ICMP 공격 방지를 위한 outbound traffic controller에 관한 연구

유권정 · 김은기*
국립한밭대학교

A study on the outbound traffic controller for prevention of ICMP attacks

Kwon-joeong Yoo · Eun-gi Kim*
*Hanbat National University
E-mail : egkim@hanbat.ac.kr

요 약

ICMP(Internet Control Message Protocol)는 TCP/IP 기반의 통신망에서 오류에 관한 처리를 지원한다. 만약 데이터 전송 과정에서 문제가 발생하면 라우터 또는 수신 호스트가 오류 발생 원인을 포함한 ICMP 메시지를 송신 호스트에게 전송한다. 하지만 이러한 과정에서 공격자가 위조된 ICMP 메시지를 호스트들에게 전송하여 호스트 간 통신을 비정상적으로 종료시킬 수 있다. 본 논문에서는 ICMP와 관련된 여러 가지 공격들을 방지할 수 있도록 하는 연구를 수행하였다. 이를 위해 호스트의 운영체제에서 공격용 ICMP 패킷이 네트워크로 전송되지 않도록 하는 아웃바운드 트래픽 컨트롤러(outbound traffic controller)를 설계하였다.

ABSTRACT

ICMP(Internet Control Message Protocol) supports the processing of error in the communication network based TCP/IP. If a problem is occurred in a data transmission process, router or receiving host sends ICMP message containing the error cause to sending host. However, in this process an attacker sends a fake ICMP message to the host so that the communication between the hosts can be abnormally terminated. In this paper, we performed a study to prevent several attacks related to ICMP. To this, we have designed outbound traffic controller so that attack packet is not transmitted to network in operating system of host.

키워드
ICMP, network attack, icmp flood, traffic preventing, outbound traffic

Ⅰ. 서 론

ICMP(Internet Control Message Protocol)란 오류 보고 기능을 지원하지 않는 IP 계층의 단점을 보완하기 위해 생겨난 프로토콜이다. 또한 호스트 또는 라우터로부터 필요한 정보들을 관리한다[1][2].

ICMP 공격에는 여러 가지 공격이 존재하는데[3], 본 논문에서는 DOS(Denial of Service)공격의 특성을 가진 랜드(land) 공격, 스머프(smurf) 공격, 죽음의 핑(Ping of Death) 공격을 방지한다. 현재 많은 운영체제는 ICMP 공격들이 불가하도록 ICMP 메시지의 수신을 거부한다[4]. 하지만 본 논문에서 제안하는 아웃바운드 트래픽 컨트롤러(outbound traffic controller)는 호스트가 전송하는 패킷들 중 공격용으로 판단되는 ICMP 메시지를 폐기하여 네트워크에서 발생할 수 있는 불필요한 트래픽을 방지한다. 또한 본 논문은 현재 ICMP 공격들을 막을 수 없는 운영체제에 적용할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 방지하는 공격의 유형 및 제안하는 아웃바운드 트래픽 컨트롤러의 설계에 대하여 기술한다. 4장에서는 결론을 다룬다.

II. 본 론

일반적으로 호스트는 핑(ping) 프로그램을 사용하는데, 핑이란 상대 호스트에게 데이터를 전송할 수 있는지 확인하는 프로그램이다. 먼저 송신 호스트는 echo request 메시지를 수신 호스트에게 전송한다. 수신 호스트로부터 echo reply 메시지가 오면 수신 호스트는 동작한다고 여기고, 응답이 오지 않으면 수신 호스트가 동작하지 않는다고 여긴다[1][4][5].

2.1. ICMP 공격의 유형

본 논문에서는 랜드 공격, 스머프 공격, 죽음의 핑을 방지하도록 설계하였다.

랜드 공격이란 공격자가 echo request 패킷의 출발지 IP 주소(source IP address)와 목적지 IP 주소(destination IP address)를 동일하게 설정하여 피해자 호스트에게 전송하는 것이다. 이를 수신한 피해자 호스트는 응답하기 위해 echo reply 패킷을 전송하게 되는데, 이때 출발지 IP 주소가 자신의 IP 주소이기 때문에 echo reply 패킷은 자기 자신에게 돌아오게 된다. 이를 반복하게 되면 피해자 호스트는 과부하에 걸리게 된다[3].

스머프 공격은 공격자 호스트가 echo request 패킷의 출발지 IP 주소를 피해자 호스트의 IP 주소로 설정하고, 목적지 IP 주소를 망 내에 있는 전체 호스트들로 설정하여 전송하는 것이다. 이를 수신한 호스트들은 응답하기 위해 피해자 호스트의 IP 주소로 echo reply 메시지를 전송한다. 피해자 호스트는 무방비 상태에서 수많은 echo reply를 수신하게 되고 시스템은 과부하 상태가 된다[3][5].

죽음의 핑 공격은 공격자가 echo request 패킷의 데이터 크기를 최대치로 설정한 뒤 피해자 호스트에게 전송하는 것이다. 이때 데이터는 MTU(Maximum transmission unit)에 맞춰 단편화(fragmentation)되어 전송된다. 이를 수신한 피해자 호스트는 단편화 된 데이터의 조각들을 재조립을 한다. 이 과정을 빠른 속도로 반복하면 피해자 호스트는 단편화 된 데이터들의 재조립을 반복하게 되면서 과부하에 걸리게 된다[3][5].

2.2. 아웃바운드 트래픽 컨트롤러의 설계

랜드 공격은 전송되는 echo request 패킷의 출발지 IP 주소와 목적지 IP 주소가 동일 할 경우 전송하지 않도록 하여 방지 할 수 있다. 이미 여러 운영체제에서는 수신한 echo request 패킷의 출발지 IP 주소와 목적지 IP 주소가 일치 할 경우에 해당 패킷을 폐기한다. 하지만 본 논문에서 제안하는 아웃바운드 트래픽 컨트롤러는 불필요한 트래픽이 발생하지 않도록 전송되는 패킷 중 공격용 ICMP 메시지로 판단된 패킷을 폐기한다. 또한 아직 랜드 공격이 유효한 운영체제를 위해 본 논문에 해당 공격 방지 기능을 추가하였다.

스머프 공격의 경우에는 전송되는 echo request 패킷의 출발지 IP 주소와 자신의 IP 주소를 비교한다. 그 결과 다를 경우 smurf 공격으로 판단하고 해당 패킷을 폐기한다.

죽음의 핑 공격은 echo request 패킷의 크기가 망의 MTU 이상일 경우에 해당 패킷을 폐기한다.

다음 (그림 1)은 본 논문에서 제안하는 아웃바운드 트래픽 컨트롤러의 전체적인 동작 알고리즘이다.

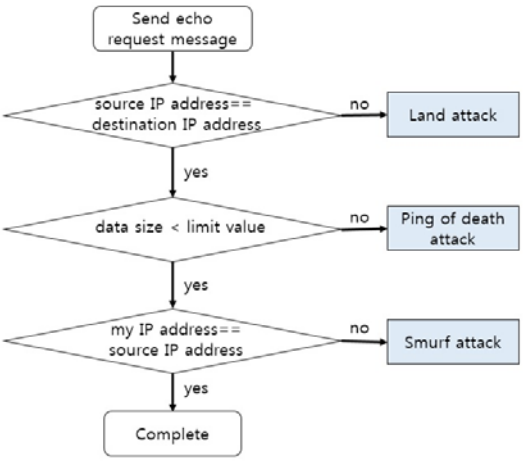

그림 1. 아웃바운드 트래픽 컨트롤러의 전체 동작 알고리즘

III. 결 론

본 논문에서는 ICMP를 이용한 다양한 공격을 방지하기 위해 호스트가 각각의 공격에 따라 발생하는 공격용 ICMP 메시지를 망으로 전송되지 않게 하는 아웃바운드 트래픽 컨트롤러를 제안하였다.

호스트에서는 정상적인 ICMP에서 전송되는 echo request 패킷의 조건과 다를 경우 공격용 ICMP 메시지로 판단하여 해당 패킷을 폐기한다.

추후에는 본 논문의 아웃바운드 트래픽 컨트롤러를 이용하여 다양한 ICMP 공격을 방지하는 할 수 있는지에 대한 연구를 수행할 예정이다.

ACKNOWLEDGMENTS

This research was financially supported by the Ministry of Trade, Industry and Energy (MOTIE) through the Promoting Regional specialized Industry (No. R0003847)

참고문헌

[1]Behrouz A. Forouzan, TCP/IP Protocol Suite Fourth edition, McGRAW.HILL INTERNATIONAL EDITION, 246, 2010

[2]R. Braden, Editor, Requirements for Internet Hosts -- Communication Layers, RFC 1122, 10, 1989

[3]양대일, 정보 보안 개론, 한빛미디어, 102-107, 2008

[4]Behrouz A. Forouzan, Data communication and networking 5E, McGRAW.HILL INTERNATIONAL EDITION, 578, 2013

[5]John Erickson, 해킹:공격의 예술, 에이콘 출판, 319, 2010