NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2016-02 Modifications to CIP Standards Drafting Team

March 22, 2018

Christine Hasha, Standard Drafting Team (SDT) Chair, called the meeting to order. Jordan Mallory reviewed the NERC Antitrust Compliance Guidelines and Public Announcement[1]. Attachment 1 identifies the SDT members who attended the March 22, 2018 conference call.

Virtualization

David Revill presented a recap of the history and current status of virtualization (Attachment 2). During the presentation, D. Revill reviewed the scope of virtualization, the three virtual infrastructures under consideration (network, storage, and server) and the many different viewpoints on virtualization risk. To supplement the presentation, several SDT members completed a risk analysis for discussion.

Following discussion of the risk analysis, the SDT identified the following 10 risks associated with virtual servers:

1. Virtual Machine (VM) Sprawl
2. Sensitive Data within a VM
3. Security of Offline and Dormant VMs
4. Security of Pre-Configured/Active VMs
5. Lack of Visibility into the Controls Over Virtual Networks
6. Resource Exhaustion
7. Hypervisor Security
8. Unauthorized Access to Hypervisor
9. Account or Service Hijacking through the Self-Service Portal
10. Workload of Different Trust Levels Located on the Same Server

The team continued discussion on the extent to which current standards address the identified risks. The question remains on whether the standards should be modified or if the risks should be addressed through alternate means.

J. Mallory will work with Matt Hyatt (TVA), Jake Brown (ERCOT), Todd Starling (Southern), David Revill (GSOC), Christine Hasha (ERCOT), Steve Brain (Dominion Energy), and Forrest Krigbaum (BPA) on Monday, March 26, 2018 to continue analysis to prepare for the upcoming in-person meeting.

[1] See page 5.

J. Mallory reviewed the upcoming meetings.

a. **March 27-29, 2018 (Atlanta, GA)**
b. **May 8-10, 2018 (Texas Reliability Entity, TX)**
c. **June 19-21, 2018 (Atlanta, GA)**
d. **July 10-12, 2018 (TBD)**
e. **September 4-6, 2018 (Atlanta, GA)**

The meeting adjourned at 2:55 p.m. eastern.

Attachment 1				
Name	**Company**	**Member/ Observer**	**Straw Vote (X)**	**Conference Call/Web (Y/N)**
Christine Hasha	Electric Reliability Council of Texas	Co-Chair		Y
David Revill	GSOC	Co-Chair		Y
Steven Brain	Dominion Energy	Member		Y
Jay Cribb	Southern Company	Member		N
Jennifer Flandermeyer	Kansas City Power and Light	Member		N
Tom Foster	PJM Interconnection	Member		Y
Forrest Krigbaum	Bonneville Power Administration	Member		Y
Mark Riley	Calpine	Member		Y
Jordan Mallory	NERC	NERC Staff		Y
Mat Bunch	NERC	NERC Staff		N
Soo Jin Kim	NERC	NERC Staff		Y
Marisa Hecht	NERC	NERC Staff		Y
Shamai Elstein	NERC	NERC Staff		Y
Tom Hofstetter	NERC	NERC Staff		N
Lonnie Ratliff	NERC	NERC Staff		N
Mike Keane	FERC	FERC		N
Jan Bargen	FERC	FERC		Y
Margaret Scott	FERC	FERC		N

Ken Lanehome	Bonneville Power Administration	PMOS		Y
Kirk Rosener	CPS Energy	PMOS		Y

NERC Antitrust Guidelines

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

NERC Standards Development Process-Participant Conduct Policy

http://www.nerc.com/pa/Stand/Documents/Standards%20Development%20Process-Participant%20Conduct%20Policy.pdf

NERC Email Listserv Policy

http://www.nerc.com/pa/Stand/Documents/Email%20Listserv%20Policy%2004012013.pdf

Virtualization Risks

3/22/2018

Virtualization Scope

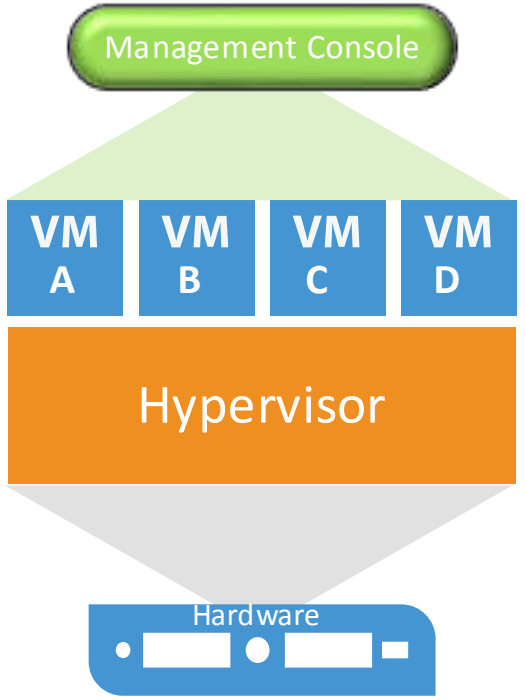
- The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies.

Three Types of Virtual Infrastructure under Consideration

- Network
- Storage
- Server

Key Question for determining next steps on addressing virtualization

- Determine the level to which mixing Cyber Asset classes on shared infrastructure is permitted (CIP-applicable with non-CIP applicable, EACMS/PACS with BCS, Low/Medium/High BCS, EACMS/PACS with non-CIP applicable, etc.).
- SDT evaluated a number of example scenarios



Virtualization Risks

- Many viewpoints on security risks associated with virtual infrastructure
  - Work developed by the NERC Project 2016-02 SDT
  - Threats outlined in NIST 800-125A
  - ISACA Article on Auditing Virtual Systems
  - Cloud Security Alliance

Threats to Virtualization – NIST 800-125A

- Breach of Process Isolation - VM Escape (HYP-T1): Major threats to any hypervisor come from rogue VMs. Rogue VMs manage to subvert the isolation function provided by the VMM/hypervisor to hardware resources such as memory pages and storage devices. In other words, the rogue or compromised VMs may access areas of memory belonging to the hypervisor or other VMs and storage devices they are not authorized to access. Possible reasons for this threat include (a) hypervisor design vulnerabilities or (b) malicious or vulnerable device drivers. Potential downstream impacts of a rogue VM taking control of the hypervisor include the installation of rootkits or attacks on other VMs on the same virtualized host.
- Breach of Network Isolation (HYP-T2): Potential threats to isolation include attacks such as IP or MAC address spoofing by a rogue VM and Traffic Snooping, or the interception of virtual network traffic, intended for a VM on the same virtual network segment. The impact of the subversion of these network controls is loss of confidentiality. Some VMs will be viewing information for which they are not authorized.
- Denial of Service (HYP-T3): Misconfigured or malicious VMs may be consuming a disproportionately high percentage of host resources, resulting in denial-of-service to other VMs on the hypervisor host.

Additional Research…2011 ISACA Article titled “Auditing Security Risks in Virtual IT Systems”

Breaks virtualization risk down into 3 categories

https://www.isaca.org/Journal/archives/2011/Volume-1/Pages/Auditing-Security-Risks-in-Virtual-IT-Systems.aspx

Architectural Vulnerability - ISACA

- The layer of abstraction between the physical hardware and the virtualised systems running the IT services is a potential target of attack. Just as the guest OS is subjected to the same security risks as a physical system, security measures (e.g., antivirus agents, spyware filters, IDs) should be installed on all VMs.

  Architectural vulnerabilities can be addressed in the following ways:

  - Vulnerability analysis—An architectural vulnerability analysis can be conducted by comparing current system attributes to a reference set that consists of valid system samples and noting the differences between the two sets. Immediate follow-up on the differences helps to make the architecture more robust and secure.
  - Regular updates of security features on VMs—All security measures should be kept up to date.
  - Proper patch management on VMs—VMs should be properly patched and monitored by the IT staff. Proper patch management should be performed regularly for all VMs including those in suspended or off status.
  - Implementation of network best practices—A VM or a group of VMs connected to the same network can be the target of network attacks from other VMs on the network. Network best practices should be applied to harden the network interfaces of the virtual machines. Network segmenting of VMs can be performed to mitigate the risks of various types of network attacks. The trust zones can be separated by using physical security devices.

Software Vulnerability - ISACA

- The most important software in a virtual IT system is the hypervisor. Any security vulnerability in the hypervisor software will put VMs at risk of failure. The following steps are necessary as precautionary measures against software vulnerabilities:
  - Prevention of single point of failure—The pervasive attribute of the hypervisor across all virtual hosts will be a cause of concern if a malicious code compromises one hypervisor instance. A single instance of replicating malware can rapidly exploit all hypervisors in the networked IT environment, thus causing a single point of failure.
  - Hypervisor updates—The hypervisor software should be regularly updated with available patches to get rid of security weaknesses.
  - Controlled access to VMs—Proper lockdown of privileges should be performed, and controlled access to virtual environments should be ensured to reduce code exploitation through malicious software.
  - Security of the host OS—The virtualisation layer resides on the host OS, so the utmost care should be taken to ensure that the host OS is not compromised by virus attacks.
  - Organisational policy for VM security—A policy-based security model for hypervisors and the host OS should be applied from an organisational level.

Configuration Risks - ISACA

- Due to the ease of cloning and copying images, a new infrastructure can be deployed very easily in a virtual environment. This introduces configuration drift; as a result, controlling and accounting for the rapidly deployed environments becomes a critical task.

  Configuration risks can be mitigated with the help of the following steps:
  - Configuration assessment—A periodic configuration assessment should be performed to achieve a known and trusted state of the virtual environment.
  - Hypervisor configuration checks—The integrity of the hypervisor configuration should be checked periodically to mitigate risk and to increase operational efficiency of the virtual IT system.
  - Authorisation and proper documentation of change— Changes to the VMs can be done instantly per need, but all such changes should be authorised and properly documented. Undetected and unauthorised changes to the VM configuration can introduce security breaches and can make the system noncompliant to organisational and regulatory standards.
  - Configuration audit and control—Implementing a proper configuration audit and control solution to the VMs can ensure environmental stability and prevent unexpected threats to the virtual IT system and the business. Configuration risks can be mitigated by regularly checking the configuration of components against defined standards.
  - Approved templates for VM deployments—There should be templates for VM deployments, and any change to the standards should be studied and approved before implementation.
  - Event monitoring—All events on VMs should be monitored using server host logs. Active-state monitoring of configuration changes to hosts, VMs, clusters, resource pools, data stores and virtual networks should be implemented.
  - Configuration management database (CMDB)—A CMDB should be maintained with the proper description of the infrastructure. The CMDB should have information about the location of the images of suspended VMs and the physical-to-virtual mapping.

Risk analysis work done by the SDT in consideration of research

(See Word Document)

Options to move forward:

- Option 1: Conclude that modifications are unnecessary
  - Option 1a: Hand off to a separate working group/committee to draft best practices/whitepaper/guidelines/etc. as they see fit
- Option 2: Modify requirement(s)/definitions
- Option 3: Write new requirement(s)/definitions
  - Option 3a: Develop CIP-015
  - Option 3b: Add new requirements to existing standards
- Option 4: Draft Implementation Guidance
- Option 5: Request outside group/committee to do a study on virtualization before proceeding with standards development