International Journal of Engineering & Technology, 7 (3.33) (2018) 165-167

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The Study on the Risk Response of Security Cyber Physical System (Focusing on Analysis of Security Access Log and Unstructured Data)

JangMook KANG*, CheolHee YOON, TaeHyeong KWON*****

** Department of Big-Data Industrial Security, Namseoul University, Cheonan city 31020, Korea,*
***Police Science Institute, Asan, Korea*
****Police Science Institute, Asan, Korea*
***Corresponding author E-mail:bertter@police.go.kr*

Abstract

Malicious hacking is evolving continuously malicious code attacks. It needs flexible solutions such as the prevention leakage of personal information, demanding the ability of institutions to prevent high level of infringement. But, typical simple's security control system is limited by responding only to the tertiary industry equipment in the ICT field. A CPS type security system is capable of responding to the transition from ICT to AI which is should be applied. This is time of reorganization from the current security domain to the artificial intelligent ICBM device, it should apply the digital twin model which we are considering the people and environment of CPS type system. In this paper, we have studied a model of how cyber - physical systems can be implemented using existing security system platform technology. We also propose a new security technology applying model through analyzing log form of security equipment that has occurred for many years.

Keywords: *Malicious hacking, Cyber Physical System. Digital Twin*

1. Introduction

Artificial intelligence-based fourth-generation industrial security is different from the third-generation industry in which uniform data was produced from a single system in the past. Security begins from where we connect the cyber world to the physical world of the real world. It is necessary to protect the devices and people connected to the Internet from the facilities related to the data of the cyber world connected with the physical space of the real world. It has changed to a security new paradigm that includes artificial intelligence that requires not only the existing data protection but also the safety of people and environment.[1] In order to cope with the change, we propose a new technology that constructs information security simulation by grasping various security threats on existing concept. Cyber-physical systems are also being researched and classified into areas such as resiliency, privacy, malicious code attack, and intrusion detection in the field of cyber security. At the same time, we are working to solve uncertainties in real environment such as system control field, hybrid model field, real-time middleware field, software verification field.

In this paper, we confirmed the applicability of CPS based technology in specific cyber security field and proposed a method to construct honey-pot security configuration as digital twin. In addition, autonomic computing for cyber security risk is configured using a complex system in which a physical system having sensors and actuators and computing systems controlling the same are interlocked. We considered CPS cyber risk response system, which is managed, coordinated, and controlled by the system itself and finally integrated.

2. Security Log Analysis for Cyber Physical System Application

Generally, security logs generated from security devices are analyzed by individual devices or through integrated analysis system. Full log management has difficulties in data processing, retrieval, analysis, and visualization due to technical constraints, capacity limitations, and error detection. The purpose of this study is to propose a cyber physical system based risk response platform model that enhances security of equipment through analysis of security log collected through honey-pot.

we suggest that technology and security technology through digital twin for service which is data storage space, high-performance collection processing, data analysis engine, search engine that can search quickly, technology to express analyzed data. [3].

2.1. Pro-Actively Diagnose through Existing Security Platforms

Table 1: Threat classification of Attempted Infringement[3]

rank	Target classification	Attempted infringement by port	Throughput
1	Injection	443	23,011T
2	Defects in authentication and session management	11201	18,126t

3	Cross-site script	11202	13,417T
4	Directly referencing unsafe objects	5489	11,795T
5	Incorrect security settings	58101	6,752T

The data collected through the integrated security log analyzing equipment monitors the end-to-end threat in real time, collecting state information of server and equipment, external intrusion information from security equipment, and traffic information from the end terminal.

After that, the intruder's path, the analysis of the invasion pattern, and the current invasion state can be accurately informed, thereby reducing the risk and making the diagnosis possible. The log data generated by the security device is generally a Syslog data type, and the data is collected using the TCP or UDP standard protocol and stored at high speed in the analysis platform. The integrated security log monitoring solution that is already built uses a method of analyzing a large amount of security log using a relational database existing in itself and Collecting legacy system business data. In the case of security log equipment using the Big Data Platform, file storage generally uses file system based Hadoop to store data in blocks of 64 MB. The Ring-Node logically configures through the DataNode server where the data is stored, then The DataNode server acts as a data store. With Hadoop's replication capabilities, we use automatic backups store and analyze data in anunnecessary passivity ways.[2]

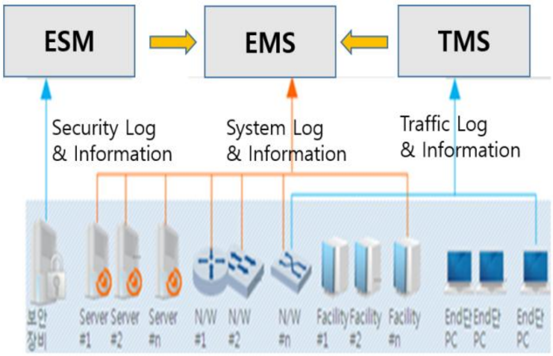

Figure 1: Pre-Diagnostics of Big Data [2]

2.2. Review of Existing Attacks based on Security Log

In this study, we analyze cyber threats collected by constructing a honeypot as an experimental environment for collecting security logs. Hacking and viruses have been identified as an integrated worm virus and attack. Infringement have been attempted, it shows the results of the analysis based on the OWASP Top 10 of the international security standard from Table 1. Among the collected security logs, the most frequent vulnerabilities are injection, authentication and session management flaws, and cross site scripting. The honeypot is structured so that the policy can be effectively applied to the log based on the approach, It is easy to analyze attack attempts against physical devices because it is possible to change it to meet the security level required by users and uses on-premises method. After classifying the per-port infringement types for the collected Web services, we can construct a digital twin model for virtual IoT equipment, cloud equipment, and mobile equipment to be constructed in the future.

As a result, a log analysis of the threat of invasion attempts gathered at the honeypot enabled the implementation of the cyber-physics-based risk response system. It can be make the policy direction against the newly challenged infringement risk

3. Implementation of CPS Application Risk Response System

3.1. Application of Cyber Physics System

Hacking attacks in the online world do not rely on solely automated tools or simple scanning techniques, but attempt to attack in a social engineering way which people analyze their targets directly. It can be seen that it is constantly evolving and developing. Therefore, it is important to analyze the pattern of collected security logs to protect against infringement countermeasures, and it is also important to implement organizational defense strategy in CPS type. In order to do this, we need an integrated security log analysis rule, which is an existing response system, and an environment that combines reality and virtual simulation environment. In addition, various information such as Source IP, Port, Target IP, and Event should be configured as digital twin. It should be configured as a digital twin to determine the possible points of occurrence. By that standard, it is a method of analyzing an unusual occurrence pattern in comparison with a case in which a normal user generates an average traffic in a specific time period, it can be created Simulations of the real world and the virtual world.

For example, the table of infringement attempts logs can be used to measure how the events are related to each other on the basis of the keys for IP and Port so that the data can be recognized from the user's point of view. It is only necessary to reconfigure it to suit the newly introduced environment.

Table 2: Infiltration Attempt Log analysis[3]

Rank	Attack attempt	Blocking count	intrusion detections Number
1	Net-bios Scan	41637	41670
2	FTP Login brute Force	5441	7641
3	HTTP Sever buffer overflow	524	202105
4	PHP Arbitrary Code Execution	208	367
5	MS Multiple Products JPEG Processing Buffer overflow	12	18

Through the digital twin, it is possible to trace the prediction of the new introduction and the related real world by measuring the order of the security equipment in which the attacking IP occurred and the detection of the equipment.

3.2. Apply of Digital Twin

A digital twin is a virtual physics system that can represent a real system. It is a multi-physics and multi-scale system that uses physical models, sensors, and system history to accurately predict the current and future world of the system. The reason for applying digital twinning to cyber-security is that it is difficult to predict the outcome throughout the information security life cycle. A Cyber Information Security There is a need for the process of modeling the necessary elements by interacting with the surrounding environment in various ways. In other words, an abstraction model called a twin model is necessary to reconstruct ports, rules, data, and processes and simulate software virtualization instead of actual physical assets. [4]

Table 3: Digital twin mechanism

Classify	Contents
Virtual manufacturing	Reduce analog work by leveraging digital collaboration Rapid and repeatable manufacturing with 3D product models
Advanced technology	Creation of new solution prototype with laser-based 3D printer

	Accelerate production of next-generation parts
Sensing	Sensors mounted on the instrument collect data Unexpected downtime prevention and increase productivity
optimization	Data-driven of maximum productivity and efficiency Real-time optimization of human processes, robot-based tasks

The digital twin fundamentally is divided into physical models of the physical world and virtualization models of the virtual world. It consists of real space physical assets, virtual space digital assets, and digital threads as components, and presents a physical and virtual integration model as shown in Table 4. [5], [6]

Table 4: Digital twin components

Classify	Component	Main technology
Physical world (Real model)	Real-world assets	Sensor data, metadata Condition (position, temperature), event (time series) data, analytics (algorithm, rule)
Virtual world (Virtualization model)	Digital Assets	Representing Digital Assets of Physical Assets VR Virtual Reality Connection Design, implement and test digital assets in virtual reality
	Digital Thread	The flow of data, the product lifecycle of a digital twin Digitization of product design and testing
Integration	Unified Repository	Linking Physical and Digital Assets From the real world to augmented reality, 2 ways connection Simulation, Control

It is possible to integrate the real world and the virtual world and simulate the real world. First, we use virtual simulation environment of digital twin based on numerical value of sensor, meta and condition data obtained in real world. Second You can get virtual results for the model you are modeling. third The result is the intersection of reality and virtual through an integrated repository. Finally, we can obtain the model and control values of the same conditions as the real world.

4. Conclusion

If you analyze and analyze the real case security log as data through dynamic system structure modeling that can predict the state, based on the results, it can be applied to real system. In this case, the system will have an effective effect preventing introduction maladjustment in terms of performance or environment. It is based on the simulation structure, the collected data continuously tracks and records the status to obtain information about the performance of the system. The dynamic system structure for predicting risk response state is as follows Figure .2 [7].

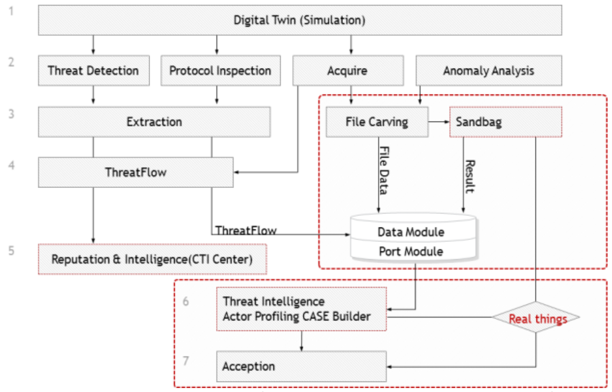

Figure 2: Response model of security cyber physical in cyber filed.

The collected data obtain information about the performance of the system continuously and tracks the status records in Digital Twin.

In this paper, As the digital twin accept the cyber security risk response system, Cyber filed can flexibly not only respond to new security threats, but also shortening the time required to respond to new security threats, error detections. We expected to have a positive security response effect. It wills him implementations of CPS-based digital security response system through digital twin.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.2018-0-00705, Algorithm design and software modeling for judge fake news based on artificial intelligence, No.2018-0-00440, ICT-based Crime Risk Prediction and Response Platform Development for Early Awareness of Risk Situation)

References

[1] Ju Hun-sik (2018). “A Study on ICT Security Change and CPS Security System in the 4th Industry Age”, Journal of Digital Contents Society, 19(2), p.294.

[2] Han Ki-hyoung, Jung Hyung-jong (2014). “A Study on implementation model for security log analysis system using Big Data Platform”, Journal of Digital Convergence 2014 Aug, 12(8), p352

[3] Kim Dong-kun, Han Ki-hyoung(2016). “ A case study of Physical security police proposals through the Security equipment log analysis in Public Educational Institution”, Korean Internet Information Society 17(1), p145,146

[4] Park Jung-min, Kang Sung- ku, Jeon In- chul, Kim Won-tae (2013). “Network-based autonomous control CPS”, The Journal of The Korean Institute of Communication Sciences 30(10), p86

[5] Kim Ji-yeon, Kim Hyung-jung, Kang Sung-ju (2014). “Development of a Real-time Simulation Technique for Cyber-physical System”, Journal of the Korea Society for Simulation, 23(4), p181-188

[6] Choi Jin-chul, Jang In-gook(2017). “System Design for Configuration Digital Twins in a Virtual environment”, Korea Information Science Society, 2017.12, p480,481

[7] Won Myung-gyu, Park Tae-joon, and Son Sang- hyuk (2013), “Present and Future of Cyber Physical System”, The Journal of The Korean Institute of Communication Sciences, 30(10), p66