KISA 한국인터넷진흥원

스마트공장 보안리빙랩

보안성 시험지원 환경

1. 보안리빙랩 소개
2. 보안 취약점 점검 도구
3. 스마트공장 보안 위협 시연
4. 보안 취약점 점검 도구 시연

1 스마트공장 보안리빙랩 소개

보안리빙랩 개요

- ✓ 스마트공장 설비, 솔루션의 신규 보안위협 발굴과 보안테스트 수행 지원
- ✓ 실제 공정 환경과 유사하게 구현한 유・무선 보안성 시험 지원 환경
  - 특정 제조사에 국한되지 않은 다양한 제품의 보안 취약점 점검
  - 다양한 산업제어 프로토콜에 대한 취약점 점검 및 모의 침투
  - 발견된 취약점이 타 제품에 미치는 영향도 파악
- ✓ 보안취약점 점검 범위를 보다 광범위하게 넓힘

※ 유·무선 통신 스마트공장 공정 환경(음료 제조, 반도체 제조)

이용자 시험 환경

보안 취약점 점검 및 모의 침투 도구

1 스마트공장 보안리빙랩 소개

유선 통신 – 음료제조 공정

- ✓ 음료 제조 공정을 4단계로 구성
- ✓ 4단계 공정 과장

  1) 블랜딩 → 2) 캐핑 → 3) 라벨링 → 4) 패키징
- ✓ 고정 Wall : 1) 블랜딩 → 2) 캐핑
- ✓ 로봇 2대 : 3) 라벨링 → 4) 패키징

스마트공장 보안리빙랩 소개

유선 통신 – 고정 Wall (블랜딩, 캐핑)

✓ 국내외 표준을 고려, 스마트공장을 대표하는 구성요소와 장비로 표현

- Level 0 (공정부) : 센서,모터,액츄에이터,카운터
- Level 1 (제어부) : 지멘스, 미쓰비씨, LS 산전 3종 PLC
- Level 2 (공정모니터부) : 생산공정 전반을 모니터링

HMI (블랜딩,캐핑) / HMI (라벨링, 패키징)

※ 각 종류별 통신 방식 선택 가능 (PLC 하단 버튼)

스마트공장 보안리빙랩 소개

유선 통신 – 6축 다관절 로봇, 스카라 로봇

✓ 6축 다관절 로봇 (라벨링)

✓ 스카라 로봇 (패키징)

스마트공장 보안리빙랩 소개

유선 통신 – 이용자 시험 탈부착 Wall

- ✓ 이용자 PLC, HMI를 탈부착 시켜 제조 공정 환경에 연동시키기 위한 Wall
- ✓ 탈착된 PLC, HMI를 연계하여 작동 할 수 있도록 구현 (RTU 하단의 버튼)
- ✓ 지멘스, 미쓰비씨, LS 산전 3종의 PLC와 HMI를 탈부착 할 수 있도록 지원

1 스마트공장 보안리빙랩 소개

무선 통신– 고정 Wall (웨이퍼, 포토 공정)

- ✓ 반도체 제조 공정
- ✓ 공정 과정 :

  1)웨이퍼 공정: 잉곳을 만들고 절단하여 웨이퍼를 만드는 공정

  2)포토 공정 : 웨이퍼에 반도체 회로 패턴을 만드는 공정

- ✓ Level별 구성 요소

  - Level 0 (공정부, WirelessHART) : 무선 온도/근접, 모터, 카운터등
  - Level 1 (제어부,Wi-Fi 6) : LS 산전 PLC (웨이퍼 공정)

    지멘스 PLC (포토 공정)
  - Level 2 (공정모니터, 5G) : 생산공정을 모니터링 할 수 있는 HMI,

    Remote HMI

스마트공장 보안리빙랩 소개

무선 통신 – Wireless HART, Wi-Fi 6

✓ WirelessHART (최초의 무선통신 표준 – 다양한 필드 장치의 신뢰성 및 가용성 높은 통신)

- 장애 시 자동으로 경로를 우회하거나 데이터를 재전송 하는 등의 뛰어난 장애 복구 능력
- 최초 연결 시 유선으로 직접 암호키 인증 기능
- 패스워드를 주기적으로 자동 변경하는 기능 / 접근권한 관리 기능

✓ Wi-Fi 6 (기존의 Wi-Fi 보다 3배 빠른 통신과 대기시간 감소)

- 민감 데이터의 고강도 암호화
- 네트워크 복원 및 보안 프로토콜 지원

※ 스마트공장에서는 데이터 수집과 AGV(Automated guided vehicle)등에 활용

✓ 5G (4G LTE보다 200배 빠르고 1,000배 이상의 데이터 처리)

- 클라우드 연계나 Remote HMI는 5G를 통해 원거리 공장에서도 현장 상황을 모니터링, 제어

◆ 제어설비, 산업용PC, 서버, 애플리케이션 등에 대한 점검 도구

CLAROTY

coverity® SYNOPSYS®

metasploit® RAPID7 AppSec Plugin for Chrome

nexpose® http://infoteksource.com/ RAPID7 AppSec Plugin for Chrome

AIRCRACK-NG

◆ 제어프로토콜(모드버스, 프로피넷) 점검도구

Defensics® SYNOPSYS®

2 보안 취약점 점검 도구

제어설비, 산업용PC, 서버, 애플리케이션 등에 대한 보안취약점 점검 도구

Claroty
(제어설비 보안 컴플라이언스 점검)

- ✓ CVE 취약점 기반으로 제어설비의 위험도 및 취약점 도출
- ✓ 스마트공장 네트워크 위협에 대한 실시간 가시성 제공

Trace32
(제어설비 디버깅 도구)

- ✓ 펌웨어 동작을 검증하고 오류를 분석
- ✓ 제어설비에 탑재된 RTOS 디버깅, I/O레지스터 관찰, 메모리값 변동 탐지 등을 수행하는 디버깅 솔루션

Nexpose & Metasploit pro
(산업용기기 취약점 분석 및 모의침투 도구)

- ✓ 산업용 네트워크 장비, 시스템, 데이터베이스, 운영체제, 기업의 스마트공장 서비스 솔루션 애플리케이션 대상 취약점 검검 지원

Coverity
(SW 정적분석 도구)

- ✓ 제어설비에 탑재된 SW에 대한 소스코드 취약점 분석
- ✓ 소스코드 내에 잠재된 오류, 버그, 보안취약점 등의 각종 결함들을 소스코드 분석을 통하여 탐지

aircrack-ng
(무선 랜 인증 취약성 점검 도구)

- ✓ 무선 랜에 대해 패스워드 크래킹을 수행하여 무선 랜이 지닌 패스워드의 취약성 점검 지원

◆ Defensics (제어프로토콜 점검)

✓ PLC에서 사용하는 모드버스, 프로피넷 등의 제어프로토콜에서 퍼징 테스트를 수행하여 알려지지 않은 취약점 탐지

◆ Defensics FuzzBox (Wi-Fi 6 AP 점검)

✓ PLC에서 사용하는 Wi-Fi 6 AP 퍼징 테스트를 수행하여 알려지지 않은 취약점 탐지

※ 퍼징 테스트 : 의도적으로 비정상 데이터를 입력해 시스템 오류를 찾는 기술

◆ 대표적인 스마트공장 해킹 사례

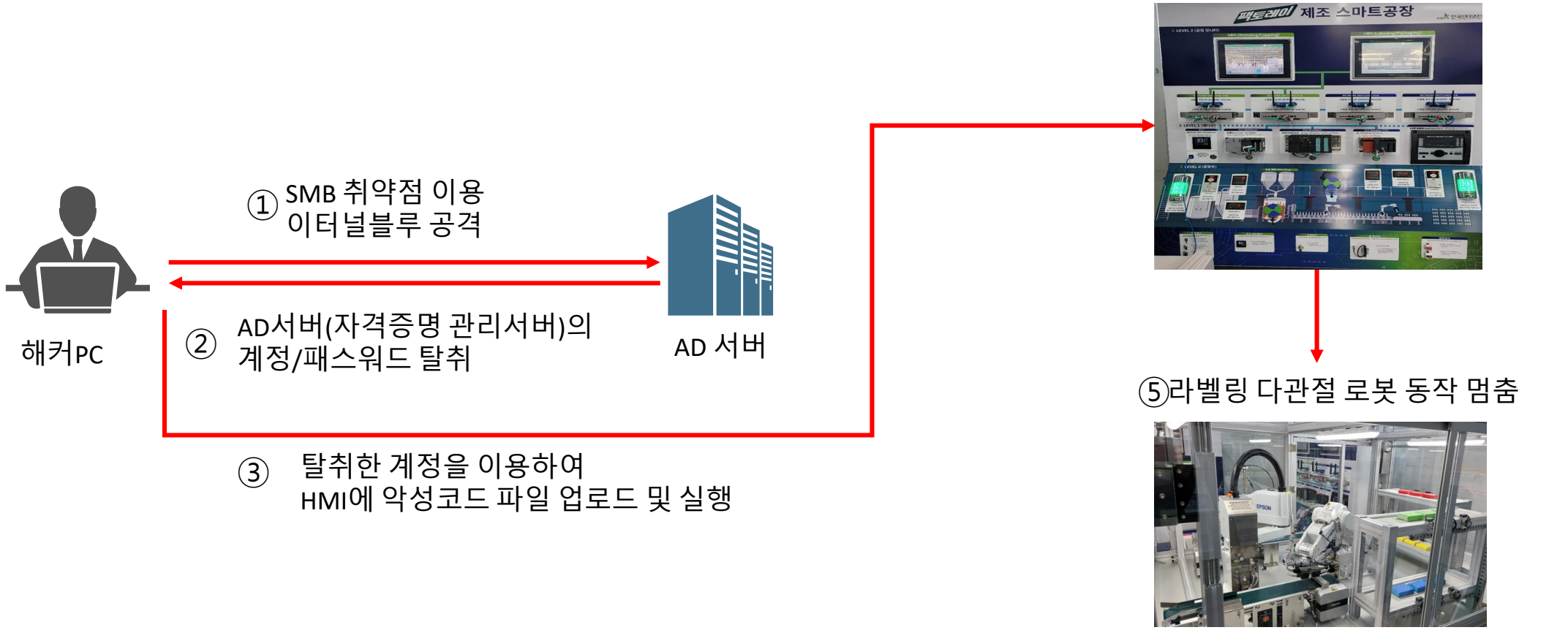
- ✓ 노르스크 하이드로 (노르웨이 기업으로 세계 최대 알루미늄 생산공장)
- ✓ 대만 TSMC (반도체 생산공장)
- ✓ 우크라이나 정전 (전력회사)
- ✓ 미국 댈러스 비상사이렌 사고 (도시 기반시설)
- ✓ 이스라엘 수자원 시설 공격시도 (정수시설)

◆ 대표적 사례를 분석하여 실제 발생 가능한 해킹 과정과 결과를 시연

◆ 사고 개요

- ✓ 2019년 3월 세계적인 알루미늄 생산 기업 노르스크 하이드로 대상 사이버 공격 발생
- ✓ 손실비용이 한화로 약 483억원과 전세계 알루미늄 생산가격을 약 1.2% 상승
- ✓ 실제 사고에 대한 상세 침투과정은 알려지지 않음
- ✓ 대외적으로 윈도우 SMB(원격파일공유) 취약점을 이용
- ✓ 원격에서 서버의 관리자 권한을 획득하고 랜섬웨어를 배포하여 시스템 파괴

◆ 시연 진행과정



※ 이터널 블루 : 미국 국가안보국(NSA)이 윈도의 취약점을 활용해 만든 해킹 도구로, 해커 조직 '섀도 브로커스'(Shadow Brokers)가 NSA에서 훔쳐 온라인상에 공개함.

◆ 대만 TSMC 사고 개요

- ✓ 2018년 폐쇄망인 웨이퍼 생산라인 공정PC에 SW업그레이드를 위해 USB 연결
- ✓ USB를 통해 공장 내 바이러스가 전파되어 내부 PLC의 오작동을 유발
- ✓ 사고 피해 : 3개 웨이퍼 생산 공장 가동 중단, 약 110억원 피해

◆ 우크라이나 정전 사고 개요

- ✓ 2016년 스피어피싱을 이용하여 우크라이나 전력회사에 악성코드 감염
- ✓ 악성코드에 감염되어 PLC(전력차단기 시스템)가 오동작
- ✓ 사고 피해 : 대규모 정전사태로 약 22만 5천가구 정전 피해

◆ 시연 진행과정

② 메일의 첨부파일(악성코드) 다운로드 / 실행 백도어 생성

관리자 PC

④ 원격으로 해커가 변조된 펌웨어를 PLC로 업로드

PLC

③ 관리자PC의 백도어로 접속

① 스피어피싱을 이용한 악성코드 첨부메일 전송

해커 PC

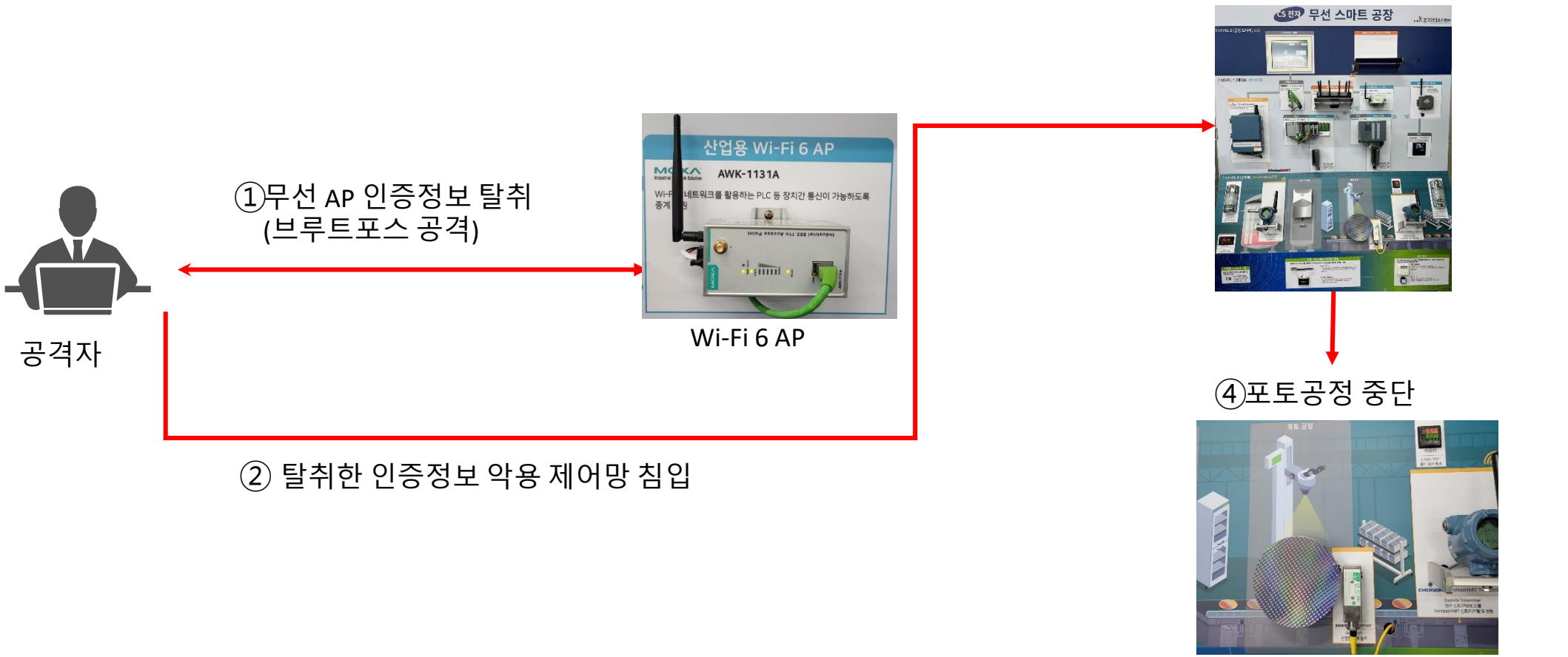
⑤ 원료배합, 캐핑 공정의 모터값, 카운터값, 배합속도 등의 오동작 발생

※ 위 두 사례는 내부 시스템에 악성코드가 감염된 이후 침투과정이 유사한 상황으로 내부 관계자가 첨부된 악성코드파일을 다운로드하여 감염되는 과정을 바탕으로 시연을 진행

◆ 사고 개요

- ✓ 2017년 4월 미국 댈러스 비상사이렌 공격
- ✓ 신원 미상의 해커가 비상관리국 사이렌 156개를 두시간 동안 울리도록 활성
- ✓ 무선AP의 취약점을 이용한 공격 방식
- ✓ 공격 대상 Wi-Fi6 AP를 스캔하여 찾아낸 다음 패스워드를 해킹하여 제어망에 접속

◆ 시연 진행과정

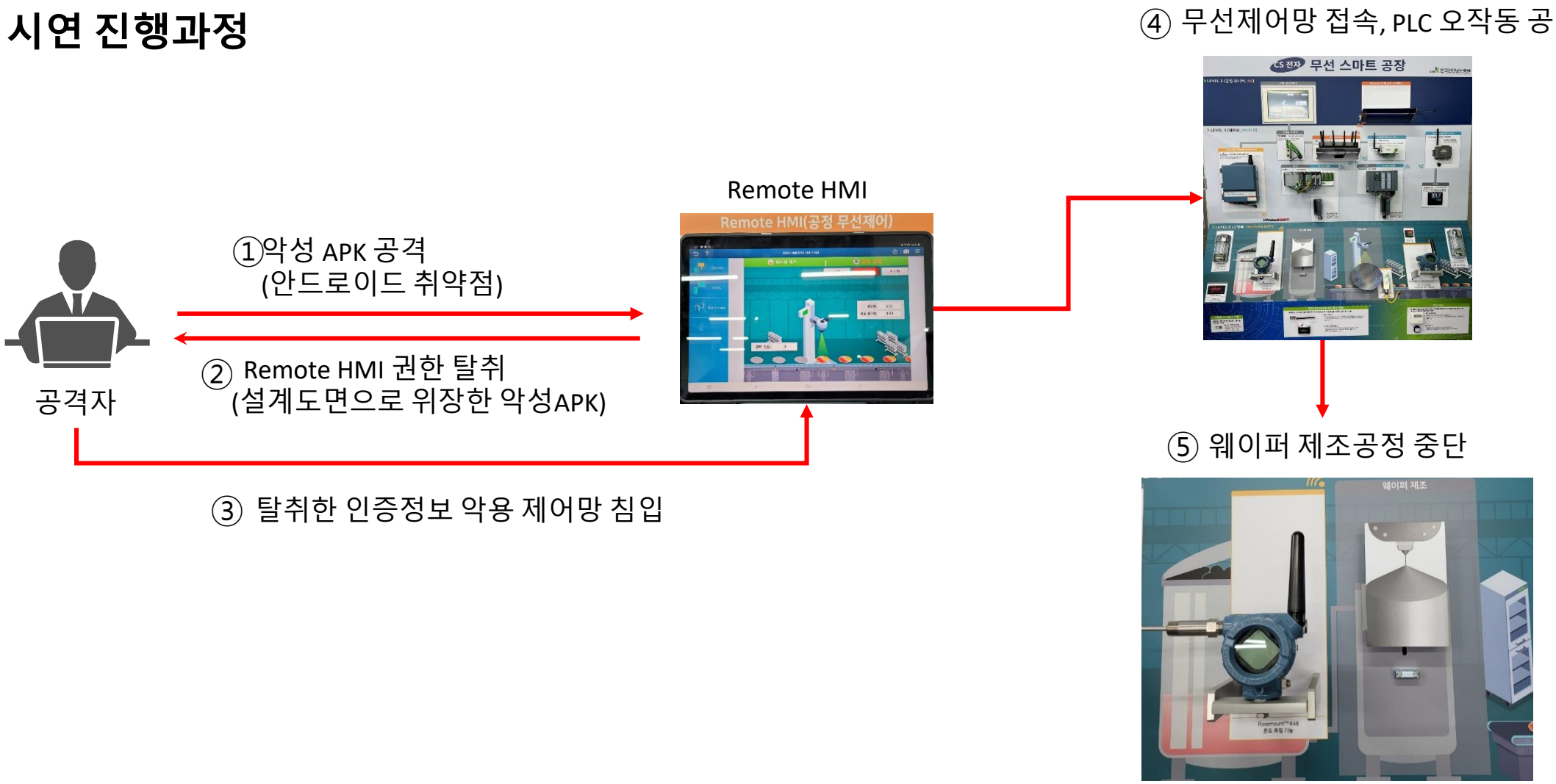


※ 브루트포스 (brute force) : 무차별 대입 공격, 값을 찾기 위해 모든 값을 무차별 적으로 대입하는 공격

◆ 사고 개요

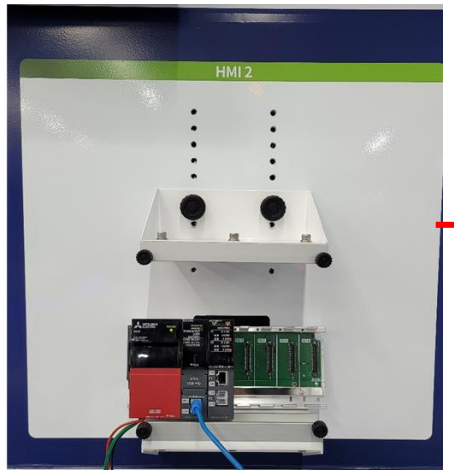
- ✓ 2020년 4월 이스라엘 수자원 시설 사이버 공격 시도 사례
- ✓ 식수의 염수 농도를 변경하여 인명 피해를 유발하려 했던 사이버 공격

◆ 시연 진행과정


④ 무선제어망 접속, PLC 오작동 공격
CS 전자 무선 스마트 공장
Remote HMI
Remote HMI(공정 무선제어)
①악성 APK 공격
(안드로이드 취약점)
② Remote HMI 권한 탈취
(설계도면으로 위장한 악성APK)
공격자
③ 탈취한 인증정보 악용 제어망 침입
⑤ 웨이퍼 제조공정 중단
웨이퍼 제조

◆ 이용자의 PLC 보안 취약점 점검

탈부착 월



이용자 PLC/ HMI
탈부착월에 탈착

고정월의
음료 제조공정 연계

생산공정 제어

◆ PLC 보안취약점 시연도구

✓ **넥스포즈**

- 이용자 PLC 취약점 점검 스캐닝

✓ **디펜직스**

- Modbus TCP Fuzzing Test

◆ PLC 보안취약점 시연도구

✓ **Defensics FuzzBox**

- 비정상 데이터 전송을 통해 알려지지 않은 취약점 도출
- Wi-Fi 6 AP Fuzzing 테스트 스위트 실행

✓ **aircrack-ng**

- 패스워드 크래킹을 수행하여 무선 랜이 지닌 인증 취약성 점검
- Wi-Fi 6 AP에 대한 인증 패킷을 스캔,수집,발생,브루트포스 공격, 정보 탈취

감 사 합 니 다.