A Method to Derive Monitoring Variables for a Cyber Security Test-bed of I&C System

Kyung-soo Han, Jae-Gu Song, Joung-Woon Lee and Cheol-Kwon Lee
Korea Atomic Energy Research Institute, I&C & HF Research Div.,
1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea
Corresponding author: ks-han@kaeri.re.kr

1. Introduction

As seen in the Stuxnet case, I&C systems cannot guarantee safety from cyber attacks against the state agency facilities. Although the level of response against cyber attacks is enhanced from design to operation, new kinds of cyber attacks may evolve continuously. Hence, it is necessary to develop automated monitoring techniques to understand intrusion attempts and already infected malicious behaviors.

In the IT field, monitoring techniques have been developed to protect the systems connected by networks from cyber attacks and incidents.

For the development of monitoring systems for I&C cyber security, it is necessary to review the monitoring systems in the IT field and derive cyber security-related monitoring variables among the proprietary operating information about the I&C systems.

Tests for the development and application of these monitoring systems may cause adverse effects on the I&C systems. To analyze influences on the system and safely intended variables, the construction of an I&C system Test-bed should be preceded.

This article proposes a method of deriving variables that should be monitored through a monitoring system for cyber security as a part of I&C Test-bed. The surveillance features and the monitored variables of NMS(Network Management System), a monitoring technique in the IT field, were reviewed in section 2. In Section 3, the monitoring variables for an I&C cyber security were derived by the of NMS and the investigation for information used for hacking techniques that can be practiced against I&C systems.

2. Review of NMS Monitoring Technique

The network management system in the IT field is a central detection system to operate devices organized by the network safely and efficiently. To monitor the devices and any failures on the network, it conducts five major functions classified as configuration management, fault management, performance management, accounting management and security management.

Form analysis of the monitoring variables corresponding to the administrative features of NMS Table 1can be obtained as below.

Table 1. Monitoring variables corresponding to the administrative features of NMS

management	Monitored Variables of NMS
Fault	Device contact lost, ups power error, ups battery error, Link failure, Port Status error information etc..
Accounting	disk use rate, process overload, execution priority of application, main memory use rate, Application's memory use information, Use rate of the application processor, etc…
Performance	Offered load, packet rate, error rate, discard rate, load_in/out, packet rate in/out, error rate in/out, discard rate in/out, etc…
Configuration	Configuration map, device / add / remove / location / address change information, device topology, system application s·w information, etc..
Security	Passwords and encrypted data link security behavior/Maintenance Records Information, etc..

Like this, the administrative features of the NMS may be used as an interface function that can integrate and manage the variables monitored relative to I&C cyber security.

3. Expected Monitoring Variables for I&C Cyber Security

To obtain monitoring variables for an I&C system cyber security test-bed, the variables used for hacking techniques and malicious behaviors that could be exercised in I&C systems were analyzed. The variables from this analysis were compared to the monitoring variables of NMS and classified into the variables related to cyber attacks.

3.1 Expected Monitoring Variables through Hacking Attacks

In general, hacking consists of the understanding of the network organization that can be acquired through the process of collecting information, the discovery of vulnerabilities residing in the system, the acquisition of the administrator's authorization and approaches to important data inside the system.

To recognize this hacking attack, the information infringed by the hacking and the section in I&C systems where attempts of hacking can be expected were classified. The results of this classification for an example I&C system can be summarized as Table 2.

Table 2: Expected hacking attacks and hacking test section

Attacks	Expected range	Behavior
Vulnerability scanning	EWS, PT Tool to PLC	Scan open port, Memory dump crack Etc..
Password attacks	EWS, PT Tool to PLC	Account access crack, enter t Encrypted connection port attack, value using the debugger seized Etc..
Spoofing	MTP to PLC, PLC to MTP	Address Resolution Protocol cache memory modulation Etc..
Sniffing	MTP to PLC, PLC to MTP	Host status of the ethernet interface in promiscuous use. Etc..
Denial of Service	EWS to PLC	Randomly generate a large amount of packets Etc..
Etc..	Etc..	Etc..

A hacking technique attempts a direct attack after approaching to the critical digital assets of I&C systems. Over 90% of these hacking incidents are caused by malicious codes. Since 2millions of new malicious codes are reported per day on average, it is very difficult to analyze the behaviors of malicious codes. Yet, the typical malicious behaviors may be classified as follows:

-Virus: Infection in the file unit
-Worm: Self- replicating and spread in the network
-Boat: Program that enables remote control
-Root-kit: Attempt to acquire administrator's authorization and change of the system
-Backdoor: User authentication bypass
-Malware: Key-logger, adware and spyware

hacking and malicious acts can form monitoring variables The above types of cyber attacks should be updated continuously in the future with the emergence of new hacking techniques and malicious codes.

3.2 Derivation of Variables Monitored for I&C Cyber Security

As a result of a comparison between the variables monitored in the NMS and the information used for hacking attacks, it was found that the variables of two groups are very similar. Among the variables monitored in the NMS, the items with a possibility of falsification by a hacking attack and all of the information used by the hacking attack should be treated as monitoring variables for I&C system cyber security test-bed.

The monitoring variables derived in this way may be used as vulnerability test data in constructing an I&C Test-bed.

The information used for hacking attacks is the very variables monitored. Yet, the biggest reason for the comparison with the NMS variables is to classify them into the administrative features of the NMS since it is necessary to manage the derived variables efficiently.

Each administrative feature should share the monitoring variables with each other and should be implemented so as to facilitate tracking when an incident takes place.

Table 4 shows a summary of the monitoring variables derived for a I&C cyber security test-bed classified into the administrative features of NMS.

Table 4 I&C Cyber Security Variables Classified into Administrative Features

Management	monitored variable of I&C CDA
Fault	Processor memory error, CPU related error, Communication module failure, the start time of the run violation error, the execution cycle, the communication module error, system error, etc..
Accounting	CPU usage, memory usage, and program execution information, the file attempts to access information, and program execution information, etc..
Performance	Application size, response time, throughput, Task using / delete / run information, file access information, etc..
Configuration	The system identification information, communication, identification, origin / destination address value, information, communication DATA, etc..
Security	OS security-related information, password information, data encryption information, etc..

4. Conclusions

The monitoring variables of NMS in the IT field and the information about the malicious behaviors used for hacking were derived as expected variables to be monitored for an I&C cyber security research.

The derived monitoring variables were classified into the five functions of NMS for efficient management.

For the cyber security of I&C systems, the vulnerabilities should be understood through a penetration test etc. and an assessment of influences on the actual system should be carried out. Thus, constructing a test-bed of I&C systems is necessary for the safety system in operation.

In the future, it will be necessary to develop a logging and monitoring system for studies on the vulnerabilities of I&C systems with test-beds.

Acknowledgement

This work has been supported by a grant from the Korea Ministry of Strategy and Finance.

REFERENCES

[1] Lee, J. W., Song, J. G., Lee, C. K., & Lee, D. Y. A Conceptual Framework for Securing Digital I&C Systems in Nuclear Power Plants. *the international conference on security and management(SAM12)2012..*

[2] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, June 2011.

[3] RFC1157 Simple Network Management Protocol(SNMP).