비공개 근거리 무선망을 이용한 공격 시나리오 추출과 예방 및 대응 방안 연구

김도연*, 김용현**, 김동화**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail:rlaehdus2003@gce.sejong.ac.kr

Extraction of attack scenarios using private local wireless networks and a study of their Prevention and countermeasures

Doyeon Kim*, Yonghyun Kim**, Donghwa Kim**, Dongkyoo Shin*, Dongil Shin*
*Dept of Computer Engineering, Se-jong University
**Agency for Defense Development

요 약

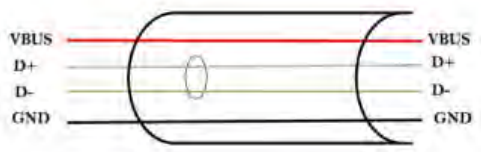
컴퓨터 기술이 발전하면서 현대사회에서의 정보의 중요도와 의존도가 나날이 증가하고 있다. 정보가 중요해진 만큼 해킹 기술도 다양하고 예측하기 어렵게 만들어지면서 정보사회가 위협받고 있다. 이와 관련된 기술을 이스라엘의 벤구리온대학 내의 사이버보안 연구센터에서 연구했다. 2014년에 개발한 Airhopper는 디스플레이 어댑터에서 출력 시 나오는 주파수를 이용해 데이터를 변조해서 휴대폰으로 수신 할 수 있도록 정보를 추출하는 공격이고, 2016년에 개발한 USBee는 USB 2.0 커넥터를 이용한 장비를 통해서 USB 데이터 와이어를 조작해 특정 주파수를 만들어 무선망을 구축하고 데이터를 추출해 내는 공격이다. 본 논문에서는 이 Airhopper와 USBee 기술을 이용한 사이버 공격 시나리오를 추출하고 이에 대한 예방 및 대응 방안을 제시한다.

1. 서론

현대사회가 정보화 시대로 바뀌면서 정보의 중요도와 의존도가 나날이 증가하고 있다. 정보가 중요해진 만큼 해킹 기술도 다양하게 만들어지면서 정보사회를 위협하고 있다. 그에 따른 해결책으로 중요한 데이터를 가지고 있는 PC를 네트워크와는 완전히 분리시켜 사용하는 방법(Air-Gap)이 있다. 하지만 이 해결책 완벽한 방법은 아니다. 이스라엘의 벤구리온대학(Ben-Gurion) 대학의 사이버보안 연구센터에서 내·외부 네트워크와도 완전히 분리되어 있는 PC에서 데이터를 추출 할 수 있는 기술인 Airhopper와 USBee을 개발했다. 본 논문에서는 이 공격기법을 이용한 공격 시나리오를 추출하고 이에 따른 예방 방법과 대응 방안을 제시한다.

2. 관련연구

Airhopper 공격 기법은 이동식 미디어 장치 또는 아웃소싱 된 소프트웨어나 하드웨어를 통해 악성코드에 감염된 PC가 네트워크를 이용해 다른 PC들을 감염시키고 이 프로그램은 해당 PC의 모니터 또는 디스플레이의 어댑터를 조작한다. 어댑터 조작을 통해 디지털 데이터를 오디오 톤으로(Audio tones) 변조하여 청취 가능한 주파수로 보내고 생성된 무선 신호를 휴대폰 FM 수신기로 수신한다. 수신된 FM 오디오는 녹음해서 데이터를 해독하거나 녹음을 공격자에게 보낸다. 공격자는 핸드폰에 미리 설치된 어플을 통해서 실시간으로 컴퓨터의 정보를 읽거나 추출 할 수 있다. 또한 모니터 기능 중 DDC/CI(일정기간 컴퓨터 미사용 시 모니터 절전모드)를 사용하면 송신기는 모니터가 꺼져 있다고 판단하고 송신만 시작 할 수 있다. 그리고



(그림 1) USB data wires,

송신기는 모니터가 절전모드를 종료하고 다시 켜지는 것을 감지는 것과 동시에 전송을 중지한다. 송신기는 이 상태를 지속적으로 폴링(polling)한다 .

USB를 사용한 기존에 해킹기법은 기기에 다른 장치를 덧붙여서 사용하거나 기기를 조작해서 사용하는 방식이였다(Ex. NSA Cottonmouth-I). 하지만 USBee는 USB커넥터를 이용하는 장치를 그대로 사용하기 때문에 기기를 따로 조작하거나 다른 기계를 덧붙이이 않고 침투 할 수 있다.

USBee공격은 USB 2.0 커넥터를 이용하는 장치에 조작된 데이터를 전송한다. 데이터 전송을 할 때 사용되어지는 USB의 데이터 버스 D-, D+의 데이터 와이어를 조작해서 Electromagnetic radiation(EMR) 생성한다. 송신된 데이터는 B-FSK를 사용하여 변조하고, 다시 데이터를 복조하기 위해 fast Fourier transform(FFT)를 사용하여 수신 된 전자기 샘플 신호를 시간영역에서 주파수 영역으로 변환한다. 수신자는 수신자 근처에 있는 무선 안테나로 데이터를 받고 복조를 통해 데이터를 얻는다 [1] [2] [3].

3. 공격 시나리오

다음 시나리오는 에어갭(Air-gap) 컴퓨터 또는 내부망(Intranet)만을 사용하는 컴퓨터에 침입하는 상태를 염두해 두었다.

3.1 Airhopper 공격 시나리오

PC에 침입경로는 두 가지로 제시를 할 수 있다. 외부 소프트웨어를 사용할 경우에 해당 소프트웨어에 미리 Airhopper를 미리 설치해서 은닉해 놓고 피해PC에 옮길 때 같이 따라 옮는 방법이 있다. 또 다른 방법으로는 외부에서 사용하는 PC에 은닉해 있다가 이동식 저장 매체가 연결이 감지가 되면 은닉된 상태로 옮겨서 잠식해 있다가 다른 PC에 연결이 되면 해당 PC에 옮겨 저장하는 방법이다. 간혹 내부망과 외부망을 같이 쓰는 PC가 있는데 이는 Airhopper를 감염시킬 수 있는 좋은 경로 중 하나가 될 것이다.

감염된 후 공격자가 휴대폰에 설치한 Airhopper 앱을 실행하면 PC에 있는 정보를 실시간으로 볼 수도 있고, 탈취할 수 있다. 정보를 빼 올 때는 파일에 이동이 있기 때문에 컴퓨터가 느려지거나 파일의 변경을 볼 수 있기 때문에 모니터가 절전모드로 바뀔 때 은밀하게 실행 할 수 있다. 사용자가 다시 PC를 사용하기 위해 절전모드를 해제하는 순간 모니터 어댑터의 주파수가 바뀌어서 실행이 중단되도록 했기 때문에 전혀 알 수가 없다.

Airhopper는 신호의 의해 거리적 제약이 생기지만(1~7m 이내), 한번에 여러 대에 휴대폰(FM수신기가 있는)으로도 접속이 가능하기 때문에 불특정 다수가 동시 접근 할 수도 있다. 그러기 때문에 거리가 제약적이라고 해도 공격자를 찾기가 쉽지 않다.

3.2 USBee 공격 시나리오

에어갭(Air-gap)컴퓨터나 내부망만을 이용하는 컴퓨터라면 USBee 악성코드에 감염되기 쉽지는 않지만 USB 커넥터를 이용한 장치들의 연결을 통해서는 감염이 될 수 있다. 감염 경로 자체는 Airhopper 공격 시나리오에 침입경로와 일치한다. 다만 다른 점이 있다면 USBee는 USB 커넥터가 연결되어 있어야 정보를 빼올 수 있는 것이고, Airhopper는 모니터가 연결되어 있어야 해킹할 수 있다는 것이다.

감염된 후 PC에서 USB커넥터를 통해 데이터를 옮기는 순간 무선망(특정 주파수)이 생기고, 침입자는 근거리에 있는 자신의 무선 안테나와 노트북을 통해 변조된 데이터를 수신 할 수 있다. 피해 PC가 에어갭(Air-gap)인 상태에 PC라면 공격자가 침투할 것이라고 의심할 만한 표식이 없기 때문에 실질적으로 공격을 식별하기 어렵다. 또한 공격자의 PC와 피해PC가 직접적으로 연결되어 있지 않아 공격자를 물리적으로 식별하기가 힘들다.

4. 예방 및 대응 방안

Airhopper 와 USBee 공격 기법은 아직 초기 단계이기 때문에 더 발전 가능성이 있고, 위험도가 높다. 그리고 악용시 피해 대상이 불특정다수이기 때문에 조기 예방과 그에 따른 대응 방안을 모색 해야 한다.

4.1 Airhopper 공격에 대한 예방 및 대응 방안

Airhopper 공격 기법은 주로 디스플레이 어댑터를 사용하기 때문에 해당 PC들의 디스플레이 어댑터를 차폐가 잘 된 케이블을 이용해서 유효 범위를 최대한 감소시켜야 한다. 차폐된 케이블을 사용한다고 해도 완벽히 차단이 안되기 때문에 물리적 범위를 지정해서 해당 PC를 중심으로 일정 거리 이내에는 휴대용 기기의 접근을 제한해야 한다. 또한 해당 컴퓨터를 사용하지 않을 때는 모니터와 기타 디스플레이 기기를 본체 PC와 분리시켜 보관해야 한다. 그리고 Airhopper를 사용하는 공격자가 은닉상태로 정보를 추출하려고 한다면, 그 시점에 모니터링을 하고 있지 않고는 알기가 쉽지 않기 때문에 데이터의 암호화해서 보호를 해야 한다.

Airhopper에 대한 대응 방안으로는 PC에 원인불명의 데이터가 있거나 기존 데이터가 의도치 않게 수정이 되었다면 해당 데이터를 확인한 다음 PC의 디스플레이 어댑터를 제거하고 컴퓨터를 종료시켜야 한다.

4.2 USBee 공격에 대한 예방 및 대응 방안

USBee 공격은 USB 2.0 커넥터를 이용해서 발생하기 때문에 USB 2.0 커넥터를 쓰는 모든 장비들은 사전에 악성코드 검사를 하고 수상한 파일이 있으면 조사를 해서 제거해야 한다. 그리고 또한 데이터의 암호화를 통해 인가된 사람만 파일을 열 수 있도록 조치를 취해야 한다.

또한 공격자가 접근하기 위해선 물리적으로도 일정거리 내에 있어야 해당 PC에서 정보를 수신 할 수 있기 때문에 일정거리 이내에 전자기기의 휴대를 제한하고, 인가된 사람만 접근 할 수 있도록 해야한다.

5. 결론

본 논문에서 소개한 Airhopper 와 USBee는 기존에 있던 해킹과는 다르기 때문에 이에 대한 공격 가능성도 열어두

고 예방과 대비책을 해야 한다. 지금으로서는 해당 기술들의 개발 방법에 대해서는 공개가 되지 않아 탐지 시스템을 만드는데 제한적이긴 하지만 추후에는 해당 기술들에 대한 탐지 시스템을 연구해야 할 필요가 있다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] Guri, Mordechai, et al. "AirHopper: Bridging the Air-gap between isolated networks and mobile phones using radio frequencies." Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on. IEEE, 2014.

[2] Guri, Mordechai, Matan Monitz, and Yuval Elovici. "USBee: Air-gap Covert-Channel via Electromagnetic Emission from USB." arXiv preprint arXiv:1608.08397 (2016).

[3] Spiegel.de. “COTTONMOUTH-I ANT Product Data.” Accessed 23 Feb. 2017 *http://www.spiegel.de/static/happ/netzwelt/2014/na/v1/pub/img/USB/S3223_COTTONMOUTH-I.jpg*