Security Management of Virtualised Supervisory I&C Systems in Nuclear Facilities

Hewes, M.[1]; Howarth, N.[1]; Hunt, C.[1]; Noonan, A.[1]

1 Australian Nuclear Science and Technology Organisation (ANSTO), Lucas Heights, Australia

Abstract: We review the functionality provided by virtualisation platforms, available to Nuclear I&C operators from a cyber security management perspective.

Keyword: ISOFIC, I&C, HMI, Cyber Security

1 Introduction

Instrumentation and Control (I&C) systems in nuclear facilities provide information and control capabilities for the operation of the plant in operational states and in accident conditions[1]. I&C system vendors are continuing to adopt virtualisation technologies in their product offerings. Consequently, nuclear facilities will continue to expand the use of virtualised I&C systems. In this paper we review a number of out of band security management techniques available to nuclear I&C operators when responding to an incident on virtualised I&C systems.

2 Change Control and Configuration Management

The inherent abstraction of a virtualised environment along with the features provided by all major virtualisation host software offerings can be leveraged to enhance Engineering Change Control and configuration management process, as recommended by IAEA guidance[2].

The use of virtualization allows for of simplified engineering and maintenance processes, while allowing for systematic enforcement of configuration management policy. For example, the application of software patches to a system can be performed on isolated instances of virtual machines for testing and validation purposes, prior to the patching of operational systems. This process can be enforced by the virtualisation environment itself, with testing, review and approval data collected and stored by the system itself, reducing the administrative overhead that may otherwise be required.

Virtual machine deployment can also be automated, providing the ability to apply predefined and authorised policies and configuration management standards when deploying new systems, further reducing the risk of introducing additional security vulnerabilities and risks.

3 Operational Considerations

The ability to perform live migration between different virtualisation hosts provides the ability to move a virtual machine between physical infrastructure while the virtual machine remains online ensuring continued operation of running plant. This can allow hardware and operating system changes to the host server, such as the application of security patches, while minimising disruption to services provided within the hosted virtual machines.

This live migration of virtual machines is achieved due to the nature of how storage is provided by the physical host to the virtual machine. In comparison to a conventional system where the raw storage media is directly accessed by the running system, the hypervisor powering the virtual infrastructure presents each virtual machine a virtual disk. This virtual disk appears as standard files to the hypervisor and can exist on a highly available and fault tolerant storage platform.

When presented to a virtual machine, the virtual disk mimics the characteristics of a raw storage medium. As these source files are accessible from the hypervisor they are able to be accessed and monitored outside of the execution context of the virtual machine itself. This enables the monitoring software to run without a threat to its integrity from malicious software able to control the execution context of the virtual machine.

4 Backups and Snapshots

Additional benefits can be realised with the use of virtual machines within Nuclear I&C by the use of Snapshots. Snapshots capture a complete image of a virtual machine including its data, virtual hardware configuration, memory state, and power state[3]. The image of the memory state can also be loaded into a number of commercial and open-source memory analysis toolsets[4]. These tools allow visibility of compromises which may leverage advanced techniques to insert malicious software into memory without any on-disk file persistence that would be uncovered from forensically investigating the disk images. These snapshots can also be used to quickly recover from unexpected failures during the course of implementing a change.

Alternatively a virtual machine snapshot can be migrated to a test environment to facilitate offline testing of changes to be implemented or enable connection to simulated I/O. During an incident it may be beneficial to allow an infected virtual machine to continue running to understand the behaviour of any compromise. Within the context of Nuclear I&C this is counter to nuclear design criteria which would see the systems restored to design basis immediately on detection. With a virtual infrastructure it is possible to clone the compromised host, restore the running instance to a known good image that operates within design basis, and migrate the compromised clone to a sandbox with simulated I/O that records any actions undertaken to gain a greater understanding of the threat actor.

The ability for a virtual machine to be cloned and restored to a known good state supports release management and change management activities by streamlining the process, minimising the risk associated with change and minimising the possibility of a negative impact to the integrity and availability of productions systems. These technologies directly contribute to both increased agility and reduction in risk during short maintenance windows, typically encountered on industrial and nuclear facilities.

5 Virtual Machine Introspection

A more advanced technique for securing and monitoring a virtual environment is by using Virtual Machine Introspection (VMI). VMI is a technique for externally monitoring the runtime state of a virtual machine, without the monitored virtual machine participating in, or having an awareness of the monitoring process[5]. Monitors can be placed in another virtual machine, within the host hypervisor, or within any other part of the virtualization architecture. For virtual machine introspection, the runtime state can be defined broadly to include processor registers, memory, disk, network, and any other hardware-level events. Using VMI, monitoring tools can perform anti-malware, intrusion prevention and detection, and many other security and compliance functions.

6 Summary

In summary, a robustly engineered, operated and maintained virtualisation based nuclear I&C system provides significant benefits to the operations and security of the facility. These benefits range from a reduction in capital and ongoing costs; improved agility both for internal customers e.g. engineering changes, and external forces e.g. security incidents and software patches; decreased recovery times in the event of failures other security incidents; and the facilitation of sophisticated virtual machine based operational and digital forensic techniques.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standard Series No. SSG-39, IAEA, Vienna (2016)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Configuration management in nuclear power plants, IAEA-TECDOC-1335, IAEA, Vienna (2003)

[3] VMWARE, INC., Understanding VM snapshots in ESXi / ESX (2015). VMWare, Inc. Retrieved 5 June 2017, from https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

[4] VOLATILITY FOUNDATION, VMware Snapshot File. (2013). GitHub. Retrieved 1 June 2017, from https://github.com/volatilityfoundation/volatility/wiki/VMware-Snapshot-File

[5] TAPASWI, Shashikala, Virtual machine introspection: towards bridging the semantic gap, Journal of Cloud Computing. Retrieved October 2017, from https://link.springer.com/article/10.1186/s13677-014-0016-2

[6] VMWARE, INC., Virtulisation (2017). VMWare, Inc. Retrieved 5 June 2017, from http://www.vmware.com/solutions/virtualization.html

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No.17, IAEA, Vienna (2011)