS. Newer virtual platforms use bare metal hypervisors which run on a scaled-down OS and are thus more secure.

- **Physical Security**
  The VM uses virtualized resources including CPU, memory, and networking. Access to physical hardware exposes the platform to threats such as access to a physical port. The physical security aspects of a virtual platform are often overlooked but these have caused security breaches. The physical access to the system needs to be restricted and monitored.

- **Virtualization Sprawl**
  Since VM creation is so easy there could be a tendency to leave VMs beyond their actual utilization period. The machine could be forgotten after being created and may continue to

use the crucial system resources and can be potential easy targets. System maintainability can become very difficult if this sprawl is not managed.

Security Hardening of an ICS

Firstco Ltd specialises in control and monitoring systems for critical infrastructures which require a high degree of security. The VDE (based on VMWare) was established at Company premises for hosting the development and production systems for development, testing and commissioning. The experience gathered from establishing and operating a VMware based private data centre helped us to understand the importance of the best practices for cyber security. In the following sections, guidelines are provided for protecting an industrial control application running on a virtual platform.

The general protective measures against cyber security as used by physical platforms do apply. Such practices can be augmented through the specific features [6], [7] provided in the virtualisation infrastructure and need to be incorporated in management policies for ensuring continuous upkeep of highest levels of security.

General Practices for Protection

Updates and Patches
The OS and other applications must be kept updated against security threats. VMware tools must also be installed on every VM.

Anti-virus and malware Prevention
The anti-virus and anti-malware should be installed, updated and used for protection against the ever changing threat scenario.

Physical Security
The access to the physical computing resources need to be restricted to the authorized personnel only. This protects the network and device ports from a malicious access through denying unauthorised connections, and resets or re-configuration of devices.

User groups and Privileges
Effective resource allocation dictates that the privileges be defined for each user group to access the virtual resources. These could be used to authenticate access to resources.

System Isolation Boundaries
The principle of least privilege dictates that the privileges should be just enough for an application or user to meet the requirements. The system boundaries should ensure that the access is restricted to a defined subset only.

Leveraging Features from VMware vSphere

The protection against cyber threats can be ensured through implementing best practices in the VM templates. This ensures that the security of a virtual infrastructure and machines is incorporated from the very conception of the system.

Restricting Resource Usage
As a general principle a VM should only be allocated resources which are fit for purpose. The resources can be elastically increased later in case of changed requirements.

VM Templates
Templates [2] serve as a design with baseline configuration from which VMs can be created. This prevents against making mistakes where every required VM is built from scratch. The templates are easier to be kept updated and hardened [8].

Virtual Appliance (VA)
VA serves as a container for one or more VMs [9], [10] designed to address a particular application. The OS used in vApp is a reduced and tailored down version of the full OS targeted to a particular application. The reduced OS also termed as Just Enough OS (JeOS) that addresses a particular application provides a reduced attack surface as a reduced set is subject to lesser vulnerabilities.

Update Manager
The security patches are issued by companies for an upgrade or to provide fixes against an identified threat. However, the need is to overcome the general tendency of not to apply a patch. VMware Update Manager provides the facility to keep the systems updated and can reduce the security vulnerabilities [11] by downloading and even keeping track of the recalled patches. The snapshot feature can help with cases where the patch process needs to be undone.

Backups and restore points
The virtual infrastructure can be used to create restore points similar to Windows platform which can be used to restore the system to a good state after it has been compromised.

High Availability
It provides failure protection against hardware and operating system failures and can reduce application downtime through an automatic restart.

Disaster Recovery
There are features in the virtualised infrastructure which can help with disaster recovery. Notable amongst these are live migration, fault tolerance, and improved disaster recovery mechanisms [11].

Layered Defence to Virtual Assets

Securing Virtual Machines
The VMs provide isolation and the crashes and failures can be contained. The segregation helps to secure the VMs from the effects of the other machines in the environment.

The unused features and services of the OS should be turned off and the unused hardware devices should be disconnected or better removed. The VM should be allocated limited resources and limited number of the log files it can create to guard against a denial-of-service attack [8].

Securing the Networking
Separate network controllers should be used for the management and VM networks [11]. Firewall protection can be added by configuring host-based firewalls.

Securing the Hosts
The hosts need to be protected by restricting access to the services and ports. If a host is compromised then the hosted VMs also get compromised. The user access to the host should be restricted [8].

Securing the Hypervisor
The hypervisor [12] should be updated with security patches and access to it must be limited. An anti-virus program must be installed on the hypervisor.

Protecting the VDE

At the highest level, the virtual infrastructure itself needs to have a restricted and limited access. It is important to segregate the corporate network from the virtual infrastructure/production LAN through firewalls (Figure 2) and by establishing a Demilitarised Zone (DMZ) [13].

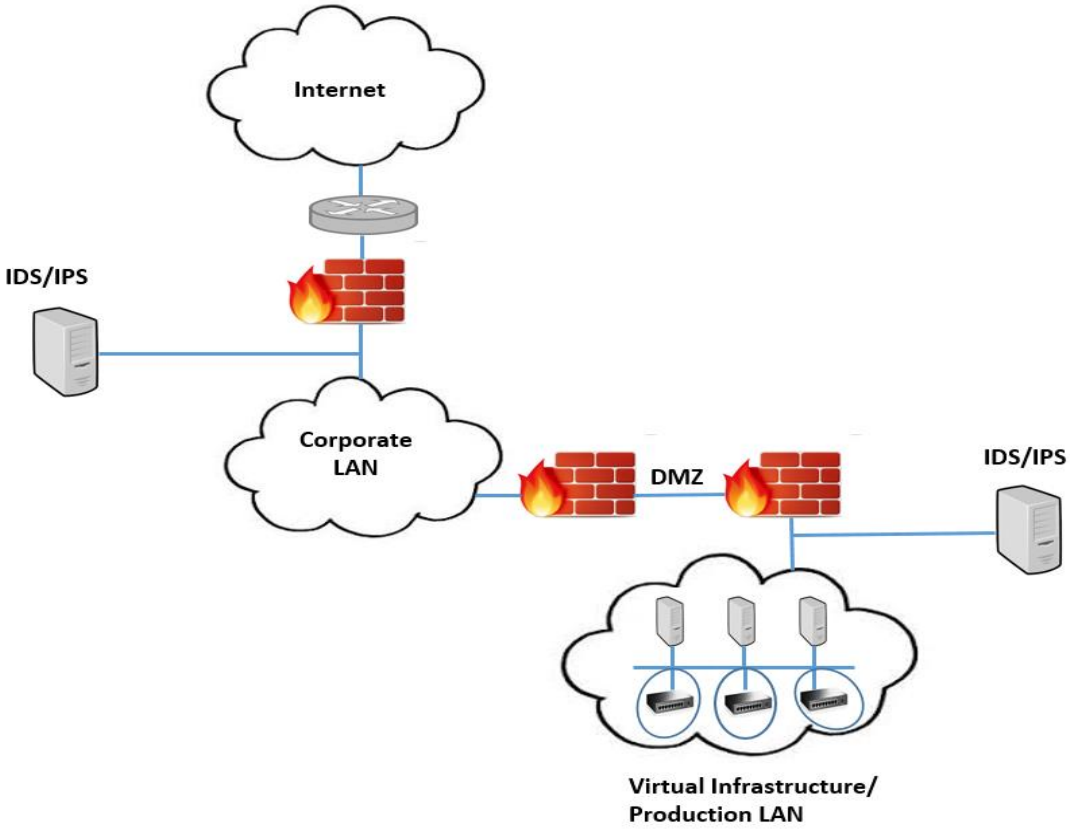

Figure 2: DMZ with separation of trust zones.

Continuous Monitoring and Improvement

The infrastructure needs to be monitored and updated continuously [14] to provide safeguards against new threats and to uncover the weaknesses in own system with a view to harden them before any exploitation takes place.

- **Anomaly Detection**

  The monitoring of events through an Intrusion Detection System (IDS) and blocking them by an Intrusion Prevention System (IPS) in the virtual infrastructure can provide protection against potential security threats. Intrusion detection and prevention tools [15] such as Snort, and OSSEC can be used. Activity logging and identifying resource usage can also help to uncover an anomalous activity.

- **Penetration Testing and Vulnerability Analysis**

  Penetration testing and vulnerability analysis can uncover potential problems. Ideally, these could be conducted in-house by someone other than the network team or could be delegated to outside professional organisations. Free tools [16] such as Metaspoilt, Wireshark, Retina, and Nmap can be used.

- **Simulation**
  The biggest hurdle to testing an operational system is that it cannot be taken out of service and there is no way to duplicate the system without incurring heavy costs. A simulated system can replicate a production system to test the effects of updates and to evaluate the security against threats.

Conclusion

This paper describes an effective defence mechanism for industrial control systems on a virtual platform by combining the best practices of the conventional approaches for protection with the features available in a virtual platform. Further adoption of virtualisation will occur with more emphasis on energy, resource and space saving and increased competitiveness. The industry would soon see more reliance on open source products and adoption of innovations such as virtual appliances to deliver the promise of truly customisable platforms.

A security hardened system gives clients an assurance of its robustness against the cyber-attacks, and it helps to check that the virtual infrastructure provider is following the best industry practices. From an implementer's perspective, it makes sense to continuously monitor their business processes to the emerging innovations and threats to stay abreast of the ever changing scenario.

References

[1] J. Vijayan, B, "Stuxnet renews power grid security concerns" Computerworld, Jul 26, 2010. Available online: http://www.computerworld.com/article/2519574/security0/stuxnet-renews-power-grid-security-concerns.html

[2] VMware White Paper, "Templates Usage and Best Practices".

[3] Amazon Web Services: https://aws.amazon.com/

[4] M. Broersma, "Virtual machine exploit lets attackers take over host" June, 2009. Available online: http://www.zdnet.com/article/virtual-machine-exploit-lets-attackers-take-over-host/

[5] T. Katsuki, "Crisis: The Advanced Malware" Available online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/crisis_the_advanced_malware.pdf.

[6] K. Scarfone, M. Souppaya, P. Hoffman, "Guide to Security for Full Virtualization Technologies" NIST Special Publication 800-125.

[7] vSphere 5.5 Security Hardening Guide, October 30, 2013.

[8] vSphere Security Update 2, ESXi 5.5, vCenter Server 5.5

[9] VMware white paper, "Understanding, Building and Deploying Virtual Appliances" Available online: https://vmware-partnerpedia-shared.s3.amazonaws.com/documents/Virtual_Appliance_Whitepaper.pdf

[10] Developer's Guide to Building vApps and Virtual Appliances, VMware EN-000207-00.

[11] VMware vSphere: Install, Configure, Manage, Student Lecture Manual.

[12] VMware white paper, "Security of the VMware vSphere Hypervisor" Jan 2014.

[13] VMware Best Practices, "DMZ Virtualization with VMware Infrastructure".

[14] J. D. Sherry, "Continuous monitoring in a Virtual Environment" Trend Micro White Paper, Nov 2013.

[15] Joe Schreiber, "Open source intrusion detection tools: a quick overview" Jan 2014. Available online: https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

[16] "18 Free Security Tools for SysAdmins" Available online: http://www.gfi.com/blog/18-free-security-tools-for-sysadmins/