KIPS Tr. Comp. and Comm. Sys.
Vol.7, No.1 pp.19~26 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.1.19

# Enhanced Server Availability for DDoS Amplification Attack Using CLDAP Protocol

Choi Suk June† · Kwak Jin††

## ABSTRACT

Recently, DDoS amplification attacks using servers that provide Microsoft Active Directory information using CLDAP protocol are increasing. Because CLDAP is an open standard application that allows a wide range of directory information to be accessed and maintained in a network, the server is characterized by its openness to the Internet. This can be exploited by the Reflector server to perform an amplification attack by an attacker. In addition, this attack can be attacked with a packet that is amplified 70 times more than the conventional UDP-based flooding attack, and it can block service to small and medium sized server. Therefore, in this paper, we propose an algorithm that can reduce the DDoS amplification attack using CLDAP server and implement the corresponding CLDAP server environment virtually, and implement and demonstrate the corresponding algorithm. This provides a way to ensure the availability of the server.

**Keywords : UDP Socket, CLDAP Protocol, DDoS Amplificattion Attack**

# CLDAP 프로토콜을 이용한 DDoS 증폭공격에 대한 서버 가용성 향상방안 연구

최 석 준† · 곽 진††

## 요 약

최근 CLDAP프로토콜을 사용하여 Microsoft Active Directory 정보를 제공하는 서버를 이용한 DDoS 증폭 공격이 점점 증가하고 있다. CLDAP는 네트워크에서 광범위한 디렉토리 정보를 접근하고 유지하도록 하는 개방형 표준 어플리케이션이기 때문에, 서버가 인터넷에 개방되어있는 특징을 가지고 있다. 이로인해, 공격자에 의해 증폭공격을 하기 위한 Reflector서버로 악용될 수 있다. 또한 이 공격은 기존의 UDP 기반 플루딩 공격보다 70배가량 증폭된 패킷으로 공격이 가능하며, 중소규모의 서버에 대한 서비스 차단을 할 수 있다. 따라서 본 논문에서는 CLDAP 서버를 활용하는 DDoS 증폭 공격을 감소할 수 있는 알고리즘을 제안하고 해당 CLDAP 서버 환경을 가상으로 구현하여, 해당 알고리즘에 대한 구현 및 실증을 진행한다. 이를 동해 공격 대상에 대한 가용성을 확보할 수 있도록 방안을 마련한다.

**키워드 : UDP 소켓, CLDAP 프로토콜, DDoS 증폭 공격**

## 1. 서 론

최근, UDP 통신 기반 CLDAP 프로토콜을 악용한 DDoS 공격이 증가하고 있다. CLDAP 서버가 패킷을 증폭하는데 악용이 가능한 Reflector 서버로 활용될 수 있는 이유는 UDP가 비연결지향의 특성을 가지고 있기 때문이다. UDP는 데이터 전송속도를 빠르게 하기 위해 통신 확인절차를 거치지 않고, 메시지를 송·수신한다. 이 경우 해당 메시지에 대한 신뢰성이 떨어지며, 반복적인 패킷 요청이 가능하여 기존 공격들보다 더 많은 트래픽을 발생시킬 수 있다[1].

또한, 공격자가 CLDAP 서버로 패킷을 보내게 될 경우 다수의 CLDAP 서버를 이용하여 패킷을 증폭하기 때문에 기존 공격보다 최대 70배의 패킷 증폭이 가능하며, 이는 중소규모의 서버를 마비시킬 수 있는 공격을 수행할 수 있다.

해당 증폭 공격에 대한 위험도는 높지만 기존 UDP 기반에 DDoS 대응 방식 외에는 대응방안이 없는 상황이다.

따라서, 본 논문에서는 CLDAP DDoS 증폭 공격을 감소시킬 수 있는 알고리즘을 제안하여 가용성을 확보하는 방안을 마련한다.

※ 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).
† 준 회 원 : 아주대학교 컴퓨터공학과 석사과정
†† 종신회원 : 아주대학교 사비버보안학과 부교수
Manuscript Received : November 21, 2017
Accepted : November 27, 2017
* Corresponding Author : Kwak Jin(security@ajou.ac.kr)

본 논문의 구성은 다음과 같다. 2장에서는 UDP 통신 구조, CLDAP 프로토콜의 구조, CLDAP DDoS 증폭 공격 등에 대하여 분석하고, 가용성을 침해하는 보안위협에 대해서 분석한다. 3장에서는 이 공격을 감소시킬 수 있는 알고리즘을 탐지, 방어, 레포트 작성 절차에 따라 제안하고, 4장에서는 해당 알고리즘을 구현하여, 가상의 실험 환경을 구성하고, 실험에 대한 결과 분석을 진행한다. 마지막으로 5장에서는 결론을 맺는다.

## 2. 관련 연구

### 2.1 UDP Socket Communication

CLDAP 서버에서 사용되는 UDP 프로토콜은 비연결지향 전송계층 프로토콜을 사용한다[2]. 해당 소켓 통신에 대한 구조는 Fig. 1과 같다.

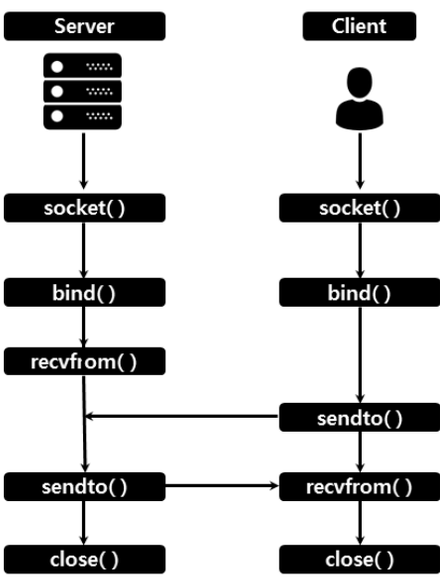


Fig. 1. UDP Socket

이와 같이 UDP 소켓 통신 구조는 서버, 클라이언트 구조가 TCP와는 다르게 Listen(), Accept() 등의 함수를 사용하지 않는다. 이는 별다른 통신 확인 절차를 거치지 않고, 수신 받는 대상자의 목적지의 주소만 있어도, 메시지를 보낼 수 있음을 의미한다. 본 논문에서는 4장에서 UDP 소켓 환경을 이용하여, 가상의 CLDAP서버가 희생자에게 메시지를 전송한다. 이때 메시지를 전송할 때 사용하는 함수는 sendto()를 이용해 희생자에게 메시지를 보내며, 목적지의 주소가 유효할 경우, 특정 포트를 지정하지 않더라도, bind() 함수에 의해 자동으로 할당된다.

- 희생자에게 UDP기반 응답 메시지를 보내기 위해, sendto()함수를 이용하여, 희생자의 주소를 지정하고 CLDAP 요청메시지에 대한 응답메시지를 전송할 때 사용한다.
- CLDAP 서버로부터 전송되는 응답메시지를 수신하기 위해서 사용되는 함수로 recvfrom()함수를 사용하며, 해당 함수는 sendto()함수를 이용하여, 희생자가 자신에게 수신되는 데이터를 받기위해 사용한다.

### 2.2 CLDAP Protocol

CLDAP(Connection-less Lightweight Directory Access Protocol)는 기존 TCP 기반의 LDAP 쿼리 전송속도의 효율성을 높여, UDP 기반으로 동작하도록 제안되었다[3-4].

UDP는 비연결지향 특성을 가지기 때문에 3-Way Handshaking을 수행하는 TCP 환경보다 상대적으로 패킷 오버헤드가 적어, 속도가 빠른 장점을 가지고 있다.

이러한 CLDAP 프로토콜은 Microsoft Active Directory 네트워크로부터 서버의 사용자 계정 및 비밀번호에 접근할 때 사용하는 프로토콜이며 Fig, 2와 같이 동작한다.

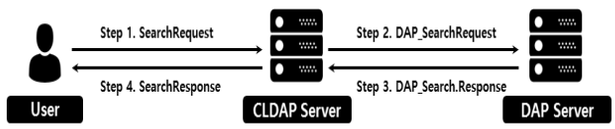


Fig. 2. CLDAP Protocol

사용자가 Microsoft Active Directory 정보를 받기 위해서는 총 4개의 패킷을 주고받으며 다음과 같다.

Step 1.
사용자는 CLDAP 서버로 Microsoft Active Directory 정보인 SearchRequest 메시지를 전송한다.

Step 2.
CLDAP 서버는 사용자가 요청한 Microsoft Active Directory 정보를 가져오기 위해 DAP_SearchRequest 메시지를 DAP 서버에 전송한다.

Step 3.
DAP 서버는 Microsoft Active Directory 응답 메시지인 DAP_SearchResponse를 CLDAP 서버에 전송한다.

Step 4.
CLDAP 서버는 Microsoft Active Directory 정보인 SearchResponse 메시지를 사용자에게 전송한다.

### 2.3 Amplification CLDAP DDoS Attack

CLDAP DDoS 증폭 공격은 CLDAP 서버들을 Reflector로 활용하여 패킷을 증폭하여 희생자에게 대량의 패킷을 전송하며 Fig. 3과 같이 공격을 수행한다[5].

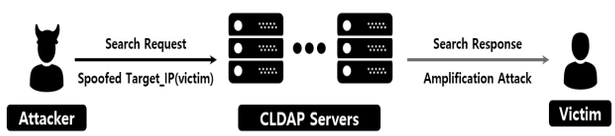


Fig. 3. Amplification CLDAP DDoS Attack

공격자는 Microsoft Active Directory 정보를 요청하는 메시지를 다수의 CLDAP 서버들에게 전송한다. 이때 메시지에 Destination IP주소를 공격 대상이 되는 희생자의 주소로 변조하여 쿼리를 보낸다. 하지만 서버는 비 연결지향 통신 특성상 정상적인 발신자인지 판단하지 않고, 요청한 메시지에 따라 변조된 희생자의 주소로 대량의 Microsoft Active Directory 정보가 전송된다. 이 방식에 따라 공격자는 노출된 CLDAP 서버를 이용해 패킷을 증폭하여 희생자에게 전송하며, 기존 DDoS 공격보다 높은 규모로 대상 서버의 가용성을 침해할 수 있다[6].

### 2.4 J.Arteaga에 의한 CLDAP Reflection DDoS 위협 분석

SIRT(Akamai Security Intelligence Response Team)에 의해 분석된 위협보고서에 따르면, CLDAP DDoS 증폭 공격은 기존 UDP 기반 DNS 서버를 이용한 공격에 필적하는 위협을 가진다고 말하고 있다.

분석한 보고서에 따르면 2017년 1월 7일, 가장 큰 CLDAP 증폭 공격이 발생했으며, 389 번 포트를 이용해 기존 DNS 공격보다 24배 높은 대역폭인 초당 24Gbps규모의 공격이 발생했다.

CLDAP 증폭 공격은 C 프로그래밍 언어 기반 공격 스크립트로 수행된다. 공격에 사용되는 옵션은 target_ip, target_port, list of reflector, time limit이 존재하며 다음과 같다.

1) Target_ip and Target_port

공격자가 CLDAP 서버에 희생자의 주소로 변조된 target_ip, target_port를 전송하기 위한 옵션으로 희생자에게 패킷을 reflection하도록 한다.

2) List of reflector

Reflectort로 사용 가능한 CLDAP 서버들의 리스트를 말하며, 해당 서버들은 인터넷에 노출되어 있는 특징을 가진다. 해당 서버들을 이용해 공격자가 패킷을 증폭하기 위해 활용되어 진다.

3) Time limit

Reflector로 악용 가능한 서버들에게 지정한 시간동안 패킷을 전송하도록 할 때 사용하는 옵션이다.

해당 공격 스크립트는 52 Byte에 해당하는 요청 메시지를 Reflector 목록에 전송하게 되며, 지정한 시간인 Time limit에 따라 요청 메시지를 전송한다. CLDAP 서버들은 공격자가 지정한 target_ip, target_port에 해당하는 희생자에게 요청한 정보에 대한 응답 메시지를 전송하며, 원치않는 응답을 받은 희생자의 서버는 가용성 침해를 일이키는 DDoS공격이 발생한다.

공격에 활용되는 CLDAP 서버는 인터넷에 노출되어 있으며, 악용될 수 있는 Reflector는 Table 1과 같이 총 78,531개의 고유한 IP로부터 취약점에 노출된 것으로 확인되었다. 또한 미국이 17,980개로 노출된 호스트가 가장 높게 발견되었으며, 그 다음으로 브라질이 6,005개의 호스트가 검출되었고, 나머지 국가들은 유사한 수치가 검출되었다[7].

Table 1. Countries with CLDAP Reflectors (Internet Scan)

| Country | Count |
|---|---|
| United States | 17,980 |
| Brazil | 6,005 |
| France | 3,542 |
| United Kingdom | 3,495 |
| Germany | 3,426 |
| China | 3,177 |
| Russian Federation | 2,583 |
| Canada | 2,207 |
| Colombia | 2072 |
| India | 1,987 |
| Other | 32,058 |

### 2.5 M.Yusof 등이 제안한 DDoS 공격 탐지 및 방어 알고리즘

M.Yusof 등은 총 4개의 유형의 DDoS 공격에 대한 탐지 및 방어 알고리즘을 제안하였다[8]. 이 알고리즘은 DDoS 공격 유형별로 탐지, 방어, 위협 보고서 제출 단계로 동작한다. 각 절차에 따른 알고리즘 동작 방식은 다음과 같다.

1) Detection

네트워크 상 들어오는 모든 패킷을 모니터링 하며, 공격 유형에 따라 UDP Flooding, TCP SYN flooding, Ping of Death, Smurf 등을 행위 기반으로 탐지한다.

2) Defense

탐지된 DDoS 공격 유형에 따라, 방어단계에서는 트래픽 차단을 진행한다. 이 때 들어온 초당 패킷의 개수가 100개 이상일 경우 제안된 알고리즘에 의해 패킷을 차단한다. 이러한 방식으로 DDoS 공격에 대한 네트워크 대역폭을 제어함으로써, M.Yusof 등이 제안한 알고리즘은 정상적인 트래픽만 네트워크에 접근할 수 있도록 한다.

3) Report of Attacks

탐지된 DDoS 공격의 유형을 기록하는 단계로 동작방식은 DDoS 공격을 차단 이후 유형별로 보고서를 작성하며, 공격에 대한 보고서는 DDoS 공격 유형, 패킷 크기, 심각도 수준, 탐지 시간, 공격자 소스로 총 5 가지 항목으로 작성된다.

- 탐지된 DDoS 공격 유형에 따라 UDP flooding, TCP SYN flooding, Ping of Death, Smurf 등으로 작성한다.
- 패킷 크기는 공격 트래픽의 패킷 크기를 랜덤 또는 오버 사이즈로 지정한다.
- 심각도 수준은 공격의 위험도에따라 낮거나 높은 수준으로 분류하여 작성한다.
- 탐지 시간은 DDoS 공격 트래픽이 탐지된 시점부터 시작해서 공격 지속시간을 작성한다.
- 공격자 소스는 공격자가 보낸 패킷에 전송된 실제 IP 또는 변조된 IP주소를 작성한다.

### 2.6 가용성 위협 분석

CLDAP 서버는 사용자가 마이크로 액티브 디렉토리 정보에 접근하기 위해 사용되며, LDAP 서버보다 쿼리 전송 시간을 효율적으로 줄이기 위해 비연결 지향 UDP 프로토콜을 사용한다. 따라서, 서비스 거부 공격에 대한 별도의 보안기능이 존재하지 않는다. 이는 공격자가 CLDAP 서버에 변조된 IP주소로 요청하는 패킷을 전송하더라도, 해당 주소가 변조 되었는지 확인할 수 없으므로 변조된 해당 주소로 증폭된 대량의 패킷이 전송되어 희생자의 서비스가 중단되는 가용성 침해가 발생할 수 있다.

## 3. 제안 사항

본 장에서는 M.Yusof 등이 제안한 DDoS 공격 방어 및 탐지 알고리즘을 기반으로 CLDAP 서버를 이용한 증폭 공격의 트래픽을 감소시킬 수 있는 알고리즘을 제안한다. 기존 연구의 경우 트래픽에 따라 DDoS공격 유형을 분석하고 이를 차단하였지만, Reflector 서버를 이용해 증폭 공격이 들어올 경우 이를 차단하거나 방지하기가 어렵다.

따라서, 본 논문에서는 Reflector 서버로부터 들어오는 패킷을 모니터링하고, C언어 기반 공격 스크립트 시그니처를 탐지할 경우에 대역폭을 감소시킬 수 있는 알고리즘을 제안하였으며, 동작 방식은 총 3가지 단계로 탐지, 방어, 공격에 대한 레포트 작성 등으로 진행한다. 전체적인 알고리즘은 Fig. 4와 같다.

### 3.1 제안하는 알고리즘

제안하는 알고리즘은 CLDAP DDoS 증폭 공격에 대한 대응 방안으로, 공격에 의해 발생할 수 있는 패킷을 해당 순서도와 같이 적용하여 패킷을 제어한다. 해당 알고리즘을 수행하기 위해서는, 앞 절에서 설명한 지역별 Reflector를 기반으로 인터넷에 노출되어있는 CLDAP에 대한 주소를 수집해야 한다. 또한 공격 스크립트에 따른, CLDAP 증폭공격에 대한 특성을 시그니처 기반으로 특성, 수집이 이루어져야 한다.

1) Detection

CLDAP 증폭 공격을 탐지하기 위한 방법으로, 탐지 알고리즘은 네트워크로 들어오는 모든 패킷을 탐지하며, 해당 패킷 중 CLDAP 프로토콜을 사용하는 Reflector 서버들을 탐지한다. CLDAP 서버 패킷을 탐지하는 방법은 총 2가지로, CLDAP 리플렉션에 활용되는 서버 즉, 2.4절 Table 1과 같이 인터넷에 노출된 서버에 대한 IP, Port 등의 주소를 통해 UDP 패킷에 대한 목적지 주소를 확인하고, 스크립트로 동작하는 CLDAP 공격 시그니처를 확인한다. 해당 절차는 Fig. 5와 같이 판단한다.

- CLDAP 서버들이 전송하는 SearchResponse 패킷에 대한 탐지를 진행한다.
- SearchResponse 패킷 중 공격 스크립트 기반 시그니처가 존재하는지 확인한다.

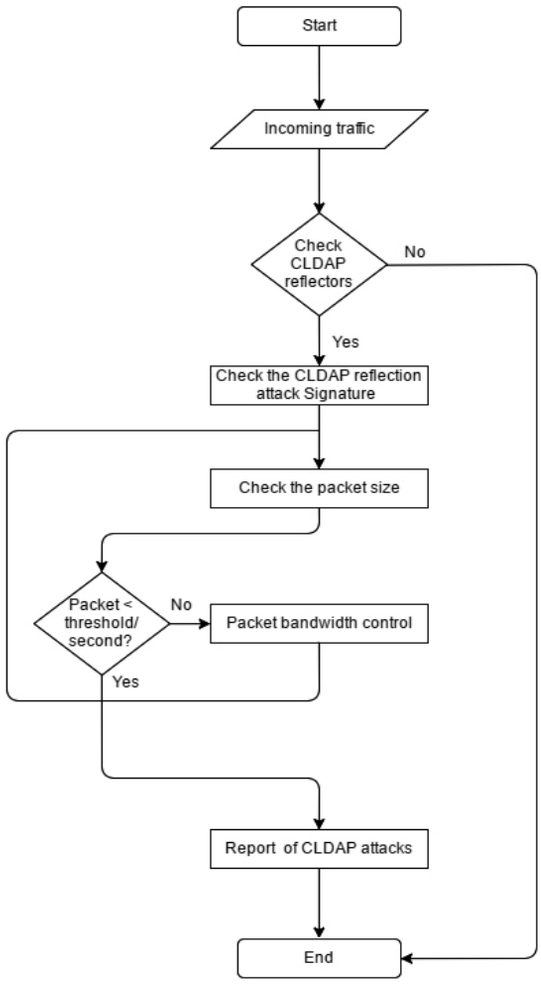


Fig. 4. Proposed Design

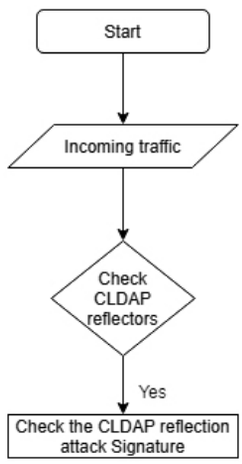


Fig. 5. Detection Phase

위와 같은 절차로 SearchResponse 패킷에 대하여 공격자로부터 악용될 수 있는 CLDAP 서버로부터 오는 패킷을 탐지한다. 이 구간에서 공격자에 의한 패킷으로 판단될 경우 제안하는 알고리즘의 다음 단계인 방어 절차를 진행한다.

2) Defense

탐지 절차에 따라 CLDAP 증폭 공격이 탐지될 경우, 해당 공격에 대한 방어 절차 알고리즘이 동작하게 된다. 이 절차에서 가장 큰 목적은 탐지된 비정상적인 CLDAP 패킷에 대역폭을 제어하는데 있다. 방어 절차는 Fig. 6과 같다.

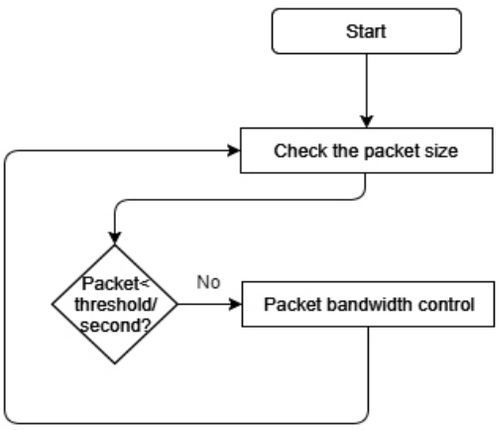


Fig. 6. Defense Phase

- SearchResponse 패킷의 크기를 체크한다.
- 해당 패킷의 크기가 서버가 수용 가능한 범위로 들어올 때까지 해당 서버로부터 들어오는 패킷의 크기를 지속적으로 체크하고, 대역폭을 제어 한다.

CLDAP 증폭 공격은 공격자가 지정한 Time Limit에 의해 일정 시간동안 변조된 희생자의 주소로 SearchRequest 메시지를 전송한다. 따라서 Time Limit 동안 대역폭을 제어하기 위해, 방어 절차에서는 패킷의 크기를 지속적으로 체크한다. 이러한 방식은 M.Yusof가 제안한 패킷 원천 차단방식과는 다르게, 패킷의 크기를 체크하여 대역폭을 제어함으로써, CLDAP 증폭 공격에 대한 대응이 가능하다.

3) Report of Attacks

이 절차에서는 탐지된 CLDAP 증폭 공격의 기준에 따라 위험성을 판단하고 식별 및 대응하는데 목적을 두고 있다. 이에 따라 공격에 대한 정보를 Fig. 7과 같이 기록한다.

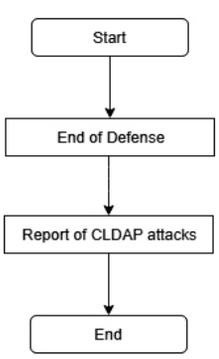


Fig. 7. Report of Attacks Phase

CLDAP 증폭 공격에 대한 네트워크 안정화가 진행된 후에 패킷 대역폭이 정상적인 범위가 확인될 경우, 공격에 대한 정보를 기록하게 되며, 공격 보고서는 공격 스크립트에 대한 특성을 기반으로 대역폭의 크기, 패킷의 크기, 어택 벡터, 공격 지속 시간, Source/Destination Port 총 5 가지 항목으로 작성한다.

- 대역폭의 크기는 발생한 CLDAP 증폭 공격의 초당 패킷 대역폭을 작성한다.
- 패킷의 크기는 공격 트래픽의 초당 발생한 패킷의 크기를 작성한다.
- 어택 벡터는 어떠한 프로토콜로부터 공격이 발생했는지에 대한 정보를 작성한다.
- 공격 지속시간은 공격이 시작된 시점으로부터 종료된 시점을 작성하며, 이는 트래픽에 대한 공격 지속시간을 의미한다.
- Source/Destination Port는 공격자가 보낸 패킷에 대한 Source Port, Destination Port를 작성한다.

### 3.2 제안하는 알고리즘을 적용한 공격 대응 시나리오

제안하는 알고리즘을 적용할 경우, 서비스 거부 공격을 통해 희생자에게 대량에 패킷이 전달되더라도, CLDAP 서버들로부터 오는 패킷에 대한 대역폭 제어가 가능하기 때문에 서비스 거부 공격을 방어할 수 있다.

Fig. 8은 CLDAP 증폭 공격과 대응 시나리오를 나타낸 그림이며, 이를 통해 제안한 알고리즘을 적용할 경우 CLDAP 증폭 공격을 감소할 수 있는 것을 보여줌으로써 안전성 분석을 진행한다.

<u>Step 1.</u> 정상적인 사용자 요청
사용자는 CLDAP 서버로 Microsoft Active Directory 정보를 요청하는 SearchRequest 메시지를 정상적인 CLDAP 서버에 전송한다.

<u>Step 2.</u> 공격자 요청
공격자는 증폭공격에 활용되는 다수의 CLDAP 서버들에게 Destination 주소를 희생자를 대상으로 IP, Port를 변조하여 마이크로 액티브 디렉토리 정보를 요청한다.

<u>Step 3.</u> 정상적인 CLDAP 서버 응답
사용자가 요청한 Microsoft Active Directory 정보에 대하여, CLDAP 서버로부터 응답 패킷이 들어올 경우, 제안한 알고리즘 동작 절차에 따라, 패킷의 크기를 체크한다. 해당 패킷의 경우 사용자가 정상적으로 요청한 패킷이므로, 대역폭의 임계값을 초과하지 않는 정상범위 안에 속한다.

<u>Step 4.</u> 공격자에 의해 증폭된 공격 패킷 응답
공격자가 요청한 Microsoft Active Directory 정보에 의해 사용자는 다수의 CLDAP 서버로부터 대량의 응답 패킷을 받게된다. 제안한 알고리즘 동작 절차에 따라, 탐지 단계에서 인터넷에 노출된 CLDAP 서버의 목록 확인 및 공격 스크립트에 따른 target_ip, target_port, list of reflector 등의

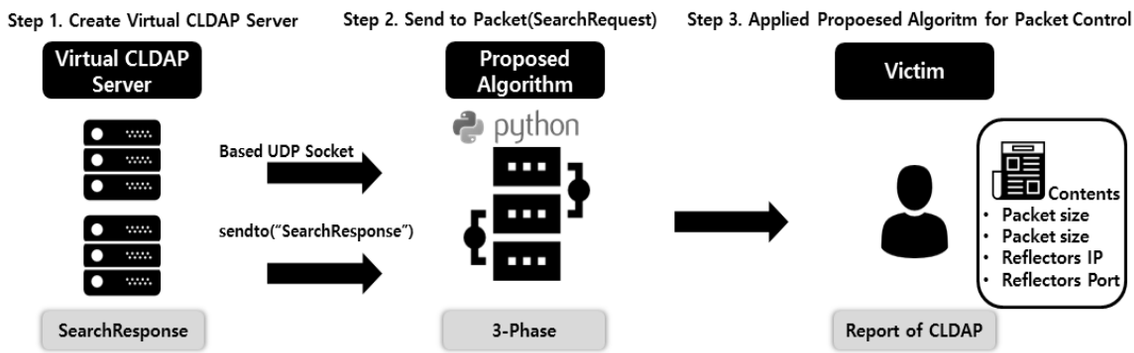


Fig. 8. Implementation Environment Structure

시그니처를 확인한다. 이와 같이 해당 패킷이 CLDAP 서버가 증폭 공격에 악용되는 것을 확인할 수 있다. 이후 지속적으로 CLDAP 응답 패킷들의 크기를 체크하고 서버가 수용할 수 있는 임계 값이 정상 범주로 돌아올 때까지 해당 패킷의 대역폭을 제어한다. 대역폭이 정상 범주로 돌아온 이후에는 해당 공격에 대한 보고서를 기록한다.

## 4. 실험 결과

### 4.1 실험 환경

해당 환경은 CLDAP 서버와 유사한 환경을 가상으로 구성하여, DDoS 증폭공격에 대한 가상 시나리오를 진행한다. 이를 통해 희생자는 제안한 알고리즘을 통해 해당 패킷을 제어하는 것에 대한 실험결과를 보여준다.

실험 환경 구성도는 Fig. 9와 같고, 해당 서버의 대한 성능은 Table 2와 같다.

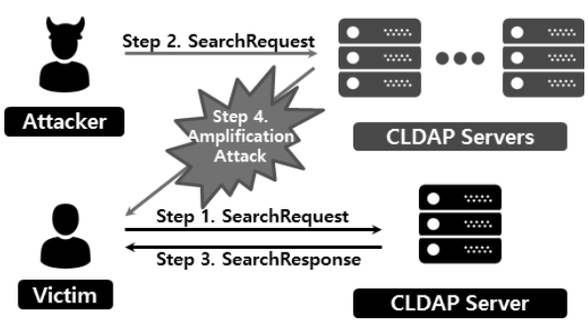


Fig. 9. CLDAP Amplification Attack Scenario

Step 1. Create Virtual CLDAP Server
CLDAP 서버와 유사한 환경을 만들기 위해 가상 CLDAP 서버를 만든다. 해당 서버는 호스트 머신 내에 설치된 VMWARE 12.1.1 환경에서 구축되었으며, 공격을 실현하기 위해 총 2개의 서버와, 희생자를 가상환경으로 구성하였으며, Ubuntu 16.04 64 bit로 설치하였다. 또한 해당 환경은 호스트 머신 내에서 각각의 가상환경들이 통신이 가능하도록 네트워크를 NAT(Network Address Translation) 환경으로 구성하였다.

Step 2. Send to Packet(SearchResponse)
가상 공격 시나리오를 위해 가상환경의 CLDAP 서버를 이용하여 공격자에 의해 변조된 주소(희생자의 IP)로 Microsoft Active Directory 요청에 대한 응답(Search-Response)을 희생자에게 지속적으로 전송한다고 가정한다. 해당 패킷을 전송하는 과정은 UDP 소켓 통신을 이용하여, 희생자의 해당 주소로 sock.sendto()함수를 이용하여, SearchResponse 패킷을 전송한다.

Step 3. Applied Proposed Algorithm for Packet Control
본 논문에서 제안한 알고리즘은 Python 기반으로 구현하였으며, CLDAP 서버로부터 들어오는 패킷을 탐지하고, 해당 패킷에 대한 대역폭을 제어한다. 이후 공격이 종료될 경우, 공격에 대한 정보를 담은 레포트를 작성한다.

Table 2. Implementation Environment

| Component | Host | Virtual CLDAP |
|---|---|---|
| OS | Windows 8.1 64bit | Ubuntu 16.04 64bit |
| CPU Core | 8 | 1 |
| RAM | 16 GB | 1 GB |
| HDD | 2 TB | 20 GB |
| Network | Static | DHCP(NAT) |

### 4.2 제안하는 알고리즘 구현 결과

제안한 알고리즘은 총 3개의 절차로, 탐지, 방어, 위협 레포트 작성으로 구성되어 있으며, 해당 절차에 대하여 Python 3.63 기반으로 구현을 진행하였다. CLDAP Reflector 서버로부터 희생자에게 데이터가 전송될 경우 알고리즘이 동작하여, 패킷을 제어한다. 또한 해당 알고리즘에 대한 구현방식을 수도코드를 기반으로 다음과 같이 결과를 작성하였다.

1) Detection

탐지 단계에서는 특항상 들어오는 패킷에 대한 탐지를 진행해야한다. 해당 단계에서는 패킷을 탐지하기 위해 인터넷에 노출된 Reflector 서버의 리스트를 받아온다. 또한 항상 탐지를 수행해야하기 때문에, while문을 사용해서 해당 패킷

에 대한 탐지를 수행한다. 패킷을 탐지하는 기준은 Reflector 서버의 IP로 부터 SearchResponse를 포함하는 UDP Datagram 전송되었을 때의 조건이 일치할 경우, CLDAP 증폭 공격에 사용되어지는 패킷이라 판단한다. Table 3은 Detection Phase 에 대한 수도코드이다.

Table 3. Detection Phase Pseudo Code

```
Algorithm detect_phase
  get CLDAP of Reflectors
  while True :
      if addr==Reflectors and SearchResponse
          Check CLDAP Packet
      end if
  end while
```

2) Defense

탐지가 이루어질 경우 방어 단계에서는 CLDAP 패킷의 크기를 가져오고 패킷 대역폭 제어를 수행한다. 패킷을 제어하기 위해서 특정 CLDAP 서버로부터 임계 값 이상 패킷이 들어올 경우 해당 주소에 대하여 일시적으로 차단한다. 대역폭 제어는 while문을 통해 패킷의 크기가 threshold(임계 값) 범위 내에 들어올 때가지 수행한다. 또한 범위 내로 패킷 크기가 들어올 경우, 대역폭 제어를 포함한 while문을 끝내고, 해당 공격이 끝났다는 flag 값을 리턴 한다.

Table 4. Defense Phase Pseudo Code

```
Algorithm defense_phase
  get CLDAP of Packets
  while CLDAP of Packets < threshold :
     Packet bandwidth control
  end while
Return End of CLDAP Attacks flag
```

3) Report of Attacks

위협 레포트 작성단계에서는 CLDAP 공격에 대한 정보를 보여준다. 해당 단계는 공격이 끝난 이후에 해당 레포트를 작성하기 때문에, 방어 단계에서 리턴한 플래그 값, 해당 공격에 대한 정보를 가져온다. 이후 공격이 끝났다는 플래그 값이 반환될 경우, 공격에 대한 정보를 출력 한다.

Table 5. Report of Attacks Pseudo Code

```
Algorithm report of attacks_phase
get End of CLDAP Attacks flag
get Information of CLDAP Attacks
  if flag==1
      display report of attacks
  end if
```

4) Result

제안한 알고리즘을 구현하여, 수행할 경우 희생자로부터 들어오는 패킷에 대한 탐지, 방어 정보 출력, 공격에 대한 정보를 출력하며, 다음과 같다. Fig. 10은 SearchResponse 패킷에 대한 탐지를 수행하며, 임계값이 넘을 경우, 해당 대역폭을 제어하는 결과를 보여준다. Fig. 11은 공격이 종료될 경우 공격에 대한 정보를 출력하며, 해당 내용은 총 5가지로, 희생자가 받은 UDP Datagram에 대한 내용, CLDAP 패킷의 크기, Reflector 서버의 주소, Port, 공격이 종료된 시간을 나타낸다.

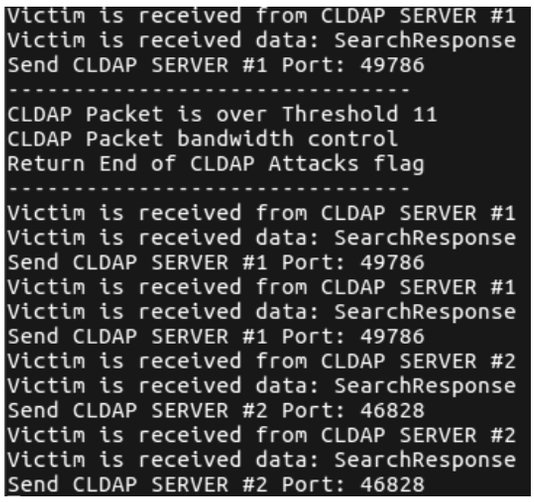


Fig. 10. Detect and Defense Result

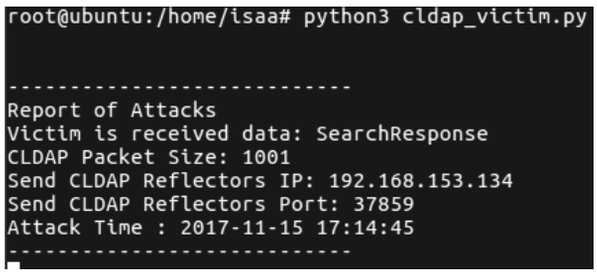


Fig. 11. Report of Attacks Result

### 4.3 가용성 보장

제안한 알고리즘은 CLDAP 서버를 이용한 DDoS 증폭 공격에 대해 3가지 절차에 따라 대역폭 제어를 수행한다. 이를 위해, 가상환경 CLDAP 서버를 이용해 희생자에 대한 DDoS 공격을 수행하였으며, 해당 알고리즘에 탐지, 방어, 위협 레포트 작성 절차에 따라 구현된 알고리즘에 대한 실험 결과를 나타냈다. 이 결과 가상 CLDAP 서버로부터 대량의 패킷이 전송되었을 때, 코드에 미리 설정한 임계값(Threshold)에 따라 대역폭을 제어하는 것을 볼 수 있으며, 희생자의 주소로 대량의 패킷이 전송되더라도, 제안한 알고리즘을 적용할 경우, 가용성을 보장해 줄 수 있다.

## 5. 결 론

비연결지향의 CLDAP 프로토콜은 기존의 LDAP에서 접근에 대한 효율성을 높이기 위해 UDP를 사용한다.

하지만 UDP 프로토콜의 특징 때문에, 공격자는 CLDAP 서버에 희생자의 IP로 변조된 패킷을 요청할 수 있으며, 이를 통해 DDoS 공격을 하기 위한 Reflector로 활용될 수 있다. 또한 CLDAP 서버는 불필요하게 인터넷에 노출되어 있기 때문에, 공격자는 손쉽게 공격에 활용할 서버 목록을 찾을 수 있다.

CLDAP를 Reflector로 하는 DDoS 증폭 공격의 경우, 중소 서버를 마비시킬 수 있을 정도로 패킷 증폭률이 월등히 높다. 이러한 CLDAP 증폭 공격은 지속적으로 증가하고 있지만, 이에 대한 대응방안이 현재로써는 미흡한 실정이다.

따라서 본 논문에서는, CLDAP Reflector 서버들을 기반으로 하는 공격을 탐지하고 패킷 대역폭을 제어할 수 있는 알고리즘을 제안하였다. 해당 알고리즘은 CLDAP 서버로부터 오는 패킷을 모니터링하고, 대역폭을 제어한다. 또한 해당 공격에 분석 및 대응할 수 있도록 발생한 위협에 대하여 공격 지속시간, 패킷 대역폭의 크기 등의 정보를 포함하는 보고서를 저장한다. 제안한 알고리즘은 CLDAP 증폭 공격에 대한 실증을 위한 가상환경을 구성하였으며, 알고리즘을 Python 기반으로 구현하여, 가상 공격에 대한 실험을 진행하였다.

본 논문에서 제안한 알고리즘은 CLDAP 서버를 악용하는 DDoS 증폭 공격으로부터, 희생자의 네트워크에 대한 가용성을 보장해주고, DDoS 증폭 공격에 대한 추가적인 연구를 진행하는 데에 기여할 수 있을 것으로 예상된다.

## References

[1] M. Kuhrer, T. Hupperich, C. Rossow, and T. Holz, “Exit from Hell? Reducing the Impact of Amplification DDoS Attacks,” *Open access to the Proceedings of the 23rd USENIX Security Symposium*, Aug., 2014.

[2] R. Gilligan, S. Thomson, J. Bound, and W. Stevens, “Basic socket interface extensions for IPv6,” No. RFC 2553, 1999.

[3] M. Wahl, T. Howes, and S. Kille, “Lightweight directory access protocol (v3),” 1997.

[4] A. Young, “Connection-less Lightweight X. 500 Directory Access Protocol,” 1995.

[5] S. Taghavi, J. Joshi, and D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” *IEEE Communications Surveys & Tutorials*, Vol.15, 2013.

[6] C. Rossow, “Amplification Hell: Revisiting Network Protocols for DDoS Abuse,” NDSS, Feb., 2014.

[7] J. Arteaga and W. Mejia, “CLDAP Reflection DDoS Threat Advisory,” Apr., 2017.

[8] M. Yusof, F. Mohd, and M. Drais, “Detection and Defense Algorithms of Different Types of DDoS Attacks,” *International Journal of Engineering and Technology*, Vol.9, Oct., 2017.

최 석 준

http://orcid.org/0000-0002-5052-1627

e-mail : sjchoi.isaa@gmail.com

2016년 아주대학교 정보컴퓨터공학부 (학사)

2016년~현 재 아주대학교 컴퓨터공학과 석사과정

관심분야 : 자동차 보안, 클라우드 컴퓨팅 보안

곽 진

http://orcid.org/0000-0001-6931-2705

e-mail : security@ajou.ac.kr

2000년 성균관대학교 생물기전공학(공학사)

2003년 성균관대학교 컴퓨터공학(공학석사)

2006년 성균관대학교 컴퓨터공학(공학박사)

2006년~2006년 일본 큐슈대학교 방문연구원

2006년~2006년 일본 큐슈시스템정보기술연구소 특별연구원

2006년~2007년 정보통신부 정보보호기획단 개인정보보호팀 통신사무관

2007년~2015년 순천향대학교 정보보호학과 교수

2008년~현 재 한국정보보호학회 상임이사

2011년~현 재 한국정보처리학회 이사

2015년~현 재 아주대학교 사이버보안학과 교수

관심분야 : 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가