스마트홈의 인증 기술 분석 및 서비스 모델제안

강원민, 문서연, 이재동, 박종혁*
서울과학기술대학교 컴퓨터공학과
e-mail:{wkaqhdsk0, moon.sy0621, jdlee731, jhpark1}@seoultech.ac.kr

Authentication Technology Analysis and Service Model Proposal in Smart Home

Won Min Kang, Seo Yeon Moon, Jae Dong Lee, Jong Hyuk Park*
Dept. of Computer Science and Engineering,
Seoul National University of Science and Technology

요 약

최근 스마트폰 및 스마트 디바이스 및 가전제품의 폭발적인 보급으로 현대인의 삶이 편리하게 바뀌고 있다. 스마트폰을 기점으로 다양한 형태의 테블릿, 스마트 TV, 스마트 냉장고, 에어컨 등 새로운 기기의 출연으로 가정에서의 삶이 변화되고 있으며 이러한 디바이스를 이용해 새로운 스마트 홈 서비스를 제공하고 하고 있다. 하지만, 이러한 서비스는 스마트 홈 보안이 적용되지 않기 때문에 개인정보의 유출이나 가전제품 해킹으로 인한 금전적 손실 등의 피해를 입을 수 있다. 따라서 주변 환경이 스마트 홈에 적용될 경우 스마트 디바이스와 같이 보안에 대한 고려가 필요하다. 스마트 홈에서 발생할 수 있는 보안 요구사항에 대해 살펴보고 보안 요구사항 중 인증에 초점을 맞추어 연구동향을 분석하고 고찰한다.

1. 서론

최근 무선 네트워크 및 센서네트워크 기술이 발달하면서 IoT(Internet of Things) 환경이 마련되고 가정에서도 사용자의 편의를 위해 다양한 서비스와 시스템이 보급되면서 우리의 삶이 편의를 갖기 시작했다. 과학기술의 발달로 스마트 디바이스 이용이 대중화됨에 따라 스마트 디바이스와 연동이 가능한 스마트홈, 스마트 헬스케어, 스마트 의료 등이 정착하고 있다[1]. 스마트홈 환경은 기존의 가정환경에서 정보통신기술을 융합하여 사용자와 가전기기가 실시간으로 정보와 데이터를 공유한다. 사용자가 스마트 디바이스 간의 무선 네트워크 기술을 통해 실시간으로 디바이스를 제어할 수 있다[2,3]. 이러한 통신으로 사용자가 3G/LTE 혹은 WiFi를 사용하여 스마트홈에 접근하여 원격 검침, 냉·난방 제어, 조명 제어, 전기 제어 등의 서비스를 제공받을 수 있다[4]. 이렇듯 스마트홈 환경은 사용자의 접근이 가능하기 때문에 보안적인 문제가 발생할 수 있다. 악의적인 사용자가 스마트홈 환경에 접근하여 데이터를 조작하거나 탈취, 오작동을 일으킬 수 있는 문제가 발생한다. 이를 예방하기 위해서는 스마트홈 환경에서 인증은 반드시 이루어져야 한다. 본 논문은 스마트홈 환경에서의 인증에 대한 분류 및 보안요구사항과 함께 현재 연구되고 있는 인증기술에 대한 동향과 고찰을 기술하고 결론을 짓는다.

Acknowledgments

이 논문은 2016년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016R1A2B4011069)

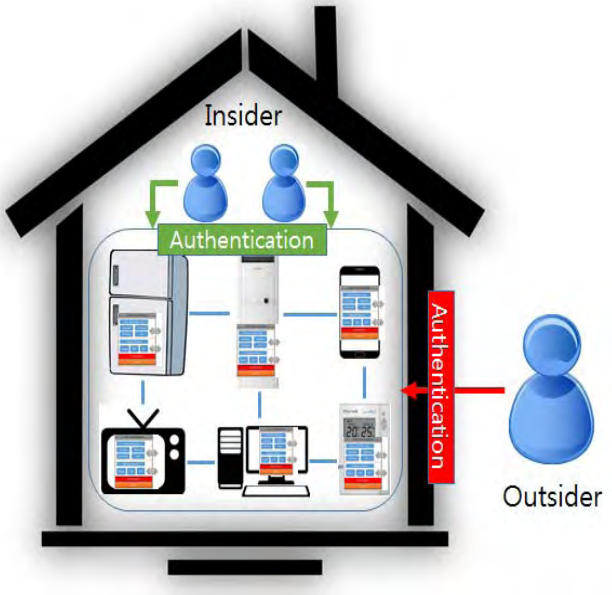
2. 관련연구

본 절에서는 스마트홈 환경에서 보안고려사항에 대해 설명하고 보안고려사항 중 인증에 초점을 맞추어 동향을 살펴본다.

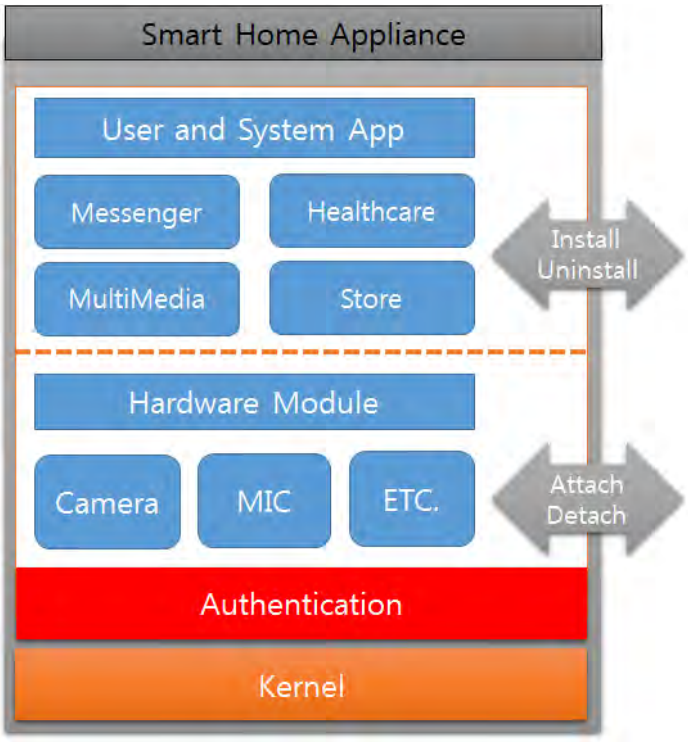
2.1 스마트홈 보안 요구사항

인증: 스마트홈 환경에서 인증은 두 가지를 생각할 수 있다. 첫 째는 스마트홈 환경에서 사용되는 디바이스에 대한 인증이다. 그림 1은 스마트홈 환경에서 인증에 대한 대략적인 개념도를 나타낸다. 대부분의 디바이스의 경우 보안을 고려하지 않고 사용되는 디바이스들이 많이 존재한다. 각각의 디바이스는 인증을 거치지 않기 때문에 스마트홈 환경에서 다양한 악의적인 행동이 가능할 수 있다. 예를 들어 디바이스는 무선네트워크 망에 모두 접속되어 있기 때문에 악성코드에 감염될 수 있다. 감염된 디바이스는 자유롭게 스마트홈 서비스에 사용되는 데이터 및 정보를 탈취하거나 변조가 가능하다. 또한 스마트홈 서비스 환경을 오염 시켜 Distributed Denial of Service (DDoS), Denial

of Service (DoS)도 유발할 가능성이 있다[3, 4, 5]. 스마트 환경에서 외부인, 내부인, 기기 등의 모든 개체는 반드시 인증을 받아야 홈네트워크에 접근이 가능하다.



(그림 1) 스마트홈 환경에서의 인증



(그림 2) 스마트홈 제품에서 내부 모듈 및 앱에 대한 인증

두 번째는 스마트 기기 내부 모듈에 대한 인증이다. 그림 2는 스마트홈 제품에서 내부 모듈 및 앱에 대한 인증을 나타낸다. 스마트홈 내부의 기기들은 기능을 제공하기 위한 하드웨어와 사용자의 편의에 맞게 서비스를 제공하는 앱의 형태로 존재하는데 이러한 형태는 모듈이라 칭한다. 스마트 기기 모듈의 경우 하드웨어 레벨에서는 각각의 모듈을 분해하거나 재결합이 가능한 형태를 가지며 User and System App 에서는 각각의 앱을 사용자가 설치하거나 삭제하는 등의 행위가 가능하다. 이러한 점은 의도적으로 악성 모듈을 삽입하거나 또한 사용자 및 개발자에 의해 사용자 앱의 형태로 스마트홈 제품에 설치하여 악의적인 행동으로 동작하게 할 수 있다. 이러한 경우도 앞서 말한 개인정보의 탈취 및 변조 더 나아가 공격자가 정상적인 모듈로 위장시킬 경우 사용자 몰래 악의적인 행동이 가능하도록 하는 백도어의 역할도 수행될 수 있고 정상적인 모듈의 기능을 저하시켜 가용성이 저하 될 수 있다. 따라서 스마트홈 환경에서 인증은 반드시 제공되어야 한다.

무결성: 스마트 홈 디바이스는 무선 네트워크 접근이 가능하기 때문에 디바이스의 보호 장치가 필요하다. 또한 공격자가 악성 소프트웨어 및 앱을 무단으로 삽입하거나 악성코드를 통해 원래의 기능이 아닌 정보수집이나 기타 악의적인 행동을 하게끔 용도를 변경할 수 있다. 만약 무결성이 보장되지 않는 다면 공격자에 의해 스마트 홈 시스템 전체가 악성코드에 감염되거나 스마트 홈 서비스의 가용성이 저하될 수 있다. 따라서 스마트 홈 디바이스의 무결성이 필요하다[5, 6].

가용성: 스마트 홈 디바이스는 무선 네트워크를 이용하여 외부에서 필요한 데이터를 공유한다. 따라서 공격자가 시스템을 장악하고 거짓정보 및 많은 양의 패킷이나 데이터를 전송한다면 스마트 디바이스의 오작동을 일으키게 하여 사용자에게 스마트 디바이스의 가용성을 저하시키게 한다. 가용성의 저하는 사용자에게 과부화로 인한 화재, 오작동으로 인한 전기요금 인상 등 금전적인 피해와 생명의 위협까지도 줄 수 있다[6, 7].

2.2 스마트홈 환경에서 인증에 대한 연구 동향 및 고찰

류호석 등 1명[3]은 스마트홈 환경에서 안전한 디바이스 관리를 위한 그룹키 관리 기법을 제안하였다. 제안 하는 기법은 새로운 스마트홈 디바이스를 스마트홈 서버에 디바이스 정보와 패스워드를 활용하여 등록하고 그룹키를 생성하는 프로토콜, 사용자가 외부에서 스마트홈 디바이스 와 통신하는 통신 프로토콜, 스마트홈 디바이스의 노후 및 고장으로 인해 디바이스를 교체 및 제거하는 탈퇴 프로토콜이다. 제안하는 기법은 최초 등록 과정에서 각 디바이스들은 서버 의 스마트홈의 그룹키를 나눠 갖고 저장함으로써 비인가 스마트 디바이스의 접근을 막을 수 있으

며 디바이스에 대한 인증을 제공하기 때문에 가용성을 저해하는 공격에 대해 방어가 가능하며, 디바이스의 정보에 대해 해시값을 생성하여 저장하기 때문에 디바이스 정보에 대해 무결성을 제공한다. 하지만 잦은 암호화 및 인증, 복호화 경우 효율성이 저하될 우려가 있다.

신광철[8]은 생체기반의 D. He scheme을 개선하여 네트워크 성능 향상과 익명성을 보장하며 URSC(Unique Random Sequence Code)와 가변식별자(variable identifier)를 이용한 실시간 인증 프로토콜을 제안하였다. 사용자의 생체정보와 ID, 패스워드, GW-node의 비밀키를 사용하여 상호 간 인증을 수행하고 패스워드의 입력을 제한하여 패스워드의 입력이 정확한지의 여부를 검사한다. GW-node 와 센서노드 간에는 URSC와 가변식별자를 경량화 하였다. 제안하는 프로토콜은 사용자의 생체정보를 활용하기 때문에 사용자의 종속적인 측면을 갖는다. 또한 사용자 생체정보와 함께 패스워드를 함께 입력하기 때문에 인증과정에 복잡성을 추가할 수 있다. 또한 GW-node 간의 난수가 생성되어 전송되기 때문에 재전송 공격 및 익명성 유지에 탁월한 면이 있다.

이대휘 등 1명[9]은 패스워드 기반의 인증 및 키 교환(PAKE)을 이용하여 사용자와 디바이스가 홈 게이트웨이를 통해 인증과 키 교환을 할 수 있는 3PAKE 기법을 제안한다. 제안방식은 XOR 연산과 해시연산을 통해 사용자와 스마트디바이스는 등록단계를 통해 홈 게이트웨이와의 패스워드를 주고받아 저장한다. 인증 및 키 교환 단계에서 정보 전송을 통해 사용자와 홈 게이트웨이, 스마트 디바이스 간의 상호 인증이 이루어진다. 또한 Diffie-Hellman 키 교환 프로토콜을 응용하여 인증과 키 교환 방식도 제안하였다. 사용자와 디바이스는 홈 게이트웨이에게 사전에 안전한 채널을 통해 패스워드 기반의 검증 값을 저장하고 홈 게이트웨이는 사용자와 스마트 디바이스에게 세션의 새로운 비밀 값을 전송한다. 사용자와 스마트 디바이스는 홈게이트웨이는 인증 값 생성단계에서 자신들의 인증 값을 생성하여 홈 게이트웨이에게 전송한다. 홈 게이트웨이는 인증 값을 사용자와 스마트 디바이스에게 분배하고, 세션키를 생성하여 상호 인증을 완료한다. 각각의 인증 방법마다 장점이 있지만 Diffie-Hellman 응용방식은 세션마다 사용자, 홈 게이트웨이, 스마트 디바이스가 생성하는 임의의 수를 모두 알 수 없기 때문에 세션키와 패스워드를 추측할 수 없어 무작위 패스워드 추측공격 방어에 장점이 있다. 하지만 한번 키가 노출되면 이후의 세션 정보도 계속 노출되는 단점과 많은 통신 회수에 대한 효율성 문제가 있을 수 있다.

3. 스마트홈에서 인증에 대한 서비스 시나리오

이번 절에서는 스마트홈에서 인증에 대한 서비스 시나리오에 대해 설명한다.

사용자 인증: 홈네트워크 접속하는 사용자를 인증하기 위해서는 사용자의 특정 비밀번호와 함께 생체정보를 사용한다.

① 사용자는 사용자가 기억하기 쉬운 비밀번호를 생성한다.

생성자ID사용자가 생성한 비밀번호는 스마트 디바이스에서 생성하는 난수 R과 함께 조합되어 변형된다.

$$PWuser = PWinit \oplus R$$

난수 R은 사용자가 결정하는 것이 아니라 스마트디바이스에서 시간을 기준으로 생성하고 테이블에 저장한다. 실질적인 비밀번호는 PWuser가 되고 사용자는 PWinit만 기억하고 대입한다.

③ 스마트 디바이스에서 사용자의 대한 인증은 입력받은 PWinit 값과 R값을 다시 조합하여 생성된 PWuser가 맞는지 확인한다. 확인이 완료되면 테이블에서 해당 값은 삭제된다.

④ 스마트 디바이스에서 인증 회수를 확인하고 인증 회수가 지정해놓은 값을 초과할 경우 외부인의 침입으로 간주하고 접근을 차단 한다.

스마트홈 디바이스 내부모듈에 대한 인증: 디바이스의 내부모듈은 하드웨어 및 user 및 system 앱으로 나뉘며 설치된 모듈의 개수, 내부에서 사용되는 난수, 버전 등을 통해 새로운 PWmodule을 만들어 사용한다.

① 인증모듈은 초기 PWmodule을 설치된 모듈의 개수 N, 내부에서 사용되는 난수 Rand, 버전 V, 생성시간 T를 조합하여 생성한다.

$$PWmodule = Rand \oplus N \oplus V \oplus T$$

② 인증모듈은 PWmodule를 커널과 공유하고 특정 메시지를 보낼 때 PWmodule를 함께 사용한다.

인증모듈→커널 : M(PWmodule, FIRST)

③ 인증모듈은 주기적으로 PWmodule을 확인하게 되는데 반드시 확인하는 경우는 모듈이 설치 및 삭제되어 모듈의 개수가 달라졌을 경우, PWmodule이 생성되고 난 후 지정된 시간이 경과하였을 경우, 조합하는 속성 중에 변화가 있을 경우, 커널이 재갱신을 요청하는 경우 PWmodule을 다시 조합하게 된다.

④ 인증모듈은 조합이 완료된 이전의 PWmodule은 삭제되고 최신 PWmodule은 다시 커널로 전송된다.

인증모듈→커널 : M(PWmodule′, RENEW)

⑤ 커널은 이전의 PWmodule과 전송받은 PWmodule′을 비교하고 이전의 PWmodule를 지우고 PWmodule′를 저장한다.

4. 결론

IoT 기술 및 정보통신 기술의 발전으로 스마트홈 환경이 점점 복잡해지고 고도화되고 있다. 스마트 홈 디바이스 간의 무선 네트워크 통신을 통해 사용자에게 편리한 서비스를 제공하고 있다. 스마트 홈 환경은 무선 네트워크를 사용하기 때문에 발생할 수 있는 다양한 보안 위협이 있다. 악의적인 스마트 디바이스 위장, 개인정보 탈취, 프라이버시 침해 등이 발생하고 있다. 따라서 이러한 보안 위협들을 방지할 수 있도록 인증 및 암호화, 무결성 제공 등이 필요하다. 본 논문에서는 스마트홈 환경에서 발생할 수 있는 보안 위협과 요구사항을 기술하였으며, 특히 스마트 홈 환경에서 인증과 관련하여 최근 연구 동향에 대해 기술하였다. 또한 각각의 제안하는 인증방법에 대한 장점과 단점을 분석하여 기술하고 정리하였다. 향 후 연구과제는 스마트홈 환경에서의 인증시스템에 대한 제안과 함께 스마트 홈 기기 내부 보안에 대한 인증방법도 연구하도록 할 것이다.

참고문헌

[1] Moo Hwan Kim, Yong Tae Shin, "A Study On The Smart Home Service Security Threat", Proceedings of Symposium of Korean Institute of communications and Information Sciences, pp 1069-1070, 2016.01

[2] 김선종, "스마트폰 환경에서 공인인증서 사용 시 소유 및 생체인증 연동 방법", 정보보호학회지 25(6), pp. 13-17, 2015.12

[3] 류호석, 곽진, "스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법", 정보보호학회논문지 25(2), pp. 479-487, 2015.4

[4] Jeong-Gi Lee, Chul-Seung Yang, Jun-Ha Kim, Kang-Jin Kim, "A Research and development of integrated Platform for data security between different smart home devices", Journal of The Korea Institute of Information and Communication Engineering, 19(5), pp 1173-1179, 2015. 05

[5] Cédric LÉVY-BENCHETON, Eleni DARRA, Guillaume TÉTU, Guillaume DUFAY, Mouhannad ALATTAR, "Security and Resilience of Smart Home Environments", European Union Agency For Network And Information Security, 2015. 12

[6] 김창희, 최성욱, 홍윤식, "스마트홈 그리드 환경에 적합한 원격접속 기기의 사용자 인증기법", e-비즈니스연구 16(1), pp. 65-82, 2015.02

[7] Pardeep Kumar, An Braeken, Andrei Gurtov, Jari Iinatti and Phuong Hoai Ha, "Anonymous Secure Framework in Connected Smart Home Environments", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 4, pp. 968-979, 2017

[8] 신광철, "무선센서네트워크 환경에서 생체기반의 개선된 사용자 인증 프로토콜", 한국전자거래학회지 18(3), pp. 107-123, 2013.8

[9] 이대휘, 이임영, "스마트홈 환경에서 패스워드 추측 공격에 안전한 개선된 3PAKE 기법에 대한 연구", 정보보호학회논문지 26(6), pp. 1471-1481, 2016.12