음향신호 기반 Covert Channel 공격 기술 분석

손우영[1], 권순홍[2], 이종혁[3]
[1]세종대학교 프로토콜공학연구실 학부과정
[2]세종대학교 정보보호학과 & 지능형드론 융합전공 박사과정
[3]세종대학교 정보보호학과 & 지능형드론 융합전공 교수
wooyoung@pel.sejong.ac.kr, soonhong@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

Analysis of Covert Channel Attack Techniques Based on Acoustic Signals

Wooyoung Son[1], Soonhong Kwon[2], Jong-Hyouk Lee[3]
[1]Protocol Engineering Lab., Sejong University
[2]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University
[3]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University

요 약

최근 국가 핵심 기반시설을 중단시키거나 파괴시킴으로서 사회적 혼란 및 국가 경제적 손실을 일으키는 공격 사례가 증가되고 있는 실정이다. 이와 같은 사이버 공격에 대응하기 위해 각 국가는 인터넷이나 다른 네트워크와 물리적 또는 논리적으로 분리되어 있는 폐쇄망 환경을 기반으로 기반시설을 구성함으로서 높은 수준의 보안성과 안정성을 유지하고자 한다. 하지만, 악의적인 공격자들은 Covert Channel을 통해 폐쇄망 환경 내 민감한 데이터 및 기밀 데이터를 탈취하고 있는 실정이다. 이에 본 논문에서는 음향신호 기반 Covert Channel 공격 기술에 대해 분석함으로써 안전한 폐쇄망 환경 구축의 필요성을 보이고자 한다.

1. 서론

2010년 발생한 스턱스넷(Stuxnet) 해킹 사례부터 2021년 발생한 콜로니얼 파이프라인 랜섬웨어 공격까지를 살펴보면, 악의적인 공격자들은 각 국가의 핵심 기반시설을 중단시키거나 파괴시킴으로써 사회적 혼란 및 국가 경제적 손실을 일으키고 있음을 확인할 수 있다. 이에 대응하기 위해 폐쇄망 환경을 기반으로 국가 핵심 기반시설을 구축함으로써 일반적인 IT 시스템과 달리 자유롭고 원활한 데이터 송수신이 수행될 수 없도록 한다. 하지만, 악의적인 공격자들은 폐쇄망 환경에서의 데이터 탈취를 위해 Covert Channel을 활용하여 국가 핵심 기반시설에 침투하고 국가적으로 민감한 데이터 및 기밀 데이터를 탈취하고 있는 실정이다. 이에 본 논문에서는 음향신호에 기반하여 통신이 허용되지 않은 Covert Channel을 활용함으로써 수행될 수 있는 공격 기술에 대한 내용을 분석하여 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 악의적인 사용자가 보안정책을 우회함으로써 정보를 전송하는 경로인 Covert Channel을 분석하며, 3장에서는 음향신호 기반 Covert Channel 공격 기술에 대해 공격 방식을 기반으로 분석한 내용을 제시한다. 4장에서는 본 논문의 결론을 맺는다.

2. Covert Channel

Covert Channel 이란, 데이터를 전송하거나 정보를 유출하는 데 사용할 수 있는 의도치 않는 통신 경로를 말한다. 이는 시스템 내 취약점을 이용해 보안 메커니즘을 우회함으로써 데이터를 비밀리에 전송하는 방법이며, 일반적으로 정보 보안 시스템에서는 해당 공격을 허용하지 않는다.

Covert channel의 유형에는 은닉 타이밍 채널과 은닉 저장 채널이 존재한다. 먼저 은닉 타이밍 채널이란, 공격자가 탈취하고자 하는 데이터의 전송 시간 변화를 이용하여 데이터를 전송하는 것으로, 패킷 간 지연 시간을 조정함으로써 인코딩을 수행하여 데이터를 탈취한다 [1]. 은닉 저장 채널은 메모리의 재사용을 위해 파일 시스템의 남은 공간이나 메모리에 데이터가 저장되는 경우, 해당 데이터가 여전히 메모리에 포함된 상태로 채널을 통해 보안 시스템을 우회함으로써 데이터를 전송하는 방식으로 공격을 수행한다 [2]. 이 외에도 시스템의 환경적 또는 물리적 속성을 활용해 정보를 전송하는 Covert Channel 유형도 존재하며, 이는 시스템의 소음, 온도 변화 및 주파수와 같은 요소를 이용한다.

이와 같이 Covert Channel의 경우, 다양한 공격 시나리오에서 활용될 수 있음에 따라 이에 효과적으로 대응하기 위해서는 상황 별 발생 가능한 Covert Channel 공격에 대해 파악해야 할 필요성이 존재한다.

3. 음향신호 기반 Covert Channel 공격 기술 분석

Covert Channel 공격은 다양한 시나리오에서 발생 가능하며, 특히 비가청 주파수를 활용하는 음향신호 기반 공격 기술의 경우, 보안에 큰 위협을 초래할 수 있다. 이러한 공격은 주변 환경의 소리를 이용하거나 초음파와 같은 비가청 주파수를 사용하여 데이터를 전송함으로써, 전통적인 보안 시스템에서 감지하기 어렵다는 문제점을 지닌다. 이에 따라 본 장에서는 음향신호 기반 Covert Channel 공격 기술을 분석함으로써 안전한 폐쇄망 환경 구축의 필요성을 보이고자 한다.

Guri et al [3]은 스피커와 마이크로폰이 있음을 전제로 하는 음향신호 표준 공격 모델이 산업 현장의 특성에 맞지 않음을 파악하고, 이에 에어갭 환경 내에서 마이크로폰이 없는 PC를 기반으로 하여 초음파를 통해 데이터를 전달할 수 있는 공격 기술인 MOSQUITO를 제시하였다. MOSQUITO 공격 기술의 경우, 유저 레벨에서 실행되는 악성 프로세스가 커널 레벨의 드라이버에 “Retasking requests”라는 요청을 보내고, 해당 요청을 기반으로 악성 프로그램은 오디오 칩을 제어함으로써 음향신호를 통한 데이터 전송이 수행된다. MOSQUITO 공격 기술의 경우, 이와 같은 공격 과정을 수행함에 따라 마이크로폰이 없는 환경에서도 스피커 대 스피커 통신을 통하여 데이터가 전달될 수 있음을 보였다.

Guri et al [4]은 음향신호 기반 Covert Channel을 제거함으로써 안전한 폐쇄망 환경을 구축하기 위해 하드웨어와 스피커가 없는 컴퓨터로 구성된 내부망에 대해서도 음향신호를 기반으로 민감 데이터를 유출할 수 있는 공격 기술인 Fansmitter을 제시하였다. 해당 공격 기술의 경우, CPU 및 섀시 팬에서 방출되는 소음을 음향 데이터 유출의 매개체로 활용함으로써 CPU 및 섀시 팬에서 방출되는 음향 파형을 조절하고 멀웨어가 해당 파형에 대한 정보를 변조하여 수신기로 전송하는 과정을 통해 스피커가 없는 폐쇄망 환경 내 컴퓨터에서도 민감 데이터를 성공적으로 유출할 수 있음을 보였다.

Guri [5]는 에어갭 환경 내 설치되어 있는 PC로부터 데이터를 수집하여 인접한 스마트폰으로 데이터를 전달할 수 있으나, 이는 일반적으로 안드로이드 OS 혹은 iOS의 보안 정책으로 인해 마이크에 접근할 수 없거나 비활성화 및 차단에 이를 수 있음을 언급하였다. 이에 [5]에서는 스마트폰 내에 내장되어 있는 자이로스코프의 특성을 활용하여 데이터를 전달할 수 있는 방식에 대해 제시하였다. 자이로스코프 센서의 특성상 각 센서 별 특정 주파수 대역에 대한 신호를 수신할 시, 이에 대한 미세한 기계적 진동을 발생시킬 수 있다는 특징이 있다. [5]에서는 이에 에어갭 환경에 존재하는 PC의 스피커로부터 초음파 주파수를 파생시켜 데이터를 전달되도록 하였으며, 인접한 스마트폰에서는 자이로스코프의 진동을 식별하여 데이터를 바이너리 정보로 디코딩함으로써 초음파 신호에 인코딩된 정보를 추출할 수 있도록 하여 내부망의 민감 데이터를 획득할 수 있음을 보였다.

4. 결론

본 논문에서는 인터넷이나 다른 네트워크와 물리적 또는 논리적으로 분리된 폐쇄망 환경에서 발생할 수 있는 음향신호 기반 Covert Channel 공격 기술에 대해 분석하였다. 이와 같은 분석 결과는 음향신호 기반 Covert Channel 공격이 다양한 시나리오에서 다양한 매개체를 통해 이루어질 수 있음을 보인다. 이는 안전한 폐쇄망 환경 구축의 필요성을 강조하며, 이에 대응할 수 있는 보안 전략을 수립하고 시스템을 보호하기 위한 효과적인 대응 방안을 도출하는데 기초자료로 사용될 것으로 기대할 수 있다.

Acknowledgement

본 연구는 2023년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(2단계)(UD230020TD)의 지원을 받아 수행되었습니다. 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송혁신인재양성(메타버스융합대학원)사업 연구 결과로 수행되었음(IITP-2023-RS-2023-00254529).

참고문헌

[1] S. Cabuk, et al., “IP covert channel detection,” *ACM Trans. Inf. Syst. Secur.,* vol. 12, no. 4, pp. 1 - 29, 2009.

[2] “Covert storage channel”. [Online]. Available: https://owasp.org/www-community/vulnerabilities/Covert_storage_channel. [Accessed: 2024-04-24].

[3] M. Guri, et al., “Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication,” in *Proc. IEEE Conf. Dependable Secure Comput.*, pp. 1-8, 2018.

[4] M. Guri, et al., “Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers,”arXiv preprint arXiv:1606.05915, 2016.

[5] M. Guri, “Gairoscope: Leaking data from air-gapped computers to nearby smartphones using speakers-to-gyro communication,” in *Proc. 18th Int. Conf. Privacy, Security and Trust (PST)*, pp. 1-10, 2021.