Survey on Standards to Harden Security of PC-Based Systems for Nuclear Facilities

Chaechang Lee* and Soomin Lim

Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea

*chiching@kinac.re.kr, s2min@kinac.re.kr

1. Introduction

As cyber attack technique evolves, various devices and software are developed to prevent the attack. However, no matter how advanced the security technology is, it is difficult to introduce and utilize it in systems that operate nuclear power plant. Before introducing security equipment into existing systems, design changes are needed and the impact on the operation of the plant, such as an increase of latency and response time, should be considered. Compatibility with the security software should also be considered.

In this paper, we will discuss the standards for enhancing security by using security configurations of existing operating systems of PC-based nuclear facilities, which are difficult to install security software and deploy security equipment.

2. Standards on Security Configurations

2.1 FDCC

The Federal Desktop Core Configuration (FDCC) is a list of security settings recommended by the National Institute of Standards and Technology for general-purpose microcomputers that are connected directly to the network of a United States government agency [1]. From March 2007, the US Air Force had applied the FDCC, which is the predecessor of the United States Government Configuration Baseline (USGCB), to Windows XP version. Currently, the USGCB has been replaced with Windows 7 to maintain the organization security configurations.

2.2 USGCB

USGCB is intended to provide federal agencies with guidance on best practices for configuring information protection [2]. It aims to enhance system security by reducing costs and increasing efficiency through standardization of IT systems to address security threats that have yet to be discovered. In other words, it recommends the secure security settings of all PCs used by federal agencies to protect hosts within federal agencies from various cyber threats. Security settings, such as access privilege restrictions, can be used to reduce the risk of operating system vulnerabilities by applying the standard that are stricter than the default security configurations of the supplied PC.

The USGCB, which adds Windows Vista, Windows 7 and RHEL 5 setup to FDCC, has been patched more than 39 times and also provides security configurations for Internet Explorer 7 and 8 versions.

2.3 CCE

The Common Configuration Enumeration (CCE) is intended to provide a unique identifier for security-related system configuration by quickly and accurately associating configuration data from

various information sources and tools [3]. While the USGCB is a set of security enhancement items for specific operating systems, the CCE defines security enhancement items from servers to applications such as Apache and Internet Information Services (IIS). The project was started at MITRE and is now managed by NIST.

2.4 NIST 800-53

The NIST Special Publication 800-53 standard provides a list of security controls for the US federal information system [4]. It addresses the steps in the risk management framework dealing with security control choices for federal information systems in accordance with the security requirements of the Federal Information Processing Standard (FIPS). The fifth revised version, Security and Privacy Controls for Information Systems and Organizations, is now available as a draft on August, 2017.

The US Nuclear Regulatory Commission (NRC) regulates nuclear licensees with Regulatory Guide (RG) 5.71, Cyber Security Programs for Nuclear Facilities, which is including all controls designated as the “High” baseline within the third revised NIST 800-53.

3. Conclusion

In this paper, we discussed standards to harden security of PC-based systems by using its own security configurations. Since digital computer and communications systems and networks in nuclear facilities have restrictions to install security software and to deploy security equipment, nuclear licensees should utilize their own security configurations.

In the next study, we will try to verify the effectiveness of the security configuration enhancement presented above by attempting cyber attacks using known vulnerabilities to the hosts to which the security configuration enhancement items are applied and to the hosts that are not applied.

REFERENCES

[1] Wikipedia, “Federal Desktop Core Configuration”, https://en.wikipedia.org (accessed April 9, 2018).

[2] NIST, “United States Government Configuration Baseline, https://csrc.nist.gov (accessed April 9, 2018).

[3] CCE, “Common Configuration Enumeration (CCE)”, https://cce.mitre.org (accessed April 9, 2018).

[4] NIST, “Security and Privacy Controls for Information Systems and Organizations”, SP 800-53 (2017).