저전력 블루투스의 보안 위협 요인들에 관한 연구★

전 정 훈*

요 약

최근 무선통신은 사물 인터넷의 등장으로 가전제품간의 통신연결뿐만 아니라, 여러 산업분야에서 근거리 통신매체로 널리 사용되고 있다. 그리고 이중에 가장 많이 사용되는 무선 통신 매체로는 와이파이(wifi)나 블루투스, NFC가 있다. 특히 블루투스는 컴퓨터의 주변 기기뿐만 아니라, 스마트 기기들 간의 통신에 널리 사용되고 있으며, 홈 네트워크 분야는 전자 제품들을 통제하는데 사용되고 있다. 그러나 블루투스의 보안 취약점들이 알려지면서, 이를 악용한 공격시도가 증가하고 있는 가운데, 블루투스의 활용범위가 확대되고 이에 따른 대응방안의 마련이 필요한 상황이다. 따라서 본 연구는 블루투스의 공격 사례 및 공격 기술들을 통해, 보안 위협요인들을 알아보고, 이에 대한 대응 방안을 제안함으로써, 향후 무선 네트워크 서비스의 보안성 향상을 위한 자료로 활용될 수 있도록 하고자 한다.

Study on the Security Threats Factors of A Bluetooth Low Energy

Jeon Jeong Hoon*

ABSTRACT

Recently, Wireless communication has been widely used as a short distance communication medium in various industrial fields as well as communication connection between home appliances due to the appearance of the Internet of Things. And Most commonly used wireless communication media include WiFi, Bluetooth, and NFC. Among them, Bluetooth is widely used for communication between smart devices as well as computer peripheral devices. And Bluetooth in the home network fields is being used to control electronic products. However, since Bluetooth security vulnerabilities are known, more and more attacks are being exploited. As the application range of Bluetooth is expanding, it is necessary to prepare countermeasures accordingly. Therefore, this study investigates the security threat factors of through Bluetooth'attack case and attack technology. And By proposing countermeasures against this problem, we intend to utilize it as data for improving the security of wireless network service in the future.

Key words : Low Energy Bluetooth, Internet of Things, Home networking, Beacon, Security threats factors, Smart Devices, Wireless network service

접수일(2017년8월22일), 수정일(1차: 2017년10월10일), 게재확정일(2017년10월24일)

★ 본 논문은 2016년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교/컴퓨터학과

1. 서 론

최근 사물 인터넷(internet of things)이나 클라우드 컴퓨팅(cloud computing), 빅 데이터(big data) 등의 다양한 IT 기술들이 융·복합되어 새로운 IT환경을 구축해 나아가고 있다. 특히 스마트폰이나 스마트기기, 사물인터넷기기 등은 융·복합 산업을 이끌어가고 있는 견인차 역할을 하고 있다 해도 과언이 아니다. 이러한 기기들을 연결하는 무선전송매체 중에 하나인 블루투스는 사물인터넷 및 스마트 기기들 간의 통신에 널리 사용되고 있으며, 단거리 무선 서비스를 제공하고 있다[1][2]. 와이파이(wifi)보다는 다소 속도가 느리지만, 전력 소모 측면을 비교해볼 때, 작은 기기나 전력 소모가 적은 장치 등에 유리하기 때문에 사물인터넷과 스마트 폰(smart phone) 등에 널리 사용되고 있다. 얼마 전까지만 해도, 스마트 폰의 사용이 점진적으로 증가함에 따라, 블루투스는 와이파이(wifi)가 해결하지 못하는 부분을 지원하는 기술에 불과했지만, 점차 일상생활에 널리 사용되는 친숙한 통신매체가 되고 있는 추세이다[1][2]. 그러나 블루투스의 여러 보안 문제점들이 속속 나타남에 따라, 이에 따른 대응방안이 필요한 상황이다.

따라서 본 논문에서는 블루투스의 공격사례 및 공격기법들을 통해, 보안위협요인들을 알아봄으로써, 향후 융·복합 산업을 비롯한 여러 응용분야에 대한 대응기술의 개발 및 분석을 위한 연구 자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 블루투스의 기술동향과 보안기능, 취약성에 대해 알아보고, 3장은 공격기술을 통한 위협요인분석을 한다. 그리고 4장의 대응방안과 마지막 5장의 결론 부분으로 이글을 마치도록 한다.

2. 관련연구

2.1 블루투스의 동향 및 전망

블루투스는 간편하면서 편리하며, 속도가 빠른 장점을 갖고 있다. 이러한 점들로 인해, 다양한 응용 서비스들이 등장하면서, 활용성이 점차 높아지고 있다. 특히 스마트폰은 블루투스의 응용범위를 더욱 넓혀줌으로써, 일상생활에서 보다 쉽게 접할 수 있도록 하였고, 2010년 4.0버전을 출시한 이후, 거의 7년 만에 새로운 업그레이드 기능을 선보이고 있어, 차세대 버전으로 사물인터넷 기술의 통신매체로 부상하고 있다[1]. 현재 최신 버전은 5.0으로 기존 버전과 다음과 같은 차이를 갖고 있다. 4.0버전은 최대 전송거리가 100m 이었으나, 5.0버전은 400m로 기존의 전송거리보다 약 4배정도 강해졌다. 그리고 최적의 통신거리는 10m에서 40m 를 지원하게 되었으며, 전송속도는 2배 이상 증가하였다. 또한 5.0버전은 별도의 페어링(pairing) 없이 주변의 비콘(beacon)과 다중통신이 가능하게 되었으며, 브로드캐스트의 용량이 8배나 늘어나, 다양한 서비스가 기대되고 있다. 이로써, 블루투스는 사물인터넷시대에 기기들의 연결매체로서 향후 와이파이와 상호 보완적인 존재로 공존하게 될 것으로 전망되고 있는 가운데, 앞으로의 전송거리 및 속도의 향상 등은 여러 산업분야에 큰 변화가 예상된다[2][3].

2.2 블루투스의 보안 기능

블루투스의 대표적인 보안기술은 3가지로 정리해 보면 다음과 같다[4]. 첫 번째로 PIN(Personal Information Number)입력 또는 저장된 링크키를 이용해 통신 장치를 식별하는 인증(authentication)기능이 있으며, 두 번째로는 도청에 의한 정보유출을 방지하기 위해 인증된 장치만 데이터에 접근을 허용하는 기밀성(confidentiality) 기능이 있다. 세 번째로는 통신장치별로 허용 가능 서비스만 제공하여 다른 서비스 이용을 차단하는 인가(authorization) 기능이 있다. 블루투스는 보안 매니저(security manager)를 통해 '서비스 관련 보안 정보관리'와 '장치관련 보안 정보관리', '프로토콜 및 응용프로그램의 보안관련 질의응답', '인증 및 암호화 수행'과 같은 장치 및 서비스에 대한 권한을 통제하기도 한다. 이밖에도 블루투스의 보안을 위해 보안 모드(security mode)를 1부터 4 레벨로 구분하고, 각 레벨에 따른 링크키를 생성 및 관리하고 있다[4].

2.3 블루투스의 보안취약성

블루투스의 보안취약성은 이미 알려진 무선 취약성

과 블루투스를 통한 주변기기의 인식, 인증에 관한 취약성 등을 포함하고 있다. 이러한 보안취약성들은 실제 침해사례로 나타나고 있으며, 2014년에는 국제 컨퍼런스 'POC2014'에서 도요타의 캠리와 현대 기아차가 제조한 소나타를 대상으로 모의해킹을 시연한 영상을 공개된바 있다.

(그림 1) 스마트 카 공격 시나리오[5]

그림1의 시연 내용을 요약해보면, 자동차 점검을 위해 사용되는 OBD2(On Board Diagnostic2)는 자동차에 탑재된 여러 전자장치(ECU)를 블루투스로 연결한다. 그리고 자동차 내의 OBD포트에 장착한 뒤, 관련 스마트폰을 이용해 블루투스로 연결하면, OBD2가 분석한 자동차의 여러 정보들을 볼 수 있다. 이와 같은 보안취약점은 다른 스마트폰으로도 공격대상 자동차 내에 부착된 OBD2 동글(dongles)로의 접속이 가능하기 때문에 공격자는 자동차에 사용되는 통신프로토콜인 'CAN(Controller Area Network)'에 명령을 내려 ECU의 조작이 가능하다[5]. 이밖에 블루투스의 또 다른 취약성으로는 DoS(denial of service)공격이나, Evaesdropping공격, 고정 PIN을 이용한 공격, Impersonation 공격, Frequency hopping 공격 등이 있으며[6]. 이중 Evaesdropping 공격은 블루투스를 이용해 전송되는 데이터 가로채기(intercept) 공격으로 주요 데이터나 PIN정보의 유출을 목표로 하고 있다[7].

최근에는 비콘(beacon)이 일 방향통신으로 보안에 안전하다고 생각할 수 있으나, 이와 같은 정보 왜곡에 따른 취약점이 가장 큰 문제가 되고 있다. [8]에 따르면 비콘 서비스는 MAC주소 또는 IP주소 등의 스푸핑(spoofing)공격과 세션 정보 및 개별 정보의 클로닝(cloning)공격, 지속적인 전파간섭 및 교란신호 공격으로 서비스가 오동작을 하거나, 블루투스 서비스 거부(BDoS) 공격 등에 매우 취약함을 언급하고 있다.

3. 위협요인

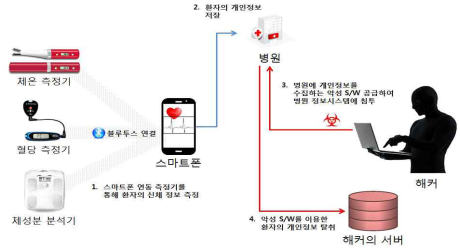
최근 블루투스는 사물인터넷 및 스마트기기 등으로 응용범위가 확대됨에 따라, 이에 따른 보안침해사례 또한 증가할 것으로 예상되고 있는 가운데, 침해사례들을 바탕으로 한 공격시나리오와 기법들에 대해 보안취약성과 위협요인들을 알아본다.

3.1 공격 시나리오

3.1.1 시나리오별 보안 취약성

(그림 2) 커넥티드 카를 통한 공격 시나리오

그림2의 시나리오는 커넥티드 카(connected car)에 악성봇이 포함된 자동차의 진단도구 프로그램을 통해, 블루투스로 원격에서 고객정보의 유출 및 기능 조작이 가능함을 보이고 있다[5].



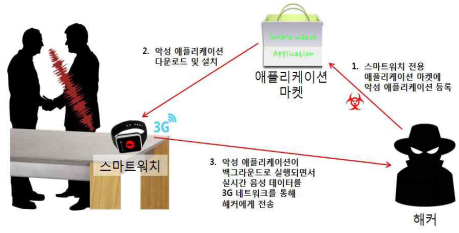
(그림 3) 병원 정보시스템의 공격 시나리오

그림3의 시나리오는 원격 의료서비스에 대한 공격으로 어플리케이션 로그인 시, 아이디와 비밀번호를 포함한 개인정보가 평문으로 전송되는 취약점을 악용해, 개인정보 뿐만 아니라 의료정보에 대해서 가로채

기 공격과 파라미터의 변조(modification)공격이 가능함을 보이고 있다[5].

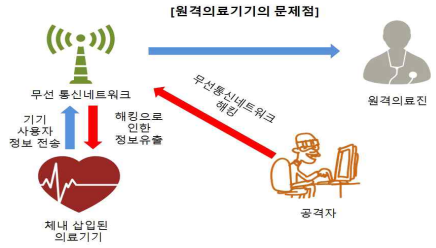
(그림 4) 스마트 포크의 공격 시나리오

그림4의 시나리오는 스마트 포크를 이용해, 사용자의 식습관을 기록하여 식습관 개선에 도움을 주는 사물인터넷 서비스에 블루투스의 가로채기 공격을 통해 정보의 유출이 가능함을 보이고 있다[5].



(그림 5) 스마트 TV의 공격 시나리오

그림5의 시나리오는 스마트 TV의 블루투스를 통해 사진을 비롯한 동영상, 음성, 시청정보, 검색기록, SNS 활동로그, 앱 사용내역 등의 개인정보들이 가로채기 공격과 원격제어 공격에 취약함을 보이고 있다[5].



(그림 6) 원격의료기기의 공격 시나리오

그림6의 시나리오는 원격진료 중, 블루투스의 무선 취약점을 이용한 의료기기 해킹 시나리오이다. 이 경우, 의료기기의 인증정보를 가로채어, 기기의 조작 및 제어가 가능함을 보이고 있다[5].

3.1.2 시나리오별 위협요인

앞서 공격 시나리오들에 대한 공통적인 위협요인들을 알아보기 위해 시나리오별 공격유형들을 살펴보면 다음과 같다. 그림2의 시나리오는 그림1에서 자동차의 ECU를 컨트롤 할, 스마트 폰을 위장한 공격으로 통신 채널의 스푸핑 기법을 통해 정상적인 사용자를 가장한 위조(fabrication) 공격과 달리, 사전 악성봇을 침투시켜, 자동차의 진단정보를 훔쳐내는 가로채기 공격이다. 그리고 그림3과 4의 시나리오는 블루투스에 대한 직접적인 해킹은 아니지만, 스마트폰의 어플리케이션을 통해 저장소에 로그인 되는 ID와 패스워드를 가로채는 공격이다. 또한 그림5의 시나리오는 블루투스의 연결 관리의 취약점을 이용한 공격으로 전송되는 정보를 가로채기 위해, 기기의 인증을 위조하는 공격이다. 마지막으로 그림6의 시나리오는 무선매체의 취약성을 이용해 블루투스 연결구간에 대한 공격으로 가로채기 공격이 이뤄졌음을 알 수 있다.

이와 같은 시나리오별 위협요인들 종합해볼 때, 블루투스는 '연결 관리' 및 '연결 데이터의 취약점'들을 악용한 가로채기와 위조 공격에 매우 취약하며, 사전에 악성봇을 기기에 침투시켜, 관리 권한을 획득하는 등, 복합적인 시나리오들이 예상되고 있어, '연결 관리'가 위협요인으로 작용하고 있음을 알 수 있다.

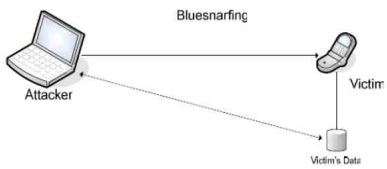
3.2 블루투스의 공격기법

블루투스는 다른 무선 전송매체와 자체 취약점을 이용한 공격들이 시도되고 있다. 그리고 몇몇 제조사들만이 대응 방안을 공개하고 있어, 앞으로 블루투스의 해킹에 따른 피해가 더욱 증가할 것으로 예상된다[9]. 이에 본 절에서는 블루투스의 공격기법들에 대한 보안 취약성과 위협요인을 알아본다.

3.2.1 공격기법별 보안 취약성

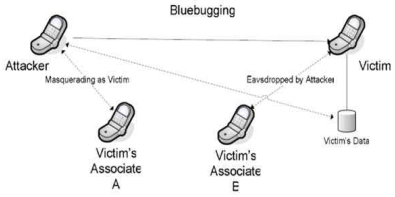
"블루스나프(BlueSnarf)"는 블루투스의 인증 취

약점을 이용해 장비의 임의 파일에 접근하는 공격이다. 그림7과 같이 공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환할 수 있는 OPP(OBEX Push Profile)의 취약점을 이용해 정보를 열람할 수 있다[9][10].



(그림 7) 블루스나프 공격 시나리오[11]

"블루버깅(BlueBugging)"은 블루투스가 지원되는 기기 간에 취약한 연결 관리를 이용한 공격이다. 그림8의 시나리오와 같이 블루투스 기기는 한 번 연결되면, 다시 연결해주지 않아도 연결되는 점을 이용해 재 연결 공격을 할 수 있다[9][10].



(그림 8) 블루버깅 공격 시나리오[11]

"블루젝킹(BlueJacking)"은 블루투스 기기들을 통해 텍스트 형태의 메시지 또는 스팸전송을 보내는 공격이다[10]. 그림9의 시나리오와 같이 블루투스 통신을 이용한 메시지 공격의 일종으로 악성봇이나 연결 관리의 취약성을 이용한 복합 공격이 가능하다.

(그림 9) 블루잭킹 공격 시나리오[11]

이밖에도 "블루프린팅(BluePrinting)"은 공격할 블루투스 장치의 검색 활동을 의미한다. 블루투스의 장치 간 종류를 식별하기 위해 서비스 발견 프로토콜(Service Discovery Protocol)을 주고받는데, 이를 악용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다[9][10]. 그리고 "마우스잭(MouseJack)"은 블루투스 통신을 사용하는 USB수신기와 무선 마우스/키보드 간의 신호를 이용해 마우스 클릭이나 키 입력정보를 탈취할 수 있으며, 100m거리에서도 위조된 신호를 보내 임의의 명령을 실행할 수 있다[9]. 또한 "블루DoS(BDoS)"는 블루투스를 기반 한 비콘이 2.45GHZ 내에 많은 채널로 나누어져 있지만 지속적인 전파 간섭 및 교란 신호 공격으로 서비스의 오동작이 가능하다.

3.2.2 블루투스 공격기법의 유형 분류

본 절에서는 공격기법에 상응하는 대응기술을 정의하기 위해 공격기법에 따른 공격유형과 위협요인의 구분이 필요하다. 따라서 앞서 3.2.2절에서 언급한 블루투스의 공격기법들에 대해 표 1과 같이 공격유형과 위협요인을 분류해 볼 수 있다.

<표 1> 공격기법의 대표적 공격 유형 분류

공격기법 명	위협요인	대표적인 공격 유형
블루스나프	- 인증 정보	- 위조(Fabrication) - 가로채기(Intercept)
블루버깅	- 인증 정보 - 연결 관리	- 위조(Fabrication)
블루젝킹	- 인증 정보 - 연결 관리	- 가로채기(Intercept) - 위조(Fabrication) - 변조(Modification)
블루프린팅	- 기기 정보	- 가로채기(Intercept) - 위조(Fabrication)
마우스잭	- 인증 정보 - 키	- 가로채기(Intercept)
블루도스	- 비콘 기능	- 방해(Interrupt)

표1의 공격기법들은 공통적으로 기기 및 사용자의 '인증정보 관리'와 '연결 관리'에 취약하며, 이러한 취약요인이 보안의 주요 위협요인으로 작용하고 있음을 알 수 있다. 그리고 블루투스 공격기법들을 정보보호의 대표적인 공격유형인 가로채기와 위조, 변조, 방해 공격과 매핑해볼 때, 정보보호 요소인 기밀성(confidentiality)과 무결성(integrity), 가

용성(availability)으로 대응이 필요함을 알 수 있다.

4. 대응방안

4.1 정보보호 요소의 대응

표1과 같이 블루투스 공격기법들은 몇 가지 대표적인 공격유형으로 분류해 볼 수 있으며, 이는 정보보호의 기본 요소인 기밀성과 무결성으로 대응이 가능하다. 블루투스의 PIN이나 링크키 등의 인증 및 연결 정보는 암호화와 해쉬 알고리즘을 통해 기밀성과 무결성을 보장받을 수 있다. 그러나 페어링 시, 암·복호화로 인해 연결 관리에 지연현상이 예상되고 있는 가운데, 다음 절에서는 PIN의 설정을 통한 대응을 알아본다.

4.2 PIN 설정 대응

앞서 연결 관리의 암호화로 인한 연결지연 문제 외에도 대부분의 블루투스 기기들은 공장에서 출시될 당시부터 PIN이 기본설정(default setting)되어 있어, 별도의 설정변경 없이 사용이 가능하도록 하고 있다. 이로 인해 기기의 인증 및 등록과정은 오히려 위협요인이 되고 있다[6][7]. 따라서 PIN의 정상적인 변경 및 개인 설정기능의 활성화를 통해 대응하도록 한다. 그러나 앞서 정보보호요소 및 PIN설정을 통한 대응방안 외에도 블루투스 기기들 간의 페어링 시, 등록 여부에 따른 공격대응이 필요하다. 따라서 다음절에서 연결 관리의 대응에 대해 알아본다.

4.3 연결 관리정책의 대응

블루투스는 연결 종단 간에 보안모듈 및 기능의 존재 여부에 따라 위협에 노출되기 쉽다. 따라서 [6]과 [7]에서 언급한 바와 같이 가로채기나 위조 공격에 대응하기 위해 불필요한 블루투스 기능의 활성화를 지양하고, 알지 못하는 기기(unknown device)의 등록 배제와 등록된 기기의 페어링 우선순위 정책의 변경, 취약점 인지를 통해 대응하도록 한다.

4.4 공격기법별 대응

블루투스의 공격기법[11]들에 대한 대응 방안을 다음과 같이 요약해 볼 수 있다. ‘블루스나프’ 공격은 블루투스 장치를 사용하지 않을 경우, 숨김으로 하고, 일시적인 연결을 요청하는 낯선 장치를 경계하고, 암호를 자주 변경하며, 민감한 데이터는 저장하지 않도록 한다. 그리고 ‘블루잭킹’ 공격은 공공장소에서 블루투스 장치의 연결을 하지 않도록 하며, 블루투스 장치는 숨김이나 찾지 못하도록 모드를 변경하고, 블루잭킹 메시지를 무시한다. 또한 ‘블루버깅’ 공격은 공공장소나 지하철 커피숍 등의 약10미터 반경에서 주로 발생함으로 스마트폰의 제조업체에 문의 또는 보안 패치를 확인한다. 마지막으로 블루투스를 사용 시에만 활성화하며, 모든 멀티미디어 메시지나 전자 명함 등은 바이러스 스캔을 통해 대응하도록 한다.

5. 결 론

최근 사물인터넷 기기들과 스마트 기기들 간의 통신이 늘고 있다. 이는 블루투스가 편의성과 신속성 등 사용자들에게 큰 장점들을 제공하고 이들의 통제 및 관리에 사용이 점차 증가하고 있기 때문으로 추정된다. 블루투스는 근거리 무선 통신망으로서 기기들에 필요한 최저 전력소모가 가능한 장점이 있기 때문에 다른 무선 전송매체보다도 선호되는 가장 큰 이유이다. 그러나 블루투스는 보안 취약점들이 알려지면서, 다양한 공격기법들에 의한 사고 사례가 증가하고 있다. 특히 커넥티드 카(connected car)나 의료기기 등에 따른 사례 등은 침해 사고의 대표적인 사례들이다.

따라서 본 논문은 사물인터넷 환경에서의 무선 전송매체인 블루투스의 보안기술과 동향, 사례를 알아보았으며, 공격 시나리오 및 기법들의 보안 위협요인에 관한 분석을 통해, 보안위협요인의 경감과 대응방안 마련, 사고예방, 보안기술의 개발 등 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 블루투스의 프라이버시(privacy)를 고려한 보안 기술의 개발과 함께, 폭넓은 응용 산업분야의 보안 위협요인 및 취약성 분석에 대한 체계적이고, 지속적인 연구를 통해 대응 방안이 마련되어야 할 것으로 사료된다.

참고문헌

[1] http://blog.skhynix.com/1860, “혁신적인 기술도 무장한 블루투스5.0”, SK Hynix 하이라이트, 2016.9.6.

[2] http://smartblog.kt.com/5892, “블루투스 5.0이 가져올 일상의 새로운 변화”, KT 스마트 블로그, 2017.01.11.

[3] 전정훈, “사물인터넷 기술동향과 전망에 관한 연구,” 융합보안학회, vol.14, no.7, 2014.12

[4] 강동호 외 2인, “블루투스 보안 기술,” 정보통신연구진흥원, 주간기술동향 no.1380, 2009.1

[5] 남서울대학교 산학협력단, “사물인터넷시대의 개인정보 침해요인 분석 및 실제사례 조사,” 개인정보보호위원회, 2015.12

[6] 유종덕, 이구연, “블루투스 인증 과정에서 보안상의 취약점 분석 및 개선방안에 관한 연구,” 한국통신학회, 학술회지 하계 상, pp32-35, 2001.7

[7] 백종경, 박재표, “블루투스 환경에서 데이터 전송 시 보안 취약점 분석 및 개선 방안 관련 연구,” 한국산학기술학회논문지, vol.12, no.6, 2011.6

[8] 김승일외 2인, “저전력 블루투스(BLE) 비콘 보안 취약점 연구.” 정보보호학회지, vol.26, no36, 2016.6

[9] http://macnews.tistory.com/4198, “무선 주변장치 취약점 이용한 신종 해킹 수법 발견. ′로지텍 • 마이크로소프트 • 델 무선 마우스 및 키보드 제품 20여종′,” 2016.2.25.

[10] https://phoenixts.com/blog/hacking-bluetooth-devices-bluebugging-bluesnarfing-bluejacking/ “Bluetooth Device attack“

[11] Saurabh Dhuri, “Bluetooth Attack and Security,” International Journal of Current Trends in Engineering & Research(IJCTER), vol.3, no.6, pp.76-81, 2017.6

〔저 자 소 개〕

전 정 훈 (Jeong-hoon Jeon)

2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사

2005년 5월~ 현 동덕여자대학교 컴퓨터학과 부교수

email : nerdrandy@dongduk.ac.kr