A Study on the Effectiveness of Technical Security Controls for Nuclear Facilities Using STRIDE threat model

Lee Chae-Chang, Kim Sang-Woo
Korea Institute of Nuclear Non-proliferation and Control
chiching@kinac.re.kr, kjoey@kinac.re.kr

1. Introduction

The NRC (Nuclear Regulatory Commission) has regulated U.S. nuclear licensees with 10 CFR (Code of Federal Regulations) Section 73.54, named "Protection of Digital Computer and Communication Systems and Networks" [1]. The NRC also published RG (Regulatory Guide) 5.71, "Cyber Security Program for Nuclear Facilities", which requires all licensees to implement security controls to address potential cyber security risks [2].

70 Technical Controls composed of access controls, audit and accountability, system and communications protection, and identification and authentication are developed by the NRC selecting requirements from other standards, along with Operational and Management Security Controls. If nuclear licensees cannot implement a technical security control with any reasonable reasons, they should prepare alternative controls and perform the attack vector and attack tree analysis for a CDA (Critical Digital Asset) to evaluate whether the measures provide the same or greater protection as the corresponding security control. If an attack vectors of one or more specific security controls for a CDA does not exist and demonstrated as a result of the analysis, the licensees can obviate the controls [2].

In this paper, tables of security threats for nuclear facilities are presented to correspond the threats from Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) model to all Technical Security Controls listed in RG 5.71 except 4 related Policy and Procedures [3]. Cyber security teams of the licensees can leverage the tables in this study to perform an attack vector and attack tree analysis of the technical controls and for their CDAs.

2. Technical Controls Corresponding security threats using STRIDE methodology

Microsoft grouped security threats into six categories: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE). Rahat Masood listed cyber security threats that can happen in I&C systems and broke them down into the categories using STRIDE model [4]. Figure 1 shows the hierarchy of the threats.

This chapter presents tables to show the technical security controls required by RG 5.71 and the corresponding STRIDE threats to be addressed by the measure. In the tables, '○' mark indicates the main purpose of the control to protect from the corresponding threats and '△' mark means its additional security effect of the control that can help to mitigate the risk from the corresponding threats.

2.1. Access Control

The access control policy requires licensees to provide high assurance that only authorized individuals, or processes acting on their behalf, can access CDAs and perform authorized activities [1]. RG 5.71 addresses Table I of technical controls for access control except Access Control Policy and Procedures.

Table I: Access Controls to protect from STRIDE security threats

No.	Controls	S	T	R	I	D	E
2.1.2	Account Management	○					△
2.1.3	Access Enforcement						○
2.1.4	Information Flow Enforcement		△		△	△	
2.1.5	Separation of Functions						○
2.1.6	Least Privilege						○
2.1.7	Unsuccessful Login Attempts	○					

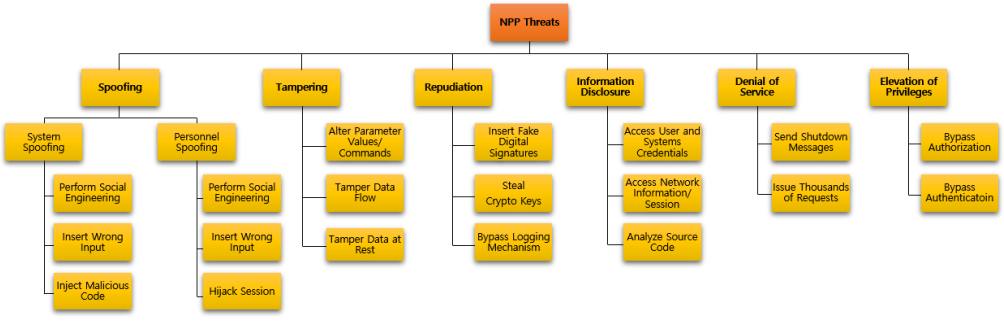

Fig. 1. Nuclear Power Plant I&C Systems Threats Hierarchy [4]

2.1.8	System Use Notification			○			
2.1.9	Previous Logon Notification	Δ		Δ			
2.1.10	Session Lock	○					
2.1.11	Supervision and Review - Access Control	Δ		○			
2.1.12	Permitted Actions without Identification or Authentication						○
2.1.13	Automated Marking				○		
2.1.14	Automated Labeling				○		
2.1.15	Network Access Control	○					
2.1.16	"Open/Insecure" Protocol Restriction		Δ			○	
2.1.17	Wireless Access Restrictions	○	Δ				
2.1.18	Insecure and Rogue Connections	○			Δ		
2.1.19	Access Control for Portable and Mobile Devices	Δ	Δ	Δ	Δ	Δ	Δ
2.1.20	Proprietary Protocol Visibility	To detect an attack on a critical system					
2.1.21	Third Party Products and Controls	To resolve or mitigate vulnerabilities continuously					
2.1.22	Use of External System	○	Δ				

In table I, the control of Wireless Access are required to implement defense-in-depth strategy of ICS network.

2.2. Audit and Accountability

Technical controls on audit and accountability for nuclear licensees to protect from security threats are listed in Table II.

Table II: Audit and Accountability to protect from STRIDE security threats

No.	Controls	S	T	R	I	D	E
2.2.2	Auditable Events		Δ	○			
2.2.3	Content of Audit Records		○	○			
2.2.4	Audit Storage Capacity			○			
2.2.5	Response to Audit Processing Failures		Δ	○			
2.2.6	Audit Review, Analysis and Reporting			○			
2.2.7	Audit Reduction and Report Generation			○			
2.2.8	Time Stamps			○			
2.2.9	Protection of Audit Information		○	○			
2.2.10	Non-Repudiation			○			
2.2.11	Audit Record Retention			○			
2.2.12	Audit Generation			○			

Table II shows that most of the controls are required to prevent from repudiation for security related incidents.

2.3. CDA and Communication Protection

To protect CDAs and communication of nuclear facilities, RG 5.71 regulates licensees with the controls in Table III and the technical controls are expected to provide the protection from STRIDE security threats.

Table III: CDA and Communication Protection with corresponding STRIDE threats

No.	Controls	S	T	R	I	D	E
2.3.2	Application Partitioning and Security Function Isolation						○
2.3.3	Shared Resources	Δ			○		
2.3.4	Denial of Service Protection					○	
2.3.5	Resource Priority					○	
2.3.6	Transmission Integrity	Δ	○				
2.3.7	Transmission Confidentiality				○		
2.3.8	Trusted Path	○					
2.3.9	Cryptographic Key Establishment and Management				○		
2.3.10	Use of Cryptography				○		
2.3.11	Unauthorized Remote Activation of Services	Δ			○		
2.3.12	Transmission of Security Parameter				○		Δ
2.3.13	Public Key Infrastructure Certificate	○					
2.3.14	Mobile Code	○					
2.3.15	Secure Name/Address Resolution Service (Authoritative/Trusted Source)	○	○				
2.3.16	Secure Name/Address Resolution Service (Recursive of Cashing Resolver)	○	○				
2.3.17	Architecture and Provisioning for Name/Address Resolution Service					○	
2.3.18	Session Authenticity	○	Δ		○		○
2.3.19	Thin Nodes				○		
2.3.20	Confidentiality of Information at Rest		Δ		○		
2.3.21	Heterogeneity/Diversity	To reduce the impact of exploitations of specific technologies					
2.3.22	Fail in Known State					○	

The control of Heterogeneity and Diversity are required to reduce the impact of exploitations of security attacks using specific technologies, so it does not purpose to respond against any STRIDE threats.

2.4. Identification and Authentication

RG 5.71 addresses Table IV of technical controls to nuclear licensees for Identification and Authentication.

Table IV: Identification and Authentication to protect from STRIDE security threats

No.	Controls	S	T	R	I	D	E
2.4.2	User Identification and Authentication	○					○
2.4.3	Password Requirements	○			Δ		
2.4.4	Non-authenticated Human Machine Interface Security		Δ	○			
2.4.5	Device Identification and Authentication		Δ	○			
2.4.6	Identifier Management			○			
2.4.7	Authenticator Management	○					
2.4.8	Authenticator Feedback				○		
2.4.9	Cryptographic Module Authentication				○		

2.5. System Hardening

Some of the controls of System Hardening are required to reduce the target surface area of CDAs by removing unnecessary functions that are potentially abused as vulnerabilities. Table V shows the technical controls that are expected to provide the protection from STRIDE security threats.

Table V: System Hardening to protect from STRIDE security threats

No.	Controls	S	T	R	I	D	E
2.5.1	Removal of Unnecessary Services and Programs	To reduce the target surface area of CDAs					
2.5.2	Host Intrusion Detection System	To provide detection and prevention capabilities for CDAs					
2.5.3	Changes to File System and OS Permissions		○				
2.5.4	Hardware Configuration	To reduce the target surface area of CDAs					
2.5.5	Installing OS, Applications and 3rd Party S/W Update	To reduce the target surface area of CDAs					

3. Conclusion

If nuclear licensees cannot implement a technical security control with any reasons that RG 5.71 requires, they should perform and document the attack vector and attack tree analysis for a CDA (Critical Digital Asset) to evaluate whether alternative controls provide the same or greater protection as the corresponding security control. This study is expected to help nuclear licensees who prepare reasonable alternative controls instead of the technical controls listed in RG 5.71.

REFERENCES

[1] U.S. NRC, Title 10 Code of Federal Regulations (CFR) Part 73, Physical Protection of Plants and Materials, 2016.
[2] U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[3] Microsoft Developer Network, The STRIDE Threat Model, http://msdn.microsoft.com/
[4] Masood, Rahat. Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives., Cyber Security and Privacy Research Institute, The George Washington University, Aug. 2016.