

캡스톤디자인 2차 레포트



날짜	2024. 04. 01
학 과	인공지능사이버보안
과 목	캡스톤디자인
조	2 조

	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

목차

1. 키포프 발표 요약 3

2. 발표 피드백 6

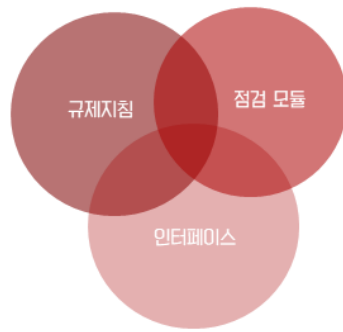
3. 결론 8

	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

1. 키포 발표 요약

저희 2조는 이번 2024-1 캡스톤 디자인에서 “제어망의 서버, PC 등 OS로 구동되는 IT 기기의 보안 취약점 점검을 자동화 할 수 있는 기술 개발” 이라는 주제와 함께 3월 27일에 키포 발표를 진행하였습니다.

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

[그림 1] 키포 발표 목표

목표는 위와 같이 규제 지침, 점검 모듈 및 인터페이스를 이용하여 Windows 운영체제를 사용하는 산업제어 시스템 보안 취약점 점검 프로그램을 구현 하는 것이 목표였습니다.

	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

업무 할당



[그림 2] 키포 발표 업무 할당

업무는 규제지침에서 자동화가 가능한 취약점을 선별하여 스크립트를 작성하는 업무, 작성된 스크립트를 이용하여 Windows 운영체제를 사용하는 시스템에 접속하여 보안 취약점 점검을 실행하는 업무, UI 와 DB를 설계하여 작성 및 운영하는 업무 이렇게 3가지 업무로 분류하여 각 2명씩 팀원에 업무를 할당하였습니다.


	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

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
	<ul style="list-style-type: none">요구 사항 확인규제 지침 조사각 취약점 확인프로그램 개발 환경 설계업무 분장		<ul style="list-style-type: none">규제 지침 스크립트(XML) 작성점검 모듈 작성UI, DB 설계 및 작성점검 모듈과 UI 연결	<ul style="list-style-type: none">점검 모듈 동작 테스트각 취약점 점검 테스트자원 사용 최적화프로그램 사용 매뉴얼 작성최종 보고서 작성
	프로젝트 진행 중			
산출물	주차별 진행사항 보고			
	기술문서 작성 및 공유 회의록 작성 멘토링			
산출물				
	<ul style="list-style-type: none">산업 제어망 보안 취약점 자동 점검 프로그램프로그램 사용 매뉴얼최종 보고서			

[그림 3] 키포프 발표 단계별 일정

이후 위 사진과 같은 일정으로 프로젝트를 진행하여 중간 발표에는 일부 선정된 취약점으로 점검을 구동할 수 있도록 작성하고 최종 때 선전된 모든 취약점 점검 항목에 대해 점검 자동화를 구동하여 결과를 UI에 보여 줄 수 있도록 계획을 세웠습니다.

	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

만 아니라 기기를 구할 수 없어 점검 테스트를 진행 할 수 없다는 점도 존재합니다.

이에 저희는 먼저 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드'에 '제어시스템 취약점 진단 분석 평가 방법' 목차가 존재하는 것을 확인하여 분석-평가 항목을 조사 후 점검 자동화 할 수 있는 항목이 존재 하면 이것을 기존에 Windows 운영체제에 대한 보안 취약점 점검과 추가하여 보안 취약점 점검을 할 수 있도록 진행할 예정입니다.

추가적으로 제어시스템에서 IPS 또는 IDS를 사용한다는 가정을 하여 이에 대한 보안 취약점 점검 또한 추가할 예정입니다.

하지만 이러한 의견은 저희 팀원들과 회의를 통해 결정된 사항일 뿐이지 교수님, 멘토님과 의견을 나누어 정해진 것이 아니기 때문에 4월 4일 오후 7시에 예정된 교수님, 멘토님과 회의를 통해 명확하게 어떻게 목표, 업무, 일정을 변경 할지 정할 수 있을 것 같습니다.

먼저 팀원들과 진행된 회의에서 결정된 의견으로 변경된 목표는


기존 : Windows 운영체제를 사용하는 제어시스템 PC에 대한 보안 취약점 점검 자동화

변경 : Windows 운영체제, 제어시스템, IPS/IDS에 대한 보안 취약점 점검 자동화

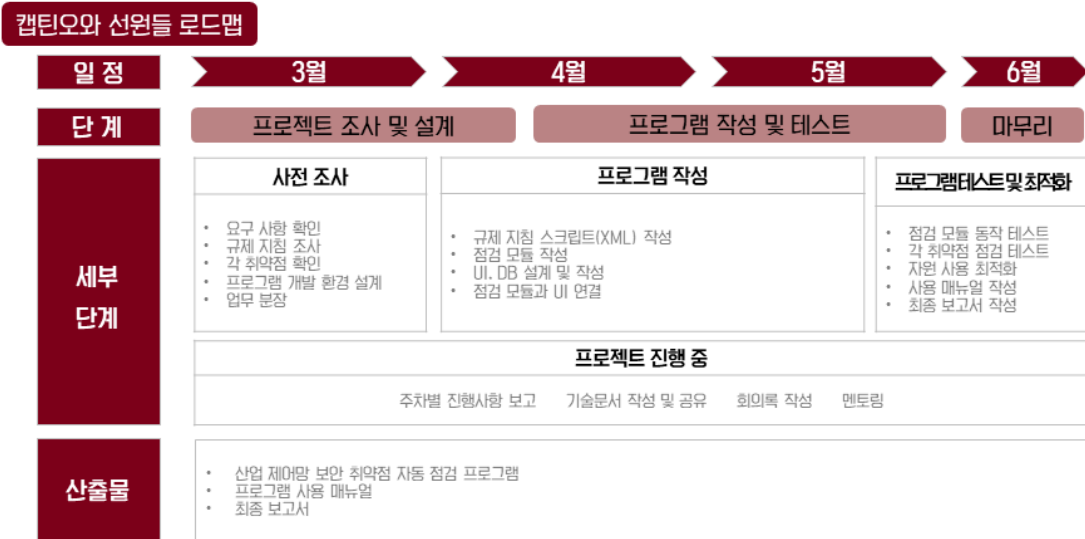
입니다.

업무 분장에 대해서는 보안 취약점 점검을 진행하는 대상이 늘어난 것이기 때문에 변경된 업무 분장은 없습니다.

단계별 일정에 관해서는 규제지침을 담당에 대한 업무량이 증가 했기 때문에 중간 발표 전까지 각 점검 대상에서 일부 항목에 대한 규제 지침 스크립트를 작성하여 동시에 점검 모듈 개발을 진행할 예정이고 최종 발표까지 모든 점검 대상에서 자동화가 가능한 규제 지침에 대한 점검 자동화를 진행할 예정입니다.

	캡스톤 디자인 2차 레포트			
	학 과	과 목	조	문서 최종 수정일
	인공지능사이버보안	캡스톤디자인	2 조	2024. 04. 01

프로젝트 단계별 일정



[그림 5] 변경된 단계별 일정

3. 결론

저희는 교수님과 멘토님의 피드백을 무겁게 받아들여, 먼저 팀원들과 업무 회의를 통해서 어떠한 방향으로 프로젝트를 진행할지 의견을 교환 하였고 교수님과 멘토님과 회의를 통해서 원래의 주제에 더 가까운 방향으로 프로젝트를 진행하여 제어망의 보안 취약점을 자동으로 점검하는 기술을 개발하는 것으로 목표로 진행할 예정입니다.

저희는 이 프로젝트를 통해 제어망에 대한 심층적인 이해를 높이고, 어떠한 위협이 존재하는지에 대해 인식하며, 취약점 점검 자동화를 위한 개발 방법에 대해 깊이 있게 탐구할 것입니다. 교수님과 멘토님들의 지도 아래, 저희 팀은 이번 캡스톤디자인 프로젝트를 성공적으로 완수하기 위해 최선을 다할 것입니다. 이를 통해 산업 제어 시스템을 보다 안전하게 발전시킬 수 있을 것으로 기대합니다.