Team No.

TONGMYONG UNIVERSITY

전공연구형_Capstone Design 신청서

과제명	국문	공공 와이파이 해킹 공격 분석 및 보안 방안에 관한 연구					
	영문	Public Wi-Fi hacking attack analysis and security measures					
과제팀명		하나차이					
참여학과		정보보호학과	교과목명	DID 인증 기술 _Capstone Design			
지도교수		성명				소속(학과)	
		신 승 수				정보보호학과	
참여 학생	구분	소속학과(전공)	학번	학년	성명	연락처	이메일
	팀장	정보보호	18학번	3	변 * *	010-3610-****	byunsp3610@gmail.com
	팀원	정보보호	19학번	3	류 * *	010-4088-****	codemail5143@gmail.com
		정보보호	20학번	3	박 * *	010-6416-****	qkrtpdbs88@gmail.com
		정보보호	17학번	3	석 * *	010-9474-****	dch1114@naver.com
수행기간		2022년 09월 ~ 2022년 12월					
유형선택		☐ 기업성장형 ☐ 사회기여형 ☐ 창업연계형					
구분 / 지원금액		■ 전공연구형	☐ 과제창출형_C유형 (예산 300,000원)				
			■ 학술연구형_D유형 (예산 200,000원)				

동명대학교 현장실습지원센터 규정에 의거, 캡스톤디자인 과제를 성실하게 수행하고자 본 과제 신청서를 제출합니다.

붙임 : 과제 제안서 1부

2022. 09. 14.

신청인(대표학생) : 변 * * (인)

과제지도교수 : 신 승 수 (인)

동명대학교 현장실습지원센터장 귀하

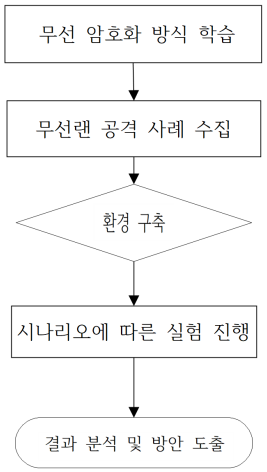
<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) 전공연구형

Capstone Design 과제 제안서

1. 과제 선정 배경 및 과제 수행 목적

- 와이파이란 무선 접속 장치(AP: Access Point)를 이용해 일정 거리 안에서 무선 인터넷을 사용할 수 있는 근거리 통신망 기술임.
- 공공 와이파이는 정부, 지자체, 통신사 등에서 제공하는 와이파이를 의미함. 공공 와이파이의 예로는 버스, 지하철 등에서 무료로 사용하는 와이파이를 들 수 있음.
- 공공 와이파이와 일반 와이파이의 차이점은 공공 와이파이는 정부 기관이 주체가 되어 주민센터, 복지시설, 버스, 지하철 등의 공공장소에서 누구에게나 무료로 제공하는 와이파이를 의미하지만, 일반 와이파이는 집, 카페, 영화관 등의 장소에서 개인이 직접 설치하여 사용하는 와이파이를 의미한다는 점임. 즉, 와이파이 제공 주체가 누구인지에 따라 차이가 있음.
- 공공 와이파이는 별도의 비밀번호 없이 무료로 제공되어 다수가 쉽게 사용 가능하지만, 그만큼 해커 또한 접근하기 쉬움. 동일한 장소에서는 같은 무선접속 장치를 사용하기 때문에 해커가 악의적인 접속을 하여 일반 사용자가 악성 프로그램을 통한 범죄에 노출될 수 있음.
- 무선랜 공격은 오픈 소스로 툴이 널리 공개되어 있기 때문에 공격자가 손쉽게 공격이 가능하며, 공격을 통해 공공 와이파이에 접속한 사용자의 네트워크 패킷을 도청하거나, 피싱 사이트로 유도를 통한 범죄 행위가 가능.
- 공공 와이파이가 실생활에서 많이 사용되는 만큼, 해킹 사례를 분석하고 공격에 대한 탐지 및 보안 방안에 대한 연구가 필요.
- 본 과제에서는 실제 공공 와이파이 환경을 구축해 모의 해킹을 시도하고, 해킹 결과 분석을 통해 공격 탐지 및 대응할 수 있는 방향을 제시하고자 함.

2. 과제 수행 방법



- 연구 진행을 위해 공공 와이파이에 사용되고 있는 보안 방법인 무선 암호화 방식(WEP, WPA, WPA2, WPA3)에 대한 사전 지식 학습.
- 와이파이는 무선 네트워크 기술 중 하나이기에 무선랜 공격 사례 수집 및 분석.
- 분석한 무선랜 공격 사례를 바탕으로 무선랜 해킹 기술 조사 및 공공 와이파이 취약점 연구.
- 해킹 시뮬레이션 진행을 위해 실생활에서 사용되는 공공 와이파이 환경과 동일한 환경 구축.
- 환경 구축과 더불어 조사한 공격 기술을 기반으로 하는 시나리오 작성.
- 작성한 시나리오에 따라 직접 해킹 시뮬레이션 실습 진행.
- 수행된 실험을 바탕으로 결과 분석 및 공공 와이파이 보안에 대한 방안 도출.

3. 결과물에 대한 기대효과 및 활용방안

[기대효과]

- 본 연구에서는 공공장소에서 많이 사용되는 공공 와이파이에 대한 보안 대책에 대해 연구함.
- 현재에는 보안상의 이유로 공공 와이파이를 이용한 중요 업무는 지양하도록 권고되고 있음.
- 공공 와이파이에 대한 해킹 공격 방지 대책 기법을 제안하여 공공장소에서 안전한 와이파이 사용이 가능할 것이라 기대함.
- 공공장소 이외에도 무선랜을 이용하여 와이파이 기술을 사용하는 모든 분야에서 안전한 사용이 가능할 것이라 기대함.
- 공공 와이파이의 보안 대책을 마련함으로써, 해킹으로 인해 발생할 수 있는 금융, 개인정보 유출 등의 2차적인 피해 발생을 예방할 수 있을 것이라 기대됨.

[활용방안]

- 공공 와이파이 해킹의 보안 대책 제시를 통해 와이파이 이외의 무선랜 통신의 안전성 있는 사용에도 활용할 수 있을 것이라 예상됨.
- IoT 기기의 발달로 스마트폰 이외에도 무선랜을 이용하는 기기가 증가하고 있음. 와이파이에 대한 보안 대책을 제시하여 스마트폰 및 각종 IoT 장비의 보안에도 활용이 가능할 것이라 예상됨.

4. 수행 일정

주요내용	추진일정				소요 기간(월)
	09	10	11	12	
연구를 위한 사전지식 학습					*3주*
관련 자료수집 및 분석					*3주*
환경 구축 및 시나리오 작성					*3주*
직접 해킹 시뮬레이션					3주
결과 분석 및 보안방안 마련					3주

5. 팀원별 역할

No.	성 명	
1.	변 * *	리더,서기 / 자료수집, 실습환경구축, 해킹실습, 결과분석
2.	류 * *	결과 보고서 작성 / 자료분석, 실습환경구축, 해킹실습, 보안방안 도출
3.	박 * *	발표 / 자료수집, 해킹 시나리오 작성, 해킹실습, 보안방안 도출
4.	석 * *	PPT 제작 / 자료분석, 해킹 시나리오 작성, 해킹실습, 결과분석

<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) **전공연구형**

6. 소요 예산

구분	용도 (과제수행과의 연관성)	품목	규격	단위	수량	단가	금액 (원)
그 외	용도 (과제수행의 연관성 기술)			산출 내역			금액 (원)
회의비	과제 수행 팀원과의 회의 진행			주 1회 한정			200,000원 (5000원 * 4명 * 10회)
합 계							200,000 원