ICS 공격 방법에 관한 연구

윤주영*, 이차규**, 최선오*
호남대학교 컴퓨터공학과
e-mail : pulpul8282@naver.com*
jnvr200409@naver.com**
suno@honam.ac.kr*

A Study on ICS Attack Method

Joo-Yeong Yun*, Cha-Gyu Lee**, Sun-Oh Choi *
Dept. of Computer Engineering, Ho-Nam University

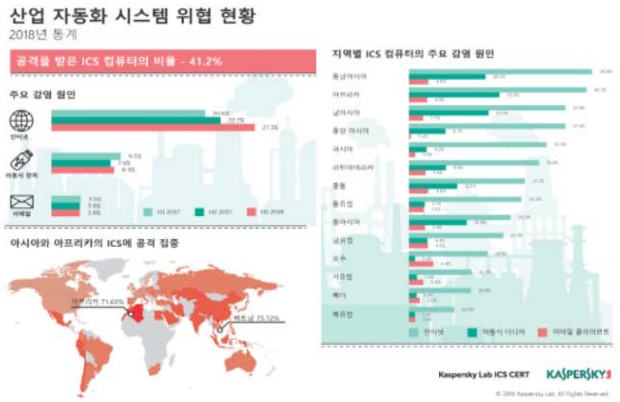
요 약

ICS 해커들의 주요 목적은 재정적 이득, 기업간첩, 테러리스트 활동, 국가간의 사이버전쟁, 잘못된 윤리적 해킹 등의 이유들이 있다. 이에 따른 해킹 경로로는 산업제어 시스템이 공용 인터넷에 노출되는 경우, 기기 초기 설정을 방치, 장기간의 비밀번호 미 변경, 포트스캐닝, 구글 해킹 등이 있다. 이에 따른 대표적인 해킹방식 5 가지가 있는데 첫째, Shodan 을 이용한 일종의 검색해킹, 둘째, ZAP 툴을 이용하여 전수공격을 하는 패스워드 퍼징, 셋째, 목표 사이트의 취약점을 이용하여 인증을 우회하는 공격인 SQL Injection, 넷째, Modbus 툴을 이용한 해당 시설의 전압을 변경하는 네트워크 공격, 다섯째, zbgoodfind 툴을 통한 원격장치공격이 있다.

1. 서론

최근 원자력발전소나 전력망 같은 국가 중요 산업시설들에 대한 사이버 공격이 심각한 수준으로 올라가면서 ICS 보안의 중요성이 대두되고 있다. 기존의 해킹은 내부에서 정보가 유출되는 형태로 되었으나 다양한 해킹툴이 개발되면서 불규칙적인 공격 방식들이 나타나고있다. ICS 해킹의 주요 감염 경로는 1 위 인터넷, 2 위 이동식 장치, 3 위 이메일 순이고 주 공격 대상은 에너지분야 32%, 생산-공정분야 27%, 관리 시스템 18%를 차지하고 있다. 이에 맞게 능동적인 보안 시스템을 갖추기 위해선 유출 경로, 기본적인 공격방식 및 해킹툴의 종류 등 전반적인 내용들을 인지해야한다.

따라서 본 논문은 ICS 공격의 기본적인 방식과 해킹툴의 종류들의 공격방법에 대하여 조사하고, 조사한 내용을 바탕으로 각각의 공격방법 및 해킹툴을 사용하여 직접 공격 실습해보며 보안의 취약점을 발견하고 연구하는 것을 목표로 한다.



(그림 1) 2018 년 산업자동화 시스템 위협 현황 [1]

2. ICS 공격의 위험성

2.1 ICS 공격의 위험성

국가 중요시설 해킹 공격에 성공 시 실질적인 테러와 인명피해로 연결될 가능성이 있다. 또한 산업 컴퓨터에 대한 사이버 공격은 피해 규모가 크고 시스템 전체의 운영을 중단을 발생하여 경제적, 인명적인 피해를입을 수 있다.

발생시기	공격대상	공격 형태 / 피해
2001년	호주 하수처리 시스템	해고된 전 직원이 외부 원격접속을 이용해 시스템 조작. 해양 하수 무단 방출로 인한 피해 발생.
2003년	미국 철도 사내 철도 시스템	사내 정보 시스템이 웜웨어에 감염되어 신호 시스템이 정지됨 6시간에 걸쳐 복구 작업을 진행하는 동안 열차 운행이 중지됨.
2009년	미 병원 HVAC 시스템	청정도, 온도, 습도를 자동 조절하는 시스템이 해킹됨
20010년	이란 나탄즈 핵 시설	원격제어시스템을 타깃으로 하는 악성코드 '스턱스넷'이 발견됨. 스턱스넷은 이란 나탄즈 핵 시설에 침투해 원심분기리를 오작동 하게 만들어 핵무기 개발을 지연시킴
2014년 12월	한국 수력원자력	원전도면이 유출됨.
2016년 3월	서울 코레일 철도교통관제센터	철도 운영기관 직원들을 대상으로 메일 계정과 비밀번호를 빼내려는 피싱 메일이 유포되는 사건이 발생. 철도교통관제 시스템에 사이버 테러를 하기 위한 사전 준비 단계로 해킹을 시도한 것으로 분석
2016년 4월	미 미시간 발전소 수자원 시설	랜섬웨어가 첨부된 이메일을 통한 스피어 피싱 공격이 발생함 내부 내트워크까지 감염이 확산되자 추가 피해 발생을 막기 위해, 회사 시스템을 일시 중단함.
2016년 11월	미 샌프란시스코 시영철도 시스템	결제 시스템 HDD 크립토의 변종인 랜바 랜섬웨어에 감염되어 2천 대 이상의 무인 발급기가 마비됨
2017년 6월	일 혼다 자동차 시야마 공장	워너크라이 랜섬웨어에 감염되어, 약 48시간동안 엔진 생산과 조립이 중단됨.

(그림 3) ICS 주요 공격 형태 및 피해 [2]

3.ICS 공격

3.1 Password Fuzzing

Password Fuzzing 은 툴(Zed Attack Proxy, Burp Suite)을 이용하여 획득한 정보를 바탕으로 무작위 데이터를 대입하거나 분석하여 패스워드를 얻어낼 수 있는 방식이다.

3.2 Zed Attack Proxy(ZAP) [3]

2010 년 시초로 OWASP 에서 진행하는 무료 보안 도구(오픈소스)중 하나이며, 수백명의 국제 자원 봉사자가 적극적으로 관리하는 프로그램으로 웹 앱에 대한 모든 요청과 그로부터 받은 응답을 볼 수 있으며, 퍼저(Fuzzer) 기능과 자동탐색, 수동탐색, 강제탐색 등의 기능을 탑재하고 있다.

3.3 웹 기반공격 종류

웹 기반 공격의 종류는 대표적으로 SQL 인젝션, 크로스 사이트 스크립트, SCRF/XSRF, LFI and RFI 4 가지가 있다.

SQL Injection 은 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격하는 방식이다.

XSS(크로스 사이트 스크립트)는 웹의 사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입하여 공격하는 방식이다.

SCRF / XSRF 는 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 하는 공격하는 방식이다.

LFI and RFI 는 공격자가 악성코드 스크립트를 서버에 전달하여 해당 페이지를 통하여 악성코드가 실행하는 공격하는 방식이고, LFI 파일을 포함시킬 때 해당파일이 공격대상 서버에 위치한다는 점에서 RFI 와 구별된다.

3.4 SQL Injection 공격 [4]

인증 우회를 통한 SQL 인젝션 공격을 말한다. 이 공격의 특징으로는 인증을 우회 할 수 있으며, 공격자가 원하는 SQL 쿼리를 실행할 수 있고, 데이터를 읽어오거나 변경하거나 삭제하는데 사용될 수 있다. 또한 경우에 따라 서버의 파일을 읽고 쓸 수 있으며 시스템 명령을 실행할 수 있다.

SQL Injection 원리로는 SELECT * FROM accounts WHERE username = “ or 1=1; -- ‘” AND password ’ 1234’ ; 의 구분에서 공격자가 username 부분에 or 1=1; --을 입력하여 뒷 부분 AND 부분 부터는 주석처리가 되어 맞지 않는 비밀번호 입력시에도 로그인에 성공할 수 있는 기본적인 공격방법이다.

4. ICS 공격과 물리적 피해 [5]

4.1 제어 서버 공격

공격자는 트래픽을 전송하는 네트워크에 접근 가능하고 제어 트래픽이 암호화 되어있진 않은 경우와 암호화되어 있건 없건 간에 트래픽 송수신 시스템을 제어 할 수 있는 경우에 제어 네트워크 트래픽을 점유하고 분석이 가능하다.

공격자가 통제 트래픽을 점유하면 다음과 같은 분석이 가능해진다. 마지막 제어점, 레지스터 및 코일 매핑(mapping), 제어 시스템의 상태 모니터링, 정상적인 통제에 대한 기록, 인증 토큰 또는 기타 원격 관리 토큰 점유 시도에 대하여 분석이 가능하며, 공격자는 Dos/DDos 공격(시스템 자원 고갈, 전파 장애 및 네트워크 매체 간섭 공격)기술을 사용하여 대상을 공격 준비할 수 있다.

이러한 공격은 매우 쉬우며, 무선의 경우 방어가 거의 불가능하다.

4.2 제어 신호 스푸핑(Spoofing Control Signals)

modbus 와 같은 많은 제어 시스템은 프로토콜을 암호화 기능을 제공하지 않기 때문에 공격자가 수정할 레지스터값을 정확히 알고 있으면 마스터 서버를 컨트롤 할 수 있다.

4.3 네트워크 프로토콜 퍼징(Puzzing Network Protocols)

퍼징은 다양한 트래픽을 처리할 수 있는 응용프로그램의 기능을 테스트 하는 수단이다. 퍼징은 입력을 허용하는 모든 응용 프로그램에서 수행 가능하다. 프로세스 편집기에서 로그파일 열기, Modbus 또는 OPC 패킷 수락이 가능하다.

4.4 네트워크 통신 공격

ModBus-TCP 의 인증과 암호화 기능은 공격에 매우 취약하다. Modbus 장치를 읽는 것 만큼 Modbus 장치를 쉽게 수정 변경이 가능하고, mbtget 툴을 사용하여 쉽게 공격을 할 수 있고 공격자는 Netcat 또는 자신이 만든 스크립트와 같은 툴로도 공격을 할 수 있다. mbtget 툴을 사용하면 정상 작동중인 기기의 전압 조정기를 공격하여 과부화, 과전압을 유도하여 기기를 망가뜨릴 수 있다.

4.5 원격 장치 공격

외부의 침입자가 목표 시스템의 쉘을 얻어내는 것을 기본 목적으로 하는 공격 예로 Format String Bugs, Buffer OverFlow 등이 있다. ICS 통신이 무선으로 전송될 경우 서비스 거부 공격을 받기 쉽고 방어하기가 거의 불가능하다. RF 주파수 또는 호핑 기술이 사용됨과 관계없이 네트워크 점유가 가능해진다.

Dos 공격자는 통신에 사용되는 주파수를 식별하여 해당 주파수에서 잡음을 생성할 수 있다. Wi-Fi 기술 뿐 아니라 ISM 대역 및 마이크로파 주파수에서도 사용가능하다.

4.6 펌웨어 공격

펌웨어는 컴퓨터 시스템이 장착된 거의 모든 기기에 들어있다. 그래픽카드, 임베디드제어장치, USB 마우스, 키보드 등에도 펌웨어가 존재한다.

해커가 펌웨어를 공격하는 이유는 펌웨어가 보안 관심밖에 있기때문에 보안에 취약함을 이용할 수 있고, 공격자는 정적 암호화 키, 암호화 알고리즘 또는 주파수 호핑 알고리즘을 분석 할 수 있다.

원격으로 악용될 수 있는 취약점을 발견하기 위하여 리버스 엔지니어링이 필요하다.

5. 결론

산업 네트워크를 구성하는 시스템의 운영체제, 애플리케이션 소프트웨어, 보안 솔루션을 정기적으로 업데이트 해야하며, 엣지 라우터와 조직의 운영 기술 네트워크에서 사용되는 포트와 프로토콜에 트래픽 제한을 설정해야 한다.

산업 네트워크와 그 경계 ICS 구성 요소에 대한 접근 제어에 감사를 실시해야하며, 시스템의 요소가 인터넷에 처음 접속하게 되는 시스템 통합 초기부터 보안에 주의해야 한다.

제어 시스템과의 통신 일체에 대한 강력한 인증 및 암호화 기능이 갖춰져 있는지 확인하고, 가장 취약한 통신 프로토콜을 파악하고, SCADA 및 IoT 네트워크로 안전하게 통신중인지 확인해야 하며 펌웨어와 물리적 공격에 대한 보안성을 간과해서는 안된다.

참고문헌

[1] 캐스퍼스키랩 새소식 ‘2018 년 상반기 ICS 컴퓨터 중 40% 이상이 악성 코드에 감염’ (출처: http://news.kaspersky.co.kr/news2018/09n/180912.htm)

[2] 중소기업 기술로드맵 전략보고서 03 정보보호 (253 쪽)

[3] OWASP Zed Attack Proxy Project 홈페이지 (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)

[4] 호남대학교 기초해킹교육 및 실습 (2019.05.21~23 KISA 박문범 책임 연구원)

[5] ICS410 ICS/SCADA SECURITY EESSENTIALS 410.2 ICS Attack Surface (Attack on Remote Devices)