스마트 홈 플랫폼 센서 관련 아티팩트 식별 및 분류

김유빈*, 이종범*, 신동혁*, 엄익채**

전남대학교 시스템보안연구센터(*대학원생, **교수)

Identifying and classifying smart home platform sensor-related artifacts

Yu-Bin Kim*, Jong-Bum Lee*, Dong-Huck Shin*, Ieck-Chae Euom**

System Security Research Center, Chonnam National University
(*Graduate student, **Professor)

요 약

사물 인터넷이 발전하면서 스마트 홈 서비스가 증가하였다. 스마트 홈 서비스는 다양한 스마트 센서로 구성되어 있어 범죄 사고가 발생했을 때 많은 증거를 수집할 수 있다. 스마트 홈 플랫폼에서 센서 데이터는 클라우드, 홈 게이트웨이, 원격 단말에 걸쳐 저장되지만 스마트 홈 플랫폼마다 생성되는 아티팩트 및 저장 방식이 다르며 이를 식별하기 위한 사전에 연구가 필요하다. 본 연구는 스마트 홈 플랫폼 중 미 홈 플랫폼을 구축하여 홈 게이트웨이와 원격 단말에서 획득할 수 있는 스마트 센서 관련 아티팩트를 식별하고 식별 여부에 따라 분류하였다.

I. 서론

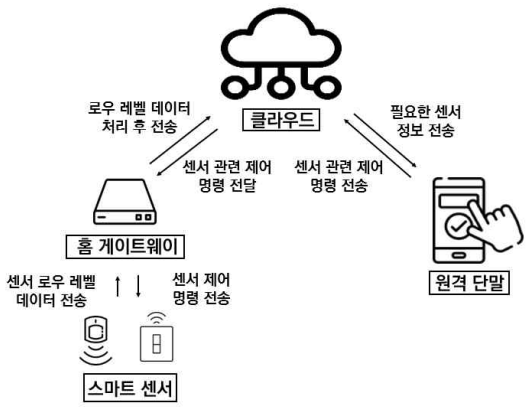
사물 인터넷 기술이 발전함에 따라스마트 홈 서비스의 발전에 따라 전 세계 스마트 홈 시장은 2022년 783억 달러 규모로 급증하면서 많은 가정에서 스마트 홈을 사용하게 되었다[1]. 이러한 스마트 홈은 다양하고 많은 정보를 수집하기 때문에 사고 조사를 위한 스마트 홈 포렌식 연구가 활발히 진행되고 있다[2]. 특히 센서 관련 아티팩트는 범죄 사고 조사에 필요하지만 홈 게이트웨이, 원격 단말, 클라우드 걸쳐 저장되기에 각 대상에 따른 데이터 식별 및 분석하는 사전 연구가 필요하다.

본 연구는 스마트 홈 플랫폼 중 샤오미가 제작한 미 홈 플랫폼 환경을 구축하여 홈 게이트웨이, 원격 단말을 대상으로 아티팩트를 식별 및 수집하였다. 그 후 식별한 아티팩트를 대상에 따라 분류하였다.

II. 스마트 홈 플랫폼 및 관련 연구

2.1 스마트 홈 플랫폼

스마트 홈 플랫폼은 [그림 1]과 같이 스마트 센서, 홈 게이트웨이, 원격 단말, 클라우드로 구성된다. 플랫폼 내에서 센서 데이터가 송수신 되며 사용자는 스마트 홈 플랫폼을 대상으로 모니터링 및 제어가 가능하다.



[그림 1] 스마트 홈 플랫폼 및 센서 데이터 흐름

스마트 센서는 로우 레벨 데이터를 게이트웨이에 송신한다. 홈 게이트웨이는 스마트 센서 데이터를 처리 후 클라우드에 전송하며 클라우드는 센서 관련 정보를 저장한다. 또한 원격 단말은 클라우드에 센서 정보를 전송받아 모니터링 하며 클라우드 서버를 통해 원격 제어 명령을 송신한다. 이 과정에서 센서 데이터가 게이트웨이, 클라우드, 원격 단말을 거치면서 많은 센서 관련 아티팩트를 생성한다.

2.2 관련 연구

스마트 홈 플랫폼을 대상으로 한 포렌식에 관한 연구는 다양하게 이루어지고 있다. Kang.S 등은 샤오미 플랫폼을 대상으로 원격 단말을 통해 획득할 수 있는 아티팩트를 식별하고 활용방안을 제시하였다[3]. Kim.S 등은 구글, 삼성, 티피링크 플랫폼을 구축해 원격 단말에 생성되는 아티팩트 수집하고 분류하였다[4]. Awasthi.A 등은 Almond 플랫폼을 대상으로 스마트 허브는 원격제어를 통해 아티팩트를 수집하였고, 원격 단말 저장소에 접근해 아티팩트를 수집 및 분석하였다[5]. Kim.J 등은 헤이 홈 플랫폼을 대상으로 API를 이용한 클라우드 데이터 수집 방안을 제시하였다[6]. Castelo Gomez.J 등은 샤오미 플랫폼 대상으로 기기 하드웨어 접근을 시도하였지만 실패하였고, 원격 단말을 대상으로 아티팩트를 수집 및 분석하였다[7].

관련 연구는 아티팩트 수집을 위해 원격 단말을 통해 수집하는 연구가 많았으며 홈 게이트웨이, 클라우드를 대상으로 하는 포렌식 연구가 부족했다. 본 연구는 게이트웨이, 원격 단말에서 얻을 수 있는 센서 관련 아티팩트 식별 및 수집을 목표로 수행하였다. 위 스마트 홈 포렌식 관련 연구를 수집 대상 및 플랫폼에 따라 [표 1]와 같이 분류하였다.

[표 1] 관련 연구 내용

관련 연구	홈 게이트웨이	클라우드	원격 단말	플랫폼
[3]	×	×	○	샤오미
[4]	×	×	○	구글, 삼성, 티피링크
[5]	○	×	○	아몬드
[6]	×	○	×	헤이홈
[7]	×	×	○	샤오미

III. 센서 관련 아티팩트 식별 및 분류

3.1 실험 환경

본 연구에서는 샤오미 플랫폼 환경에 아카라 스마트 홈 기기를 등록하여 스마트 홈 인프라를 구축하였다. 원격 단말로는 루팅된 스마트 폰을 이용했으며 미 홈 애플리케이션을 설치해 실험 환경 기기들을 연결하였다. 아래 [표 2]는 실험에 사용한 애플리케이션, 스마트 홈 기기, 스마트 폰 이름과 펌웨어 및 소프트웨어 버전이다.

[표 2] 스마트 홈 실험 환경 기기 및 버전

분류	이름	버전
애플리케이션	Mi home	8.6.710.2101
홈 게이트웨이	Aqara Hub M1S	4..0.10002
스마트 센서	Aqara door and window sensor T1	1.0.40
	Aara Humidity Sensor T1	39
원격 단말	Galaxy A 12	andoroid 12

센서 관련 아티팩트 수집 대상 중 클라우드 대상으로 한 디지털포렌식 조사는 클라우드 특성상 물리적인 서버가 없어 접근이 어려우며 클라우드 포렌식을 위한 도구도 부족해 어려운 문제로 남아있다[8]. 따라서 수집 대상은 접근이 가능한 홈 게이트웨이와 원격 단말을 대상으로 진행하였다.

3.2 센서 관련 아티팩트 식별

센서 관련 홈 아티팩트를 식별하기 위해 홈 게이트웨이의 파일 시스템과 원격 단말의 미 홈 애플리케이션 패키지를 대상을 전수조사를 진행하였다. 홈 게이트웨이는 텔넷을 통한 원격 접속으로 파일 시스템에 접근하였고 미 홈 애플리케이션은 원격 단말을 루팅해 내부 저장소에 접근하였다.

3.2.1 홈 게이트웨이

홈 게이트웨이는 리눅스 시스템의 기본 디렉토리 구조와 비슷하게 /etc, /bin, /dev, /usr 등등 총 13개의 디렉토리가 존재하였다. 그 중 센서 관련 아티팩트를 식별할 수 있는 디렉토리는 /data 이였다. /data 하위 디렉토리는 총 9개가 존재하였으며 그 중 /zigbee, /storage 에서 다음과 같은 센서 관련 아티팩트를 식별할 수 있었다. 2개의 디렉토리에서 센서가 사용하는 Zigbee node ID, 센서 디바이스 id, 센서 모델 명, MAC 주소, Zigbee nwk key, 연결된 센서 리스트와 같은 홈 네트워크 관련된 정보를 식별할 수 있었다.

3.2.2 원격 단말

원격 단말은 내부 저장소에 미 홈 애플리케이션 관련 정보가 저장되는 패키지 명은 /data/data/com.xiaomi.smarthome 이며, 총 20개의 디렉토리로 구성되어 있다. 디렉토리 중 shared_prefs 디렉토리는 106개의 xml 파일이 존재하였고 home_env_info.xml 파일에서 Home id, Room id, 및 Room id와 연결된 센서 리스트, 디바이스 id, 모델 명을 식별할 수 있었다. 패키지 내의 20개의 디렉토리 중 files 중 하위 디렉토리인 /plugin/install/rn 내에는 연결된 센서의 로그 정보를 식별할 수 있었다. 본 실험 환경에서는 문열림센서의 문열림 닫힘 정보와 시간 정보를 식별할 수 있었고, 온습도 센서의 온도, 습도, 시간 정보를 식별할 수 있었다.

3.3 식별된 센서 관련 아티팩트 분류

스마트 홈 플랫폼에 식별할 수 있는 아티팩트를 수집 대상에 따라 [표 3]과 같이 분류를 하였다. 홈 게이트웨이 및 원격 단말을 통해 센서 모델명, MAC 주소, 디바이스 id, 센서 리스트를 식별 할 수 있었지만 홈 네트워크 관련된 정보는 홈 게이트웨이에서만 센서의 위치 및 로그 정보는 원격 단말에서만 식

별할 수 있음을 확인하였다.

이는 스마트 홈 대상으로 디지털포렌식을 진행할 때 수집 대상에 따라 획득 가능한 센서 관련 아티팩트가 다르며 필요한 아티팩트에 따라 수집 대상을 좁힐 수 있음을 알 수 있다.

[표 3] 스마트 홈 플랫폼에서 획득 가능한 센서 관련 아티팩트 및 파일 타입

센서 관련 아티팩트	게이트웨이		원격단말	
	식별 여부	아티팩트 파일 타입	식별 여부	아티팩트 파일 타입
센서 모델명	○	info, json	○	xml
센서 MAC 주소	○	info	○	xml
센서 디바이스 id	○	info	○	xml
센서 리스트	○	info, json	○	xml
센서 Zigbee 채널	○	info, log	×	-
센서 Zigbee 노드 ID	○	info	×	-
센서가 사용하는 nwk key	○	info	×	-
센서 관련 로그	×	-	○	xml
센서가 존재하는 home ID	×	-	○	xml
센서가 존재하는 rome ID	×	-	○	xml

IV.결론 및 향후 연구

사물인터넷 기술 발전으로 스마트 홈 시장 또한 급격히 증가하였다. 스마트 홈 플랫폼의 스마트 센서는 가정에서 많은 정보를 수집하기에 범죄 사고가 발생했을 때 많은 증거를 남길 수 있다. 또한 스마트 센서는 스마트 센서 이외에 홈 게이트웨이, 클라우드, 원격 단말에 걸쳐 저장된다. 하지만 플랫폼 및 기기에 따라 관련 아티팩트가 저장되는 방식 및 저장 위치가 상이하다. 따라서 범죄 사고가 발생했을 시 효과적으로 스마트 센서 관련 아티팩트를 수집할 필요가 있으며 플랫폼 및 기기에 따른 생성 아티팩트 식별 연구가 사전에 진행돼야 한다. 본 연구는 스마트 홈 제품 중 샤오미 플랫폼을 아카라 제품으로 구축해 분석하였다. 홈 게이트웨이와 원격 단말을 중심으로 아티팩트를 식별하였으며 각 대상에 따라 획득할 수 있는 센서 관련 아티팩트를 정리하였다. 향후 연구는 스마트 홈 플랫폼을 대상으로 체계적인 아티팩트 식별 및 수집 방안이 필요하다.

Acknowledgment

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

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 2106061)

[참고문헌]

[1] “explodingtopics”, Smart Home Market Value & Industry Growth (2023-2032), https://explodingtopics.com/blog/smart-home-marketme-market

[2] “Etnews”, 홈 IoT 데이터로 범죄 수사한다..사상 첫 디지털 포렌식 기법 개발 착수, https://www.etnews.com/20210802000190

[3] 강수진, 신수민, 김소람, 김기윤, and 김종성, 샤오미 스마트홈 아티팩트 분석 및 활용 방안 연구, 디지털포렌식연구 15(1), 54-66

[4] Kim, Soram, Myungseo Park, Sehoon Lee, and Jongsung Kim. 2020. "Smart Home Forensics—Data Analysis of IoT Devices" Electronics 9, no. 8: 1215

[5] Awasthi, Akshay, et al. "Welcome pwn: Almond smart home hub forensics." Digital Investigation 26 (2018): S38-S46

[6] 서승희, 차해성, 김역, and 이창훈. (2022). 스마트 홈 헤이 홈 Air 의 클라우드 아티팩트 원격 수집 방안 연구. Journal of Korean Society for Internet Information, 23(5)

[7] Gómez, J. M. C., Carrillo-Mondéjar, J., Martínez, J. L. M., & García, J. N. (2022). Forensic analysis of the Xiaomi Mi Smart Sensor Set. Forensic Science International: Digital Investigation, 42, 301451

[8]YASSIN, Warusia, et al. Cloud forensic challenges and recommendations: A review. OIC-CERT Journal of Cyber Security, 2020, 2.1: 19-29.