# 사이버 보안 위협에 따른 해킹 기법과 대응 방안 조사

김슬기[1], 손성호[1], 홍준기[1], 방인규[2]▪, 김태훈[1]▪

[1]국립한밭대학교 컴퓨터공학과, [2]국립한밭대학교 지능미디어공학과

{20211870, 20201773, 20191759}@edu.hanbat.ac.kr {ikbang, thkim}@hanbat.ac.kr

# Investigation of Hacking Techniques and Countermeasures against Cyber Security Threats

Seulki Kim[1], Seongho Son[1], Jungi Hong[1], Inkyu Bang[2]▪, Taehoon Kim[1]▪

[1]Dept. of Computer Engineering, Hanbat National University

[2]Dept. of Intelligence Media Engineering, Hanbat National University

요 약

무선 네트워크 기술의 발전으로 누구나 시간과 장소의 제약 없이 무선 네트워크를 통해 인터넷을 이용할 수 있다는 장점이 있으나 전파를 통신매개로 이용한다는 특성 때문에 유선 네트워크에 비해 보안성이 취약하다는 단점이 있다. 인터넷 사용률이 늘어남에 따라 무선 네트워크의 보안 위협 문제 역시 증가하고 있다. 따라서, 본 논문에서는 무선 네트워크의 공격 유형과 대응 방안을 정리하여 사이버 보안 위협에 대비하기 위한 시사점을 제시한다.

## Ⅰ. 서 론

무선 네트워크 기술의 발전으로 무선 네트워크를 이용한 와이파이, 블루투스, 셀룰러 통신, IoT 등 다양한 기술이 발전했다. 무선 네트워크 장비가 있는 곳에서는 누구든 무선 네트워크에 쉽게 연결하여 인터넷을 이용할 수 있다는 장점이 있으나, 무선 네트워크는 전파를 통신매개로 이용하기 때문에 유선 네트워크보다 보안성이 낮다는 단점이 있다.

2023년 만 3세 이상으로 국민을 대상으로 인터넷 이용 실태조사를 한 결과 국내 가구 인터넷 접속률은 99.97%, 인터넷 이용자 수는 94%, 5년간 70대 이상 고령층 인터넷 이용률이 1.7배 증가했다는 사실을 알 수 있다 [1]. 증가하는 인터넷 사용률과 더불어 무선 네트워크의 보안 문제 역시 증가하고 있다. 본 논문에서는 무선 네트워크의 공격 방식과 대응 방안에 대해 조사한 내용을 정리하며 진화하는 사이버 보안 위협에 대응하기 위한 시사점을 제시하고자 한다.

## Ⅱ. 공격 유형

### 가. 스푸핑 (Spoofing)

스푸핑은 '속이다'라는 의미로, IP 주소, DNS, ARP 등을 위조하여 비정상적인 시스템을 정상적인 시스템처럼 보이도록 속이는 공격 기법을 말한다. 대표적으로 IP 스푸핑, DNS 스푸핑, ARP 스푸핑이 있다. IP 스푸핑은 인터넷 프로토콜의 취약점을 이용한 공격으로, 인증이 없는 source IP를 위조하여 IP패킷을 전송하는 기법이다 [2]. DNS 스푸핑은 DNS 서버의 취약점을 이용해 사용자와 DNS 서버 사이에 공격자가 개입하여 가짜 IP주소를 반환하여 사용자를 속이는 행위를 말한다 [3]. ARP 스푸핑은 동일한 네트워크에 존재하는 공격 대상의 IP주소를 공격자의 랜카드 주소와 연결하여 다른 디바이스에 전송돼야 하는 정보를 가로채 가는 공격을 말한다 [4]. 위에 소개한 스푸핑 기법들은 스니핑 공격의 준비 단계로 분리되기도 한다.

### 나. 스니핑 (Sniffing)

스니핑이란 평문 데이터에 불법적으로 접근해 개인정보, 계좌정보, 아이디/비밀번호 등 데이터를 도청하는 공격이다. 이는 시스템을 직접 공격하는 것이 아니므로 소극적인 공격으로 분류된다 [5]. 스니핑을 통해 공격자는 네트워크에서 송수신기 사이에 전달되는 데이터를 모니터링하고 표 1에 나열된 정보를 캡처할 수 있다 [6].

| | |
|---|---|
| 1 | FTP(File Transfer Protocol) 비밀번호 |
| 2 | 라우터 구성 |
| 3 | 텔넷 비밀번호 |
| 4 | DNS 트래픽 |
| 5 | 이메일 트래픽 |
| 6 | 웹 트래픽 |
| 7 | 채팅 세션 |

표 1. 스니핑으로 캡처 가능한 정보

스위치 재밍은 'Fail Open' 정책을 따른다는 특징을 이용하여 맥 주소를 연속적으로 보내 스위치의 맥 주소 테이블을 가득 채운다 [7]. 테이블이 가득 찬 스위치는 더미 허브처럼 입력받은 프레임을 모든 포트에 브로드캐스트하며 공격자는 사용자의 패킷을 스니핑 할 수 있도록 한다.

ARP Redirect 공격은 위조된 ARP Reply를 네트워크에 지속적으로 브로드캐스트하여 다른 호스트들이 공격자를 수신자로 착각하도록 만들어서 모든 트래픽이 공격자를 향하도록 하여 정보를 탈취하는 공격이다 [7].

ICMP Redirect 공격은 송수신 과정에서 라우팅 경로에 문제가 생겼을 경우 최적 경로를 다시 설정해 주는 기능을 악용하여 공격자가 송신자와 수신자 사이의 라우팅 과정을 가로채서 자신을 정상적인 라우터처럼 보이도록 위장하여 공격자가 송.수신 과정을 스니핑을 하는 방법이다.[8]

### 다. DoS & DDoS

DoS(Denial of Service)는 서비스 거부 공격이라고 하며, 대량의 데이터 패킷을 전송하거나 접속 시도를 수없이 하는 등의 행위로 시스템의 리소스를 고갈시켜 서비스를 이용 못 하게 만드는 공격이다. 이보다 발전된 DDoS(Distributed DoS attack)는 여러 대의 공격자가 동시에 DoS 공격을 하는 것을 말한다.

▪ Corresponding Author: Inkyu Bang (ikbang@hanbat.ac.kr) and Taehoon Kim (thkim@hanbat.ac.kr)

Ping of Death은 과도한 ICMP 패킷으로 시스템을 마비시키는 공격을 말한다. ICMP 패킷이 방화벽에 의해 차단되지 않는다면 시스템 공격 수단으로 이용될 수 있는데, 버퍼 크기를 초과하는 핑 패킷으로 공격대상의 IP 스택을 오버플로우시킨다. TCP SYN Flooding은 3-way handshake 통신 방식의 취약점을 악용한 공격이다. 클라이언트가 다량의 SYN 패킷을 전송하면 서버는 SYN+ACK 패킷을 전송하지 못하고 서비스가 멈추게 된다. DHCP Starvation은 대량의 DHCP 요청을 보내 사용 가능한 모든 IP주소를 차지하여 DHCP 서버는 더 이상 IP주소를 발급하지 못하도록 하는 공격 방식이다 [9].

## Ⅲ. 대응 방안

### 가. 스푸핑 대응방안

IP 스푸핑은 HTTP, SSL과 같은 보안 프로토콜을 이용해서 보안을 강화하거나 패킷 필터링으로 대응할 수 있다. 수신 필터링을 진행하여 외부 공격자가 내부 시스템의 주소를 스니핑 하는 행위를 방지할 수 있다 [10].

DNS 스푸핑은 IPsec터널을 구성해 요청 및 응답을 통해 DNS 서버로 리디렉션하여 보호하거나 [11], DNS 모니터링 도구(DNSWatcher, OpenDNS)로 방지하는 방법이 있다. 또한, DNS 서버를 최신 상태로 유지해 취약점을 방어한다. ARP 스푸핑 대응책으로는 ARP 테이블에 맥 주소를 정적으로 고정하거나, ARP 패킷 변경 여부를 모니터링 하는 방법이 있다. 또 포트에 할당된 맥 주소를 하드웨어 장비로 고정하거나 ARP 패킷 암호화를 하여 공격을 막을 수 있다 [12].

### 나. 스니핑 대응방안

스니핑 공격은 소극적인 공격이기 때문에 감지하기 어렵지만, 몇 가지 대응책이 있다. 가장 효과적인 방법은 스니핑이 평문으로 된 데이터를 대상으로 진행되기에 데이터를 암호화하는 것이다. 암호화 방법으로는 SSL(Secure Sockets Layer), SSH(Secure Shell)가 있다. 이 암호화 기법들은 스니퍼를 무력화하지는 않지만, 스니퍼가 데이터를 탈취해가도 암호문으로 되어 있어 해독 할 수 없게 된다 [13].

두 번째 방법은 무차별 모드로 동작하는 스니퍼를 탐지하는데 유용한 ping을 이용한 기법이다. 스니퍼에 IP주소와 잘못된 맥 주소를 사용하여 ping 요청을 보내면, 어댑터는 이를 거부하지만 스니퍼는 다른 맥 주소의 패킷을 거부하지 않고 이에 응답하기에 스니퍼 탐지가 가능하다 [14].

세 번째 방법은 DNS를 이용하는 방법이다. 역방향 DNS 조회를 통해 IP주소로 도메인 이름을 찾을 때, 스니퍼가 이 방식을 사용한다면 네트워크 트래픽이 증가하여 스니퍼의 유무를 판단할 수 있다 [14].

마지막으로, decoy 방식이다. 스니퍼 공격자는 사용자의 계정을 도청하고 도청한 계정으로 다른 시스템을 공격하기 때문에 네트워크 상에 미리 설정된 계정을 지속적으로 흘려서 공격자가 이 계정을 사용하게 만든다. 관리자는 네트워크 감시 프로그램이나 IDS를 이용하여 미리 설정된 계정을 사용하는 시스템을 탐지하여 스니퍼를 탐지할 수 있게 된다 [7].

### 다. DoS & DDoS 대응방안

DoS 공격 방어 방법은 다음과 같다. 라우터의 Unicast RPF 기능으로 패킷의 출발지 주소를 확인하고, 허용되지 않은 경로에서 온 패킷을 폐기해 위조된 패킷을 차단한다. 그리고, TCP 차단으로 SYN Flooding 공격을 막는다. 또, TCG에서 발표한 TPM 규격으로 무작위 번호를 생성하여 등록된 클라이언트만 서버에 접근하도록 한다. 마지막으로, VPN과 같은 인증 시스템을 사용해 방어한다 [15].

## Ⅳ. 결 론

본 논문에서는 무선 네트워크 기술의 발달함에 따라 증가하는 사이버 위협에 대비하기 위해 스푸핑, 스니핑, DoS 공격을 중심으로 특징과 대응 방안에 대해 살펴보았다. 그러나 이러한 공격 방식 이외에도 다양한 종류의 위협이 존재하며, 기술과 함께 사이버 보안 위협 역시 진화하고 있어 새로운 공격 기법들이 계속해서 등장할 것이다.

이러한 사이버 공격에 대비하지 않는다면 해킹 공격으로 인한 개인 정보 유출, 금전적인 손해 등 다양한 피해가 일어날 것으로 예상되기에 현재 존재하는 공격 유형을 파악하고, 이에 적합한 대응 전략을 수립하여 보안 체계를 강화하는 것이 중요하다.


## ACKNOWLEDGMENT

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음(2022-0-01068)


## 참 고 문 헌


[1] 2023년 인터넷이용실태조사 요약보고서, 정보통신기획평가원.

[2] A. Mukaddam, I. Elhajj, A. Kayssi and A. Chehab, "IP Spoofing Detection Using Modified Hop Count," 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, pp. 512-516, 2014

[3] DNS 스푸핑을 이용한 포털 해킹과 파밍의 위험성, 최재원, 한국정보통신학회논문지 Vol.23, No. 11: 1451~1461, Nov. 2019

[4] 서초롱, "IoT 환경에서의 CoAP을 이용한 ARP Spoofing 공격 시나리오 및 대응방안," 한국융합학회논문지 제7권 제4호, 2016

[5] 최재영, "암호화 기반의 스니핑 및 세션하이재킹 공격 대응 모델," 경상대학교 박사학위논문, 2017

[6] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017

[7] 홍성혁, "효율적인 Sniffing 공격 대응방안 연구," 중소기업융합학회 논문지 제6권 제2호 pp. 31-36, 2016.

[8] Jae-Yeong Choi, "The Responding Model for Sniffing and Session HijackingUsing Traffic Variation Information and RST Signal Analysis," JKITS, vol.12, no.3, pp. 439-446, 2017

[9] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017

[10] C. Manusankar, S. Karthik and T. Rajendran, "Intrusion Detection System with packet filtering for IP Spoofing," 2010 International Conference on Communication and Computational Intelligence (INCOCCI), Erode, India, 2010, pp. 563-567.

[11] A. A. Maksutov, I. A. Cherepanov and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," 2017 Siberian Symposium on Data Science and Engineering (SSDSE), Novosibirsk, Russia, pp. 84-87, 2017

[12] 홍승표, "신뢰적인 ARP 테이블 운영을 통한 효율적인 ARP Spoofing 공격 방어 기법," 국내석사학위논문 숭실대학교 대학원, 2012.

[13] S. Ansari, S. G. Rajeev, "Packet sniffing: a brief introduction," in IEEE Potentials, vol. 21, no. 5, pp. 17-19, Dec. 2002-Jan. 2003

[14] Ruchi Tuli, "Packet Sniffing and Sniffing Detection," IJIET, Volume 16 Issue 1 April 2020.

[15] Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," 2011 International Conference on Intelligence Science and Information Engineering, Wuhan, China, pp. 426-429, 2011