IPv4와 IPv6의 병행사용 환경에서의 DSTM 보안 기술 연구

김병욱*, 박석천*

*경원대학교 소프트웨어학부, *경원대학교 소프트웨어학부

Study on Security Method of DSTM Mechanism in IPv4/IPv6 Environment

Kim, Byung Wook* , Park, Seok Cheon*

*Division of Software, Kyungwon University

E-mail : bwdream@gmail.com, scpark@kyungwon.ac.kr

요 약

IPv4와 IPv6가 병행해야할 향후 몇 년간은 서로 다른 호스트주소를 가지는 IPv4/IPv6 기반 네트워크망에서 서로 원활한 통신을 하기 위한 기술이 필수적으로 요구된다. 이미 많은 분야에서 IPv4/IPv6 병행사용을 위한 여러 가지 기법들이 개발 되었으며 또한 거기에 따른 보안 문제들도 함께 연구되고 있다. 본 논문에서는 IPv4/IPv6 터널링 기술 중 하나인 DSTM에 대해 설명하고 DSTM에서 발생할 수 있는 보안의 문제점을 분석하고 그에 따른 해결책을 제시하였다.

1. 서론

IPv4 주소 고갈로 인해 제안된 IPv6[1] 는 앞으로 IPv4주소체계를 대체하여 쓰일 것이지만 현재 구축 되어 있는 IPv4기반 인터넷 환경에서 점진적으로 IPv6가 도입될 전망이다. 이러한 상황 하에 IPv4와 IPv6의 공존을 위해서 다양한 IPv4/IPv6 변환기술들이 제시되었다. IPv4/IPv6 변환기술은 한시적으로 쓰일 것 이지만 차후에 모든 네트워크망이 IPv6로 대체되기까지는 어쩔 수 없이 거쳐 가야할 과도기 중에 꼭 필요한 기술이므로 이 분야에 대한 연구나 보안상의 위협 같은 이슈들도 크게 부각 되었다.

IPv4/IPv6 변환 기술을 크게 세 가지로 나누면 듀얼스택(dual stack)[2] 기술, 터널링(tunneling) 기술, 변환(translation) 기술로 분류할 수 있다. 듀얼스택 기술은 하나의 시스템(호스트 또는 라우터)에서 IPv4와 IPv6를 동시에 처리하는 기술이고 터널링 기술은 기존 IPv4 망을 전달망으로 사용해 패킷이 IPv4망을 마치 터널을 통과하는 것처럼 이동하여 떨어져 있는 IPv6 망들을 연결시켜 주는 기술이고 변환 기술은 IPv4 망과 IPv6 망 사이를 연동하는 기술로 IPv6 클라이언트가 IPv4 서버에 접속할 때 또는 IPv4 클라이언트가 IPv6 서버에 접속할 때 사용된다.

현재와 같이 IPv4/IPv6 환경에서도 여러 가지 비정상적인 방법으로 인한 불법적인 시도는 계속 될 것이다. 그 중 하나가 터널링 기술 중 DSTM(Dual Stack IPv6 Dominant Transition Mechanism) [3] 에 IPv6 스푸핑을 이용하여 자원을 고갈시키는 문제인데 악의적 의도를 가진

* 경원대학교 일반대학원 전자계산학과 석사과정
** 경원대학교 IT대학 교수(교신저자)

공격자가 DSTM이 가지고 있는 IPv4 주소들을 불법적으로 할당 받아 사용 하여 IPv4 글로벌 풀(Pool)에 있는 주소들을 고갈 시킬 여지가 있다. 따라서 본 논문에서는 DSTM 메커니즘의 동작 방식과 DSTM상에서 일어날 수 있는 보안상의 문제점을 분석하고 이를 해결하기 위한 보안 대책을 제시한다.

2. 관련연구

2.1 스푸핑

스푸핑은 자기 자신의 식별 정보를 속여 상대방을 공격하는 기술이다. 해킹 시 자신의 정보(IP 주소, DNS 이름, MAC 주소 등)를 감춤으로써 자신을 드러내지 않고 목표를 공격하게 된다[4].

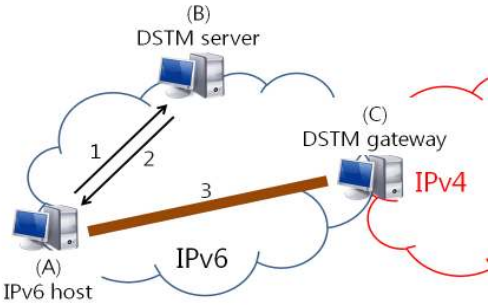
<표 1> 대표적인 스푸핑 공격의 종류

구분	내용
IP Spoofing	IP 정보를 속여서 다른 시스템을 공격
ARP spoofing	ARP 프로토콜상의 32bit IP-48bit의 네트워크 카드 주소 테이블을 위조하여 트래픽을 자신에게 우회시키는 공격
E-mail spoofing	이메일 발송시 송신자의 주소를 위조
DNS spoofing	도메인의 DNS 컴퓨터를 장악하여 통제, 다른 홈페이지로 연결하게 하여 정보 갈취

공격자는 표 1과 같은 시도를 하여 데이터를 도청, 변조, 파괴함으로써 상대방에게 피해를 입히게 된다. 이것은 공격대상을 공격하는 것과 동시에 자신의 정보가 노출되지 않음으로 임의의 상대를 공격자로 오인 받게 만들 수 도 있고 또한 실제로 많은 경우에서 그런 공격이 행해진다.

2.2 DSTM

IPv4와 IPv6가 혼용되는 초창기에는 소수의 IPv6네트워크가 존재하고 다수의 IPv4기반의 네트워크가 존재한다. 이 상황에서 IPv6호스트가 정상적으로 IPv4단말과 통신하기 위해서는 IPv4주소를 할당받아야 하는데 이 역할을 하는 것이 DSTM 기술이다. DSTM의 전제조건은 IPv6 호스트가 IPv4와 IPv6 스택을 모두 지원하는 듀얼 IP계층이 있어야 한다. DSTM은 IPv6전용 노드에 대한 솔루션이 아니며 IPv6 호스트가 IPv4 호스트에 접근할 수 있게 만들어주는 기술이기 때문이다. 그림 1은 DSTM의 구조를 나타내고 그림 2는 기본적인 DSTM process과정을 나타내고 있다.



[그림 1] DSTM 구조

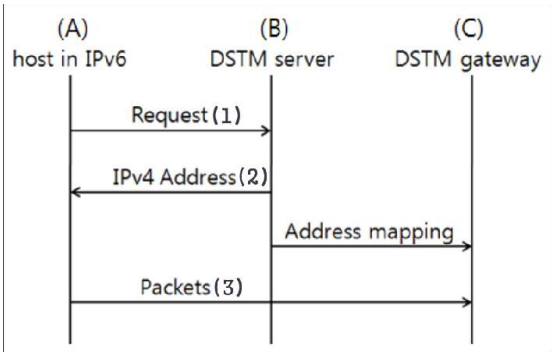
그림 1의 구성요소 A, B, C는 다음과 같다.

A) IPv6 host : IPv4를 사용해서 통신을 해야 하는 듀얼스택 호스트

B) DSTM server : Global IPv4주소를 담고 있는 IPv4 pool과 DSTM gateway (TEP)를 관리하는 DSTM 서버

C) DSTM gateway : IPv4 over IPv6 패킷을 encapsulation/ decapsulation 하는 DSTM gateway

DSTM 구조에서는 오직 (C)만 IPv4 와의 직접적인 접속 그리고 영구적인 IPv4주소 하나를 필요로 한다.



[그림 2] 기본적인 DSTM 프로세스

DSTM의 기본적인 동작 절차는 다음과 같다.

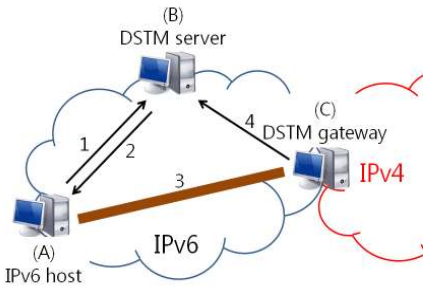
IPv6에 속해있는 호스트(A)가 IPv4로의 통신을 필요로 할 때 DSTM 서버에 임시적인 IPv4주소를 요구한다. (1) 그림 2에서 DSTM 서버 (B)는 (A)를 위한 하나의 IPv4 어드레스를 IPv4 어드레스 풀에서 꺼내어 응답으로 제공한다. 응답 메시지 (2)는 또한 할당된 주소의 유효시간과 DSTM gateway (TEP)에 관한 정보를 담고 있다.

이 메시지 교환에 따라서(DHCPv6, RPC 등을 사용해 수행될 수 있는) (A)는 자신의 IPv4 스택에 할당받은 주소를 설정한다. 연결 (3)부터 A로부터 오는 모든 IPv4 패킷들은 encapsulation /decapsulation을 수행하기 위해 터널링(IPv4 over IPv6)되어 (C)로 향한다. DSTM gateway (C)는 인트라넷 호스트들의 IPv4와 IPv6 주소를 매핑시킨 테이블을 가지고 있다. 양 방향 통신을 확실히 하기위해 IPv4 라우팅은 (C)를 통하여 (A)를 지나는 모든 패킷에 대하여 보장해야한다[5].

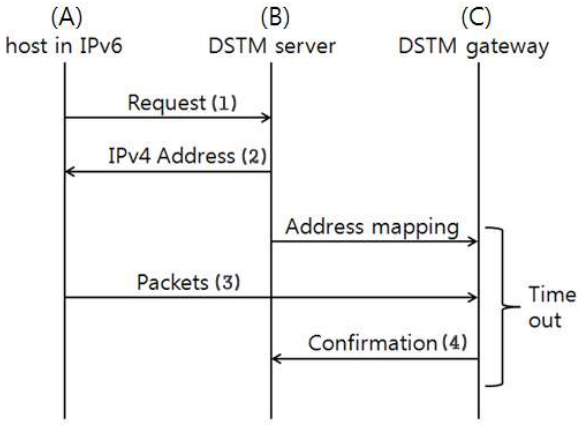
살펴본 DSTM 과정에서의 보안상 문제는 IPv4 주소 할당에 대한 인증 절차가 전무하여 DSTM 서버가 속한 네트워크에 있는 어떠한 호스트의 요청이라도 모두 응답을 해준다는 것이다. 만약 악의적인 공격자가 IP 스푸핑을 이용하여 IPv4주소 할당을 여러 차례 요구 한다면 DSTM서버는 그 때 마다 자신의 IPv4 어드레스 풀에 있는 글로벌 IPv4 주소들을 할당해 주어 나중에는 IPv4 주소가 고갈 될 수 있다[6].

3. 인증절차 설계 DSTM 인증 제안

IPv6 네트워크에 있는 악의적인 공격자 호스트에 대한 IPv4 글로벌 주소 할당 스푸핑 문제에 대하여 본 논문은 사용자 유효성 검사와 더불어 실제 사용 확인을 위한 다음과 같은 인증방식을 제안한다. 개선된 DSTM 구조는 그림3과 같고 개선된 DSTM 절차는 그림 4와 같다.



[그림 3] 개선된 DSTM 구조



[그림 4] 개선된 DSTM 절차

개선된 DSTM 절차에서의 차이점은 DSTM gateway의 확인패킷 송신에 있다. DSTM 서버(B)는 확인패킷을 수신 받게 되는데 그것에는 두 가지 의미가 있다. 첫째로 네트워크 내의 유효한 IPv6 호스트(A)가 Request를 했다는 것을 확인하는 것과 실제로 (A)가 IPv4 네트워크 내의 목표 단말인 목적지 호스트에 패킷을 보냈다는 것을 확인한다는 의미를 가진다. 확인패킷은 표 2와 같은 정보를 가지고 있다.

<표 2> 확인패킷의 구조

항목	내용
src	DSTM gateway address(IPv6)
dst	DSTM server address(IPv6)
sender	host (A) address(allocated IPv4)
recv	dst host address(IPv4)
time	current time

만약 임의의 공격자가 DSTM 서버내의 글로벌 IPv4를 고갈시키기 위해 IP 스푸핑을 사용하여 무작위로 Request메시지(1)을 보낸다면 할당 되었던 글로벌 IPv4 어드레스는 얼마 안가 타임아웃 시간 내에 DSTM 서버가 확인패킷을 받지 못하게 됨으로 수신 부재에 의해 회수된다. 이 때 보내지는 스푸핑 메시지는 송신자 호스트의 존재 유무에 따라 두 가지로 나뉜다.

첫째, 유효한(존재하는 host) IPv6로 스푸핑된 Request 메시지, 둘째, 유효하지 않은(실제 존재하지 않은) IPv6 호스트 주소로 스푸핑 된 경우이다. 제안한 방법을 적용하면 설명한 두 가지 스푸

핑 경우에 대해 동일하게 적용된다.

DSTM gateway (TEP)는 첫 번째 패킷이 IPv6 호스트(A)에서 자신을 거쳐 IPv4 네트워크 내의 목적지 호스트에 보내지면 확인패킷을 DSTM 서버에 보내게 된다. 만약 지정된 타임아웃 시간 안에 DSTM 서버가 DSTM gateway (TEP) 로부터 확인패킷을 수신 받지 못하면 할당했던 글로벌 IPv4를 다시 회수함과 동시에 DSTM gateway로 재 매핑 요청을 하게 된다.

확인패킷에 의한 패킷전송 확인 절차를 사용해 IP 스푸핑에 의한 글로벌 IPv4의 무분별한 할당을 방지할 수 있으며 이로 인해 DSTM 서버에 있는 자원을 효과적으로 관리할 수 있다.

4. 결론

현재 구성되어 운영되고 있는 IPv4 네트워크망 기반에서 IPv6가 점진적으로 확대될 것이다. 이에 따라 많은 기관에서는 DSTM등 IPv4/IPv6 병행 사용 환경에서의 기술을 만들었고 그 부분에서 많은 보안상의 취약점 들이 노출 되어있다. 본 논문에서는 DSTM 방식에서의 보안상의 문제점을 분석하고 이를 위해 DSTM의 터널링을 위한 IPv6호스트로의 IPv4주소할당 과정을 살펴보았다. 그 절차 중에서 스푸핑에 의한 무분별한 IPv4주소 할당에 대해 분석하고 확인패킷을 통해 보안상의 문제점을 극복할 수 있는 방법을 제안하였다. 이 절차에 의해 DSTM서버는 자신의 확인패킷 수신여부에 따라 부당한 방법으로 할당된 IPv4 주소의 회수가 가능하게 되었고 그 결과 IP 스푸핑에 의한 글로벌 IPv4주소의 고갈 문제를 해결할 수 있게 되었다.

향후 과제로는 제안한 이론에 대한 실제 구현과 테스트, 그리고 그에 따른 네트워크 부하에 대해서 연구 되어야 할 것이다.

[참고문헌]

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC2460, December 1998.

[2] Y. Shirasaki, S. Miyakawa, T. Yamasaki, A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service," RFC4241, December 2005.

[3] Jim Bound (Nokia Networks), "Dual Stack Transition Mechanism (DSTM)," IETF, Mar 2001.

[4] L. Todd Heberlein , Matt Bishop, "Attack Class: Address Spoofing," Department of Computer Science University of California, Oct 1996.

[5] http://www.ipv6.rennes.enst-bretagne.fr/dstm/

[6] 최인석, 정수환, 김영한, “IPv6 전환 기술의 보안 위협 분석 및 보안 설계에 대한 연구”, 한국 통신학회 논문지, Nov. 2005.