

한국정보보호학회 충청지부

제 23회 정기총회 및 정보보호학술논문발표회

2019년 10월 18일 – 19일
대전, 한남대학교(공과대학-9호관)

Organized by

한국정보보호학회 충청지부



대신정보통신(주)



2. 국내 정보보호 연구 경향 분석 - KCI 등재학술지 논문을 중심으로
- 송민경, 김동희, 김소정 (국가보안기술연구소)
3. 타임스탬프 위변조 도구에 의한 안티포렌식 기법에 대한 대응방안(안티-안티포렌식)
- 조규상
4. 블록체인과 Deep Learning을 활용한 악성코드 탐지의 관한 연구
- 최용철, 이덕규 (서원대학교)
5. 블록체인을 활용한 공간공유 시스템에 관한 연구
- 송지훈, 황용운, 이임영 (순천향대학교)
6. 스마트 스피커 환경에서 중간자 공격을 이용한 음원 불법 추출 방안
- 유영웅, 최슬기, 곽진 (아주대학교)
7. 블록체인을 이용한 앱 미터기에서의 요금 산정 기법
- 권용빈, 권혁동, 장경배, 서화정 (한성대학교)
8. 블록체인 확장성 개선을 위한 오프체인과 프라이빗 스마트 컨트랙트 연구
- 김혜빈, 정병규, 신상욱 (부경대학교)
9. 류크 랜섬웨어 동작 과정 분석
- 김의진, 박소희, 정해선, 곽진 (아주대학교)
10. 블록체인 기반 수소차와 수소 충전소 관리
- 심민주, 권혁동, 서화정 (한성대학교)
11. 원전 네트워크 보안성 강화를 위한 광전송설비 보안기술 연구
- 최호영, 김태훈, 이종진, 김성철
12. 실제 분장이 가능한 딥러닝 기반 얼굴인식 모델 기만공격
- 류권상, 최대선 (공주대학교)
13. 4차식 모듈러스 NTT를 이용한 LAC 구현
- 이주엽, 김수리, 홍석희 (고려대학교)
14. QR 코드 기반의 효율적인 이미지 보호 기법 설계
- 김영세, 김건우 (한국전자통신연구원)
15. 국가사이버안보전략의 기술과제 분포 분석
- 유영인, 배선하, 김소정 (국가보안기술연구소)

스마트 스피커 환경에서 중간자 공격을 이용한 음원 불법 추출 방안

유영웅*, 최슬기**, 곽진***

*,***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과 정보보호응용및보증연구실

Illegal Sound Source Extraction Using Man-In-The-Middle Attack in Smart Speaker Environment

Young-Woong You*, Seul-Ki Choi**, Jin Kwak***

*,***Department of Cyber Security, Ajou University.

**ISAA Lab., Department of Computer Engineering, Ajou University.

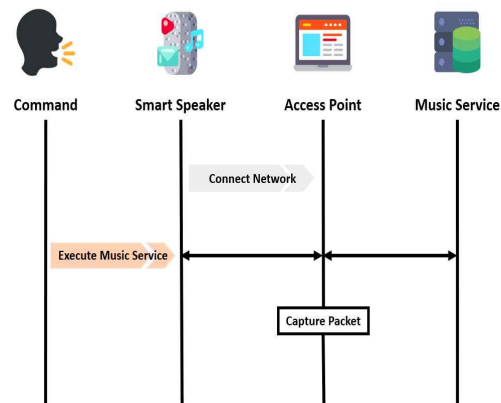
요 약

스마트 스피커는 사용자의 음성을 인식하여 명령을 수행하는 무선 스피커이며, 와이파이(Wi-Fi), 블루투스 등의 무선 통신 프로토콜을 이용한 인터넷 연결을 통해 뉴스, 날씨, 정보 검색, 음악 스트리밍 등의 콘텐츠를 제공한다. 하지만 스마트 스피커가 취약한 인터넷 환경을 이용하고 있을 경우 교환되는 정보가 노출될 수 있다. 본 논문에서는 3종의 스마트 스피커에서 음악 스트리밍 서비스를 수행할 때 중간자 공격을 통해 음원을 추출하는 방안을 서술하고, 이를 통해 안전한 통신 프로토콜 사용의 중요성 및 디지털 저작물의 저작권 보호를 강조한다.

I. 서론

음악 및 라디오 재생, 기기 컨트롤, 알람 설정 등의 기능을 가진 스마트 스피커는 일상생활의 많은 부분에서 이용된다. 하지만 음악, 라디오 등의 디지털 저작물을 이용하는 스피커가 취약한 환경에서 동작할 경우 해당 저작물이 유출될 수 있다. 본 논문의 2장에서는 3종의 스마트 스피커 환경에서 음악 스트리밍 서비스를 이용할 때 중간자 공격을 이용한 음원 추출 방안을 제시하고, 3장에서 안전한 통신 프로토콜 사용의 중요성과 디지털 저작물의 안전한 이용 및 보관을 강조하며 마무리한다.

(그림 1)과 같이 중간자 공격 환경을 구성하였다.



(그림 1) 음원 추출 시나리오

II. 음원 추출

중간자 공격[1]을 이용한 음원 추출을 위해 테더링[2] 기능이 내장된 노트북을 AP로 하여

음원 추출 순서는 다음과 같다.

Step 1. 스마트 스피커의 네트워크 연결
스마트 스피커는 노트북의 테더링 기능을 이용하여 무선 통신 네트워크에 연결한다.

본 연구는 문화체육관광부 및 한국저작권위원회의 2019년도 저작권기술개발사업의 연구결과로 수행되었음.

네트워크에 정상적으로 연결된 스피커에 “노래 들려줘”와 같은 음악 스트리밍 서비스를 실행할 수 있는 명령어를 입력한다.

패킷 캡처 프로그램을 이용해 음악 스트리밍 서비스가 진행 중인 스피커와 해당 서비스를 제공하는 서버 사이의 패킷을 캡처한다.

파일 헤더 검색, 실행 여부 확인을 통해 획득한 패킷에서 음원을 추출 및 실행할 수 있는지 확인한다.

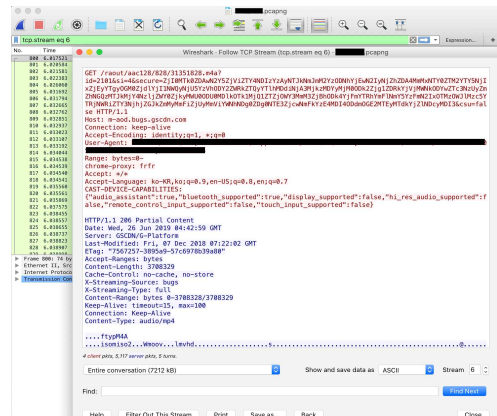
음원 추출이 가능할 경우, 파일 카빙 프로그램 등을 이용하여 해당 패킷으로부터 음원 파일을 추출한다.

파일을 직접 실행하여 정상적으로 재생이 되는지 확인한다.

[표 1] 스피커 별 음원 추출 결과

	A	B	C
음원 추출 여부	X	O	X
음원 실행 여부	X	O	X
패킷 암호화	O	O	O

복사하여 m4a 형식의 새 파일로 저장했고,
정상적으로 음원 파일이 실행되었다.



III. 결론

본 논문에서는 중간자 공격을 활용한 스마트 스피커 환경에서 음원 불법 추출 방안을 서술하였다. 3 종의 스마트 스피커에 대해 해당 공격을 시도해본 결과, 스피커 B가 해당 공격에 취약하였고, 해당 스피커를 제외한 스피커 A, C는 공격에 피해를 받지 않았다. 스피커 B의 경우 http 프로토콜을 이용하여 통신을 수행했기 때문에 패킷 획득 및 파일 추출 과정에서 정상적인 음원 파일을 얻을 수 있었다.

디지털 저작물을 이용할 때 데이터를 보호할 수 없는 통신 방식을 사용할 경우, 저작권을 침해하는 사례가 발생할 수 있다. 저작물에 대한 서비스를 제공하는 제공자는 해당 데이터에 대한 공격과 저작권 침해로부터 안전한 환경을 위해 암호화 프로토콜 사용, 데이터에 대한 저작권 보호 조치 이용 등을 통해 저작권 보호를 위해 노력해야 한다.

[참고문헌]

- [1] 한국정보통신기술협회, “중간자 공격, Man In The Middle attack, MITM”, 한국정보통신기술협회 정보통신용어사전
- [2] 한국정보통신기술협회, “테더링, tethering”, 한국정보통신기술협회 정보통신용어사전