제어망의 서버,PC 등 OS로 구동되는 IT 기기의 보안 취약점 점검을 자동화 할 수 있는 기술 개발

고려대학교

인공지능사이버보안학과

킥오프 발표

KOREA UNIVERSITY

CONTENTS

CONTENTS

팀 소개

캡틴오와 선원들

교수님

조금환 교수님

멘토님

심영복 대표님

이름 오병윤

담당 자동화 모듈

이름 김연수

담당 자동화 모듈

이름 이도현

담당 점검 스크립트

이름 최정민

담당 점검 스크립트

이름 김건희

담당 UI, DB

이름 조유빈

담당 UI, DB

개요

■ 개요

□ 상호 운영성 문제, 엄격한 가동 시간 요구사항이 존재하는 제어망 시스템은 보안 취약점 점검 및 조치가 늦음

□ 이러한 문제를 악용하여 산업 전반에 걸쳐 산업용 장비에 대한 공격이 증가

보안

산업제어시스템이 위험하다…“1/3 이상 취약점 패치 안돼”

Lucian Constantin | CSO 2023.01.25

핵심 인프라를 겨냥한 사이버 공격이 급증하고 있음에도 아직 산업제어시스템(ICS) 3분의 1 이상이 패치되지 않아 취약점에 노출돼 있는 것으로 나타났다.

Lucian Constantin, 산업제어시스템이 위험하다…“1/3 이상 취약점 패치 안돼”, Itworld, 2023.01.25, https://www.itworld.co.kr/news/274153

개요

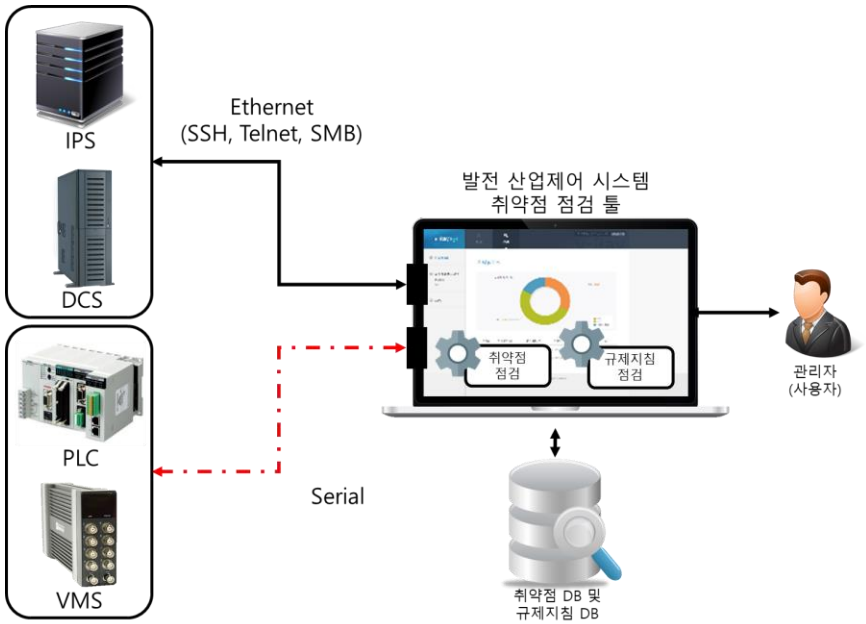
■ 개요

□ 이러한 문제를 해결하기 위해 보안 취약점을 사전에 발견하여 선조취를 취할 수 있도록 도와주는 시스템 제안

□ 이 시스템을 현장에 적용함으로써 사이버 보안 위협을 사전에 발견 가능

□ 시리얼 및 네트워크 통신을 사용하여 시스템에 접속하여 취약점을 점검

□ 점검한 결과는 UI로 확인 할 수 있도록 설계

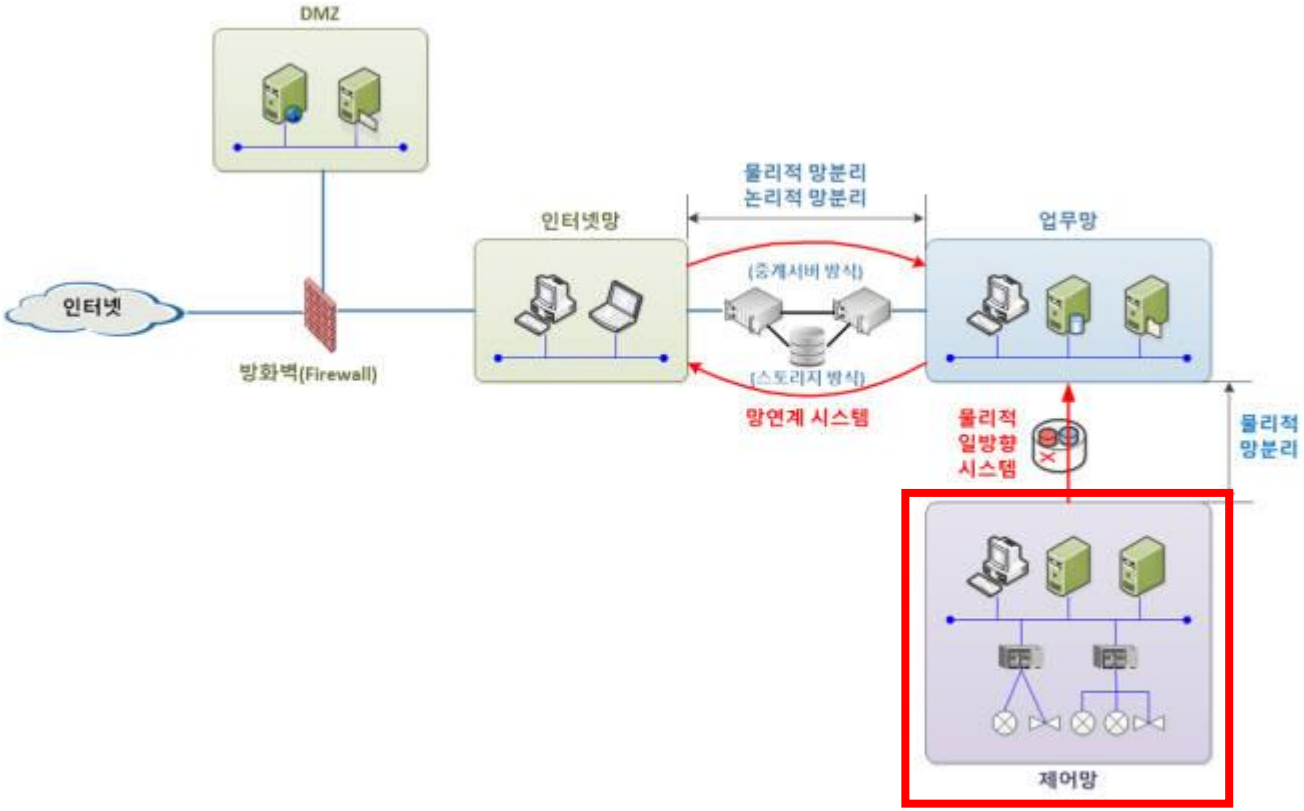


산업제어 시스템 보안 취약점 점검 시스템 구성도

기술 설명

■ 제어망

□ 산업 및 인프라 시스템에서 사용하는 네트워크 환경
□ 시스템의 제어, 감시 및 자동화를 위해 사용
□ 일반적으로 외부에서 접근할 수 없는 폐쇄망으로 운영

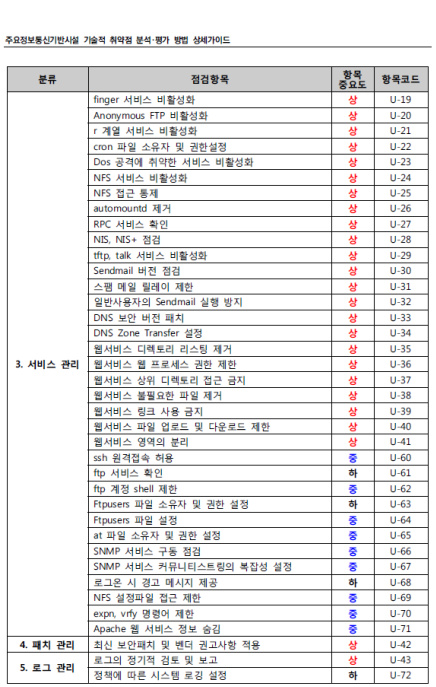


인터넷망과 업무망, 제어망 구성도

기술 설명

■ 규제 지침

- □ 주요정보통신기반시설을 각종 전자적 침해행위로부터 보호하기 위해 준수해야 하는 구체적 사항
- □ 구조정보통신기반시설을 관리하는 일부 공공기관과 민간기업의 경우 법적인 의무사항에 해당하여 매년 정기적으로 보안 취약점에 대한 분석 및 평가를 실시
- □ 한국인터넷진흥원에서 제공하는 “주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드“ 사용



기술적 취약점 분석 평가 방법 상세 가이드

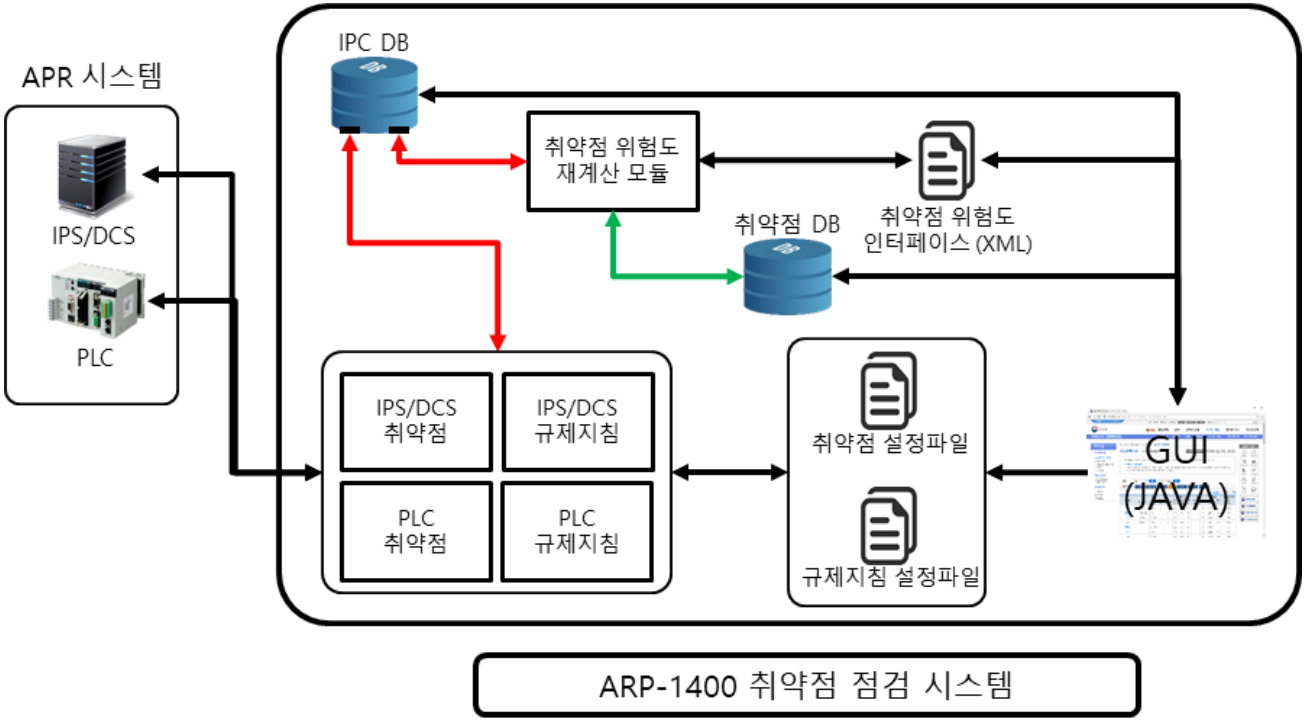
기술 설명

■취약점 점검 자동화

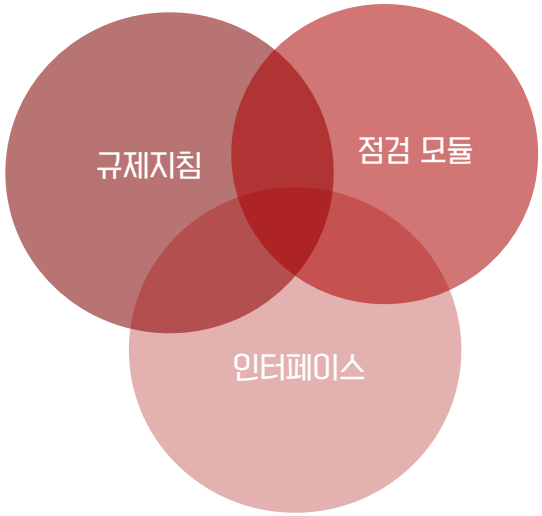
□ 보안 취약점을 식별하고 진단하는 과정을 자동화

□ 보안 엔지니어 또는 시스템 관리자의 작업 부담을 줄이고 보안 수준을 향상

□ 전체 시스템 또는 특정 업무 그룹별, 서버 기종별로 점검할 수 있도록 절차 구축 가능



목표



취약점 점검 자동화 시스템 구현

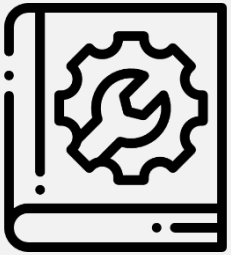
- ✓ 본 프로젝트의 수행을 통하여 Windows 운영체제를 사용하는 산업제어 시스템 보안 취약점 점검 프로그램 구현
- ✓ 규제지침 중 자동화가 가능한 점검 항목을 선별하여 점검 프로그램 구현
- ✓ 산업제어 시스템 보안 수준 향상을 통한 안정적 서비스를 제공할 수 있는 기반을 마련

수행내용


요구사항 확인 및 취약점 리스트화
점검 자동화 프로그램 구현
프로그램 테스트 및 마무리
개발 환경 설정
요구 사항 목록화
점검할 취약점 리스트화
취약점 별 결과 판별 정의
UI 화면 설계
DB 설계
점검 모듈 개발
UI, DB 개발
점검 모듈, UI 연결
프로그램 동작 테스트
코드 리팩토링
프로그램 사용 매뉴얼 작성
최종 보고서 작성

예상결과물

수행 내용



규제 지침

자동화 모듈

인터페이스

예상 결과물

- 취약점 점검 프로그램
- 최종보고서
- 사용 매뉴얼

업무 할당

규 제 지 침

- ✓ 규제지침 확인
- ✓ 취약점 선별
- ✓ XML 스크립트 작성
- ✓ 스크립트 별 점검 방식 문서화

이도현

최정민

점 검 모 듈

- ✓ 점검 모듈 동작 설계
- ✓ 점검 대상 접속
- ✓ 스크립트로 점검 실행
- ✓ 점검 결과 저장
- ✓ 프로그램 동작 테스트

오병윤

김연수

UI, DB

- ✓ UI, DB 설계
- ✓ UI, DB 구현
- ✓ 점검 모듈과 UI 연결
- ✓ 사용 메뉴얼 작성

김건희

조유빈

프로젝트 단계별 일정

캡틴오와 선원들 로드맵

일 정	3월	4월	5월	6월
단 계	프로젝트 조사 및 설계	프로그램 작성 및 테스트		프로젝트 마무리

세부 단계

사전 조사	프로그램 작성	프로그램 테스트 및 최적화
• 요구 사항 확인 • 규제 지침 조사 • 각 취약점 확인 • 프로그램 개발 환경 설계 • 업무 분장	• 규제 지침 스크립트(XML) 작성 • 점검 모듈 작성 • UI, DB 설계 및 작성 • 점검 모듈과 UI 연결	• 점검 모듈 동작 테스트 • 각 취약점 점검 테스트 • 자원 사용 최적화 • 프로그램 사용 매뉴얼 작성 • 최종 보고서 작성

프로젝트 진행 중

주차별 진행사항 보고 기술문서 작성 및 공유 회의록 작성 멘토링

산출물

- 산업 제어망 보안 취약점 자동 점검 프로그램
- 프로그램 사용 매뉴얼
- 최종 보고서

결론

추후 방향

❍ Windows 운영체제 뿐만 아니라 Linux 운영체제 또한 관련 규제 지침을 통해서 보안 취약점 점검을 할 수 있는 도구 개발

❍ 새로운 규제 지침을 인터페이스를 통해 쉽게 추가할 수 있는 기능 개발

❍ 규제 지침에 나와 있는 항목을 제외한 버그 헌팅 사이트에 나와있는 One-Day 취약점 또한 점검 할 수 있는 도구 개발

Thank you

KOREA
UNIVERSITY