정 보 보 호 학 회 지
제27권 제1호, 2017. 2

IoE 환경에 적합한 보안 경고 디스플레이를 활용한 개인정보 보호 기법

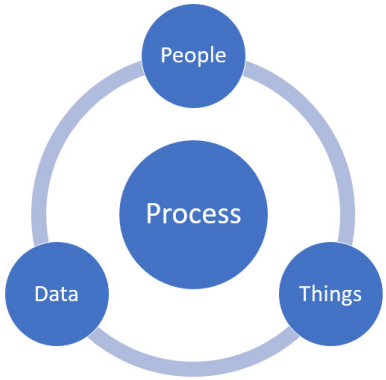
류 정 우*

요 약

최근, Internet of Everything (IoE)는 Internet of Things (IoT)의 영역을 급속히 확장하며 그 범위를 넓혀가고 있다. IoT가 여러 가지 다양한 센서들을 인터넷에 연결하는 기술이라면 IoE는 우리주변의 모든 기기들 (예를 들면 가전제품이나 보안 시스템)을 IoE와 아울러서 통합된 망을 구축함으로써 여러 가지 상승효과를 모색하는 정보산업의 새로운 흐름이라 할 수 있겠다. 하지만, IoE의 많은 장점에도 불구하고, 새롭게 개발되고 있는 기술이라는 특성상, 아직도 보완해야 될 점이 많은 것이 사실이다. 특히, IoE 환경의 경우, 가정이나 사무공간에서 연결되고 있는 기기나 장비들이 개인용품이 많다는 특성상 정보 보안에 문제가 생길 때 개인정보 유출의 우려가 클 수밖에 없는 것이 사실이다. 하지만, 많은 IoE 서비스 이용자들이 이런 보안상의 문제점들에 대해서 인지하지 못하고 있는 것이 현실이다. 따라서 본 논문에서는 보안경고 디스플레이 기술을 활용하여 일반인들에게 개인정보 유출에 대한 경각심을 일으키고 구체적인 대응방안을 모색해 볼 수 있도록 유도하는 디자인 기법들의 가능성들을 모색해 보고자 한다.

Ⅰ. 서 론

IoE (Internet of Everything) 는 특성화된 센서 중심의 장비들을 인터넷으로 연결하는 방식의 (Internet of Things: IoT) 를 확장하는 기술이다[2]. IoE 의 경우 기존의 IoT와는 달리 그 영역을 비약적으로 확장해 사용자, 프로세스, 데이터를 일반인들이 사용하는 다양한 전자 제품이나 가정용 혹은 사무용 장비들과 상호 접속시켜 상승 효과를 얻고자 하는 기술을 통칭하는 용어이다 (그림 1). IoE 기술을 활용하면 사이버 공간의 정보가 물리적 공간에 영향을 미치도록 하는 것이 가능하다. 사용자가 주택에 장치된 센서를 통해 가스 밸브 상태를 원격으로 확인하고 필요할 경우 잠그는 것이 그 좋은 예이다.



〔그림 1〕 IoE 의 정의

근래에 들어 IoE 기기들은 우리 주변에 점점더 많은 자리를 차지하고 있다. 하지만 많은 사용자들이 자기 주변에 얼마나 많은 IoE 기기들이 존재하며 이들이 정확히 어떤 보안 위협을 내재하고 있는 지를 파악하지 못하고 있는 실정이다[1]. 이에 관한 대표적인 예로 최근에 발생한 IoE 기기들을 활용한 DoS 공격을 들 수 있다.)

따라서 위협 정도의 체계적인 정량화와 효율적인 시각화를 통해 개인 사용자의 IoE 기기들이 가지는 보안 위협에 대한 의식을 높이는 것이 중요한 연구 과제로 대두되고 있다. IoT 분야의 경우 이와 관련된 연구가 아주 제한된 분야에서 소규모로 진행된 적은 있다[3,4].

이 문제에 대한 해결 방안으로 본 논문에서는 IoE에 특성화된 개인용 보안 경고 디스플레이를 제안하고자 한다. 이를 위해서는 디스플레이에서 제공하게될 정보 수집이 필수적인데, 바로 다음 절에서 논의하게 될 IoE 위협 시나리오 분석이 그에 대한 단초를 제공한다.

* Pennsylvania 주립대학교 정보과학기술학과 (jryoo@psu.edu)

본 논문의 주된 목적은 IoE 와 개인 정보 보안에 대한 연결 고리를 시각화를 통해 개인 사용자들이 쉽게 접근할 수 있도록하는 방안을 모색하는데 있다. 이를 위해서는 구체적인 해결방안을 제공하기 보다는 먼저 어떤 종류의 연구가 필요하며 전체적인 연구 흐름에 대한 방향 설정이 필요한데 이에 대한 시발점으로 본 논문의 역할에 대한 주된 의미를 두고자 한다.

Ⅱ. IoE 보안 위협 시나리오

IoE 관점에서 볼때, 일반 사용자가 직접 기기의 보안 취약점을 분석하고, 업데이트해야 한다는 점에서 전통적인 사이버 보안과는 많은 차이점을 갖는다. 따라서 일반 사용자 입장에서 효과적으로 사용할 수 있도록 보안 경고를 제공할 수 있는 방법을 고안해야 한다. 따라서 본 절에서는 여러가지 IoE 보안 위협 시나리오들을 먼저 고려해 보고자 한다. IoE 사용에 따른 보안위협은 크게 두가지로 분류해 볼 수 있다. 첫째는 모든 IoE활용에 대한 전반적인 위협들이고, 둘째는 적용 분야별로 생각해 볼 수 있는 위협들이다.

2.1. 일반적인 IoE 위협

IoE가 이용되는 분야는 다양할 수 있지만 이에 상관없이 공통적으로 생각해 볼 수 있는 위협들을 본 절에서 다뤄 보고자 한다.

2.1.1. 성공적인 침입과 IoE 기기 장악의 경우

공격에 취약한 IoE 기기가 외부 침입자에 의해서 성공적으로 장악된 경우를 생각해 보자. 이런 상황에서는 다음과 같은 여러가지 사후 위협들을 생각해 볼수 있다.

- 장악된 IoE 기기들이 Denial of Service (DoS)와같은 외부 공격에 사용될 가능성 (예를 들면 Mirai Botnet)
- 회사 기밀과 같은 민감한 정보 유출에 이용될 가능성
- 일반 사용자들의 사생활을 감시하고 개인 정보 수집 및 악용에 이용될 가능성
- IoE 하드웨어를 오작동 시킴으로써 물리적인 위해를 가하는 시나리오 (예를 들면 건물의 냉난방 기능에 장애를 주거나 온수를 차단하는 경우등을 생각해 볼 수 있다.)

특히 정보 유출과 감청의 경우 IoE 장비에 탑재되어 있는 센서들의 종류와 기능에 따라서 여러가지 다양한 공격이 이루어 질 수 있다. 따라서, IoE 기기에 연관된 위협 정도를 가늠해 볼때 이들 sensor들의 본질과 성능을 고려해 보는것이 필수적이라 할 수 있겠다.

2.1.2. IoE 기기들에 대한 신호 교란 및 방해와 DoS 공격

신호 교란과방해는 무선 전파 차단을 통해 IoE 하드웨어를 무력화 시킬 수 있다. DoS 공격은 IoE 장치에 과부하를 가함으로써 사용불능 상태로 만들 수 있다.

2.1.3. 스푸핑

스푸핑의 경우 침입자에 의해서 점령된 IoE 장비가 같은 망에 연결된 다른 기기들을 속여서 마치 시스템에 접근 권한이 있는 것처럼 한다음 정보를 빼내가는 기법을 말한다.

2.1.4. 물리적인 보안 공격

이 경우에는 공격자가 IoE장비들을 물리적인 힘을 가해 파괴하거나 훔치는 것을 가정해 볼 수 있다.

2.1.5. 취약한 기본 환경 설정값

다른 여러 인터넷 장비의 경우처럼 IoE 기기도 제작될 당시에 쉽게 추정이 가능한 비밀번호로 기본값이 설정되어 있을 수 있다. 이와같은 경우에 IoE 제품들이 헤커들의 공격에 당연히 취약할 수 밖에 없다.

2.1.6. 사이버와 물리적 보안간의 상호 의존성

사이버보안에 문제가 생겼을때 결과적으로 물리적인 보안에 영향을 주게될 가능성도 많다. 예를들면 IoE 기기의 취약점을 통해 건물 경비 시스템이 공격을 당했을때 잠금장치가 해제될수도 있다.

2.2. 적용 분야별 IoE 위협

각각의 IoE 기기가 처한 주변환경에 따라 앞에서 언급된 여러 위험요소들이 더 세분화 되고 독특한 시나리

오로 전개될 수 있다.

2.2.1. 가정이나 사무실

스마트 홈은 자동화된 가정 주택을 일컫는 말이다. 스마트홈 거주자들은 원격으로 건물을 감시하고 냉난방 장치를 제어할 수 있다. 특히, 현재는 건물보안에 사용되는 조명이나 경보와 장금장치 같은 물리적 보안 자동화가 빠른 속도로 진행되는 중이다.

스마트홈의 여러가지 편리함에도 불구하고 보안상의 문제가 생길경우 거주자들의 생활에 치명적인 악영향을 미칠 수 있다. 상수도나 전기공급이 끊기게 하는 것은 물론이고 심한 경우에는 주택 전체를 볼모로 삼는 새로운 유형의 랜섬웨어 (ransomware)가 나올 가능성도 배제할 수 없다.

2.2.2. 자동차

IoE 기술은 자율주행 자동차 기술을 보편화 하는데 아주 중요한 기반 기술중의 하나이다. 이와같은 장점에도 불구하고 보안 전문가들은 자동차에 사용되는 여러 IoE 센서들이 보안 취약점으로도 이용될 수 있다는 점에 주목하고 있다. 특히 자동차의 여러 부품들이 통신망으로 상호 연결되어 있고 심지어는 주행하는 차간에도 교통 정체나 충돌방지 문제등을 해결하기 위하여 인터넷을 통한 접속이 가속화되고 있는것이 현실이다. 따라서 자동차에 사용되는 IoE의 보안 취약점을 면밀히 살펴보고 대비책을 강구하는 것이 절실한 것이 현시점에서 중요한 문제로 대두되고 있다.

교통신호는 자동차와 연결된 또다른 IoE기술 적용분야이다. 이분야 역시 보안 공격이 성공할 경우 보행자와 운전자 안전에 치명적인 위험을 줄수 있다. 예를들어, 신호 오작동의 경우 대형 교통사고로 이어질 가능성이 아주높다는 것은 별다른 분석없이도 쉽게 추정이 가능하다.

2.2.3. 의료

의료부문의 경우 불순한 의도를 가진 집단들이 환자들의 생명에 직접 지장을 줄 수 있는 인슐린 공급장치나 심장박동 보조장치같은 의료 장비에 연결된 IoE 기기들을 공격할 가능성이 점점더 가시화되고 있다.

Ⅲ. 보안 경고 디스플레이 디자인

본 논문에서는 지금까지 거론된 IoE와 관련된 여러 보안 위협 시나리오중에, 특히 개인정보 보호와 직결되는 부분을 집중적으로 다루고자 한다.

좀더 구체적으로 이야기 하자면, 적용 분야별 IoE 위협들 중에서는 가정이나 사무실에 존재하는 위협들에 촛점을 맞추어 어떤식으로 개인 사용자들에게 주변에 존재하는 IoE와 관련된 위협들을 효과적으로 보안 경고 디스플레이 형태로 보여줄 수 있을지에 대해 심도있는 분석을 해 보고자 한다.

3.1. 성공적인 침입과 IoE 기기 장악의 경우

Common Vulnerabilities and Exposures (CVE) 는 현재 가장 널리 사용되고 있는 취약점 자료 목록이다. 따라서 특정한 IoE 기기가 얼마나 공격에 취약한지를 파악하기 위한 한 방법으로 CVE 목록을 살펴보는 것이 가능하다. 물론, CVE에 아무런 정보가 없는 경우 이방법은 별로 효율적이지 못할 수도 있다. 이럴 경우, 대중매체 (social media) 나 인터넷상의 다른 출처들을 취약점 파악에 활용하는 방법은 여전히 유효하다.

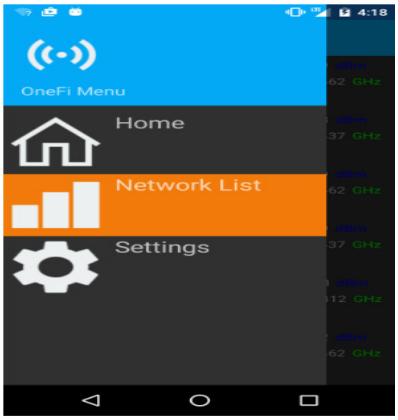
또 다른 방법은 IoE 기기들의 취약점을 원격 검증절차 (remote attestation) 를 통해 직접 확인해 보는 방법이다. 일례로, 이런 경우에 IoE 장비가 기본설정 암호값을 제공했을때 접근을 허용하는 지 확인해 보는 것이 가능하다.

IoE 장비가 구체적으로 어떤 위험에 노출되어 있는 지를 가늠하는 방법으로는 다음과 같은 접근이 가능하다.

- IoE 장비보안에 관한 위험성을 가늠해 보는데 유용할만한 접근허용 정도에 관한 정보 확인
- IoE 장비에 장착된 센서의 종류와 기능 (이 경우 센서의 오남용 가능성을 고려해 보는 것이 핵심이다.) 확인
- 보안이 허술한 네트워크 프로토콜 (network protocol) 이 IoE 기기에 의해서 사용되고 있는지 확인

3.2. IoE 기기들에 대한 신호 교란 및 방해와 DoS 공격

이런 종류의 공격을 감행하기 위해서는 공격자가 IoE 기기들 주변으로 상당히 접근하는 것이 필요하다. 따라서 본 논문에서 추구하는 보안 경고 디스플레이에는 필수적으로 그림 2에서처럼 개인 사용자 주변에 어떤 수상한 기기들이 존재하는 지를 보여주는 기능이 필수적으로 추가되어야 한다.



〔그림 2〕 주변 무선기기 표시 기능

3.3. 스푸핑

스푸핑의 경우IoE 기기들이 작동할때 이상 징후가 있는 지 살펴 보는 것이 중요하다. 이를 위해서는 작동 상태의 변화를 감지할 수 있도록 정상적인 행동과 비정상적인 행동간의 현저한 차이를 식별할 수 있는 수단을 강구하는 것이 연구의 주요과제가 된다. 일례로, 방화벽에 열려 있는 통신 포트 (open ports) 에 변화가 생긴다던가 기기가 가지고 있는 고유의 특성에 차이가 생겼는지를 알아보는 것 (fingerprinting) 등이 이상 징후 감지에 쓰일수 있다.

3.4. 취약한 기본 환경설정 값

많은 IoE 장비들이 제조시 취약한 기본 환경설정 값으로 설정되어 있다. 따라서 IoE 장비의 위험정도를 분석하는 척도의 하나로 이들 장비들이 기본 환경 값으로 설정되어 있는 지 아닌 지를 알아보는 방법을 적용해 볼 수 있다.

3.5. 사이버와 물리적 보안간의 상호 의존성

위치나 어떤 정보를 처리하는 가의 맥락에 따라서 IoE 장비가 안전에 연관된 하드웨어와 명확한 연관성이 있는 지를 확인해 볼 필요가 있다.

Ⅳ. 정량화와 시각화

지금까지는 개인 환경에서의 IoE 기기와 연관된 위협 요소들과 이들을 구체적으로 정량화하고 파악하는 방법에 대해서 논의해 보았다. 본 절에서는 어떤 형태로 이런 정보를 시각화 해볼 수 있을 지에대해서 이야기해 보고자 한다.

4.1. 시각화의 조건

본 연구가 지향하는 보안 경고 디스플레이 시스템이 개인용 이라는 점을 감안할 때, 개인용 통신 단말기를 보급 수단으로 활용하는 것이 가장 효율적일 수 있다. 따라서 시각화의 조건 중에 하나는 개인용 앱(app)을 개발에 사용하는 것이다. 이런 제약 때문에 작은 공간에서 최적화된 시각화 기법을 적용하는 것이 중요하다.

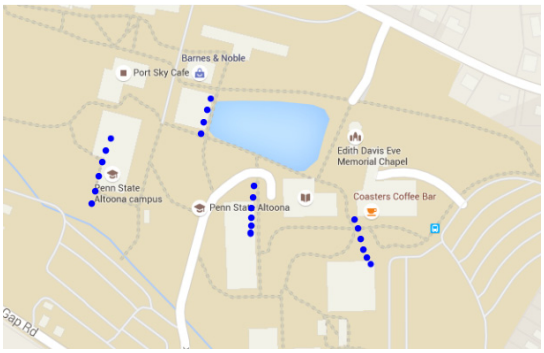
4.2. IoE 기기의 개별적인 시각화와 위험정도 분석

일반 사용자는 주변에 얼마나 많은 IoE 위협이 존재하며 이들 각자가 잠재적으로 어느 정도의 위험을 내포하고 있는 지를 알고 싶어 한다. 또한 위험 정도를 줄이기 위해서 당장 실행에 옮길 수 있는 행동 요령도 원한다.

4.2.1. IoE 기기 자체의 시각화

이런 사용자의 요구사항을 만족시키기 위해서는 그림 3에서처럼 사용자 주변에 어떤 IoE 기기가 존재하는 지를 보여주는 것이 첫번째 과제이다. IoE 기기 감지를 위해서 이들이 사용하는 무선 신호를 감지하는 방법을 사용한다. 가장 보편적으로 사용되는 신호는 와이파이 (Wi-Fi) 나 블루투스 (Bluetooth) 를 들 수 있다.

위치 파악 이후에는 감지된 IoE 기기들 각자의 본래 용도와 기능들을 보여 주는 것이 도움이 된다. 이를 통해서 사용자는 일단 본인이 그 존재를 모르고 있던 IoE



〔그림 3〕 신호 감지의 예

기기들 (rogue devices) 을 신속히 파악할 수 있다. 특히 이 경우에 신호 방해나 교란같은 공격 감지에 도움이 된다.

4.2.2. IoE 기기별 위험정도 분석

기기들의 위치 파악이후에 다음 단계로는 IoE 장비 각자가 가지는 위험 정도 분석이 될 수 있다. 일단 사용자들에게 전반적인 위험 정도를 수치화 해서 보여줄 필요가 있다. 예를 들어, 건물 보안용 감시 카메라가 본 논문에서 제안하는 개인 정보 보호 앱에 감지되는 경우, 감시 카메라의 보안 취약점을 분석하고, 만약 취약하다고 판단된다면, 보안 경고 디스플레이는 색깔 변경 등과 같은 다양한 시각화를 통하여 사용자에게 보안 경고를 줄 수 있다.

좀더 구체적인 위험 정도는 사용자가 카메라를 대표하는 아이콘을 터치할때 아래와 같이 표시된다.

- 전체적인 위험 정도 인덱스 수치: 92
- IoE 기기가 (카메라) 악성 코드에 감염되었을 가능성: 89%
- 스푸핑 가능성: 57%
- 취약한 환경 설정 기본 값: 아니오

그리고 앱은 사용자가 각자의 표시된 항목을 터치할 때 구체적으로 어떤 행동을 취해야 표시된 보안 위험성을 줄일 수 있는 지에 대해서도 정보를 제공한다.

4.2.3. Common Vulnerability Scoring System (CVSS)

위에서 논의된 기기별 위험정도를 분석하기 위해서는 이미 널리 사용되고 있는 Common Vulnerability Scoring System 을 활용해 볼 수 있다.

Ⅴ. 결 론

이 논문에서는 IoE 고유의 정보 보안 취약점과 위협 시나리오를 분석해 보고 이에대한 해결책으로 개인용 경고 디스플레이를 제안하였다. 특히 경고 디스플레이 제작시 구체적으로 어떤 요소들에 촛점을 맞추고 이를 시각화 해 볼지에 되해서 고민해 보았다. 특히 IoE 만이 가지는 위협의 종류와 정도의 경우는 시나리오를 통해서 상당히 구체적으로 설명되었다. 따라서, 이런 일련의 논의들이 본 논문의 가장 현저한 가치와 중요성을 제공한다고 할 수 있다. 후속 논문에서는 본 논문에서 제안된 다양한 아이디어들을 좀 더 심도있게 다루어 볼 예정이다. 특히, CVSS를 활용한 IoE 위협의 정량화 부분의 경우 개발 과정에 상당히 많은 노력이 필요할 것으로 예상된다.

참 고 문 헌

[1] M. Abomhara, G. Koien, “Security and Privacy in the Internet of Things: Current Status and Open Issues,” *In Proceedings of* the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), May 2014.

[2] J. Kietzmann, K. Robson, “Introduction to the Internet of Everything: Connecting People, Things, and Data Minitrack,” *In Proceedings of* the 2016 49th Hawaii International Conference on System Sciences, pp. 3918, January 2016

[3] P. Sarigiannidis, E. Karapistoli, A. Economides. “A Threat Visualization Tool for IoT Systems Security,” *In Proceedings of* the IEEE ICC 2015 - Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems, pp. 2633-2638, June 2015.

[4] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, “EyeSim: A Mobile Application for Visual-Assisted Wormhole Attack Detection in IoT-enabled WSNs,” *In Proceedings of* the 2016

9th IFIP Wireless and Mobile Networking Conference (WMNC), July 2016.

〈저자소개〉

류 정 우 (Jungwoo Ryoo)

1998년 5월 : 미국 Missouri 주립 대학교 컴퓨터공학과 졸업
2000년 5월 : 미국 Missouri 주립 대학교 컴퓨터공학과 석사
2005년 5월 : 미국 Kansas 주립 대학교 컴퓨터공학과 박사
관심분야 : 소프트웨어 보안, 소프트웨어 공학, 정보보호