정 보 보 호 학 회 지
제 29 권 제6호, 2019. 12

AI 음성인식 기반 차량 인포테인먼트 포렌식 기술 동향

신 영 훈*, 김 민 주**, 정 다 안**, 손 태 식***

요 약

최근의 차량 인포테인먼트 시스템은 모바일 네트워크 및 스마트폰과 연결하여 다양한 서비스를 제공한다. 과거에는 제조사에서 독자적으로 개발한 OEM 인포테인먼트 시스템이 주를 이뤘지만, Android Auto, Apple CarPlay, Amazon Echo Auto 등의 개방형 플랫폼 생태계가 구축됨에 따라 다양한 차량들이 AI 음성인식 기반 차량 인포테인먼트 시스템을 탑재하고 있다. 이러한 차량 내 인포테인먼트 시스템은 스마트폰과 연동되며, 사용자에 대한 방대한 정보를 저장하고 처리함으로써 사용자의 선호도에 따른 On-Demand 서비스 등 다양한 편리성을 제공한다. 하지만 사용자에 대한 다양한 정보를 차량에 연동하여 사용하는 만큼 개인정보 문제로 이어질 수 있다. 그렇기 때문에 차량 인포테인먼트 시스템은 스마트폰과 같이 포렌식 관점에서 많은 증거를 획득할 수 있는 매체가 된다. 더욱이 스마트폰과 연동되는 시스템이기에 기존 모바일 포렌식 기법을 적용할 수 있다. 따라서 본 논문에서는 차량 인포테인먼트 시스템을 대상으로 수행된 포렌식 연구 분석을 통해 기존 연구에서의 포렌식 기법과 보완점을 도출하고자 한다.

Ⅰ. 서 론

5G의 도입 및 자율주행차량의 등장과 더불어 차량 내 인포테인먼트 시스템 또한 빠른 속도로 발전하고 있다. 차량 인포테인먼트 시스템의 발전으로 인해 차량이 제공할 수 있는 서비스가 확장되고 있으며, 최근에는 모바일 네트워크 및 스마트폰과 연결하여 더욱 다양한 서비스를 제공할 수 있다.

초기의 차량 인포테인먼트 시스템은 Ford의 차량에 탑재된 SYNC, 현대차그룹의 ccOS와 같이 제조사에서 독자적으로 개발한 OEM 인포테인먼트 시스템이 주를 이루었다. 하지만 최근에는 GENIVI Alliance, Android Auto, Apple CarPlay 등 개방형 플랫폼의 등장으로 인해 다양한 제조사의 차량이 AI 음성인식 기반 차량 인포테인먼트 시스템을 지원하며, 기존의 OEM 인포테인먼트 시스템 또한 이를 지원하기 위해 재설계되고 있다.

AI 음성인식 기반 차량 인포테인먼트 시스템은 스마트폰과 연결되며 음성인식 서비스를 제공하는 등 사용자에게 편리함을 제공하지만, 차량 및 스마트폰에 사용자에 대한 다양한 정보가 저장 될 가능성이 있다. 이는 데이터 보안, 개인 정보 보호 등의 문제로 이어질 수 있다. 포르쉐는 Android Auto가 활성화 될 때마다 전체 OBD2 덤프 데이터를 전송하기 때문에, 데이터 보안 및 개인정보보호를 위해 2017년에 출시할 차량에 Android Auto 대신 Apple CarPlay만을 지원한다고 밝힌 바 있다[1]. 이와 같이 사용자에 대한 다양한 정보가 기기 내에 저장되거나 서버로 전송되는 것은 개인정보 문제를 야기할 수 있다. 하지만 포렌식 관점에서 차량은 범죄 수사에서 중요한 증거를 획득할 수 있는 매체가 될 수 있으므로, 범죄를 해결하는 데 도움을 줄 수 있다. 예를 들어 차량이 도난당한 경우 인포테인먼트 시스템 및 GPS 정보를 범인을 파악하는 데 활용할 수 있다[2]. 또한 차량이 네트워크에 연결됨에 따라 PC 또는 스마트폰에서 발생할 수 있는 다양한 보안 위협에 노출될 수 있어 차량 포렌식의 중요성이 높아지고 있다. 실제로 DEFCON 26에서 블루투스 취약점, Wi-Fi 공격, USB를 통해 차량 인포테인먼트 시스템을 해킹하는 방법에 대한 발표가 진행된 바 있다[3].

차량 인포테인먼트 시스템은 모바일 기기와 유사한 특징을 가져 모바일 포렌식에 사용되는 도구와 기법이 적용될 수 있다. 본 논문은 차량 인포테인먼트 시스템을 대상으로 수행된 포렌식 연구 분석을 통해 기존 연구에

* 아주대학교 컴퓨터공학과 (syh2347@ajou.ac.kr)
** 아주대학교 사이버보안학과 (klklkl098@ajou.ac.kr, gong3gong@ajou.ac.kr)
*** (교신저자) 아주대학교 사이버보안학과 (tsshon@ajou.ac.kr)

서의 주요 포렌식 기법과 보완점을 도출하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 차량 인포테인먼트 시스템들의 동향에 대해 설명한다. 3장에서는 차량 인포테인먼트 시스템을 대상으로 수행된 디지털 포렌식 연구들을 다루고. 4장에서는 AI 음성인식 기반 차량 인포테인먼트 시스템 포렌식 방안을 다룬다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 차량 인포테인먼트 시스템 동향

최근 현대, 아우디, 폭스바겐 등 다양한 제조사의 차량들은 인포테인먼트 시스템을 기본적으로 탑재하여 출시된다[1]. 과거의 차량 인포테인먼트 시스템들은 제조사에서 직접 개발하여 탑재되었지만, 최근의 인포테인먼트 시스템들은 OEM 인포테인먼트 시스템에 아마존 알렉사와 같은 음성 인식 서비스, Android Auto, Apple CarPlay 등의 플랫폼을 연계하여 스마트폰 및 음성으로 차량을 제어할 수 있는 기능을 제공한다. 본 장에서는 제조사에서 직접 개발한 OEM 인포테인먼트 시스템, GENIVI Alliance, 오픈 플랫폼인 Android Auto와 Apple CarPlay에 대해서 다룬다.

2.1. OEM 인포테인먼트 시스템

OEM 인포테인먼트 시스템은 대표적으로 Ford의 SYNC가 있다. SYNC는 차량 내 통신 기능 및 엔터테인먼트 시스템 역할을 한다. Ford는 2007년 SYNC 1세대를 출시하였고, 2010년에 SYNC 2세대 마이포드 터치를 출시하였다. SYNC 2세대부터 운전자가 스마트폰과 차량을 연결할 수 있게 되었고, 2014년도에 출시된 SYNC 3세대에서는 Android Auto와 Apple CarPlay를 지원하여 스마트폰과 연동성을 갖게 되었다. 또한 아마존의 알렉사를 접목시켜 AI 비서 기능을 제공한다. Ford에 따르면 2020년에 출시되는 SYNC 4세대는 이러한 엔터테인먼트 시스템을 강화시키고, 클라우드 서비스에 크게 의존성을 두어 사용자의 편의성을 확장시킬 것이라 전했다.

Ford 이외에도 토요타는 차량에 MirrorLink와 아이폰을 동시에 지원하는 차량 인포테인먼트 시스템을 탑재하였다. 르노삼성은 KT와 개발 협력을 통해 인공지능 기반의 차량용 인포테인먼트 시스템 이지 링크를 출시하였다.

2.2. GENIVI Alliance

GENIVI Alliance(이하 GENIVI)는 차량 인포테인먼트 시스템 및 커넥티드 차량 솔루션을 위한 플랫폼을 개발 및 표준화를 주도하는 공개 커뮤니티이다. GENIVI는 2009년 3월 2일 BMW Group, Delphi, GM, Intel, Magneti-Marelli, PSA Peugeot Citroen, Visteon 및 Wind River Systems에 의해 설립되었다. 현재 140개 이상의 회사가 참여중이며, 국내에는 현대자동차, LG 전자, 현대 모비스 등의 업체가 멤버에 속해있다.

GENIVI는 차량 인포테인먼트 시스템 생태계의 조성 및 표준화를 위해 다양한 프로젝트를 진행하고 있다. 차량 인포테인먼트 시스템의 개방형 플랫폼 생태계 조성을 위해 GDP(GENIVI Development Platform)를 제공하고 있으며, 차량 운전석에 있는 다양한 운영체제의 통합을 용이하게 하기 위해 Android Automotive Special Interest Group과 Multi-OS Integration Project를 운영하고 있다. 또한, 차량을 대상으로 하는 위협 및 해킹으로부터 시스템을 보다 안전하게 만들기 위해 차량용 하이퍼바이저 인터페이스 표준화를 진행하고 있다.

2.3. Android Auto

Android Auto는 2015년 구글이 출시한 차량용 안드로이드 운영체제이다. 차량 내부에 있는 디스플레이 장치에 안드로이드 실행 환경을 미러링하는 플랫폼으로, 현재 Ford, Audi, Jeep, 현대, 기아 등 50개 회사의 500종류가 넘는 차량이 Android Auto를 지원한다. Android Auto 앱은 2019년 11월 기준으로 4.8.594324 버전이며 지속적인 보안 업데이트 및 기능 업데이트가 진행되고 있다.

운전자는 USB 또는 Wi-Fi 연결을 통해 안드로이드 기기를 차량 내 디스플레이에 연결할 수 있으며, 블루투스 연결을 통해 알림을 표시하고 연락처 정보를 동기화하는 등의 기능을 사용할 수 있다. Android Auto는 전

1) Global Auto News, http://global-autonews.com/bbs/board.php?bo_table=bd_028&wr_id=43&page=3. Accessed at 2019.11.23.

화, 음악, 내비게이션, 차량 진단, 인터넷 검색의 5가지 기본 메뉴를 제공하며 Google 지도, 카카오내비 등과 같은 Android Auto와 호환되는 앱을 사용할 수 있다.

2.4. Apple CarPlay

Apple CarPlay는 애플이 2014년 3월에 발표한 차량용 운영체제이다. 차량 내부에 있는 헤드 유닛이 디스플레이 및 아이폰용 컨트롤러 역할을 할 수 있도록 하는 플랫폼으로 쉐보레, 현대, 르노 삼성 등 총 72개 회사의 500종류가 넘는 차량이 Apple CarPlay를 지원한다. Apple CarPlay는 iOS 내장 기능으로 iOS 7.1 이상의 iPhone 5 모델부터 사용할 수 있으며, iOS 업데이트와 함께 지속적으로 기능 업데이트가 진행되고 있다.

운전자는 USB 또는 블루투스 연결을 통해 아이폰을 차내 디스플레이에 연결할 수 있으며, 아이폰의 시리(Siri)를 이용해 음성으로 전화번호 검색, 메시지 확인, 애플 지도, 음악 재생 등을 기능을 사용할 수 있다. 이외에도 iOS12 부터는 호환되는 써드파티 앱을 사용할 수 있다.

Ⅲ. 차량 인포테인먼트 포렌식 연구

3장에서는 차량 인포테인먼트 시스템을 대상으로 수행된 포렌식 연구에 대해 설명한다. 차량 인포테인먼트 시스템 포렌식의 연구 대상은 크게 OEM 인포테인먼트 시스템, Android Auto, Apple CarPlay 세 가지로 나뉜다.

3.1. OEM 인포테인먼트 시스템 포렌식 연구

본 절에서는 OEM 차량 인포테인먼트 시스템을 대상으로 수행된 연구를 다룬다. Ford SYNC 1세대와 2세대를 대상으로 수행된 Jesse Lacroix et al.의 연구[4], Ford SYNC 3세대를 대상으로 수행된 Cohen의 연구[5]를 설명한다.

3.1.1. Jesse Lacroix et al.의 연구

Jesse Lacroix et al.은 Ford의 음성인식 인포테인먼트 시스템 SYNC 1세대와 2세대의 데이터를 획득하고 해당 시스템에 저장된 아티팩트를 도출하는 연구를 수행하였다. 논리적 데이터 획득 기법과 하드웨어 인터페이스인 JTAG 포트를 사용해 Ford f-150 차량에 탑재된 SYNC의 데이터를 획득할 수 있음을 보였으며, 이후 수집한 덤프 이미지를 대상으로 Encase, FTK(Forensic Toolkit), Autopsy 등의 상용 디지털 포렌식 도구를 사용하여 포렌식 분석을 수행했다. 이를 통해 인포테인먼트 시스템에 연결된 기기 목록, 전화번호부, 설정, 로그 정보 등 다양한 아티팩트를 도출함으로써 차량 인포테인먼트 시스템에도 일반적인 파일시스템 포렌식 기법이 적용될 수 있음을 보였다.

3.1.2. Cohen의 연구

Cohen은 SYNC 3세대가 탑재된 Ford 차량을 대상으로 포렌식 연구를 수행하였으며, 포렌식 관점에서 유의미한 정보를 획득할 수 있는 SYNC 모듈과 헤드 유닛의 데이터를 획득하기 위해 다양한 기법을 사용하였다. SYNC 모듈의 다양한 정보가 저장되는 NAND Flash의 데이터를 획득하기 위해 하드웨어 인터페이스인 USB 포트 및 JTAG 포트를 사용했으며 Chip-off 기법을 통한 NAND Flash의 데이터의 획득 또한 가능하다고 언급했다. 이후 수집한 데이터를 분석하여 페어링된 기기의 블루투스 연결 정보, 연락처, 전화 기록, SMS 메시지 등의 아티팩트를 도출했다. 또한, 헤드 유닛의 다양한 정보가 저장되는 하드 드라이브의 데이터를 획득하기 위해 업데이트 프로세스 익스플로잇 기법 및 하드웨어 펌웨어 Reflash 기법을 사용하였다. 이외에도 일반적인 하드 드라이브 덤프 기법을 통해서도 헤드 유닛의 데이터를 획득할 수 있음을 언급하였다. 이후 획득한 데이터를 분석하여 주행 정보, 위치 정보, 목적지 목록 등의 내비게이션 정보 등 다양한 아티팩트를 도출하였다.

3.2. Android Auto 포렌식

본 절에서는 Google에서 출시한 차량 인포테인먼트 시스템인 Android Auto를 대상으로 수행된 연구에 대해 다룬다. Sarah Edwards et al.의 연구[6], Amit Kr Mandal et al,의 연구[7]를 설명한다.

3.2.1 Sarah Edwards et al.의 연구

Sarah Edwards et al.은 Android Auto와 연동된 스마트폰 앱에 대해 일반적인 안드로이드 포렌식 기법을 적용하였다. GMC Yukon Denali와 닛산 Sentra 차량과 연결했던 Samsung J7 Prime으로부터 앱 데이터를 획득한 후, 앱 디렉토리에 저장된 xml, database 파일에 대해 분석을 수행하였다. Android Auto 앱 디렉토리에 저장된 파일들을 분석하여 마지막 앱 사용 시간, 계정 연결 로그, 블루투스 연결 정보, 블루투스 설정 정보, 연결된 당시 지역의 날씨 등의 아티팩트를 도출하였다. 앱 디렉토리에 저장된 파일을 분석하는 과정에서 스마트폰의 연락처를 차량과 동기화하는 로그를 발견하였고, 차량에 연락처 정보가 저장될 수 있다고 언급하였다. 또한 메시지, 전화, 구글 지도 앱 디렉토리에 저장된 파일들을 분석하여 통화 시간, 메시지 전송 내용, 구글 지도 앱의 TTS(Text-To-Speech) 사용 기록 등의 아티팩트를 도출하였다.

3.2.2 Amit Kr Mandal *et al.*의 연구

Amit Kr Mandal et al.는 Android Auto 앱의 취약점 분석을 통해 외부 파일 접근, 파일 쓰기 권한, 암호화, IP 네트워킹, 미디어 자동 플레이, 음성 명령 등 9가지의 잠재적인 보안 위협을 식별하였다. 식별한 보안 위협을 분석하기 위해 JuliaSoft의 Dalvik Bytecode 분석 라이브러리인 The Julia Static Analyzer를 기반으로 Android Auto 앱 정적 분석기 Android Auto Checker를 제안했다. Android Auto Checker는 앱 소스코드 난독화로 인한 정적 분석의 어려움을 Julia Bytecode 표현을 통해 해결하며, 취약점이 존재하는 API를 사용하는지 식별한다.

Android Auto 앱을 대상으로 Amit Kr Mand al et al.의 연구에서 제안한 정적 분석 도구 Android Auto Checker를 사용하기 위해서는 일반적인 안드로이드 앱 디컴파일 분석 기법과 동일하게 apktool과 dex2jar 도구가 사용된다. 이후 제안한 도구를 사용해 Android Auto 앱 정적 분석을 수행한 결과, 대부분의 앱이 취약점이 존재할 수 있는 Entrypoint를 가지고 있다고 언급하였다. 또한 구글 플레이스토어에 등록된 Android Auto 앱의 약 80%가 잠재적인 보안 위협을 가지며, 이 중 25%의 경우 Javascript 취약점을 가지고 있음을 보였다.

3.3. Apple CarPlay 포렌식

본 절에서는 Apple CarPlay를 대상으로 수행된 연구인 Sarah Edwards et al.의 연구[6]를 설명한다.

3.3.1 Sarah Edwards et al.의 연구

Sarah Edwards et al.은 Android Auto 뿐만 아니라 Apple CarPlay와 연동된 스마트폰 앱에 대해 일반적인 iOS 포렌식 기법을 적용하여 스마트폰에 저장된 아티팩트를 도출하였다. Audi S3 차량과 연결했던 iOS 12.1.1 버전의 탈옥된 아이폰 X로부터 앱 데이터를 획득한 후, 기기에 저장된 plist, database 파일에 대해 분석을 수행하였다. Apple CarPlay 관련 database 파일을 분석하여 기기 연결 정보 및 CarPlay 설정 정보를 도출하였다. 또한 메시지, 시리, 위치 등 다양한 앱 분석을 통해 송수신한 메시지 내용, 시리 이용 기록, 사용한 앱 기록, 현재 위치, 차량의 이동 상태 및 속도 등의 아티팩트를 도출하였다. 특히 앱 사용 정보와 위치 정보에 정확한 타임스탬프가 기록되어 있어 이를 토대로 타임라인 기반 포렌식을 수행할 수 있으며, 이는 포렌식 수사 시 증거로서 활용될 수 있음을 언급하였다.

Ⅳ. AI 음성인식 기반 차량 포렌식 방안

본 장에서는 다양한 차량 인포테인먼트 시스템을 대상으로 수행된 포렌식 연구들을 통해 AI 음성인식 기반 차량 포렌식 방안에 대해 다룬다.

기존에 수행된 연구들은 차량 인포테인먼트 시스템과 모바일 기기가 유사한 특징을 가지는 점을 이용해 일반적인 모바일 포렌식 기법과 파일시스템 포렌식 기법을 적용하였다. OEM 인포테인먼트 시스템을 대상으로 수행된 연구에서는 데이터 수집을 위해 물리적/논리적 방법, Chip-off, 하드웨어 인터페이스(USB, JTAG)를 활용하였다. 이후 Encase와 같은 상용 포렌식 도구를 사용한 포렌식 분석을 수행하였다. 이를 통해 차량 인포테인먼트 시스템을 대상으로 일반적인 파일시스템 포렌식을 적용할 수 있음을 보였다. Android Auto와

Apple CarPlay를 대상으로 수행된 연구에서는 기기 데이터 수집을 위해 루팅 및 탈옥된 기기를 사용하였다. 이후 수집한 데이터를 대상으로 일반적인 모바일 포렌식 기법을 적용해 차량 사용자에 대한 다양한 정보를 도출할 수 있음을 보였다. 이는 Android Auto와 Apple CarPlay가 안드로이드 및 iOS 기기와 연결되어 동작하기 때문이며, 최근에는 OEM 인포테인먼트 시스템 또한 Android Auto 및 Apple CarPlay 플랫폼을 지원하기 때문에 모바일 포렌식 기법의 중요성이 더욱 증가할 것이다.

앞서 설명한 다양한 연구에서 볼 수 있듯이 모바일 기기에 설치된 차량 인포테인먼트 앱을 대상으로 일반적인 모바일 포렌식 기법을 적용할 수 있다. 하지만 차량의 Android Auto와 Apple CarPlay를 대상으로 하는 포렌식 연구는 아직 수행된 바 없다. 차량에 저장되는 정보는 모바일 기기와 일부 상이할 수 있으므로, 차량에 최적화된 타임라인 기반 데이터 수집 및 포렌식 기법과 차량용 포렌식 수사 모델에 대한 연구가 필요한 상황이다. 또한, 최근의 차량 인포테인먼트 시스템은 AI 음성인식 기능을 지원하고 있는 추세이다. 대표적인 AI 음성인식 기기인 AI 스피커가 범죄 사건의 증인으로 지목되었던 미국 아칸소 사건과 같이 음성인식 관련 정보는 실제 포렌식 수사에서 중요한 증거로 작용할 수 있다[8]. 이와 같은 배경에서 AI 스피커를 대상으로는 기기 내에 저장된 음성 답변 파일 및 기기 사용 기록과 웹프록시를 사용해 클라우드에 저장되어 있는 음성명령 기록을 획득하는 연구가 이미 수행된 바 있다[9]. 차량 인포테인먼트 시스템 또한 기기 내에 저장된 음성 파일 및 음성 명령 기록 저장 여부에 대한 포렌식 연구도 필수적으로 수행되어야 한다. 마지막으로 개인정보보호 관점에서 차량 및 스마트폰 앱이 클라우드와 통신하는 과정에서 주고받는 정보와 클라우드에 저장되는 정보를 파악하기 위한 포렌식 연구는 아직 수행된 바 없다. 최근 아마존 알렉사, 네이버 클로바를 비롯한 AI 스피커가 사용자의 음성 데이터를 머신러닝을 위해 클라우드에 저장하고 있었던 사례에서 볼 수 있듯이[10], 차량 및 클라우드에 저장되는 정보들의 저장 기간, 저장 유무, 암호화해야 하는 정보들에 대한 연구가 수행되어야 할 것이다.

Ⅴ. 결 론

본 논문에서는 차량 인포테인먼트 시스템의 동향을 파악하고, OEM 인포테인먼트 시스템, Android Auto, Apple CarPlay를 대상으로 수행된 포렌식 연구를 설명하고 분석하였다. 이를 통해 차량 인포테인먼트 시스템을 대상으로 일반적인 파일시스템 포렌식 기법과 모바일 포렌식 기법이 적용 가능하다는 것을 도출하였고, 기존에 수행된 연구들의 보완점과 최근 늘어나고 있는 AI 음성인식 기반 차량 인포테인먼트 시스템을 대상으로 수행되어야 할 포렌식 연구 주제들을 다뤘다.

AI 음성인식 기반 차량 인포테인먼트 시스템의 사용자 수는 5G와 커넥티드 카의 활성화에 따라 점차 증가할 것이고, 이에 대한 포렌식의 중요성 또한 같이 높아질 것이다. 차량 인포테인먼트 시스템 시장이 빠르게 변화하는 추세에 맞춰 다양한 포렌식 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] Berla Staff, “Android Auto, CarPlay, and Data Tracking,” BERLA, 2016.11.23, https://berla.co/android-auto-CarPlay-and-data-tracking

[2] Jesse Lacroix, “Vehicular infotainment forensics: collecting data and putting it into perspective,” Diss, 2017.

[3] Jay Turla, “Car Infotainment Hacking Methodology,” DEFCON 26, Unpublished, 2018. [video presentation].

[4] Jesse Lacroix, Khalil El-Khatib, and Rajen Akalu, “Vehicular Digital Forensics: What Does My Vehicle Know About Me?,” Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, ACM, 2016.

[5] Cohen, T, “Look At What My Car Can Do,” DEFCON 19, Unpublished, 2011. [video presentation].

[6] Sarah Edwards, Heather Mahalik, "They See Us Rollin, They Hatin – Forensics of iOS CarPlay and Android Auto," SANS DFIR, 2019.

[7] Mandal, Amit Kr, et al. "Vulnerability analysis of Android Auto infotainment apps," Proceedings of the 15th ACM International Conference on Computing Frontiers, ACM, 2018.
[8] Nicole Chavez, "Arkansas judge drops murder charge in Amazon Echo case," CNN, 2017.12. 02, https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html.
[9] Jo, Wooyeon, et al. "Digital Forensic Practices and Methodologies for AI Speaker Ecosystems," Digital Investigation 29 (2019): S80-S93.
[10] Natasha Lomas, "Alexa, does the Echo Dot Kids protect children's privacy?," TechCrunch, 2019.05.09, https://techcrunch.com/2019/05/09/alexa-does-the-echo-dot-kids-protect-childrens-privacy

〈저 자 소 개〉

신 영 훈 (Yeonghun Shin)
학생회원
2019년 : 아주대학교 사이버보안학과 졸업 (학사)
2019년~현재 : 아주대학교 컴퓨터공학과 재학 (통합)
<관심분야> AI 스피커 포렌식, IoT 보안, 파일시스템 포렌식

김 민 주 (Minju Kim)
학생회원
2016년~현재 : 아주대학교 사이버보안학과 재학
<관심분야> 파일시스템 포렌식, IoT 보안, 윈도우 포렌식

정 다 안 (Daan Jeong)
학생회원
2017년~현재 : 아주대학교 사이버보안학과 재학
<관심분야> 파일시스템 포렌식, 윈도우 포렌식, IoT 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> ICS/SCADA, DFIR, Anomaly Detection