산업 제어시스템 호스트보안 연구

조진호, 박광철, 최선오
호남대학교 컴퓨터공학과
e-mail : whwlsgh1144@naver.com
arl6204@naver.com
suno@honam.ac.kr

A Study on Host Security for ICS

Jin-ho Cho, Gwang-Cheol Park, Sunoh Choi
* Dept. of Computer Engineering, Ho-Nam University

요 약

오늘날, 우리는 운영체제에 사용할 수 있는 기술과 보안 방어에 초점을 맞추고 있다. 사람이 현장에서 찾아야 하는 가장 일반적인 서버 및 워크스테이션 운영체제에 대한 기본적인 지식을 제공하며 OS 의 주요 특징, 약점, 그리고 기본적인 보안 방어에 대해 이야기 한다.

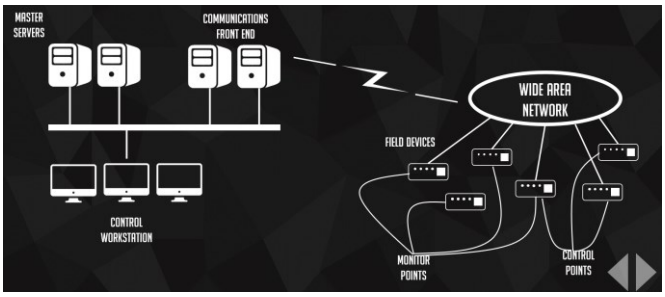
1. 서론

워크스테이션 및 서버 강화 기술은 종종 많은 수의 다른 ICS 시스템에 구현될 수 있다. 대부분의 서버와 워크스테이션의 운영체제는 Microsoft Windows 와 UNIX/Linux 을 사용한다.

2. 본론

2.1 ICS 서버와 워크스테이션

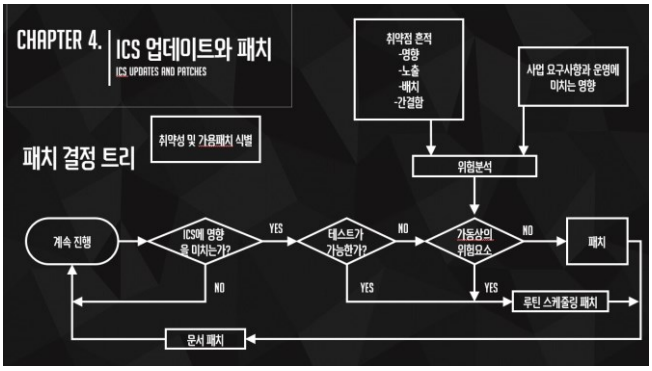
공격자는 ICS 서버와 워크스테이션에 침입하는 방법으로 네트워크 방화벽 제어를 통해 전파하며 서버간 신뢰관계를 이용한다. 그 후 개발사나 엔지니어를 위해 구축된 연결에 원격으로 접속하는데, 원격을 이용한 공격은 공격자 스스로에게 부담이 적기 때문이다. 이것을 표적으로 삼는 이유는 TCP/IP 네트워크가 공격자에게 있어 더 친숙하고, ICS 프로세스를 직접 보고 제어 할 수 있으며, 최고권한의 제어가 가능하다.[1] ICS 소프트웨어는 이러한 공격을 방어하기 위해 필요한 환경구성과 강화가 필요하며 각 개발사의 소프트웨어마다 보안 수준이 서로 다르며, 일반목적의 OS 에서 작동한다. 따라서 OS 의 취약점들이 가장많이 기록되고 악용되며 대표적으로 네트워크로의 입력을 노출한다. 그러므로 OS 가 피해를 받으면 ICS 응용프로그램이 받는것과 같고 피해가 발생하지 않도록 보호해야한다.[2]



(그림 1. 서버와 워크스테이션 분포도)

2.2 ICS 업데이트와 패치

제어 프로세스를 실행하는 워크스테이션 및 서버는 시스템 업데이트 시 보안에 취약 할 수 있다. 또한 ICS 시스템은 시스템내부의 시스템인 경우가 많으며 패치를 진행하는 것은 상호 의존적인 시스템에 문제를 일으킬 수 있다. 허나 패치의 문제점으로 긴급, 잠재적 충돌 및 결과와 위험 분석을 수행해야 하며, 운영 관리에 따라 패치를 승인하고 예약하는 경우가 자주 발생한다.



(그림 2. 패치 결정 트리)

2.3 자동화 및 감사

그래픽 도구로 수행 할 수 있는 작업의 95%는 명령줄 또는 자체 스크립트로 수행 할 수 있다. Windows 및 UNIX/Linux 모두 `자동화 기능을 제공하며 방대한 양의 검사 데이터를 추출 할수 있는데, 지원 도구, 리소스 키트, 타사 도구, 스크립트, 작업 스케줄러과와 같은 도구로 추출 가능하다.

2.4 엔드포인트 보안

응용프로그램 화이트리스팅은 애플리케이션에 대해 암호화/해시 바이너리를 실행하기 전 확인할 수 있으며, 시스템에서 멀웨어가 실행되지 않도록 지원한다. Windows에는 AppLocker 형식의 기본 기능이 제공된다. 많은 타사 솔루션도 추가 기능 및 관리 기능에 사용할 수 있다.
응용프로그램 샌드박싱은 실행 프로세스를 특정 OS 상호작용으로 제한하도록 지원한다.
Windows(Home/Pro 제외)는 AppLocker 에서 기본 기능을 제공한다. Linux는 배포에 따라 SELinux, AppArmor, GRSecurity 등 세 가지의 강력한 솔루션이 내장되어있다.[3]

2.5 로그 관리

모든 Windows 시스템은 최소 응용프로그램, 보안, 시스템 3가지의 이벤트로그가 있다. 이벤트뷰어에서 이러한 로그들을 볼 수 있으며, 도메인 컨트롤러의 경우, 디렉토리 서비스와 파일복제서비스의 로그 또한 존재, DNS가 설치되어 있다면 DNS서버 로그 또한 존재한다. 개체감사를 위한 2가지 단계로는 우선 개체 접근 감사 정책을 활성화하고 개체 환경설정하는 것이 있다. NTFS 파일/폴더, 레지스트리 키, 프린터로 접근을 감사하는 것은 두 단계의 과정이 필요하다. 먼저 개체접근감사를 활성화하고 원하는 개별 파일과 폴더 키의 SACL로 접근한다.[4] 하나의 개체의 SACL은 정확히 어떤 유저나 그룹이 개체와 상호 작용 되는지 정의한다. 더 나아가, 어떤 상호작용이 기록되는지도 설정할 수 있다.

2.6 데이터베이스와 이력 장치

데이터베이스는 ICS를 보호할 때 고려할만한 큰 응용프로그램 카테고리이다. 몇몇 데이터베이스는 다른 ICS 아키텍쳐와 솔루션에서 볼 수 있으며, 대부분 ICS 솔루션들은 구성 요소와 프로세스들의 환경 구축을 보조하기 위해 엔지니어링 워크스테이션내부의 데이터베이스를 사용한다. 이력장치들은 네트워크 신뢰경계를 넘고 덜 신뢰되는 기업 네트워크에 존재하면서 공격분석으로부터 특수하게 호출될 수 있다. 공격자가 방화벽을 통해서 보호, 고립된 제어 네트워크를 공격 시도 하는 대신 비즈니스 네트워크의 이력장치 서버를 공격하고 이용한다. 공격자가 접근한 후, 비즈니스 네트워크 이력장치 서버와 고립된 네트워크의 연결 채널에 코드를 주입하여 제어 시스템 네트워크를 제어할 수 있게 된다. 제어 환경 접근을 통해 운용의 가용성, 온전성 모두에 부정적인 영향을 줄 수 있다.

3. 결론

워크스테이션, 운영체제에 관한 제어 네트워크는 모든 곳에서 찾을 수 있다. 마스터 서버의 대부분은 소수의 중앙 집중화된 위치에 있을 수 있고 대부분의 필드 네트워크 의 원격 스테이션에 배치된 중간서버를 찾을 수 있는데, 이 모든 시스템은 공격을 받을 수있고, 이것에 대한 보안 방어선을 보완할 때 고려해야 한다. 호스트는 대개 가장 많은 수의 장치와 프로세스를 제어하기 때문에 조직에 가장 큰 위험을 제시한다.

참고문헌

[1] LG CNS, ICS 보안에 대한 이해와 약점, 대응방안 2018

[2] 유성민, ICS 보안의 출발점 'OT 관리' 2019

[3] Vivek Gite, Linux Kernel Security (SELinux vs AppArmor vs Grsecurity)

[4] Daniel Ulrichs , ACL, DACL, SACL and the ACE