202334843 이동하

영화 다이하드 4에 등장한 다양한 해킹기법 정리.

1. 신호등 제어를 통한 교통 트래픽 제어

영화에서 해커가 신호등을 제어하는 장면이 나온다.

신호등 시스템의 경우, 아래와 같은 작동구조를 가진다고 한다.

교통 신호등 제어장치의 스위치에서는 일반적으로 브로드 캐스팅을 통해 신호등에게 패킷을 전송하여, 신호등을 제어한다고 한다.

브로드 캐스팅(Broadcasting)이란 네트워크에 연결된 모든 호스트에게 패킷을 전송하는 방식으로, 브로드 캐스팅 패킷은 특정한 목적지가 없으며, 네트워크에 연결된 모든 호스트에게 전송되어야 하는 경우에 사용한다. 이러한 특징을 고려하였을 때, 내가 스위치에 접근 할 수 있다면, 영화에서 등장한 신호등 해킹이 가능하겠다는 생각이 들었다.

수업시간에는 모든 신호등이 초록불로 뜨는 신호는 불가능하며, 이러한 오류 상황에는 점멸등으로 자동 전환된다고 배웠다.

하지만 스위치 자체에 물리적으로 접근할 수 있다면, 또다른 가능성을 확인할 수 있을 것이라 생각한다.

이 사진은 2023년 4월 12일에 촬영된 사진으로, 개별 신호등 내부에서는 논리 검증과정이 없음을 확인할 수 있는 사진이었다. 즉, 외부 제어 신호를 신호등 제어기가 받는 과정에서는 논리 검증과정을 거치기 때문에, 모든 신호등이 초록불로 켜지는 것과 같은 오류가 발생할 수 없겠지만, 스위치 내부에서 임의의 패킷이 신호등으로 전달되었다면 신호등은 그 패킷의 명령대로 동작할 것이다.(적어도 위 신호등 체계에서는 그럴 것이라고 생각된다)

스위치에 해커가 이더넷을 연결하고, 와이어 샤크와 같은 패킷을 스니핑 할 수 있는 툴을 사용하여 각각의 신호등이 동작하는 패킷을 찾아낸다면, 브로드 캐스트로 replay attack 등을 사용하여 신호등을 모두 원하는 상태로 작동시킬 수 있을 것이다.

영화의 경우, 신호등을 현장에서 제어한 것이 아니기 때문에, 사전에 신호제어기 내부 스위치 이더넷 포트에 원격 컴퓨터와 같은 백도어를 설치했을 것이라고 추측한다.

신호등 해킹에 대하여 조금 더 조사해 보았더니, 다양한 자료가 존재하여 읽어보았다.

우선 국내에서는 BOB 4기 멤버 프로젝트로 신호등 해킹 시연을 진행한 것이 있었으며,

이 리포트에서 내가 다룬 내용과는 상이한 관점에서 쓰였지만 <Green Lights Forever: Analyzing the Security of Traffic Infrastructure> 이라는 논문에서도 신호등 해킹에 대해서 다루고 있었다. 신호등 시스템에 대해서 3가지 취약점을 제시하였는데, 다음과 같다.

1. 암호화되지 않은 무선 신호로 인한 네트워크 접근 허용

2. 디폴트 username과 password 사용으로 인한 네트워크 디바이스의 보안 인증 부재

3. 공격하기 쉬운 디버깅 포트

연구 팀에서 신호등 제어기에 들어가는 장비와 같은 장비를 구매하여 실험한 결과, 신호등에서 사용하는 프로토콜과 같은 프로토콜을 사용하였고, 심지어 몇몇 장비는 초기 ID/PS를 사용하여 허무하게 해킹이 되었다고 한다. 또한 명령을 전달할 수 있는 유저에 대한 검증을 거치지 않아서 추가적인 취약점이 발견되었다고 한다.

이 외에도 DEFCON 22 에서 발표된 신호등 해킹시연도 확인해볼 수 있었다.

https://www.youtube.com/watch?v=_j9lELCSZQw

2. CCTV 해킹

영화를 처음 보면서 든 생각은 모든 CCTV가 충분한 보안 장비를 갖추기는 현실적으로 어려우며, 최근 CCTV설치 경향을 보았을 때에는 하나의 장비가 해킹되었을 때, 망을 공유하는 다수의 카메라가 해킹될 수 있다는 문제를 가졌기 때문에, 이러한 해킹이 가능할 것이라는 생각이 들었다. 최근에 CCTV설치, 설계 아르바이트를 하면서 알게 된 것인데, CCTV또한 신호등과 거의 유사한 방법으로 스위치를 두고 이더넷으로 모든 카메라가 스위치로 연결되며, 스위치는 CCTV 녹화, 스트리밍 장비와 함께 연결되어 있는 구조로 구성된다. 여기서 사용되는 스위치는 PoE 스위치로, 이더넷을 통해 전력을 공급할 수 있는 스위치인데 이를 통하여 CCTV에 연결되는 이더넷으로 외부 전원을 대체하고 있다.

이러한 구조의 최대 단점이라고 생각되는 부분이 위에서 언급한 PoE 스위치이다.

PoE 스위치를 거쳐서 외부 네트워크에 연결되는 과정에는 업체가 요구하는 조건에 맞추어 다양한 보안 솔루션이 도입된다. 따라서 일반적으로 외부망을 타고 CCTV에 접근하는 것은 현실에서 발생하기 어렵고, 영화에서 나온 것처럼 지속적으로 모니터링이 가능할 정도로 로그를 안남기는 것은 더더욱 어려울 것이라 생각한다.

하지만 PoE 스위치에 물리적 접근이 가능할 경우에는 로그도 적게 남기면서 CCTV에 접근할 수 있을 것이라고 생각한다. 특히 PoE 스위치는 전력 공급도 가능하여 스위치 이더넷 단자에 소형 컴퓨터를 설치하는 것이 훨씬 용이하다.

이 보고서를 작성하면서 집에 있던 PoE 스위치에 라즈베리파이를 연결하여 추가 전원없이 라즈베리파이가 부팅되는 것을 확인해보았다. (RF 송신 장비도 동작하였다)

3. RF 해킹

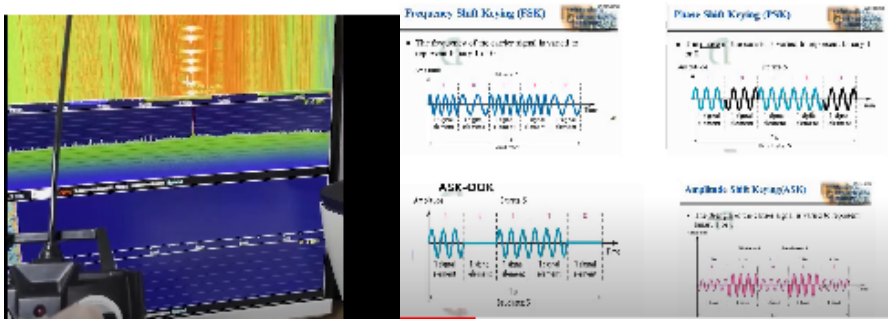
무전을 도청하고 무전에 대신 대답하는 장면이 등장하는데, 이는 간단하게 시연이 가능한 해킹이라고 생각한다.

이를 확인하기 위하여 LimeSDR을 통해 rf신호를 읽어보았고 그 중 무전기 주파수로 확인되는 대역의 신호를 들어보니 집 앞 이마트에서 사용하는 무전기 속 대화내용이 들릴 정도로 무전에 대한 보안이 취약했다. (공개 무전을 청취하는 것은 법적 이슈가 없음)

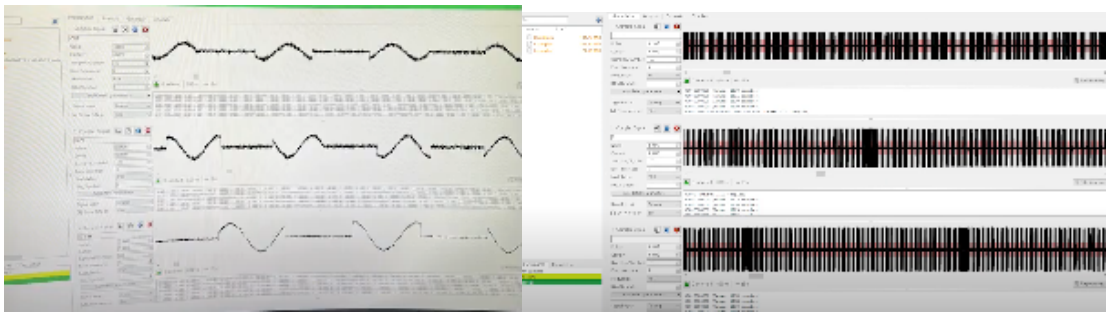
공개 무전으로 암호화가 되어있지 않았기에 가능한 것일수도 있으므로 조금 더 어렵고 합법적인 실험을 찾던 중, rc드론과 rc카를 떠올리게 되었다.

인터넷으로 데이터를 찾아보니 무선통신은 디지털에 비해서 복호화가 간단하다고 한다.

취약한 정도를 알아보기 위해서 아래와 같은 실험을 진행해 보았다.



같은 신호를 반복적으로 보내면서 통신에 사용하는 주파수 대역을 발견하였다.



왼쪽 결과물을 보고 ASK-OOK 암호화라고 생각하였는데, 바이너리로 전환하여 같은 신호를 생성하여도 Replay 어택이 계속하여 실패하는 모습을 보고 몇일 더 조사해보았다.

조사 결과 오른쪽 사진과 같이 FSK방식의 암호화였다. 이를 이진화하여 신호를 따라 만들고 전송하였더니 rc카와 rc드론이 하이재킹되었다. 결과적으로 비행 중이던 rc드론을 원하는 위치에 착륙시킬 수 있게 되었다. 이러한 결과를 통해 rf 통신을 사용하는 무전을 도청하고 대신 응답하는 해킹은 충분히 간단한 방법으로 현실에서 실현 가능하다고 생각한다. (https://www.youtube.com/watch?v=SN1OQZncOd0 : 실제 실험영상)

4. 탄저균 허위 경고

서버에 물리적으로 접근하여 백도어를 설치하고 RCE Exploit 을 실행하였다.

서버에 물리적 접근이 없는 상황에서 rce exploit 을 실현시키는 것은 매우 어렵다.

RCE Exploit 은 백도어를 통해 시스템에 접근한 해커가 원격으로 명령어를 실행할 수 있게 만드는 것인데, 이를 성공시키기 위해서는 시스템 취약점을 이용해야 한다.

주로 웹 어플리케이션의 취약점을 이용하여 공격하는데, 웹 어플리케이션은 사용자의 입력을 받아 처리하기 때문에 입력 값 검증이 충분하지 않으면 해커가 입력 값을 조작하여 취약점을 이용할 수 있기 때문이다.

영화에서 나온 것처럼 백도어를 심는다면 위와 같은 과정도 거치지 않고 익스플로잇이 가능할 것으로 보인다. 아래는 백도어를 통한 rce exploit 과정이다.

윈도우와 칼리 리눅스를 설치하여 가상머신 2 대를 이용하여 실습하였다.

rce 익스플로잇이 발생한 이후에는 서버에서 특정 명령을 실행하는 등의 활동이 가능하므로 탄저균 허위 경고와 같은 작업을 할 수 있다.

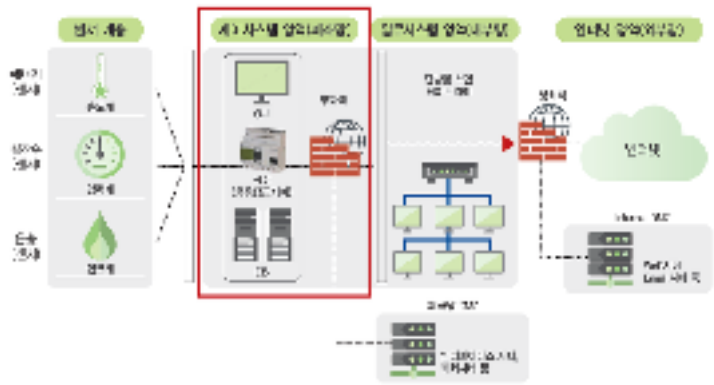
이러한 공격을 대처하기 위해서는 물리적으로 서버실 보안을 증설하는 방법이 있을 것이라고 생각한다.

영화에서는 해킹을 당한 직후에 대처하는 모습이 보이지 않았는데, 현실적으로는 해킹이 감지된 직후에 서버 관리자에게 알림이 전달되면서 대응하는 프로세스가 진행되어야 한다고 생각한다.

5. 기반시설 해킹

영화에서 전기, 가스, 터널 전력 등 다양한 기반시설 해킹을 이용한 사건들이 일어났는데, 이러한 해킹은 SCADA 시스템, PLC 시스템에 밀접한 관련이 있을 것 같아, PLC 프로그래밍과 PCL 해킹에 대해서 많이 조사해보았다.

대부분의 기반시설은 아래와 같은 구조의 네트워크를 가지고 있다고 한다.



(출처 : LG CNS)

일반적으로 PLC 를 제어하여 물리적인 기계 장치를 네트워크로 제어할 수 있는데, 이때 PLC 를 전반적으로 모니터링, 컨트롤하는 중앙 장치가 SCADA 시스템이다.

위 그림과 같이 외부망과 PLC 사이에 여러 방화벽이 존재하며, 망 분리 사업의 결과로 PLC 와 외부 망이 완전히 단절된 케이스도 존재한다고 한다. 따라서 외부에서 PLC 까지 접근하는 것은 현실적으로 매우 어려우며, ISP 등 여러 보안 장치에 의해서 적발될 확률이 높다. 영화에서 나온 것처럼 실질적으로 사건을 일으키기 위해서는 어느정도 해킹이 지속될 수 있어야 하는데, 외부에서 접속하는 방법은 현실적인 방법이 되지 못한다.

하지만 아래와 같은 기사가 나올 정도로 PLC 제어 보안에 대한 취약점이 이론적으로 전혀 존재하지 않는 것은 아니다.

https://www.boannews.com/media/view.asp?idx=57985

<기사내용>

망분리가 '절대적인 방어법'이 아니라는 건 과거에도 익히 증명된 바 있다. 그 유명한 스턱스넷(Stuxnet)은 USB 스틱을 통해 망분리 된 시스템을 공략했다. 그 외에도 여러 대학 연구 기관에서 음파, 라디오 주파수 등을 통해 망분리를 무력화시킬 수 있다는 걸

증명해 발표한 바 있다. 이스라엘의 벤구리온 대학이 이런 방면에서 특히 많은 성과를 거뒀다.

앗치와 라센코가 지멘스 S7-1200 PLC 를 해킹하기 위해 사용한 건 래더 로직(ladder logic) 코드로, 주파수 변조 무선 주파수 신호를 생성하는 것이 핵심이다. 이 주파수는 AM 라디오 주파수 바로 아래에 깔리며, 훔쳐낸 데이터를 인코딩 해서 전송하는 데에 사용될 수도 있다. 네트워크 구조에 관한 데이터에서부터 핵 시설 설계도까지 거의 모든 데이터가 탈취 및 전송 가능하다.

디코딩은 소프트웨어 정의 라디오(Software Defined Radio)와 PC 를 통해 실시할 수 있다. 앗치와 라센코는 "드론을 공격하는 곳 근처로 띄워 이러한 정보들을 수신할 수 있다"고 말한다. "아예 드론에 소프트웨어 정의 라디오와 PC 를 탑재시켜 정보를 수집하는 것 또한 가능합니다."

악성 코드 자체는 PLC 내 스토리지에 입력된다. PLC 를 리부팅해도 시스템 내에 남아 활동을 지속하기 위해서다. "PLC 에는 무선 주파수를 생성하는 기능이 없습니다. 그래서 래더 로직 코드를 심어 인위적으로 무선 주파수를 발생시키는 것이죠. 악성 코드가 기기를 '라디오'로 만들고, 이 라디오 전파를 통해 문건을 훔쳐내는 게 이번 연구로 얻어낸 결과입니다."

무슨 말이냐면, PLC 시스템의 취약점을 익스플로잇하지 않아도 공격이 가능하다는 것이다. 패치가 안 된다는 뜻이기도 하다. "실제 산업 단지에서 PLC 시스템은 크게 보호받지 않아요. 인증 시스템도 없고 있어도 약합니다. 안티 멀웨어 솔루션도 없습니다. 멀웨어 설치하기가 의외로 용이합니다. 그러한 환경이 저희가 익스플로잇 한 취약점이라고 볼 수 있습니다." 그렇다면 멀웨어를 최초에 어떻게 PLC 에 심을 수 있을까? "담당 엔지니어의 랩톱을 훔치거나 USB 를 사용해 접근할 수 있습니다. 소셜 엔지니어링도 효과적인 기법이고요."

위 내용에서 언급된 스턱스넷은 지멘스사의 WinCC/PCS 7 SCADA 제어 소프트웨어인 Step 7 을 감염시켜, WinCC 의 핵심 라이브러리인 s7otbxdx.dll 의 내용을 변경한다. 이후

스턱스넷은 감염된 라이브러리를 통해 WinCC 와 지멘스 PLC 사이의 데이터 통신을 스니핑하여, PLC 를 제어하면서 동시에 WinCC 가 감염된 PLC 의 메모리를 감지하여 스턱스넷을 찾아내는 것을 방해한다.

이 외에도 나는 SCADA 망에 접근할 수 있는 권한을 가진 내부 컴퓨터에 exploit 이 가능하다면 PLC 장치를 해킹할 수 있을 것이라 생각한다. 기업 내부의 컴퓨터이므로 피싱 메일을 사용하여 특정한 직원의 컴퓨터를 해킹할 수도 있을 것이며 내부 컴퓨터에 설치된 프로그램의 취약점, 내부 망에 존재하는 서버의 취약점등을 사용하여 해킹을 시도하면 PLC 장치에 대한 접근 권한을 얻을 수 있는 방법이 다양하게 존재할 것이라고 생각한다.

최근 80 번 포트를 이용한 해킹 방법들이 많아진 만큼, 기존에 포트 별 트래픽을 모니터링하여 해킹을 감지하고 방어하던 장비들이 변화에 맞추어 새로운 방어체제를 구축해야 한다는 생각이 들었다.