정 보 보 호 학 회 지
제 31 권 제6호, 2021. 12

스마트 홈 IoT 포렌식 기술 동향

김 민 주*, 손 태 식**

요 약

다양한 스마트 홈 IoT가 개발됨에 따라 가정 내에서 IoT를 활용한 서비스가 확장되고 있다. 스마트 홈 IoT와 IoT가 등록된 스마트 폰은 서비스 제공을 위해 클라우드 서버와 통신을 수행한다. 클라우드 서버와 통신 과정에서 스마트 홈 IoT와 스마트 폰, 클라우드 서버에는 사용자에 대한 다양한 정보가 저장될 가능성이 있다. 사용자에 대한 다양한 정보가 클라우드 서버로 전송되는 것은 개인정보 문제를 야기할 수 있지만, 포렌식 관점에서는 범죄를 해결하는 데 증거로 사용될 수 있다. 따라서 본 논문에서는 클라우드 서버와 통신을 수행하는 클라우드 기반의 스마트 홈 IoT를 대상으로 데이터를 수집하는 기법을 알아보고 데이터 수집 기법이 적용된 기존의 스마트 홈 IoT 연구를 스마트 홈 IoT 기기 별로 나누어 분석한다.

Ⅰ. 서 론

인터넷의 발달과 5G의 도입으로 가정에서 활용되는 다양한 스마트 홈 IoT가 개발되고 있다. 다양한 스마트 홈 IoT가 발전됨에 따라 가정 내에서 IoT를 활용한 서비스가 확장되고 있다. 특히, 신축 아파트에서는 스마트 가스 차단기, 스마트 도어락 등 스마트 홈 IoT가 기본적으로 내재되어 있을 뿐만 아니라 내재된 스마트 월패드를 사용하여 스마트 홈 IoT를 제어할 수 있다.

스마트 홈 IoT는 사용자에게 다양한 서비스를 제공하기 위해 스마트 폰에 등록하여 사용된다. 이 때, 스마트 홈 IoT와 IoT가 등록된 스마트 폰은 서비스 제공을 위해 클라우드 서버와 통신을 수행한다. 클라우드 서버와 통신 과정에서 스마트 홈 IoT와 스마트 폰, 클라우드 서버에는 사용자에 대한 다양한 정보가 저장될 가능성이 있다. 이는 사용자의 개인 정보 보호 문제로 이어질 수 있다. 실례로 레이드 포럼 웹 사이트에서 한국의 아파트를 찍은 사진이 유통되는 것이 확인되었다[1]. 레이드 포럼은 한국인의 개인 정보가 불법적으로 유통되는 해외 웹 사이트로 아파트 내의 월패드의 카메라가 해킹되어 영상이 유출된 것이다. 해당 사건에서 한 아파트의 여러 세대에 설치된 월패드가 공용 인터넷 망을 사용하였기 때문에 하나의 월패드가 해킹되면 동일한 아파트의 다른 가정의 월패드 또한 손쉽게 해킹할 수 있었다. 이처럼 사용자에 대한 다양한 정보가 클라우드 서버로 전송되는 것은 개인정보 문제를 야기할 수 있지만, 포렌식 관점에서는 범죄를 해결하는 데 증거로 사용될 수 있다.

따라서 본 논문에서는 클라우드 서버와 통신을 수행하는 클라우드 기반의 스마트 홈 IoT를 대상으로 데이터를 수집하는 기법을 알아보고 기존 연구에서 수행된 포렌식 연구 분석을 통해 스마트 홈 IoT에서 사용되는 주요 포렌식 기법을 도출하고자 한다. 구성은 다음과 같다. 2장에서는 클라우드 기반의 스마트 홈 IoT에 적용될 수 있는 대표적인 포렌식 수행 방법에 대해 설명한다. 3장에서는 대표적인 스마트 홈 IoT에 수행된 디지털 포렌식 연구들을 기기별로 나누어 다루고, 4장에서 결론을 맺는다.

Ⅱ. 클라우드 기반 스마트 홈 IoT 데이터 수집 기법

클라우드 기반 스마트 홈 IoT는 클라우드 서버 및 스마트 폰과 통신을 수행하며 서비스를 제공한다. 이 때 사용자의 개인 정보가 통신 과정에서 전송되고 클라우드 서버와 스마트 폰, 스마트 홈 IoT 내부에 저장될 것이다. 본 장에서는 스마트 홈 IoT에서 수행될 수 있는 데이터 수집 기법에 대해 다룬다. 스마트 홈 IoT에서 수행될 수 있는 데이터 수집 기법은 통신 데이터를 수집하는 네트워크 스니핑과 MitM (Man-in-the-Middle), 기기 내 저장되는 데이터를 수집하는

* 아주대학교 AI융합네트워크학과 (대학원생, klklkl098@ajou.ac.kr)
** 아주대학교 사이버보안학과 (교수, tsshon@ajou.ac.kr)

Chip-off로 나눌 수 있다.

2.1. 네트워크 스니핑

스마트 홈 IoT가 스마트 폰과 클라우드 서버와 통신을 할 때 공격자는 패킷 스니핑을 통해 패킷을 탈취할 수 있다. 스니핑은 네트워크 상의 패킷을 도청하는 것이다. 네트워크 스니핑을 수행하여 패킷 데이터를 수집하면 사용되는 스마트 홈 IoT에서 발생되는 데이터와 스마트 홈 IoT로 전송되는 전체 네트워크 트래픽을 수집할 수 있다. 네트워크 스니핑은 암호화 되지 않은 패킷이라면 패킷의 내용을 확인할 수 있기 때문에 사용자 정보에 대해 암호화를 하지 않고 데이터를 전송할 경우 네트워크 스니핑을 통해 사용자 정보를 확인할 수 있다. 하지만, 네트워크 스니핑을 수행하여 데이터를 수집하는 경우 암호화 된 패킷 데이터를 수집할 수 있지만 암호화되어 있기 때문에 수집된 데이터를 분석할 수 없다는 단점이 있다.

대표적인 네트워크 패킷 스니핑 도구는 Wireshark이다 [2]. Wireshark는 실시간으로 네트워크 패킷을 수집하는 도구로 Windows, Linux 등 다양한 플랫폼에서 사용 가능하다. 또한, 다양한 구간에서 데이터를 수집할 수 있고 사용된 네트워크 프로토콜을 확인할 수 있다.

2.2. MitM

네트워크 스니핑을 수행하여 네트워크 패킷 데이터를 수집하는 경우 스마트 홈 IoT가 주고 받는 모든 패킷 데이터를 획득할 수 있지만 암호화 된 패킷의 내용은 확인이 불가능하다. 사용자의 민감한 데이터를 보호하기위해 스마트 홈 IoT는 TLS (Transport Layer Secure) 암호화 통신을 사용한다. 따라서 암호화 된 패킷을 수집하기 위해서는 MitM 기법을 활용하여 패킷 데이터를 수집할 수 있다. MitM이란 공격자가 클라이언트와 서버 사이에서 대신 통신하는 것으로 클라이언트에게 공격자를 신뢰할 수 있게 만들어 패킷 내용을 확인할 수 있다. TLS 통신 과정에서 MitM 공격을 수행하고 클라이언트와 서버를 대신하여 통신하는 과정은 다음과 같다. ① 공격자의 인증서를 클라이언트에 주입하여 클라이언트에게 공격자를 신뢰할 수 있도록 만든다. ② 공격자의 인증서가 클라이언트에 주입되면 공격자는 클라이언트가 서버에 보내는 요청을 가로챌 수 있다. 이 경우 공격자는 패킷의 내용도 확인할 수 있고 클라이언트의 패킷 대신 자신의 패킷을 서버에 보내 자신이 원하는 내용을 서버에 요청할 수 있다. ③ 서버는 클라이언트의 요청 또는 공격자의 요청에 대한 응답을 공격자에게 보낸다. ④ 공격자는 서버에게 받은 응답 내용을 받아 확인한 후 클라이언트에게 보내거나 서버에게 받은 응답 내용이 아닌 자신이 조작한 응답을 클라이언트에게 보낼 수 있다.

MitM 공격을 수행하여 패킷을 탈취하는 대표적인 도구는 웹 프록시 도구는 Burp Suite이다 [3]. Burp Suite는 클라이언트에 인증서를 설치하여 TLS 암호화 통신을 수집하고 분석할 수 있다. 하지만 홈 IoT 기기에 직접 인증서를 삽입하는 것은 기기의 크기나 메모리 용량과 같은 문제 때문에 데이터를 수집하는데 한계가 있다.

2.3. 칩오프 (Chip-off)

칩오프는 물리적으로 데이터를 수집하는 기법으로 소프트웨어나 하드웨어 수준으로 데이터를 획득할 수 없을 경우 마지막으로 수행되는 기법이다. 대부분의 IoT 기기에는 PCB (Printed Circuit Board)가 있다. PCB는 프로세서, 메모리, 센서 등 IoT를 구성하는 데 필요한 구성 요소들이 있는 기판이다. PCB에는 IoT 기기의 데이터가 저장되는 플래시 메모리가 있다. PCB에서 NAND 플래시 메모리를 물리적으로 획득하여 데이터를 수집할 수 있다. 칩오프는 PCB에 열을 주어 플래시 메모리 칩을 분리하는 것이다. 이는 히트건, 솔더링 장비 등의 다양한 장비와 칩오프 및 Hardware에 대한 높은 이해도가 요구된다. 칩오프를 통해 획득된 NAND 플래시 메모리는 리더기를 사용하여 PC에 마운트 된다. 마운트 된 NAND 플래시 메모리의 데이터는 raw 이미지 형태로 획득 가능하다. 획득된 raw 이미지 형태의 데이터는 기기에 저장된 모든 데이터이고 파일 시스템 분석을 통해 데이터를 분석할 수 있다 [4].

그러나 다수의 스마트 홈 IoT 기기들은 소형화 되어 있어 메모리가 적거나 클라우드 서버에 데이터를 저장한다. 이 경우에는 PCB에 NAND 플래시 메모리가 존재하지 않으며, 단일 메모리 칩이 아닌 SoC (System on Chip)에 구현되어 있다. SoC는 프로세서, 메모리, 스토리지 등의 모든 블록이 단일 칩으로 구현되어 있

는 것이다. 이 경우 NAND 플래시 메모리를 특정하여 데이터를 획득하는 데 어려움이 있다. 각 스마트 홈 IoT 기기들의 NAND 플래시 메모리 유무, 구현 형태 등은 공개되어 있지 않기 때문에 칩오프를 수행하기 위해서는 스마트 홈 IoT 기기를 직접 분해하여 칩오프의 적용 가능성을 확인해야 한다.

Ⅲ. 클라우드 기반 홈 IoT 포렌식 연구

3장에서는 클라우드 기반 홈 IoT를 대상으로 수행된 포렌식 연구에 대해 설명한다. 클라우드 기반 홈 IoT에 대한 포렌식 연구 분석은 대표적인 스마트 홈 IoT인 스마트 TV와 AI 스피커에 대한 포렌식 연구 분석으로 나뉜다.

3.1. 스마트 TV 포렌식

본 절에서는 스마트 TV에 수행된 포렌식 연구에 대해 분석한다. 스마트 TV는 네트워크에 연결되어 TV를 시청하는 것 뿐만 아니라 인터넷 검색, OTT (Over-The-Top) 스트리밍 서비스를 사용할 수 있다. 2014년에 출시된 삼성의 스마트 TV (UE40F7000SLXXN)를 대상으로 수행된 Boztas *et al.*의 연구[5]와 2018년에 출시된 삼성의 스마트 TV (UN43NU7400FXKR)에 수행된 Nemayire *et al.*의 연구[6]를 설명한다.

3.1.1. Boztas *et al.*의 연구

Boztas *et al.*은 스마트 TV에서 데이터 추출을 위해 세 가지 방식을 사용하였다. 세 가지 방식은 NAND 플래시 메모리에 시그널 연결, MTK II (NFI Memory Toolkit II) 사용, 애플리케이션 사용이다. 세 가지 방식 중 MTK II를 사용하여 데이터를 획득하였다. MTK II는 메모리 칩에서 사용자 데이터를 추출해주는 도구이다. 삼성의 UE40F7000S
LXXN 스마트 TV에서 사용된 플래시 메모리는 삼성의 KLM4G1FE3B-B00이다. NAND 플래시 메모리의 칩을 획득하기 위해 칩오프를 수행하여 스마트 TV의 NAND 플래시 메모리를 추출하였다. 획득된 칩 내의 데이터를 획득하기 위해 MTK II 도구를 사용하여 사용자 데이터를 추출하였다. 해당 도구를 사용하여 스마트 TV의 사진, 연결된 장치, 웹사이트 방문 기록과 같은 데이터를 획득하였고 스마트 TV의 칩오프 가능성을 보였다.

3.1.2. Nemayire *et al.*의 연구

Nemayire *et al.*은 스마트 TV에서 포렌식을 위해 애플리케이션 레벨, 네트워크 레벨, 디바이스 레벨로 나누어 포렌식을 수행하였다. 이 중 디바이스 레벨에서는 칩오프를 수행하여 데이터를 획득할 수 있었다. 삼성의 UN43NU7400FXKR 스마트 TV는 칩오프를 수행하여 NAND 플래시 메모리 칩을 분리할 수 있었다. 본 연구에서는 데이터 분석을 위해 한컴 GMD에서 개발된 MD-Reader와 MD-NEXT를 사용하여 데이터를 분석하였다. 해당 NAND 플래시 메모리는 VDFS (Vertically Deliberate improved performance File System) 파일 시스템을 사용하였고 [7], 파일 시스템 분석을 통해 이미지, 음성, 비디오 파일과 같은 미디어 파일, 브라우저 히스토리, 구글 검색 기록을 획득하였다.

3.2. AI 스피커 포렌식

본 절에서는 AI 스피커를 대상으로 수행된 연구에 대해 설명한다. AI 스피커는 가정에서 많이 사용되는 홈 IoT 중 하나로 음성 명령을 통해 날씨 알림, 일정 추가와 같은 기능 뿐만 아니라 음성 명령으로 타 IoT를 제어할 수 있다. Jo *et al.*의 연구[8], Shin *et al.*의 연구[9]에 대해 살펴본다.

3.2.1. Jo *et al.*의 연구

Jo *et al.*은 스마트 홈 IoT와 페어링하여 사용되는 AI 스피커 에코시스템에 대한 디지털 포렌식 연구를 수행하였다. 이 연구에서는 AI 스피커 포렌식을 3개의 포렌식 영역으로 나누어 5가지 분석 방법을 제안하였다. 세 가지 포렌식 영역은 네트워크 포렌식, 모바일 포렌식, AI 스피커 포렌식 영역으로 나눠진다. 네트워크 포렌식 영역에서는 AI 스피커와 안드로이드 모바일 앱의 패킷을 분석하였다. 분석을 위해 MitM 기법을 사용하는 Fiddler 도구를 사용하여 패킷 데이터를 획득하였다. 클라우드 서버와의 통신 패킷을 분석하여 사용자 이름, 계정 정보, 이메일 등의 사용자 정보와 시간 정보 등을 획득하였다.

3.2.2. Shin *et al.*의 연구

*Shin et al.*은 AI 스피커와 클라우드 서버 사이의 암호화된 트래픽을 분석하기 위해 인증서를 AI 스피커에 주입하는 다섯 가지 방법을 제안했다. 다섯 가지 방법 중 AI 스피커 앱 취약점 분석과 플래시 메모리 재작업을 통해 인증서를 주입할 수 있었다. AI 스피커에 인증서를 주입하여 암호화된 트래픽을 분석할 수 있었고 사용자의 스케줄, 메모, 음성 명령어 등을 획득하였다. 해당 방법은 AI 스피커 뿐만 아니라 칩오프가 가능한 타 스마트 홈 IoT 기기에도 적용할 수 있을 것으로 추정된다.

Ⅳ. 결 론

본 논문에서는 클라우드 기반 스마트 홈 IoT의 데이터 수집 기법을 설명하고 스마트 홈 IoT인 스마트 TV와 AI 스피커에 포렌식을 수행한 연구를 분석하였다. 이를 통해 클라우드 기반 스마트 홈 IoT를 대상으로 MitM 기법을 활용한 네트워크 포렌식과 칩오프를 수행한 포렌식 기법을 활용할 수 있음을 확인하였다.

클라우드 기반 스마트 홈 IoT는 점점 더 다양하고 증가할 것이다. 이에 따라 클라우드 기반 스마트 홈 IoT에 대한 포렌식의 중요성 또한 함께 증가할 것이다. 따라서 클라우드 기반 스마트 홈 IoT에 대한 다양한 포렌식 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] 보안뉴스, 아파트 월패드 해킹 이슈 일파만파... 해킹 아파트 리스트 유포중, https://www.boannews.com/media/view.asp?idx=102768, Accessed at 2021.12.29.

[2] Wireshark, https://www.wireshark.org/, Accessed at 2021.12.29.

[3] Burp suite, https://portswigger.net/burp, Accessed at 2021.12.29.

[4] Lee, S., Jo, W., Eo, S., & Shon, T. (2019). ExtSFR: scalable file recovery framework based on an Ext file system. Multimedia Tools and Applications, 1-19.

[5] Boztas, A., Riethoven, A. R. J., & Roeloffs, M. (2015). Smart TV forensics: Digital traces on televisions. Digital Investigation, 12, S72-S80.

[6] Nemayire, T., Ogbole, A., Park, S., Kim, K., Jeong, Y., & Jang, Y. (2019). A 2018 Samsung Smart TV Data Acquisition Method Analysis. 디지털포렌식연구, 13(3), 205-218.

[7] A. V. Konradi, Performance Optimization of the VDFS Verified File System, MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

[8] Jo, W., Shin, Y., Kim, H., Yoo, D., Kim, D., Kang, C., ... & Shon, T. (2019). Digital forensic practices and methodologies for AI speaker ecosystems. Digital Investigation, 29, S80-S93.

[9] Shin, Y., Kim, H., Kim, S., Yoo, D., Jo, W., & Shon, T. (2020). Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. Forensic Science International: Digital Investigation, 33, 301010.

〈저 자 소 개〉

김 민 주 (Minju Kim)
학생회원
2020년 : 아주대학교 사이버보안학과 졸업
2020년~현재 : 아주대학교 AI융합네트워크학과 재학 (통합)
<관심분야> 네트워크 포렌식, IoT 포렌식, 모바일 포렌식

손 태 식 (Taeshik Shon)

종신회원

2000년 2월 : 아주대학교 정보및컴퓨터공학부 졸업 (학사)
2002년 2월 : 아주대학교 정보통신전문대학원 졸업 (석사)
2005년 8월 : 고려대학교 정보보호대학원 졸업 (박사)
2004년 2월~2005년 2월 : University of Minnesota 방문연구원
2005년 8월~2011년 2월 : 삼성전자 통신· DMC 연구소 책임연구원
2017년 3월~2018년 2월 : Illinois Institute of Technology 방문교수
2011년 3월~현재 : 아주대학교 정보통신대학 사이버보안학과 교수
<관심분야> Digital Forensics, ICS/Automotive Security