사물인터넷 기기 보안평가를 위한 기술요소 기반의 모델 설계 및 체크리스트 적용

한 슬 기*, 김 명 주**

요 약

사물인터넷의 수요가 증가하면서 사용자의 중요 정보들을 수집하는 사물인터넷 기기의 보안에 대한 필요성 또한 꾸준히 증가하고 있다. 하드웨어, 프로세서, 에너지 등의 제약이 있는 사물인터넷 특성상 기존의 보안시스템을 그대로 적용하기 어렵기 때문에, 사물인터넷에 특화된 보안가이드라인 및 관련문서가 만들어지고 있다. 그러나 이들은 사물인터넷 기기 각각에 특화된 보안을 구체적으로 다루기보다는 포괄적이며 일반화된 수준의 보안을 다루고 있다. 더구나 이들은 개발자 및 서비스 제안자의 입장에서 작성되었기 때문에 특정 사물 인터넷 기기를 사용하고자 하는 일반 사용자의 입장에서 특정 사물인터넷 기기가 어느 정도 보안성을 갖추고 있는지 파악하기가 어렵다. 본 논문에서는 사물인터넷과 관련된 기존 가이드라인과 문서들을 토대로 사물인터넷 기기 각각에 대하여 보다 구체화된 보안평가용 평가모델을 설계하여 제시하였다. 아울러 이 평가모델을 토대로 대표적 사물인터넷 기기인 스마트워치를 대상으로 체크리스트를 적용하여 작성해 봄으로써 특정 사물인터넷 기기를 사용하기 전에 보안성 평가를 일반 사용자도 용이하게 할 수 있음을 보여준다.

A Design of Technology Element-based Evaluation Model and its Application on Checklist for the IoT Device Security Evaluation

Han Seul Ki*, Kim Myuhng Joo**

ABSTRACT

As the demand for Internet of Things(IoT) increases, the need for the security of IoT devices is increasing steadily. It is difficult to apply the conventional security theory to IoT devices because IoT devices are subject to be constrained by some factors such as hardware, processor, and energy. Nowadays we have several security guidelines and related documents on IoT device. Most of them, however, do not consider the characteristics of specific IoT devices. Since they describes the security issues comprehensively, it is not easy to explain the specific security level reflecting each characteristics of IoT devices. In addition, most existing guidelines and related documents are described in view of developers and service proposers, and thus ordinary users are not able to assess whether a specific IoT device can protect their information securely or not. We propose an security evaluation model, based on the existing guidelines and related documents, for more specific IoT devices and prove that this approach is more convenient to ordinary users by creating checklists for the smart watch.

Key words : IoT device security, IoT device checklist, IoT security evaluation model

접수일(2018년 6월 2일), 수정일(1차: 2018년 6월 26일), 게재확정일(2018년 6월 29일)

* 서울여자대학교 대학원 정보보호학과
** 서울여자대학교 정보보호학과

1. 서 론

2014년 이후 IT 산업을 이끌어 갈 차세대 기술로 사물인터넷(IoT, Internet of Things)이 주목을 받아왔다. 지금까지는 사람이 개입하여 네트워크상에서 정보를 공유했다면, 사물인터넷 환경에서는 사람의 직접적인 개입이 없어도 사물들끼리 서로 네트워크를 통하여 정보를 공유한다. 이러한 사물인터넷은 홈 네트워크, 헬스케어, 공공안전, 의료 및 제조 등 다양한 분야에서 사용되고 있다. 글로벌 시장조사기관인 가트너(Gartner)는 오는 2020년에는 전 세계 사물인터넷 기기의 사용량이 204억대에 이를 것으로 전망하고 있다. 사물인터넷은 주변의 사물들이 네트워크로 연결되어 정보를 수집, 가공 및 공유하여 서비스를 제공한다. 이러한 서비스들은 대부분 실제 사물들과 연결되므로 보안 문제가 발생했을 경우 직접적인 피해가 발생할 수 있으며, 이와 같이 사물인터넷 기반의 초연결 사회로의 진입은 기존 데스크탑 환경의 취약점과는 다른 새로운 형태의 보안위협을 야기하고 있다[1][2]. 따라서 향후 사물인터넷 환경이 안정적으로 정착하기 위해서는 사물인터넷의 보안에 대한 신뢰가 보장되어야 한다[12].

이에 따라 국내외 다양한 기관 및 협회에서 사물인터넷 보안 표준화에 대하여 연구를 진행하여 가이드라인을 제시하였다. 그러나 기존의 문서들은 사물인터넷 보안에 대해 다소 포괄적으로 다루고 있어 다양한 성능을 가지고 있는 사물인터넷에 개별적으로 적용시키기 힘들다. 그리고 기존의 문서들은 서비스제공자 및 개발자의 입장에서 작성된 문서가 대부분이므로, 일반 사용자들이 자신이 사용하고 있는 사물인터넷 기기의 보안수준을 확인하기 어렵다.

본 논문에서는 기존의 사물인터넷 보안 가이드라인 및 표준화 문서를 기반으로 하여 보안평가모델을 설계하고 대표적 사물인터넷 기기인 스마트워치에 적용가능한 보안평가체크리스트를 작성하고 적용하였다.

2. 관련 연구

데스크탑 및 모바일 기기가 주를 이루었던 사이버환경에서 점차 IoT 환경으로 변화하면서 주체 및 방법, 보호 대상 등에 있어서 새로운 접근이 필요하게 되었다. IoT 환경에서는 기존처럼 단순한 정보 유출 및 해킹, 금전피해가 주를 이루었던 것에서 벗어나 시스템 정지, 더 나아가서는 사용자의 생명까지도 위협할 수 있다[3]. 기존의 데스크탑 환경과 더불어 사물인터넷 환경에서도 정보보호 3대 요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 측면의 보안이 동일하게 요구된다. 그러나 사물인터넷 환경은 기존 데스크탑 및 모바일 중심이었던 사이버환경과는 변화된 형태이므로 구체적 특성에 따른 추가적인 보안 요구사항이 필요하다[4]. 사물인터넷 기기의 사용량이 증가하면서 사용자의 중요한 개인정보를 다루는 사물인터넷 기기 및 서비스에 대한 보안 문제의 중요성 또한 증가하고 있다. 이에 따라 기존의 정보보호 기술을 기반으로 하여 다양한 사물인터넷 기기환경에 적용되는 보안서비스를 제공하는 연구가 전 세계적으로 진행되고 있다[5]. 이번 장에서는 각각 다른 사물인터넷 기기에 적용할 수 있는 보안평가항목을 작성하기 위하여 사물인터넷 기기의 보안과 국내외 다양한 기관들의 보안 가이드라인에 대하여 검토 해 본다.

2.1 사물인터넷 기기 보안

사물인터넷 환경에서는 센서와 같은 초소형/초경량 사물인터넷 기기부터 시작하여 자원에 제약을 거의 받지 않는 스마트 기기에 이르기까지 다양한 종류의 기기들이 연결되어 서로 정보를 주고받기 때문에 기기의 성능 및 특성에 따라 보안 요구사항을 상이하게 정의할 필요가 있다[6]. 사물 인터넷 포럼의 연구결과에 따르면, 사물인터넷 기기는 각 기기의 성능 및 능력에 따라 등급 0부터 등급 3까지 총 4가지 등급으로 분류될 수 있다. 이러한 등급별 특징 및 대상기기를 <표 1>과 같이 정리하였다.

<표 1> 사물인터넷 기기 등급별 특징 및 대상기기

등급	특징	대상 기기
0	◆ 메모리, 프로세싱 능력 제약 ◆ Keep Alive 시그널 응답 ◆ 아주 작은 설정파일로 미리 구성 ◆ 통신에 필요한 자원 제약 ◆ 기기 상태정보 전송	초소형, 초경량, 초절전 센서
1	◆ 경량 IoT 프로토콜 사용가능 ◆ 기존 통신 프로토콜 스택을 적용한 기기와 쉬운 통신 불가 ◆ 프로세싱 능력,자원 제한 ◆ IP사용을 위한 코드 스페이스, 메모리, 전력 소비 등 제한필요	의료헬스 기기 스마트홈 기기 웨어러블 밴드
2	◆ 기존 통신 프로토콜 스택 지원가능	스마트폰
3	◆ 등급 2이상의 능력 ◆ 프로세싱 능력과 자원에 제약 없음 ◆ 기존 프로토콜 변형 없이 사용가능 ◆ 전원공급에 대한 제약은 여전히 존재	PC 노트북

이들 사물인터넷 기기는 각각 다른 성능을 지니고 있으므로 그에 따른 보안요구사항 또한 다르다. 사물인터넷 포럼의 연구결과에 따른 사물인터넷 기기 등급 분류에 따른 보안요구사항을 정리하면 <표 2>와 같다.

<표 2> 사물인터넷 기기 등급별 보안요구사항

보안요구사항 \ 등급		등급 0	등급 1	등급 2	등급 3
기밀성	전송 메시지 암호화		○	○	○
	악성코드 대응				○
	데이터 암호화		○	○	○
	부당 변경 방지			○	○
	식별정보 관리	○	○	○	○
무결성	데이터 무결성		○	○	○
	플랫폼 무결성			○	○
	시큐어 부팅			○	○
가용성	로그기능				○
	상태정보 전송	○	○	○	○
	외부공격 대응				○
	보안 감사 및 관리				○
	보안 패치		○	○	○
	보안정책 설정				○
	소프트웨어 안정성		○	○	○
인증 및 인가	사용자 인증		○	○	○
	기기 인증		○	○	○
	비밀번호 관리		○	○	○
	상호 인증		○	○	○
	권한 제어		○	○	○
	접근 제어		○	○	○
	식별 정보 검증			○	○

성능 및 능력에 따라 분류된 기기 등급에 따라 각 기준에 맞는 보안요구사항이 제시되어 있으며, 등급이 높을수록 프로세싱 능력 및 자원에 따라 고려되어야 하는 보안요구사항 또한 많아지는 것을 확인할 수 있다.

2.2 사물인터넷 보안가이드라인 분석

국내·외 여러 기관들이 각각 다른 관점에서 사물인터넷 보안에 대한 표준 가이드라인을 개발해 왔는데 이들에 대한 현황을 비교해보면 <표 3>과 같다. 그러나 이와 같은 보안가이드라인들이 들여다보면 사물인터넷 기기를 구성하는 3가지 구성요소인 디바이스, 네트워크, 서비스에 대해서 일반적이고 포괄적인 보안요구사항을 많이 포함하고 있어서 전반적으로 모든 보안가이드라인의 내용이 유사하다는 느낌을 주고 있다[6].

<표 3> 국내·외 사물인터넷 보안가이드라인 비교

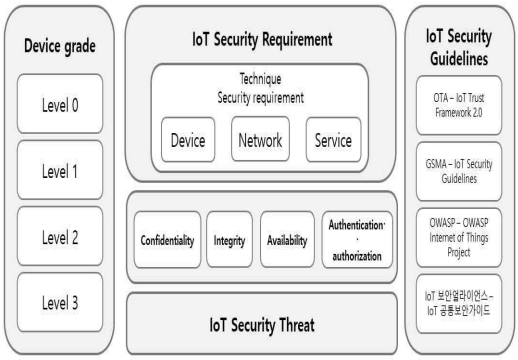
구분 \ 개발기관			OTA	OWASP	GSMA	IoT보안 얼라이언스
개발기준			IoT 생명주기 4가지 핵심 영역	IoT Top10 취약점	IoT 서비스 구성요소	IoT 공통보안 7대원칙
구성 내용	정책		○	-	○	○
	위험분석		-	-	○	○
	설계 · 개발		○	○	○	○
	운영 · 보수	설치	○	○	○	○
		HW	○	○	○	○
		SW	○	○	○	○
		통신 기능	○	○	○	○
	폐기		○	-	○	○
	네트워크		○	○	○	○

3. 보안평가 모델 설계

사물인터넷 기기의 기밀성, 무결성, 인증, 가용성 등 보안 기능을 구현하기 위해서는 제일 먼저 해당 기기의 활용분야 또는 요구사항, 정보의 조작 과 탈취를 통한 기밀성/무결성 공격과 프라이버시 침해, 서버와 단말에 대한 불법 접근을 통한 가용성 침해 등의 보안위협등을 분석하여 서비스에 요구되는 보안수준을 결정해야 한다[7][11]. 기존 사물인터넷 보안가이드라인 및 문서의 경우 그 내용이 상당히 포괄적이기 때문에 각기 다른 사양을 지닌 사물인터넷 기기에 맞추어 구체적으로 다루기 힘들다는 한계를 갖는다. 더욱

이 대부분의 이들 문서가 사용자의 관점이 아닌 서비스제공자 혹은 개발자의 입장에서 작성되었기에 사물인터넷 디바이스를 직접 이용하는 일반 사용자의 시각에서 본인이 사용하고 있는 사물인터넷 장비의 보안수준에 대하여 확인하기가 어렵다.

본 장에서는 이러한 불편함을 개선하기 위해 사물인터넷 포럼에서 정의한 등급별 기기정보 및 정보보안 3요소 및 인증/인가에 대한 보안 요구사항을 고려하여 (그림 1)과 같은 등급에 따른 사물인터넷 기기에 대한 보안평가모델을 제안한다. 본 논문에서 제안하고 있는 보안평가항목은 등급1에 해당하는 기기로 제한한다. 따라서 본 논문에서는 등급1에 해당하는 사물인터넷 기기에 대한 기존 보안가이드라인과 사물인터넷 기기 등급별로 필요한 보안 요구사항 및 보안위협을 함께 고려하여 보안평가항목을 설계한다.



(그림 1) IoT device security evaluation model

3.1 사물인터넷 기기 보안요구사항 및 보안위협

사물인터넷의 기술적 요소에 따른 보안평가모델을 제안하기에 앞서 사물인터넷 기기 등급별 보안요구사항 및 사물인터넷 기기의 기술적 3요소에 대한 보안요구사항을 먼저 정리하였다. ITU-T가 정의한 사물인터넷의 참조모델에 따르면, IoT 계층은 디바이스, 네트워크, 서비스 및 어플리케이션 지원계층, 어플리케이션 계층으로 구분하여 분류되고, 각 계층별로 관리기능 및 보안기능으로 구성된다. 이러한 사물인터넷 기기의 기술적인 요소로는 디바이스, 네트워크, 서비스로 구성된다[8]. 또한 ITU와 사물인터넷 보안 기술연구(장봉임 외,2014), 미래창조과학부에서 발표한 사물인터넷 정보보호로드맵(2014)에서 정의한 각 요소별 특징에 따른 보안요구사항 및 보안위협을 정리한 내용은 <표 4>와 같다.

이 외에도 다양한 기술이 융합되어 서비스를 제공하는 사물인터넷의 특성상 보안기술을 알아보기 위해서는 각 요소 기술에 대한 보안기술 및 통합·연동시의 보안취약성을 고려한 보안기술도 고려해야 한다[13].

<표 4> 기술 요소별 보안요구사항과 위협

요소	보안요구사항	보안위협
Device	· 권한설정 · 인증 · 액세스 제어 · 데이터 기밀성 · 무결성 보호 · 기기별 맞춤 디바이스 보안기술 · 디바이스 정지/오작동 방지기술 · 경량 및 저전력 암호기술	· 기기의 기밀성, 무결성 침해 · 분실 및 도난 · 기기의 물리적인 · 손상, 복제 공격 · 비 인가된 접근
Network	· 권한설정, 데이터 신호 · 정보의 기밀성 및 무결성 보호 · 보안통신 및 접속제어 · 단말 상호간 인증, · 네트워크 모니터링관리	· 데이터 위 · 변조 · 인증 방해 · 신호 데이터의 기밀성 및 무결성 침해 · 서비스 거부 · 정보유출
Service	· 권한설정 · 데이터의 기밀성 · 무결성 · 프라이버시 보장 · 안티 바이러스 설치 · 보안 감사 수행 · 기기 간 인증 및 키 관리 · 접근제어, 보안플랫폼	· 데이터 위 · 변조 · 비 인가된 서비스 및 사용자 접근 정보유출 · 데이터의 기밀성, 무결성, 프라이버시 침해

등급1 기기에 해당하는 보안요구사항 및 위협은 앞서 언급한 문서를 토대로 정보보호 3요소인 기밀성, 무결성, 가용성 및 인증·인가로 구분하여 등급1 기기에 대한 요구사항 및 보안위협을 고려하여 도출하였는데 이를 정리하면 <표 5>와 같다.

<표 5> 사물인터넷 등급1 기기 보안요구사항과 위협

분류	보안요구사항	보안 위협
기밀성	메시지전송 (message transfer)	– 통신 프로토콜 인증 · 전송 · 기기 간의 통신 및 인증차단 – 게이트웨이 공격자 동작제어 · 재전송 공격, 메시지 위 · 변조로 특정 동작 수행메시지 주입 – 정보유출 및 권한 탈취 · 불법 침입 및 접근
	데이터 암호화	–개인정보 유출 · 중간자 공격, 도청, 메시지 위 · 변조, 불법적인 스니핑

	식별정보 확인	– 기기 · 데이터 복제 · 고유 식별정보 외부 유출 및 변경을 통한 기기복제
무결성	데이터 무결성	– 개인정보 유출 · 도청, 중간자 공격, DDos공격, 메시지 위 · 변조
가용성	상태정보전송	– 데이터 및 기기탈취 · 물리적 파괴/제거 및 비정상적인 설치 시도
	보안패치	– 개인정보 유출 및 데이터 탈취 · 도난 및 분실, 설치 및 폐기
	소프트웨어 안정성	– 시스템 오작동
인증 및 인가	기기인증	– 권한 탈취 및 불법 접근 및 정보 유출 · 비 인가된 불법 사용자 접근 – 기기 및 데이터 탈취 · 기기 변경, 도용, 복제
	사용자인증	
	비밀번호 관리	
	상호 인증	
	권한 제어	
	접근 제어	

3.2 사물인터넷 기술적 요소에 따른 기기 보안 평가모델

IoT를 실현하기 위해서는 다양한 기술요소가 필요하다[9]. 본 절에서는 사물인터넷 보안평가 항목을 크게 사물인터넷의 기술적 3요소인 디바이스, 네트워크, 서비스로 구분 하여 각각의 보안 요소와 그에 대한 세부적인 요구사항들을 목적에 따라 정리하였다. 각 보안요구사항 및 세부사항은 본 논문에서 정의하고 있는 등급1에 해당되는 사물인터넷 기기의 보안 요구사항 및 기존의 국내·외 보안 가이드라인에서 참고 했으며, 각 요소별 보안 요구사항에 대한 평가 항목 내용은 <표 6>, <표 7>, <표 8>과 같다.

<표 6> 디바이스 보안 요구사항

Task No.	D	요소 (Component)	Device
목적(Purpose)	디바이스 자체의 보안 품질 향상		
보안요구사항		보안세부사항	
D–01	디바이스에 대한 설명을 자세히 표기 및 제공해야 한다.	· 사용상의 주의사항을 설명서에 표기해야 한다. · 데이터 보존 정책 및 보유기간을 명시해야 한다. · 개인정보보호 정책 등 각종 보안에 관한 내용을 명시해야 한다. – website, QR코드, URL, 제품포장	
D–02	소프트웨어 및 펌웨어 · 패치가 신뢰할 수 있는 것임이 입증 되어야 한다.	–	
D–03	주기적인 업데이트가 존재해야한다.	패치 및 업데이트는 사용자의 동의 없이 이루어지면 안 된다.	
D–04	보안 패치에 대한 기간을 공개해야 한다.	기기의 예상수명과 일치해야 한다.	
D–05	기기의 기본 값을 재설정할 수 있어야 한다.	사용자의 프라이버시 보호를 위해 사용자가 공장출하 상태로 기기를 재설정 할 수 있어야 한다.	
D–06	기기 분실 시 기기의 데이터를 삭제 및 제로화 할 수 있어야 한다.	–	

<표 7> 네크워크 보안 요구사항

Task No.	N	요소 (Component)	Network
목적(Purpose)	이기종 사물인터넷 디바이스간 안전한 연동 및 통신		
보안요구사항		보안세부사항	
N–01	통신할 때 주고받는 데이터를 보호하기 위하여 암호화 프로토콜을 사용해야 한다.	· 기기의 사양에 적합한 IoT 프로토콜을 사용해야 한다. – 기존 통신프로토콜 : Wi–fi, Ethernet, Bluetooth,BLE(Blueto oth Low Energy), 3G/4G, Zigbee, IPv6 등 – IoT 장치를 위한 신규 프로토콜 : MQTT, CoAP,LwM2M(Light w eight M2M) 등 – HTTP를 사용할 경우 프로토콜의 표준보안 버전인 HTTPS(HTTP Secure)를 사용해야 한다.	
N–02	IoT를 지원하는 Website는 사용자 세션을 암호화 해야 한다.	· 장치에서 백 엔드 서비스 까지 사용자 세션을 암호화해야 한다.	
N–03	장치의 보안상태 모니터링 및 관리 기술이 필요하다.	–	
N–04	사용하지 않는 포트 및 서비스는 비활성화 되어 있어야 한다.	· 사용하지 않는 포트 및 서비스를 비활성화 시킬 수 있는 기능이 제공되어야 한다. – 악의적인 제 3자가 사용하지 않는 포트를 통해 침입하는 것을 차단	

<표 8> 서비스 보안 요구사항

Task No.	S	요소 (Component)	Service
목적(Purpose)	사용자의 프라이버시 보호 및 사후관리		
보안요구사항		보안세부사항	
S-01	데이터가 유출되었을 경우 공격자에게 무의미 하도록 변형되어 저장되어야 한다.	· 저장 시 데이터에 대한 암호화 기능필요	
S-02	일반적으로 인증되는 암호 복구기능을 사용해야 한다.	· 암호 시스템 · 다중인증	
S-03	강력한 암호를 설정해야 한다.	· 적용 가능한 경량 암호기술 중 강력한 암호를 설정 – KISA '암호 알고리즘 및 키 길이 이용안내서 (2013)' 참고	
S-04	계정을 잠그는 기능이 있어야 한다.	· 일정횟수초과 로그인 시도 시 계정 잠금	
S-05	새 암호를 요구하는 옵션이 있어야 한다.	· 90일 이후 새 암호 요구	
S-06	기기 간의 처음 페어링 시 사용자 승인요청 및 통보를 해야 한다.	· 페어링이 끊어진 경우 제품 기능에 미치는 영향을 공지	
S-07	사용자 액세스 시 인증해야 한다.	· 고유 비밀번호 · 일회성 비밀번호 · 인증시 SALT 값을 이용한 Hash 암호 사용	
S-08	암호 재설정 및 변경 시 사용자에게 인증 및 통보해야 한다.	–	
S-09	디바이스 초기화 작업 시 인증해야 한다.	–	
S-10	2단계 인증옵션을 사용해야 한다.	2-Factor Authentication	

4. 스마트워치 보안평가 체크리스트 작성 및 적용

사물인터넷 기기 시장이 점차 증가하면서, 대표적인 기기로 스마트워치가 부각되고 있다. 글로벌 시장예측 기관인 IDC는 전 세계 웨어러블 기기 출하량은 2018년 1억2천490만대에서 2022년 1억9천980만대로 4년새 8.2% 증가할 것으로 예상하고 있으며, 그중 스마트워치 출하량이 2018년 4천350만개에서 2022년 8천910만개로 증가할 것으로 전망했다.

이처럼 스마트워치의 수요는 매년 증가하고 있으며, 웨어러블 기기 시장을 선두하고 있다. 다루고 있는 사물인터넷 등급 1 기기중 대표적 기기인 스마트워치의 보안요구사항 및 보안위협에 대하여 살펴보고 앞에서 연구하였던 사물인터넷 보안평가 항목을 적용하여 스마트워치의 보안에 대해 파악할 수 있는 체크리스트를 작성하였다. 또한 본 장에서 다루고 있는 체크리스트의 내용 및 표는 저자의 학위논문[14]을 기반으로 재구성하였다.

4.1 스마트워치 보안요구사항 및 위협

스마트워치는 본 논문에서 언급하고 있는 사물인터넷 기기의 보안 요구사항 및 위협을 가지고 있는 대표적인 기기이다. 스마트워치는 보안요구사항으로 내부 공격자로부터 공격에 대비하여 노드에 대한 탄력성, 급격한 성능저하 방지 기능 등을 제공해야 한다. 사물인터넷의 기술적인 3요소인 디바이스, 네트워크, 서비스로 스마트워치의 보안요구사항을 구분하면 다음의 <표 9>와 같다[10].

<표 9> 스마트워치 보안요구사항

구분	보안요구사항
디바이스	무결성, 기밀성, 디바이스간 인증기술
네트워크	안전하게 통신할 수 있는 인증기술
서비스	펌웨어 관리, 비 인가된 사용자의 접근제어, 바이러스 및 악성코드 공격 대처 방안

스마트워치는 스마트폰과 동일한 운영체제를 탑재하고 있다. 따라서 스마트워치 또한 같은 운영체제를 탑재하고 있는 스마트폰의 보안위협을 가지고 있을 가능성이 높다. 따라서 스마트워치는 중간자 공격, 비인가 된 사용자 및 서비스 접근, 개인정보 및 프라이버시 위협, 기밀성 및 무결성 등의 보안 위협을 가지고 있으며 그에 따른 세부적인 사항은 다음 <표 10>에서 확인할 수 있다.

<표 10> 스마트워치 보안위협

보안위협	보안위협 세부사항
중간자공격	스마트폰과 통신수행 시 네트워크 벡터 영역에서 중간자 공격에 노출
비인가 된 사용자 및 서비스 접근	도난 및 분실 시 비 인가된 사용자의 접근 및 서버의 데이터 유출
개인정보 및 프라이버시 위협	사용자의 중요 정보 유출
기밀성 및 무결성 위협	IoT환경에서 발생하는 공격기법 적용가능

4.2 스마트워치 보안평가 체크리스트

기존의 보안가이드라인 및 문서는 주로 사물인터넷

서비스 제공자, 제조자 관점에서 작성되었다. 물론 사용자가 사물인터넷 기기를 구매하기 전 보안에 대해 고려해야 할 점을 제시해 주는 가이드라인도 존재하나 이는 대부분 사용자들이 이해하기 어렵고 접근하기 힘들다는 문제가 있다. 따라서 본 논문에서는 앞서 설명하였던 등급 1에 해당하는 스마트워치에 특화된 체크리스트를 제안한다. 체크리스트는 앞에서 연구한 내용 및 사물인터넷 기기의 보안요소를 고려하여 작성하였다[14]. 사물인터넷 기기를 제조 및 서비스 할 경우 앞에서 제시한 보안 요구사항을 만족해야 한다. 사물인터넷 서비스 제공자 및 제조자는 이러한 보안 요구사항을 수행 하였는지의 여부를 보안 체크리스트를 통하여 체크할 수 있으며, 기기를 사용하는 사용자의 경우 자신이 구매하고자 하는 기기가 보안 요구사항을 얼마나 충족시키는 지 확인할 수 있다. 체크리스트 적용 사례로 S사의 S watch를 활용하였다. 본 체크리스트는 질문항목마다 가부 또는 유무의 표시를 하는 평점법을 적용하였으며, 평가 란은 사실 유무(Yes, No), 해당 없음(N/A) 항목으로 나누었고 세부점검항목에서는 적용하고 있는 항목을 체크할 수 있도록 되어있다[14]. 항목체크 판단기준은 S watch의 설명서이며, 이를 참고하여 체크리스트 항목에 체크하였다. 확인 가능한 항목의 경우 Yes or No, 사용 및 설명서로 확인 불가한 항목에 대해선 N/A에 표시하였다. 체크리스트에 적용한 S watch의 성능은 다음 <표 11>과 같다.

<표 11> S watch 성능표

Device Name		S watch
Spec	Network Infra	Bluetooth Only
	Connect	Wi-Fi - 802.11 b/g/n 24.GHz Bluetooth Version -v4.2 NFC
	OS	Tizen
	Processor	CPU : Dual-Core /1GHz
	Memory	RAM Size (GB) : 0.75 ROM Size (GB) : 4GB Available Memory : 1.5 GB
	Battery	380 mAh

4.2.1 디바이스 보안요소 체크리스트

스마트워치의 디바이스 요소에서 보안요구사항을 수행했는지 체크할 수 있도록 하는 체크리스트가 <표 12>에 지시되었다. 본 디바이스 보안요소 체크리스트는 암호, 디바이스정보, 소프트웨어 업데이트, 데이터 관리 총 4개의 요인항목으로 구성되어 있으며, 10개의 세부점검항목으로 이루어져 있다. 각 세부 점검항목에서는 스마트워치의 디바이스 보안요소의 항목에 따른 세부적인 내용을 체크하도록 다루고 있다.

<표 12> 스마트워치 디바이스 보안요소 체크리스트

디바이스				
항목	세부점검항목	평가		
		Yes	No	N/A
암호	1. 디바이스에 비밀번호를 설정하는 기능을 제공하고 있는가?	√		
	※ 사용자의 프라이버시 보호를 위하여 다양한 상황에서 비밀번호를 설정하는 기능을 제공해야 한다.			
	2. 디바이스의 비밀번호를 분실했을 경우를 대비해서 일반적으로 사용되는 비밀번호 복구 기능을 제공하고 있는가?		√	
	① 계정에 연결된 메일을 통한 복구			
	② SMS 수신을 통한 복구			
	③ 본인확인 질문에 대한 답변을 통한 복구			
	④ 기타			
	※ 일반적으로 사용되는 암호 복구기능을 사용해야 한다. ※ 비밀번호 설정이 가능한 디바이스경우 비밀번호 복구를 위한 기능이 존재해야 한다.			
디바이스 정보	3. 디바이스에 대한 설명이 제공되고 있는가?	√		
	① 사용상의 주의사항	√		
	② 데이터 보존 정책 및 보유기간			√
	③ 보안관련 사항	√		
	④ 개인정보정책	√		
	※ 사용자의 프라이버시 보호 및 디바이스 사용 시 필요한 부분에 대한 설명이 명시되어 있어야 한다.			
	4. 디바이스에 대한 설명을 볼 수 있는 방법이 다양한 방법으로 존재하는가?	√		
	① Website	√		
	② 제품포장	√		
	③ QR코드			√
	④ 기타 (애플리케이션, 설명서)	√		
	※ 디바이스에 대한 설명이 사용자들이 잘 볼 수 있는 장소에 기재되어 있어야 한다.			
소프트웨어 업데이트	5. 소프트웨어와 관련된 업데이트가 있는가?	√		
	6. 소프트웨어의 업데이트에 대한 기간이 디바이스의 예상수명과 일치하고 있는가?			√
	※ 소프트웨어의 업데이트에 대한 기간이 디바이스의 예상수명과 일치해야 한다.			
데이터 관리	7. 디바이스 사양에 맞추어 데이터가 적절하게 암호화되어 저장되는가?			√
	※ 데이터가 외부로 유출되었을 경우 데이터가 공격자에게 무의미하도록 데이터는 암호화 되어 저장되어야 한다. ※ 적용 가능한 경량 암호기술 중에 강력한 암호를 적용해야 한다.			

	8. 디바이스의 기본 값을 재설정 할 수 있는 옵션이 있는가?	√		
	9. 디바이스 재사용 잠금 기능이 제공되고 있는가?	√		
	10. 디바이스 분실 시 디바이스의 데이터를 원격으로 삭제 할 수 있는 기능이 있는가?	√		
	※ 디바이스를 분실했을 경우 제 3자가 기기를 초기화 했을 때 임의로 사용하지 못하도록 재사용 잠금 기능이 제공되어야 한다.			

4.2.2 네트워크 보안요소 체크리스트

스마트워치의 네트워크요소에서 보안요구사항을 수행했는지 체크할 수 있도록 하는 체크리스트를 <표 13>에서 보여준다. 본 네트워크 보안요소 체크리스트는 프로토콜, 데이터관리 총 2개의 요인항목 과 4개의 세부점검항목으로 구성되어 있으며, 각 세부 점검항목에서 스마트워치의 네트워크 보안요소 항목에 따른 세부적인 내용을 체크하도록 다루고 있다.

<표 13> 스마트워치 네트워크 보안요소 체크리스트

네트워크				
항목	세부점검항목	평가		
		Yes	No	N/a
프로토콜	1. 통신할 때 주고받는 내용을 보호하기 위해 어떠한 방법으로 데이터전송을 하고 있는 가 ?	√		
	① Bluetooth	√		
	② Wi-Fi	√		
	③ 3G/4G			√
	④ 기타 (NFC)	√		
	※ 데이터를 안전하게 전송할 수 있도록 디바이스 사양에 적합한 전송방법을 사용해야 한다. 또한 각 전송방법에서 준수하고 있는 데이터 보호를 위한 정책을 따라야 한다.			
데이터 관리	2. 사용자의 데이터를 보호하기 위해 데이터를 주고받을 때 암호화가 되어 있는가?			√
	3. 디바이스의 보안상태에 대한 모니터링 및 관리를 하고 있는가?			√
	4. 개인정보 보호를 위해 디바이스에서 서버까지의 전 통신 구간을 별도로 암호화 하여 전송 하고 있는가?			√

4.2.3 서비스 보안요소 체크리스트

스마트워치의 서비스요소에서 보안요구사항을 수행했는지 체크할 수 있도록 하는 체크리스트를 <표 14>에서 보여준다. 본 서비스 보안요소 체크리스트는 암호관리, 계정관리, 페어링, 인증 총 4개의 요인항목 및 8개의 세부점검항목으로 구성되어있으며, 각 세부 점검항목에서 스마트워치의 서비스 보안요소 항목에 따른 세부적인 내용을 체크하도록 다루고 있다.

<표 14> 스마트워치 서비스 보안요소 체크리스트

서비스				
항목	세부점검항목	평가		
		Yes	No	N/a
암호관리	1. 일정기간 이후 새 비밀번호를 요구하는 옵션이 있는가?			√
	※ 일반적으로 새 암호를 권장하는 기간은 암호생성 및 변경일 기준 90일 이후이다.			
계정관리	2. 계정을 잠그는 기능이 있는가?	√		
	① 디바이스 분실 시 원격으로 계정잠금	√		
	② 일정횟수 로그인 초과 시 계정잠금		√	
	※ 일정횟수초과 로그인 시도에는 계정을 잠그는 기능이 존재해야 한다.			
	3. 프라이버시 보호를 위해 화면 잠금 기능이 제공되고 있는가?	√		
페어링	4. 디바이스 간 처음 연결 할 경우 사용자 승인요청 및 통보하는가?	√		
	① 인증번호 입력을 통한 사용자 승인요청		√	
	② 일련번호 확인을 통한 사용자 승인요청	√		
	③ 디바이스 연결 후 SMS 통보		√	
	④ 디바이스 연결 후 E-mail 통보		√	
인증	5. 사용자가 디바이스를 사용하기 위해 연결 할 경우 인증하고 있는가?	√		
	① 아이디 / 패스워드 인증		√	
	② 핀번호 인증		√	
	③ OTP 인증		√	
	④ 일회용 패스워드		√	
	⑤ 생체인식		√	
	⑥ 기타 (일련번호 확인)	√		
	※ 일반적인 인증방법으로는 사용자의 고유한 비밀번호 입력 혹은 일회성 비밀번호 입력 등이 존재한다.			
	6. 디바이스 암호 재설정 및 변경 시 사용자에게 인증 및 통보하는가?		√	
	① SMS를 통한 사용자 인증요청			
	② E-mail 확인을 통한 사용자 인증요청			
	③ 디바이스 페어링 후 SMS 통보			
	④ 디바이스 페어링 후 E-mail 통보			
	⑤ 인증안함			
	⑥ 통보안함			
	7. 디바이스 초기화 기능이 존재 하는가?	√		
	8. 다중인증 기능이 제공 되는가?	√		
	※ 인증기능으로 단일방식 인증 및 다중인증이 존재한다. 다중인증은 여러 인증요소를 함께 사용하는 인증 방식으로, 사용자 본인 확인 시에 보다 높은 수준의 보안을 위해 사용된다.			

5. 결 론

본 논문에서는 사물인터넷 기기를 등급별, 기술요소에 따른 보안 요구사항 및 보안 위협을 도출하고 기존 보안가이드라인을 분석 하였다. 그리고 등급 1에 해당하는 사물인터넷 기기에 대한 보안인증항목 도출 방법을 제시하고 그에 적용 가능한 보안 인증 항목을 성능과 기술적 요소에 따라 각각 분류 하고 정리하였다. 이렇게 분류된 보안인증 점검 항목을 기반으로 스마트워치에 적용 가능한 보안체크리스트를 작성하였다. 본 논문에서 작성한 스마트워치 보안요소 체크리스트를 활용할 경우 소비자는 특정 사물인터넷 디바이스를 구매하기 전 보안요소를 일목요연하게 파악할 수 있게 된다. 본 논문은 지금까지 전체적인 사물인터넷 보안을 다룬 연구와는 다르게 특정등급의 사물인터넷 기기에 대한 보안을 정의하고 다룰 수 있게 해준다. 또한 사물인터넷 기기를 직접 사용하는 소비자가 기기를 구매하기 전 보안에 대한 부분을 파악할 수 있도록 이를 체크리스트로 작성할 수 있도록 제공함으로써 특정 사물인터넷 기기에 대한 구체적인 보안을 고려하여 구매 여부를 신중하게 결정하도록 해준다는 측면에서 유용하다. 앞으로 본 연구결과를 토대로 각 분야의 사물인터넷 기기들 각각에 적용 가능한 보안 인증항목 및 변형된 체크리스트를 마련할 계획이다.

참고문헌

[1] 허신욱, 김호원, “사물인터넷 보안 요구사항과 oneM2M 표준 보안 기술 분석” 정보과학회지, 제35권, 제1호, pp. 16-22, 2017.

[2] 강병완,“사물인터넷(IoT)디바이스의 보안평가지표체계에 관한 연구”, 박사학위논문,2016.

[3] 미래창조과학부, “사물인터넷(IoT) 정보보호 로드맵”, 2014.

[4] 문형진, 최광훈, 황윤철, “사물인터넷 통신기술에 내재된 보안위협과 대응 전략” 중소기업융합학회 논문지, 제6권, 제2호 pp.37-44, 2016.

[5] 김정녀, 진승헌, “초연결 환경에서 보안위협 대응을 위한 사물인터넷(IoT) 보안 기술 연구” 한국통신학회지(정보와통신), 제34권, 제3호, pp. 57-64, 2017.

[6] 사물인터넷포럼, “사물인터넷 기기 등급 분류 및 보안 요구사항”, 2015.

[7] IoT 보안얼라이언스, “IoT 공통보안가이드”, 2016.

[8] Recommendation ITU-T Y.2060, Overview of the Internet of Things, ITU-T, 2012.

[9] 박건태, 그림으로 공부하는 사물인터넷 구조, 제이펍, 2016.

[10] H. S. Park, ‘Privacy issues and implications surrounding the wearable computer‘, KOITA, 2013.

[11] 장봉임, 김창수, “사물인터넷 보안 기술 연구", 보안공학연구논문지, 제11권5호, pp 429-438, 2014.

[12] 이동혁, 박남제. “IoT 제품 보안 인증 및 보안성 유지 관리방안” 한국통신학회지(정보와통신), 제33권, 제12호, pp 28-34, 2016.

[13] http://terms.naver.com/entry.nhn?docId=2851205&cid=56756&categoryId=56756

[14] 한슬기, “사물인터넷(IoT) 기기의 보안 평가 모델 설계 및 스마트워치에의 적용실험”, 석사학위논문, 2017.

〔저자소개〕

한 슬 기 (Seul-Ki Han)
2015년 2월 서울여자대학교 중어중문학 학사
2017년 8월 서울여자대학교 정보미디어학과 석사
email : cocoq@swu.ac.kr

김 명 주 (Myuhng-Joo Kim)
1986년 2월 서울대학교 컴퓨터공학과 공학사
1988년 2월 서울대학교 대학원 컴퓨터공학과 공학석사
1993년 8월 서울대학교 대학원 컴퓨터공학과 공학박사
1993년 9월 ~ 1995년 8월 서울대학교 컴퓨터신기술공동연구소 특별연구원
1995년 9월 ~ 현재 서울여자대학교 정보보호학과 교수
email : mjkim@swu.ac.kr