JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 18, No. 5, pp. 1001-1008, Aug. 2017

산업제어시스템(ICS) 암호모듈 적용방안 연구

석 병 진 · 김 역 · 이 창 훈*
서울과학기술대학교 컴퓨터공학과

A Study on Application Method of Crypto-module for Industrial Control System

Byoungjin Seok · Yeog Kim · Changhoon Lee*
Department of Computer Engineering, Seoul National University of Science and Technology

[요 약]

산업제어시스템에 대한 사이버공격은 막대한 금전적 손실이나 인명피해로 이어질 수 있어 산업제어시스템 사이버보안에 대한 표준화 및 연구가 활발히 진행되고 있다. 이와 관련된 제도로 사회기반시설의 산업제어시스템은 전자정부법에 따라 검증필한 암호모듈을 탑재해야 하며 산업제어시스템의 보안요구사항에 맞는 적절한 보안통제가 실시되어야 한다. 그러나 운영계층, 제어계층, 현장장치 계층으로 구성되는 산업제어시스템은 보안통제 실시로 인해 각 계층별로 주요기능 수행에 문제가 발생할 수 있다. 본 논문에서는 이러한 문제 해결을 위해 산업제어시스템의 각 계층에 요구되는 보안요구사항에 대한 보안통제 수행에서 확인해야할 사항과 적절한 적용방안을 제시한다.

[Abstract]

Because cyber attacks on industrial control systems can lead to massive financial loss or loss of lives, the standardization and the research on cyber security of industrial control systems are actively under way. As a related system, the industrial control system of social infrastructures must be equipped with the verified cryptographic module according to the e-government law and appropriate security control should be implemented in accordance with the security requirements of the industrial control system. However, the industrial control system consisting of the operation layer, the control layer, and the field device layer may cause a problem in performing the main function in each layer due to the security control implementation. In this paper, we propose things to check when performing security control in accordance with the security control requirements for each layer of the industrial control system and proper application.

색인어 : 산업제어시스템, 암호모듈, 사이버위협, 주요기반시설, 산업제어시스템 보안요구사항
Key word : ICS(Industrial Control System), Crypto module, Cyber threat, Critical infrastructure, Security requirements for Industrial Control System

http://dx.doi.org/10.9728/dcs.2017.18.5.1001

Received 26 August 2017; **Revised** 30 August 2017
Accepted 31 August 2017

***Corresponding Author; Changhoon Lee**

Tel: +82-2-970-6712
E-mail: chlee@seoultech.ac.kr

Ⅰ. 서 론

산업제어시스템(ICS; Industrial Control System)은 전기, 화학, 가스, 수도 등의 국가나 사회 주요기반시설의 설비를 효과적으로 제어하기 위해 사용되는 컴퓨터 기반의 시스템을 말하며 분산제어시스템(DCS; Distributed Control System), 원방감시제어시스템(SCADA; Supervisory Control And Data Acquisition) 등의 제어시스템을 포함한다[1][2]. 본래의 산업제어시스템은 일반적인 IT 시스템과 다르게 인터넷과 같은 외부 네트워크와 분리되어 내부 장비들만 연결하는 독자적인 네트워크로 폐쇄적이었지만 최근 산업제어시스템의 규모가 커짐에 따라 효율적인 관리를 위하여 IT(Information Technology) 시스템과 융합되면서 이러한 주요기반시설을 대상으로 한 사이버 공격이 증가하고 있다[1][3]. 실제로 국내외에서 2010년 스턱스넷(Stuxnet) 악성코드에 의한 이란 부셰르 원자력 발전소 운영 마비, 2011년 4월 DDoS(Distributed Denial of Services) 공격으로 인한 한국 농협 전산망 장애, 2012년 8월 사우디 아람코(Saudi Aramco) 시스템 파괴, 2014년 1월 일본 몬주 원전 해킹 시도, 2014년 6월 유럽에서의 SCADA 설치 프로그램에 포함된 하벡스(Havex) 악성코드, 2014년 12월 한국수력원자력 해킹 공격, 2015년 12월 우크라이나 발전소 공격에 따른 대규모 정전 사태 등 주요기반시설을 대상으로 한 사이버 공격이 있었다[4][5]. 이와 같이 산업제어시스템은 우리 사회의 기반시설이나 실생활의 필수적인 요소들과 직접적으로 연관되어 있어 공격으로 인한 피해는 막대한 금전적 손실 또는 인명피해를 초래할 수 있다.

산업제어시스템 보안의 중요성이 부각됨에 따라 각 국에서는 여러 표준화와 정책이 시행되고 있다. 특히 국내에서는 주요기반시설에 탑재되는 암호모듈은 전자정부법 시행령 제 56조와 동법 시행령 제 69조에 의거 '암호모듈 시험 및 검증지침'에 따라 국가정보원의 검증을 획득한 암호모듈을 탑재해야 한다.

하지만 산업제어시스템의 보안을 위한 암호모듈 탑재는 지연을 발생시켜 해당 시스템의 본래 기능에 영향을 줄 수 있다[2]. 또한, 상기 소개한 것과 같이 산업제어시스템은 다양한 분야의 주요기반시설에서 사용되고 있고 그 구조에 따라 우선시 되어야 하는 특성이 존재한다. 따라서 본 논문에서는 산업제어시스템 구조와 특성에 따른 암호모듈을 적용하는 방안을 모색하고자 하며 2장에서는 각 분야별 산업제어시스템의 사이버 위협, 3장에서는 산업제어시스템 구조, 4장에서는 산업제어시스템 암호모듈 적용방안을 다루고 5장에서는 원자력 발전소의 비안전등급(NNS; Non-Nuclear Safety) 제어기기에서 단위 제어기에 암호모듈을 적재하여 실행 결과를 다룬다. 현재 국내에서 원전 제어시스템을 대상으로 제어기기에 암호모듈 도입은 존재하지 않아 본 실험을 통해 향후 원자력 발전소 비안전계통에 사이버보안 규제 지침을 기반으로 하는 기술 개발에 큰 의의가 있다. 6장에서 결론을 통해 마치고자 한다.

Ⅱ. 산업제어시스템의 사이버 위협

최근 미국 국토안보부(DHS; Department of Homeland Security)의 사이버 및 기반시설 분석실에서 주요기반시설 사이버보안 강화를 위한 후속조치 중 하나로 주요기반시설을 16개 분야로 분류해 각 영역별 특징과 보안위협 현황을 정리한 보고서인 'Sector Risk Snapshots'을 발간하였다. 이 보고서에 따르면 댐, 식료 및 농업, 일부 교통 시스템 하위 항목을 제외한 대부분의 주요기반시설에 사이버 위협이 존재하고 이는 해당 분야에만 영향을 주는 것이 아니라 연계된 다른 기반시설에까지 연쇄피해를 가할 수 있다는 점에 주목하고 있다. 하지만, 해당 보고서는 자료 제공을 목적으로 하여, 각 리스크에 대한 대응책이나 해결 방안은 제시하지 않고 있다[6].

'Sector Risk Snapshots'에서 분류된 주요기반시설 중 산업제어시스템을 사용하는 기반시설은 화학(Chemical), 주요제조시설(Critical Manufacturing), 댐(Dams), 에너지 - 전력, 석유 및 가스(Energy - Electricity, Oil & Natural Gas), 핵발전 및 처리시설(Nuclear Reactors, Materials and Waste), 수자원 및 수처리 시스템(Water and Wastewater Systems)으로 6개의 분야이며 이들은 주요 자원을 다루기에 다른 기반시설 분야들과 있어서 상호의존적이거나 큰 영향력을 행사한다[7]. 따라서, 상기 6개 분야의 산업제어시스템을 대상으로 한 사이버공격은 해당 분야뿐만 아니라 다른 주요기반시설에도 연쇄적인 영향을 주어 더욱 큰 피해로 이어질 수 있음을 의미한다.

표 1. 'OCIA Sector Risk Snapshots'에서 분류한 산업제어시스템을 사용하는 주요기반시설 분야의 사이버보안 위협

Table 1. Cyberthreats of critical infrastructures with Industrial Control System at OCIA Sector Risk Snapshots

Infrastructures with ICS	Cyberthreats
Chemical	Cyberattacks or intrusions for remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems
Critical Manufacturing	Unauthorized on-site or remote intrusion into industrial control system and SCADA system of Critical Manufacturing Sector
Dams	Cyberattacks and intrusions for taking authority of control directly, due to increasing use of standardized industrial control systems technology on Dams.
Energy - Electricity, Oil & Natural Gas	Cyberattacks and intrusions using structure that connects with Internet through organization's internal network
Nuclear Reactors, Materials, and Waste	Cyber attack and intrusions for taking authority of control on industrial control system
Water and Wastewater Systems	Cyber attack and intrusions for taking authority of control on SCADA system

표 2. 'OCIA Sector Risk Snapshots'에서 분류한 산업제어시스템을 사용하는 6개의 주요기반시설과 관련된 인프라
Table 2. Critical infrastructures with Industrial Control System and related Infrastructures at OCIA Sector Risk Snapshots

Infrastructures with ICS	Related Infrastructures
Chemical	• Water and Wastewater Systems • Critical Manufacturing • Defense Industrial Base • Emergency Services • Food and Agriculture • Healthcare and Public Health • Nuclear Reactors, Materials, and Waste
Critical Manufacturing	• Communications • Information Technology • Defense Industrial Base • Nuclear Reactors, Materials, and Waste
Dams	• Energy • Transportation Systems - Maritime • Food and Agriculture
Energy - Electricity, Oil & Natural Gas	• Chemical • Dams • Communications • Emergency Services • Financial Services • Commercial Facilities • Critical Manufacturing • Information Technology • Defense Industrial Base • Water and Wastewater Systems • Food and Agriculture • Government Facilities • Healthcare and Public Health • Transportation Systems - Aviation, Rail, Maritime, Highway
Nuclear Reactors, Materials, and Waste	• Energy
Water and Wastewater Systems	• Chemical • Commercial Facilities • Communications • Critical Manufacturing • Defense Industrial Base • Energy • Information Technology • Emergency Services • Financial Services • Food and Agriculture • Government Facilities • Education Facilities • Healthcare and Public Health • Nuclear Reactors, Materials, and Waste

이들 분야의 산업제어시스템은 초기에는 작은 소자들을 배치한 하드웨어 형태의 서킷보드에서 집적회로에 프로그램이 가능한 PLC(Programmable Logic Controller) 제어기 형태로 발전하게 됨으로써 산업제어시스템의 연결성 및 원격 접근성의 향상을 통한 효율적인 관리를 위해 IT 시스템을 점진적으로 수용하면서 산업시스템 사이버 보안 위협은 기존 IT 시스템이 가지는 사이버보안 위협에 기인한다[8].

산업제어시스템의 사이버보안 측면에서의 취약점은 정책 및 절차의 취약성, 플랫폼의 취약성, 네트워크의 취약성으로 분류할 수 있고 이들은 패스워드 강제 사용 등과 같은 보안 정책 및 절차를 적용하고 보안프로그램 사용, 네트워크 통신의 암호화 등 다양한 보안통제를 적용함으로서 취약점을 제거하거나 완화시킬 수 있다[8]. 상기 'Sector Risk Snapshots'에서 지적한 주요기반시설 산업제어시스템의 사이버보안 위협에 대한 대응을 위해서는 보안 정책 및 절차, 다양한 보안 통제의 적용이 필요하고 이를 위해서는 암호모듈의 적용이 필수적이다.

Ⅲ. 산업제어시스템 구조 및 보안요구사항

산업제어시스템은 [그림 1]과 같은 형태의 네트워크로 구성되며 [그림 2]와 같이 필드의 센서, 액츄에이터 등의 상태 데이터를 계측, 수집하는 현장장치계층(Field device layer)과 계측, 수집된 데이터를 운영계층에 전달하거나 필드의 장치들을 제어하는 제어계층(Control layer), 필드 장치의 상태를 모니터링하거나 제어 명령을 제어계층에 전달하는 운영계층(operation layer) 등 3계층으로 구분된다[8]. 또한, 필드 장치의 제어 기능을 수행하는 하드웨어 또는 시스템은 제어 계층에 존재하고 이들은 운영계층에서 SCADA 네트워크로 연결되고 IT 시스템과 연결되어 운영된다.

또한, 각 계층은 그 어떤 상황에서도 운영이 중단되어서는 안 되는 산업제어시스템의 특성 상 아래 [표 4]의 네트워크 견고성, 서비스 지속성, 보안기능 등의 요구사항을 만족해야 하며 이는 각 계층에서 영향을 주지 않고 독립적으로 작용한다.[9] 따라서, 각 계층의 구성요소는 해당 계층의 특성에 따라 적합한 보안원칙 및 통제가 필요하다.

표 3. 산업제어시스템 각 계층별 핵심기능
Table 3. Major role of each layer of Industrial Control System

Layer	Role
Field device layer	Measuring and collecting state data of field devices such as sensors, actuators
Control layer	Controlling field devices and transferring the collected data to operation layer
Operation layer	Monitoring the status of field devices and transferring control commands to the control layer

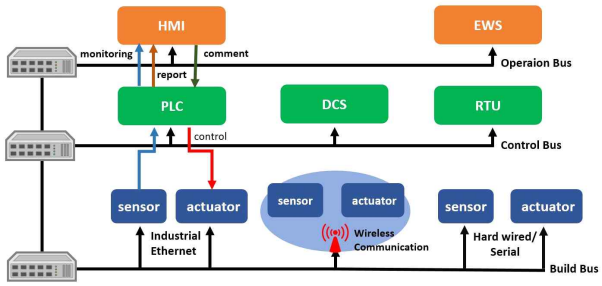

그림 1. 산업제어시스템 구성
Fig. 1. Industrial Control System Configuration

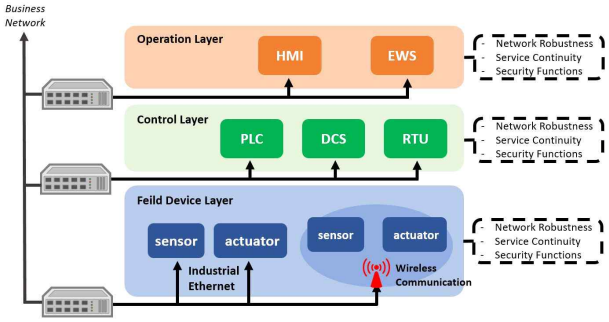

그림 2. 산업제어시스템 보안 참조 모델
Fig. 2. Security reference model for Industrial Control System

표 4. 산업제어시스템 보안요구사항
Table 4. Security Requirements for Industrial Control System

Security Requirements	Explanation
Network Robustness	Industrial control system components must provide industrial control system essential services such as command, control, reporting and monitoring, even if abnormal communication data or excessive amounts of communication data are flow into industrial control system.
Service Continuity	Industrial control system components must provide functionality to ensure business continuity. This includes ensuring the availability of resources used by industrial control systems such as power, storage, and protection against physical attacks.
Security Functions	Industrial control system components must provide security functions to ensure the protection of industrial control system components such as identification and authentication, access control, transmission and storage data protection.

Ⅳ. 산업제어시스템 암호모듈 적용방안

2장에서 소개한 'Sector Risk Snapshots'의 산업제어시스템 사이버위협은 산업제어시스템의 계층 구조에 따라 분류 할 수 있다. 산업제어시스템 사이버 위협 중 기반시설 설비에 대한 직접적인 제어에 대한 위협은 현장장치계층에 대한 사이버 공격, 현장장치들을 제어하는 제어 계층에 대한 사이버 공격으로 분류할 수 있고 제어계층과 현장장치계층에 제어명령을 전달하는 제어권 탈취 및 원격 해킹과 같은 위협은 산업제어시스템의 운영 계층에 대한 사이버 공격으로 분류할 수 있다. 하지만, 3장에서 언급한 바와 같이 각 계층에는 구성장치와 목적에 차이가 있으며 독립적인 보안통제가 적용되어져야 하므로 각 계층의 암호모듈도 각 계층의 특성에 맞춰 적용되어야 한다.

표 5. 계층별 암호모듈 적용시 효과
Table 5. Effects of Crypto-module application to each layer

Security Requirements	Effects of Crypto-module application
Field device layer	• Prevention of communication data forgery, tampering and leakage
Control layer	• Prevention of communication data forgery, tampering and leakage • As the application of various security controls such as authentication and access control becomes possible, it is possible to control field devices secure.
operation layer	• Prevention of communication data forgery, tampering and leakage • As the application of various security controls such as authentication and access control becomes possible, it is possible to protect the control right to the lower layer(Field device layer, Control layer)

산업제어시스템의 현장장치계층은 현장에서 데이터를 수집, 측정하는 단일 기능의 센서 혹은 액츄에이터 등으로 구성되어 있고 제어 계층은 어떤 상황에서도 적시에 필드장치들을 제어할 수 있도록 DCS, PLC, RTU(Remote Terminal Unit)과 같은 산업 프로세스에 특화된 장치들로 구성되어 있어 보안기능을 위한 메모리 용량 및 컴퓨팅 자원에는 제한이 있다[10]. 반면에, 산업제어시스템의 운영계층은 하위계층 네트워크에서 수집된 데이터를 모니터링하고 제어 및 운영할 수 있도록 HMI(Human Machine Interface), EWS(Engineering Workstations)와 같은 장치들로 구성되며 이들은 PC 기반의 고성능 장치들이다. 실제로 [표 6]에서 제시하고 있는 ABB, Honeywell, Schneider Electric 등 산업제어시스템 분야 주요 벤더 제품의 메모리 및 CPU에서 산업제어시스템의 제어계층과 운영계층의 성능차이를 확인할 수 있다[11][12][13]. 즉, 현

장장치계층, 제어계층을 이루고 있는 구성요소들은 특정 기능 수행에 특화된 장치들로 암호모듈 적용시 그에 따라 발생하는 지연으로 인해 본래 수행해야 할 제어 기능에 영향을 줄 수 있고 이는 곧 산업제어시스템 보안요구사항을 침해할 수 있다. 또한, 운영계층을 이루고 있는 구성요소들은 PC 기반의 고성능 장치이지만 하위계층에 대한 제어명령을 내릴 수 있는 제어권을 소유하고 있어 이에 대한 사이버공격이 이루어질시 하위계층 전역에 걸쳐 영향을 줄 수 있고 이는 역시 산업제어시스템 보안요구사항의 침해로 이어진다.

표 6. 산업제어시스템 분야 주요 벤더 제품 사양
Table 6. Specifications of major vendor's product for Industrial Control System

Category	Company / Product	Specification
Programmable Logic Controller	ABB / AC500 Series	• Memory Size for Data : 28 ~ 5632KB • Memory Size for Program : 64 ~ 4096KB
	Schneider Electric / Modicon M340 Series	• Memory Size for Data : 128 ~ 256KB • Memory Size for Program : 1792 ~ 3584KB
Remote Terminal Unit	Honeywell / RTU2020	• Processor : Dual Core ARM Cortex-A9 Core (32 bit) 667MHz • Dynamic memory(RAM) : 128MB • Program memory(Flash) : 32MB • Nonvolatile memory : 4Mbits
Human Machine Interface	Schneider Electric / HMIBM Series	• Processor : Intel Celeron 2980U 1.6 GHz, Intel Core i3 2120, Intel Core i7 4650U 등 • Memory : 4 ~ 8GB RAM DDR3 internal, 512KB MRAM internal

암호모듈에 사용되는 암호 및 해시 알고리즘들은 [표 7]와 같이[14] 암호 알고리즘의 종류, 키 길이, 사용되는 운영모드 등에 따라 보안강도와 성능이 달라진다. 따라서, 산업제어시스템의 현장장치계층, 제어계층에 적용되는 암호모듈은 구성요소들의 성능을 고려하여 본래 기능 수행에 영향을 주지 않도록 시간대비 처리량이 좋은 경량암호나 해시 알고리즘, 운영모드, 상대적으로 작은 키 길이 등을 사용한 암호모듈을 적용해야 한다. 또한, 산업제어시스템의 운영계층에 적용되는 암호모듈은 운영계층을 구성요소의 성능과 해당 계층이 가지는 중요도 또는 영향력으로 견주어 봤을 때 제어계층보다 더 강한 안전성을 가지는 암호 또는 해시 알고리즘, 운영모드, 상대적으로 더 큰 키 길이 등을 사용한 암호모듈의 적용이 적합하다. 또한, 암호모듈에 사용되는 암호 및 해시 알고리즘은 적용할 수 있는 최적화 기법을 사용해 구현해야 한다.

표 7. 암호 및 해시 알고리즘의 처리속도 비교 예시(Library : Crypto++, Test OS : Fedora release 25(x86_64), Test CPU : Skylake 6th generation 3.14 GHz)
Table 7. Example of comparing throughput of cryptographic algorithms (Library : Crypto++, Test OS : Fedora release 25(x86_64), Test CPU : Skylake 6th generation 3.14 GHz)

Algorithm	Cycles Per Byte
AES/CTR(128-bit key)	0.8
AES/CTR(192-bit key)	0.9
AES/CTR(256-bit key)	1.1
AES/CBC(128-bit key)	3.4
AES/CBC(192-bit key)	4.0
AES/CBC(256-bit key)	4.6
AES/OFB(128-bit key)	3.6
AES/CFB(128-bit key)	3.5
AES/ECB(128-bit key)	0.7
ARIA/CTR(128-bit key)	26.1
ARIA/CTR(256-bit key)	33.8
SHA-256	13.4
SHA-512	8.7
...	...

Ⅴ. 실 험

본 논문에서는 상기 제시한 암호모듈 적용방안에 대한 실험으로 국내 원자력발전소의 비안전등급 제어기기(DCS)에 포함된 단위 제어기(Control Unit)에 암호모듈을 적재하고 실행하고 일반적 PC 환경에서 동일한 암호모듈을 적재하여 비교하는 실험을 진행하였다. 비교 실험에 사용된 비안전등급 제어기기는 다수의 단위 제어기가 캐비닛에 설치되는 임베디드 시스템으로 각 단위 제어기의 CPU 모듈에는 비안전계통을 제어하는 소프트웨어 로직이 실행된다.

실험에 사용된 제어기의 사양은 다음과 같다.

- CPU : Single Core, 450 MHz
- Memory : 96 MByte
- Word Size : 32-Bit
- Endianness : Big-Endian
- Operating System : VxWorks version 5.5.1

또한, 실험에 사용된 PC의 사양은 다음과 같다.

- CPU : Intel i5 7500, 3.4 GHz
- Memory : 16 GByte
- Word Size : 64-Bit
- Endianness : Little-Endian
- Operating System : Windows 10

본 실험은 두 가지 방식과 키 길이에 따른 수행시간을 비교했으며 수행시간 측정은 패딩(Padding) 과정을 제외한 암호화를 총 10만번 반복 실행한 후 평균 실행시간을 산출했다. 상기 실험으로 [표 9]과 같은 결과를 얻을 수 있었으며 이를 통해 최적화 기법 적용 유무와 암호키 길이에 따른 수행시간의 차이를 확인할 수 있었고 운영환경에 따른 수행시간 또한 확인할 수 있었다.

표 8. 비안전등급 제어기와 PC의 ARIA 수행시간 비교
Table 8. Comparing of execution time on Non-Nuclear Safety control unit VS PC

Module Version	Environment	Result of each key length (ms)		
		128 bit	192 bit	256 bit
general ARIA	Control Unit	0.02878	0.03287	0.03697
	PC	0.00383	0.00435	0.00497
optimized ARIA	Control Unit	0.00760	0.00799	0.00809
	PC	0.00372	0.00421	0.00489

Ⅵ. 결 론

산업제어시스템은 주요기반시설에서 사용되는 제어시스템으로 이에 대한 사이버공격은 방대한 규모의 금전적 손실 또는 인명피해로 이어질 수 있다. 이를 방지하기 위해 다양한 보안통제 적용을 위한 암호모듈의 적용이 필수적이다. 산업제어시스템은 수행하는 기능과 구성 장치에 따라 현장장치 계층, 제어 계층, 운영 계층으로 분류되며 구성되는 장치에 성능 차이가 있다. 따라서, 본 논문에서는 각 계층에 적합한 암호모듈 적용 방안으로 DCS, PLC, RTU 등과 같은 보안기능을 위한 메모리 용량과 컴퓨팅 자원에 제한이 있는 장치로 구성된 제어 계층은 경량 암호나 상대적으로 작은 키 길이, 시간복잡도의 암호 또는 해시 알고리즘을 사용한 암호모듈의 적용을, HMI, EWS 등과 같은 PC 기반의 고성능의 장치로 구성되었지만 하위 계층에 대한 제어권을 가지고 있어 상대적으로 더 높은 보안성을 요구하는 운영계층에는 제어계층보다 더 큰 키 길이, 시간복잡도의 암호 또는 해시 알고리즘을 사용한 암호모듈의 적용과 암호모듈의 최적화 구현 기법 적용을 제시하였다.

감사의 글

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(원전 비안전등급 제어기기(DCS) 사이버침해 예방 및 탐지 기술 개발, No. 20161510101810).

참고문헌

[1] Y. H. Cha, B. H. Cho, and J. C. Na, “Security Technology Trends and prospective of Industrial Control System”, KEIT PD Issue Report, Vol. 13, No. 6, pp. 79-100, 2013.

[2] K. Stouffer, J. Falce, K. Scarfone, “Guide to industrial control systems(ICS) security”, NIST Special Publication, 800-82, 2011.

[3] S. G. Lee, S. Y. Lee, J. C. Kim. "A Study on Security Vulnerability Management in Electric Power Industry IoT". *Journal of Digital Contents Society*, Vol. 17, No. 6, pp. 499-507, Dec 2016

[4] “[Analysis Report]Critical Infrastructure Threats”, AhnLab ASEC Analysis Report, 2016.

[5] J. H. Oh, Y. I. You, K. H. Lee. "Infrastructure Accident and Control System Standard Trends". *Korea Institute of Information Security and Cryptology*, Vol. 27, No. 2, pp. 5-11, Apr 2017

[6] “The Department of Homeland Security, Sector Risk Snapshots Released", KISA Internet & Security Bimonthly, Vol. 3, pp.24-28, 2014.

[7] “Sector Risk Snapshots”, U.S. Department of Homeland Security, 2014.

[8] D. Y. Kim. "Vulnerability Analysis for Industrial control System Cyber Security", *The Journal of the Korea Institute of Electronic Communication Sciences*, Vol. 9, No. 1, pp. 137-142, Jan 2014.

[9] “Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model”, Telecommunications Technology Association, TTAK.KO-12.0307, 2017.

[10] Y. H. Chen, "Introduction of Information Security for Industrial Control System," *Korea Institute of Information Security and Cryptology*, vol. 19, no. 5, pp. 52-59, Oct 2009.

[11] ABB Group. Information of AC500 PLC Series producted by ABB Group. Available : http:/new.abb.com/plc/programmable-logic-controllers-plcs

[12] Honeywell. Information of RTU2020 producted by

Honeywell. Available:
https://www.honeywellprocess.com/en-US/explore/products/control-monitoring-and-safety-systems/scada-systems/Pages/controledgertu.aspx

[13] Schneider Electric. Information of PLC, HMI produced by Schneider Electric. Available :
http://www.schneider-electric.com/b2b/en/products/automation-and-control.jsp

[14] Crypto++ maintained by Jeffrey Walton and Crypto++ community. Speed benchmarks for some commonly used cryptographic algorithms. Available :
https://www.cryptopp.com/benchmarks.html

석병진(Byoungjin Seok)

2012년 ~ 2017년 8월 : 서울과학기술대학교 컴퓨터공학과 학사
2012년 9월 ~ 현재 : 서울과학기술대학교 일반대학원 컴퓨터공학과 석사과정
※관심분야 : 정보보호(Personal Information), 암호학(Cryptography, 디지털 포렌식 (Digital Forensic) 등

김 역(Yeog Kim)

1992년 : 성신여자대학교 전산학과 (이학사)
2003년 : 고려대학교 정보보호대학원 (공학석사)
2010년 : 고려대학교 정보경영전문대학원 (공학박사)
2005년 3월~2007년 8월 : 동양미래대학교 전임강사
2017년~현재: 서울과학기술대학교 전기정보기술연구소 연구원
※관심분야 : 정보보호(Personal Information), 디지털 포렌식(Digital Forensics), 암호모듈평가 등

이창훈(Changhoon Lee)

2001년 : 한양대학교 자연과학부 수학전공 학사
2003년 : 고려대학교 정보보호대학원 석사
2008년 : 고려대학교 정보경영전문대학원 정보보호전공 박사
2008년 4월~2008년 12월 : 고려대학교 정보보호연구원 연구교수
2009년 3월~2012년 2월 : 한신대학교 컴퓨터공학부 조교수
2012년 3월~2015년 3월 : 서울과학기술대학교 컴퓨터공학과 조교수
2015년 4월~현재 : 서울과학기술대학교 컴퓨터공학과 부교수
※관심분야 : 정보보호(Personal Information), 암호학(Cryptography), IoT(Internet of Things), 디지털포렌식 (Digital Forensics) 등