사물인터넷 환경에서의 보안 관제 방향에 관한 연구

고근호* · 이성렬** · 안성진***

요 약

정보통신기술의 급진적인 발달로 인해 우리 주위의 모든 사물들이 인터넷으로 연결되어 서로 정보를 주고받으며 각각의 사물들이 제공하던 것 이상의 새로운 가치를 제공하는 사물인터넷(IoT) 시대를 맞이하고 있다. 사물인터넷 환경에서는 기존과 다르게 인터넷에 연결되는 사물의 수가 급격히 증가하기 때문에 그만큼 보안 위협도 많아지게 될 것이다. 또한 셀 수 없이 많은 사물들을 어떻게 보호하고 관리할 것인지에 대해 새롭게 생각해 볼 필요가 있다. 본 논문에서는 기존의 보안 관제의 역할과 절차에 대해 살펴본다. 아울러 IoT 환경에서의 보안 관제의 방향에 대해 소개한다.

A study on the direction of security control of IoT environment

Keunho Koh* · Sungryoul Lee** · Seongjin Ahn***

ABSTRACT

With radical development of information and communication Technology, Internet of Things(IoT) era – all the things around us are connected through internet so that it enables objects to exchange data with connected devices and is expected to offer new advanced services that goes beyond the value where each existing objects could have offered respectively – has come. Concerns regarding security threat are being raised in adopting IoT as the number of internet-connected appliances are rapidly increasing. So, we need to consider how to protect and control countless objects. This paper covers the role and procedures of existing security control. Futhermore, it provides information about the direction of security control when it comes to IoT.

Key words : Internet of Things, security threat, security control

접수일(2015년 9월 18일), 수정일(1차: 2015년 9월 21일, 2차: 2015년 9월 22일), 개재확정일(2015년 9월 24일)

* 성균관대학교 컴퓨터교육과
** ETRI 부설연구소
*** 성균관대학교 컴퓨터교육과, 교신 저자

1. 서 론

최근 들어 TV나 책에서 IoT(Internet of Things)에 관련된 내용을 접하는 경우가 종종 있을 것이다. 지금까지 인터넷(Internet)은 컴퓨터, 스마트폰 등에만 연결되어 있었다. 하지만 곧 다가올 세상에는 컴퓨터, 스마트폰뿐만 아니라 냉장고, 화분, 전등, 에어컨, 자동차, 의료기기, 주위의 온도·밝기·위치 등을 파악하는 센서 등 셀 수 없이 많은 종류의 사물들이 인터넷에 연결되어 서로 데이터를 교환하게 된다. 요즘에도 인터넷에 연결된 사물을 몇몇 찾아볼 수 있지만, 이들이 서로 통신을 하려면 사람이 명령하거나 직접 조작해야 했다. 하지만 IoT가 가져오는 세상에는 사람의 개입 없이 사물들끼리 서로 정보를 주고받을 수 있게 된다. 집에 있는 전등을 예로 들면, 기존의 경우에는 컴퓨터나 휴대폰으로 전등의 상태나 조도를 제어할 수 있었다. 물론 전등이 인터넷에 연결되어서 가능했을 수도 있지만, 이는 진정한 의미의 사물인터넷이 아니다. IoT의 환경에서는 전등이 사람의 위치를 인식해 근처에 오면 자동으로 켜지거나 화재감지기를 통해 화재의 징후를 감지하면 전등이 빠르게 점멸되는 등 빛을 제공하는 전등 본연의 업무 외에 다양한 서비스를 제공할 수 있게 된다. 이와 같이 수없이 다양한 사물들이 연결된 인터넷을 사물인터넷이라 하며, 이렇게 인터넷에 연결된 수많은 사물들이 사람의 개입 없이 생성한 데이터들을 수집, 분석, 가공하여 사람들에게 서비스로 제공하는 것을 사물인터넷 서비스라 한다. 이는 우리에게 기존과는 다른 차원의 편리함을 제공하겠지만, 그에 못지않게 해결해야 할 과제가 많다. 그 중 하나로는 보안 관제를 들 수 있다. 기존에는 PC, 모바일 등으로 인터넷에 연결된 대상의 수가 한정되어 있었지만, 앞으로는 다양한 사물들이 연결되므로 보안 관제에 대한 시각을 달리해야 한다.

따라서 본고는 기존의 보안 관제와 IoT 환경에서 적합한 보안 관제 방향에 대해 다루고자 한다. 2장에서는 사물 인터넷의 구조와 기존의 보안관제의 역할 및 절차에 대해 알아보고, 3장에서는 새로운 보안 관제의 필요성과 IoT 보안 관제의 방향에 대해 알아본다. 4장은 결론 부분으로 이 글의 마무리를 맺는다.

2. 사물인터넷과 보안

2.1 사물인터넷의 구조

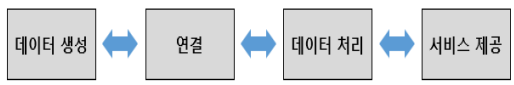
사물인터넷의 구조는 데이터 생성, 데이터 연결, 데이터 처리, 서비스 제공 이렇게 크게 4부분으로 구분할 수 있다[1].

데이터의 생성은 여러 사물들이 주위 환경의 정보들을 수집하여 서버로 전송하는 과정이다. 서버로 전송되는 데이터들은 사물에서 디지털화된 값으로 변환된다.

데이터의 연결은 사물들이 생성한 데이터들을 인터넷상의 서버로 전송하는 과정이다. 이더넷이나 3G/LTE와 같은 이동통신 기술을 이용해서 사물이 직접 인터넷에 연결될 수 있고, 스마트폰이나 모바일 라우터 같은 중개 장치를 통해 인터넷에 연결되기도 한다. 이렇게 사물들과 인터넷 사이에 연결되어 데이터를 전달해주는 장치를 IoT 게이트웨이라 한다.

데이터의 처리는 다양한 통신 기술을 통해 사물로부터 전송된 데이터들을 수집·저장·분석·가공하는 과정이다. 이 과정에서는 서버에 수집된 데이터들 중에서 필요한 데이터만 걸러내는 데이터 필터링 기술, 서로 다른 형식으로 전송된 데이터를 효율적으로 저장하는 데이터 저장 기술, 데이터로부터 유용한 지식을 추출하기 위한 데이터 과학 기술 등이 필요하다.

서비스 제공은 분석과 가공을 거친 데이터들이 사람들에게 판독될 수 있는 방식으로 나타내지는 과정이다. 스마트폰이나 컴퓨터에서 사용되는 어플리케이션이나 웹의 형태가 될 수도 있고, 키오스크나 디지털 사이니지와 같은 전용 디스플레이 장치를 통해 전달될 수도 있다.



(그림 1) 사물인터넷 구조

2.2 보안 관제

2.2.1 보안 관제 역할

보안시스템 통합 관리: 서로 다른 기종간의 에이전

트들을 모니터링 및 관리한다.

일관된 정책 구현: 중앙에서 일관된 정책을 통합 관리하여 일관성 있게 침해 사고에 대응할 수 있다.

신속한 대응처리: 모니터링, 사전 대응, 효율적인 정책 구현 등 침해 사고에 대한 사전 예방활동을 강화한다. 또한 실시간 감시, 장애 처리, 업무 중단에 대한 위협요소를 감소한다.

최적의 보안체계 운영: 정보자산의 보호에 대한 효과적인 방안을 마련할 수 있게끔 보안 환경을 구성한다.

2.2.2 보안 관제 절차

보안 관제의 수행 절차는 일반적으로 탐지, 분석 및 조치, 사고 조사, 복구 지원, 결과 보고의 식으로 이루어진다.[2]

- 탐지

탐지는 대상 기관의 정보 기술, 개인정보 등을 해킹, 바이러스 등과 같은 다양한 사이버 공격 시도를 사전에 알아내는 과정이다. 악성 코드, DNS 정상 작동 여부, 홈페이지 단절·지연·오류 등의 현상을 24시간 365일 내내 모니터링한다.

탐지하는 방법으로는 다음과 같다. 대상 기관의 통신망에 사이버 공격 정보를 수집하는 장치를 설치하고 실시간으로 모니터링해서 시스템 및 장비에서 발생하는 이벤트를 수집한다. 그리고 수집한 이벤트와 이전에 알려진 공격들을 분석해서 만든 탐지 패턴들을 비교·분석한다. 비교·분석 결과 공격 징후가 보이는 이벤트는 보안 관제 모니터링 시스템으로 전달된다. 또한 대상 기관으로부터 신고 접수를 통해서도 사이버 공격에 관한 정보를 수집할 수 있다.

- 분석 및 대응

분석 및 대응은 보안 관제 시스템에서 사이버 공격 관련 정보를 탐지하거나 대상 기관의 신고를 통해 접수된 공격 이벤트에 대해 조사 및 분석을 실시하여 실제로 사이버 공격을 당했는지 확인하고 공격 유형을 파악하여 그에 맞게 대응하는 과정이다.

탐지 결과 사이버 공격이라고 인정되면 우선 피해 유무를 파악하고 피해 확산의 우려가 있을 경우에는 공격 IP 차단 및 피해 시스템을 통신망에서 분리하거나 침입 차단 시스템 또는 라우터 등의 접근 제어 정책 설정을 통하여 피해가 더 이상 확산되지 않도록 필요한 조치를 수행하도록 한다. 만약, 시스템을 통신망에서 분리할 수 없는 경우에는 관련 시스템의 백업을 수행하고 백도어 및 시스템 취약점을 즉시 검사하여 제거한다.

- 사고 조사

사고 조사는 분석 및 대응 과정에서 수집, 분석한 침해 사고 관련 정보를 보고서로 작성하고 사고 조사 담당자에게 인계하여 침해당한 통신망의 로그 정보를 수집, 정밀 분석 및 피해 시스템 조사 등을 통하여 공격자 정보·공격 시간·공격 기술과 방법·피해 시스템의 보안 취약점 등 침해 사고의 원인을 알아내고 저장 자료 유출 및 관리자 권한 피탈 등의 피해 규모를 파악하는 과정이다. 사고 원인이 규명될 때까지 로그 자료 보존 및 관련 자료의 삭제 또는 피해 시스템의 포맷의 금지 등 증거 보존에 필요한 조치를 수행한다.

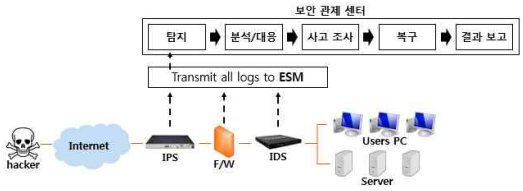
사고의 원인 및 피해 규모 파악 결과, 이상 징후 및 예상되는 사이버 위협에 대한 대응 전략을 수립하며, 발생된 사고 피해에 대한 보완 대책을 수립·지원한다. 침해 사고에 대한 정밀 분석 및 사고 조사가 완료되면, 이를 토대로 사이버 위협 경보 발령 여부, 공격자 추적 및 복구 지원 등 침해 유형별로 적절한 대응 방안과 추진 전략을 수립하고 그에 따라 필요한 조치를 한다.

- 복구

복구는 사이버 공격으로 인한 피해가 발생한 시스템에 대해 복구 기술을 지원함으로써 피해의 확산 및 재발 방지를 위한 과정이다. 사고 조사 단계에서 파악된 공격자 정보와 취약점 정보를 활용하여 피해 시스템이 정상적으로 운영될 수 있도록 신속하게 전문 기술을 제공하며 공격에 사용한 해킹 도구 및 기법을 토대로 해당 해킹 공격 탐지 기술을 개발하여 앞으로의 보안 관제 업무에 적용함으로써 동일한 침해 사고의 발생을 방지한다.

- 결과 보고

결과 보고는 침해 사고에 대한 사고 조사 및 복구 지원을 완료한 후에 사고 대응 결과 보고서를 작성하여 기록으로 유지하고 후에 유사한 침해 사고가 발생할 경우에 참고한다.



(그림 2) 기존의 보안 관제 체계도

방화벽(Firewall): 외부 네트워크에서 내부 네트워크로 접근하려면 반드시 거치도록 하여 내부 네트워크의 정보 및 자원을 보호하는 시스템이다. 방화벽의 기본 보안 정책은 내부 네트워크로부터 인터넷으로 나가는 모든 패킷은 허락하고, 인터넷으로부터 들어오는 모든 패킷은 거절한다. 또한 외부 인터넷으로부터 접근하는 패킷을 필터링하여 불법적인 패킷을 폐기시키거나, 인증을 통해 패킷을 허용한다.

침입 탐지 시스템(IDS): 네트워크에서 송·수신되는 이벤트를 실시간 모니터링하여 침입 발생 여부를 탐지하고 대응하는 자동화된 시스템이다. 침입 사실이 발견되면 즉시 휴대전화, 전자우편 등을 통해 관리자에게 알릴 수 있으며, 관리자의 부재 시에도 보안을 유지할 수 있게 한다.

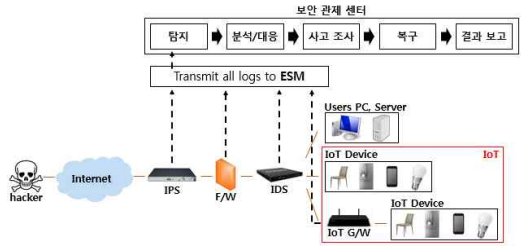
침입 방지 시스템(IPS): 수동적인 방어 개념의 침입 탐지 시스템(IDS)와는 달리 다양한 보안 기술을 이용하여 악성코드 및 해킹 등의 침입이 일어나기 전에 실시간으로 침입을 막고, 유해 트래픽을 차단하기 위한 능동형 보안 시스템이다.

ESM: IDS, IPS, 방화벽, VPN 등 다양한 종류의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템이다.

3. IoT 환경에서의 보안 관제

3.1 새로운 보안 관제의 필요성

기존에는 PC 및 모바일 중심으로 인터넷이 연결되었기 때문에 보호대상의 개수가 한정되어 있었다. 반면, IoT 환경에서는 주위의 모든 사물들에 센서가 내장되어 인터넷을 통해 서로 다양한 종류의 데이터를 수집하고 전송하게 된다. 이는 보호대상이 명확하지 않고 그만큼 보호해야할 대상이 늘어나게 됨을 의미한다. 하지만 현재의 보안 관제 시스템으로는 보호 및 관리가 어려울 수 있다.



(그림 3) IoT 환경에서의 보안 관제 체계도

그림 3에서 볼 수 있듯이 IoT 환경에서도 기존의 보안 관제 모델과 흡사하다. 기존 보안 관제와 동등하게 외부 인터넷망과 내부 네트워크의 경계점에 방화벽, IDS, IPS 등 네트워크 보안 장치를 설치한다. 차이점으로는 기존에는 PC와 모바일만 관제 대상이었지만 IoT 환경에서는 중간에 IoT 게이트웨이로 연결되는 IoT 사물과 직접 인터넷과 연결되는 사물도 추가로 관리해야 한다는 점이다.

기존의 PC, 스마트폰과 비슷한 성능, 사양 등을 지닌 사물의 경우는 기존의 보안 관제의 방식을 따르면 된다. 하지만 의자, 화분, 전등 등 인터넷에 연결되는 주위의 사물들 중 대부분은 기존의 PC, 스마트폰과는 비해 한정된 자원을 가지고 작동된다. 따라서 이들은 중개 장치인 IoT 게이트웨이를 통해 관리하는 것이 더 효율적이다.

3.2 IoT 환경에서의 보안 관제 방향

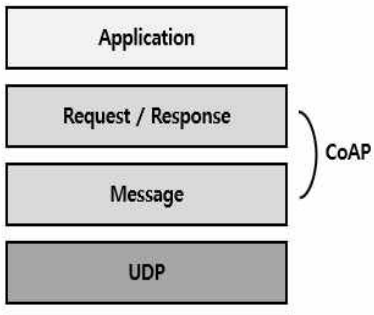
3.2.1 다양한 통신 방식을 수용

기존의 웹 공간에서는 HTTP라는 프로토콜로 통신할 수 있었지만 IoT 시대에는 다양한 사물들이 새로운 프로토콜을 통해 통신하게 될 것이다. 시계, 전등, 가전제품 등 일반적인 사물들은 비용 성능 등의 문제

로 PC, 스마트폰 등에서 사용되는 WiFi 대신 저렴한 무선 통신 장치나 잡음이 심한 유선을 사용하고 PC, 스마트폰에 비해 제한된 컴퓨팅 성능을 가지기 때문에 기존의 프로토콜로는 적합하지 않을 수 있다. 또한 각각의 사물의 특성상 모든 사물이 같은 프로토콜로 통신할 수 없으므로 여러 가지의 프로토콜이 혼재하게 된다. 이러한 사물들의 효율적인 데이터 전송을 위한 대표적인 프로토콜로는 CoAP, MQTT, XMPP 등이 있다[3].

- **CoAP(Constrained Application Protocol)**

CoAP는 저전력, 소용량 기기 등의 제한적인 네트워크 환경에서 사용되는 응용계층 프로토콜이다[4]. 그림 4과 같이 UDP를 기반으로 하는 Request와 Response가 상호작용하는 방식을 가진다[5]. 또한 CoAP 자체가 비동기적으로 사용된다. 따라서 CoAP를 사용하는 기기는 슬립 모드로 대기하다가 트래픽이 발생할 때만 처리하므로 기기의 전원을 절약할 수 있다.



(그림 4) CoAP의 추상적 계층

- **MQTT(Message Queue Telemetry Transport)**

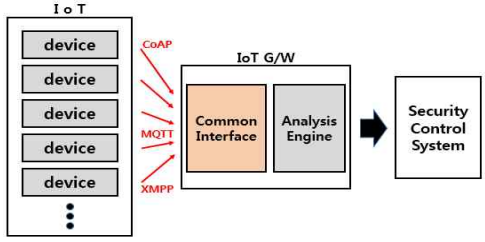
MQTT는 낮은 대역폭, 높은 지연, 데이터 제한 또는 불안정한 네트워크를 위해 설계된 프로토콜이다. MQTT는 Request/Response 방식을 대신한 Publish/Subscribe 방식으로 통신한다. MQTT는 기본적으로 Broker 서버와 Publish, Subscribe 클라이언트로 구성된다. Broker 서버는 2개의 클라이언트 사이에서 중개자 역할을 한다. Publish 클라이언트가 Topic을 발행하고 메시지를 Broker 서버로 전달하면, Subscribe 클라이언트는 서버로부터 Topic을 받게 된다[6].

(그림 5) Publish/Subscribe 방식 통신 모델

- **XMPP(eXtensible Messaging and Presence Protocol)**

XMPP는 XML 기반 인터넷 통신을 위한 오픈 프로토콜로 인터넷 상의 두 지점 간 통신 규격이다[7]. 두 지점은 이메일 주소와 같은 방식으로 표현되며 이들 지점 간 확장 가능한 메시지 그리고 프레즌스를 거의 실시간으로 전달해주는 규격이다[8]. 또한 XMPP는 적은 양의 정보를 전달할 때 적합하므로 MSN 메신저, 페이스북 등의 채팅이나 메신저에서 주로 사용되고 있다.

IoT 게이트웨이에 이렇게 많은 사물들의 통신 방식을 각각 지원하기 위해 개별적인 인터페이스를 가진다는 것은 현실적으로 어려울 수 있다. 뿐만 아니라 새로운 통신방식이 나올 때마다 그에 해당하는 인터페이스를 만들어야 하는 번거로움이 발생하게 된다. 따라서 다음과 같이 공통된 인터페이스를 가져야 한다. 또한 중앙 관제 시스템에서도 이러한 다양한 통식 방식을 통해 들어오는 정보들을 처리할 수 있어야 한다.



(그림 6) 공통 인터페이스를 통한 통신 구조

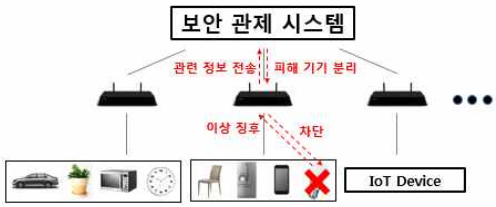
그림 6은 IoT 게이트웨이가 다양한 통신 방식을 가진 사물로부터 공통 인터페이스를 통해 데이터들을 수집해서 중앙 관제 시스템으로 전송하는 과정을 나타낸 것이다.

3.2.2 변화 관리 측정

IoT 환경에서는 사물의 수가 급격하게 증가하기

때문에 중앙 관제 시스템에서 모든 IoT 기기들을 관리하는데 어려움을 겪게 된다. 따라서 기존과는 다르게 중개 장치인 IoT 게이트웨이에서의 추가적인 역할이 필요하다.

IoT 게이트웨이는 인터넷에 직접 연결되어 센서나 사물들이 생성한 데이터를 전달해 주는 역할을 한다. 또한 데이터 수집 및 전송뿐만 아니라 사물의 전원장치의 오작동, 바이러스 및 해킹 등으로 인한 데이터의 트래픽 변화를 감지하고 이상 징후가 보이면 관련 정보를 중앙 관제 시스템으로 전송해야 한다. 중앙 관제 시스템에서는 관련 정보를 바탕으로 피해 확산 방지를 위해 공격 IP 차단 및 피해 기기를 통신망에서 분리하거나 침입 차단 시스템 또는 게이트웨이 등의 접근 제어 정책 설정을 통하여 피해가 더 이상 확산되지 않도록 조치한다. 따라서 중앙 관제 시스템에서는 모든 IoT 기기들을 대상으로 하지 않고 중개 역할을 하는 IoT 게이트웨이들만 관리하면 전체적인 보안 관리가 가능하게 된다.



(그림 7) IoT 게이트웨이의 관리 방식

3.2.3 종단간 암호화

지금까지 보면 수많은 정보들이 IoT 게이트웨이를 통해 중앙 관제 시스템으로 이동하게 된다. 앞서 소개한 새로운 통신 방식들은 모두 암호화를 지원하고 있지만, 일반적으로 암호화된 특정 정보가 무선 통신 기술을 통해 게이트웨이에 도착하면 게이트웨이는 이를 복호화하고 다시 암호화하는 과정을 거치게 된다. 게이트웨이에는 특정 정보가 일반 평문으로 저장되게 된다. 따라서 해커들의 공격 대상이 될 수 있다. 이를 방지하기 위해서는 발신부터 수신까지의 모든 단계에서 정보를 모두 암호화하는 방식인 종단간 암호화 기법을 이용해야한다[9,10]. 즉, 특정 정보가 한 사물에서 게이트웨이를 통해 인터넷까지 가는 동안 항상 암호로 이루어져 있으므로 IoT 게이트웨이에서도 해킹의 위험에 대비할 수 있게 된다.

(그림 8) 종단간 암호화 방식

위에서 다룬 기존과 IoT 환경에서의 보안 관제의 차이점을 정리하면 표 1와 같다.

<표 1> 기존과 IoT 환경의 보안 관제 비교

	기존	IoT 환경
보호 대상	PC, 모바일	주위 모든 사물
통신 방식	NetBiOS 등	CoAP, MQTT, XMPP 등
게이트웨이 기능	프로토콜 변환 네트워크간 연결	기존 + 변화 관리 측정
암호화 방식	공개키 암호화	종단간 암호화

4. 결 론

본 논문에서는 IoT가 가져오는 세상에서의 보안 관제 방향을 설계하기 위해 사물인터넷의 구조와 기존의 보안 관제의 역할 및 절차에 대해 알아보았다. 이를 바탕으로 IoT 환경이 오게 되면 기존의 보안 관제 방식으로는 어려움을 겪게 되므로 새로운 보안 관제의 필요성을 제시하였다. 또한 기존의 보안 관제와의 차이점에 대해 분석하고 그에 따라 IoT 환경에서의 보안 관제 방향 3가지를 다음과 같이 제안하였다.

- 다양한 통신 방식이 혼재하므로 이들을 수용할 수 있는 시스템이 요구된다.
- 기존의 게이트웨이에서 IoT 기기들의 변화 관리 측정하는 기능이 추가적으로 필요하다.
- 새로운 암호화 방식인 종단간 암호화 기술을 적용해야 한다.

참고문헌

[1] 김학용, '사물인터넷 개념, 구현기술 그리고 비즈니스', 홍릉과학출판사, 2014
[2] 안성진, 이경호, 박원형, '보안관제학', EHANMEDIA, 2014
[3] 박예찬, Thang Le Duc, 정순교, 염상길, 손민한, 추현승, "사물인터넷과 무선센서네트워크의 연결을 위한 게이트웨이 및 활용방안", 한국컴퓨터종합학술대회 논문집, 2015
[4] Z.Shelby, 'Constrained RESTful Environments (CoRE) Link Format',RFC 6690,2012
[5] J.Postel,'User Datagram Protocol",RFC 768,1980
[6] Message Queuing Telemetry Transport. http://mqtt.org
[7] XMPP Standards Foundation,http://xmpp.org/
[8] Jack Moffitt, 'Professional XMPP Programming with JavaScripted jQuery',2010
[9] Christopher Fife, blogs.citrix.com/2015/07/24/securing-the-iot-gateway
[10] 박철웅, 김기홍, 류재철, "이기종 전술통신망 종단간 암호화 통신을 위한 메커니즘", Journal of The Korea Institute of Information Security & Cryptology, VOL 24, NO 4,pp625-634,2014

[저 자 소 개]

고 근 호 (Keunho Koh)

2011년 성균관대학교 컴퓨터교육과

email : keuno0923@gmail.com

이성렬 (Sungryoul Lee)

2001년 서강대학교 컴퓨터학과 학사
2003년 서강대학교 컴퓨터학과 석사
1995년 서울대학교 컴퓨터공학과 박사

email : srlee0525@nsr.re.kr

안성진 (Seongjin Ahn)

1988년 성균관대학교 정보공학과 학사
1990년 성균관대학교 정보공학과 석사
1998년 성균관대학교 정보공학과 박사

email : sjahn84@gmail.com