IPv6 전환 기술의 보안 위협 분석 및 보안 설계에 대한 연구

준회원 최 인 석*, 정회원 정 수 환*, 김 영 한*

A Study on Security Analysis and Security Design for IPv6 Transition Mechanisms

Inseok Choi* *Associate Member*, Souhwan Jung*, Younghan Kim* *Regular Members*

요 약

IPv4로부터 IPv4/IPv6로의 전환 및 상호공존을 위한 처리 과정에서의 보안적인 고려는 상당히 중요한 문제이다. IPv4 네트워크와 IPv6 네트워크사이의 이질적인 문제로 인해 기존의 IPv4 네트워크에서는 일어나지 않았던 다양한 위협이 존재한다. 본 논문에서는 지금까지 제안된 IPv4/IPv6 전환 기술에 대해 살펴보고, 전환 기술에서 나타날 수 있는 다양한 보안적인 위협에 대해서 분석을 하고, 그에 대한 대응방안에 대해 제시하였다. 6to4 전환 기술에서는 DoS 및 DRDoS 공격 위협을 분석하고, 주소 무결성 검사방법을 해결책으로 제시하였다. 또, DSTM 과 NAT-PT 전환 기술에서는 IPv4 주소를 할당하는 IPv4 주소 pool을 가진 서버에 대한 IPv4 주소 고갈 위협을 분석하였고, IPv4 주소 고갈 위협 문제를 해결하기 위해서 DSTM 전환 기술에서는 challenge-response 메커니즘 방안을 제시하였다.

Key Words : IPv6, IPv6 Transition, 6to4, DSTM, NAT-PT, Security.

ABSTRACT

The IETF has created the v6ops Working Group to assist IPv6 transition and propose technical solutions to achieve it. But it's quite problem which security consideration for a stage of IPv4/IPv6 transition and co-existence. There are new security problem threat that it caused by the characteristics of heterogeneity. In this paper, we describe IPv6 transition mechanisms and analyze security problem for IPv6 transition mechanism. also we propose security consideration and new security mechanism. We analyzed DoS and DRDoS in 6to4 environment and presented a address sanity check as a solution. We also showed an attack of address exhaustion in address allocation server. To solve this problem, we proposed challenge-response mechanism in DSTM.

Ⅰ. 서 론

1.1 개 요

인터넷의 급격한 성장으로 IPv4의 주소공간의 문제가 발생하였다. 그에 대한 해결을 위해 새로운 인터넷 프로토콜인 IPv6[1]가 등장하였다. 하지만 당장 IPv6를 IPv4로 대체할 수는 없기 때문에 IPv4와 IPv6 공존을 위해서 다양한 IPv4/IPv6 전환 기술[2][3]들이 제시되어 왔다. 하지만 IPv4 네트워크와 IPv6 네트워크 사이의 이질적인 문제로 인해 기존의 IPv4 네트워크에서 가능하지 못했던 다양한 보안적인 위협이 존재하게 되었다. IPv6/IPv4 터널링

* 숭실대학교 정보통신전자공학부
교신저자 : 정수환 souhwanj@ssu.ac.kr
논문번호 : KICS2005-01-055, 접수일자 : 2005년 1월 31일
※본 연구는 숭실대 교내 연구비 지원으로 수행하였습니다.

방법[2]에서는 공격자가 소스 주소를 스푸핑한 IPv6 데이터그램을 IPv4 헤더로 캡슐화하여 DoS[4]공격을 할 수 있고, 또 IPv4/IPv6 변환에서는 IPv4 노드와 통신을 지원하기 위해서 IPv6 노드에게 IPv4 주소를 할당하는 IPv4 주소 서버들에 대한 고갈 공격이 발생할 수 있는 위협이 존재한다. 그렇기 때문에 IPv4/IPv6 전환 과정에서 발생할 수 있는 보안적인 위협을 분석하는 것은 IPv4/IPv6 전환을 실질적으로 적용하기 전에 반드시 선행되어야 한다. 본 논문에서는 IPv4/IPv6 전환 과정에서 발생할 수 있는 보안적인 위협에 대해 분석하고, 보안적인 문제를 해결하기 위한 대응 방안을 제시할 것이다.

1.2 IPv6 전환 기술

1.2.1 IPv4/IPv6 듀얼 스택 방법

IPv6 노드가 IPv4 전용 노드와 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 이용하는 방법이다. IPv4/IPv6 듀얼스택 노드는 IPv4와 IPv6 패킷을 모두 주고받을 수 있는 능력이 있다. IPv4 패킷을 사용하여 IPv4 노드와 직접 통신을 하거나 IPv6 패킷을 사용하여 IPv6 노드와 직접 통신을 할 수 있다.

1.2.2 IPv4/IPv6 터널링 방법

IPv4/IPv6 호스트와 라우터는 IPv6 데이터그램을 IPv4 패킷에 캡슐화하여 IPv4 라우팅 토폴로지 영역을 통해 터널링을 할 수 있다. 터널링은 기존의 IPv4 라우팅 인프라를 이용하여 IPv6 트래픽을 전송하는 방법을 제공한다. 이러한 터널링 방법은 크게 설정 터널링(configured tunneling) 방식과 자동 터널링(automatic tunneling) 방식[2][3]으로 구분된다.

1) 설정 터널링(configured Tunneling) 메커니즘

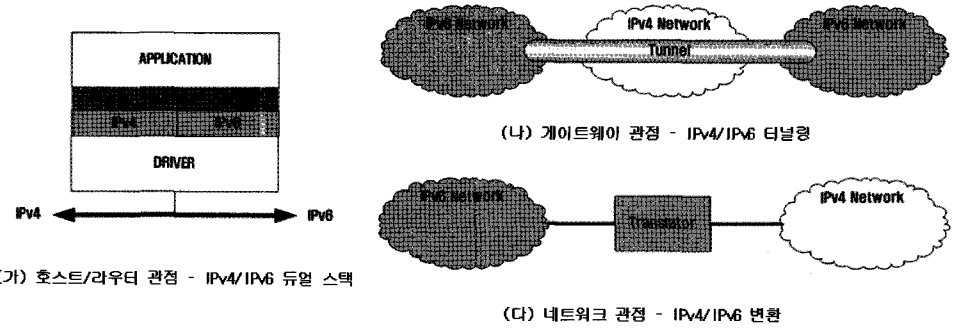
6Bone에서 주로 사용하는 방법으로 두 라우터간(혹은 호스트간)의 IPv4 주소를 통해 매뉴얼하게 정적 터널을 설정하는 방식이다. IPv4/IPv6 전환 방법에서의 설정 터널링은 주로 수동으로 IPv4 네트워크를 통과시켜 IPv6 네트워크사이의 통신을 하게 된다.

2) 자동 터널링(Automatic Tunneling) 메커니즘

IPv6로의 전환되는 초기에는 설정 터널링을 이용하는 방법을 사용하겠지만 네트워크의 구성이 복잡해질수록 설정 터널링 방법보다는 동적으로 터널을 형성해주는 방법이 점차적으로 널리 사용될 것이다. 이러한 자동 터널링 방법은 IPv4 호환주소를 IPv6 주소에 포함시켜 자동으로 IPv4 네트워크를 통과할 수 있게 한다. 최근에는 이러한 자동 터널링을 이용하기 위해 6to4[5], ISATAP[6], Teredo[7]와 같은 향상된 자동 터널링 방법을 표준으로 정하고 있다. 하지만 자동 터널링 방법에서는 IPv4와 IPv6 경계 라우터들은 IPv6 소스 주소가 위조된 IPv6 패킷을 IPv4 헤더로 캡슐화하여 공격자가 계획한 네트워크로 쉽게 전달될 수 있다는 문제점을 가지고 있다.

1.2.3 IPv4/IPv6 변환 방법

IPv4/IPv6 변환 방법[8]은 IPv4 노드와 IPv6 노드가 서로 통신이 가능하도록 IP 헤더를 변환해주는 방법을 사용한다. 즉, IPv4 노드와 IPv6 노드와 통신을 하기 위해서 IPv4 헤더를 IPv6 헤더로 변환하거나 IPv6 헤더를 IPv4 헤더로 변환하는 방법을 사용한다. 이러한 변환 방법으로는 DSTM[9], NAT-PT[10], SIIT[11], BIS[12], BIA[13] 방법들이 있다. IPv4/IPv6 변환 방법에서는 일반적으로 IPv6 노드는 라우팅이 가능한 IPv4 주소를 얻기 위해서 Pool of IPv4 주소서버를 통해 IPv4 주소를 할당받아 사용하게 된다. 그렇지만 IPv6 노드와 Pool of IPv4 주소서버와의 인증 절차가 부재하기 때문에 Pool of



(가) 호스트/라우터 관점 - IPv4/IPv6 듀얼 스택

(나) 게이트웨이 관점 - IPv4/IPv6 터널링

(다) 네트워크 관점 - IPv4/IPv6 변환

그림 1. IPv4/IPv6 전환 기술의 분류

IPv4 주소 서버로의 IPv4 주소 고갈 공격이 일어날 위협이 존재한다.

Ⅱ. IPv6 전환 기술의 위협 분석

IPv4/IPv6 전환 과정에서 다양한 보안적인 위협이 존재한다. 기존의 IPv4 네트워크에서 존재했던 보안적인 위협뿐만 아니라 IPv4/IPv6 전환 과정에서의 새로운 보안적인 위협이 존재하게 된다.

2.1 자동 터널링 방법에서의 위협 분석

IPv4/IPv6 터널링 방법은 주로 IPv6 데이타그램을 IPv4 헤더로 캡슐화하여 IPv4 네트워크를 경유하여 IPv6 호스트끼리의 통신을 가능하게 한다. 하지만 자동 터널링 방법에서 IPv4와 IPv6 사이의 경계 라우터는 IPv6를 캡슐화하기 위한 IPv4 헤더를 단순히 IPv6 헤더의 주소필드에서 IPv4 주소를 추출하여 IPv4 헤더를 구성하기 때문에 공격자가 IPv6 헤더를 조작하여 IPv4 캡슐화를 통해 숨겨서 보낼 수 있는 문제가 발생한다[14]. 특히 자동 터널링 방법을 사용하는 6to4 방법은 ingress 필터링[15]을 적용한다고 해도 IPv4 네트워크에 위치한 공격자가 IPv6 헤더부분을 위조하여 IPv4 헤더로 캡슐화하여 IPv6 네트워크로 패킷을 전달할 수 있기 때문에 주소 스푸핑을 이용한 서비스 거부 공격(DoS), 분산 반사 서비스 거부 공격 (DRDoS)[16] 등 다양한 공격이 일어날 수 있는 위협이 존재한다.

그림 2는 6to4 전환 방법에서의 자동 터널링을 이용한 DRDoS 공격을 나타내었다. 그림에서 공격자가 6to4 릴레이 라우터를 이용하여 DRDoS 공격을 수행하는 시나리오는 다음과 같다.

① 공격자는 IPv6 소스 주소를 공격대상 (victim)으로 설정하여 공격 패킷을 구성하고, ingress 필터링을 통과하기 위해서 합법적인 IPv4 헤더로 캡슐화하여 자신의 엑세스 라우터로 패킷을 전달한다.

② 엑세스 라우터는 공격 패킷의 ingress 필터링을 수행한 후 (해당 IPv4 소스 주소는 합법적인 주소이므로 ingress 필터링을 통과한다.) 6to4 릴레이 라우터까지 전달한다.

③ 공격자가 보낸 패킷을 전달받은 6to4 릴레이 라우터는 공격 패킷의 IPv4 헤더를 제거하고 반사 노드 (reflector)로 패킷을 전달한다.

④ 반사 노드는 공격자의 IPv6 패킷에 대한 응답으로써 공격 패킷의 IPv6 소스 주소를 목적지로 하여 IPv6 패킷을 생성하고, 6to4 릴레이 라우터로 패킷을 전달한다. 이때, 해당 IPv6 목적지 주소는 공격자가 목표로 하는 공격대상의 주소가 된다.

⑤ 6to4 릴레이 라우터는 반사 노드로부터 전달받은 패킷을 공격대상으로 전달함으로써 DoS 공격이 이루어지게 된다.

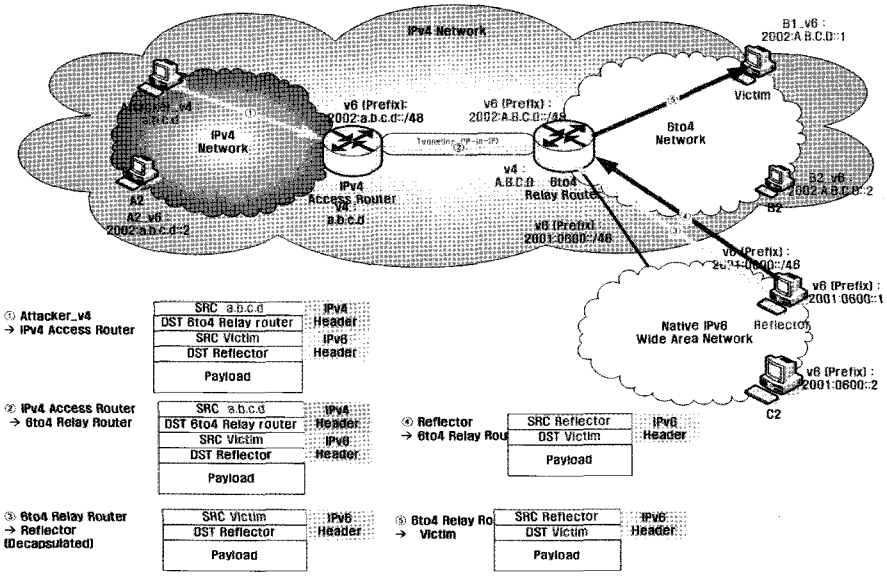


그림 2. 6to4 릴레이 라우터를 이용한 DRDoS 공격

이러한 유형의 공격은 공격자가 IPv4 네트워크에 위치하고 있고, 공격자 스스로가 6to4 주소를 생성하여 공격을 수행하기 때문에 공격자의 패킷을 전달하는 라우터들은 공격자의 IPv6 소스 주소에 대한 스푸핑 여부를 알 수 없을 것이다. 그러므로 이러한 공격을 효과적으로 차단하는 방안이 필요하다.

2.2 Pool of IPv4 주소 서버로의 IPv4 주소 고갈 공격

Pool of IPv4 주소서버는 IPv6 노드가 IPv4 노드와 통신을 가능하게 하도록 IPv6 노드에게 공인 IPv4 주소를 직접제공하거나 IPv6 노드가 보낸 IPv6 패킷을 IPv4 패킷으로 변환하기 위해 해당 노드의 IPv6 주소에 대응되는 IPv4 주소를 할당하여 매핑하는 방법을 통해 IPv6 노드가 IPv4 노드와 통신을 가능하도록 제공하는 서버이다. NAT-PT 또는 DSTM 방법에서는 이러한 IPv4 주소를 Pool of IPv4 주소서버를 이용하여 해결하게 되는데 IPv4 주소 할당에 관한 인증절차가 부재하기 때문에 Pool of IPv4 주소서버에 대한 서비스 거부 공격이 발생할 수 있는 취약점이 존재한다.

2.2.1 DSTM 서버에 대한 IPv4 주소 고갈 공격

DSTM 서버는 DSTM 노드인 IPv6 노드에게 IPv4 주소를 할당하기 위한 서버이다. 현재 IETF v6ops 워킹그룹에서는 DSTM 서버에 대한 논의가 이루어지고 있고, DHCPv6 서버가 가장 유력할 것으로 보인다.

DSTM 노드가 IPv4 노드와의 통신을 위한 IPv4 주소를 획득하는 과정을 살펴보면, DSTM 노드는 IPv4 주소를 얻기 위해서 DSTM 서버로 주소 할당 요청 메시지를 보낸다. 주소 할당 요청을 받은 DSTM 서버는 자신이 가지고 있는 IPv4 주소 중에 하나를 선택하여 DSTM 노드에게 응답하게 된다. 하지만 이러한 방법에서는 IPv4 주소를 할당에 관한 인증 방법이 제시되어 있지 않으므로 DSTM 서버가 가진 IPv4 주소가 고갈될 수 있는 위협이 존재한다. 즉, 공격자는 DSTM 서버가 가진 IPv4 주소를 고갈시키기 위해 DSTM 서버로 IPv6 주소를 스푸핑한 IPv4 주소 할당 요구 메시지를 끊임없이 보낸다. DSTM 서버는 해당 요구에 대해서 IPv4 주소를 할당하게 되는데 이러한 과정이 반복됨에 따라 DSTM 서버가 가지고 있는 IPv4 주소 pool은 고갈된다. 따라서 IPv4 주소 고갈 위협에 대한 대응 방안이 요구된다. 그림 3은 IPv4 주소 서버에 대한 IPv4 주소 고갈 공격을 수행하고 있는 상황을 보여주고 있다. 그림에서 공격자가 DSTM 서버의 IPv4 주소 고갈 공격을 수행하는 시나리오는 다음과 같다.

① DSTM node_Attacker는 IPv6 소스 주소를 스푸핑하여 IPv4 주소 할당 요청 메시지를 DSTM Server에게 보낸다.

② DSTM Server는 해당 IPv6 주소에 대한 IPv4 주소를 할당하여 자신의 IPv4 주소 매핑 테이블에 해당 정보를 기록하고, DSTM 도메인의 경계 라우터인 TEP에게 해당 매핑 정보를 전달한다.

③ DSTM Server는 IPv4 주소 할당 요청 메시지에 대한 응답으로서 IPv4 주소 할당 응답 메시지를 DSTM 노드에게 보낸다. 이 때, IPv4 주소 할당 요청 응답 메시지를 받는 노드는

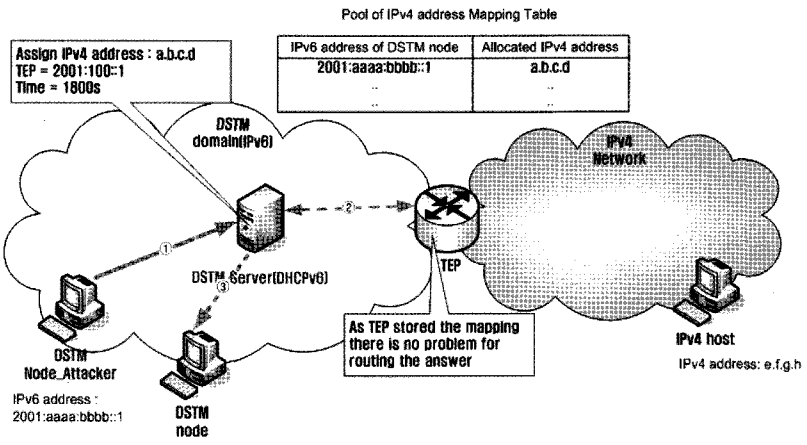


그림 3. DSTM 서버에 대한 IPv4 주소 고갈 공격

실제로 존재하지 않거나 할당 요청 메시지를 생성하지 않은 노드일 것이다.

④ 공격자는 IPv6 소스 주소를 계속적으로 변화시키면서 위의 ①에서 ③까지의 과정을 반복함으로써 DSTM 서버가 가지고 있는 IPv4 주소를 고갈 시킬 수 있다.

이러한 유형의 공격이 가능한 이유는 DSTM 서버에서의 IPv4 주소 할당에 관한 인증 메커니즘이 부재하기 때문이다. 따라서 IPv4 주소 할당에 관한 인증 메커니즘이 필요하다.

2.2.2 NAT-PT서버에 대한 IPv4 주소 고갈 공격

1) NAT-PT 노드에 의한 IPv4 주소 고갈 공격

IPv6 노드에서 IPv4로 패킷을 전송할 경우 NAT-PT 서버는 자신이 가지고 있는 IPv4 주소 pool을 사용하여 IPv6 노드가 보낸 패킷의 IP 헤더를 변환하고, 해당 IPv6 노드의 주소와 할당한 IPv4 주소를 매핑함으로서 IPv6 노드와 IPv4 노드 사이의 통신이 이루어질 수 있다. 하지만 NAT-PT 서버와 NAT-PT 노드 사이의 주소 할당에 관한 인증 메커니즘이 부재하기 때문에 NAT-PT 도메인에 있는 공격자에 의해 IPv4 주소 pool이 고갈될 수 있는 위협이 존재한다. 그림 4는 NAT-PT 서버가 가지고 있는 IPv4 주소 pool에 대한 고갈 공격을 수행하고 있는 상황을 보여주고 있다. 그림에서 공격자는 IPv6 소스 주소를 스푸핑하여 IPv6 패킷을 구성한 후 NAT-PT 서버로 패킷을 전달한다. NAT-PT 노드의 IPv6 패킷을 전달받은 NAT-PT 서버는 해당 IPv6 패킷의 IPv6 소스 주소에 대한 IPv4 주소를 할당하여 해당 목적지로 패킷을 전달한다. 공격자는 계속적으로 IPv6 주소를 스푸핑하여 NAT-PT 서버로 전달함으로써 NAT-PT 서버가 가진 IPv4 주소 pool을 모두 고갈시킬 수 있다.

2) 외부 IPv4 노드에 의한 IPv4 주소 고갈 공격

NAT-PT 외부 도메인에 있는 IPv4 노드들이 NAT-PT 내부의 IPv6 노드들과 통신할 수 있는 IPv4 주소를 얻기 위해 IPv4 타입의 질의를 보내면 NAT-PT 서버의 같은 네트워크의 위치하는 DNS-ALG[17]는 NAT-PT 서버에게 IPv4 주소 할당 요구를 하게 되고, 그에 관한 응답으로 NAT-PT서버는 해당 NAT-PT 내부 노드의 IPv6 주소에 해당되는 IPv4 주소를 할당하여 DNS-ALG에게 보내게 된다. 만약 IPv4 공격자가 짧은 시간에 수많은 DNS 질의를 보내면 IPv4 주소가 고갈될 수 있는 문제가 있다. 그림 5는 NAT-PT 서버가 가지고 있는 IPv4 주소 pool에 대한 고갈 공격을 수행하고 있는 상황을 보여주고 있다. 그림에서 IPv4 네트워크에 위치한 공격자는 NAT-PT 노드에 대한 DNS 질의를 IPv4 네

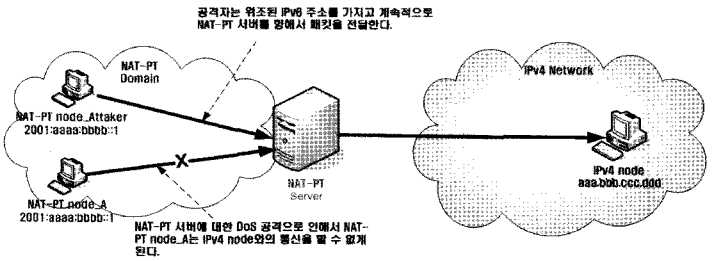


그림 4. NAT-PT 노드에 의한 IPv4 주소 고갈 공격

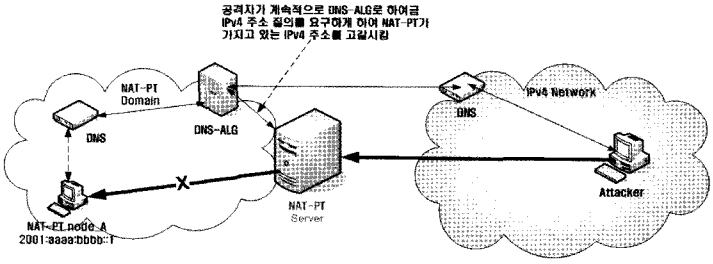


그림 5. 외부 IPv4 노드에 의한 IPv4 주소 고갈 공격

트워크의 DNS 서버에게 보낸다. IPv4 DNS 서버는 해당 질의를 NAT-PT 도메인의 DNS-ALG로 보내게 되고, DNS-ALG는 해당 도메인에 대한 IPv4 주소 할당 요청을 수행한다. NAT-PT 서버는 해당 NAT-PT 노드에 대한 IPv4 주소를 할당하고, DNS-ALG로 전달하게 된다. 공격자는 계속적으로 다른 NAT-PT 노드에 대한 DNS 질의를 보냄으로써 NAT-PT 서버가 가진 IPv4 주소 pool을 모두 고갈시킬 수 있다.

Ⅲ. 실험 결과

본 절에서는 6to4 전환 기술에서의 DRDoS 공격 실험과 그에 따른 결과를 설명한다. 본 논문에서의 실험은 공격자가 6to4 전환 방법에서의 6to4 릴레이 라우터를 이용한 DRDoS 공격을 실험하였다.

3.1 실험 시나리오

전체적인 공격 시나리오 구성은 그림 6과 같다. 공격자는 victim의 IPv6 주소를 출발지 주소로 설정하고, reflect node를 IPv6 목적지 주소로 설정하여 ICMPv6 요청 패킷을 생성한다. 또, 6to4 relay 라우터까지 IPv6 패킷을 전달하기 위해 IPv4 헤더로 IPv6 패킷을 캡슐화하여 6to4 릴레이 라우터로 패킷을 전달한다. 일반적인 IPv4 라우터에서는 해당 IPv4 패킷이 정상적인 패킷이기 때문에 ingress 필터링을 통과하여 6to4 릴레이 라우터까지 IPv4-in-IPv6 패킷이 전달된다. Reflect node는 ICMPv6 요청 패킷에 대한 IPv6 출발지 주소를 목적지 주소로 설정하여 ICMPv6 응답 패킷을 생성하고, 6to4 릴레이 라우터로 전달한다. 결국 ICMPv6 패킷의 IPv6 목적지 주소는 victim이기 때문에 victim은 원하지 않은 ICMP -v6 응답 메시지 받게 된다.

3.2 실험 환경 및 실험 노드 설명

본 논문에서의 실험을 위해 한국 전산원에서 현재 시범 운영하는 6to4 서비스를 이용하였다. 해당 실험을 위한 노드들에 대한 설명은 아래와 같다.

- 공격자 : IPv4 네트워크에 위치한 Linux (Red-hat 9.0) 운영체제를 사용하는 듀얼 스택 노드로써 IPv6 호스트와 통신을 하기 위해 6to4 주소를 가지고 있는 노드
- 반사 노드 : 공격자가 DRDoS를 수행하기 위해서 이용된 IPv6 노드
- 희생자 : Windows XP를 운영체제를 사용하는 6to4 네트워크에 위치한 6to4 노드로써 반사 노드로부터 DRDoS 공격을 받는 노드
- 6to4 릴레이 라우터 : 한국 전산원에서 제공하는 라우터로써 IPv6 네트워크와 6to4 네트워크를 연결하는 기능을 가진 라우터

3.3 실험 결과

그림 7과 8은 각각 공격자가 생성한 ICMPv6 요청 패킷과 공격 대상이 받게 되는 ICMPv6 응답 패킷의 내용을 보여주고 있다. 그림 7에서와 같이 공격자는 ICMPv6 요청 메시지를 생성하여 6to4 릴레이 라우터를 통해 reflect node까지 패킷을 전달한다. 또, 그림 8에서 victim은 reflect node로부터 원하지 않은 ICMPv6 응답 패킷이 받게 되는 것을 볼 수 있다. 결론적으로 공격자는 기존의 IPv4 네트워크에서 스푸핑을 막기 위한 ingress 필터링의 제약

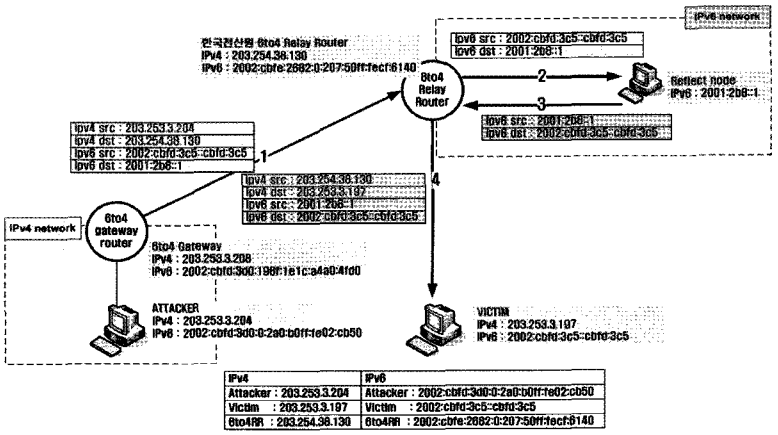


그림 6. 실험 동작 패킷 설명 시나리오

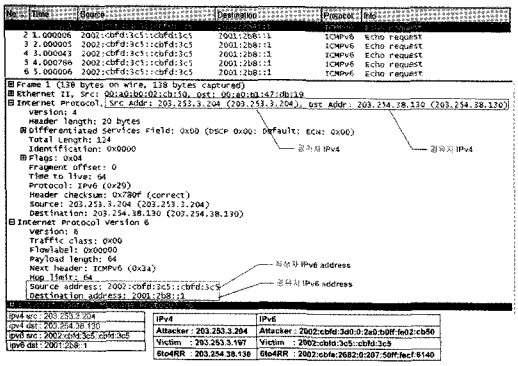


그림 7. 공격자가 생성한 ICMPv6 요청 메시지

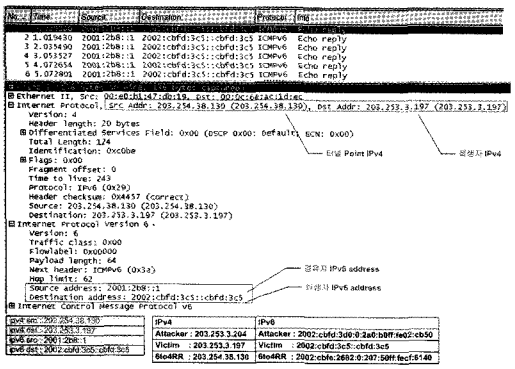


그림 8. 반사 노드에 의한 ICMPv6 응답 메시지

을 받지 않고 6to4 릴레이 라우터를 통해 쉽게 DRDoS 공격을 수행할 수 있다.

Ⅳ. IPv6 전환 기술의 보안 위협에 대한 대응 방안

4.1 자동 터널링 방법에서의 무결성 검사

자동 터널링 방법은 공격자가 ingress 필터링을 통과하기 위해 라우팅이 가능한 IPv4 헤더를 사용하여 스푸핑된 IPv6 패킷을 숨길 수 있다는 문제가 존재한다. 자동 터널링을 지원하는 6to4 라우터는 IPv6 헤더의 출발지 주소의 스푸핑 여부를 검사하는 ingress 필터링 기능을 가지고 있어야 한다. 특히 IPv4 네트워크에 속한 공격자가 IPv6-in-IPv4 패킷을 직접 구성하여 6to4 릴레이 라우터를 통해 공격하는 방법에서는 6to4 릴레이 라우터에서 IPv4 헤더의 출발지 주소와 IPv6 헤더의 출발지 주소에 내포된 IPv4 주소가 일치하는지에 대한 주소 무결성 검사를 수행해야 한다. 그림 9은 주소 무결성 검사 방법에 대해 나타내고 있다.

4.2 DSTM 메커니즘에서의 안전한 IPv4 주소 할당 방법

DSTM 전환 기술에서 DSTM 노드에게 IPv4 주소를 제공하는 DSTM 서버에 대한 IPv4 주소 고갈 공격이 가능한 이유는 DSTM 노드와 DSTM 서버 사이의 주소 할당에 대한 보안 메커니즘이 부재하기 때문이다. 일반적인 DSTM 서버에 대한 IPv4 주소 고갈 공격을 살펴보면, 공격자는 스푸핑한 IPv6 주소를 가지고 해당 IPv6 주소에 대한 IPv4 주소를 DSTM 서버에게 요구하게 된다. 하지만 실제 DSTM 서버가 할당해준 IPv4 주소에 대응되는 IPv6 주소는 실제로 존재하지 않거나 해당 DSTM 노드가 IPv4 주소 할당을 요청하지 않았을 경우일 것이다. 따라서 DSTM 서버는 IPv4 주소를 DSTM 노드에게 할당을 하기 전에 해당 DSTM 노드가 실질적으로 IPv4 노드와 통신을 원하는지에 대한 여부를 확인하는 절차가 필요할 것이다. 본 연구에서는 DSTM 서버에 대한 IPv4 주소 고갈 공격을 막기 위해서 기존의 DSTM 서버가 IPv4 주소를 할당

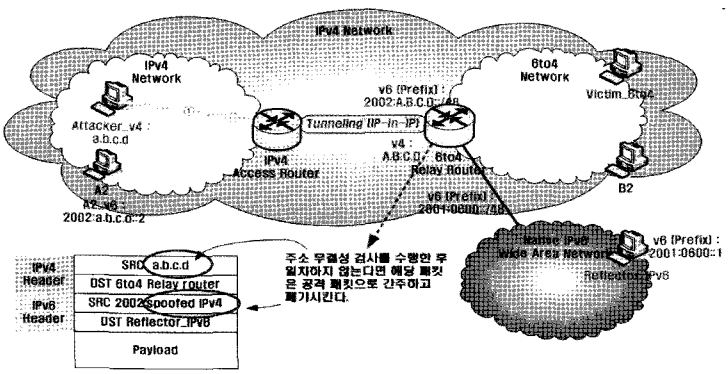


그림 9. 주소 무결성 검사

하는 절차 이외의 Challenge-Response 메시지를 교환하는 과정을 제안한다. 그림 10은 안전하게 IPv4 주소를 DSTM 노드에게 할당하는 과정을 보여주고 있다. 그림 10에서 DSTM 서버가 DSTM 노드에게 안전하게 IPv4 주소를 제공하는 절차는 다음과 같다.

① DSTM 노드는 IPv4 노드와 통신하기 위한 IPv4 주소를 DSTM 서버에게 요구하는 메시지를 보낸다.
② DSTM 서버는 IPv4 주소를 요구한 DSTM 노드에게 Time stamp와 nonce 정보가 포함된 challenge 메시지를 보낸다.
③ DSTM 서버의 challenge 메시지에 대한 Response 메시지를 보낸다. 이때, Time stamp 정보는 challenge 메시지의 Time stamp와 같은 정보를 사용하고, nonce 값에 1을 더해서 Response 메시지를 보낸다. 이 때, DSTM 서버측에서 해당 정보가 일치하지 않을 경우에는 Reject 메시지를 DSTM 노드에게 전달한다. IPv4 주소 제공 절차를 중단한다.
④ 해당 DSTM 노드에 대해서 IPv4 주소를 할당하고, 할당한 IPv4 주소와 DSTM 노드의 IPv6 주소의 매핑 정보를 TEP에게 통보한다.
⑤ DSTM 노드에게 IPv4 주소 정보를 제공한다.

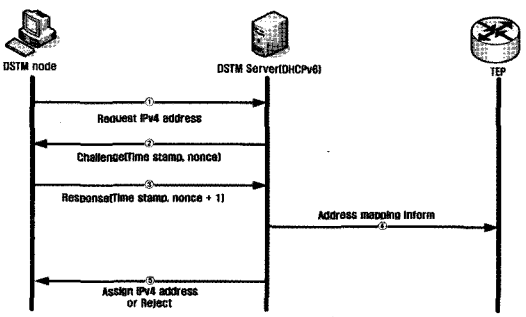


그림 10. Challenge-Response를 이용하여 안전하게 DSTM 노드에게 IPv4 주소를 제공하는 절차

V. 결 론

차세대 인터넷망의 핵심 기반 프로토콜인 IPv6가 전체 인터넷 망과 단말기에 적용되는 완전한 IPv6 망이 구성되기까지 상당한 기간 동안 IPv4 기반의 망, 단말, 응용 등이 함께 공존하게 될 것이다. 이를 위하여 IETF에서는 다양한 형태의 IPv4와 IPv6 간의 연동 및 전환 기술을 개발하여 제공하고 있다. 따라서 실질적인 IPv6 전환 단계에서 발생할 수 있는 보안에 대한 분석과 그에 따른 대응 방안에 관한 보안 메커니즘의 개발은 필수적이다.

본 연구에서는 IPv6 전환 기술들에 대해 살펴보고, 각 IPv6 전환 기술에 따른 보안 위협을 분석하였다. 또, 해당 보안 위협에 따른 대응 방안을 제시하였다. 6to4 전환 기술에서는 공격자가 6to4 릴레이 라우터를 이용한 DoS 및 DRDoS 공격 위협을 분석하였고, 그러한 문제를 해결하기 위해서 주소 무결성 검사방법을 제시하였다. 또, DSTM과 NAT-PT 전환 기술에서는 IPv6 노드가 IPv4 노드와의 통신을 위해 필요한 IPv4 주소를 할당하는 IPv4 주소 pool을 가진 서버에 대한 IPv4 주소 고갈 위협을 분석하였고, IPv4 주소 고갈 위협 문제를 해결하기 위해서 DSTM 전환 기술에서는 challenge-response 메커니즘을 사용하여 안전하게 IPv4 주소를 할당하기 위한 방안을 제시하였다.

향후 과제로는 IPv6 전환 기술을 실제 망에 적용하는 과정에서 본 연구에서 제시한 보안 문제외의 추가적인 새로운 보안적인 문제가 발생할 수 있을 것이다. 따라서 IPv6 전환 기술에서 발생할 수 있는 보안적인 문제를 분석하고, 그에 대한 해결방안을 찾기 위한 지속적인 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] *차세대 인터넷 프로토콜 : IPv6*, IPv6 포럼 코리아, 3월 2002.
[2] J. Wiljakka (ed.), "Analysis on IPv6 Transition in 3GPP Networks," Internet Draft, draft-ietf-v6ops-3gpp-analysis-09.txt, March 2004.
[3] E. Nordmark and R. E. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," Internet Draft, draft-ietf-v6ops-mech-v2-02.txt, January 30, 2004.
[4] William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, ISBN 0-201-63357-4, 1994.
[5] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," RFC 3056, February 2001.
[6] F. Templin, T. Gleeson, M. Talwar, and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)," Internet Draft,

draft-ietf-ngtrans-isatap-21.txt, April 2004.

[7] C. Huitema, "Tunneling IPv6 over UDP through NATs," Internet Draft, draft- huitema-v6ops-teredo-03.txt, November 2004.

[8] J. William Atwood, Kedar C. Das, and Xing (Scott) Jiang, "IPv4/IPv6 Translation: Allowing IPv4 hosts to communicate with IPv6 hosts without modifying the software on the IPv4 or IPv6 hosts"

[9] Jim Bound, "Dual Stack Transition Mechanism," Internet Draft, draft-bound-dstm-exp-01.txt, April 2004.

[10] G. Tsirtsis and P. Srisuresh, "Network Address Translation-Protocol Translation (NAT-PT)," RFC 2766, February 2000.

[11] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)," RFC 2765, February 2000.

[12] K. Tsuchiya, H. Higuchi, and Y. Atarashi, "Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)," RFC 2767, Februaary 2000.

[13] S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, and A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)," RFC 3338, October 2002.

[14] P. Savola and C. Patel, "Security Considerations for 6to4," Internet Draft, draft-ietf-v6ops-6to4-security-02.txt, March 2004.

[15] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2267, January 1998.

[16] Steve Gibson, "DRDoS (Distributed reflection Denial of Service)," Gibson Research Cor- poration, February 2002.

[17] P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)," RFC 2694, September 1999.

최 인 석(Inseok Choi) 준회원

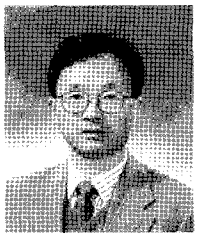
2003년 2월 숭실대학교 정보통신전자공학과 학사

2005년 2월 숭실대학교 정보통신공학과 석사

2005년 2월~현재 (주)주홍정보통신연구원

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안 RFID/USN 보안

정 수 환(Souhwan Jung) 정회원



1985년 2월 서울대학교 전자 공학과 학사

1987년 2월 서울대학교 전자 공학과 석사

1998년~1991년 한국통신 전임연구원

1996년 6월 미 워싱턴 주립대(시애틀) 박사

1996년~1997년 Stellar One SW Engineer

1997년~현재 숭실대학교 정보통신전자공학부 부교수

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안 RFID/USN 보안

김 영 한(Younghan Kim) 정회원

1984년 2월 서울대학교 전자공학과 학사

1986년 2월 한국과학기술원 전기 및 전자공학과 석사

1990년 8월 한국과학기술원 전기 및 전자공학과 박사

1987년 1월~1994년 8월 디지콤정보통신연구소 데이터통신연구부장

1994년 9월~현재 숭실대학교 정보통신전자공학부 부교수, 통신학회 인터넷 연구회 위원장, VoIP포럼 차세대기술분과위원장

<관심분야> 컴퓨터네트워크, 인터넷 네트워킹, 이동 데이터 통신망.