음향 Air-Gap 공격의 최신 동향과 실용성에 대한 연구

조건희 [1], 이연준 [2]
[1] 한양대학교 소프트웨어융합대학 컴퓨터학부 학부생
[2] 한양대학교 컴퓨터공학과 교수
no1gun2@hanyang.ac.kr, yeonjoonlee@hanyang.ac.kr

A Survey on Acoustic Air-Gap Attacks

Gun-Hee Cho[1], Yeonjoon Lee[2]
[1]College of Computing School of Computer Science, Hanyang University ERICA
[2] Department of Computer Science and Engineering, Hanyang University

요 약

본 논문은 에어갭 (물리적 분리된 네트워크 환경) 공격 벡터 중 음향 신호를 중점적으로 다루며, 음향 신호 공격 벡터에 대한 연구 동향과 실제 사용 가능성을 조사한다. 연구 결과, 에어갭 공격은 높은 수준의 스텔스와 무결성이 필요하며, 환경적 제약과 사회적 요소도 고려해야 한다. 또한, 실제 공격에는 다단계 프로세스와 통합된 모듈이 필요하며, 이러한 조건을 충족하는 공격은 제한적일 것으로 보인다. 제한적인 공격이 실제로 가능하더라도, 공격 성공 시 파급력이 크기 때문에, 본 논문은 에어갭 보안에 대한 중요성을 강조하며, 공격을 무력화 할 수 있는 높은 보안 수준을 유지하기 위한 연구와 대응책이 필요함을 강조한다.

1. 서론

컴퓨터 네트워크는 인터넷과 논리적 연결이 없는 경우에 Air-Gap (이하 에어갭)으로 분리된 것으로 간주한다. 이런 조치는 악성 프로그램의 유입이나 정보의 유출을 막기 위해 시행된다. 하지만 높은 수준의 격리에도 해커들은 공급망 공격과 사회 공학과 같은 정교한 공격 벡터를 사용하여 에어갭 네트워크를 손상시킬 수 있다[1].

본 논문에서는 에어갭 공격 벡터 중 음향 신호를 활용하는 공격에 대한 연구 동향을 살펴보고 해당 공격 벡터가 실제 상황에서 쓰이기 위해 필요한 조건들에 대해 논의한다.

2. 배경지식

에어갭이란 네트워크 또는 컴퓨터 시스템을 물리적으로 분리하여 외부 네트워크와의 연결을 차단하는 보안 조치이다. 주요 Air-Gap 공격 벡터는 음향 신호, 전자기파, 광 신호가 있다.

음향 신호를 활용하는 경우에는 에어갭으로 분리된 환경에서 스피커, 마이크를 이용해 음향 신호를 재생, 녹음하여 내부 데이터를 외부로 유출할 수 있다. 전자기파를 활용하는 경우에는 컴퓨터 내부에서 컴퓨터 동작에 따라 다르게 발생되는 전자기파를 활용해 정보를 유출할 수 있다. 마지막으로, 광신호를 활용하는 경우, 광섬유 케이블이나, 레이저, 키보드 LED 등을 활용하여 데이터를 유출한다.

본 연구에서는 위 3 가지 공격 벡터 중 음향 신호를 이용한 공격 방식에 초점을 맞춘다.

3. 음향 벡터의 주요 공격 방식

일반적인 환경에는 스피커와 마이크가 존재하고 해당 스피커를 통해 데이터를 소리 파일로 바꾸어 재생하는 방법이 대표적이며 이러한 경우에는 양방향 통신도 가능하다[2]. 이때 데이터를 이진 신호로 변환하여 직관적으로 데이터를 유출하거나 높은 Hz 를 활용해 은밀성을 강화하기도 한다. 하지만 폐쇄 네트워크 환경에선 보안 정책으로 인해 스피커가 없을 가능성이 높기에 정확한 공격을 수행하기 위해선 스피커가 아닌 다른 하드웨어를 활용해야 한다.

컴퓨터에 CD/DVD 가 있는 경우 드라이버의 모터를 이용해서 데이터를 유출할 수 있다. CD/DVD 드라이버에는 총 2 개의 모터가 있고 각 모터의 역할은 트레이 열기/닫기, CD 읽기/중지이다. 트레이를 열고 닫을 때 나는 소리, 모터가 읽기 작업과 중지 시에 나는 소리, 읽기 과정에서의 RPM 차이라는 총 3 가지 방법이 존재하고 공격자는 각 작업을 조절하여 공격을 진행한다[3]. 하지만 CD/DVD 드라이버의 경우 트레이가 열리고 닫히거나 모터가 돌아가는 물리적 변화를 인간(감시자)이 쉽게 파악할 수 있다는 단점이 존재한다. 따라서 물리적 변화를 쉽게 감지하지 못하고 동시에 폐쇄 네트워크 환경이라 하더라도 필수적으로 존재해야 하는 하드웨어를 이용해 공격을 진행해야 한다. PC 를 구성하는 필수 요소 중 하나인 Power Supply 는 이러한 앞서 말한 2 가지 요소를 모두 만족하는 하드웨어이다. 오늘날의 대부분 PC 에서 사용되는 전원 공급 장치인 SMPS (Switch Mode Power Supplies)에 DC 공급은 스위칭 MOSFET 또는 전원 트랜지스터에 의해 높은 속도로 켜지거나 꺼지는

인버터로 공급되며, 이 스위칭 속도를 조절하여 20kHz~20MHz 사이의 고주파수를 생성한다. 공격자는 이러한 스위칭 속도를 조절하여 고주파수를 생성하는데 이때 생성되는 주파수를 이용하여 데이터를 추출한다[4].

앞선 연구들은 데이터를 추출하는 송신기에 집중한 반면 은밀성을 강화한 수신기에 접근한 연구도 있다. M. Guri et al [5] 연구에서는 스마트폰과 같은 대부분의 전자 장비에 있는 센서 중 하나인 MEMS(Micro Electro Mechanical System) 자이로스코프를 이용한 공격을 제시했다. MEMS 자이로스코프는 장치의 로컬 X, Y, Z 축을 중심으로 회전 속도를 측정하지만 구동축과 감지축의 오정렬이라는 기계 구조적 결함이 존재한다. 이러한 오정렬로 인해 18kHz 이상에서 공진 주파수가 발생하는데 이러한 취약점을 이용하여 내부 데이터를 공진 주파수로 송신하고 수신기(스마트폰)의 마이크가 이를 감지하여 정보를 탈취한다.

이 밖에도 PC Fan, HDD 등의 방법이 있으며 구체적인 성능은 아래 그림 1과 같다.

Type	Medium	Distance (m)	Speed (256 bit)	CO	AV	CD
AC	Speaker acoustic signals [40]	>8 m	High (2–20 s)	High	High	Bi-dir.
AC	PC FAN noise signals [41]	Smartphone: >8 m	Low (1000–2000 s)	High	High	Dir.
AC	HDD noise signals [42]	Smartphone: >2 m	Medium (100–200 s)	High	High	Dir.
AC	PSU noise signals [52]	>2.5 m	High (>5 s)	High	High	Dir.

(그림 1) Air-Gap AC 공격벡터별 특징(AC: Acoustic, CO: Covertness, AV: Availability, CD: Communication Direction)

4. Acoustic Air-Gap 특징과 실용성 측면에서의 한계점

현재까지 연구된 음향 신호 공격의 경우 에어갭 공격 사례가 없고, 은밀성, 무결성 공격 범위 측면에서 한계점이 명확하다.

은밀성. Air-Gap으로 공격은 기본적으로 폐쇄 환경에 침투하여 수행되기 때문에 스텔스 요소가 매우 중요하다. 따라서 인간의 귀로는 들을 수 없는 비가청 대역에서 공격이 수행된다. 하지만 음향 신호를 이용한 공격에서는 스피커의 성능이 20 kHz 까지만 지원하는 경우가 대다수이기 때문에 데이터 전송에 활용 가능한 주파수 대역이 좁아 공격의 실용성이 떨어질 수 있다.

CD/DVD 벡터를 이용한 공격에서는 비가청 영역의 소리뿐 아니라 가청 영역에서의 소리와 함께 트레이 여닫힘, LED 점등 등의 물리적 변화가 발생함으로 공격의 실용성이 떨어지고 사용되는 장치가 어떤 장치인지 미리 알아야 한다는 큰 단점이 있다.

무결성. 최근 연구된 에어갭 공격들은 B-FSK(Binary Frequency Shift Keying) 방식을 이용하여 데이터를 이진 형식으로 인코딩한다. 즉 비트 하나하나의 정확성이 데이터의 내용을 판가름하는데 매우 중요한 역할을 한다. 하지만 볼펜 소리, 코 훌쩍이는 소리 등에 의해 수신기에서 오류가 발생할 수 있으며, 오류가 발생했다 하더라도 송신기와 수신기의 일방향 통신 때문에 송신기가 오류 전송을 알아차리기 어렵다.

범위. 에어갭 환경은 일반적으로 군사 시설, 은행 금고, 국가 보안 시설 등에 채택된다. 따라서 연구자들은 단순히 네트워크만 분리해 놓은 환경을 실제 환경이라고 가장하고 연구를 수행하게 된다. 하지만 이러한 연구들은 환경을 축소화했을 뿐만 아니라 공격의 범위까지 축소했다. 단순한 문자열이나 '01010101'과 같은 단순한 정보를 이용해 공격이 가능하다는 가능성만을 보여준다.

5. 결론

에어갭 공격 벡터 중 음향 신호에 의한 최신 연구 동향을 살펴본 결과, 해당 공격이 실제 환경에서 쓰이기 위해서는 여러 가지 제약과 도전이 존재한다. 먼저, 스텔스와 무결성 측면에서 높은 수준의 정교함이 필요하며, 환경적 제약과 관련된 문제도 극복해야 한다. 게다가, 에어갭 환경에서의 실제 공격은 복잡한 프로세스와 사회적 조사가 필요하며, 데이터 수집, 인코딩, 전송, 기록 삭제, 공격 벡터 변경과 같은 다양한 단계를 포함하는 통합된 모듈이 필요하다.

이러한 이유로, 실제 공격 사례는 매우 제한적일 것으로 예상된다. 그러나 보다 높은 보안 수준을 유지하기 위해 에어갭 환경에서도 주의가 필요하며, 향후에도 이러한 보안 도전 과제에 대한 연구와 대응책 마련이 중요할 것이다.

ACKNOWLEDGEMENT

본 연구는 2023년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음. (2018-0-00192)

6. 참고문헌

[1] Mordechai Guri, CD-LEAK: Leaking Secrets from Audioless Air-Gapped Computers Using Covert Acoustic Signals from CD/DVD Drives, IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid-Spain, 2020, pp. 808-816

[2] Guri, M. Solewicz, Y. Elovici, Y. Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to- speaker communication. In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 10–13 December 2018, pp. 1–8.

[3] M. Guri, "CD-LEAK: Leaking Secrets from Audioless Air-Gapped Computers Using Covert Acoustic Signals from CD/DVD Drives," *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Madrid, Spain, 2020, pp. 808-816

[4] M. Guri, "POWER-SUPPLaY: Leaking Sensitive Data From Air-Gapped, Audio-Gapped Systems by Turning the Power Supplies into Speakers," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 313-330

[5] M. Guri, "GAIROSCOPE: Leaking Data from Air-Gapped Computers to Nearby Smartphones using Speakers-to-Gyro Communication," *2021 18th International Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 2021, pp. 1-10