산업 제어시스템 네트워크 공격유형 및 보안방법의 연구

채승언, 김봉현, 최선오
호남대학교 컴퓨터공학과
e-mail : eirinlove@gmail.com
kibohy4853@gmail.com
suno@honam.ac.kr

A Study on ICS Network Attack and Security

Seung-Un Chae, Bong-Hyun Kim, Sunoh Choi
Dept. of Computer Engineering, Ho-Nam University

요 약

산업제어 시스템의 네트워크 인프라는 시대가 흐름에 따라 파생되는 많은 공격방법에 대해 보호절차를 지니기 위해 개발되어 왔다. 따라서 산업 제어 시스템은 외부에 사용되는 시스템을 비슷하게 사용하지만 보다 더 독립적인 절차와 장비들을 지니는 경우가 많다. 따라서 실제 이용되는 프로토콜과 보안정책에 대해 연구해보려고 한다.

1. 서론

정보화 산업의 발전에 따라 보안 중심설계가 인프라 구축자들에게 요구되고 있다 주요 기관에 대한 공격으로 인해 기업층의 손실액은 매년 커지는 추세에 있다. 유/무선 통신에서는 단말간 상호작용에서 발생하는 모순과 물리적인 한계점이 존재하여 그에 대한 네트워크 구조에 대한 간접적인 공격행위가 증가될 우려가 있다. 따라서 본 논문에서는 산업 제어 시스템과 외부 시스템의 가용 프로토콜과 시스템의 공통점에 대해 기술하고 그에 대한 취약점과 보안 가능성을 제기하려고 한다.

2. 본론

2.1 MODBUS [1]

모드버스는 마스터-슬레이브의 관계로 나누어진 통신 프로토콜을 말하며 공장 혹은 기기를 자동화하고 제어하는 목적으로 사용되는 PLC(Programmable Logic Controller)와의 통신에 사용된다.

2.2 MODBUS 통신

MODBUS 는 이에 대해 동적인 프로토콜이며 마스터-슬레이브 간의 통신을 전제로 하고 있다. 일반적인 이더넷 통신에서는 네트워크 상에 존재하는 어떤 노드라도 상호간 요청관계가 성립하지만, MODBUS 의 통신 구조에서는 마스터로 설정되는 장비 만이 슬레이브에게 정보의 요청과 읽기, 쓰기가 가능하다.

(그림 1) MODBUS 를 지원하는 게이트웨이 장비 EKI-1242(좌) 와 EKI-5528(우)

2.3 PROFIBUS 통신

산업현장에 있어서 PC 와 PLC 간의 메시지 교환을 위한, 쓰임에 있어서는 MODBUS 와 비슷하지만 PROFIBUS 는 연결되는 노드의 종속관계가 1:1 에서 다:다 관계로 형성된다. PROFIBUS 는 Field Level 로부터 Cell Level 까지의 분산된 디지털 장비를 서로 연결할 수 있도록 직렬 Fieldbus System 의 기술적, 기능적 특징을 지닌다.

.

2.4 유/무선 통신에서의 ICS

모든 ICS 장치 뿐 만 아니라 모든 네트워크 기기는 WAN 혹은 LAN 과 같은 통신 프로토콜에서의 작동을 보장하여야 한다. 제어 시스템에서는 유지 보수, 연결성 등을 위해 통신 인프라의 구축 방향을 결정하며, 유선 연결 방법과 무선 연결 방법을 제공한다. 기존 유선 네트워크의 방향성을 고려하여 선택하는 측면도 있으나, 유선 액세스가 불가능한 원격위치에서 ICS 장비의 보급이 증가함에 따라 ICS 환경에서의 무선통신이 증가하는 추세이다.

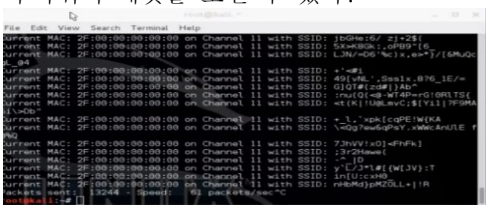
2.6 보안 위협요소

ICS 통신은 많은 가용성 있는 프로토콜을 사용하고, 거기에 따른 장비들로 구성되어 외부 통신시설과 그 형태가 유사하다. 따라서 관리자는 망 내에 있는 송수신 가능한 장비들의 데이터 관리와 장비의 물리적 연결 그리고 인력 등의 관리를 철저히 하여야 할 것이다.

2.7 누킹 (Nuking)

ICS 통신은 때때로 무선 통신에 의존해야 하는 경우가 있다. 이런 경우에 대비되지 않은 시스템에서의 취약점은 항상 발견될 수 있다. 공격자에 대한 누킹 행위는 이런 경우에 ICS 통신에 있어 치명적인 위험을 유발할 수 있다. 하나 혹은 다수의 단말로 하여금 하나의 서버에 트래픽을 흘려보내 서버가 과도한 트래픽 소모 및 프로세스 진행, 과도한 입출력 등을 통해 정상적인 작동을 할 수 없게 만드는 공격방법으로, ICS 네트워크에서의 무선 통신의 경우 접근자가 무선통신의 대역을 이용해 서비스 세트 식별자를

알아내고 무작위의 패킷을 보낼 수 있다.



(그림 2) 다수의 장치로부터 패킷을 보내는 클라이언트

2.8 버퍼 오버플로 (Burffer Overflow)

OS 등의 제어 소프트웨어를 통해 시스템의 메모리 영역으로부터 데이터를 삽입해 인위적인 오버플로 현상을 일으키는 공격으로, [2] 입력 받는 값이 버퍼의 용량 이상으로 증가하게 되면 기존의 데이터가 덮어씌워지거나 일부가 제거되거나 다른 영역으로 이동되는 취약점을 이용한 공격이다.

2.9 하트블리드 (HeartBleed)

버퍼 오버플로 취약점을 이용한 공격으로 OpenSSL 의 TLS 라이브러리 내 취약점을 이용해 서버의 메모리에 액세스 할 수 있도록 한다. 데이터의 양을 검사하는 곳에서 사용자의 단말이 얼마만큼의 데이터를 보냈는지 거짓으로 명시할 경우에 요청에 대한 쿼리를 만족하기 위해 데이터가 포함된 블록의 길이를 모두 보여주기 때문에 발생하는 취약점이다.

2.10 셸 쇼크 (Shell Shock)

유닉스 계열 운영체제의 셸에서 발생하는 보안 취약점으로 배쉬 셸 버그를 악용하여 관리자의 루트권한을 탈취하고 임의의 코드를 실행할 수 있는 공격이다.

셸 쇼크는 OS 의 취약점을 이용한 것이며 최근 실시되는 마이크로 소프트사(MicroSoft)의 윈도우 계열의 OS 에서도 업데이트를 통해 발생하는 경우가 있었다.

2.11 직접 접근 (Direct Access)

모든 시스템 및 네트워크는 노드 간의 통신을 위해

통신 중개소가 위치한다. 이는 네트워크 간의 연결을 위한 중요한 장소이지만 조직들은 이에 대한 보호조치를 크게 취하려 하지 않는다. 따라서 이는 공격자에게 가장 효과적이며, 직접적인 공격방법이 될 수 있다.

2.12 보안 가능성 및 기대사항

언제나 ICS 혹은 기업의 시스템에 공격을 취할 수는 있지만 기관 혹은 기업이 대처를 한다면 무조건적으로 위험하다고 단정지을 수 없다. 보안은 기업의 손실을 줄이고 신뢰성을 확보하기 위한 마무리 단계이며, 유지보수의 시작단계이다.

2.13 방화벽 (Firewall)

미리 정의된 보안정책에 따라 네트워크 트래픽을 모니터링 하고 제어하는 보안 시스템으로, 내부에서 세션을 제어하고 송, 수신되는 패킷을 정의된 규칙에 따라 필터링 하여 접근 허용할 수 있다.

2.14 허니팟 (HoneyPot)

공격자를 유인하기 위해 모조 시스템을 구축하여 공격을 유도하는 방식으로 공격자의 공격행위에 대해 사전에 탐지하고 대응할 수 있는 방법을 마련한다. 이는 곧 제로데이 공격이나 직접적 위험에 속하는 공격 행위에도 효과적으로 대처할 수 있다. 허니팟은 용도에 따라 고 상호작용의 허니팟과 저 상호작용의 허니팟으로 구성되며, 공격자의 행동을 읽어낼 것인지 장기적인 데이터를 수집할 것인지에 대한 용도에 따라 그 쓰임새가 다르다.

2.15 컨트롤러 보호

컨트롤러 보호의 미비는 제어장치의 감염과 PLC 에 대한 공격행위를 유발할 수 있다. 과거 이란의 핵 발전소를 무력화시킨 스턱스 넷에서 그 예시를 들 수 있듯이, 컨트롤러의 취약점은 최근까지도 산업 제어 시스템에 위협을 가하고 있다.

[3] 컨트롤러의 보호 정책으로서, 인증된 사용자만이 USB 를 사용하거나 PLC 를 제어할 수 있게 하는 방법 그리고 계정의 액세스 권한을 만들고 사용자를 제한함으로써 컨트롤러에 대해 간접적인 공격에 대처가 가능한 방법이 있다.

2.16 암호화 (Encrypt)

메시지를 가로채는 사람이 메시지를 이해할 수 없도록 메시지를 왜곡시킨다. 대부분의 암호화 알고리즘은 암호화와 암호 해독이라는 두가지 과정을 거치고, 암호화는 메시지의 의미를 감추는 방식으로 메시지를 코딩한다.

크게 대칭키 암호화 방식과 비대칭키 암호화 방식 해쉬 암호화 방식으로 나뉘며 이는 메시지의 키와 변조방식에 따라 차이를 보인다.

3. 결론

산업 제어 시스템 네트워크는 폐쇄적이면서도 외부의 시스템과 그 특성이 매우 닮아 있으므로 외부에서 사용되는 많은 프로토콜 및 장비나 소프트웨어의 취약점에 대해 같은 위험을 받을 수 있음을 알 수 있다. 따라서 관리자는 외부에서 사용되거나 혹은 문제가 제기될 수 있는 취약점을 면밀히 분석하여 보다 더 안정적인 네트워크 인프라를 구축할 필요성이 있다.

참고문헌

[1] 권태연, Modbus 취약성 분석 및 보안 모델링, 2016

[2] 이구호, 버퍼 오버플로 공격과 방어기술에 대한 분류법, 2008

[3] 주성호, Analysis of Security Weakness and Countermeasure in PLC-based Homenetwork, 전력전자학술대회 논문집, 2006