광학신호 기반 은닉 채널 기술 분석

이정민*, 손우영*, 권순홍**, 이종혁**

*세종대학교 프로토콜공학연구실 (학부생)

**정보보호학과 & 지능형드론 융합전공, 세종대학교 (대학원생, 교수)

Analysis of Covert Channel Techniques Based on Optical Signals

Jeongmin Lee*, Wooyoung Son*, Soonhong Kwon**, Jong-Hyouk Lee**

*Protocol Engineering Lab., Sejong University (Undergraduate student)
**Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University (Graduate student, Professor)

요 약

전쟁의 양상이 물리전에서 사이버전으로 변화됨에 따라 지능화된 공격자들은 적국의 기밀 정보를 수집하고, 이를 전략적으로 이용하고자 한다. 이에 대응하기 위해 국내에서는 기밀 정보를 중요도에 따라 분류한 후, 에어갭 환경을 구축하여, 기밀 데이터를 차등적으로 보호하고 있는 실정이다. 하지만, 공격자들은 시스템 보안 정책을 우회하여 에어갭으로 분리된 내부망 내 데이터를 탈취하고자 하며, 이러한 정세에 맞추어 광학, 음향, 전자기파 등 다양한 매체를 활용한 에어갭 공격에 대한 연구가 지속적으로 수행되고 있다. 이에 본 논문에서는 선행연구된 광학신호 기반 은닉 채널 구축 기술에 대한 분석을 수행함으로써 해당 공격을 이해하고, 이에 대응하는 기틀을 마련하는데 기여하고자 한다.

I. 서론

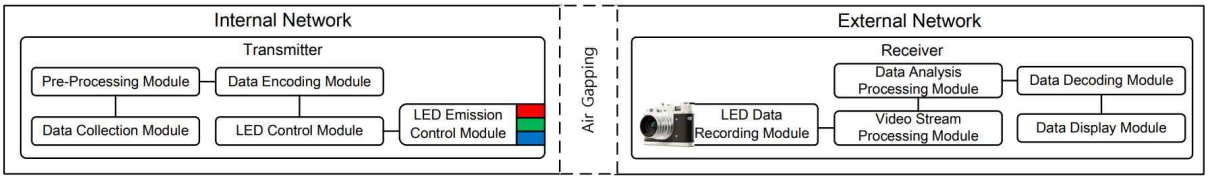
오늘날 기술 발전의 가속화는 국가 간의 패권 경쟁을 사이버 공간으로까지 확장시켜 그 치열함을 더하고 있다. 특히 사이버전의 중요성이 증대됨에 따라, 국가핵심기반시설을 대상으로 하는 사이버 공격과 정보 유출의 위험이 증가하고 있는 실정이다. 이러한 상황에서 공격자들은 기밀 정보를 수집하고, 이를 전략적으로 이용할 수 있다.

국내에서는 기밀 정보를 중요도에 따라 1급, 2급, 3급, 대외비로 분류 및 관리하며, 특히 상위 등급의 기밀 정보를 보호하기 위해서 망분리 기술 중 하나인 에어갭 기술을 기반으로 인터넷망과의 차단을 통해 외부 네트워크로부터의 접근을 차단하고 있다. 이는 외부에서의 무분별한 공격으로부터 방어를 수행할 수 있음을 의미한다. 그러나, 최근 이러한 보안 노력에도 불구하고 최근 에어갭 환경을 우회하여 기밀 정보를 수집하려는 고도화된 사이버 공격이 등장하고 있다. 이와 같은 고도화된 은닉 채널을 통한 정보 탈취 사례가 증가함에 따라 이에 대한 효과적인 방어 대책 마련이 필요한 실정이다. 이에 본 논문에서는 광학신호 기반 은닉 채널 기술을 비교/분석함으로써, 공격 기술의 한계점을 파악하고, 보호 메커니즘을 연구/개발함에 있어 기틀을 제공하고자 한다.

본 논문의 2장에서는 광학신호 기반 은닉 채널이 가지는 특징을 분석하며, 3장에서는 선행 연구된 광학신호 기반 은닉 채널 기술을 비교/분석함으로써 해당 공격 기술의 한계점을 파악한다. 4장에서는 본 논문의 결론을 맺는다.

II. 광학신호 기반 은닉 채널

1973년 Butler W. Lampson이 Covert Channel로 명명한 은닉 채널 대한 개념을 제시한 이래로, 프로토콜 필드에 데이터를 삽입하거나 패킷 타이밍을 통해 인코딩하여 데이터를 전송하는 방식으로 연구가 이루어진 바 있다 [1]. 즉, 은닉 채널은 시스템 보안 정책을 우회하여 두 개체 간 정보를 비밀리에 전송하는 통신 경로로 정의된다.



(그림 1) 광학신호 기반 은닉 채널 구성을 위한 송수신기 구성도

이와 같은 은닉 채널 중, 광학신호를 기반으로 한 은닉 채널의 경우, 직진성, 투과성과 같은 빛의 특성을 활용한다. 공격자는 데스크탑 혹은 공유기의 상태 표시 LED(Light Emitting Diode)와 같은 디바이스를 통해 불빛 및 화면 송출을 수행함으로써 특정 규칙의 가시적 변화를 통해 내부망의 민감 데이터를 송신한다. 수신기에서는 이를 카메라 센서를 통해 수신 및 녹화를 수행하고 분석함으로써 공격자가 물리적 접근이 제한된 환경에서도 은밀하게 기밀 데이터를 수집할 수 있다. 광학신호 기반 은닉채널을 구성하기 위한 송수신기 구성도는 (그림 1)과 같다 [2].

광학신호 기반 은닉 채널 구성 방식의 경우, 밝기 차를 이용하여 모니터 내 QR(Quick Response) 코드를 숨기는 방식, 민감 데이터를 송신하기 위한 상태 표시 LED의 깜빡임이나 밝기 변화를 활용하는 방식이 제시된 바 있다. 이 외에도 최근 광학신호 은닉 채널을 통한 공격의 실효성을 보이기 위해 내부망에서 발생하는 화면 변화를 드론 내 카메라로 녹화하는 방식 또한 제시되고 있는 실정이다.

이와 같이, 최근 다양한 매체 및 화면 변화 방식을 통한 광학신호 기반 은닉 채널이 제시됨에 따라 본 논문에서는 선행 연구된 광학신호 기반 은닉 채널을 활용한 데이터 탈취 공격을 분석함으로써 이를 이해하고 대응하는데 초석을 마련하고자 한다.

III. 선행 연구된 광학신호 기반 은닉 채널 기술 분석

광학신호를 기반으로 한 은닉 채널을 구축하여 데이터를 탈취하고자 할때, 중요하게 고려되어야 하는 성질 중 하나는 은닉성이다. 즉, 광학신호를 기반으로 은닉 채널을 구축하고, 데이터를 탈취하고자 하는 시도를 적국 혹은 상대가 식별 혹은 인지할 수 없어야 함을 의미한다. 이에 광학신호 기반 은닉 채널 기술에 대한 많은 선행 연구/개발에서 은닉성을 보장하기 위한 노력이 이어지고 있음에 따라 본 장에서는 각 공격 기술의 공격 방식에 대해 파악하고 공격 기술 별 한계점에 대해 분석한다.

VisiSploit [3]은 사람의 시각적 한계를 이용하여 육안으로는 보이지 않는 이미지 형태의 정보를 모니터에 투사하는 기법이다. 모니터 디스플레이에 이미지 정보를 숨기기 위해 배경과 유사한 밝기를 이용하여 이미지를 삽입하는 방법과 모니터 주사율을 기반으로 일부 프레임에 이미지를 삽입하는 방법을 함께 사용한다. 해당 연구에서는 정보 전달에 사용되는 이미지 유형으로는 사진, 도면과 같은 이미지 형태의 정보, 텍스트 형태의 정보, 마지막으로 QR 코드 형태의 정보를 사용하였으며, 실험을 통해 QR 코드 형태로 인코딩을 수행하여 정보를 전송하는 방식이 정확도가 높음을 확인하였다. 해당 기법에서는 사용자가 모니터를 주시하며 작업 중인 상황에서도 사용될 수 있는 기법이라는 장점을 갖지만, 주변 조도 환경에 따라 공격이 탐지될 가능성이 변화한다는 한계점을 가진다.

xLED [4]는 이전에 발표된 광학신호 기반 은닉 채널의 경우, 네트워크 장비의 상태 LED를 기반으로 공격을 수행하는 연구가 존재하지 않는다는 점을 언급하며 LAN(Local Area Network) 스위치 및 라우터의 상태 LED를 통해 내부망의 민감 데이터를 유출할 수 있음을 보였다. LED를 통해 데이터가 유출되는 네트워크 스위치 또는 라우터는 펌웨어에 감염된 후, LED가 꺼진 상태를 0, 켜진 상태를 1로 인식하는 변조 방식을 기반으로 변조를 수행한다. 변조의 대상은 내부망 내 민감 데이터를 기반으로 한 비트열이며, 이들은 프리앰블, 페이로드, 체크섬으로 구성된다. 수신기로는 카메라 또는 광센서를 사용하며, 카메라를 수신기로 사용하는 경우, 수신기는 내부망으로부터 전송된 광학신호를 녹화한 후, 해당 비디오를 프레임 단위로 분석하여 내부망의 민감 데이터를 탈취하며, 이때 해당 공격의 성능은 라우터 LED에 대한 카메라의 시야와 가시성에 영향을 받는다. 광센서 수신기의 경우, 송신기로부터 전송된 광학신호를 샘플링하고, 이때, 송신기에서 방출되는 광 신호를 크게 증폭시킴으로써 광 신호가 성공적인 수신이 불가능한 경우, 해당 기능을 통해 더욱 정확한 데이터 탈취를 수행하도록 한다. 수신된 광학신호는 변조

[표 1] 광학신호 기반 은닉 채널 기술 비교

Method	Transmitter	Receiver	Max Distance	Max Bit Rate
VisiSploit [3]	Monitor Display	Camera	8 m	N/A
xLED [4]	Switch/Router Status LED	Camera, Light Sensor	N/A	2000 bit/sec
BRIGHTNESS [5]	Monitor Display	Camera	9 m	10 bit/sec
ETHERLED [6]	NIC	Camera	50 m	100 bit/sec

를 수행한 방식에 따른 복조를 수행함으로써 다시 이진 데이터로 디코딩하여 내부망의 민감 데이터를 획득할 수 있다. 해당 기법의 경우, 스위치 및 라우터의 배치에 영향을 받는다는 한계점이 존재한다.

BRIGHTNESS [5]는 모니터 화면의 밝기를 수정하여 데이터를 전송하는 기법이다. 이는 사람의 시각적 한계를 이용하여 모니터 디스플레이를 통해 정보를 전송한다는 점에서 VisiSploit 기법과 유사하나, 모니터 디스플레이 전체의 밝기를 수정하여 데이터를 전송하는 점에서 VisiSploit 기법과 차별점을 가진다. 해당 기법에서는 모니터 픽셀의 RGB(Red, Green, Blue) 구성 요소를 주어진 양만큼 변경하는 방식으로 데이터를 전송한다. 이에 실험을 통해 RGB 구성 요소 중 R(Red) 요소를 조정하는 것이 최적의 통신 성능을 가진다는 것을 보였다. 해당 기법 또한, 주변 조도 환경에 따라 공격이 탐지될 가능성이 변화한다는 한계점을 가진다.

ETHERLED [6]는 NIC(Network Interface Controller)의 상태 LED를 이용하여 정보를 전송하는 기법이다. NIC는 일반적으로 두 개의 LED를 가지고 있으며, 하나는 색상을 통해 현재 링크 속도를 나타내고 다른 하나는 LED가 켜고 꺼짐을 통해 네트워크 활동을 표시한다. 이러한 LED의 경우 드라이버/펌웨어를 통한 하드웨어 레벨에서의 제어뿐만 아니라, ethtool, netsh 과 같은 도구를 통해 루트/관리자 권한에서 네트워크 설정을 변경함으로써 간접적으로 표시 상태를 변화시킬 수 있다. 해당 연구에서는 각각의 방법들에 대해 구현 및 성능 평가를 수행하였다. 이에 드라이버 및 펌웨어 제어를 통해 LED를 제어하는 방식에서는 초당 약 100비트의 전송률로 데이터 전송을 수행하였으며, 링크 상태를 제어하는 방식에서는 초당 약 2비트, 인터페이스 활성화 여부를 제어하는 방식에서는 초당 1비트의 전송률을 보였다. 해당 기법은 디바이스 제어 수준에 따라 초당 비트 전송률이 큰 차이를 가진다는 한계점이 존재한다.

이처럼 다양한 광학신호 기반 은닉 채널 기술에 대한 연구/개발이 이루어지고 있으며, 각 공격 기술에서의 송수신기 및 주요 성능은 [표 1]을 통해 확인할 수 있다.

IV. 결론

최근 전쟁의 양상이 물리전에서 사이버전으로 변화됨에 따라, 에어갭으로 분리된 환경에서 내부망의 데이터를 탈취하는 것의 중요성이 증가하고 있다. 이에 따라, 광학, 음향, 전자기파 등 다양한 매체를 통한 에어갭 공격에 대한 연구가 지속적으로 수행되고 있다. 이에 본 논문에서는 광학신호 기반 은닉 채널 기술에 대한 분석을 수행함으로써 이에 대응하고자 하였다. 본 연구는 광학신호 기반 은닉 채널 기술의 주요 제한점을 분석하여, 수신기 성능 및 송신기 구성의 영향을 파악하였다. 향후 연구는 다수의 LED를 활용해 더욱 실시간성 있는 전송이 가능한 고속 광학 은닉 채널 구현에 중점을 두어야 할 것이다.

Acknowledgement

본 연구는 2023년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(2단계)(UD230020TD)의 지원을 받아 수행되었습니다.

[참고문헌]

[1] B. W. Lampson, “A note on the confinement problem,” *Communications of the ACM*, vol. 16, no. 10, pp. 613-615, 1973.

[2] J. Lee, et al., “Optical Air-Gap Attacks: Analysis and IoT Threat Implications,” *IEEE Network*, 2024.

[3] M. Guri, et al., “VisiSploit: An optical covert-channel to leak data through an air-gap,” *arXiv preprint* arXiv:1607.03946, 2016.

[4] M. Guri, et al., “xled: Covert data exfiltration from air-gapped networks via switch and router leds,” in Proc. 16th Annual Conf. on Privacy, Security and Trust (PST), pp. 1-12, 2018.

[5] M. Guri, et al., “Brightness: Leaking sensitive data from air-gapped workstations via screen brightness,” in *Proc. 12th CMI Conf. on Cybersecurity and Privacy (CMI)*, pp. 1-6, 2019.

[6] M. Guri, “ETHERLED: sending covert Morse signals from air-gapped devices via network card (NIC) LEDs,” in *Proc. IEEE Int. Conf. on Cyber Security and Resilience (CSR)*, pp. 163-170, 2022.