

# 실무형 프로젝트 주제 회의

## K-Shield 주니어 보안사고 분석대응 7기

2021.08.30  
5팀 파이쉴드주니어

01

하나,

프로젝트 주제  
선정 목적



02

두울,

첫 번째  
주제



03

세엣,

두 번째  
주제

01

하나,

프로젝트 주제  
선정 목적

02

두울,

첫 번째  
주제

03

세엣,

두 번째  
주제

## 선택한 주제는 “와이파이”

전체적인 큰 틀의 주제는 와이파이로 고정, 그 안에서 세부 주제 고민중

### 첫 번째 주제

Wi-Fi의 취약점을  
이용하여 사용자의  
정보를 유출하는 것

### 두 번째 주제

기존의 공공 Wi-Fi와  
같은 Wi-Fi를  
생성하여 공격하는 것

# 프로젝트 주제 선정 목적

큰 주제로 와이파이로 선택한 이유

과학기술정보통신부

## 과도한 우려

와이파이6(IEEE 802.11ax)로  
데이터 전송량, 속도, 연결성과  
WPA3(Wi-Fi Protected  
Access 3) 지원으로 보안성도  
한층 강화됐다.

정보보안 전문가들

## 여전히 보안 위험

WPA3도 보안취약점이 발견된 바  
있고 완벽한 보안은 없다고 강조하며  
공공와이파이는 개방된 환경으로  
인해 보안위협에 노출될 여지가  
크다고 주의를 당부했다.

## 공공와이파이 ‘보안’ 논란…과 기부 “범용 서비스, 문제 없어”

과기부, 보안표준 적용 일반 사용에 문제없어  
보안업계, 이용자 사용수칙취약점 주기 점검 필요  
KT, 대중들이 보편적 사용할 수 있는 관리 중요

김영민 기자 | 승인 2021.02.24 07:00 | 댓글 0



출처 : 이뉴스투데이

## 프로젝트 주제 선정 목적

큰 주제로 와이파이가로 선택한 이유

실제로 어떤 환경에 노출되어 있는지 확인해보고 싶어서

발생 가능한 피해 및 공격들이 존재하는지 알아보기 위해서

## 프로젝트 목표

### 1) 공공 와이파이의 안전성

- 악의적인 와이파이 공격에 대한 위험성을 보여서 공공 와이파이 보안 허점에 대한 경각심을 일깨우고, 이에 대한 솔루션과 보안 대책을 도출한다.

### 2) 무료 와이파이의 안전성

- '와이파이'는 실생활에서 가장 쉽게 접근할 수 있는 보안 키워드이므로 사람들에게 경각심을 일깨우려함

01

하나,

프로젝트 주제  
선정 목적

02

두울,

첫 번째  
주제

03

세엣,

두 번째  
주제



## 첫 번째 주제 Wi-Fi의 취약점을 이용하여 사용자의 정보를 유출하는 것

### 새로운 보안 프로토콜 WPA3

#### + WPA2의 보안 문제를 해결할 수 있다

유무선 공유기나 액세스 포인트에 접속할 때마다 총 4번에 걸쳐 암호화 키를 주고 받으며 서로 확인하는 과정에 다른 기기가 끼어들어 통신 내용 알 수 있다는 문제점

#### - WPA3의 문제점 '드래곤블러드(Dragonblood)'

- 1) 호환 모드를 이용하여 WPA2로 강제로 접속한 뒤 비밀번호를 알아내는 것
- 2) 유무선 공유기나 액세스포인트, 혹은 접속한 기기에 DDoS 공격하는 것

## 첫 번째 주제 Wi-Fi의 취약점을 이용하여 사용자의 정보를 유출하는 것

WPA3의 호환 모드를 이용하여 WPA2로 접속한 후

WPA2의 취약점을 이용하여 사용자 정보를 유출시키는 것을 목표

출처 : 남지현, 이주엽, 권송희, 최형기(2019). 안전한 무선랜 환경을 위한 WPA3 표준의 보안 프로토콜 비교 및 분석

WPA3 호환모드 이용,  
WPA2로 접속

사전 공격 실행 후  
비밀번호 탈취

이후 STA와 AP간의  
통신에 참여, 공격 실행

4-way Handshake  
메시지 획득

중간자 공격으로  
STA와 AP간 메시지  
복호화 가능

## 첫 번째 주제 Wi-Fi의 취약점을 이용하여 사용자의 정보를 유출하는 것

**WPA3를 WPA2로  
강제로 접속시키게  
하는 팀1**

**WPA2의 취약점으로  
공격을  
실행하는 팀2**

## 첫 번째 주제 Wi-Fi의 취약점을 이용하여 사용자의 정보를 유출하는 것

노랑-공통 / 빨강-팀1 / 파랑-팀2

| 단계/주차     | 9월1주 | 9월2주 | 9월3주 | 9월4주 | 10월1주 | 10월2주 | 10월3주 | 10월4주 | 11월1주 | 11월2주 | 11월3주 |
|-----------|------|------|------|------|-------|-------|-------|-------|-------|-------|-------|
| 스터디       | 노랑   | 노랑   |      | 파랑   | 파랑    |       |       |       |       |       |       |
| 계획서<br>작성 |      |      | 노랑   |      |       | 파랑    |       |       |       |       |       |
| 공격 수행     |      |      |      | 빨강   | 빨강    |       | 파랑    | 파랑    |       |       |       |
| 결과 분석     |      |      |      |      | 빨강    | 빨강    |       | 파랑    | 파랑    |       |       |
| 보고서<br>작성 |      |      |      |      |       | 빨강    | 빨강    |       | 파랑    | 파랑    |       |
| 논문 작성     |      |      |      |      |       |       | 빨강    | 빨강    | 노랑    | 노랑    | 노랑    |

01

하나,

프로젝트 주제  
선정 목적

02

두울,

첫 번째  
주제

03

세엣,

두 번째  
주제

## 두 번째 주제 **가짜 Wi-Fi를 이용하여 사용자의 정보를 유출하는 것**

공격자가 공공 와이파이와 같은 이름을 사용하여 연결을 유도한 후  
사용자의 정보 유출하는 것을 목표

### 모의 해킹 환경

OO대학교의 교내 공공 와이파이를 가장한 환경

\*선택 이유 : 대학교 공공 와이파이에 접속한 사용자가 e-class와 같은 교내 계정에  
로그인을 시도할 가능성이 높기 때문에 대략적인 목표 대상을 정해 원하는  
해킹 목적을 달성하기 쉬울 것 같아서

## 두 번째 주제 **가짜 Wi-Fi를 이용하여 사용자의 정보를 유출하는 것**

### 목표 대상

○○대학교 학생/교직원의 교내 계정 해킹

### 해킹 목적

- 1) 탈취한 ○○대학교 학생 A의 계정으로 e-class에 업로드된 과제물 훔치기
- 2) 탈취한 ○○ 대학교 교직원 B교수의 계정으로 e-class 퀴즈 문제 훔치기
- 3) 게시판 관리자 계정으로 가짜 공지사항 등록하기 등

## 두 번째 주제 **가짜 Wi-Fi를 이용하여 사용자의 정보를 유출하는 것**

### 해킹 과정

학교 피싱 사이트를 제작 후 사용하는 과정 (또는 제작 X)

- 1) 해킹용 가짜 Wi-Fi를 생성하여 사용자가 와이파이에 접속하도록 유도
- 2) 공격자는 DNS를 변조하여 사용자가 위조된 사이트에 로그인하도록 함
- 3) 사용자는 로그인 정보를 입력
- 4) 공격자는 사용자들이 입력하는 정보들을 탈취하고, 분석(필요 시 해독)하여 ID/PW와 같은 중요 정보 탈취
- 5) 탈취한 ID/PW 정보로 교내 사이트에 접속하여 악위적인 행위(해킹 목적) 시도



## 두 번째 주제 **가짜 Wi-Fi를 이용하여 사용자의 정보를 유출하는 것**



**가짜 Wi-Fi를  
생성하는 팀1**

**가짜 피싱 사이트를  
제작하는 팀2**

## 두 번째 주제 가짜 Wi-Fi를 이용하여 사용자의 정보를 유출하는 것

[illegible]

**감사합니다!**