Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1305

스마트 팩토리 망에서 DPI와 자기 유사도 기술 기반의 OPC-UA 프로토콜 게이트웨이 융합 보안 기술*

심 재 윤,† 이 준 경‡
㈜나온웍스

Convergence Security Technology of OPC-UA Protocol Gateway based on DPI & Self-Similarity for Smart Factory Network*

Jae-Yoon Shim,† June-Kyoung Lee‡
NAONWORKS Co., Ltd.

요 약

스마트 팩토리는 제품의 전 생산 과정에 정보통신기술(ICT: Information and Communications Technologies)을 접목하여, 생산 비용의 절감 및 공정 개선 등을 이룰 수 있는 지능형 공장을 의미한다. 스마트 팩토리를 구현하기 위해서는 필연적으로 내부 설비들이 외부 네트워크와 연결되어야 하며, 이는 기존 폐쇄 망으로 운영되던 설비들이 외부 네트워크에 노출됨으로써 보안 취약성 증가하게 된다. 이러한 문제점을 해결하기 위해서 일반 네트워크에 사용하고 있는 보안 장비를 적용할 수는 있으나 이 방법만 가지고는 스마트 팩토리 망에서의 보안 위협을 완벽하게 차단하는 것은 불가능하며 보안 침해 사고가 발생 시 물리적, 경제적 피해는 산정할 수 없을 정도로 클 것이다. 이에 본 논문에서는 스마트 팩토리에 적용 가능한 보안 기법들을 알아보며 안전한 스마트 팩토리를 위한 전용 보안 게이트웨이 및 보안 게이트웨이가 가져야할 주요 융합 보안 기술을 제안한다.

ABSTRACT

The smart factory, a combination of ICT technology to the entire production process of a product, means can you intelligent factory is to achieve such reduction and process improvement of the production cost. To implement the smart factory, inevitably must have an internal equipment connections to the external network, this is by equipment which is operated by the existing closure network is exposed to the outside network, the security vulnerability so that gender is increased. In order to solve this problem, it is possible to apply security solutions that are used in normal environments. However, it is impossible to have just completely blocking security threats that can occur in a smart factory network. Further, considering the economic damage that can occur during security breach accident, which cannot be not a serious problem. Therefore, in this paper, a look to know the security measures that can be applied to smart factory, to introduce the main fusion security technology necessary to smart factory dedicated security gateway.

Keywords: Smart Factory, DPI(Deep Packet Inspection), OPC-UA, Protocol Gateway, Convergence Security

Received(09. 01. 2016), Accepted(09. 28. 2016)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보보호핵심원천기술개발사업의 연구결과로 수행되었음(IITP-2016-B0717-16-0119).
† 주저자, jyshim@naonworks.com
‡ 교신저자, darkelan@naonworks.com(Corresponding author)

I. 서 론

대한민국은 제조업의 비중이 높은 나라중의 하나로 과거 국가 경제 발전 계획의 일환으로 제조업 육성 정책을 펼친 결과 1960년대 이후 제조업의 지속적인 성장을 이끌었고 경제 성장을 견인하였다. 70년대 경공업 중심의 제조업을 시작으로 90년대 전자공업 등이 부상하고 최근에 와서는 자본 및 기술 집약적인 제조업 형태를 이루고 있다. 하지만 최근에 들어서 저유가와 중국의 성장률 둔화, 그리고 생산인력의 감소 등에 따르는 복합적인 문제점으로 인해 점점 경쟁력을 잃어가고 있는 것이 현실이며 제조업 중심의 수출 경쟁력을 강화할 수 있는 방법이 무엇보다도 절실한 시점이다. 이러한 상황을 극복하기 위해서 제조업의 세계 최고 수준의 독일은 2011년 '하이테크 비젼 2020'에 ICT(Information and Communications Technologies) 융합을 기반으로 한 제조업 혁신 전략인 인더스트리 4.0 을 주요 테마로 포함시켜 강도 높게 추진하였다. 인더스트리 4.0은 전체 생산 공정에 ICT 기술을 융합하여 제조업의 전반적인 경쟁력 향상에 목표를 두고 있다. 이에 국내에서도 선진국의 사례를 본받아 제조업 혁신 3.0 프로젝트를 추진하고 있다. 제조업 혁신 3.0 프로젝트의 일환으로 정부는 IT, SW, 사물 인터넷 융합으로 2020년까지 1만개 공장의 스마트화 추진 계획을 가지고 있다. 민관 공동으로 1조원 규모의 제조혁신 재원을 조성하고, '스마트 팩토리 추진단'을 구성하여 IT, SW 역량이 부족한 중소/중견 제조기업의 스마트화를 맞춤 지원하도록 하고 있다.

산업통상자원부 보도에 따르면 지금까지 1,240여개의 스마트 팩토리 구축을 지원하여 생산성을 25%나 향상시키는 성과를 거두었으며 2016년 한 해에만 정부는 약 800개사(누적 2,000개사) 스마트 팩토리 구축 지원에 나설 계획을 가지고 있다. 이처럼 정부는 갈수록 악화되는 제조업의 경쟁력 향상을 위해 스마트 팩토리 구축에 속도를 내는 실정이지만 자세히 들여다보면 정작 이러한 구축과정에 스마트 팩토리의 보안성 확보를 위한 적합한 보안 가이드라인이 제안되지 않은 것은 매우 우려되는 점이다. 이러한 현실에서 추후 보안사고 발생 시 피해 업체의 수와 규모는 산정할 수 없을 정도로 클 것이다.

본 논문은 산업용 프로토콜 전용 패킷 필터링 기술과 자기 유사도 분석 및 상관분석 기술과 같은 스마트 팩토리에 특화된 보안 기법들을 알아보며 안전한 스마트 팩토리를 위한 프로토콜 변환기능을 갖는 OPC-UA 프로토콜 보안 게이트웨이와 산업용 제어 프로토콜 보안 게이트웨이가 가져야할 주요 융합 보안 기술을 제안한다.

II. 스마트 팩토리 네트워크 보안의 문제점

산업제어 시스템에 대한 여러 보고서의 결과[1][2]에 따르면 네트워크 보안에서의 문제점은 다음과 같다.

2.1 폐쇄된 네트워크 정책

스마트 팩토리는 기본적으로 인터넷이 연결되지 않은 고립된 네트워크, 즉 폐쇄된 네트워크를 보안의 기본으로 삼고 있다. 폐쇄된 네트워크가 우리의 기대보다 안전하지 않다는 사실은 스턱스넷[3]과 한수원 사이버테러 보안사고[4]로 증명되었다. USB 등의 비인가 매체나 이-메일 첨부파일 등을 통한 스피어 피싱(spear phishing) 공격으로 일단 내부 네트워크에 침투할 수 있다면 외부보다 보안이 덜 적용된 내부 네트워크는 공격하기 쉬운 표적이 될 것이다. 또한, 높은 수준의 스마트 팩토리 구현을 위해서는 설비가 인터넷에 연결되어야 함으로 폐쇄된 네트워크 정책은 더 이상 유효할 수 없는 상황이다.

2.2 보안이 고려되지 않은 산업용 프로토콜

폐쇄되고 신뢰된 네트워크(trusted network)에서의 사용을 전제로 한 산업용 프로토콜들은 보안이 중요해지기 이전에 만들어진 만큼 다음과 같은 문제점을 가지고 있다.

2.2.1 프로토콜 정보 암호화 부재

제어 스테이션과 제어기(Controller) 간의 송수신 패킷을 분석하여 프로토콜 유형 및 메모리 정보 등을 파악할 수 있어 취약점에 노출되어 있다.

2.2.2 통신 주체간의 식별 및 인증 부재

임의의 통신 주체간의 상호 인증 과정 없이 통신이 가능한 구조로 공격자 또는 유효하지 않은 주체로부터의 접근 허용으로 취약점에 노출되어 있다.

2.2.3 프로토콜 제어데이터 유효성 검사부재

패킷에 포함된 값의 유효성 또는 값 읽기/쓰기에 대한 접근 권한이 유효한지를 확인 없이 그대로 전달하는 취약점에 노출되어 있다.

III. 관련 연구 및 동향

산업 제어 시스템에서 사용 가능한 보안 기술은 다음과 같다.

3.1 DPI(Deep Packet Inspection)

DPI 기술은 기본적으로 패킷의 프로토콜 데이터(Payload)의 내용까지 확인하는 기술을 의미한다[5][6]. 패킷의 프로토콜 데이터 내용을 보게 되면서 서버와 클라이언트간의 프로토콜 규약 정보까지 파악이 가능하고 정상적이거나 비정상적인 통신이 이루어지는지 파악이 가능하다.

SCADA, HMI와 같은 제어스테이션(Control Station)에서 PLC(Programmable Logic Controller) 등의 제어기에 요청하는 프로토콜 프레임은 대개 엔지니어링이 종료된 시점에서 변경되지 않으며 정해진 동작이 반복되는 패턴을 가지고 있다. 즉, 미리 정한 커맨드나 메모리 영역에 대한 읽기/쓰기 요청이 패턴화 되어 나타난다. 이에 그 패턴을 Rule 화하여 입력해두고 패턴에 어긋나는 요청이 시도되면 비정상 요청이 시도됨을 감지하여 파악할 수 있게 된다.

이상에서 언급한 DPI 기술의 적용 범위는 제어스테이션(SCADA/HMI)과 제어기(PLC) 사이인 공장자동화 레벨에서의 사용으로 한정된다. 극단적인 실시간성이 요구되는 제어 프로토콜이나 로봇/모션 제어 레벨의 경우 DPI 기술을 적용함에 있어 패킷 처리 모드(proxy/bridge), 보안 처리 모드(탐지/차단) 등과 같은 패킷 처리 지연 시간 감소를 위한 추가적인 고려가 필요 하다.

3.2 OPC(OPC Classic)

OPC(Ole for Process Control)는 산업자동화 시스템의 공정 데이터 통합을 위한 프로토콜로서 1996년 OPC Foundation에 의해 표준이 처음 발표된 프로토콜이다. 이름에서도 알 수 있듯이 Microsoft Windows 의 OLE (COM/DCOM) 기반 기술위에 구현된 프로토콜로서 주 대상이 Windows 운영체제에서 동작하는 제어스테이션 프로그램이 되었다[7]. OPC를 사용하게 됨으로써 PLC의 특정 프로토콜(Modbus/Profibus 등)을 표준화된 인터페이스 SCADA나 HMI로 제어스테이션에서 손쉽게 연결할 수 있도록 만들어 주었다. 이와 같은 이점에도 불구하고 Windows 플랫폼에 종속적인 한계를 지님에 따라 OPC 프로토콜을 제어기 내부에서 구현하기 어려웠으며, 통신 타임아웃을 별도로 설정할 수 없는데다가 방화벽에 친화적이지 않은 문제점들이 존재하게 되어 다음에 설명할 OPC-UA가 출현하게 되었다.

3.3 OPC-UA(OPC-Unified Architecture, IEC62541)

OPC Foundation에 의해 2006년 처음 발표된 프로토콜로 이전 OPC 프로토콜에 비해 향상된 기능을 가진다.

또한 기존 OPC 프로토콜이 DA(Data Access), HDA(Historical Data Access),

Table 1. OPC-UA Security Technologies

	Main Goal(s) / Algorithm(s)/ Standard(s)	Usage
MACs	Authentication, Integrity HMAC-SHA1 HMAC-SHA256	Message authentication
Signature	Authentication, Integrity RSA-SHA1	Signing certificates, security handshaking
Symmetric Encryption	Confidentiality AES-128-CBC AES-192-CBC AES-256-CBC	Message Encryption
Asymmetric Encryption	Confidentiality RSA-PKCS1 RSA-OAEP	Security handshaking
Key Generation	Confidentiality P-SHA1	Session Key generation
Certificates	Authentication, Authorization X.509 X.509v3 (Extensions)	Application authentication, user authentication, key exchange

Table 2. IEC62541 Overview

ID	Title
IEC TR 62541-1	OPC Unified Architecture Part 1: Overview and Concepts
IEC TR 62541-2	OPC Unified Architecture Part 2: Security Model
IEC 62541-3	OPC Unified Architecture Part 3: Address Space Model
IEC 62541-4	OPC Unified Architecture Part 4: Services
IEC 62541-5	OPC Unified Architecture Part 5: Information Model
IEC 62541-6	OPC Unified Architecture Part 6: Mappings
IEC 62541-7	OPC Unified Architecture Part 7: Profiles
IEC 62541-8	OPC Unified Architecture Part 8: Data Access
IEC 62541-9	OPC Unified Architecture Part 9: Alarms and Conditions
IEC 62541-10	OPC Unified Architecture Part 10: Programs
IEC 62541-11	OPC Unified Architecture Part 11: Historical Access
IEC 62541-13	OPC Unified Architecture Part 13: Aggregates
IEC 62541-100	OPC Unified Architecture Part 100: Device Interface

A&E(Alarm & Events) 등 여러 개의 서비스로 나누어져 있던 것을 단일 서비스로 통합하여 제공한다. 2011년 OPC-UA는 IEC에 의해 IEC62541의 산업 표준에 지정되기에 이르렀으며 내용은 다음의 "Table 2"와 같다[9].

IV. 스마트 팩토리 융합 보안 기술

이상적인 환경에서는 제어스테이션과 제어기 모두 보안 프로토콜을 이용하여 서로 안전하게 데이터를 송수신해야 한다. 하지만 폐쇄되고 신뢰된 네트워크 환경을 전제로 만들어진 보안이 결여된 기존 프로토콜로 통신하는 수많은 제어스테이션과 제어기가 전 세계의 주요 시설들에 이미 설치되어 동작되고 있는 실정이다. 운영 중인 제어 스테이션과 제어기 전부를 보안 프로토콜을 적용하는 것은 시간과 비용 문제로 인해 어렵기 때문에 이상적이지 못한 현실 상황에 적합한 보안 솔루션의 개념 도입이 시급한 형편이다.

이에 본 논문에서는 Fig.1과 같은 형태의 스마트 팩토리 전용 보안 게이트웨이 및 보안 장비가 가져야 할 융합 보안 기능을 제안한다.

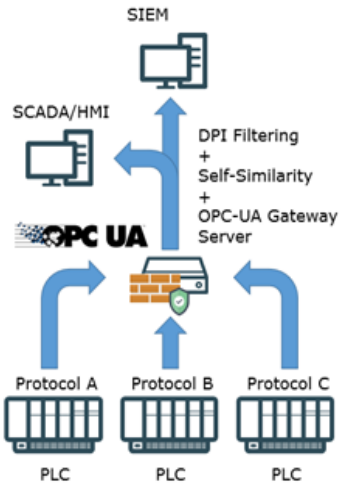

Fig. 1. Overview of Security Gateway System

첫째, 산업용 프로토콜 DPI 기술과 OPC-UA 프로토콜 게이트웨이 기술을 단일 보안 장비에서 구현한다. DPI 기능만을 적용한 장비만으로 보안을 구축하면 이상 징후 탐지는 가능하지만 프로토콜 보안이 되지 않는다. 반면에 OPC-UA 프로토콜 게이트웨이 기능으로만 보안을 구축하면 프로토콜 보안은 되지만 변경할 수 없는 기존 시스템에 대한 이상 징후 탐지는 할 수가 없다. 따라서 두 기술을 모두 사용해야 보다 안전한 보안 시스템을 구축 할 수 있다. 하지만 장비를 여러 종류 설치하면 필연적으로 비용과 유지보수 문제가 발생한다. 본 논문에서 제안하는 기술은 DPI 기술을 기본으로 수행하며 기존 SCADA, HMI 등 별도의 장치에서 제공되는 OPC-UA 프로토콜 게이트웨이 기술을 내장함으로서 보안 및 서비스를 함께 제공하여 도입 비용 절감 등의 경제성을 확보할 수 있다.

둘째, 보안 감사 데이터를 상위 보안 이벤트 분석 시스템으로 안전하고 정확하게 전달할 수 있는 기능도 갖추어야 한다. 자기 유사도 분석 및 상관관계 분석을 위한 이벤트 데이터 제공자로서의 역할을 충실히 수행하는 기술이 필요하다.

본 논문에서 제안한 스마트 팩토리에 특화되어 통합된 보안 게이트웨이가 제공하는 보안 기술은 다음과 같다.

4.1 산업용 프로토콜 전용 패킷 필터링 기술(DPI Filtering 기술)

일반 방화벽 장비는 IP와 포트에 기반한 필터링만을 수행하므로 패킷 내 데이터의 내용을 확인할 수 없는 단점을 가지고 있다. 산업용 프로토콜 필터링 기술을 수행하려면 프로토콜에 대해 알아야하고 패킷의 내용을 들여다 볼 수 있는 기술이 필요하다. 산업용 프로토콜 전용 필터링 기술은 제어스테이션과 제어기 사이에 송수신되는 모든 패킷을 대상으로 해당 기술이 적용된다. 이 기술은 로컬 네트워크에서 제어기로 전달되어야 하는 패킷의 Payload 부분을 분석하여 정적 및 동적 정책에 따라 패킷을 통과시키거나 차단시킨다. 이러한 동작을 수행하여 제어 설비의 공격을 사전에 탐지 및 차단할 수 있는 선제적 방어 수단을 확보할 수 있게 된다.

4.2 자기 유사도 분석 및 상관분석 기술

1:29:300의 법칙으로도 불리는 하인리히 법칙이 있다[10]. 대형 사고가 발생하기 전에 그와 관련된 수많은 경미한 사고와 징후들이 반드시 존재한다는 것을 밝힌 법칙이다. 산업제어 시스템에 대한 사이버 공격도 이와 유사한 징후들이 존재한다. 그러나 이런 징후를 개별 장치에서 탐지하는 것은 불가능에 가깝다. 따라서 자기 유사도 분석 및 상관 분석 기술을 스마트 팩토리 망 통합 보안 게이트웨이에 적용한다면 다양한 공격 징후를 감지하여 대형 보안 사고를 방지할 수 있을 것이다. 나아가서 보안 게이트웨이에서 수집된 각종 통계 및 이벤트 데이터를 상위 보안 이벤트 분석(SIEM, Security Information And Event Management) 시스템에 전달하여 빅 데이터(Big Data) 기반의 전역적 분석을 시스템 차원에서 수행한다면 스마트 팩토리 네트워크의 이상 징후를 조기에 탐지 및 차단할 수 있을 것이다.

4.3 OPC-UA 프로토콜 게이트웨이 기술

OPC Classic 은 PLC 등의 프로토콜 통합에 대한 표준 인터페이스 정의에 치중되어 상대적으로 보안이 결여된 문제점이 있었으나 OPC-UA 의 등장으로 기존 프로토콜 통합의 기술에 추가로 보안이 대폭 강화되었다.

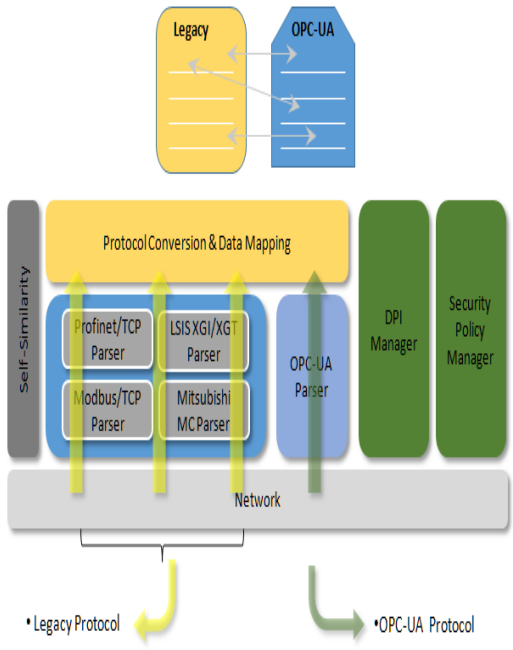

Fig. 2. OPC-UA Security Gateway Architecture

본 논문에서는 이상에서 언급한 DPI 보안 기술, 자기 유사도 및 상관관계 분석 기술, 프로토콜 변환 및 제어 메시지 매핑 기능을 포함하는 OPC-UA 프로토콜 보안 게이트웨이 전체적인 시스템 아키텍쳐를 Fig.2와 같이 정의하였다. OPC-UA 프로토콜 보안 게이트웨이를 통해 보안성이 없는 기존 프로토콜이 OPC-UA 프로토콜로 연계 가능하고 DPI 보안 기술, 자기 유사도 및 상관관계 분석 기술을 통해 보안성을 확보함으로써 기존의 설비를 변경하지 않고도 보안이 되지 않은 기존 프로토콜에 보안을 강화한 서비스를 제공할 수 있게 된다.

또한 기존 OPC Classic 프로토콜이 수행하던 MES(Manufacturing Engineering System), ERP(Enterprise Resource Planning) 및 PLM(Product Lifetime Management) 등의 외부 시스템과의 인터페이스도 OPC Classic 프로토콜이 방화벽을 이용하여 사용하던 터널링(Tunneling)과 같은 추가적인 기법이 필요 없이 OPC-UA 프로토콜 게이트웨이 기술을 통합 보안 게이트웨이 기술에 적용하면 보안성이 확보된 스마트 팩토리 프로토콜 게이트웨이 구현이 가능할 것이다.

V. 결 론

본 논문에서는 스마트 팩토리 보안 문제점들을 확인하였으며 그에 대한 현재 사용가능한 방안들을 알아보았다. 그리고 더 나아가서 스마트 팩토리 전용 보안 게이트웨이가 가져야할 융합보안 기술을 제안하였다.

기술의 발전에 따라 이더넷이 아닌 전용 필드버스나 시리얼 인터페이스를 사용하던 제어기가 이더넷 인터페이스를 사용하는 추세가 점점 늘어나고 있으며 사물 인터넷(Internet of Things)과 같은 기술트렌드의 확산으로 사물이 센서와 통신기능을 내장하여 별도 제어기의 도움 없이 스스로 인터넷에 연결되는 상태에까지 이르렀다. 산업 제어 네트워크 보안도 이러한 시대적인 변화에 빠르게 대응해야 하지만, 산업 제어 설비의 교체 주기가 긴 특징과 기존 설비에 대한 교체 비용 등의 문제들로 인해 전 구간에 대한 보안 프로토콜 구현 완료에는 상당 기간 시간이 걸릴 것으로 예상된다. 당분간은 제안된 주요 기능을 가진 보안 장비가 스마트 팩토리의 핵심 보안 및 서비스 기능을 담당하는 형태를 가질 것으로 전망한다.

본 논문에서 제안한 개념들을 통해 스마트 팩토리 구축 시 참고할 수 있는 보안 방안이 될 것이며, 비슷한 상용 제어기를 사용하는 국가 기간망의 산업제어 시스템, 스마트 그리드, 스마트 빌딩 그리고 스마트 홈 등의 보안에도 역시 적합할 것이다.

향후 연구에서는 본 기술을 적용함에 따른 다양한 제어기 및 제어스테이션의 정보처리성능 및 대역폭 영향성평가와 같은 후속 연구가 수행될 것이다.

References

[1] Y.-H. Chen, "Introduction of information security for industrial control system," Korea Institute of Information Security and Cryptology, 19(5), pp. 52-59, Oct. 2009.

[2] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to industrial control system security," NIST SP800-82, Jun. 2011.

[3] N. Falliere, L. O. Murchu, and E. Chien, "Win32.stuxnet dossier," Symantec Security Response, Feb. 2011.

[4] Y.S. Choi, "Middle investigation reports for korea hydro & nuclear power plant cyber terror incidents," The Joint Investigation Team for Personal Information Crimes, Mar. 2013

[5] S.W. Shin, D.H. Kang, K.Y. Kim, and J.S. Jang, "Analysis of deep packet inspection technology," Electronics and Telecommunications Trends, 19(3), pp.117-124, Jun. 2004.

[6] R. Stiennon, "DPI: next phase of firewall technology," Technology T-18-0340 Report, Gartner Group, Nov. 2002.

[7] OPC Foundation, "OPC common 1.10 specification," OPC Task Force, Dec. 2002

[8] Nathan Pocock, Darek Kominek, and Paul Hunkar, "OPC-UA security how it works," Information Revolution 2014, Aug. 2014

[9] "OPC unified architecture - part 1:overview and concepts," IEC62541, International Electrotechnical Commission, Feb. 2010

[10] H.W. Heinrich, Industrial accident prevention : a scientific approach, McGraw-Hill, New York, 366pg Jan. 1931

〈저 자 소 개〉

심 재 윤 (Jae-Yoon Shim) 정회원
2005년 2월: 수원대학교 컴퓨터학과 졸업
2005년 2월~2011년 1월: ㈜이지엔에스 전임연구원
2011년 1월~2015년 10월: ㈜싸이몬 차장
2016년 1월~현재: ㈜나온웍스 책임연구원
〈관심분야〉 산업제어시스템 보안

이 준 경 (June-Kyoung Lee) 종신회원
1993년 2월: 인하대학교 전자계산학과 졸업
1995년 2월: 인하대학교 전자계산학과 석사
2000년 8월: ㈜LG정보통신 선임 연구원
2007년 7월~현재: ㈜나온웍스 대표
〈관심분야〉 네트워크, 융합 보안