디바이스의 DDoS 공격 여부 판단 및 대응 시스템 설계

김효종* · 최수영 · 김민성 ·신승수

동명대학교

Device RDoS Attack Determination and Response System Design

Hyo-jong Kim* · Su-young Choi · Min-sung Kim · Seung-soo Shin

Tongmyong University

E-mail : rlaqywhd019@naver.com / suyoung@tu.ac.kr / minsung@tu.ac.kr / shinss@tu.ac.kr

요 약

2015년부터 IoT 프로토콜을 사용한 공격이 지속적으로 보고되고 있다. 다양한 IoT 프로토콜 중 공격자는 SSDP(Simple Service Discovery Protocol)를 사용하여 DDoS 공격을 시도하고 있으며, 사이버 대피소 통계로 한국은 약 100만 개의 개방형 SSDP 서버를 보유하고 있다. 인터넷에 연결된 취약한 SSDP 서버는 50Gb 이상의 트래픽을 생성 할 수 있으며 공격 위험은 점진적으로 증가한다. 최근까지도 분산 서비스 거부 공격과 분산 반사 서비스 거부 공격이 보안 문제로 대두되고 있다. 따라서 본 연구의 목적은 기존 SSDP 프로토콜의 요청 패킷을 분석하여 증폭 공격을 식별하고 증폭 공격이 의심되는 경우 대응을 회피하여 다량의 응답 패킷 발생으로 인한 네트워크 부하를 방지하는 것이다.

ABSTRACT

Since 2015, attacks using the IoT protocol have been continuously reported. Among various IoT protocols, attackers attempt DDoS attacks using SSDP(Simple Service Discovery Protocol), and as statistics of cyber shelters, Korea has about 1 million open SSDP servers. Vulnerable SSDP servers connected to the Internet can generate more than 50Gb of traffic and the risk of attack increases gradually. Until recently, distributed denial of service attacks and distributed reflective denial of service attacks have been a security issue. Accordingly, the purpose of this study is to analyze the request packet of the existing SSDP protocol to identify an amplification attack and to avoid a response when an amplification attack is suspected, thereby preventing network load due to the occurrence of a large number of response packets due to the role of traffic reflection amplification.

키워드

SSDP Server, DRDoS amplification attack, IoT

Ⅰ. 서 론

SSDP(Simple Service Discovery Protocol)는 서비스검색 요청 메시지를 전달하고 탐색요청 메시지에 응답 메시지를 서비스하는단순 전달 및 응답 프로토콜이다. 근래에 확산 되고 있는 DDoS (Distributed Denial of Service)공격은 분산 서비스 거부 공격으로 여러 대의 기기들을 이용하여 동시에 특정 서버나 네트워크가 많은 서비스 요청에 의하여 동작 불능하도록 유도하는 해킹기법이다. 인터넷에 연결된 취약한 SSDP 서버들은 50Gb 이상의 트래픽 발생이 가능하고 공격의 위험성은 점차 증가한다. 최근까지도 분산 서비스 거부 공격과 분산 반사 서비스 거부 공격은 보안상 이슈가 되고 있다[1-3].

이에 따라 본 연구의 목적은 기존 SSDP 프로토콜의 요청 패킷을 분석하여 증폭 공격을 파악하고 증폭 공격 의심 시 응답을 회피함으로써 트래픽 반사 증폭 역할로 인해 대량의 응답 패킷 발생으로 인한 네트워크 부하를 방지한다.

* speaker

II. SSDP Protocol

SSDP(Simple Service Discovery Protocol)는 UPnP의 네트워크 서비스나 정보를 찾기 위해 사용하는 네트워크 프로토콜이다. SSDP를 이용하면 DHCP와 DNS 같은 네트워크 서버 또는 정적인 호스트 없이도 정보를 찾는 서비스가 가능하다[3]. SSDP는 일반 거주지와 소규모 사무 환경에서 UPnP(Universal Plug and Play)를 위한 기본적인 프로토콜로 이미 널리 사용되고 있다. 1999년 MS와 HP가 IETF에 드래프트 했다. IETF 제안이 만료된 이후 SSDP는 UPnP표준에 포함됐다.

SSDP의 전송 방식에는 UPnP Protocol을 지원하는 기기에서 자신의 기기와 서비스를 광고(Advertisement)하기 위해 검색 기능 메시지를 멀티캐스팅 방식으로 전달하는 광고 메시지 전달 방식과 검색 방식인 M-search 통신 2가지로 분류된다[4].

2.1. SSDP 증폭공격

SSDP는 소스 IP 주소 위조와 증폭 요소를 가능하게 해 주는, 연결이 없는 상태라는 자체 속성 때문에 공격에 활용되는데, 주로 광고 전송 및 M-SEARCH 메소드 부분의 취약점을 활용한 공격이다. SSDP 증폭 공격의 가장 큰 장점으로는 홈 IoT 장비에 패킷을 위장하기 때문에 바로 공격자의 IP 정보를 알기 어렵다[2]. 홈 IoT 기기의 반사체들 또한, 공격자의 정보를 가지고 있지 않으며 IoT 관련 반사체들이 연계 네트워크 내에만 있다고 가정 할 수가 없다. 즉 SSDP 프로토콜 증폭 공격은 해커의 위치와 정보를 찾기 어려운 특징을 가지고 있다[4].

SSDP 프로토콜은 네트워크에 연결된 다른 기기와 통신할 수 있게 허용하는데 이 시스템에 공격자는 지속적으로 패킷을 보낸다. 이런 공격은 손쉽게 50기가바이트(GB) 이상의 트래픽을 발생시킨다. 트래픽의 증가는 실제 시스템에는 문제가 발생하지 않지만 시스템이 속한 네트워크를 마비시켜 네트워크 서비스를 사용자가 이용할 수 없게 만든다. 공격자가 수많은 패킷을 보내면 이 패킷들은 호스트 사이를 반복적으로 왕복하여 네트워크의 부하를 기하급수적으로 증가시킨다[5-6].

2.2. SSDP 증폭 공격 패턴

① 공격자는 여러 개의 IoT 기기를 활용하여 특정 호스트로 증폭 공격을 시도
② 여러 개의 IoT 기기를 통해 요청 패킷의 Source IP를 위조하여 전송
③ 요청 패킷을 수신한 IoT 기기들은 특정 호스트로 응답 메시지를 전송
④ 요청에 의한 다수의 IoT 기기들의 응답 패킷으로 인해 네트워크 부하 발생
⑤ 특정 호스트는 대량의 응답패킷으로 인해 시스템 부하가 발생하여 정상적인 서비스 불가

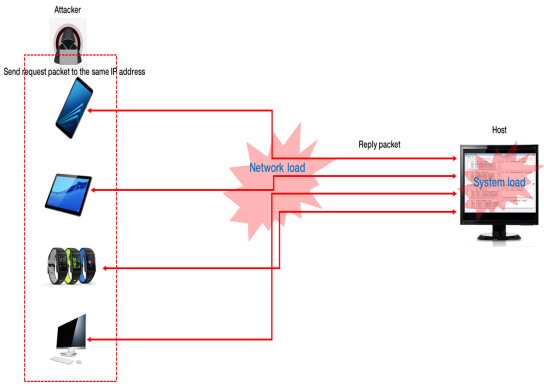

그림 1. Amplified Attack Scenario

III. 대응 시스템 개발

공격자는 외부에서 서비스가 오픈된 IoT 기기를 찾기 위해 M-Search 패킷을 네트워크상에 전송하게 되고 IoT 기기로부터 수신된 M-Search 패킷으로 IoT 기기의 정보를 수집한다. 이후 수집된 IoT 기기에 지속적으로 동일한 요청 패킷을 보내어 네트워크 부하 및 응답 메시지로 인한 특정 호스트의 시스템 부하를 야기 시킨다. 따라서 IoT 기기에서 첫 요청 패킷을 수신하였을 때 출발지 IP 주소와 수신 시간을 저장하여 특정 Time-Out 내에 동일한 출발지 IP로 요청 패킷이 들어오는지를 모니터링하여 동일한 패킷이 Time-Out 내에 들어오면 해당 요청을 무시하고 dissconnection 하여 네트워크 부하 및 시스템 부하를 사전에 방지한다.

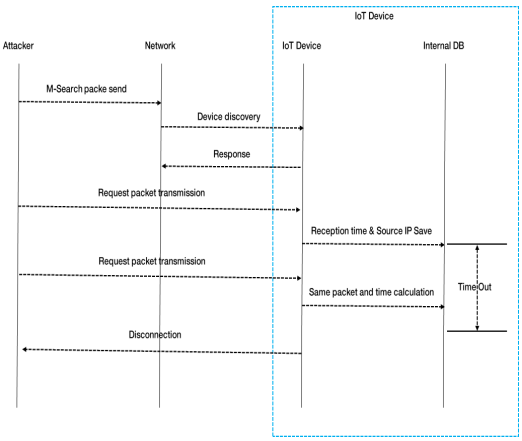

그림 2. DDoS 공격 대응 시스템 패킷 흐름도

① IoT 기기에 요청 패킷이 수신되면 수신된 패킷의 시간과 출발지 IP를 내부 DB에 저장한다.

② 첫 요청 패킷이 수신된 이후에 카운터를 시작하여 정해진 Time-Out 내에 동일한 출발지 IP로 같은 요청 패킷이 수신되는지를 모니터링한다.
③ 동일한 요청 패킷이 Time-Out 내에 수신되었다면 악의적인 공격으로 판단하여 요청 패킷을 무시하고 해당 세션을 끊는다.

Ⅳ. 결 론

SSDP는 기기가 네트워크에 연결된 다른 기기를 찾고 통신할 수 있게 허용하는 프로토콜이다. 공격자는 SSDP의 취약점을 악용하여 시스템에 지속적으로 요청 패킷을 보낸다. 이런 공격은 쉽게 50GB 이상의 트래픽을 발생시키고 더불어 웹사이트나 네트워크의 부하로 인한 서비스 중단 사태를 발생시킨다. 본 논문에서는 이러한 DDoS 공격 패턴을 분석하여 공격자가 요청 패킷을 보낸 후 첫 요청 패킷을 수신하였을 때 출발지 IP 주소와 수신 시간을 저장하여 특정 Time-Out 내에 동일한 출발지 IP로 요청 패킷이 들어오는지를 모니터링하여 동일한 패킷이 Time-Out 내에 들어오면 해당 요청을 무시하고 dissconnection 하여 네트워크 부하 및 시스템 부하를 사전에 방지한다.

Acknowledgement

“이 논문은 2020년도 BB21+사업에 의하여 지원되었음”

References

[1] Shin, Jung-Hwa; Shin, Weon; , “A New Defense against DDoS Attacks using Reputation”, Journal of the Korea Institute of Information and Communication Engineering, Vol. 15, No.8, pp.1720-1726, 2011
[2] So Ra Jung ,Hee Yong Yun , "Adaptively Flexible Service Discovery and Advertisement for SSDP of UPnP in Wireless ad-hoc Network", The KISS Transactions:Part A, Vol.17-A, No. 5, pp. 237-248, 2010
[3] H Choi, H Park, H Lee ,“A Study on Amplification DRDoS Attacks and Defenses”, The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 8, No. 5, pp.429-437, 2015
[4] Kwang-ok Park, Da-sol Park, Jong-kun Lee “ A Countermeasure Structure for Attack of SSDP Amplification Used Mac Address authorizatio”, Journal of the Korean Information Science Society, pp1109-1111, 2017
[5] Im-Geol Oh, Jong-Il Lee, "A Study for Vulnerability of Security of the UPnP Home-Networking", The Journal of Korea Society of Industrial Information System, Vol. 12, No. 2, pp. 30-36, 2007.
[6] Ju-Hye Oh ,Keun-Ho Lee ,“Attack Scenarios and Countermeasures using CoAP in IoT Environment”, Journal of the Korea Convergence Society, Vol. 7, No. 4, pp.33-38, 2016
[7] Hyung-Jin Mun , Gwang-Houn Choi ,Yooncheol Hwang,“Countermeasure to Underlying Security Threats in IoT communication”, Journal of IT Convergence Society for SMB, Vol. 6, No. 2, pp.37-44, 2016