JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 5, pp. 809-816, May. 2021

Check for updates

ARP 스푸핑 툴 기반의 포이즈닝 공격 탐지 및 차단 모델

최 준 호[1] · 백 용 진[1] · 서 영 건[2*]
[1]경상대학교 컴퓨터과학과 대학원생, [2*]경상대학교 컴퓨터과학과 교수

Poisoning Attack detection and blocking model based on ARP Spoofing tool

Jun-Ho Choi[1] · Yong-Jin Baek[1] · Yeong-Geon Seo[2*]

[1]Graduate School Student, Department of Computer Science, Gyeongsang National University, 501 Jinju-daero, Jinju, Gyeongnam, Korea
[2*]Professor, Department of Computer Science, Gyeongsang National University, 501 Jinju-daero, Jinju, Gyeongnam, Korea

[요 약]

오늘날 네트워크 환경은 일반 사용자들도 자신이 필요로 하는 정보에 쉽게 접근한 후 서비스를 받을 수 있는 환경으로 빠르게 발전하고 있다. 그렇지만 이러한 네트워크에 대한 의존도는 관련 보안 문제도 함께 발생시키고 있는 상황이다. 네트워크를 기반으로 하는 보안 사고에는 다양한 문제점들이 존재하고 있는데, 그중 ARP 기반의 공격 기법은 해당 취약점이 발견된 이후 최근까지도 피해 사례가 꾸준히 증가하고 있다. ARP 포이즈닝은 공격 대상 시스템으로 비정상적인 ARP 응답 패킷을 반복적으로 전송한 후 이를 이용하여 ARP 캐시 테이블 정보를 변경시키는 공격이다. 그다음 공격 대상 시스템에 대해 불법적인 접근을 시도한 후 스니핑 공격을 하는 것이다. 본 논문은 ARP 포이즈닝에 대해 실질적으로 그 공격 과정을 보인 다음 이를 방어할 수 있는 기법을 제안하고 있다. 이를 위해 ARP 포이즈닝 공격 패턴을 분석하고 해당 신호의 응답 시간에 대한 오차 범위를 분석한 자료를 기반으로 ARP 포이즈닝 공격을 탐지하고 이를 차단하도록 하였다.

[Abstract]

Today, the network environment is rapidly evolving into an environment where end users can easily access the information they need and then receive services. However, this dependence on the network is also causing related security issues. There are various problems with network-based security incidents, among which ARP-based attack techniques have steadily increased the number of damage cases since the vulnerability was discovered. ARP Poising is an attack that repeatedly sends abnormal ARP response packets to the target system and then exploits them to change ARP cache table information. Then, attempt an illegal access to the target system and then make a sniffing attack. This paper proposes a technique that can substantially demonstrate its attack process against ARP Poising and then defend it. To this end, we analyze ARP poising attack patterns and detect and block ARP poising attacks based on the data that analyzed the error range for the response time of the corresponding signal.

색인어 : ARP, ARP 스푸핑, ARP 포이즈닝, 스니핑, 접근시간
Key word : ARP, ARP Spoofing, ARP Poisoning, Sniffing, Reach Time

http://dx.doi.org/10.9728/dcs.2021.22.5.809

Received 16 April 2021; **Revised** 10 May 2021
Accepted 10 May 2021

***Corresponding Author; Yeong-Geon Seo**

Tel: ※ 개인정보 표시제한
E-mail: young@gnu.ac.kr

Ⅰ. 서 론

오늘날 네트워크 환경은 일반 사용자들도 자신이 필요로 하는 정보에 쉽게 접근한 후 서비스를 받을 수 있는 환경으로 빠르게 발전하고 있다. 그렇지만 이러한 네트워크에 대한 의존도는 관련 보안 문제도 함께 발생시키는 상황이다. 네트워크를 기반으로 하는 보안 사고에는 다양한 문제점들이 존재하고 있는데 대표적인 공격 기법으로는 서비스 거부 공격(DoS), 스니핑(Sniffing), 스푸핑(Spoofing), 포이즈닝(Poisioning), 세션 하이재킹(Session hijacking) 등 수많은 공격 기법들이 있으며, 이러한 기법들은 조직 및 개인에게 치명적인 피해를 발생시킨다. 또한 ARP 스푸핑 공격 기법은 더미 허브 환경뿐만 아니라 스위치 환경에서도 스니핑 공격이 가능하다. 하지만 우리나라는 스위치 환경에서는 스니핑 공격에 대해 안전하다고 생각하고 있다. 대표적으로 중국 등 해외 여러 나라에서는 자동화와 고도화된 툴이 제작되어 무단 배포되고 있다. 그러나 우리나라는 현 문제에 대해 큰 인식을 못 하고 있으며 이러한 인식은 보안 사고 발생의 가능성을 높이고 있다. 그중에서 ARP(Address Resolution Protocol) [1]는 1982년부터 취약점이 발견됐지만 근 40년이 지난 최근에도 ARP 스푸핑을 이용한 피해사례들이 발생하고 있는 현실이다. 이러한 보안 위협에 대하여 오랜 기간 동안 많은 연구들이 진행되었지만, 고가의 장비가 필요하여 특정 기관에만 설치하고 운영되고, 새로운 프로토콜[2], [3]의 제안, Client-Agent와 MAC-Agent[4], Static Table[5]의 생성과 관리, 현 네트워크 체계에 적용하는데 실현 가능성이 작거나 한계점이 존재하였다. 이에 본 논문에서는 ARP 포이즈닝 공격 과정을 보인 다음 이를 방어할 수 있는 기법을 제안하고 있다. 즉, ARP 포이즈닝 공격은 비정상적인 ARP 응답 패킷을 공격 대상에게 반복적으로 전송하여 ARP 캐시 테이블 정보를 변경시킨다. 이러한 과정에서 ARP 응답 패킷에 대해 발생 시간을 기록하고 반복적으로 발생하는 ARP 응답 패킷의 도달 시간들의 평균값과 도달 시간의 오차 범위를 분석한 자료를 기반으로 ARP 포이즈닝 공격을 탐지하고 이를 차단하도록 하였다.

Ⅱ. 배경지식

2-1 ARP 스푸핑 & ARP Poisoning

ARP은 RFC 826[1]에서 정의한 바와 같이 네트워크 계층 주소(IP 주소)를 데이터 링크 계층 주소(MAC 주소)로 대응시키기 위해 사용되는 프로토콜이다. 스푸핑은 '속이다'라는 의미를 가지며, ARP 스푸핑은 ARP 메시지의 무결성 검증이 보증되지 않은 점을 이용하여 조작된 ARP 응답 패킷을 타깃(target)에 보내 MAC 주소를 속여 정상적인 서비스를 방해하는 공격방식이다. ARP 포이즈닝은 비정상적인 ARP 응답 패킷을 반복적으로 타깃에 전송한다. 그림 1과 그림 2에서 Host(1)의 IP 주소는 '0.0.0.1' MAC 주소는 'AA.AA', Host(2)의 IP 주소는 '0.0.0.2' MAC 주소는 'BB.BB', 공격자의 IP 주소는 '0.0.0.3' MAC 주소는 'CC.CC' 라고 가정한다.

그림 1은 ARP 스푸핑 공격이 일어나기 전 정상적인 통신의 흐름을 나타낸 그림이다. Host(1)에서 Host(2)로 통신을 시도할 때 MAC 주소가 필요하며, 이때 IP 주소 '0.0.0.2'를 가지고 있는 Host를 찾기 위해 ARP 요청 메시지를 Broadcasting 방식으로 전달한다. IP 주소 '0.0.0.2'를 가지고 있는 Host(2)는 ARP 응답 메시지를 Host(1)에게 전달해 자신의 MAC 주소 정보를 알려준다. 이후 ARP 캐시 테이블을 이용하여 Host(1)와 Host(2)는 정상적인 통신 과정을 수행하며, 그림 2는 ARP 스푸핑 공격이 발생한 후의 통신 흐름을 나타낸 그림이다.

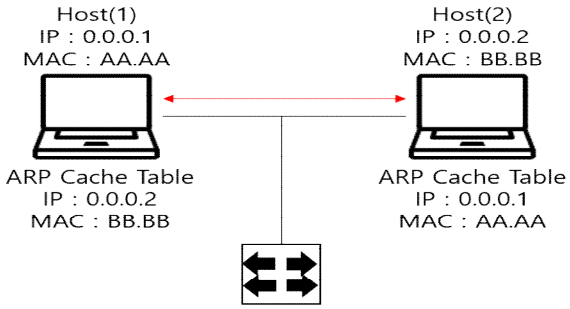

그림 1. ARP 스푸핑 전 통신 과정
Fig. 1. Communication process before ARP Spoofing

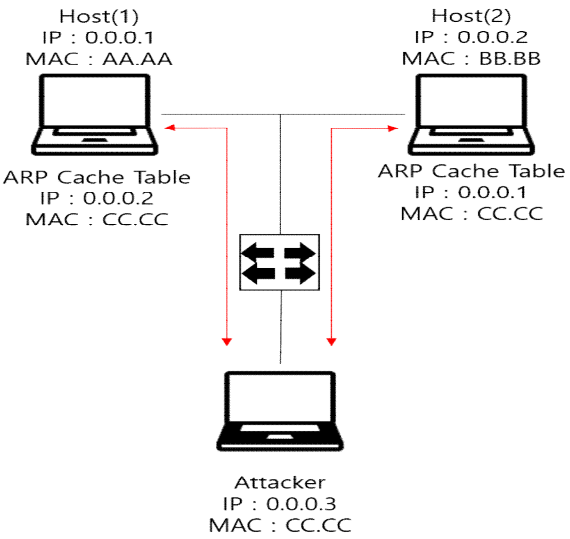

그림 2. ARP 스푸핑 후 통신 과정
Fig. 2. Communication process after ARP Spoofing

그림 1 과정 중 Host의 MAC 주소를 찾기 위해 ARP 요청 메시지를 Broadcasting 하게 된다. 이때 공격자는 Host(1)에게는 Host(2)의 MAC 주소가 'CC.CC'라고 속이고 Host(2)에게는 Host(1)의 MAC 주소가 'CC.CC'라고 속인다. 결과적으로 Host(1)와 Host(2)는 서로 정상적인 통신을 하는 것처럼 보이지만 사실은 공격자와 통신을 하며, 공격자에게 정보를 유출하는 결과가 발생한다.

2-2 스니핑

네트워크 상에서 송신자와 수신자가 주고받는 중간에서 패킷을 도청하는 것을 의미하며, 스니퍼(Sniffer) 프로그램을 사용하여 스니핑이 가능하다. 더미 허브 환경에서는 NIC(Network Interface Card)를 Promiscuous Mode로 설정하여 스니핑이 가능하며, 스위치 환경에서는 모니터링 포트를 사용하거나 스위치 재밍 혹은 스푸핑 공격을 사용하면 스니핑 공격이 가능하다. 앞서 언급한 ARP 스푸핑 공격은 스니핑 공격의 가장 기본으로 활용되고 있다.

2-3 SARP 외 다른 공격

SARP(Secure ARP)은 ARP 요청에 대해 어떤 인증 절차도 수행하지 않고 ARP 응답 패킷을 수신하는 문제점에 대해 제안되었으며, ARP 응답 패킷을 수신하는 과정에 인증 절차를 추가하여 새롭게 정의한 프로토콜이다[2].

Server Agent & Client Agent는 MAC 주소를 관리하는 MAC Agent와 ARP 테이블의 변조를 막는 Client Agent를 설치하여 MAC 주소를 ARP 테이블에 자동으로 갱신하는 방법이다[4].

시큐어 LAN의 구조와 프로토콜은 현 네트워크 체계에서 사용 중인 ARP를 사용하지 않고 ARP 테이블을 유지하기 위해 데이터베이스로 사용할 DHCP 서버를 구축해 정적인 ARP 테이블을 관리하여 ARP 스푸핑 공격을 방어하는 방법을 제안한다[5].

Ⅲ. 포이즈닝 공격 탐지 및 차단 모델

3-1 제안 모델

본 논문에서는 ARP 포이즈닝 공격을 탐지하기 위해 ARP 패킷 컨트롤러를 사용하였으며, 제안 모델 동작 과정을 구성하는 정보 구조는 표 1과 같다. 표 1의 SP_MAC은 Starting Point MAC Address의 약어이며, ARP 응답 패킷의 출발지 MAC 주소를 의미한다. TP_MAC은 Temporary Point MAC Address의 약어이며, SP_MAC의 정보를 임시로 저장해 놓기 위함으로 사용한다. RSP_MAC은 Re-receiving Starting Point MAC Address의 약어이며, SP_MAC과 동일하게 ARP 응답 패킷의 출발지를 정보를 담고 있는 재수신 된 ARP 응답 패킷이다.

표 1. 제안 모델의 약어와 의미
Table 1. Abbreviations and their meaning of the proposed model

Abbreviations	Meaning
SP_MAC	Starting Point
TP_MAC	Temporary Point
RSP_MAC	Re-receiving Starting Point
OT	Occurrence Time
RT	Reach Time
RT_Avg	Divide Full Reach Time

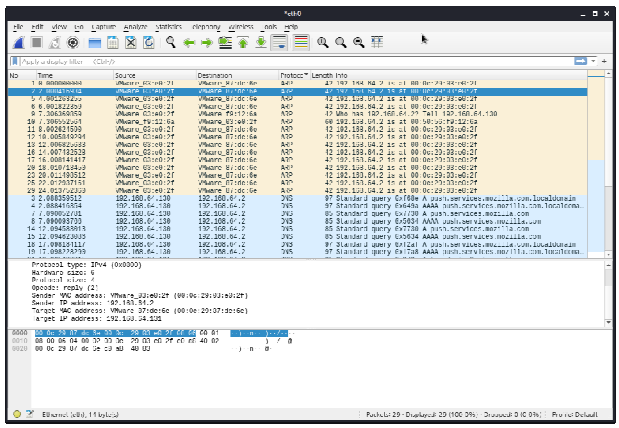

그림 3. Wireshark를 이용한 arpspoof 툴의 ARP 패킷 분석
Fig. 3. ARP Packet analysis of arpspoof tool using Wireshark

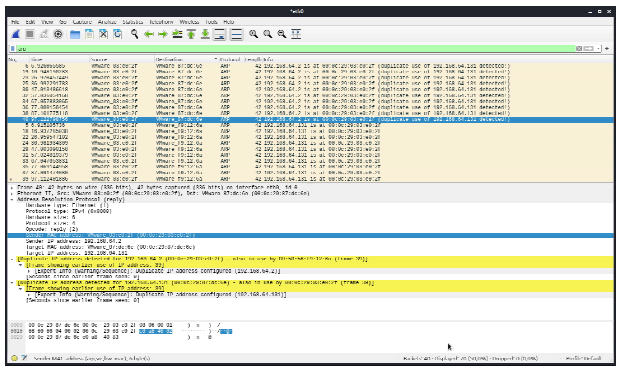

그림 4. Wireshark를 이용한 ettercap 툴의 ARP 패킷 분석
Fig. 4. ARP Packet analysis of ettercap tool using Wireshark

OT는 Occurrence Time의 약어이며, ARP 응답 패킷의 발생 시간을 기록하고 있다. RT는 Reach Time의 약어이며, ARP 응답 패킷의 발생 시간을 기록하는 OT부터 다음 재수신되는 ARP 응답 패킷의 OT까지의 도달 시간을 의미한다. RT_Avg는 Divide Full Reach Time을 의미하며, OT부터 다음 OT까지의 도달 시간을 기록하는 RT의 평균값을 의미한다. 그림 3은 arpspoof 툴(Tool)을 이용하여 ARP 포이즈닝 공격을 하였을 때, 와이어샤크를 통해 ARP 응답 패킷을 분석한 그림이다. 분석한 결과에 대해서는 표 2에 나타내었으며, 그림 4와 표 3은 ettercap 툴을 그림 3과 동일하게 ARP 포이즈닝 공격을 하였을 때 분석을 한 결과이다. 분석 결과와 같이 ARP 포이즈닝 공격을 시도하면 비정상적인 ARP 응답 패킷이 지속해서 타깃에 전송되며, 타깃 PC의 ARP 캐시 테이블의 내용 변조가 일어난다. ARP 캐시 테이블의 변조가 발생하면 스니핑 공격이 가능하게 되어 타깃의 ID, PW 등 개인 정보들이 공격자에게 노출되는 문제가 발생한다. 이러한 문제를 방지하고자 본 논문에서 제안하는 모델의 동작 과정을 그림 5로 도식화 하였으며, ARP 응답 패킷이 발생하면 다음과 같은 과정을 수행한다.

STEP 1. ARP Packet Controller에게 ARP Reply Packet을 전송한다.
STEP 2. ARP Packet Controller는 ARP Reply Packet의 출발지 MAC Address와 ARP Cache Table의 MAC Address를 비교하는 과정을 수행한다.
. 2-1 두 개의 MAC Address가 동일한 경우 Normal ARP Reply로 판단한다.
. 2-2 두 개의 MAC Address가 동일하지 않다면 STEP 3 과정을 수행한다.
STEP 3. Packet의 Occurrence Time을 기록하기 위해 Timer를 실행한다.
STEP 4. TP_MAC[a]에 SP_MAC과 OT를 저장한다.
STEP 5. Timer가 종료되기 전 NEW ARP Reply를 확인하는 과정을 수행한다.
. 5-1 NEW ARP Reply Packet을 수신한다면 STEP 6 과정을 수행한다.
. 5-2 NEW ARP Reply Packet을 수신하지 못한다면 Timer를 종료시킨다.
STEP 6. 재수신된 ARP Reply Packet의 MAC Address와 TP_MAC[a]의 MAC Address를 비교하는 과정을 수행한다.
. 6-1 두 개의 MAC Address가 동일한 경우 STEP 7 과정을 수행한다.
. 6-2 두 개의 MAC Address가 동일하지 않다면 Normal ARP Reply로 판단한다.
STEP 7. STEP 4 과정에서 TP_MAC[a]에 저장한 내용을 훼손하지 않기 위해 다음 배열인 TP_MAC[a+1]에 RSP_MAC과 OT를 저장한다.
STEP 8. TP_MAC[a]과 TP_MAC[a+1]에 기록된 OT를 이용하여 TP_MAC[a]에서 TP_MAC[a+1]까지의 Reach Time을 구하기 위해 TP_MAC[a]의 OT와 TP_MAC[a+1]의 OT를 서로 뺀 후 절댓값을 취하여 Reach Time을 구한다.
STEP 9. Reach Time의 평균을 구하기 위해 Reach Time의 개수를 비교하는 과정을 수행한다.
. 9-1 RT의 개수가 2개 이상이면 STEP 10 과정을 수행한다.
. 9-2 RT의 개수가 2개 미만이면 STEP 5 과정을 수행한다.
STEP 10. RT_Avg를 구하기 위해 전체 Reach Time의 평균값을 구하는 과정을 수행한다.
STEP 11. 정상적인 ARP Reply Packet과 비정상적인 ARP Reply Packet을 구분하기 위해 RT_Avg를 100% 기준으로 두고 RT를 %로 변환시킨다.
STEP 12. 변환된 RT의 Error Range가 1%를 초과하는지 비교한다.
. 12-1 RT의 Error Range가 1% 미만이면 STEP 13 과정을 수행한다.
. 12-2 RT의 Error Range가 1% 이상이면 STEP 5 과정을 수행한다.
STEP 13. 일정하고 반복적인 ARP Reply Packet이며, ARP Poisoning 공격으로 판단하여 RT를 구하기 위해 사용되었던 ARP Reply Packet의 MAC Address를 확인하여 Switch Port를 차단한다.

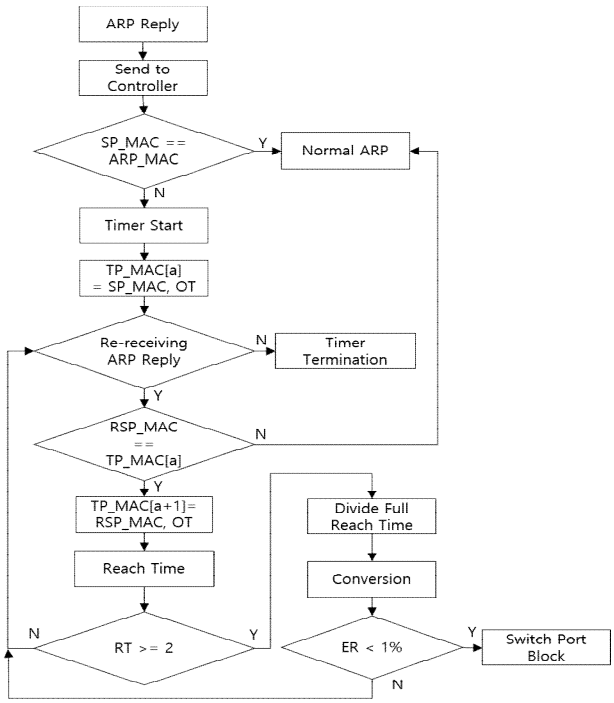

그림 5. 제안 모델 동작 과정
Fig. 5. Executing process of the proposed model

Ⅳ. 실험 및 평가

본 연구에서 제안하는 도달 시간을 이용한 ARP 포이즈닝 공격 탐지를 위한 시뮬레이션 환경은 다음과 같다. 공격자 시스템은 Kali Linux 운영체제를 사용하였고, 타깃 시스템의 운영체제는 Window 10, 서버의 운영체제는 CentOS 7을 사용하였다. ARP 포이즈닝 공격을 위한 해킹 툴은 해킹 툴로써 많이 사용되고 있는 arpspoof 와 ethercap 프로그램을 사용하였고, 실험에서 ARP 응답 패킷을 분석하기 위한 프로그램으로는 WireShark 3.4.3을 사용하였다. 그림 6은 ARP 포이즈닝 공격 전의 타깃 PC의 ARP 캐시 테이블을 보여준다. 여기서 '203.255.3.1'은 게이트웨이, '203.255.3.72'는 서버, '203.255.3.240'은 공격자이다.

일반적인 네트워크 환경에서 ARP 해킹 툴을 사용하여 타깃 PC를 공격하면 그림 7과 같이 '203.255.3.1'의 게이트웨이의 MAC 주소(00-00-0c-9f-f0-03)가 '203.255.3.240' 공격자 PC의 MAC 주소(10-05-01-4d-86-01)로 변경된 타깃 PC의 ARP 캐시 테이블의 정보가 변경된 것을 볼 수 있다.

그림 8은 ARP 해킹 툴을 사용하여 타깃 PC를 공격한 결과이다. 서버의 MAC 주소(00-e0-91-54-4c-ad)가 공격자 PC의 MAC 주소(10-05-01-4d-86-01)로 변경된 ARP 캐시 테이블을 확인할 수 있다.

그림 9는 ARP 포이즈닝 공격 전 서버의 ARP 캐시 테이블이며, 그림 10은 ARP 해킹 툴을 사용하여 서버 PC를 공격한 결과이다. 그림 10을 보게 되면 타깃 PC의 MAC 주소(00-d8-61-9b-c9-48)가 공격자 PC의 MAC 주소 (10-05-01-4d-86-01)로 변경된 ARP 캐시 테이블을 확인할 수 있다.

```
Interface: 203.255.3.90 --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           00-00-0c-9f-f0-03     dynamic
  203.255.3.3           00-de-fb-84-d4-43     dynamic
  203.255.3.4           00-3a-9c-ba-e9-c3     dynamic
  203.255.3.41          da-08-40-11-19-6c     dynamic
  203.255.3.51          8c-89-a5-2d-6f-8a     dynamic
  203.255.3.72          00-e0-91-54-4c-ad     dynamic
  203.255.3.91          00-0c-29-3a-38-66     dynamic
  203.255.3.115         34-9f-7b-a5-4c-b4     dynamic
  203.255.3.116         24-4b-fe-7e-37-b2     dynamic
  203.255.3.140         2c-f0-5d-d4-63-10     dynamic
  203.255.3.142         30-cd-a7-27-92-0b     dynamic
  203.255.3.180         e0-d5-5e-14-95-14     dynamic
  203.255.3.223         84-25-19-b1-ca-67     dynamic
  203.255.3.232         72-3c-56-fe-66-ad     dynamic
  203.255.3.240         10-05-01-4d-86-01     dynamic
  203.255.3.241         e8-03-9a-6b-ba-26     dynamic
  203.255.3.255         ff-ff-ff-ff-ff-ff     static
```

그림 6. ARP 포이즈닝 공격 전의 타깃 PC의 ARP 캐시 테이블
Fig. 6. ARP cache table of the target PC before ARP poisoning attack

```
Interface: 203.255.3.90 --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           10-05-01-4d-86-01     dynamic
  203.255.3.3           00-de-fb-84-d4-43     dynamic
  203.255.3.4           00-3a-9c-ba-e9-c3     dynamic
  203.255.3.41          da-08-40-11-19-6c     dynamic
  203.255.3.51          8c-89-a5-2d-6f-8a     dynamic
  203.255.3.72          00-e0-91-54-4c-ad     dynamic
  203.255.3.91          00-0c-29-3a-38-66     dynamic
  203.255.3.115         34-9f-7b-a5-4c-b4     dynamic
  203.255.3.116         24-4b-fe-7e-37-b2     dynamic
  203.255.3.140         2c-f0-5d-d4-63-10     dynamic
  203.255.3.142         30-cd-a7-27-92-0b     dynamic
  203.255.3.180         e0-d5-5e-14-95-14     dynamic
  203.255.3.223         84-25-19-b1-ca-67     dynamic
  203.255.3.232         72-3c-56-fe-66-ad     dynamic
  203.255.3.240         10-05-01-4d-86-01     dynamic
  203.255.3.241         e8-03-9a-6b-ba-26     dynamic
  203.255.3.255         ff-ff-ff-ff-ff-ff     static
```

그림 7. 게이트웨이를 대상으로 ARP 포이즈닝 공격 후의 타깃 PC의 ARP 캐시 테이블
Fig. 7. ARP cache table of the target PC after ARP poisoning attack aiming at the gateway

```
Interface: 203.255.3.90 --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           00-00-0c-9f-f0-03     dynamic
  203.255.3.3           00-de-fb-84-d4-43     dynamic
  203.255.3.4           00-3a-9c-ba-e9-c3     dynamic
  203.255.3.41          da-08-40-11-19-6c     dynamic
  203.255.3.51          8c-89-a5-2d-6f-8a     dynamic
  203.255.3.72          10-05-01-4d-86-01     dynamic
  203.255.3.91          00-0c-29-3a-38-66     dynamic
  203.255.3.115         34-9f-7b-a5-4c-b4     dynamic
  203.255.3.116         24-4b-fe-7e-37-b2     dynamic
  203.255.3.140         2c-f0-5d-d4-63-10     dynamic
  203.255.3.142         30-cd-a7-27-92-0b     dynamic
  203.255.3.180         e0-d5-5e-14-95-14     dynamic
  203.255.3.223         84-25-19-b1-ca-67     dynamic
  203.255.3.232         72-3c-56-fe-66-ad     dynamic
  203.255.3.240         10-05-01-4d-86-01     dynamic
  203.255.3.241         e8-03-9a-6b-ba-26     dynamic
  203.255.3.255         ff-ff-ff-ff-ff-ff     static
```

그림 8. 서버를 대상으로 ARP 포이즈닝 공격 후의 타깃 PC의 ARP 캐시 테이블
Fig. 8. ARP cache table of the target PC after ARP poisoning attack aiming at the server

```
[junho@localhost ~]$ arp
Address                  HWtype  HWaddress
class.gnu.ac.kr          ether   72:3c:56:fe:66:ad
203.255.3.180            ether   e0:d5:5e:14:95:14
203.255.3.239            ether   00:e0:4c:36:05:37
203.255.3.3              ether   00:de:fb:84:d4:43
203.255.3.54             ether   52:11:d8:cf:64:c3
203.255.3.238            ether   90:9f:33:e3:55:81
gateway                  ether   00:00:0c:9f:f0:03
203.255.3.90             ether   00:d8:61:9b:c9:48
```

그림 9. ARP 포이즈닝 공격 전의 서버 PC의 ARP 캐시 테이블
Fig. 9. ARP cache table of the server PC before ARP poisoning attack

```
[junho@localhost ~]$ arp
Address                  HWtype  HWaddress
203.255.3.240            ether   10:05:01:4d:86:01
class.gnu.ac.kr          ether   72:3c:56:fe:66:ad
203.255.3.180            ether   e0:d5:5e:14:95:14
203.255.3.239            ether   00:e0:4c:36:05:37
203.255.3.3              ether   00:de:fb:84:d4:43
203.255.3.54             ether   52:11:d8:cf:64:c3
203.255.3.238            ether   90:9f:33:e3:55:81
gateway                  ether   00:00:0c:9f:f0:03
203.255.3.90             ether   10:05:01:4d:86:01
```

그림 10. ARP 포이즈닝 공격 후의 서버 PC의 ARP 캐시 테이블
Fig. 10. ARP cache table of the server PC after ARP poisoning attack

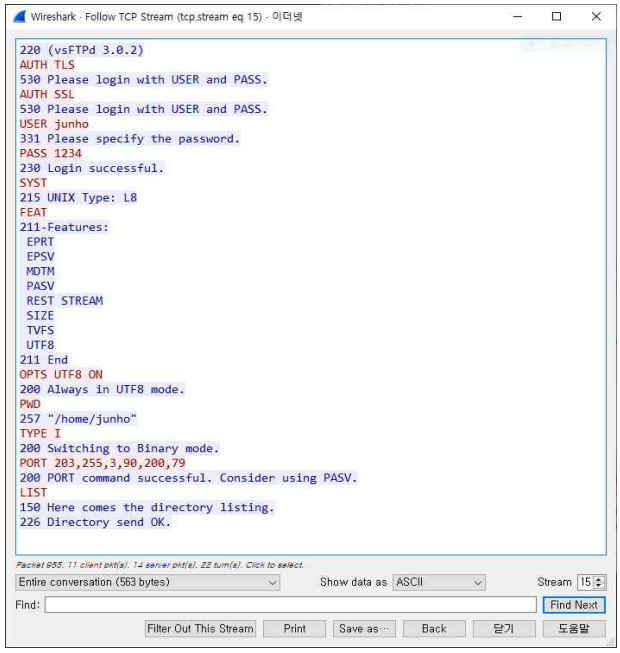

그림 11. ARP 포이즈닝 공격 후 패킷 스니핑
Fig. 11. Packet sniffing after ARP poisoning attack

위와 같은 과정의 공격을 진행한 후 패킷을 스니핑 하게 된다면 그림 11과 같이 서버에 접속하기 위해 로그인 과정을 진행하였던 사용자의 'ID : junho'와 'PW : 1234'를 볼 수 있게 되고, 공격자의 공격으로 인하여 정보가 노출되는 문제점을 확인할 수 있다.

자동화된 툴을 사용하게 되면 타깃 PC의 ARP 캐시 테이블 변조를 위해 동일한 내용을 담은 위조된 패킷이 반복적으로 발생하

게 된다. 이때 패킷의 발생 시간(Occurrence Time)을 기록하여 n번째 패킷의 발생 시간에서 n+1번째 패킷의 발생 시간까지의 도달 시간(Reach Time)을 계산한 결과를 표 2와 표 3에 도출하였다.

표 2. arpspoof 툴의 Occurrence Time을 이용한 Reach Time
Table 2. Reach time using occurrence time of arpspoof

Packet(n)	Occurrence Time (s)	Reach Time (n -> n+1(s))
1	0.000000000	2.000416934
2	2.000416934	2.000846321
3	4.001263255	2.000559104
4	6.001822359	2.000802231
5	8.002624590	2.003224704
6	10.005849294	2.000976339
7	12.006825633	2.000606895
8	14.007432528	2.000708889
9	16.008141417	2.002572033
10	18.010713450	

표 3. ettercap 툴의 Occurrence Time을 이용한 Reach Time
Table 3. Reach time using occurrence time of ettercap

Packet(n)	Occurrence Time (s)	Reach Time (n -> n+1(s))
1	6.926065585	10.022124698
2	16.948190283	10.022267166
3	26.970457449	10.021834334
4	36.992291783	10.021194835
5	47.013486618	10.022567550
6	57.036054168	10.021828897
7	67.057883065	10.022275389
8	77.080158454	10.021616664
9	87.101775118	10.021023638
10	97.122798756	

표 4와 표 5에서 사용되는 RT_Avg(1~2)의 의미는 1번째 도달 시간의 값부터 2번째 도달 시간의 값을 의미하고 RT_Avg(1~2) 아래의 적힌 값은 1~2까지의 도달 시간의 평균값을 의미하며, 평균값은 100%의 기준값이 된다. 도달 시간의 개수가 2개 이상이면 도달 시간의 RT_Avg를 구하여 100%의 기준값으로 두고 n개의 도달 시간들을 RT_Avg 값에 대응 시켜 변환시킨다. 변환된 도달 시간들은 RT_Avg와 비교하여 오차 범위가 1% 미만인 것을 확인할 수 있다. 오차 범위가 1%를 넘지 않는 이유는 원활한 스니핑을 하기 위해 공격자는 조작된 ARP 패킷을 지속적으로 타깃 PC에 전송하여 타깃 PC의 ARP 테이블 내용 변조를 해야 한다. 이때 수동적으로 조작된 ARP 패킷을 전송하게 되면 타깃 PC의 ARP 테이블 내용 변조가 원활하지 않아 스니핑 공격이 어려워지게 되고 원활한 스니핑 공격을 위해서 자동화 툴을 사용해 조작된 ARP 패킷 전송을 하게 된다. 하지만 이러한 자동화 툴은 조작된 ARP 패킷을 전송하는 과정에서 일정한 시간 주기를 가지고 조작된 ARP 패킷을 전송하게 된다. 본 논문에서 제안하는 모델은 반복적으로 수신되는 ARP 패킷에 대해 오차 범위가 1% 미만이 일 때 일정하고 반복적인 비정상적인 ARP 응답 패킷인 것을 확인할 수 있으며, ARP 포이즈닝 공격으로 판단해 해당 MAC 주소를 가진 PC의 포트를 차단한다. 아래의 그림 12는 ARP 포이즈닝 공격을 판단하기 전의 정상적인 스위치의 MAC 주소 테이블이다.

그림 12에서 MAC 주소 (0000.0c9f.f003) 포트 'Fa0/24'는 게이트웨이이고, MAC 주소 (00d8.619b.c948) 포트 'Fa0/1'는 타깃 PC, MAC 주소 (1005.014d.8601) 포트 'Fa0/2'는 공격자 PC, MAC 주소 (00e0.9154.4cad) 포트 'Fa0/3'은 서버 PC이다.

표 4. arpspoof Tool의 도달 시간의 개수에 따른 평균값과 평균값에 의한 도달 시간의 변환
Table 4. Average according to the number of arrival times and conversion of arrival time by average of arpspoof

Reach Time (s)	RT_Avg(1~2) [2.000941098][100%]	RT_Avg(1~5) [2.000732483]	RT_Avg(1~9) [2.000678332][100%]
2.000416934	99.98926871409%	99.96237576752%	99.96135053717%
2.000846321	100.01073128591%	99.98383256681%	99.98280711639%
2.000559104		99.96948011198%	99.96845480877%
2.000802231		99.98162935553%	99.98060392771%
2.003224704		100.10268219816%	100.10165552881%
2.000976339			99.98930414941%
2.000606895			99.97084293737%
2.000708889			99.97593960388%
2.002572033			100.06904139047%

표 5. ettercap Tool의 도달 시간의 개수에 따른 평균값과 평균값에 의한 도달 시간의 변환
Table 5. Average according to the number of arrival times and conversion of arrival time by average of ettercap

Reach Time (s)	RT_Avg(1~2) [10.022195932][100%]	RT_Avg(1~5) [10.0219977166][100%]	RT_Avg(1~9) [10.02185924122222][100%]
10.022124698	99.9992892376 %	100.00126702683 %	100.00264877775 %
10.022267166	100.0007107624 %	100.00268857974 %	100.0040703503 %
10.021834334		99.99836976016 %	99.99975147104 %
10.021194835		99.9919888068 %	99.99337042952 %
10.022567550		100.00568582648 %	100.00706763846 %
10.021828897			99.99969721963 %
10.022275389			100.00415240094 %
10.021616664			99.99757951877 %
10.021023638			99.99166219359 %

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c9f.f003    DYNAMIC     Fa0/24
   1    00d8.619b.c948    DYNAMIC     Fa0/1
   1    00e0.9154.4cad    DYNAMIC     Fa0/3
   1    1005.014d.8601    DYNAMIC     Fa0/2
```

그림 12. 정상적인 스위치의 MAC 주소 테이블
Fig. 12. MAC address table of normal switch

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c9f.f003    DYNAMIC     Fa0/24
   1    00d8.619b.c948    DYNAMIC     Fa0/1
   1    00e0.9154.4cad    DYNAMIC     Fa0/3
Switch>
```

그림 13. 공격자 차단 후 스위치의 MAC 주소 테이블
Fig. 13. MAC address table of switch after blocking the attacker

그림 13은 ARP 포이즈닝 공격을 인지하여 해당 MAC 주소를 가진 공격자 PC의 포트를 차단한 후 스위치의 MAC 주소 테이블의 모습이다.

Ⅴ. 결 론

네트워크에 대한 의존도가 높아질수록 관련 보안 문제도 빈번하게 발생하고 있으며, 이러한 네트워크 기반의 보안 사고로 인한 피해 사례도 급격하게 증가하는 추세이다. 본 논문은 이러한 문제점들과 피해 사례를 방지하는 데 그 목적이 있다. ARP 포이즈닝 공격은 원활한 스니핑 공격을 위해 자동화 툴을 사용해 비정상적인 ARP 응답 패킷을 반복적으로 전송하게 된다. 이러한 공격에 대해 실질적으로 그 공격 과정을 보인 다음 공격 패턴을 분석하고 해당 신호의 응답 시간에 대한 오차 범위를 분석한 자료를 기반으로 ARP 포이즈닝 공격을 탐지하고 이를 차단하는 결과를 보였다. 하지만 아직 해결되지 않은 ARP의 취약점을 개선하기 위한 연구가 지속되어야 할 것이다.

참고문헌

[1] David C. Plummer, “RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware,” *Internet Engineering Task Force*, Network Working Group, 1982.

[2] D. Bruschi, A. Ornaghi and E. Rosti, “S-ARP: A Secure Address Resolution Protocol,” *19th Annual Computer Security Applications Conference*, pp. 66-74, 2003.

[3] W. Lootah, W. Enck and P. McDaniel, “TARP: Ticket-based Address Resolution Protocol,” *21st Annual Computer Security Applications Conference (ACSAC'05)*, pp. 9-116, 2005.

[4] Seungpyo Hong, Myeongjin Oh, Suyeon Lee and Sangjun Lee, “Efficient Technique for Preventing ARP Spoofing Attacks using Reliable ARP Table,” *The Journal of KIISE : Computing Practices and Letters*, Vol. 17, No. 1, pp. 26-30, January 2011.

[5] D. Pansa and T. Chomsiri, “Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol,” *2008 Third International Conference on Convergence and Hybrid Information Technology*, Vol. 2, pp. 21-26, November 2008.

[6] S. Kumar and S. Tapaswi, “A Centralized Detection and Prevention Technique against ARP Poisoning,” *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* pp. 259-264, 2012.

[7] B. Scott and et al., “An Interactive Visualization Tool for Teaching ARP Spoofing Attack, *2017 IEEE Frontiers in Education Conference (FIE),* pp. 1-5, 2017.

[8] Hyo Sung Kang and Choong Seon Hong, “A Defense Technique against ARP Spoofing Attacks using a Keystone Authentication Table in the OpenStack Cloud Environment,” *The Journal of KIISE,* Vol. 45, No. 8, pp. 755-760, August 2018.

[9] Ahmed M.AbdelSalam and Ashraf B. El-Sisi Faculty, “Mitigating ARP Spoofing Attacks in Software-Defined Networks,” *Menoufia University*, 2015.

[10] S. Y. Nam, D. Kim and J. Kim, “Enhanced ARP: Preventing ARP Poisoning-based Man-in-the-middle Attacks, *in IEEE Communications Letters,* Vol. 14, No. 2, pp. 187-189, February 2010.

최준호(Jun-Ho Choi)

2020년 : 경상대학교 컴퓨터과학과 (공학학사)
2020년~현 재: 경상대학교 대학원 컴퓨터과학과 석사과정

※관심분야 : 정보보호(Personal Information), 네트워크 보안(Network Security) 등

백용진(Yong-Jin Baek)

2015년 : 경남과학기술대학교 컴퓨터공학과 (공학학사)
2019년 : 경상대학교 대학원 컴퓨터과학과 (공학석사)
2019년~현 재: 경상대학교 대학원 컴퓨터과학과 박사과정

※관심분야 : 정보보호(Personal Information), 네트워크 보안(Network Security) 등

서영건(Yeong-Geon Seo)

1987년 : 경상대학교 전산과(이학사)
1997년 : 숭실대학교 전산과(공학박사)
1989년~1992년 : 삼보컴퓨터
1997년~현 재 : 경상대학교 컴퓨터과학과 교수

※관심분야 : 의료 영상 처리, 머신 러닝, SLAM, 영상 인식, 컴퓨터 네트워크 등