스카다(SCADA) 보안

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

목 차

- 스카다 시스템 개념
- 스카다 시스템의 위협과 취약점
- 스카다 시스템의 침해 사례 및 동향
- 스카다 공격 시뮬레이션

스카다 시스템 개념

❖ 산업제어시스템 (ICS : Industrial Control System)

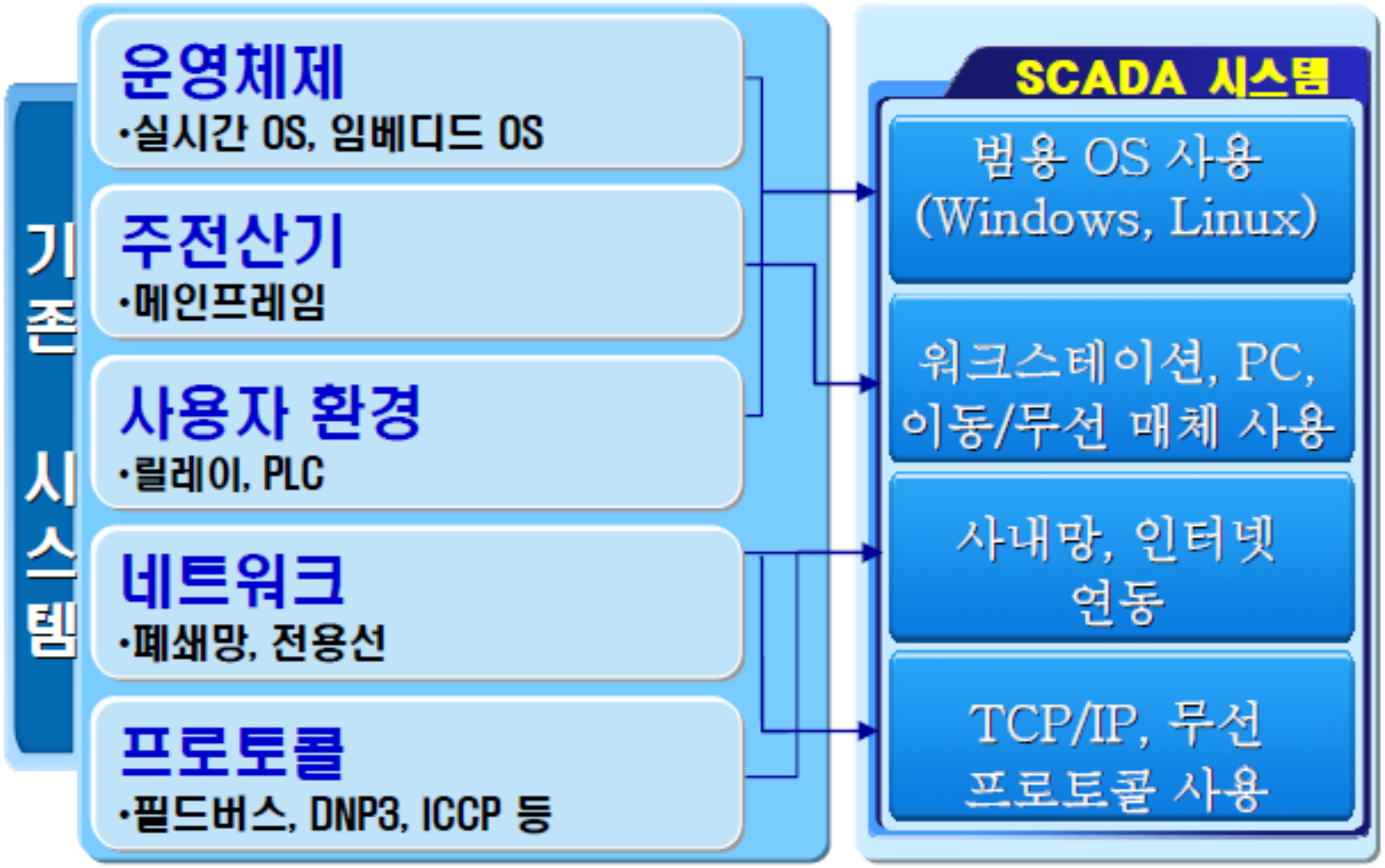
전력, 가스, 에너지 설비, 철도 산업 등 대규모 산업 플랜트를 운영하는 핵심 시스템

❖ 대표적으로 SCADA (Supervisory Control And Data Acquisition) 시스템이 있음

- SCADA 시스템은 1960년대 원격지의 시스템을 효과적으로 감시하고 제어하기 위하여 사용되기 시작
- 장치마다 상호 또는 외부 기기와 연결하여 각각의 장치에 대한 원격 접근과 제어 가능
- 여러 명령 및 조작이 가능하도록 양방향 통신 서비스 환경 구축

스카다 시스템 개념

❖ 스카다 시스템의 발전



스카다 시스템의 위협과 취약점 (1/2)

❖ 스카다 시스템의 위협 요인

- 표준화 : 제어시스템의 연결을 위하여 표준 프로토콜 사용 확대
- 사이버 테러 : 해킹 도구의 광범위한 보급, 사이버 절도, 습관적 해킹
- 정보전 : 테러리즘 및 정보전쟁 등의 확대, 컴퓨터 활용인구의 급속한 증대
- 관리부재 : 기업 합병, 다운사이징, 합리화, 자동화, 비용 절감 등의 압력 증대로 전·현직 종업원의 불만 확대
- 원격접속 : 전화나 인터넷 등 공공통신서비스를 이용한 원격접속 증대

스카다 시스템의 위협과 취약점 (2/2)

❖ 스카다 시스템의 취약점

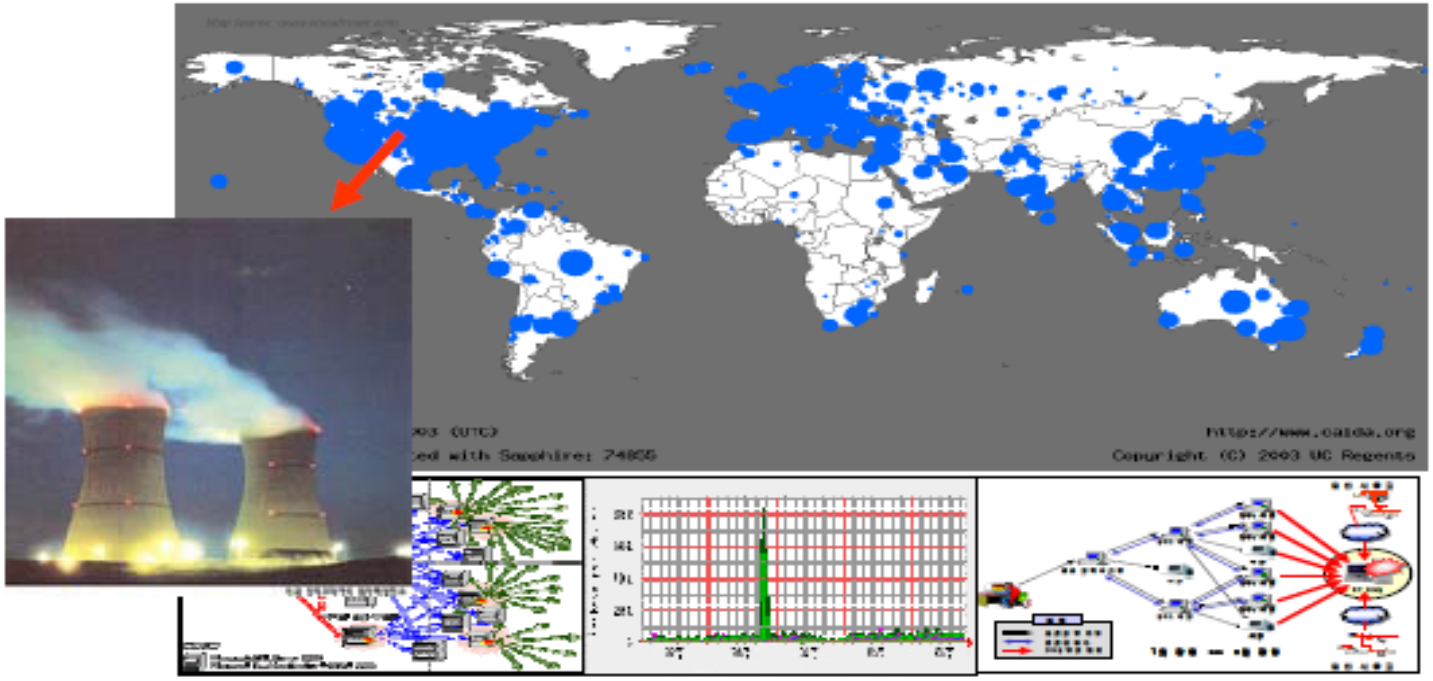
- 폐쇄 망으로 운영되어 정보보호시스템 미 구축
- 업데이트 및 보안 패치 미비
- 생산공정을 중단 후 보안시스템 설치 불가
- 다양한 운영체제 및 프로토콜로 인한 취약점 산재
- 수많은 버그((bug))의 존재
- 간단한 공정 제어 정보의 유통
- 관리자의 보안의식 능력 부족

스카다 시스템의 침해 사례 및 동향 (1/6)

❖ 스카다 시스템 침해 사례

1. 슬래머 웜 - 1.25 인터넷 침해 사고

2003년 SQL 슬래머 웜이 미국 오하이오에 위치한 Davis-Besse 원자력발전소의 감시계통 컴퓨터에 감염됨
관련 설비의 작동이 5시간 이상 불능 상태로 유지되었으며, 여타 발전소 제어망 통신에도 영향을 미친 것으로 보고됨



스카다 시스템의 침해 사례 및 동향 (2/6)

2. 하수처리시스템 제어권 탈취사고

- 2000년 호주의 퀸즈랜드에서 발생한 사고
- 회사에 불만을 가진 전직 직원이 하수처리시스템의 제어권을 탈취하여 수백만 리터의 처리되지 않은 오/폐수를 인근 공원 및 강으로 방류한 사건으로 분류됨
- 사고를 일으킨 전직 직원은 본인의 노트북에 회사의 소프트웨어를 설치하고, 회사의 통신망에 최소한 46번 이상 무단 침입하여 하수처리시스템의 제어권을 탈취함

3. CSX 기차신호시스템 사고

- 2003년 플로리다 잭슨빌에 위치한 CSX*사의 컴퓨터시스템의 바이러스감염
- Sobig 컴퓨터바이러스가 기차신호시스템을 정지시키는 원인이 되었다.
- 이로 인해 신호 및 급전 등의 이상으로 기차운행중단 및 지연됨

*(철도업체 Seaboard Coast Line Industries X 철도운송업체 Chessie System)

스카다 시스템의 침해 사례 및 동향 (3/6)

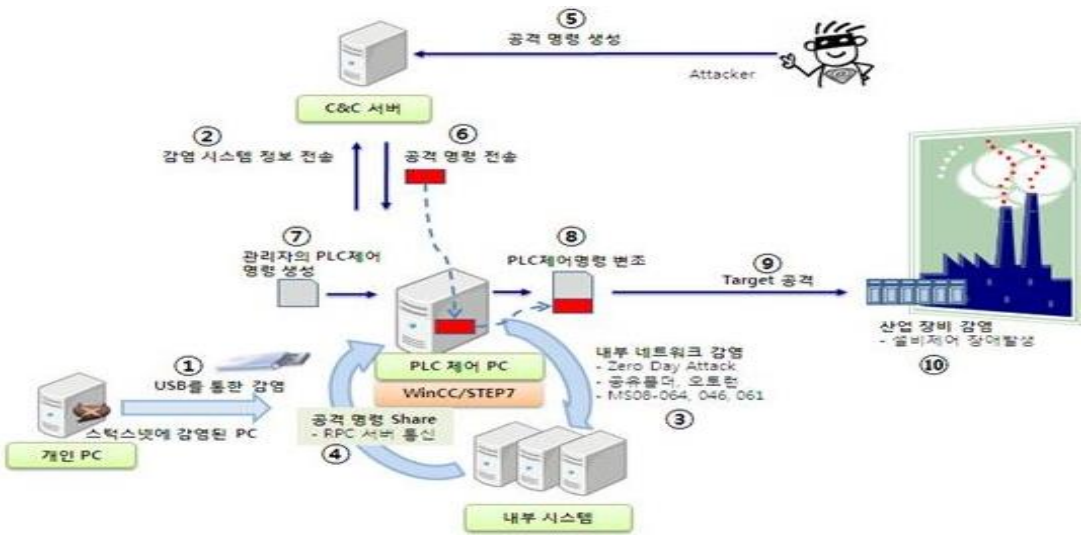
4. Browns Ferry 원자력발전소 정지사고

- 2006년 미국 Alabama 주에 위치한 이 발전소는 두 개의 원자로 재순환 펌프의 고장으로 수동 정지되는 사고가 발생함
- 발전소컴퓨터시스템 네트워크에 연결된 이중의 PLC에 의해 작동되도록 설계된 재순환펌프의 VFD (variable frequency drive) 제어기가 반응하지 않음
- 조사결과, 발전소컴퓨터시스템 네트워크의 과도한 트래픽으로 기인된 사고로 분석되었으나, PLC 자체의 고장인지, 아니면 과도한 네트워크 트래픽으로 인한 VFD 제어기의 미 반응 결과인지에 대한 확인은 이루어지지 않았음
- 이는 확인되지 않은 네트워크의 취약점으로 인한 정지사고로 추측할 수 있음

스카다 시스템의 침해 사례 및 동향 (4/6)

5. Stuxnet

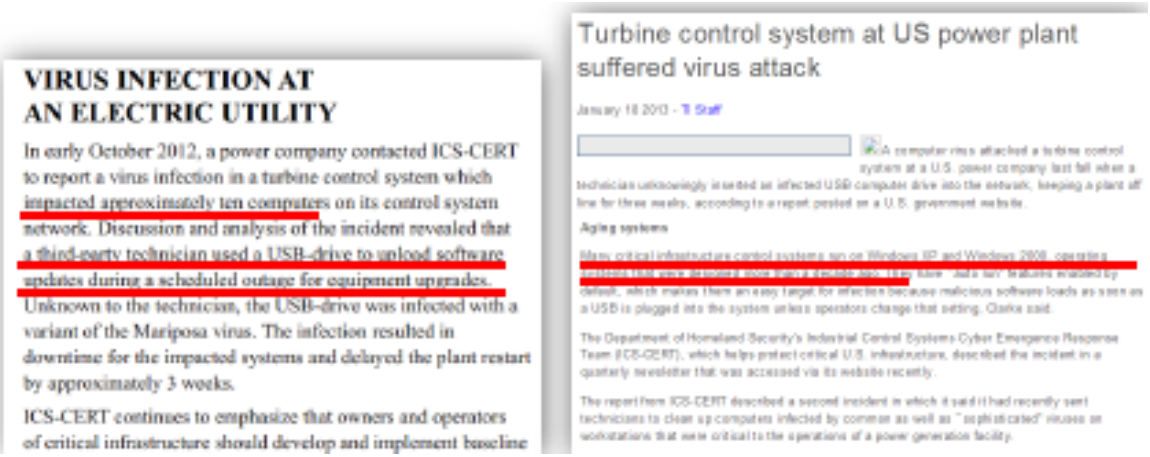
- 2010년 6월에 컴퓨터 보안회사 VirusBlokAda에 의해 처음 발견, 코드 내에 Stuxnet라는 키워드가 다수 등장하여 Stuxnet이라 명명함
- Stuxnet은 Microsoft Windows와 SCADA 시스템 중 지멘스(Siemens)사의 SIMATIC PCS7, S7 PLC 시스템을 공격하도록 설계함
- 무작위로 전염되지만, 감염된 컴퓨터에서 지멘스 소프트웨어를 발견하지 못하면 휴면 상태로 전환.
- 2010년 6월24일에는 자기 자신을 삭제하는 안전장치를 포함
- 목표는 전세계에서 Stuxnet에 감염된 PC중 60%가 소재한 이란이고, 나탄즈 우라늄 농축시설 또는 부셰르 원자력 발전소가 공격 대상이라고 추측함
- 실제로, 기술적인 문제로 인해 농축시설이 여러 차례 정지 되었고, 이로 인해 핵 농축 원심분리기가 파괴되어 숫자가 줄었음



스카다 시스템의 침해 사례 및 동향 (5/6)

6. 터빈 제어 시스템 바이러스 감염

- ICS-CERT, 2012년 10월, 약 10대 컴퓨터 감염, 약 3주간 발전소 운영 지연문제 발생함
- USB를 통한 폐쇄망 바이러스 전이 : 대부분의 기간시설에서는 구식 운영체제(Windows XP, 2000) 사용, USB 자동실행 기능이 기본 설정, 인터넷 망에서 감염된 USB의 자동실행 기능을 통한 폐쇄 망으로의 바이러스 전이 위험 존재함



VIRUS INFECTION AT AN ELECTRIC UTILITY

In early October 2012, a power company contacted ICS-CERT to report a virus infection in a turbine control system which impacted approximately ten computers on its control system network. Discussion and analysis of the incident revealed that a third-party technician used a USB-drive to upload software updates during a scheduled outage for equipment upgrades. Unknown to the technician, the USB-drive was infected with a variant of the Mariposa virus. The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately 3 weeks.

ICS-CERT continues to emphasize that owners and operators of critical infrastructure should develop and implement baseline

Turbine control system at US power plant suffered virus attack

January 18 2013 - IT Staff

A computer virus attached a turbine control system at a U.S. power company last fall when a technician unknowingly inserted an infected USB computer drive into the network, keeping a plant off line for three weeks, according to a report posted on a U.S. government website.

Aging systems

Many critical infrastructure control systems run on Windows XP and Windows 2000, operating systems that were developed more than a decade ago. They have "auto run" features enabled by default, which makes them an easy target for infection because malicious software loads as soon as a USB is plugged into the system unless operators change that setting, Clarke said.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which helps protect critical U.S. infrastructure, described the incident in a quarterly newsletter that was accessed via its website recently.

The report from ICS-CERT described a second incident in which it said it had recently sent technicians to clean up computers infected by common as well as "sophisticated" viruses on workstations that were critical to the operations of a power generation facility.

스카다 시스템의 침해 사례 및 동향 (6/6)

7. 한수원 해킹

스카다 공격 시뮬레이션

Reference

[1] http://www.nshc.net/wp/

[2] 건국대학교, Special Topic in Software Engineering - Cyber Security

[3] 국가보안기술연구소, 주요 제어시설의 사이버 보안 동

[4] 원자력안전규제 정보회의, 국내 원자력 시설 사이버보안 기술개발 및 적용 현황

[5] http://www.energy-news.co.kr/news/articleView.html?idxno=33814

[6] 한국수력원자력

Q & A