디지털 포렌식을 위한 스마트 홈 플랫폼 아티팩트 수집 및 식별 방안

김유빈* ,신동혁*, 엄익채**

전남대학교 시스템보안연구센터 (*대학원생, **교수)

Research on the Collection and Identification of Smart Home Platform Artifacts for Digital Forensics

Yu-Bin Kim*, Dong-Hyuk Shin*, Ieck-Chae Euom**

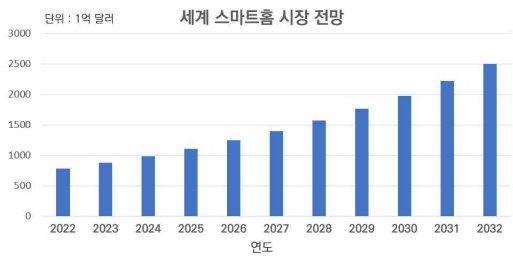
System Security Research Center, Chonnam National University
(*Graduate student, **Professor)

요 약

스마트 홈 기기는 영상, 음성, 다양한 센서 정보를 수집하기 때문에 범죄사고가 발생했을 때 많은 증거를 생성할 수 있다. 그러나 스마트 홈 기기는 제조사 및 제품 유형이 다양함에 따라 로그 저장방식이 달라 표준화된 로그 수집 및 분석 방법이 부족하다. 따라서, 본 연구는 스마트 홈 플랫폼인 스마트싱스 환경을 구축하여 기기와 연동된 스마트폰 애플리케이션을 통해 생성되는 아티팩트를 식별하고 수집한다. 또한, 스마트싱스 환경에서 얻을 수 있는 아티팩트를 표로 제시하여, 필요한 로그의 위치를 식별할 수 있고 적은 시간 내에 아티팩트를 수집하는 데 기여할 수 있다.

I. 서론

네트워크가 발전하면서 사물인터넷이 다양한 분야에 쓰이고 있으며, 스마트홈 분야의 관심도 높아지고 있다. [그림 1]와 같이 전 세계 스마트홈 시장의 수익이 2022년에는 미화로 783억 달러에 달했으며 2032년에는 2,504억 달러까지 증가할 것이라고 예상했다[1]. 이러한 스마트 홈 기기는 다양한 정보를 수집해 포렌식을 위한 증거물로 사용될 수 있다. 스마트홈 기기의 디지털 포렌식의 중요성은 증가하고 있다]. 하지만 스마트 홈 기기의 데이터 저장 방식은 기기 및 제조사 별로 달라 포렌식 조사를 위한 기술 및 연구가 부족한 상황이며 기기에 따른 데이터 습득 방법 및 분석에 관한 사전연구가 필요하다[2].



[그림 1] 세계 스마트홈 시장 전망

본 연구는 스마트 홈 플랫폼 스마트싱스 환경을 구축하여 스마트 홈 기기와 연동된 스마트폰 애플리케이션을 분석해 생성되는 데이터를 획득하고 분석한다. 또한, 관련 기기에 따라 생성되는 로그 파일을 식별하고 이를 표로 제시한다. 논문 구성은 다음과 같다. 2장에서 관련 연구 및 스마트싱스에 대해 서술한다. 3장에서는 분석 환경을 서술하고 스마트싱스에 생성되는 데이터를 수집하고 분석한다. 마지막으로 4장에서 결론을 짓는다.

II. 관련 연구 및 배경

2.1 관련연구

스마트 홈 기기 대상으로 한 포렌식에 관한 연구는 다양하게 이루어지고 있다. Lee.J 등은 스마트 홈 기기 대상으로 디버깅포트 접근, 칩오프, 연동되는 스마트폰 애플리케이션 접근 등 다양한 방법을 사용하여 데이터 획득을 시도했으며, 이를 통해 사용자 정보 및 기기 정보 등 여러 아티팩트를 획득하였지만, 상세한 아티팩트 생성 파일을 정리하지 않았다[3]. Kang.S 등은 샤오미 스마트홈 대상으로 생성되는 로그 및 데이터베이스를 분석하고 가상 범죄 시나리오를 통해 활용방안을 제시했지만, 추가적인 스

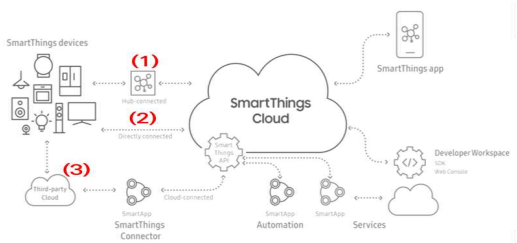
마트 홈 기기에 대한 연구가 필요하다[4]. Iqbal.A 등은 스마트 홈 기기 중 스마트 플러그에 중점을 두어 포렌식 조사를 수행할 때 어려운 문제를 분석하고 이를 해결하기 위해 패킷 캡처를 다양한 네트워크 환경에서 실험했지만 활용 부분에서 한계가 있다[5]. Kim.s 등은 다양한 스마트 홈 기기를 애플리케이션, 웹 인터페이스, API를 통해 데이터를 수집하고 분석했지만, 포렌식 관점에서의 활용성을 제시하지 않았다[6]. Hutchinson.S 등은 스마트 홈 기기 11개 기기에서 인증서, 사용자 정보, 엑세스 토큰 등 생성되는 로그를 식별하고 공격자의 관점으로 접근했을 시 취약한 정보가 있음을 확인했고, 이를 통해 가능한 공격 시나리오를 제시했다. 하지만 이를 활용한 로그 활용은 제시하지 않았다[7]. [표 1]은 관련 연구를 분석한 내용이다. 본 연구는 수사관이 스마트 홈 기기에서 쉽게 로그를 수집하고 활용할 수 있는 사전연구가 필요하기에 다양한 기기들의 추가적인 연구와 생성되는 로그 전수조사 후 활용방안을 제시한다.

[표 1] 관련 연구 내용

관련 연구	디바이스	수집 방법	아티팩트 활용 방법
[3]	TV, 카메라	모바일, 메모리 덤프	×
[4]	샤오미 스마트 기기	모바일	○
[5]	각종 스마트 플러그	패킷 캡쳐	×
[6]	스마트싱스, 구글 홈	모바일, 웹	×
[7]	구글 홈 및 각종 기기	모바일	×

2.2 스마트 홈

스마트 홈이란, 인터넷을 통해 연결된 가전제품, 조명, 난방 등의 기기들이 상호 연동되어 집안을 자동으로 제어하고, 사용자와 상호작용할 수 있도록 만든 시스템이다. 스마트 홈 기기는 각각의 플랫폼마다 연결되는 제품이 다르며, 본 연구은 스마트싱스 플랫폼을 다룬다. 스마트싱스 플랫폼은 스마트홈 기기 관리를 위해 삼성이 개발했으며, 스마트싱스와 연동되는 여러 기기를 통해 스마트 홈을 구축할 수 있다. 스마트 홈 기기 연결 방법은 총 3가지가 있으며, [그림 2]과 같이 허브와 연결되는 기기, 허브가 필요하지 않고 직접 연결되는 기기 그리고 서드파티 클라우드 통해 연결하는 기기가 있다. 각 기기들의 수집 데이터는 클라우드에 저장되며 사용자는 애플리케이션을 통해 수집 데이터를 받아와 기기를 모니터링하고 제어할 수 있다.



[그림 2] 스마트싱스 아키텍처

III. 실험 환경 구축 및 아티팩트 수집

본 연구에서는 삼성 스마트싱스를 대상으로 스마트 홈 인프라를 구축하였다. [표 2]과 같이 애플리케이션, 스마트 홈 기기, 분석 도구 및 스마트폰으로 구성하였으며, 제시한 소프트웨어/펌웨어 버전에 대해 실험을 진행하였다.

[표 2] 스마트 홈 기기 및 분석 도구

분류	이름	버전
애플리케이션	SmartThings	1.8.01.22
스마트 홈 기기	Samjin IoT Hub	000.047.00011
	Samjin Multipurpose Sensor	-
	IMILAB SmartThings Cam 360	2.1.3
분석 도구	DB Browser for SQLite	3.1.12
스마트폰	Galaxy A 12	andoroid 12

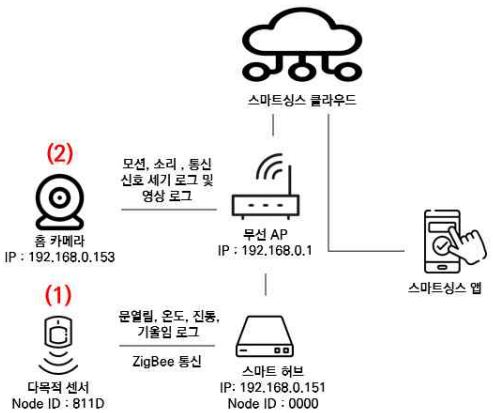
3.1. 실험 환경 구성

실험은 스마트 홈 기기가 허브와 연결되어 클라우드로 저장되는 방식(1)과 허브와 연결되지 않고 직접 클라우드에 저장되는 방식(2)으로 두가지 통신 환경으로 구성하였다.

(1) 다목적 센서는 Zigbee 통신으로 허브와 데이터를 주고받으며, 허브는 무선 AP를 통해 클라우드와 인터넷으로 연결되어 데이터가 저장된다.

(2) 홈 카메라는 WLAN 기반으로 무선 AP를 통해 클라우드에 데이터가 저장된다.

실험 환경에 대한 전체적인 구성은 [그림 2]와 같이 도식화하였다. 여기서, 스마트싱스 애플리케이션에 접근하기 위해서 스마트폰(단말기)를 루팅하였고, DB Brower for SQlite 소프트웨어를 활용하여 아티팩트를 식별 및 분석하였다.



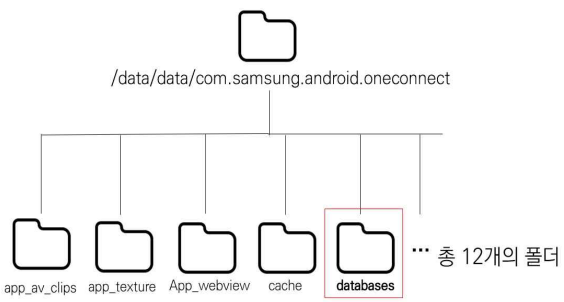
[그림 3] 실험 환경 구축

[표 3] 스마트싱스에 생성된 데이터베이스와 관련 로그 분류

데이터 베이스	총 테이블 수	총 필드 수	내용	허브	카메라	다목적 센서	사용자 정보	스마트싱스 기본 정보
ATMEntityDatabase.db	7	63	연결된 기기 정보 및 생성되는 로그 값 정보	○	○	○		
CamActivityHisory.db	3	13	카메라 관련 로그 정보		○			
Catalog.Db.db	7	117	스마트싱스와 연결 가능한 기기 정보					○
Cloud.db	9	73	연결된 기기 정보	○	○	○		
CommonData.db	8	42	연결한 사용자 정보				○	
ControlsProvider.db	3	33	연결된 기기 아이콘 정보	○	○	○		
DashboardDeviceData.db	3	17	사용자 대시보드에 표시된 정보	○	○	○		
DashboardUi.db	7	40	연결된 기기 정보	○	○	○		
DeviceCapbilityStatusData.db	5	30	연결된 기기의 마지막 로그 정보	○	○	○		
DeviceData.db	3	30	허브 정보 및 연결된 기기 기능 정보	○	○	○		
DeviceHealthData.db	3	6	연결된 기기 연결 상태 정보	○	○	○		
DevicePresentationData.db	4	25	연결된 기기에서 생성될 수 있는 로그에 대한 정보	○	○	○		
EasySetupContentsDb.db	9	57	스마트싱스 앱에서 사용하는 도움말 정보					○
FavoriteData.db	3	12	스마트싱스 앱 즐겨찾기 관련 정보					○
history.db	3	10	연결된 기기의 로그 정보	○	○			
InternalSettings.db	3	7	사용자의 정보, 클라우스 서버 ip 정보, 클라우드 토큰 등 클라우드 관련 정보				○	○
LandingUi.db	12	153	각종 센서 로그 정보	○		○		○
NotificationDb.db	3	27	연결된 기기의 알림 정보					
notifications.db	3	29	스마트싱스 기기 알림 정보	○	○	○		
PersistentLogData.db	3	12	데이터베이스 업데이트 및 각종 이벤트 정보	○	○	○		
PersistentServiceData.db	3	16	연결된 기기 관련 정보	○	○	○		○
SeviceData.db	11	107	스마트싱스 관련 기기 정보					○
SmartApps.db	4	15	스마트싱스와 연결 가능한 기기의 id 정보					○
SummaryData.db	4	7	온도 측정 관련 로그			○		

3.2 스마트싱스 아티팩트 수집

스마트싱스 애플리케이션의 패키지 명은 com.samsung,android.onconnect이다. 애플리케이션의 데이터는 스마트폰의 내부 저장소에 저장된다. 패키지 안에는 [그림 4]와 같이 12개의 폴더가 존재했으며, 폴더 중 로그가 주로 저장되는 databases 폴더만 수집 및 분석하였다. database 폴더에는 58개의 데이터베이스 파일이 존재하며 33개의 데이터베이스 파일에서 데이터가 식별되었다. 33개의 파일 중 9개의 파일은 내용이 중복돼 제외하였다. 데이터베이스 파일은 기기가 연결되면 생성되는 로그 및 센서 로그와 사용자 정보 로그가 있고, 스마트싱스 애플리케이션을 설치했을 때 생성되는 스마트싱스 기본 정보 존재한다. 각 기기의 관련 정보 및 사용자 정보는 [표 3]과 같이 여러 데이터베이스에서 확인할 수 있으며 같은 정보라도 여러 데이터베이스에 로그가 저장되는 것을 확인하였다.



[그림 4] 스마트싱스 패키지 폴더

3.2.1 허브 관련 정보

허브 정보는 스마트싱스에 등록된 디바이스 Id, 디바이스 Type 그리고 사용자가 설정한 디바이스 Name이 식별 된다. 그리고 허브의 펌웨어 버전과 드라이브 버전도 식별 된다. 무선통신 관련 정보는 허브 Mac 주소, 내부망 ip 주소, Zigbee 노드 주소, Zigbee 채널, Zigbee 펌웨어 버전, Z-wave 노드 주소, Z-wave 펌웨어 버전을 수집하였다.

3.2.2 카메라 및 센서 관련 정보

카메라 정보는 스마트싱스에 등록된 디바이스 Id, 디바이스 Type, 디바이스 name을 식별하였다. 또한. 카메라에 장착된 소리 감지 센서, 동작 감지 센서, 무선 통신 신호 세기 센서 측정된 데이터를 수집하였다. 센서 정보도 위와 동일하게 디바이스 Id, Type, Name을 확인하였다. 다목적 센서에서는 문열림 센서, 온도 센서, 기울임 센서, 진동센서와 관련된 데이터를 수집하였고, Zigbee 통신을 위한 Node Id도 수집하였다.

3.2.3 사용자 및 스마트싱스 관련 정보

사용자 관련 정보는 사용자 계정의 Uuid, 삼성 계정 Id, 사용자 이름, 사용지 E-mail 그리고 사용자 권한을 수집하였다. 스마트싱스 관련 정보는 연동된 기기와 상관없이 존재하는 데이터이다. 스마트싱스에 연동 가능한 기기의 정보와 스마트싱스 앱에서 사용하는 도움말과 같은 텍스트 데이터를 수집하였다

3.2.4 활용방안

각 기기들의 로그 정보는 [표 3]과 같이 하나의 데이터베이스에 저장되는 게 아니라 여러 데이터베이스에 저장된다. 만약 특정 데이터베이스가 지워졌을 경우 다른 데이터베이스를 통해 로그를 수집할 수 있다. 예를 들어 카메라 관련 로그는 CamActivityHisory.db, history.db, PersistentLogData.db에 저장되기 때문에 한 데이터베이스에 접근을 못 하더라도 다른 데이터베이스에서 로그를 얻을 수 있다. 또한, 적은 시간 내에 원하는 로그를 얻는데 활용될 수 있다.

IV.결론

사물인터넷 발전으로 스마트홈 기기의 사용량도 늘어났다. 스마트홈 기기는 지속적으로 정보를 수집하기 때문에 보안사고나 범죄사고가 발생했을 시 주요 증거물로 활용될 수 있다. 하지만 스마트홈 기기는 플랫폼 및 기기마다 저장되는 형태가 달라 이를 사전에 분석하고 연구할 필요가 있다. 본 연구는 스마트홈 제품 중 스마트싱스 기기로 환경을 구축해 분석했다. 스마트싱스 애플리케이션을 통해 스마트 기기의 각종 로그 정보가 데이터베이스로 저장되는 것을 확인하였다. 이를 분석해 각 기기의 관련된 로그 정보와 로그들이 존재하는 데이터베이스를 식별하고 이를 표로 제시하였다. 제시된 표는 기기 관련 데이터베이스가 파일이 지워졌을 경우 다른 데이터베이스를 통해 정보를 얻거나, 적은 시간 내에 필요한 로그를 수집하는 데 기여할 수 있을 것으로 생각된다.

Acknowledgment

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

[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] 이진오, and 손태식, 스마트홈 가전 및 IoT 기기 포렌식을 통한 범죄 수사에 사용될 수 있는 아티팩트 획득, 디지털포렌식연구 16.2 (2022): 98-115.

[4] 강수진, 신수민, 김소람, 김기윤, and 김종성, 샤오미 스마트홈 아티팩트 분석 및 활용방안 연구, 디지털포렌식연구 15(1), 54-66.

[5] Iqbal.A., Olegård.J, Ghimire.R., Jamshir.S, and Shalaginov.A, Smart Home Forensics: An Exploratory Study on Smart Plug Forensic Analysis, IEEE International Conference on Big Data, December, 2020.

[6] Kim.S, Park.M, Lee.S, and Kim.J, Smart home forensics－data analysis of IoT devices, Electronics, July, 2020.

[7] Hutchinson.S, Yoon, Y. H, Shantaram.N, and Karabiyik.U, Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory, ASEE Virtual Annual Conference Content Access., June, 2020.