NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program
Mixed Trust Authentication Environments

Version: September 8, 2015

This document is designed to convey lessons learned from NERC's various CIP version 5 transition activities. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Purpose

The purpose of this Lesson Learned is to provide guidance related to steps Responsible Entities can take to consider mixed trust authentication environments and the effort required to comply with requirements of the CIP version 5 standards. A mixed trust authentication environment refers to a security architecture where a BES Cyber System shares an authentication mechanism with a non-BES Cyber System. While mixed trust authentication environments are not prohibited by the CIP version 5 Reliability Standards, such environments increase the effort required for a Responsible Entity to comply with the standards, as discussed below.

Background

BES Cyber Systems and non-BES Cyber Systems that share an authentication mechanism (e.g., RADIUS servers, Active Directory servers, certificate authorities), are considered to be a mixed trust environment (i.e., a single platform authenticates and/or authorizes access for multiple zones with different security levels).

Nothing in the CIP version 5 Reliability Standards prohibits a Responsible Entity from implementing a mixed trust environment and using an access control server to authenticate access to an Electronic Security Perimeter (ESP) or a BES Cyber Asset as well as non-BES Cyber Assets. If, however, a Responsible Entity chooses to use a single implementation to perform the access control function to an ESP or BES Cyber Systems, the servers, by definition, become Electronic Access Control and Monitoring Systems (EACMS) associated with one or more BES Cyber Systems.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

An EACMS is defined in the NERC Glossary of Terms as follow:

> ***Electronic Access Control or Monitoring Systems (EACMS)*** – Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

The Background section of Reliability Standard CIP-002-5 provides examples of an EACMS, such as Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, certificate authorities), security event monitoring systems, and intrusion detection systems.

All of the following Reliability Standards have one or more requirements applicable to an EACMS associated with medium impact or high impact rating BES Cyber Systems: CIP-003-5, CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1. It is important to evaluate the Applicable Systems column for each requirement within the standard to ensure that appropriate controls have been applied to any Cyber Asset performing the function of an EACMS.

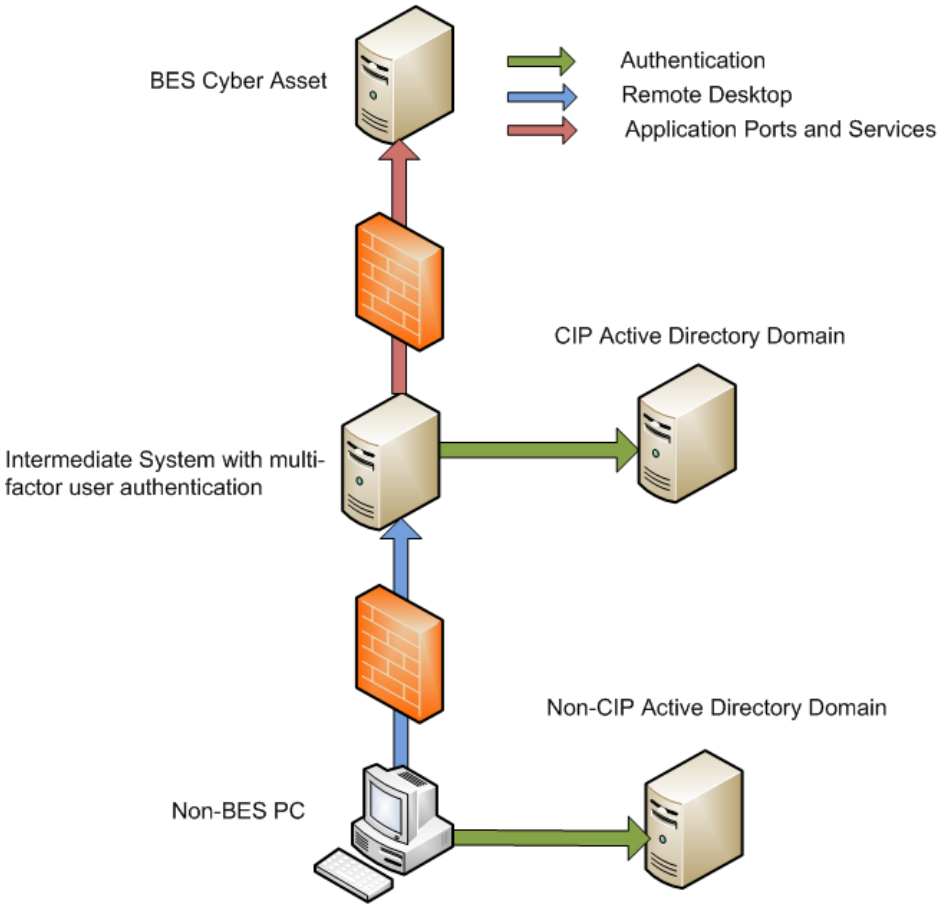
Approach

Based on the effort required to ensure all of the applicable controls had been applied to the EACMS in a mixed-trust environment, one of the Study Participants in NERC's CIP Version 5 Implementation Study decided to create a separate Microsoft Active Directory forest to authenticate access to BES Cyber Systems. By adopting this approach to avoid a mixed trust environment, the Responsible Entity was able to significantly reduce the effort required to manage an Active Directory forest used to authenticate users to both BES Cyber Assets as well as non-BES Cyber Assets.

The diagram below illustrates the two separate trust environments. First, the user authenticates to their non-BES PC as usual. The user then initiates an encrypted remote desktop session to the Intermediate System where multi-factor authentication is enforced by the dedicated CIP domain. Once the user is authenticated at the Intermediate System, only then is the user permitted to access the BES Cyber Assets inside of the ESP.

By taking this approach, the Responsible Entity was able to leverage existing controls and infrastructure in place to meet the CIP version 5 standard requirements listed above while reducing the effort required to protect the Cyber Assets that had no role in authenticating users to BES Cyber Assets inside of the ESP. .

Figure 1: Non-mixed Trust Authentication



When designing authentication schemes using Active Directory, Responsible Entities may also consider a forest with both CIP and non-CIP domains. For example, a Responsible Entity might have a distribution systems domain (i.e., Cyber Assets that ***are not*** BES Cyber Systems), as well as a transmission substation domain (i.e., Cyber Assets that ***are*** BES Cyber Systems), both of which reside in the same forest in order to take advantage of shared resources at the forest root (e.g., anti-malware, security updates), but do not have the same compliance requirements. A forest can include CIP and non-CIP child domains provided the root domain is afforded all the controls required for an EACMS. It should be emphasized that if authorization for resources between the CIP and non-CIP child domains is allowed to occur, the non-CIP domain would be brought into scope for CIP compliance.

Mixing CIP and non-CIP domains under a common forest increases the complexity and effort required to protect the assets and demonstrate compliance with the CIP version 5 standards.