CISC-W'20

무선 공유기별 초기 패스워드 보안 수준 분석과 이에 따른 무선 공유기 패스워드 패턴 및 보안 수준 강화에 관한 연구

중부대학교

김종식 염정현 조재현 최예지

0. Index

01 주제 소개

1-1 배경

1-2 주제

높은 무선 AP 사용 비중,
비해 낮은 보안 수준

1.많은 공공장소에서 낮은 보안 수준의 비밀번호 사용 

2.통신사 공유기의 높은 점유율 및 기본 보안 설정 문제 존재

3.ARP Spoofing과 같은 MITM(Middle In The Man)
공격을 통한 개인정보 노출 위협 존재

1. 주제 소개 - 주제

무선 공유기별 초기 패스워드 보안 수준을 분석,
패스워드 패턴 및 보안 수준 강화 방식을 제안

02 자료 조사

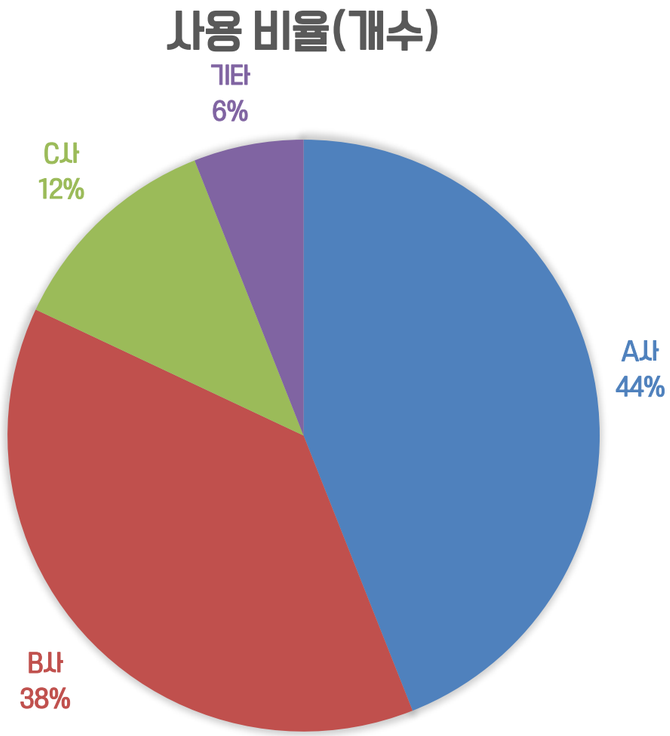
2-1 통신사 공유기 사용 비율

2-2 초기 패스워드 사용 비율

2. 자료 조사 - 통신사 공유기 사용 비율

지하철역, 카페, 학원 등 공공기관 50곳 기준 조사

높은 통신사 공유기 사용 비율 확인 가능



A사 : 22곳

B사 : 19곳

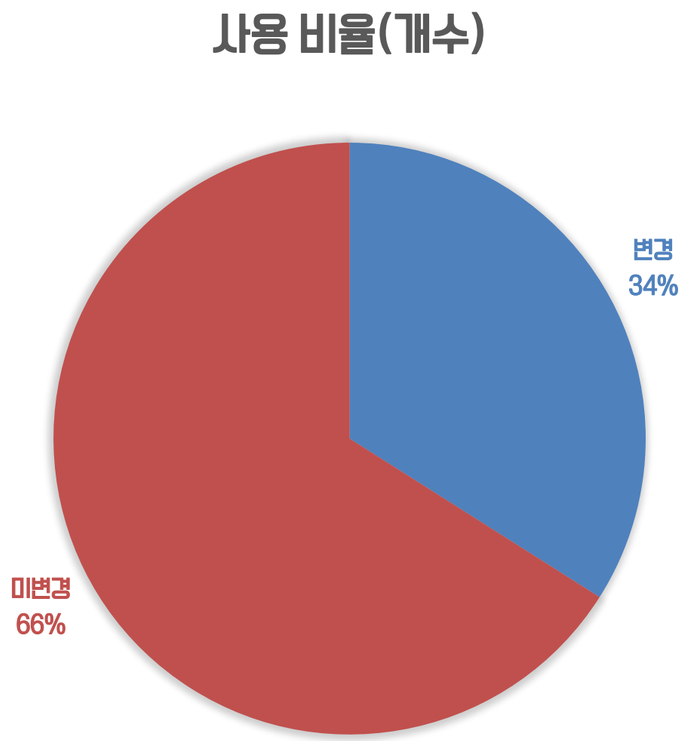
C사 : 6곳

기타 : 3곳

2. 자료 조사 - 초기 패스워드 사용 비율

지하철역, 카페, 학원 등 공공기관 50곳 기준 조사

많은 곳에서 초기 패스워드 그대로 사용



그대로 사용 : 66%

변경하여 사용 : 34%

+ 낮은 패스워드 복잡도

03 연구 과정 및 결과

3-1 패턴 분석

3-2 테스트

3-3 결과

3. 연구 과정 및 결과 - 패턴 분석

A사

* * * * * * * * * *

임의의 숫자 + 알파벳 소문자

제조번호 마지막 3자리

↓

알파벳 소문자 경우
m ~ w 범위 알파벳 사용 X

3. 연구 과정 및 결과 - 패턴 분석

B사

* * * * * * * * * *

제조번호의 숫자 10자리 그대로 사용

맨 앞자리는 대부분 1 or 2

3. 연구 과정 및 결과 - 패턴 분석

C사

* * * * * * * * * *

제조번호의 숫자 10자리 그대로 사용

맨 앞자리는 대부분 1 ~ 4

대부분 5자리는 0으로 채움

분석 결과

1. 각 AP의 초기 패스워드 패턴 존재,
   Brute-Force에 취약한 숫자만으로 된 패스워드도 사용되고 있음

2. 최소 10자리 이상, 영어 대문자, 소문자, 숫자, 특수문자 중 2종류 이상
기준에 부합하더라도 패턴 분석을 통한 Brute-Force 범위 축소 가능

3. 제품 명마다 패턴이 변할 수 있으나, SSID를 통해 구분 가능

테스트

1. 허가된 안전한 환경 구성

2. Monitor mode를 이용한 EAPOL 패킷 수집

3. Hastcat을 이용한 Brute-Force Attack 수행

시연 영상

3. 연구 과정 및 결과 - 결과

	8자리(숫자)	9자리(숫자)	10자리(숫자)	C사 (숫자/패턴존재)
GTX-1050TI	10m	2h	1d	6s
GTX-1660TI	4m	52m	10h	5s
GTX-1070	3m	45m	7.5h	5s

A사, B사의 경우 Wordlist 크기가 커 해당 테스트 대상에선 제외

04 제안

4-1 사용자

4-2 제조사

사용자의 관점

1. 사용자들의 보안 위협 인지 필요

2. AP를 보이지 않는 곳에 설치(제조 번호 노출, Reset 등 방지)

3. 초기 패스워드를 복잡도를 가진 패스워드로 변경하여 사용 등
(최소 10자리 이상의 영어 대문자, 소문자, 숫자, 특수문자 포함)

제조사(기업)의 관점

1. 초기 패스워드 변경 가능하도록 설계

2. 초기 패스워드는 복잡도를 가진 패스워드로 설정
(최소 10자리 이상의 영어 대문자, 소문자, 숫자, 특수문자 포함)

3. 설치 시 비밀번호를 꼭 변경해야 인터넷 사용 가능하도록 설계 등

Q & A