스크린세이버 기반 은닉 채널: 에어 갭 환경에서의 새로운 정보 유출 공격

정예림[1], 김연진[2], 이일구[3]
[1]성신여자대학교 융합보안공학과 학부생
[2]성신여자대학교 융합보안공학과 석사 과정
[3]성신여자대학교 융합보안공학과 교수
20221130@sungshin.ac.kr, 220246046@sungshin.ac.kr, iglee@sungshin.ac.kr

Screen Saver Covert Channels: A Novel Information Leakage Attack in Air-Gapped Environments

Ye-Rim Jeong[1], Yeon-Jin Kim[1], Il-Gu Lee[1]
[1]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

에어 갭 환경은 물리적으로 시스템을 분리하여 사이버보안을 강화하기 위해 활용된다. 에어 갭 환경의 보안을 실질적으로 강화하기 위해서는 에어 갭 공격에 관한 연구가 필요하다. 본 논문에서는 스크린세이버를 이용한 에어 갭 공격 기법을 제안하고 공격 실현 가능성을 입증한다. 제안 방식은 비눗방울 스크린세이버 외에도 리본, 3차원 텍스트 등 다양한 시각적 요소에 적용 가능하며, 수십 미터에 이르는 전송 범위를 가지고 탐지 회피성이 높다는 장점이 있다. 실험에 따르면 QR 코드를 이용한 공격 방식보다 공격 가능 커버리지가 약 14배 증가했다.

1. 서론

에어 갭 환경은 외부 네트워크와 물리적으로 분리하여 시스템을 보호하며, 이를 통해 외부 침입 및 내부 정보 유출의 위험을 최소화하는 보안 체계이다. 에어 갭은 국가 기반 시설, 군사 시스템 등 고도의 보안이 요구되는 환경에서 사용된다. 그러나 컴퓨터 구성 요소 및 다양한 IoT(Internet of Things) 기기에 의해 생성된 전자기, 광학, 진동 등을 활용한 에어 갭 내부 데이터 유출 공격에 관한 연구가 활발히 진행되고 있다[1]. 이러한 공격은 전통적인 네트워크 기반 방어 체계로는 탐지가 어렵기 때문에, 에어 갭 환경의 보안을 실질적으로 강화하기 위해서 에어 갭 공격에 관한 심층적인 연구가 선행되어야 한다.

Mordechai Guri[2]는 이미지에 QR(Quick Response) 코드를 삽입하는 방식의 에어 갭 공격을 제안하였다. 하지만 스마트폰 카메라로 촬영했을 때 QR 코드 인식 가능 범위가 최대 1m이고, 공격 패턴이 가시적이라는 한계점이 있다. Jeo Loughry[3]는 LED 상태 표시등을 이용한 에어 갭 공격을 제안하였다. 하지만 9m 이상부터 전송이 어려웠다. 이와 같이 광학, 진동 등을 이용한 종래의 공격은 전송 범위 등에 한계가 있다.

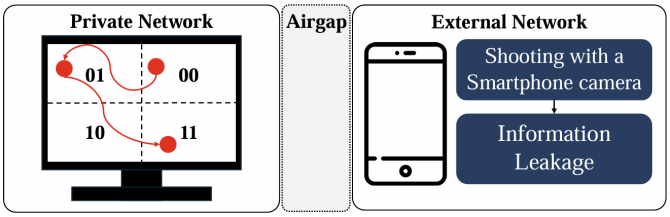
본 논문에서는 종래의 에어 갭 데이터 유출 공격의 한계점을 개선한 스크린세이버 기반의 정보 유출 방식을 제안하고 공격의 효과와 실현 가능성을 입증한다. 화면을 사분면으로 분할하여 각 사분면에 두 개의 비트를 할당한다. 유출 데이터를 이진수로 변환하고, 공격자만 알아볼 수 있는 표식을 각 사분면에 이동하는 것으로 정보를 유출한다. 제안하는 기법은 스크린세이버라는 정상적인 시스템을 이용하여 사용자가 공격으로 인식하기 어려우며, 사용자 부재 시 실행되는 스크린세이버의 특성으로 인해 탐지 회피성이 뛰어나다. 또한 화면 크기에 비례하여 전송 가능 범위가 증가한다.

본 논문의 기여점은 다음과 같다.

- 스크린세이버를 이용한 에어 갭 공격의 메커니즘을 제안한다.
- 화면의 밝기에 따른 에어 갭 공격의 효과와 공격 실현 가능성을 실험적으로 증명한다.

본 논문은 다음과 같이 구성된다. 2장에서는 제안 모델을 설명하고, 3장에서는 실험 결과를 분석한다. 4장에서 결론을 맺는다.

2. 스크린세이버를 활용한 정보 유출 방식

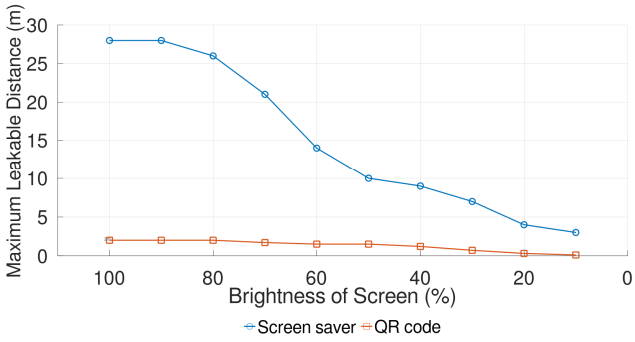


[그림 1] 스크린세이버를 이용한 공격 방식

[그림 1]은 제안 방식의 동작 방법을 보여준다. 먼저, 에어 갭 내부 PC에 멀웨어를 감염시켜 유출하고자 하는 정보를 수집한 뒤, 이를 이진수로 변환한다. 이후, PC의 스크린세이버를 사분면으로 나누고, 각 구역은 00, 01, 10, 11의 2비트 값을 표현하도록 할당한다. 공격이 시작되면 스크린세이버 상의 비눗방울 중 특정 색의 비눗방울이 이진수로 변환된 정보에 따라 해당하는 사분면으로 이동하여 일정 시간 동안 정지하는 동작을 반복한다. 이때 해당 비눗방울은 다른 일반적인 비눗방울과 섞여 동작하므로 사용자는 이상 행동을 인지하기 어렵다. 에어 갭 외부의 공격자는 카메라로 화면 보호기를 촬영 후 비눗방울의 움직임을 분석하여 정보를 복호화한다. 제안 방식은 비눗방울 스크린세이버 외에도 리본, 3차원 텍스트 등 다양한 시각적 요소에 적용 가능하며, 수십 미터에 이르는 전송 범위를 가지며 탐지 회피성이 높다는 장점이 있다.

3. 성능 평가

본 실험은 삼성 갤럭시북4 프로 노트북의 스크린세이버 화면을 갤럭시 s25 카메라를 이용하여 촬영하고 이미지 처리하여 정보를 추출했다. 화면과의 거리를 단계적으로 증가시키며 촬영을 수행했으며, 자동화된 스크립트를 통해 유출 데이터를 복호화하였다. 종래 모델은 유출 데이터를 QR 코드로 생성하여, 가시성을 낮춰 이미지에 삽입하는 에어 갭 공격 방식을 구현하였다. 제안 모델은 파이썬으로 구현한 스크린세이버를 이용하여 정보를 유출하는 공격 방식이다.



[그림 2] 화면 밝기에 따른 최대 유출 가능 거리

[그림 2]는 화면 밝기에 따른 최대 유출 가능 거리를 나타낸다. 제안하는 공격 기법은 유출 가능 거리가 최대 약 28m까지 도달하며 비교적 긴 전송 거리를 보였다. 반면, 종래 연구는 최대 2m로 제한되었다. QR 코드는 고정된 패턴을 사용하고 카메라 기반 인식에 의존하여 조도 변화에 대한 견고성이 낮기 때문이다.

이는 제안 방식이 정보 유출 거리 측면에서 높은 성능을 가지며, 특히 화면 밝기가 확보되었다면 장거리 유출 가능성이 있음을 보여준다.

4. 결론

종래의 에어 갭 공격은 유출 데이터 전송 범위에 한계가 있다. 따라서 본 논문에서는 스크린세이버를 통해 에어 갭 데이터 유출 공격을 수행하는 방법을 제안한다. 실험 결과에 따르면, 제안 기법이 종래 기법보다 최대 유출 가능 거리가 약 14배 증가했다. 특히 화면이 밝다면 장거리에서 데이터를 유출할 수 있었다. 후속 연구에서는 현실적인 테스트베드에서 전송 속도를 개선한 스크린 세이버 기반 은닉 채널 기법을 제안할 계획이다.

ACKNOWLEDGEMENT

본 논문은 2024년도 산업통상자원부 및 한국산업기술진흥원의 산업혁신인재성장지원사업(RS-2024-00415520)과 정보보호핵심원천기술개발사업(RS-2024-00437252)의 연구결과로 수행되었음.

참고문헌

[1] Park, Jangyong, et al. "A survey on air-gap attacks: Fundamentals, transport means, attack scenarios and challenges." Sensors 23.6 (2023): 3215.

[2] Guri, Mordechai. "Optical air-gap exfiltration attack via invisible images." Journal of Information Security and Applications 46 (2019): 222-230.

[3] Loughry, Joe. "(“Oops! Had the silly thing in reverse”)—Optical injection attacks in through LED status indicators." 2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE. IEEE, 2019.