http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.25, No.2, May 2020, pp.99-108
https://doi.org/10.7838/jsebs.2020.25.2.099

제어 네트워크의 프로토콜을 이용한 보안 위협 연구

A security study for Control Network: Security Threat Using Control Protocol

최동준(DongJun Choi)*, 이재우(JaeWoo Lee)**

초 록

산업제어 시스템은 일반적인 IT 환경과는 다르게 보안성보다 안전성, 연속성이 중요시 되는 환경이다. 산업제어 시스템에 보안 사고가 발생할 경우 물리적인 동작을 컨트롤 할 수 있으므로 안전성과 연속성을 보장받을 수 없다. 따라서 물리적인 피해가 발생할 수 있고, 물리적인 피해가 인명피해까지 초래할 수 있다. 산업제어 시스템에 대한 사이버 공격은 단순히 사이버 피해라고 볼 수 없으며 테러라고 볼 수 있다. 그러나 아직까지 산업제어 시스템에 대한 보안이 많이 강화되지 않은 상태이고 실제로 많은 취약점들이 발생하고 있다. 본 논문에서는 산업제어 시스템에서 사용하는 PLC 프로토콜을 대상으로 연결과정 및 패킷을 분석하고 프로토콜에 존재하는 보안 메커니즘을 우회하여 PLC를 원격에서 컨트롤 할 수 있음을 보인다. 이를 통해 산업제어 시스템에 대한 보안 경각심 제고를 하고자 한다.

ABSTRACT

Unlike a general IT environment, an industrial control system is an environment where stability and continuity are more important than security. In the event of a security accident in the industrial control system, physical motion can be controlled, so physical damage can occur and physical damage can even result in personal injury. Cyber attacks on industrial control systems are not simply cyber damage, but terrorism. However, the security of industrial control systems has not been strengthened yet, and many vulnerabilities are actually occurring. This paper shows that the PLC can be remotely controlled by analyzing the connection process and packets for the PLC protocol used in the industrial control system and bypassing the security mechanism existing in the protocol. Through this, we intend to raise the security awareness of the industrial control system.

키워드 : 산업제어시스템, 보안, 프로토콜, 재전송공격
Industrial Control System, Security, Protocol, ReplayAttack

이 논문은 2018년도 중앙대학교 연구장학기금지원에 의한 것임

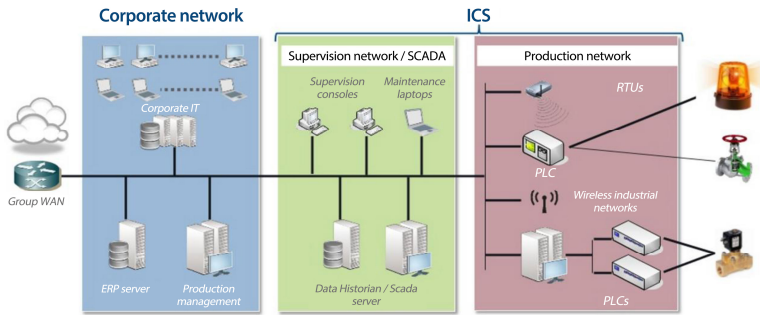
* First Author, Master's Course, Department of Convergence Security, Chung-Ang University(zzczzc123@cau.ac.kr)
** Corresponding Author, Professor, Department of Industrial Security, Chung-Ang University(jaewoolee@cau.ac.kr)
Received: 2020-04-06, Review completed: 2020-04-16, Accepted: 2020-05-18

1. 서 론

현재 소프트웨어 시스템이 점점 대규모화되고 복잡해짐에 따라 서로 다른 이기종 시스템에서 제공하는 기능을 통합하여 새로운 기능을 효율적으로 지원하는 방법이 필요하게 되었다[5]. 이러한 움직임은 산업제어 시스템에서도 발생하였으며 산업제어 시스템의 자동화, 원격화 시스템을 구성하게 되었다. 산업 제어시스템(ICS, Industrial Control System)이란 원격의 설비를 측정, 계측, 감시하고 이를 제어하는 시스템을 말한다. 발전, 배전, 가스 등의 에너지 분야, 항공 철도, 항만, 도로 등 교통시설, 상수도, 하수도 댐 등 수자원 분야, 석유 화학, 정유 제조 등 플랜트 분야 등에서 다양하게 사용되고 있다[8]. 과거에는 폐쇄 망으로 운영되었으나 정보통신 기술의 발달로 개방형으로 변화하고 다양한 ICT 환경과 연계되어 상호 의존적 시스템을 구성하고 있다. 따라서 폐쇄 망으로 구성되어 있어서 안전하다는 의견을 갖고 있었으나, 최근 우회적 공격이 지속적으로 발생함에 따라 독립적인 네트워크로 대처하는 것에는 한계가 드러나고 있다[12].

또한, 스마트 제조 기술 공정의 도입으로 IT 시스템에 대한 의존도가 높아지고 있으며, 시간이 지남에 따라 산업 자동화 시스템과 기존의 IT 시스템 간의 차이점이 점점 사라지고 있다. 산업제어시스템의 네트워크 구성은 <Figure 1>과 같이 이루어져 있으며 센서에서 센싱된 정보를 HMI(Human Machine Interface)에 전송하고, 관리자가 해당 정보를 바탕으로 판단한다.

그 후 판단을 바탕으로 명령을 내리면 PLC(Programmable Logic Controller)에 명령이 입력되고 입력 값에 알맞은 출력 값을 엑추에이터에 전달하여 동작하게 된다. 여기서 말하는 PLC란 Programmable Logic Controller로 원하는 동작 Logic을 프로그래밍할 수 있는 기기이며 산업제어시스템에서 동작에 관련된 가장 중추적인 역할을 수행하고 자동화의 핵심 역할을 한다. 이러한 산업제어시스템에서는 IT 시스템에 비해서 운영의 연속성이 매우 중요하다. 보안사고로 산업제어시스템의 운영 중단 발생 시 사람의 안전 및 건강에 대한 중대한 위험, 환경에 대한 심각한 피해, 생산 손실과 같은 재정 문제 및 나아가 국가 경제까지 영향을 끼칠 수 있다[13]. 실제로 2010년 발생한 Stuxnet은 이란 부셰르 원자력핵발전소와 중국 1천여 개 주요 산업 시설을 비롯해 전 세계 여러 국가에 감염이 확산된 것으로 알려지고 있다[7]. 이뿐만 아니라 2018년엔 이란의 원거리 망과 관련 통신시설을 공격하는 시도도 있었다.



〈Figure 1〉 ICS Network[12]

〈Table 1〉 Cyber Attack Cases for Industrial Control Systems[6]

Date	Field	Target	Content
2003	nuclear power	Davis-Besse Power Plant, Ohio, USA	Surveillance system virus infection for 5 hours
2005	Produce	DaimlerChrysler	13 hours in factories stopped operating due to operating system infection
2007	traffic	LA Transportation System	System infringement by insiders
2010	nuclear power	Iran uranium centrifuge	1,000 centrifuge infections due to stuxnet infection
2012	waterworks	Houston Waterworks, USA	Uncontrolled malware infection in the control system
2014	power plant	Korea Hydro Nuclear Power Plant	Malware infection through e-mail. Drawing spill
2015	Power station	Ukrainian power station	Enhanced blackout due to malicious code (Black Energy, Kill disk)

이 공격은 Stuxnet을 기반으로 한 변종 악성 코드였으나 방어에 성공하여 실질적인 피해를 주지는 못하였다[11]. 이처럼 국가 기반시설에 해당하는 발전소, 통신망 등 산업제어 시스템에 대한 사이버 공격은 끊임없이 이루어지고 있으며 앞서 기술 하였듯, 물리적인 피해, 인명 피해뿐만 아니라 기반시설에 대한 공격이 성공할 경우 큰 사회적 혼란까지 일으킬 수 있다.

따라서, 본 연구에서는 산업제어시스템에서 사용하는 통신 프로토콜을 분석하여 보안 위협을 확인한 뒤 공격 가능함을 증명함으로써 위험성을 보이고자 한다.

본 논문은 다음과 같이 구성된다. 제 2장에서는 산업제어 시스템에서 사용되는 여러 프로토콜 중 지멘스 사 PLC에서 사용되는 프로토콜 대한 분석을 진행한다. 해당 프로토콜은 여러 버전으로 나누어져 있으며 버전별 차이점에 대해 설명한다. 제 3장에서는 PLC와 TIA 포탈 간의 연결 패킷을 캡처하여 프로토콜의 구성과 보안 요소를 확인하고, 보안 요소를 우회할 방법을 확인한다. 그 후 제 4장에서 PLC가 Stop, Start 할 때 발생하는 패킷을 캡처하여 재전송 공격을 진행하고 제 5장에서 결론으로 마무리 짓는다.

2. 관련 연구

2.1 Review on Cyber Vulnerabilities of Communication Protocols in Industrial Control Systems

XU Y et al.[17]에서는 ICS 환경에서 사용되는 프로토콜들을 대상으로 보안성을 체크하는 리뷰를 진행하였다. 대상으로 하는 프로토콜은 DNP3, Modbus, IEC 60870-5-104, IEC61850, IEC61400-25, IEEE C37,118이며 보안성을 체크하는 항목은 Lack of Integrity, Lack of Confidentiality, Lack of Availability, Lack of Authentication, Lack of Authorization, Lack of Encryption이었다. 그러나 해당 논문에서는 S7Comm 프로토콜에 대한 보안성 체크는 이루어지지 않았다.

2.2 S7Comm 프로토콜[16]

S7 프로토콜은 모든 SEMANTIC S7 및 C7 컨트롤러에서 사용하며 이 컨트롤러에는 사용자 프로그램이 데이터를 읽고 쓸 수 있는 S7 통신 서비스가 포함되어 있다. 따라서 이 기능들은 사용된 버스 시스템에 상관없이 사용할 수 있다. 데이터 전송은 1byte에서 64kbyte까지 할 수 있으며 하드웨어에 따라 성능이 달라진다. 주로 S7-200, S7-300, S7-400 PLC 간의 통신에서 사용되나 Anti-Replay 메커니즘이 포함되어 있지 않다.

2.3 S7CommPlus 프로토콜(Early)[9]

S7CommPlus 프로토콜(Early)은 TPKT와 ISO 8073을 모두 사용하는 바이너리 프로토콜이며 102번 TCP 포트를 사용한다. 이 프로토콜은 S7Comm 프로토콜보다 복잡하며 Anti-Replay 매커니즘을 세션 ID 라는 2바이트 필드로 구현하였다. 주로 S7-1200 V3.0간 통신에서 사용되어 진다.

2.4 S7CommPlus 프로토콜(Late)[9]

S7CommPlus 프로토콜(Late)은 기본적으로 S7comm (Early)와 같은 스펙을 가지고 있지만 S7-1200 v4.0과 S7-1500간 통신에 사용되고 Anti-Replay 메커니즘이 복잡한 암호를 적용하여 좀 더 강화되었다.

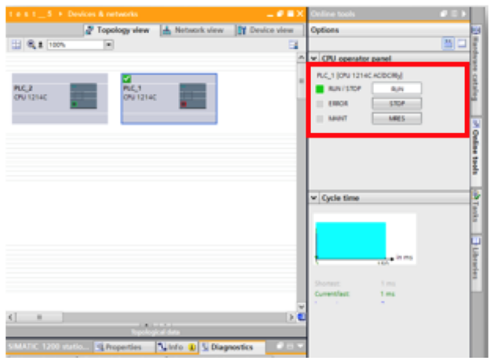
2.5 재전송 공격[10]

재전송 공격은 보안 영역에서 아주 오래전부터 나온 개념이며 많은 논의가 돼 왔다[1, 2, 4, 15]. 이런 논의를 거쳐 재전송 공격의 정의는 다음과 같이 일반화될 수 있다. 다른 상황에서 원래 상황에 메시지를 재전송하는 프로토콜에 대한 공격으로 해당 공격을 통해 기존 통신 주체가 프로토콜 실행을 성공적으로 완료했다고 착각하게 만드는 방법이다.

3. 연구방법 및 제어시스템 프로토콜 보안 취약점 분석 환경

3.1 연구 방법

PLC에 사용자가 프로그래밍하기 위해서는 TIA 포탈에 PLC를 연결하는 과정이 필요하며, 연결 후에는 원격에서 PLC를 Stop, Start 할 수 있는 기능이 TIA 포탈 내에서 제공되어 진다.



〈Figure 2〉 PLC Start, Stop Function in TIA Portal

본 연구에서는 TIA 포탈과 PLC연결이 이루어질 때의 패킷, TIA 포탈에서 PLC Start, Stop 버튼을 눌렀을 때의 패킷을 중간에 가로채서 해당 패킷의 내용을 분석하고 TIA 포탈로 위장하여 연결이 이루어질 때의 패킷 내용을 전송

하여 PLC와 연결을 형성한다. 그 후 Start, Stop 버튼이 눌렸을 때의 패킷을 재전송하여 같은 네트워크상에 존재하는 PLC를 대상으로 원격에서 Start, Stop 할 수 있는 연구를 진행하였다.

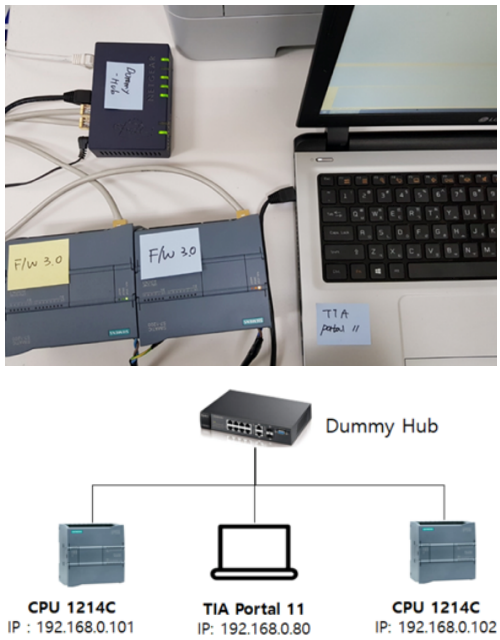
3.2 분석 환경

본 연구에서 사용되었던 PLC는 S7-1200시리즈이므로 S7Comm 프로토콜 Early에 대해서 패킷 분석을 진행하였다. 해당 프로토콜의 통신을 분석한 분석 환경과 네트워크 구성은 다음과 같다.

〈Table 2〉 Analysis Environment

Field	Content
Analysis Target	Siemens PLC 1212c AC/DC/Rly, 1214 AC/DC/Rly
O/S	Windows 7 Ultimate K
Wire shark Version	Version 2.4.2
TIA Portal Version	Version 11
PLC Version	Version 3.0

<Figure 2>에 존재하는 TIA 포탈[3]이란 HMI, PLC와 그 외 자동화에 필요한 모든 기기를 한데 묶은 통합 자동화 솔루션이다. 컨트롤러와 분산 I/O의 엔지니어링을 비롯해 HMI 장치 구성, 프로세스 시각화(SCADA), 드라이브 및 안전 기능 시험 운전 등이 공통 소프트웨어 프레임워크에 통합되어 있다. PLC와 HMI 등을 각각의 소프트웨어 안에서 별도의 프로그래밍 작업 후 이들을 서로 연동시켜야 했던 기존과 달리, TIA 포탈을 사용하면 각 기기들을 따로 작업할 필요가 없다. 지멘스사의 제품을 사용하는 많은 제어시스템에선 TIA 포탈을 사용하며 원격에서 컨트롤하기 위해서는 네트워크 연결이 필요하다. 따라서 <Figure 2>와 같이 PLC와 TIA 포탈의 네트워크를 구축하였다.

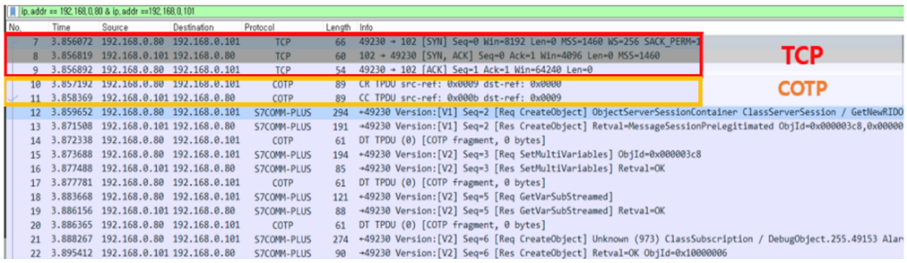


〈Figure 2〉 Analysis Environment

4. 제어시스템 프로토콜 보안 취약점 분석 및 결과

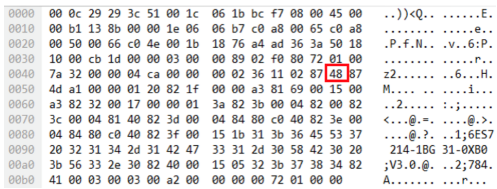
4.1 TIA 포탈과 PLC의 연결 프로토콜 분석

TIA 포탈과 PLC 사이 연결될 때의 패킷 내용을 보면 총 6번의 연결이 이루어진다. 먼저 TCP와 COTP 연결이다. TCP 연결은 SYN, SYN+ACK, ACK로 일반적인 통신을 위한 3Wayhand Shake 과정을 통해 이루어진다. 그 후 COTP 프로토콜로 연결이 한번 이루어지고, S7 Comm-PLUS 프로토콜로 데이터를 주고받게 된다.

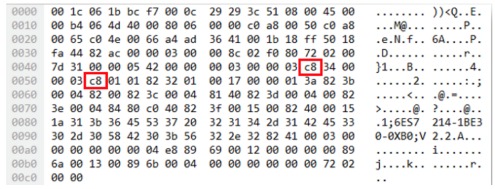


〈Figure 4〉 S7CommPlus Connect Packet

S7CommPlus 연결 패킷에서 TIA 포탈은 사용 PC에 대한 상태정보를 PLC 기기에 문자열 데이터로 전송해준다. 이때 PLC는 앞서 설명한 프로토콜의 특성상 Anti-Replay 랜덤 비트를 TIA 포탈에 다시 전송한다. 이는 재전송 공격을 방어하기 위한 방어 기법이다. Request 값에 따라 Response 값이 매번 변경되므로 Request 없는 무분별한 Replay 공격을 방어할 수 있다. 따라서 해당 패킷의 데이터 내용을 Hex Data로 저장하여 단순히 재전송할 경우 S7Comm Plus에서 제공하는 Anti- Replay 메커니즘에 의해 연결에 실패하게 된다.



〈Figure 5〉 Random Byte Transmission



〈Figure 6〉 Random Byte Bypass

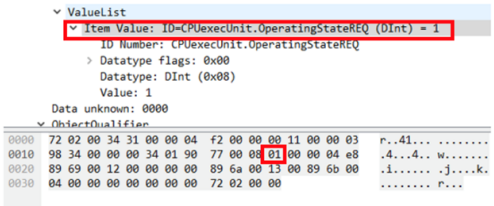
4.2 S7CommPlus 프로토콜 Anti-Replay 매커니즘 우회

S7CommPlus 연결에서 전송되는 Anti-Replay 랜덤 비트를 우회하는 방법은 응답 패킷에서 오는 챌린지 값에 고정된 0x80 값을 더해주어 특정 필드 영역 안에 넣어주면 우회할 수 있다. 아래 Figure 5에 보이는 영역에 랜덤 비트를 넣어 챌린지 값을 전송하게 되고 0x80 값을 더해 전송하는 응답 패킷을 보면 <Figure 6>과 같다. 랜덤바이트를 우회하는 방법은 다음과 같다[14] Anti-Replay = Challenge(0x48) + Fixed Value(0x80) = 0xc8

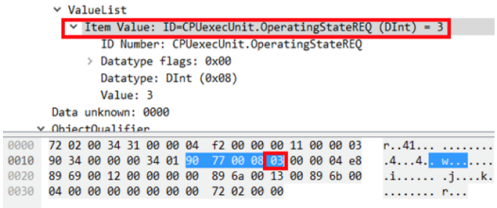
4.3 S7CommPlus 프로토콜 PLC Stop, Start 패킷 분석

연결 설정 후에 원격에 있는 Tia Portal에서 PLC Stop 명령을 내렸을 때 패킷이다. PLC Stop 기능을 하는 패킷을 좀 더 자세히 살펴보면 Item value:ID = CPUexecUnit.OperationgStateREQ(Dint) 영역 하나의 비트에 따라 PLC의 기능이 달라지는 것을 확인할 수 있다.

PLC가 Start 할 때는 Item Value가 0x03이고 Stop일 때는 0x01인 걸 확인할 수 있다. 위의 내용을 종합해 보면, S7CommPlus 프로토콜 연결 과정에 Anti-Replay 매커니즘이 구현되어



〈Figure 7〉 PLC Stop Packet



〈Figure 8〉 PLC Start Packet

있지만 간단한 산술 연술로 우회할 수 있음을 확인하였고, PLC는 SetMultiVariable 패킷 중 Item value:ID = CPUexecUnit.OperationgState REQ(Dint) 의 하나의 바이트로 Stop과 Start 명령을 구분하는 것을 확인하였다. 또한, 관련 연구[9]에서 프로토콜 특성상 102번 포트를 항상 Open하여 사용함을 확인하였다. 따라서 처럼 소켓 프로그래밍을 통해 S7CommPlus 프로토콜의 구조로 Anti-Replay 메커니즘을 우회하여 102번 포트에 패킷을 전송하면 재전송 공격이 가능하다는 결론을 도출할 수 있다. 재전송 공격을 위해 C언어로 코드를 작성하여 동작한 결과 정상적으로 재전송 공격을 수행하는 것을 확인하였다.

5. 결 론

본 논문에서는 S7CommPlus의 메시지 포맷과 특성, 데이터 구조 및 데이터를 분석하였다. 또한, 실제 산업제어시스템에서 사용하는 환경을 구성하기 위해 테스트베드 환경인 지멘스사

〈Figure 9〉 PLC Stop, Start Packet Re-Play Code(Part)

〈Figure 10〉 PLC Stop, Start Re-Play Program

〈Figure 11〉 PLC Actually Stopped Due to Replay Attack

의 PLC 1214c AR/DC/Rly, TIA Portal Version 11를 네트워크 허브인 더미 허브와 연결하여 내부 네트워크 환경을 구축하였다. 재전송 공격을 위해 TIA Portal 11과 PLC 기기간 연결 설정 패킷, TIA Portal에서 제어 명령을 내릴 시 발생하는 패킷을 분석하였다. 분석 결과, TIA 포탈과 PLC 간 연결 과정에서 S7Comm Plus 프로토콜에 Anti-replay byte가 전송되지만, 우회가 가능함을 확인하였고 이를 통하여 재전송 공격을 할 경우 PLC기기를 원격에서 제어할 수 있음을 확인하였다. 또한, S7Comm Plus 프로토콜의 특성상 102번 포트가 열려 있기에 중요한 동작을 하는 PLC 기기일 경우, 타겟 PLC 기기로 선정하여 PLC를 멈추게 하는 공격도 가능할 것으로 예상한다. 따라서 본 연구를 통하여 제어망에서의 통신 및 제어 프로토콜을 이용한 보안 위협이 발생할 수 있다는 것을 알 수 있었다. 이는 외부망과 연결된 내부 접점 또는 외부에서 제어망으로의 침투가 가능한 공격 시나리오만 있다면 정상 작동 중인 PLC를 멈추어 버려 큰 피해를 발생시킬 수 있을 것으로 예상된다.

향후 연구 방향으로는 최근에 산업제어시스템을 대상으로 발생한 보안 위협 사례들을 분석하고, 최근 펌웨어 및 소프트웨어의 업그레이드 통한 암호화가 적용된 제어망 프로토콜에 어떠한 보안 기법들이 사용되었는지에 대한 조사 연구와 프로토콜의 취약성을 통하여 새로운 보안 위협에 대한 시나리오 및 그에 대응하는 방안을 연구할 계획이다.

References

[1] Aura, T., “Strategies against replay attacks,” In Proceedings of the 10th IEEE Computer Society Foundations Workshop, Rockport, MA, IEEE Computer Society Press, pp. 59-68, 1997.

[2] Denning, D. and Sacco, G., “Timestamps in key distribution protocols,” Communications of the ACM, Vol. 24, No. 8, pp. 553-536, 1981.

[3] FA Journal, “Siemens wins with TIA Portal,” 2013.

[4] Gong, L. and Syverson, P., “Fail-stop protocols: An approach to designing secure protocols,” In 5th International Working Conference on Dependable Computing for Critical Applications, pp. 44-55, 1995.

[5] Jung, I. K., “A Development Method of Web System Combining Service Oriented Architecture with Multi-Software Product Line,” The Journal of Society for e-Business Studies, Vol. 24, No. 3, pp. 53-71, 2019.

[6] Kim, J. Y., “Understanding and importance of industrial control system security,” SK Infosec Official Blog, 2016.

[7] Kwon, J. W. and Park, J. H., “The new paradigm of malware, Stuxnet,” AhnLab Special Report 3, 2010.

[8] Lee, J. H. and Kim, U.-N., “Standard Introduction-Industrial Control System Security Requirements,” TTA Journal, Serial No. 173, pp. 62-66, 2017.

[9] Lei, C.., Donghong, L.., and Liang, M., “The spear to break the security wall of S7 CommPlus,” BlackHat.

[10] Malladi, S., Alves-Foss, J., and Heckendorn, R. B., “On Preventing Replay Attacks on Security Protocols,” Proc. International Conference on Security and Management, 2002.

[11] Monn, G. Y., “Stuxnet’s Resurrection? Iran claims Israel has attacked,” security news, 2018.

[12] Na, J. H., “Safe firmware update of ITU-T SG17 industrial control system,” TTA ICT Standard Weekly, 2016.

[13] Sohn, J. M., Lee, I. T., and Lim, H. C., “Enhancement of Industrial Control Systems(ICS) Security for Service Company,” The Korea Service Management Society, Vol. 20, No. 4, pp. 183-200, 2019.

[14] Spenneberg, R., Brüggemann, M., and Schwartke, H., “PLC-blaster: a worm living solely in the PLC,” in: Black Hat Asia 2016, Singapore, p. 16, 2016.

[15] Syverson., P., “A taxonomy of replay attacks,” In Proceedings of the Computer Security Foundations Workshop(CSFW97), pp. 187-191, 1994.

[16] Wire Shark Wiki, https://wiki.wireshark.org/S7comm.

[17] Xu, Y., Yang, Y., Li, T., Ju, J., and Wang, Q., “Review on cyber vulnerabilities of communication protocols in industrial control systems,” 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, pp. 1-6, 2017.

저 자 소 개

최동준	(E-mail: zzczzc123@cau.ac.kr)
2018년 2월	순천향대학교 정보보호학과 졸업
2018년 9월~현재	중앙대학교 융합보안학과 (석사과정)
관심분야	Vulnerability analysis, System Security, CPS

이재우	(E-mail: jaewoolee@cau.ac.kr)
2006년	서울대학교 컴퓨터공학부 (학사)
2008년	서울대학교 컴퓨터공학부 (석사)
2017년	University of Pennsylvania, Ph.D in Computer and Information Science
2018년~현재	중앙대학교 산업보안학과 조교수
관심분야	실시간 시스템, 사이버 물리 시스템 보안