한국융합보안학회 2023년 추계학술대회 논문집

스마트 홈 침해사고 아티팩트 커버리지 확대를 위한 데이터 흐름 분석 연구

김유빈[1]*, 이종범[1], 한승주[1], 엄익채[2]
전남대학교 시스템보안연구센터(대학원생[1] ,교수[2])

Research on data flow analysis to expand coverage of smart home intrusion artifacts

Yu-Bin Kim0[1]*, Jong-Bum Lee[1], Seung-Ju Han[1] ,Ieck-Chae Euom[2]

요약 : 스마트 홈은 집에서 사용하는 기기를 사람이 원격으로 제어할 수 있는 기술 및 서비스로서 사용자와 밀접한 공간인 집에서 작동하는 기기라 침해사고가 발생 시 피해 규모가 크며 이를 조사하는 스마트 홈 포렌식 기술 역시 중요하다. 스마트 홈은 많은 데이터를 생성하고 전송하면서 침해사고 발생 시 많은 증거를 남기게 되지만 증거는 하나의 기기에 국한되지 않고 스마트 홈 인프라에 걸쳐 저장되면서 정확한 증거 식별이 어려워진다. 따라서 본 연구는 스마트 홈 대상 침해사고가 발생 시 발생하는 증거를 식별하기 위해 스마트 홈 환경 데이터 흐름을 분석하여 DFD(Data Flow Diagram)를 작성하여 증거 식별에 용이하도록 한다.

Key Words : IoT(사물인터넷), Smart home(스마트 홈), Digtal Forensics(디지털 포렌식), DFD(데이터 플로우 다이어그램)

1. 서론

네트워크의 발전에 따라 의료, 헬스, 공장, 자동차, 스마트 홈 등과 같은 다양한 분야에 사물인터넷이 확장되었다, 특히 가정의 안정성과 편리함을 제공하는 스마트 홈 분야의 관심이 높아지고 있으며 통계업체 'statista'는 전 세계 스마트 홈 시장 수기은 2022년에는 미화로 783억 달러에 달했으며 2032년에는 2,504억 달러까지 증거할 것이라고 예상했다[1].

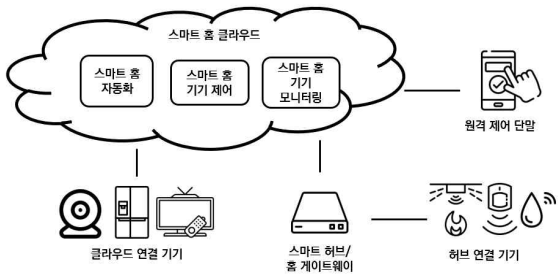
스마트 홈 기기는 사용자와 밀접한 공간인 집에 작동하게 되면서 민감한 데이터를 생성하기에 침해사고가 발생할 시 피해 규모가 크며 이를 조사하기 위한 스마트 홈 포렌식 기술도 중요하다.[2] 하지만 스마트 홈 기기 데이터는 기기에 국한되지 않고 스마트 홈 환경에 거쳐 데이터가 처리되고 저장된다.[3] 이러한 스마트 홈 환경은 침해사고 발생 시 조사자가 분산된 증거들의 식별을 어렵게 만든다.

따라서 본 연구는 스마트 홈 환경에 대해서 데이터를 전송하는 객체를 파악하고 객체간의 데이터 흐름을 분석하였다, 또한 침해사고 발생 시 생성되는 증거 추적을 보다 용이하도록 데이터 흐름도를 작성하였다.

2. 배경

2.1 스마트 홈

스마트 홈이란 주요 가전제품과 서비스를 연결하고 원격으로 제어 및 모니터링 할 수 있는 통신 네트워크를 통합한 주거 공간이다. 스마트 홈 환경 클라우드를 중심으로 구성되어 있으며, 크게 기기, 클라우드, 원격 제어 단말로 구성되어 있다. 기기는 WiFi를 이용해 클라우드와 바로 연결되는 스마트 TV, 스마트 냉장고, 스마트 카메라 등이 있으며 Zigbee, Z-wave, Bluetooth, Lora와 같은 근거리 통신망을 이용해 스마트 허브와 연동해서 사용하는 여러 센서 등이 존재한다.

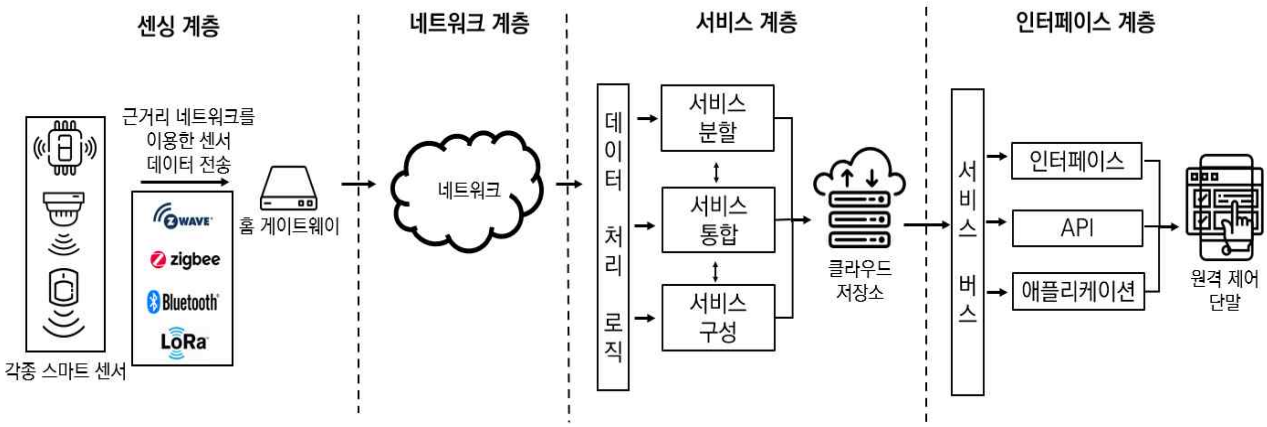


[그림 1] 스마트홈 환경

기기는 클라우드에 각종 센서 데이터를 전송하며 스마트 홈 관련 데이터는 클라우드에 저장된다. 사용자는 모바일과 같은 원격 제어 단말을 이용해 클라우드에 저장된 데이터를 수신하며 스마트 홈을 자동화하고 제어한다.

2.2 DFD(Data Flow Diagram)

DFD는 위협 모델링 단계에서 첫 번째로 수행되며 네트워크나 설계된 시스템에 데이터의 흐름을 추상적으로 보여주기 위해 일반적으로 사용된다. DFD는 주요 요소로 프로세스(Process), 데이터 흐름(Data Flow), 데이터 저장소(Data Store), 외부 객체(External Entity)로 구성된다. 본 연구는 데이터 흐름 분석을 용이하게 하기위해 DFD(Data Flow Diagram)을 이용하였다. [표]은는 각 DFD(Data flow Diagram)의 요소와 표현 방법을 보여 준다.



[그림 2] 스마트 홈 환경 데이터 흐름

[표 1] DFD(Data Flow Diagram) 구성요소

Element	Appearance	Meaning
Process	Process	any running code
Data Flow	data flow	Communication between processes, or between processes and data
Data store	Data Store	Things that store data
External entity	External Entity	people, or code outside your control
Trust Boundary	Trust Boundary	change of privilege levels

3. 데이터 흐름 분석 및 모델링

3.1. 스마트 홈 환경 데이터 흐름

스마트 홈 아키텍처에서 센서 데이터가 사용자에게 도달하기까지 [그림 2]와 같이 센싱, 네트워크, 서비스, 인터페이스 4가지 계층을 거쳐 사용자에게 제공된다[4]. 센서에서 생성된 원시 데이터는 Zigbee, Z-wave와 같은 저전력 프로토콜을 이용하여 홈 게이트웨이로 전송되며 홈 게이트웨이는 원시 데이터를 처리해 클라우드에 전송한다. 클라우드에 저장된 데이터는 클라우드 서비스에 따라 저장되고 처리된다. 그 후 원격 제어 단말 대상의 요청에 따라 데이터를 전송하게 되며 원격 제어 단말이 보내는 명령은 센서가 보내는 순서와 역순으로 진행해 데이터를 전송하게 된다.

3.2 데이터 흐름 모델링

스마트 홈 환경 대상으로 데이터 흐름을 보다 쉽게 파악하기 위해 [그림]과 같이 데이터 흐름 모델링을 진행하였다. 스마트 홈 환경을 가전기기에 원격으로 지시하는 Control Device Zone, 명령을 수행하는 기기가 존재하는 Smarthome Device Zone, 중간에 서비스를 제공하는 Service Zone으로 총 3가지 영역으로 분류하였다. 각 영역별 세부 프로세스 이전의 주요 프로세스 중심으로 데이터 흐름을 작성하였으며 외부 엔티티는 원격 제어 기기, IoT 허브, 홈 기기로 구성되며 저장소는 IoT 허브 저장소, 원격 제어 기기 저장소, 클라우드 저장소 3개로 구성하였다. 다음은 엔티티 및 저장소에 대한 설명이다.

(1) IoT Hub

스마트 홈 환경에서 Zigbee, Z-wave와 같은 저전력 프로토콜을 이용하여 Home Device와 통신하는 기기이다. Home Device와 지속적으로 통신하며 Home Device 데이터를 server로 전송해주는 역할을 한다.

(2) Home Device

스마트 홈 가전 기기 및 센서를 말한다. 스마트 TV, 스마트 냉장고, 문열림센서, 온습도 센서와 같이 다양한 기기들이 해당하며 기기에 따라 IoT Hub와 양방향 통신을 하는 액추에이터와 IoT Hub에 지속적으로 일방향 데이터를 보내는 센서로 나눠진다.

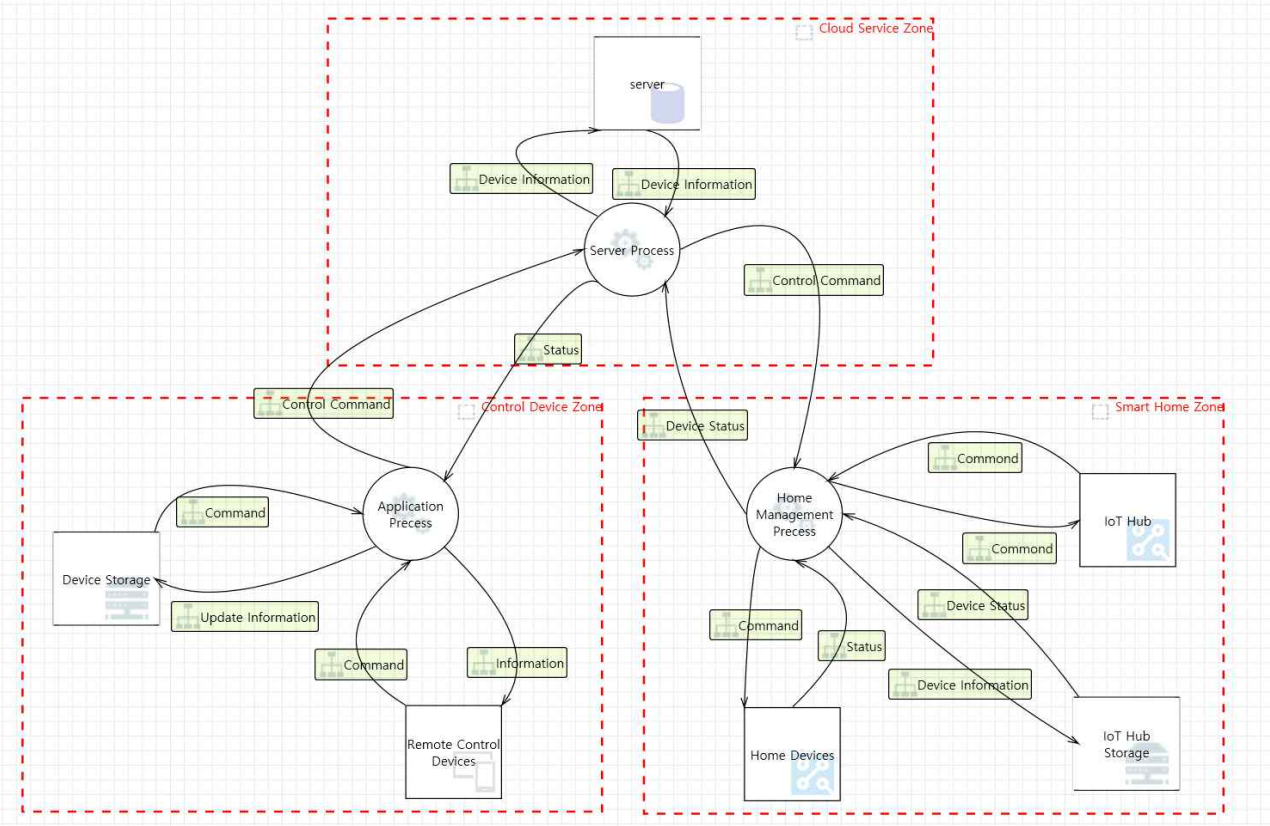
(3) IoT Hub Storage

IoT Hub의 내부 저장장치로서 저장장치 내부에 스마트 홈 기기의 등록정보를 저장하며 제조사에 따라 로그도 저장한다.

(4) Remote Control Device

사용자가 스마트 홈을 제어하기 위해 사용하는 스마트폰과 같은 기기이며 인터페이스 및 애플리케이션을 통해 server 통신하여 데이터를 받아오거나 명령을 전송한다.

(5) Device Storage



[그림 2] 스마트 홈 환경 데이터 흐름 모델링

Remote Control Device의 저장장소를 나타낸다. 스마트 홈을 제어하는 애플리케이션이 설치되는 공간이며 애플리케이션 관련 로그가 저장되거나 스마트 홈 로그가 저장된다.

(6) Server

서비스를 제공하는 측면의 서버로써, 사용자들의 정보 및 등록된 기기의 정보가 등록되어 있다. 스마트 홈 기기의 등록 및 삭제, 제거와 같은 기능과 자동화 서비스를 제공한다. 제공하는 서비스는 플랫폼에 따라 차이가 있으나 보통 기기 관련 서비스를 제공한다.

4. 결론 및 향후연구

사물인터넷 발전으로 다양한 분야의 관련 서비스가 증가하면서, 스마트 홈 서비스도 증가하였다. 스마트 홈 서비스는 사용자와 밀접한 공간인 집에서 이루어지기에 침해사고 시 많은 피해가 발생하며 이를 대상으로 한 디지털포렌식 조사는 중요하다. 하지만 침해사고 발생 시 증거는 기기만이 아니라 스마트 홈 환경에 걸쳐 많은 영역에 존재하기 때문에 수사자는 침해사고에 대한 정확한 증거 식별이 필요하다. 본 연구는 스마트 홈 환경에 발생하는 데이터를 분석하여 추상적인 데이터 흐름 모델을 작성함으로 침해사고가 발생 시 증거의 출처를 파악하기 용이하게 기여할 것이라고 예상한다. 향후 연구로 작성된 데이터 흐름을 기반으로 세부적인 기능을 추가한 모델 작성이 필요하다. 또한 이를 활용해 위협 모델링을 작성하여 그에 따라 발생 가능한 침해사고 도출하고 침해사고 별 생성 가능한 증거를 연결시키는 연구를 진행할 예정이다.

Acknowledgment

"이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2022-0-01203)

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2022R1G1A1010506).

참고문헌

[1] "Statista", https://www.statista.com/outlook/283/100/smart-home/worldwide.

[2] PLACHKINOVA, Miloslava; VO, Au; ALLUHAIDAN, Ala. Emerging trends in smart home security, privacy, and digital forensics. 2016.

[3] BOUCHAUD, François; GRIMAUD, Gilles; VANTROYS, Thomas. IoT Forensic: identification and classification of evidence in criminal investigations. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. p. 1-9.

[4] BOUCHAUD, François; VANTROYS, Thomas; GRIMAUD, Gilles. Forensic analysis of IoT ecosystem. In: 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2021. p. 115-122.