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

4월 4일 미팅 자료

고려대학교

인공지능사이버보안학과

KOREA UNIVERSITY

CONTENTS

1. 피드백
2. 팀원 의견
3. 변경된 일정
4. UI 와이어프레임

피드백

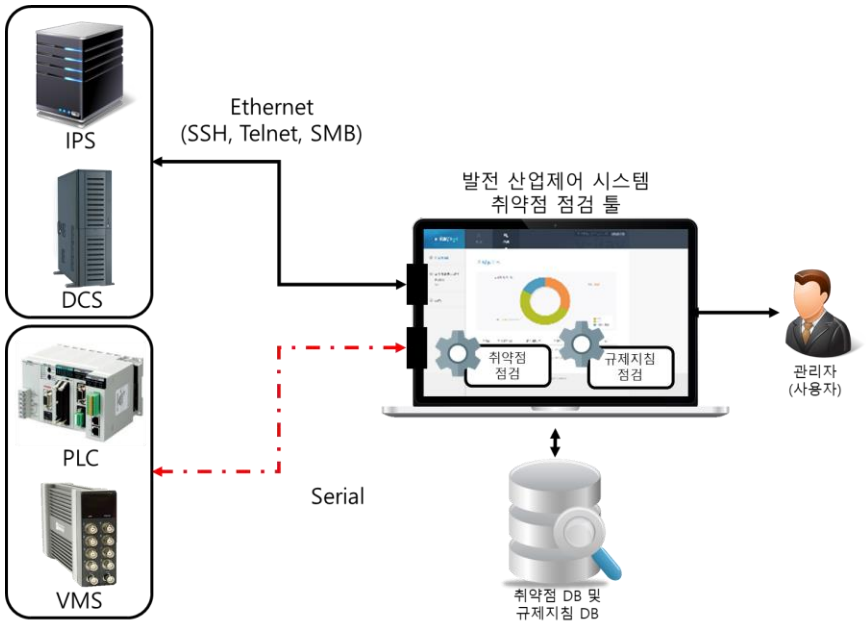
■ **캡스톤 목표**

□ Windows 시스템을 대상으로 보안 취약점 자동 점검 기술 개발

■ **킥오프 발표 피드백**

□ 제어 시스템에는 다양한 시스템이 존재함(ex, L3, L2, L1)

□ 현재 진행하고자 하는 취약점 점검 프로그램은 제어망에 특성을 고려한 것이 아닌 일반적인 Windows PC에 대한 취약점 점검과 다르지 않음

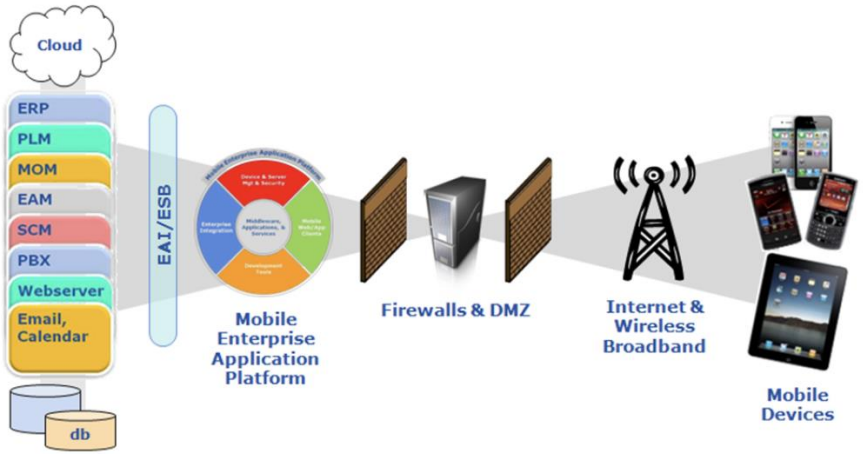


산업제어 시스템 보안 취약점 점검 시스템 구성도

팀원 의견

- HMI OS 점검 추가
  - Human Machine Interface OS : 프로세서 시스템과 운영자 간의 인터페이스
  - 대부분의 HMI시스템은 Window or Linux OS 위에서 구동
  - HMI 전용 OS 가 존재 하긴 하지만 회사 자체 제작

  - 이러한 문제점이 존재하여 진행하기 어려움



Mobile Enterprise Application Platforms Connectivity to Mobile Devices, Which Often Provide Thin-Client Access via Server-Based HMI Software

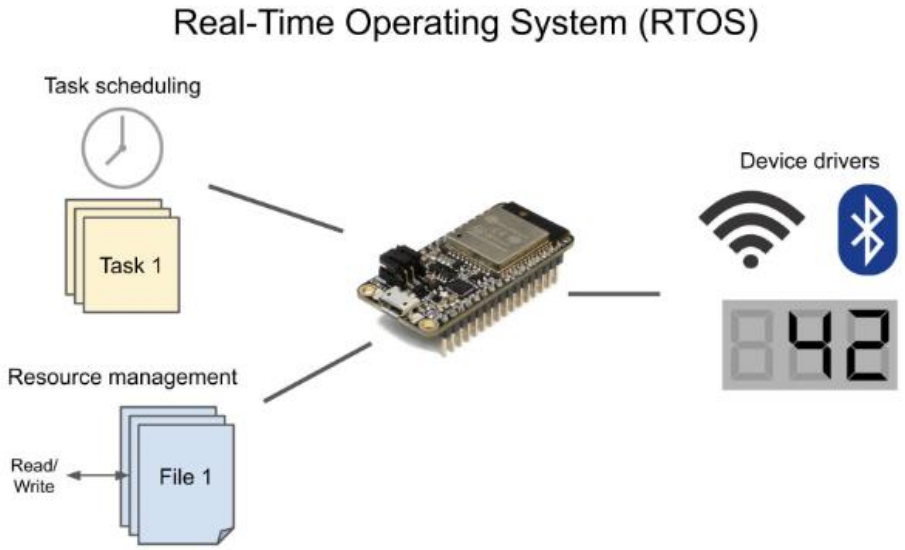
HMI OS 구성도

팀원 의견

■ RTOS 점검 추가

- □ Real Time Operating System : 실시간 운영체제
- □ 제어망에서 널리 사용되지만, 일반적으로 제어망에서 널리 사용되지만, 일반적으로 정보 유출 버그 또는 원격 코드 실행 버그 등 보안 취약점에 노출될 수 있음
- □ 체계적인 가이드라인이 부족함
- □ 제어 시스템에 사용되는 RTOS나 Linux의 보안 취약점을 실제 기기로 테스트하고 점검하기 쉽지 않음

- □ 이러한 문제점이 존재하여 진행하기 어려움



RTOS 예시

팀원 의견

■ PLC 기기 점검 추가

□ Programmable Logic Controller : 자동화 제어 장비

□ 표준화된 가이드 라인 부족한 상황

□ 기기를 구할 수가 없음

□ 테스트를 진행하지 못하기 때문에 정확하게 점검을 수행하는 프로그램을 제공하지 못함

□ 이러한 문제점이 존재하여 진행하기 어려움

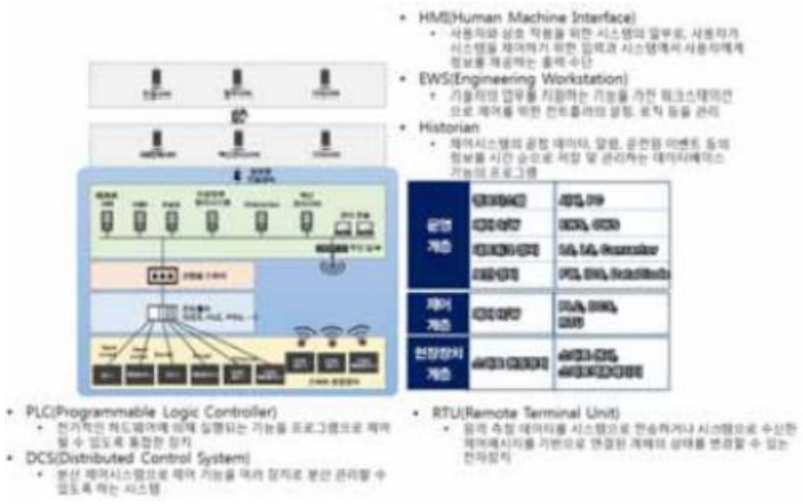
PLC 기기 예시

팀원 의견

■ 제어시스템 점검 추가

□ 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드에 '제어시스템' 항목 존재

□ 제어시스템 진단 항목에서 자동화 가능한 일부 점검 항목을 추가



[그림] 제어시스템의 기본 구성도 및 각 구성요소 예시

HMI 및 PLC 예시

[그림] HMI 화면 예시

[그림] PLC 기기 예시

상세 가이드에서 제공하는 일반적인 제어시스템 예시

분류	점검항목	중요도	항목코드
1. 계정관리	계정기능이 있는 제어시스템 구성요소에 대해 계정을 설정하여 사용	상	C-01
	제어시스템 계정의 로그인/로그아웃, 사용명령 등 사용기록을 저장	상	C-02
	제어시스템 계정입력 시 패스워드 마스킹 처리, 입력값 에러 발생 시 제공 정보 제한 수행	상	C-03
	제어시스템 계정을 관리, 운영, 유지보수 등 용도에 따라 분리하고 운용	중	C-23
	제어시스템 계정에 대해 관리, 운영, 유지보수 등 용도에 맞는 최소 권한 부여	중	C-24
	제어시스템 운전원 별 유일 계정 부여 또는 시간별 사용자 기록 유지	중	C-25
2. 서비스 관리	제어시스템 구성요소에 대한 시각 동기화 수행	상	C-04
	제어시스템에 불필요한 서비스 및 취약한 서비스 제거 또는 보완대책 수행	상	C-05
	제어시스템 구성요소에 대한 관리자 페이지 운영 시 이에 대한 접근통제(사전인가 접근만 허용) 수행	중	C-26
	제어시스템 내 파일/디렉토리 접근권한 및 신뢰관계를 적절히 부여	중	C-27
	제어시스템 내 제어와 직접적인 관련이 없는 불필요 프로그램 삭제	중	C-28
	제어시스템 운영 정보, 제어명령 등 중요정보에 대한 위변조 및 replay 공격 방지 대책 적용	중	C-29
	제어시스템 내 전달되는 제어명령 및 파라미터의 정상 범위를 식별하고 관리	중	C-30
	제어시스템 내 사용자 통신세션에 대해 세션타임아웃 적용	중	C-31
	GPS 스푸핑/재밍 공격 등 시각동기화 서비스를 교란하기 위한 공격에 대비한 보안조치 수행	중	C-32
3. 패치관리	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 제조사 협력방안, 테스트 방안 등의 절차 수립	상	C-06
	외부 업체, 인터넷을 통한 다운로드 등의 경로로 반입된 각종 패치·업데이트 파일에 대해 무결성 검증 및 클린 PC를 통한 악성코드 존재 여부 검사 수행	상	C-07
	제어시스템 구성요소의 알려진 취약점에 대해 보안패치 적용 또는 상응하는 대응책 적용	상	C-08
	운영체제, 응용프로그램, 펌웨어 등에 대해 안정성이 확인된 최신버전의 소프트웨어 사용 및 기술지원이 종료된 제품 미사용	중	C-33
	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축	중	C-34
4. 네트워크 접근통제	제어 네트워크는 업무망, 인터넷, CCTV망 등 외부망과 물리적으로 분리하여 사용	상	C-09
	제어 네트워크 외부로 자료전달 시 물리적 일방향 자료전달 환경을 구축하여 외부에서 제어 네트워크로의 침입을 차단	상	C-10
	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 등의 외부망 연결을 제한하고 주기적으로 점검	상	C-11
	제어 네트워크에 비인가된 시스템/기기에 대한 연결 및 접속을 차단	상	C-12
	물리적 일방향 자료전달 환경의 올바른 동작 및 운용에 대한 주기적인 점검 수행	상	C-13
	제어 네트워크를 용도에 따라 세분화하고, 접근제어를 수행하여 제어시스템 운영에 필요한 네트워크, 시스템 간의 통신만 허용	중	C-35

제어시스템 취약점 진단 항목

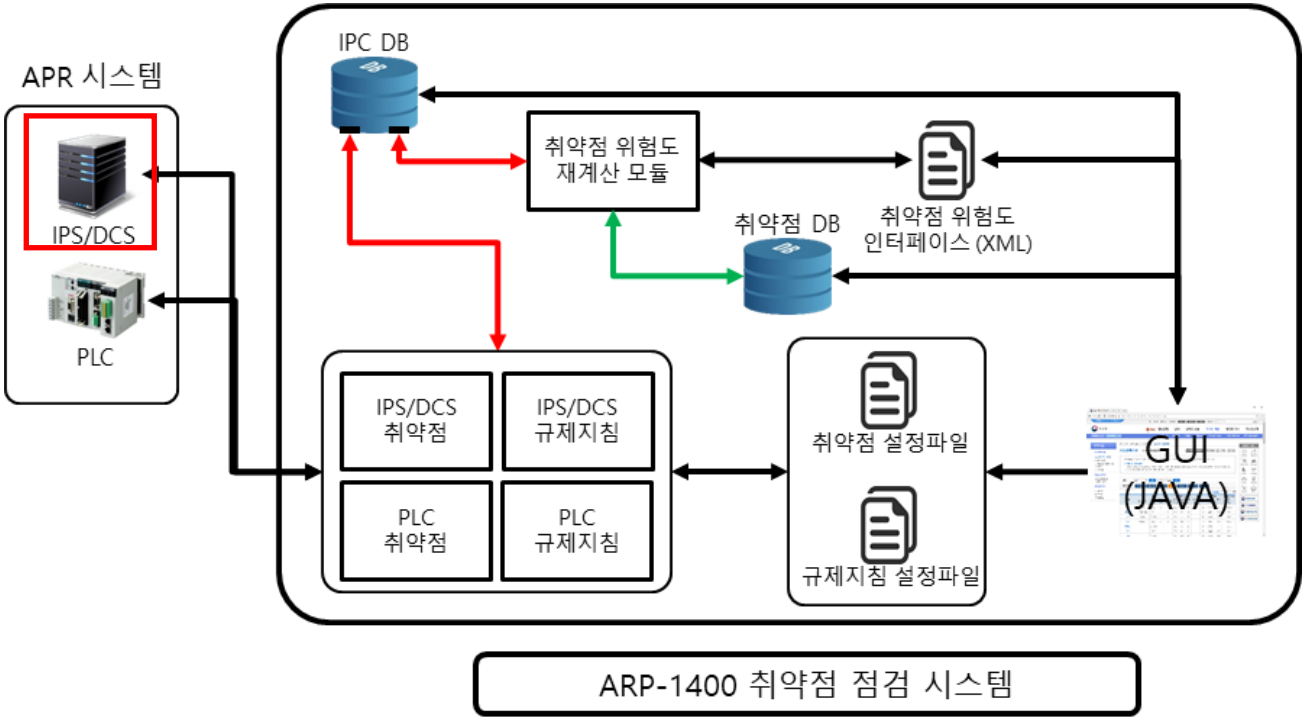
팀원 의견

■ IPS/IDS 점검 추가

□ Intrusion Prevention System: 침입 방지 시스템

□ 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드에 'IPS/IDS' 항목 존재

□ 가상으로 구동한 IPS에 대해 취약점 점검이 가능하다면 IPS를 점검 대상에 추가



변경된 일정

■ 변경된 일정

□ Windows 대상으로 각 항목별 1~2개의 점검 항목만 스크립트화

□ 일부 항목을 자동으로 점검하는 모듈 개발 및 UI 일부, DB를 중간 전까지 작성

□ 최종 발표 전까지 모든 일정 진행

캡틴오와 선원들 로드맵

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

세부 단계

사전 조사	프로그램 작성	프로그램테스트및최적화
• 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 • 사용 매뉴얼 작성 • 최종 보고서 작성

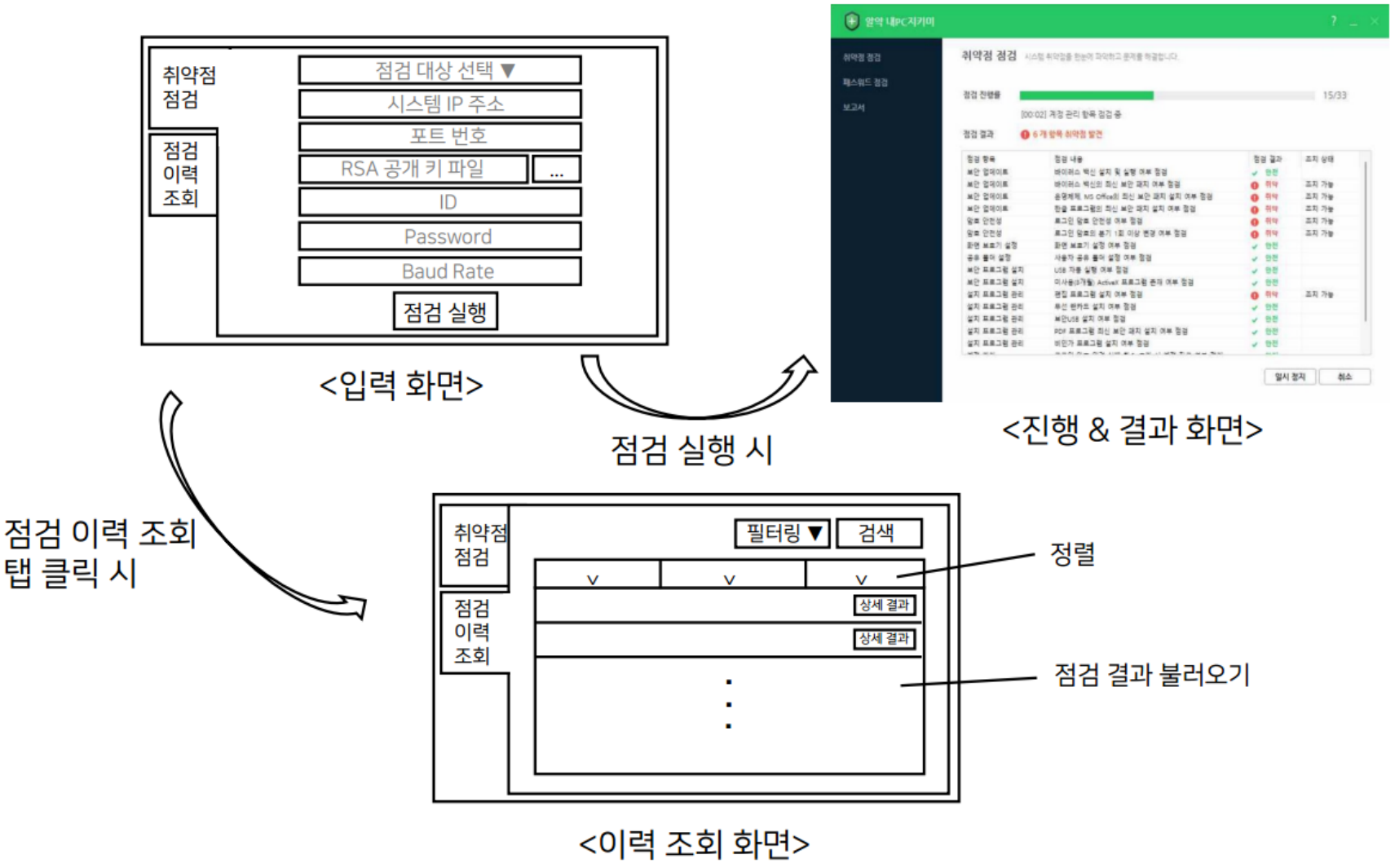
프로젝트 진행 중

주차별 진행사항 보고 기술문서 작성 및 공유 회의록 작성 멘토링

산출물

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

UI 와이어 프레임

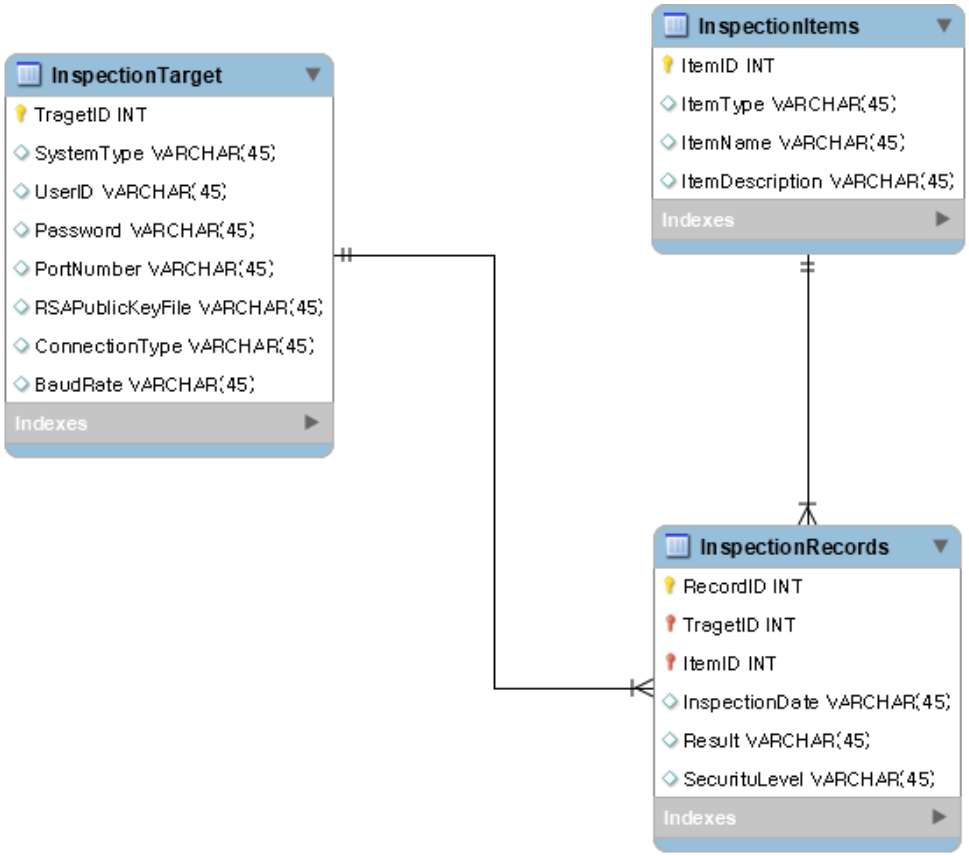

취약점 점검
점검 이력 조회
점검 대상 선택 ▼
시스템 IP 주소
포트 번호
RSA 공개 키 파일
...
ID
Password
Baud Rate
점검 실행
<입력 화면>
점검 실행 시
<진행 & 결과 화면>
점검 이력 조회 탭 클릭 시
취약점 점검
점검 이력 조회
필터링 ▼
검색
상세 결과
상세 결과
정렬
점검 결과 불러오기
<이력 조회 화면>

DB 설계

■ DB 설계

□ 점검 대상에 대한 테이블, 규제 지침에 대한 테이블, 점검 기록에 관한 테이블로 구성

□ Target 테이블과 Items 테이블은 Records 테이블과 각각 1:N 관계로 구성



데이터베이스 관계도

Thank you

KOREA
UNIVERSITY