International Journal of Engineering & Technology, 7 (2.33) (2018) 1243-1248

International Journal of Engineering & Technology

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

Research paper

A Design of Service Protocol Based Security Framework for ICT Convergence Industry Environment

Seong-Woo Lee[1], June-Kyoung Lee[2*], Kyoung-Hak Lee[3]

[1,2]NAONWORKS, 271 Digital-roGuro-gu Seoul , 08381, Korea
[3]IACFKwangWoon University,20 Kwangwoon-ro Nowon-gu Seoul, 01897, Korea
**Corresponding author E-mail: darkelan@naonworks.com*

Abstract

Background/Objectives: Numerous cyber security incidents in the field of ICT have become more intelligent and are being reproduced in the ICT convergence industry.

Methods/Statistical analysis: Convergence security technology targeting from domestic facilities such as electricity and transportation to household products such as TV and refrigerator have become necessary.It is necessary to develop security functions for each protocol layer that can detect and block threats in industries based on convergence security technology.Therefore, it is urgent to develop a security framework that enables developers to implement security functions easily and quickly at low cost.

Findings: This paper analyzes vulnerabilities of service-based protocols used in ICT convergence industry such as smart grid, smart factory, smart traffic, smart home, smart healthcare, etc., and proposes technologies that can detect and block security threats.we also defined protocol common security elements and designed a security modules for each protocol layer that contained them.In other words, we designed a service-oriented protocol security framework that enables the development of security functions easily and quickly in an open environment.It will be possible to develop a flexible and fast convergence security system in the ICT convergence industrial environment where various protocols are used by developing a framework structure in which protocol-independent security modules and protocol-specific security modules are separated.In addition, the overall security level of the ICT industry network can be improved by adding on the necessary security module on the system in operation. And In the field of industrial security, you can improve productivity by reusing each security module.

Improvements/Applications: Future research on the development of various ICT convergence industry control security systems based on the developed security framework will be carried out.

Keywords: *ICT Convergence Industry, Security Vulnerability, Security Measures, Service-Oriented Protocol , Security Framework*

1. Introduction

With the development of ICT, all industries are converged on the basis of ICT technology, and as the barriers between industries are collapsed, existing industries are being developed and accelerated to a smart convergence environment. In figure 1, industries such as finance, transportation, home, energy, factory, medical/health, and media are developing through the convergence with ICT. However, since many cyber security incidents that occurred in the existing ICT field become more intelligent and can be reproduced in the ICT convergence industry, there is a desperate need for convergence security technology to overcome this problem[1,2].

Convergence security refers to the convergence of physical security and information security, or security products and services that are created by combining security technologies with non-IT technologies. As ICT convergence industry spreads, convergence security technology that can overcome complexity and multi - channel security threat is needed. The technology should cover everything from major national facilities such as electricity, gas and transportation to home appliances such as TVs, washing machines and refrigerators. Based on this convergence security technology, it is necessary to design and develop a security function for each protocol layer that can monitor/detect/block service threats and infringements in various industrial fields. As a result, it is urgent to develop a convergence security framework that allows system developers to implement convergence security technology easily and quickly at low cost.

Section 2 of this paper analyses security threats that may be generated by convergence between ICT and traditional industry sectors, and proposes security technologies to overcome security threats. Section 3 describes the design and development of service-oriented protocol convergence security framework based on the proposed security technology. Finally, Section 4 summarizes the results of this paper and summarizes future research tasks.

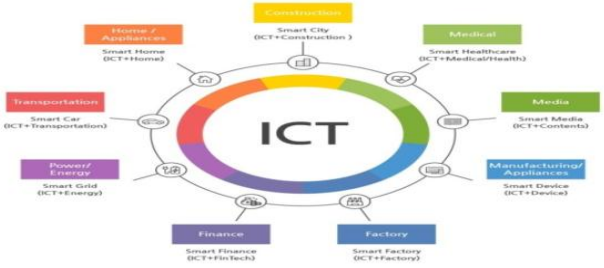


Figure 1:. ICT-based convergence industry

2. Security Vulnerability and Security Technology of ICT Convergence Industry

2.1. Security Vulnerability of ICT Convergence Industry

ICT is a technology developed in computer and network environments, which can lead to various security incidents based on bidirectional and open communication technology. Data firewalls targeting TCP / UDP packets have limitations in ensuring security[3, 4]. In the ICT environment, protocol security technology is mainly used as a security standard recommendation using TLS(Transport Layer Security). With the exception of transport layer security methods such as TLS, vulnerability analysis specific to protocol services and development of security technology to counter threats are insufficient. Currently, most commonly used security methods have no other alternative but Web firewalls. However, if the convergence industry service is activated due to the difficulty of responding to the weaknesses related to the ICT convergence protocol as the web firewall, various security threats are expected as follows.

- Cyber attack threatens control of industrial system
- Personal information leaked by transmission data hacking
- Threat of control of consumer use by abnormal external control
- National disasters such as blackouts

In this way, security threats from the nation to the individual have risks of social problems such as not only economic loss but also maximization of public anxiety. The following security threats may exist in the ICT convergence industrial environment, which features open and bi-directional communications.

- Unauthorized access from inaccessible users
- Port scanning to retrieve service ports
- Brute force attack for decryption
- Tapping service information
- Forging data that modulates normal data
- Denial of service attack that causes a large number of attack messages
- Session hijacking intercepting service connection sessions
- Open source security vulnerability attack
- Protocol message syntax errors and service flow attacks

In addition to the common weaknesses in the ICT convergence industry, it is necessary to analyze the vulnerability of each service protocol used in various ICT convergence industries. Service-oriented protocol security technology that can derive a security factor that matches protocol and service characteristics is needed. For example, in a smart grid environment, protocol security technologies such as openADR, SEP2.0, and DLMS / COSEM are required[5]. Also, protocol security technologies such as CoAP and MQTT are required in smart city environment[6, 7]. We summarizes the protocols required for service-based security technology used in ICT convergence industrial environments as shown in table 1.

Table 1: Protocols used in the ICT convergence industry

Industry Area	Protocol
Smart Grid	openADR 2.0a, openADR 2.0b, SEP 2.0, DLMS/COSEM
SmartFactory	Melsec, Modbus, Mitsubishi, PROFINET, LSIS XGI/XGT, DNP3, OPC-UA, BACNet/IP,OPC Classic, EtherCAT, Ethernet/IP
Smart Home	openADR 2.0a, openADR 2.0b, SEP 2.0, CAN, IEC61859, Modbus, DNP3, DLMS/COSEM
Smart City	HTTP, MQTT, CoAP
Smart Healthcare	IEEE 11073-20601, ANSI HL7
Smart Work	SIP, H.323, RTP/RTCP

2.2. Security Technology of ICT Convergence Industry

In an ideal ICT convergence environment, all service systems must transmit and receive secure and reliable data using a service protocol with security technology. Therefore, existing industries are based on closed and reliable networks and communicate with existing protocols that are not considered security at all. Convergence security technology is required to develop these previous industries into ICT convergence industry. The following presents the security technologies required in the ICT convergence environment to overcome the security threats mentioned in Section 2.1.

2.2.1Unidirectional Communication Technology

Unidirectional communication technology is a technology to overcome the security threat caused by connecting a closed network to an open two-way network. This technology uses non-routable communication technology without IP address using encoding / decoding technology, unidirectional encryption technology which encrypts transmission information so that it cannot be hacked, and transmission error Forward error correction (FEC) technology, retransmission technology in case of failure, and agent communication technology for unidirectional communication for communication between security non-security area systems.

2.2.2 DPI Filtering Technology

Since the Internet firewall system performs filtering based on the source / destination IP and the port information, the Internet firewall system has a vulnerability that cannot analyze payload contents including substantial protocol information. DPI(Deep Packet Inspection) filtering technology is a technology that detects the violation of the communication protocol by analyzing the internal contents of the packet[8]. In order to apply the DPI filtering technology to the protocols used in the ICT convergence industrial environment, the protocol standard should be analyzed in terms of packet structure analysis, parameter analysis, service flow procedure analysis, and service behavior pattern analysis. In addition, this technology is applied to all packets transmitted and received, and it should be accompanied by technologies for collecting and analyzing packets in real time, security profiling automation technology for various protocols, and filtering result storing and reporting techniques.

2.2.3 Self-Similarity and Correlation Analysis Technology

Like the Heinrich Law, "there is no accident without warning," the ICT convergence industry can detect cyber attack patterns that anticipate major accidents in advance. Applying self-similarity and correlation analysis techniques to all attacks will prevent large-scale security accidents in advance. This technology is based on statistical collection technology by packet, protocol, service stage and various monitoring period, statistical vector extraction technique which compares statistical data collected in the present and past, and the comparison of similarity through statistical vectors and the technique of correlation analysis algorithm.

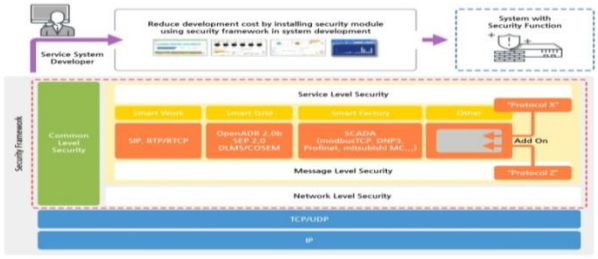
2.2.4 Service-Oriented Protocol Convergence Security Technology

Currently, protocol security methods in various industries use open architecture and general security methods through data

encryption. Therefore, there is a need for a service-oriented protocol security technology capable of dealing with a variety of hacking attacks that may occur in an open communication network by deeply analyzing attack vulnerabilities in protocol and service-specific aspects. Also, it is necessary to convert OPC-UA protocol, which is industry standard protocol for industry 4.0 protocol, without changing the installation of legacy protocol control systems used in existing industry[9]. It is possible to minimize the cost, time, and change in ICT convergence industry service construction and to provide OPC-UA protocol conversion function to secure the security of existing industrial control system that is not considered security and to integrate SCADA data in monitoring.

3. Service-Oriented Protocol Convergence Security Framework Design

In the same environment as a smart factory where more than a hundred kinds of protocols are used, service developers have relatively low experience of security function recognition and security technology. On the other hand, security solution developers are experiencing a gap in security area due to the diversity of service protocols to be supported and the rapid increase of organizations and companies demanding security requirements.



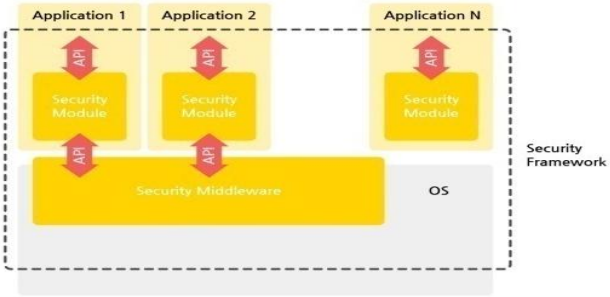


Figure 2:. Service-oriented protocol security framework

It is inefficient to develop security systems for each protocol in the ICT convergence industry and build a security system with them. In this paper, we developed a security framework that can secure security functions for various service protocols with more security functions. A framework is an environment that provides design and implementation of software functions in a form that can be reused to facilitate the development of software applications or solutions. In this paper, we define a security element common to protocols and design a layer-specific security module for each protocol including corresponding elements. We propose a service-oriented protocol security framework implemented as an API to easily and quickly develop security functions in an open environment.

In figure 2, the service protocol-independent security functions are divided into an information protection product common level security framework and a network level security framework. In addition, service protocol-specific security functions can be classified into a message level security framework and a service level security framework. The detailed functions according to each framework level are shown in table 2.

Table 2: Security function by framework level

Level	Security Function	Level	Security Function
Network	Network Traffic Attack Detection	Service	Service Threshold Detection
	Network Access Attack Detection		Service Flow Attack Detection
	Network DPI Detection		Service Entry Attack Detection
	Network Session Attack Detection		Service Session Attack Detection
Message	Message Syntax Error Detection		Service Behavior-Based Attack Detection
	Message ACL Detection		
	Message Parameter Threshold Detection		
	Message Forgery Attack Detection	Common	User Access Manager
	Message Signature Attack Detection		Integrity Supervisor
	Message Threshold Detection		System Resource Monitoring

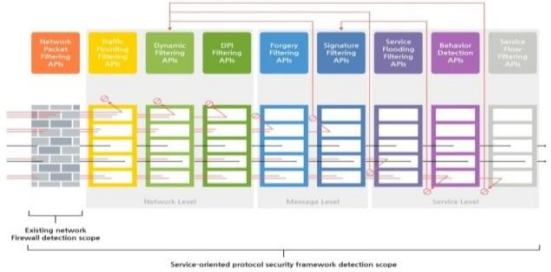


Figure 3:. Security framework functions &flow

In figure 3, the flow of security function execution through the security framework proposed in this paper can be confirmed through an example of network level security framework, message level security framework, and service level security framework detailed functions.

3.1. Network Level Security Framework

It is a framework that can be implemented as a middleware that performs security functions on packets received from the OS kernel level to the network. It uses API to communicate security software and application level security software, and performs security function of packet level to gather security policy, audit data and traffic monitoring result. It provides detailed functionality as shown in figure 4.

Figure 4: Network level security framework

3.1.1 Network Session Attack Detection

It monitors the state of the session between network nodes that send and receive traffic to and from each other. When a packet that violates the current session state is received between interworking nodes, it detects it as a session attack. This function detects abnormal packet attacks by monitoring TCP connection status, transaction status, and so on.

3.1.2 Network Traffic Attack Detection

It identifies interworking nodes and interworking services per protocol layer (L2 / L3 / L4) and monitors traffic based on the profile to detect traffic attacks. It performs a flooding detection function to monitor DoS and DDoS when a traffic threshold is exceeded using 5-Tuple delimiter. It also performs over-threshold detection of special packets such as GARP, ARP, ICMP, SYN, Broadcast MAC, Broadcast IP, and IP Segment.

3.1.3. Network DPI Detection

First, the interworking protocol for the traffic is identified and the packet structure is analyzed. And it performs traffic control and DPI attack detection according to the service right for the interworking node. It detects packet header DPI attack and packet payload DPI attack per protocol in payload, and detects DPI attack by function code, range, and value.

3.1.4 Network Access Attack Detection

It is the ability to detect all access to unauthorized attackers. It is divided into the following detailed functions.

- Access control based on IP / PORT of origin and destination
- Access control based on service address of origin and destination(domain, email address, etc.)
- Access control to network protocols except allowed protocols
- Access control based on national code(GeoIP)
- Access control based on White/Black List
- Access control based on Static/Dynamic List

3.2. Message Level Security Framework

Service protocol standard is analyzed and protocol parser is designed to provide security function related to protocol message.

3.2.1 Message Syntax Error Detection

Through the message parsing by protocol, it detects attack by monitoring abnormality of message syntax error, display format error, default parameter error, and parameter correlation error.

3.2.2 Message Parameter Threshold Detection

It is a function to detect attack by monitoring message length, parameter length, parameter range error, etc. for each protocol. Thresholds can detect attacks against minimum and maximum values and can be saved as profile data so that set values can be operated differently according to service system.

3.2.3 Message ACL Detection

It provides access control attack detection function through ACL on message type per protocol. It detects access control attack based on white/black list and static/dynamic list.

3.2.4 Message Forgery Attack Detection

It is a function that detects whether the message component is changed when communicating using the service protocol. It detects IP forgery, header order forgery, header value forgery, and so on.

3.2.5 Message Signature Attack Detection

It performs a negative signature attack detection function for detecting a message using a banned word for each protocol. Conversely, it also provides positive signature attack detection, which detects message that do not contain mandatory words.

3.2.6 Message Threshold Detection

It detects message thresholds for each protocol. It provides the ability to detect various threshold-exceeded attacks as 5-Tuple threshold, message type threshold, session threshold, etc.

3.3. Service Level Security Framework

By analyzing the standards for each service protocol, it provides the following security functions specialized for the service based protocol.

3.3.1 Service Threshold Detection

It is a function that detects an attack that exceeds a threshold of service resources, a threshold of service failure, or a threshold of abnormal behavior for each system providing the service. It detects attack that exceeds the threshold of an acceptable service interworking node, a threshold of an acceptable service entry, a threshold of a concurrent acceptable service session, a threshold of a service request to be attempted per second, a threshold of a service request failure and a threshold of a service abnormal.

3.3.2 Service Flow Attack Detection

It is a function to detect attacks that violate the defined service flow for each protocol. It provides the ability to detect attacks such as flow for service response without service request, flow for termination request for session other than service maintenance state, and flow for abnormal sequence service.

As shown in figure 5, it analyzes the service flow for all protocols and provides a function to detect an erroneous request and response situation as an attack.

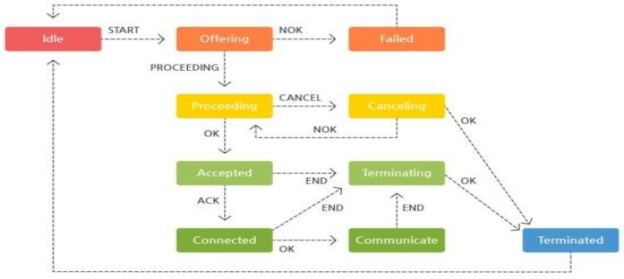


Figure 5: Service flow analysis sample

3.3.3 Service Entry Attack Detection

This function monitors the entry registration status of the service linked to each protocol. It is an ability to detect an attack, which is an abnormal registration of service status and an abnormal service request. It provides the ability to detect attacks such as service requests for unregistered entries, unregistered service requests for registered entries, and unauthorized registration change requests for registered entries.

3.3.4 Service Session Attack Detection

This provides the ability to detect attacks such as an abnormal termination request for a service session, an abnormal change

request for a service session,

3.3.5 Service Behavior-Based Attack Detection

This is a function that monitors behavior based attacks through analysis of service usage histories by protocol and detects attacks as abnormal behavior. It provides the ability to detect attacks such as an abnormally repetitive service request, an abnormally repetitive short session maintenance, an abnormally repetitive short time interval service request, and an unspecified number of service requests.

3.4. Common Level Security Framework

The service-independent security technologies such as the information security product common security requirement function required to be installed in national and public institutions are shown in figure6. This requires user access manager framework technology, *Integrity Supervisor* framework technology, and system resource monitoring framework technology.

3.4.1 User Access Manager

It is a function to judge and authenticate the administrator authority so that only allowed operation managers can access the system. This provides the ability to forcibly block connections in case of successive failures of authentication. It also provides a management access band identification and security function that identifies the network of the operating system requesting access and allows access only from the IP address for which access is permitted.

3.4.2 Integrity Supervisor

This function monitors key operational data and process integrity. It provides a security function to judge unauthorized operation attempts and tampering.

3.4.3 System Resource Monitoring

This function monitors system resources likecpu, memory, and data storage. As CPU and memory usage increases, APIs are used to enable upper-level applications to perform appropriate management. It also periodically monitors the free space of the storage where the system security audit data is stored. It provides storage management functions to prevent situations where there is insufficient data storage space to prevent audit data storage failures.

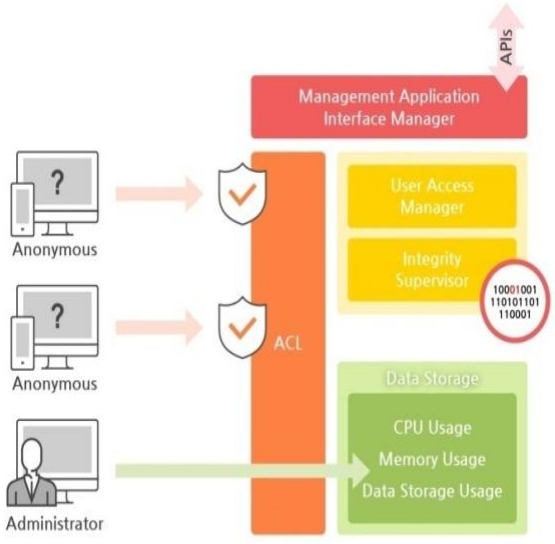


Figure 6:. Common level security framework

3.5. Analysis and Review of Security Framework

Currently, security systems used in the ICT convergence environment have no alternative but network and web firewall. General network-based firewalls allow network address-based security functions of interworking systems, but do not provide security functions for interworking service protocols. In addition, the general web firewall has similar security for HTTP, but REST-specific HTTP security technology does not exist. Therefore, it has a shortcoming as a security system for HTTP-based service protocol[10]. On the other hand, the standard security measures for various service protocols are defined by the organizations that published the standards, and they are mainly defined using the TLS-based transport layer security protocol. The security framework proposed in this paper not only includes existing network and web firewall security functions but also provides security functions specific to service-based protocols through analysis of service protocol messages and status monitoring as shown in figure 7.

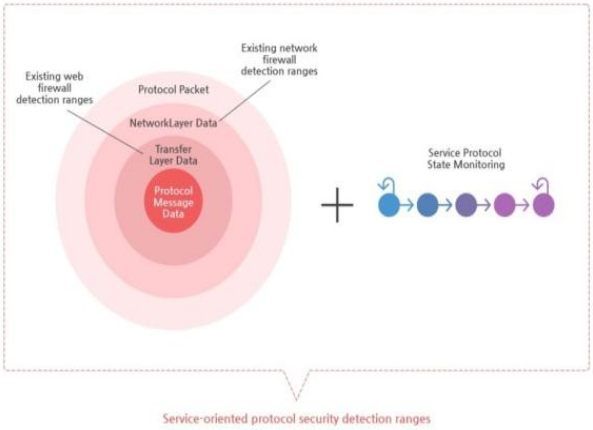


Figure7:. Core technology of security framework

4. Conclusion

In this paper, we analyze the complex and multi-channeled security vulnerabilities in the ICT convergence industry environment and propose the technologies to cope with these security vulnerabilities. In addition, we defined a security element common to protocols and designed a security module for each protocol layer including corresponding elements, and designed a service-oriented protocol security framework that allows for quick and easy development of security functions in an open environment. In the network environment where various protocols are used, applying the service - oriented protocol security framework proposed in this paper can provide a flexible convergence security system development environment in rapidly evolving networks. Future research on the development of various ICT convergence industry security systems based on the proposed security framework will be carried out.

Acknowledgment

This work was supported by the Korea Evaluation Institute of Industrial Technology(KEIT) grant funded by the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea(No. 10077303)

References

[1] Mohamed A.& Geir M. K. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 4(1), 65-88. doi: 10.13052/jcsm2245-1439.414.

[2] Isaac Ghansah. (2012). SMART GRID CYBER SECURITYPOTENTIAL THREATS,VULNERABILITIES AND RISKS(California Energy Commission No. CEC- 500- 2012- 047). Retrieved fromhttp://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf.

[3] Kristen Noakes-Fry. (2003). Firewalls: Technology Overview(Gartner GroupTechnology Overview DPRO-90318).Retrieved fromhttp://www.bus.umich.edu/kresgepublic/journals/gartner/research/90300/90318/90318.pdf.

[4] Web Application Security Consortium. (2006). Web Application Firewall Evaluation Criteria. Retrieved fromhttp://projects.webappsec.org/f/wasc-wafec-v1.0.pdf.

[5] openADR Alliance. (2012). OpenADR 2.0 Profile Specification B Profile. http://cimug.ucaiug.org/Projects/CIM-OpenADR/Shared%20Documents/Source%20Documents/OpenADR%20Alliance/OpenADR_2_0b_Profile_Specification_v1.0.pdf.

[6] Internet Engineering Task Force. (2014). The Constrained Application Protocol (CoAP). Retrieved from https://tools.ietf.org/html/rfc7252.

[7] OASIS. (2014). MQTT Version 3.1.1. Retrieved fromhttp://upfiles.heclouds.com/123/ueditor/2016/07/14/184e2dd5bc35bd9de59abc740665faac.pdf.

[8] Computer Science and Engineering Department, THAPAR University. (2009). Deep Packet Inspection in Linux Kernel Firewall. Retrieved fromhttp://dspace.thapar.edu:8080/jspui/bitstream/10266/862/3/862%20Vaibhav%20Bhadade%20%2880732004%29.pdf .

[9] Federal Office for Information Security. (2017). OPC UA Security Analysis. Retrieved fromhttps://opcfoundation.org/wp-content/uploads/2017/04/OPC_UA_security_analysis-OPC-F-Responses-2017_04_21.pdf.

[10] OWASP. (2017). OWASP Top 10 - 2017.Retrieved fromhttps://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.