DSTM 터널링 보안 취약점 분석

조혁현* · 김정욱** · 노봉남***

Analysis for Security Vulnerabilities on DSTM Tunneling

Hyug-hyun Cho* · Jeong-wook Kim** · Bong-nam Noh***

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행 되었음
(IITA-2007-C1090-0701-0027)

요 약

IPv6는 IETF가 IPv4를 대체하기 위해 제안한 프로토콜이며, 기존 IPv4 네트워크와 새롭게 추가되는 IPv6 네트워크 간의 원활한 통신을 위해 다양한 메커니즘이 연구 및 개발되었다. IPv4/IPv6 전환 메커니즘 중 DSTM 터널링 방법은 IPv6 네트워크 내의 듀얼스택 호스트가 동적으로 IPv4 주소를 할당 받아 IPv4 주소만을 가지는 노드와 통신을 할 수 있으며, IPv6 네트워크에서 IPv4 전용 어플리케이션을 수정 없이 사용할 수 있다는 특징을 가지고 있다. 본 논문에서는 DSTM을 이용하는 네트워크에서 발생 가능한 DHCP 공격, TEP 공격, 소스 스푸핑 공격에 대한 보안 취약점들에 대해서 기술하고, 실험을 통하여 이를 확인하였다.

ABSTRACT

IPv6 is a protocol to solve the address space limitation of IPv4 by IETF. Many transition mechanism to communicate between IPv4 and IPv6 in mixed IPv4/IPv6 network are proposed. DSTM tunneling is a mechanism that dual stack in IPv6 network is able to communicate with node in IPv4 network by dynamic allocating the IPv4 address. This mechanism supports the execution of IPv4 dependent application without modification at IPv6 network. In this paper, we explain the security vulnerability at DSTM network for DHCP attack, TEP attack, and source spoofing attack then describe the result of attacks.

키워드

Attack, DSTM, IPv4/IPv6, Security, Transition mechanism

Ⅰ. 서 론

IPv6가 IETF에 의해 제안된 이후[1], IPv4에서 IPv6로 전환하기 위한 많은 연구가 진행되고 있다. 또한 IPv6를 지원하는 네트워크 장비들이 상용화되고 있다. 그러나 현재 대부분의 인터넷을 이용하는 호스트 및 라우터 등의 네트워크 장비가 IPv4만을 지원하는 것을 고려할 때, 모든 네트워크를 IPv4에서 IPv6로 전환하는 것은 비용과 시간적인 점을 고려할 때 불가능하다. 따라서 IPv4와 IPv6가 공존하는 네트워크가 상당 기간 존재할 것이다. 이를 위하여 IPv4와 IPv6가 혼재한 네트워크에서 원활한 통신을 위한 다양한 메커니즘이 연구

* 전남대학교 문화콘텐츠학부
** 전남대학교 정보보호협동과정
*** 전남대학교 전자컴퓨터정보학부
접수일자 : 2007. 10. 25
심사완료일자 : 2007. 11. 29

및 개발되었다.

IPv4/IPv6 전환 메커니즘에는 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation)이 있다. 이러한 기술들은 다양한 사용자의 컴퓨팅 환경과 요구를 충족시키기 위하여 제안 및 개발되었고, 대부분의 기술이 IETF에서 RFC 문서로 표준화가 완료되었다[2][3].

IPv4/IPv6 전환 메커니즘 중 터널링 방법에서 DSTM(Dual Stack Transition Mechanism)[4]은 자동 터널링 방식 중에 하나로써, IPv6 네트워크의 노드가 IPv4 네트워크의 IPv4 주소만을 가지는 노드와 원활한 통신을 위해 개발된 메커니즘이다. 특히 DSTM은 IPv4 프로토콜을 그대로 사용할 수 있기 때문에 IPv6 네트워크에서도 IPv4 전용 어플리케이션을 수정 없이 사용할 수 있다는 특징을 가지고 있다. 따라서 IPv4 전용 어플리케이션을 이용하기를 원하는 IPv6 노드의 경우 DSTM을 이용할 것이다.

본 논문에서는 2장에서 터널링 기술과 DSTM에 대해서 기술하고, 3장에서 DSTM을 이용함으로써 나타날 수 있는 보안 취약점에 대해서 기술한다. 4장에서는 기술된 보안 취약점에 대한 실험 및 결과에 대해서 기술한다.

II. 관련 연구

2.1 IPv4/IPv6 터널링

IPv4/IPv6 전환기술은 IPv4와 IPv6가 공존하는 네트워크에서 서로 다른 두 프로토콜간의 원활한 통신을 위해 연구되어진 기술이다. IPv4/IPv6 전환기술에는 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation) 메커니즘이 있다. 듀얼 스택은 하나의 시스템에서 IPv4 프로토콜 스택과 IPv6 프로토콜 스택을 모두 가지고 IPv4와 IPv6 프로토콜을 동시에 지원한다. 터널링 기술은 다른 프로토콜과 통신을 위해 새로운 IP 헤더로 캡슐화하여 패킷을 전송하는 기술이며[5], 변환 메커니즘은 듀얼 스택을 지원하지 않는 IPv6 전용 단말과 IPv4 단말 사이의 통신을 지원하기 위해 패킷의 특정 계층을 변환하는 기술이다.

터널링 기술은 6in4, 6to4, ISATAP, DSTM, Tredo, Tunnel Broker와 같은 터널링 방법을 표준으로 정하고 있다. 표 1은 터널링 기술의 기본 개념과 유용성에 대해서 설명한다[2][3].

표 1. 터널링 기술의 기본 개념과 유용성
Table 1. Tunneling concept and facility

구분	기본 개념	유용성
6in4	수동 터널링 방식으로 IPv4 망을 통하여 IPv6 패킷 통신 필요	관리자 설정에 의해 정적 터널 유지 및 라우터 사이의 터널 연결에 유용
6to4	동적 터널링 방식으로 IPv4 망을 통하여 IPv6 패킷 통신 필요	필요 시 자동 터널 생성 및 호스트 간 터널 연결에 유용
ISATAP	IPv4 인트라넷에 있는 Dual Stack 호스트가 IPv4 인프라를 통해 IPv6 메시지 자동 터널링	IPv4 기반의 인트라넷에서 IPv6 호스트 설치 가능
DSTM	IPv6 호스트가 IPv4 호스트 및 어플리케이션 이용 필요	IPv4 전용 어플리케이션의 수정 불필요
Teredo	IPv4 NAT 내부에서 사설 IP를 이용하는 호스트가 IPv6 호스트와 통신 필요	인터넷 공유기를 사용하는 가정이나 소규모 기업에서도 IPv6 통신 가능
Tunnel Broker	Tunnel Broker라는 전용 서버를 구축하여 사용자의 터널 요청을 자동으로 관리	관리자에 의한 설정 터널링을 자동으로 관리함으로 관리 오버헤드 감소

2.2 DSTM 터널링

Internet-Draft Dual Stack IPv6 Dominant Transition Mechanism[6] 문서에서 IPv6 전환기술 중 하나로써 정의되고 있는 DSTM 기술은 듀얼스택 호스트 상의 IPv4 응용이 IPv4 호스트와 통신을 필요로 하는 환경에서 IPv4-in-IPv6 터널링을 제공한다.

DSTM 터널링은 그림 1과 같이 DSTM 서버, TEP (Tunnel End Point), DSTM 호스트로 구성된다. DSTM 서버는 DSTM 호스트에 할당되는 IPv4 주소를 관리하고, TEP는 IPv6 전용 네트워크와 IPv4 네트워크 간의 경계 라우터 역할을 하며 IPv4-in-IPv6 패킷에 대한 캡슐화 및 디캡슐화 작업을 수행한다. 그리고 DSTM 호스트는 DSTM 서버로부터 일시적으로 사용 가능한 IPv4 주소를 할당받은 듀얼스택 호스트이다[7].

그림 1은 DSTM 통신을 나타내며 다음과 같은 순서로 이루어진다.

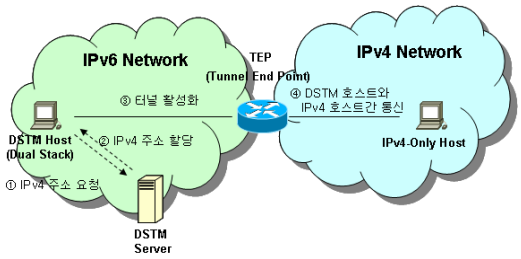

그림 1. DSTM 통신
Fig. 1 DSTM communication

① 듀얼스택인 DSTM 호스트는 IPv4 호스트와의 통신을 위해서 DSTM 서버에게 일시적으로 사용 가능한 IPv4 주소를 요청

② 서비스 요청을 받은 DSTM 서버는 DSTM 호스트에게 공인 IPv4 주소를 UDP패킷으로 할당하고, 동시에 IPv4-in-IPv6 터널 통신을 수행할 TEP의 IPv6 주소를 제공

③ DSTM 호스트는 DSTM 서버로부터 할당받은 IPv4 주소를 이용하여 IPv4 프로토콜을 설정하고 TEP의 IPv6 주소 정보를 이용하여 DSTM 호스트와 TEP 간의 IPv4-in-IPv6 터널 인터페이스를 활성화 시킨 후 터널 기반 통신을 시작

④ IPv4 호스트에서 IPv4주소로 DSTM 호스트로 패킷을 전송하면, TEP에서 DSTM 호스트의 IPv4 주소와 IPv6주소의 매핑 테이블을 관리하고 있기 때문에 IPv4 호스트에서 DSTM 호스트로 이상 없이 통신이 가능

III. DSTM 보안 취약점

DSTM은 서버와 클라이언트 또는 TEP와 클라이언트간의 인증 기능이 없기 때문에 DSTM의 구성 요소들이 역할을 수행하지 못하거나 신뢰할 수 없을 경우 많은 보안 취약점을 가지고 있다. DSTM 서버나 TEP가 공격자에 의해 공격당해 역할을 수행하지 못할 경우 서비스 거부 공격이 가능하며, DSTM 서버나 TEP를 가장한 공격자에 의해 서비스 거부 공격이나 중간자 공격이 가능하다[8].

3.1 DHCP 공격

공격자에 의한 DSTM 서버 공격은 서비스 거부 공격을 유발할 수 있다. DSTM 클라이언트로 가장한 공격자는 다량의 DHCP 요청을 발생함으로써 DHCPv6 (DSTM) 서버의 과부하를 초래하고, 관리 중인 주소 공간의 오버플로우로 정상적인 질의/응답 처리를 방해할 수 있다. 공격자는 DSTM 서버로 다량의 DHCPv6 요청 패킷을 보낸다. 이때 DSTM 서버가 관리하는 주소 영역에서 사용가능한 주소를 선택한 후, 주소를 요청노드로 제공하는데, 공격자가 다량의 요청 패킷을 보내는 경우, DHCPv6 서버가 관리하는 주소공간이 급격히 감소되어 고갈될 수 있다. 이후 정상적인 DSTM 클라이언트에 의한 주소 요청은 실패하게 되어 서비스 거부 공격에 노출된다.

3.2 TEP 공격

TEP 공격은 서비스 거부 공격, 중간자 공격을 유발할 수 있다. 공격자는 TEP를 가장함으로써 DSTM 클라이언트간의 통신을 방해하고 패킷의 내용을 변경할 수 있다. DSTM 서버를 가장한 공격자는 클라이언트의 DHCPv6 질의에 대한 응답으로 공격자의 IPv6 주소를 TEP에 지정하여 전송한다. 응답을 수신한 클라이언트는 IPv4 헤더의 소스 주소에 자신의 IPv4 주소를 지정하고, 패킷에 지정된 TEP의 IPv6 주소로 패킷을 전송한다. 패킷을 수신한 공격자는 클라이언트의 패킷을 가로채어 임의의 곳으로 전송하거나 내용을 변경할 수 있다. 또한, 공격자는 패킷 내부의 IPv4 주소를 자신의 IPv4 주소로 변경하여 TEP로 전송할 수 있다. 목적지 호스트로 부터의 응답 패킷은 TEP를 경유하여 공격자로 전송되며, 공격자는 IPv4 목적지 주소를 DSTM 클라이언트의 IPv4로 변경하여 DSTM 클라이언트로 전송한다. 결국 DSTM 클라이언트와 목적지 호스트 간의 모든 트래픽은 항상 공격자를 경유하게 된다.

DSTM 서버를 가장한 공격자는 DHCPv6 응답 시 특정 TEP 주소를 지정함으로써 DSTM 도메인 내의 모든 패킷의 전달 경로 상에 위치하도록 하고, TEP의 처리 부하를 발생시킨다. DSTM 서버는 DSTM 클라이언트

의 DHCPv6 요청에 대한 응답으로 클라이언트에 할당할 IPv4 주소, TEP의 IPv6 주소, 유효 시간 및 옵션을 전송한다. 이때 모든 DSTM 클라이언트가 보내는 요청에 특정 TEP의 주소를 지정하게 되면, 모든 DSTM 클라이언트는 항상 동일한 TEP으로 패킷을 전송하게 되며, IPv4로의 응답 패킷도 같은 TEP을 경유하게 되므로 TEP에서의 트래픽 처리 부하가 발생할 수 있다.

3.3 소스 스푸핑 공격

소스 스푸핑은 서비스 거부 공격을 유발할 수 있다. DSTM 서버를 가장한 공격자는 잘못된 IPv4 주소를 할당함으로써 IPv4 네트워크의 특정 노드로 원하지 않은 패킷을 보낼 수 있다. DSTM 클라이언트의 DHCPv6 질의에 대한 응답으로 희생 노드의 IP 주소를 할당해 준다. 클라이언트는 할당 받은 IPv4 주소를 소스 주소로 지정하고 패킷 외부에 IPv6 헤더를 추가하여 TEP으로 전송한다. TEP은 IPv6 헤더를 제거하고 IPv4 패킷을 특정 호스트로 전송한다. Node A는 수신 패킷에 지정되어 있는 소스 IPv4 주소로 응답 패킷을 전송한다. 이때 희생 호스트는 자신이 원하지 않은 패킷을 수신하게 되고, 서비스 거부 공격에 노출될 수 있다.

Ⅳ. 실험 및 분석

본 장에서는 3장에 기술된 취약점에 대한 실험 및 결과를 기술한다. 실험 환경은 DSTM 서버, TEP, 클라이언트는 리눅스 환경에서 DSTM.0610[9] 패키지 설치를 통해 실험환경을 구축하였다. DSTM 서버와 TEP는 동일한 시스템에서 동작한다. 그리고 패킷 분석을 위하여 이더리얼 0.99[10]를 이용하였다.

4.1 DHCP 공격 실험

그림 2는 DSTM DHCP 공격을 실험하기 위한 환경을 나타낸 것으로써 DHCP 공격 실험 방법은 다음과 같다.

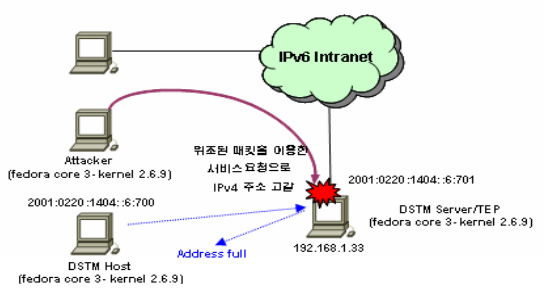

그림 2. DSTM DHCP 공격 실험 환경
Fig. 2 The configuration of DSTM for DHCP attack

① DSTM Host로 가장한 공격자는 IPv6 소스 주소를 스푸핑하여 DSTM 서버에게 IPv4 주소를 요청
② DSTM 서버는 DSTM Host로 가장한 공격자에게 IPv4 주소를 할당
③ 공격자는 IPv6 소스 주소를 반복적으로 위조하여 ①②과정을 반복하여 DSTM 서버의 주소 고갈
④ 정상적인 DSTM Host의 주소 요청에 IPv4 주소 할당 확인을 통해 공격 검증

그림 3과 그림 4는 공격자가 정상적인 DSTM 서비스 패킷을 수집하여 위조할 수 있음을 알 수 있다. 공격자는 IPv6 소스 주소를 반복적으로 위조하여 DSTM 서버에게 IPv4 주소를 요청함으로써 DSTM 서버가 가지고 있는 IPv4 주소를 고갈시킬 수 있다.

그림 5는 정상적인 DSTM 호스트의 IPv4 주소 요청에 “no avaliale lease”를 출력하며 주소 할당이 되지 않음을 확인할 수 있다. 이는 주소 고갈에 의한 서비스 거부 공격에 노출 될 수 있음을 보여준다.

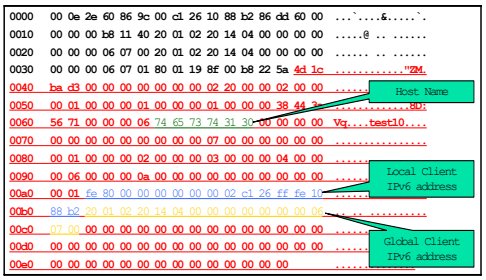

그림 3. 정상적인 DSTM 서비스 패킷
Fig. 3 Normal DSTM packet

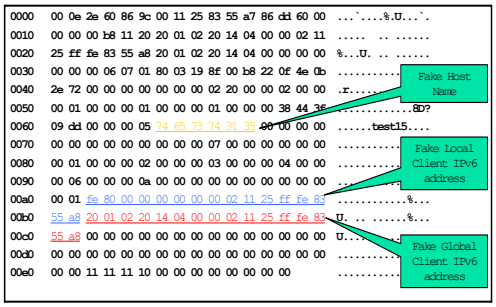

그림 4. 위조된 DSTM 서비스 패킷
Fig. 4 Fake DSTM packet

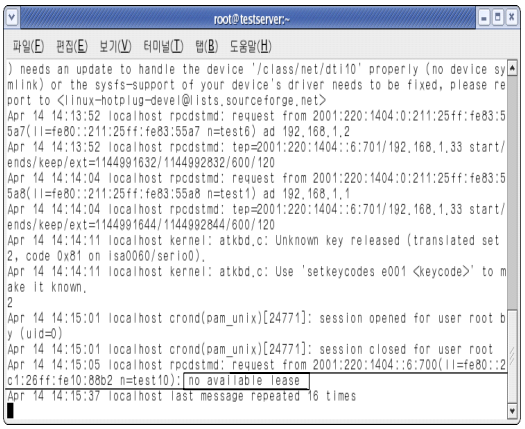

그림 5. DSTM 서버로 부터의 주소고갈 메시지
Fig. 5 Address depletion message from DSTM server

4.2 TEP 공격 실험

그림 6은 DSTM TEP 공격을 실험하기 위한 환경을 나타낸 것으로써 TEP 공격 실험 방법은 다음과 같다.

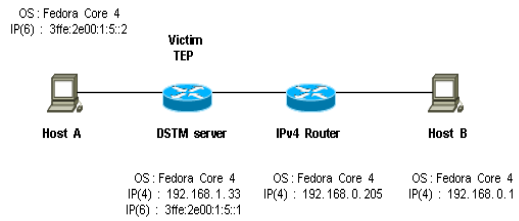

그림 6. DSTM TEP 공격 실험 환경
Fig. 6 The configuration of DSTM for TEP attack

① Host A는 DSTM 서버에게 IPv4 주소를 요청
② DSTM 서버는 Host A에게 IPv4 주소 할당과 공격자 TEP 주소 응답
③ Host A는 TEP에게 Host B에게 보낼 패킷 전송
④ TEP는 패킷 수신 후 패킷 수정 또는 삭제
⑤ 정상 패킷과 위조되어 전송된 패킷의 TTL 값을 통해 공격 검증

그림 7은 호스트 A에서 전송한 Echo Request 메시지로 Hop limit 값이 64임을 보여준다.

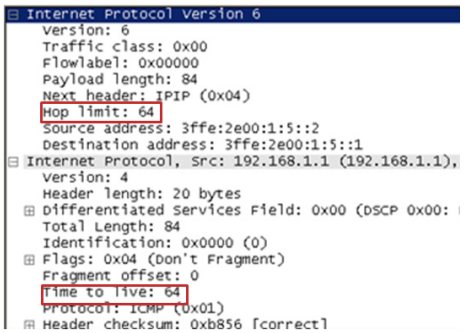

그림 7. Host A에서 전송한 echo request
Fig. 7 Echo request from host A

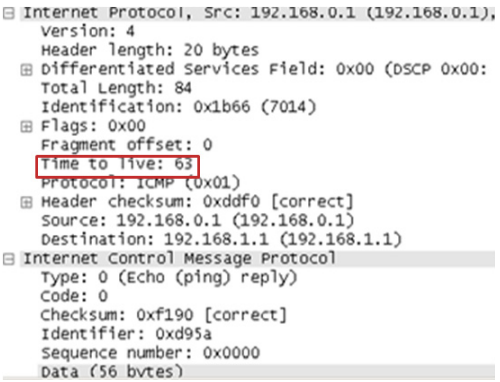

그림 8. Host A에서 수신한 비정상 echo reply
Fig. 8 Host A receives abnormal echo reply

그림 8은 Host A에서 수신한 Echo Reply 메시지로 TEP에서 패킷 수정 후 전송된 패킷을 나타낸다. TEP에서 전송되었기 때문에 Time to live 값이 63임을 확인할 수 있다. 이는 TEP를 가장함으로써 서비스 거부 공격이나 중간자 공격에 노출 될 수 있음을 보여준다.

4.3 소스 스푸핑 공격 실험

그림 9는 DSTM 소스 스푸핑 공격을 실험하기 위한 환경을 나타낸 것으로써 소스 스푸핑 공격 실험 방법은 다음과 같다.

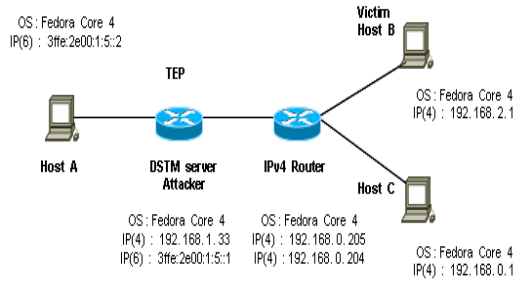

그림 9. DSTM 소스 스푸핑 공격 실험 환경
Fig. 9 The configuration of DSTM for source spoofing attack

① Host A는 DSTM 서버에게 IPv4 주소를 요청
② DSTM 서버를 가장한 공격자는 Host B의 주소와 같은 IPv4 주소를 할당
③ Host A는 TEP를 통해 Host C에게 패킷 전송
④ Host C는 Host A가 전송한 패킷 수신 후, Host B에게 응답 패킷 전송
⑤ Host B에서 Host C가 응답한 패킷 수신 확인을 통해 공격 검증

```
⊞ Internet Protocol Version 6
⊟ Internet Protocol, Src: 192.168.2.1 (192.168.2.1),
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00:
    Total Length: 84
    Identification: 0x0000 (0)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0xb756 [correct]
    Source: 192.168.2.1 (192.168.2.1)
    Destination: 192.168.0.1 (192.168.0.1)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x376a
    Identifier: 0xde79
    Sequence number: 0x0000
    Data (14 bytes)
```

그림 10. Host A에서 Host C로 전송한 echo request
Fig. 10 Echo request from host A to host C

Host A는 IPv4 노드와 통신을 위해 DSTM 서버로 IPv4 주소를 요청했지만, 공격자에 의해서 Host B와 동일한 주소를 할당받는다. Host A는 할당 받은 주소를 이용하여 Host C로 통신하기 위해서 자신의 IPv6 주소를 소스 주소로, DSTM TEP를 목적지 주소로 하는 IPv6 헤더로 캡슐화하여 패킷을 전송한다. 그림 10은 Host A에서 Host C로 전송한 Echo Request 패킷의 소스 주소를 보여준다. IPv4 헤더의 소스 주소가 Host B와 같은 주소로 위조되어 있는 것을 확인할 수 있다.

```
⊟ Internet Protocol, Src: 192.168.0.1 (192.168.0.1)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00:
    Total Length: 84
    Identification: 0xe90e (59662)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x0e48 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.2.1 (192.168.2.1)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x3f6a
    Identifier: 0xde79
    Sequence number: 0x0000
    Data (54 bytes)
```

그림 11. Host B에서 수신한 echo reply
Fig. 11 Host B receives echo reply

그림 11은 Host A에서 전송한 Echo Request에 대한 응답으로, Host C에서 전송된 패킷이 Host B에서 수신된 것을 나타낸다. 이는 공격자가 의도한 잘못된 IPv4 주소 할당함으로써 Host B는 원치 않는 패킷을 수신하게 되어 서비스 거부 공격에 노출될 수 있음을 보여준다.

V. 결 론

DSTM은 IPv4/IPv6 전환 메커니즘 중 터널링 방법의 하나로 IPv6 네트워크 내의 듀얼스택 호스트가 IPv4 네트워크 내에 존재하는 IPv4 노드와 통신을 할 수 있게 해준다. 본 논문에서는 DSTM 터널링을 이용함으로써 발생할 수 있는 보안 취약점인 DHCP 공격, TEP 공격, 소스 스푸핑 공격에 대해서 기술하고, 실제 실험 환경을 구축하여 실험하였다.

실험결과, DSTM 터널링은 서버와 클라이언트 또는

TEP와 클라이언트 간의 인증기능이 없기 때문에 DSTM의 구성 요소들이 역할을 수행하지 못하거나 신뢰할 수 없을 경우 많은 보안 취약점을 가지고 있으며, 공격자의 DHCP 공격, TEP 공격, 소스 스푸핑 공격에 의해 서비스 거부 공격이나 중간자 공격에 노출될 수 있음을 확인했다.

향후에는 본 논문에서 설명한 보안 취약점에 대한 대응방안을 연구할 필요가 있다.

참고 문헌

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 Specification", RFC 2460, IETF, Dec. 1998.

[2] T. Narten and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, Jan. 2001.

[3] F. Templin, T. Gleeson, M. Talwar and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol", RFC 4214, IETF Oct. 2005.

[4] J. Bound, L. Toutain and JL. Richier, "Dual Stack IPv6 Dominant Transition Mechanism", draft-bound-dstm-exp-04.txt, IETF, Oct. 2005.

[5] B. Carpenter, "Connection of IPv6 Domains via IPv4 clouds", RFC 3056, Feb. 2001.

[6] http://www.6bone.net/ngtrans/

[7] 이희철, 이주철, 김용운, 김형준, "IPv6망을 기반으로 하는 IPv4/IPv6 연동 메커니즘 : DSTM", Telecommunication Review Vol. 14, No. 5, Oct. 2005.

[8] 시스템보안연구센터, "IPv4/IPv6 전환기술 보안 해설서", 2006.

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

[10] Ethereal, http://www.ethereal.com/

저자 소개

조혁현(Hyug-hyun Cho)

1984년 2월 : 홍익대학교 전자계산학과 학사

1989년 2월 : 전남대학교 대학원 전산통계학과 석사

1997년 2월 : 전남대학교 대학원 전산통계학과 박사수료

1989년 3월~현재 : 전남대학교 문화콘텐츠학부 교수

※관심분야 : 정보보안, 침입탐지, 시스템 및 네트워크 보안, 데이터베이스

김정욱(Jung-wook Kim)

2005년 2월 : 전남대학교 컴퓨터정보학부 졸업

2006년 3월 ~ 현재 : 전남대학교 대학원 정보보호협동과정

※관심분야 : 네트워크 침입탐지, 침입 패턴 분석, IPv6 네트워크 보안

노봉남(Bong-nam Noh)

1978년 2월 : 전남대학교 수학교육과 학사

1982년 2월 : KAIST 대학원 전산학과 석사

1994년 2월 : 전북대학교 대학원 전산과 박사

1983년 ~ 현재 전남대학교 전자컴퓨터정보학부 교수

2000년 ~ 현재 시스템 보안연구 센터 소장

※ 관심분야 : 컴퓨터와 네트워크 보안, 정보보호시스템, 디지털 포렌식, 사이버사회와 윤리