IPv4/IPv6 혼재 네트워크에서 터널링 메커니즘 기반 공격 실험*

경계현, 김가을, 강성구, 고광선, 엄영익

성균관대학교 정보통신공학부

Experiment of Tunneling Mechanism based Attacks in IPv4/IPv6 Coexistence Networks*

Gyehyeon Gyeong, Ka Eul Kim, Seong-Goo Kang, Kwangsun Ko, and Young Ik Eom

School of info. and Comm. Eng., Sungkyunkwan University

요 약

최근까지 IPv4/IPv6 혼재 네트워크에서 서로 다른 네트워크에 존재하는 다수의 호스트들 간 통신이 가능하도록 지원해주는 기술에 대해 많은 연구가 진행되고 있으며, 대표적인 연구 분야로는 듀얼스택 메커니즘, 터널링 메커니즘, 그리고 프로토콜 변환 메커니즘이 있다. 본 논문에서는 듀얼스택과 터널링 메커니즘에서 예상되는 세 개의 공격에 대한 실험내용을 보이고자 한다. 실험 순서는 먼저 IPv4/IPv6 혼재 네트워크를 위한 실험망을 구축하고, 구축된 실험망에서 각 메커니즘별 공격 결과를 보임으로써 해당 공격이 발생할 수 있다는 실질적이면서 구체적인 근거를 제시하도록 구성되어 있다.

I. 서론

인터넷 영영의 범위가 기하급수적으로 넓어짐에 따라 IPv4 프로토콜의 주소 고갈 문제와 해당 프로토콜 자체가 가지는 기본적인 결함을 극복하기 위하여 새로운 IPv6 프로토콜이 개발되었다[1]. 그러나 현재의 IPv4 네트워크에서 IPv6 네트워크로의 전환은 아주 오랜 연구와 수행과정을 거쳐 이루어질 것으로 전망되기에, IPv4/IPv6 혼재 네트워크가 상당기간 상호 공존할 것으로 예상된다. 이러한 혼재 네트워크 환경을 지원하기 위하여 듀얼스택 메커니즘, 터널링 메커니즘, 프로토콜 변환 메커니즘과 같은 다양한 기술이 연구되고 있으며[2], 특히 IPv4/IPv6 혼재 네트워크는 IPv4 네트워크와 IPv6 네트워크에서 발생할 수 있는 보안 문제점 이외의 새로운 보안 문제점이 발생할 수 있기 때문에 이에 대한 연구가 중요한 이슈로 대두되고 있다.

본 논문에서는 듀얼스택 메커니즘과 두 개의 터널링 기술이 적용된 IPv4/IPv6 혼재 네트워크에서 발생할 수 있는 공격에 대해서 실질적이면서 구체적인 실험 내용을 보이고자 한다.

* 본 연구는 정보통신부 및 정보통신진흥연구원의 대학 IT 연구센터 육성지원 사업의 결과로 수행되었음

이를 위하여 리눅스 시스템을 이용하여 IPv4/IPv6 혼재 네트워크 실험망을 구축하는 과정을 먼저 설명하고, 몇가지 공격 기법을 구축된 실험망에 직접 적용하는 순서로 기술한다.

본 논문의 구성은 2장에서 리눅스 시스템을 기반으로 구축한 실험망 구축방법에 대해 설명하고, 3장에서는 세 가지 공격 기법 실험 내용을 보인다. 마지막 4장에서는 결론 및 향후 연구내용을 제시한다.

II. 실험망 구축

본 장에서는 리눅스 시스템을 이용하여 듀얼스택 메커니즘과 두 개의 터널링 메커니즘을 지원하는 IPv4/IPv6 혼재 네트워크 실험망을 구축하는 방법을 소개한다.

2.1 듀얼스택 메커니즘

듀얼스택 메커니즘이란 하나의 시스템에서 IPv4 프로토콜 스택과 IPv6 프로토콜 스택이 동시에 존재하여 두 가지 프로토콜 기반 통신이 가능하도록 지원하는 메커니즘을 의미한다. 즉, 물리적으로는 하나의 시스템이지만, 논리적으로는 IPv4 프로토콜과 IPv6 프로토콜을 각각 지원하는 두개의 시스템이 있는 것처럼 볼 수

있으며[3], 듀얼스택 메커니즘의 네트워크 계층을 그림 1에서 보인다.

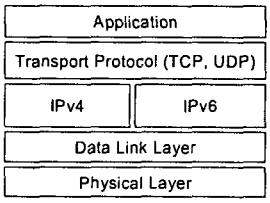

그림 1. 듀얼스택 메커니즘의 네트워크 계층

듀얼스택 메커니즘의 경우, 리눅스 커널에서 기본 제공하고 있으므로, 커널 설정 시, 'The IPv6 Protocol' 항목을 커널에 포함시키거나 모듈로 컴파일 함으로써 간단히 구축할 수 있다[4]. 본 논문의 실험을 위하여 구축된 듀얼스택 메커니즘 기반 IPv4/IPv6 혼재 네트워크는 그림 2와 같다.

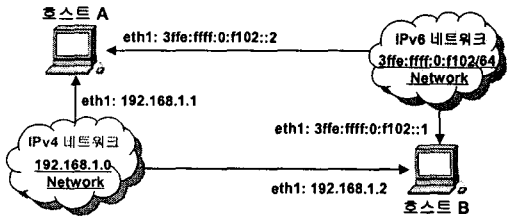

그림 2. 듀얼스택 메커니즘 기반 IPv4/IPv6 혼재 네트워크 구성도

그림 2에서 보이는 바와 같이 호스트 A와 호스트 B는 모두 IPv4 프로토콜을 이용하여 IPv4 네트워크와 통신이 가능하고 IPv6 프로토콜을 이용하여 IPv6 네트워크와도 통신이 가능하다.

2.2 터널링 메커니즘

터널링 메커니즘이란 고립되어 있는 동일 네트워크들(예: IPv6 네트워크) 간의 통신을 위하여 다른 네트워크(예: IPv4 네트워크)와의 경계에서 터널을 생성함으로써 고립되어 있는 동일 네트워크들이 직접 연결되어 있는 것처럼 만들어주는 메커니즘을 의미한다. 대표적인 터널링 메커니즘으로는 6in4, 6to4, ISATAP, DSTM, Teredo, Tunnel Broker 등이 있지만[3], 본 논문에서는 실질적인 공격이 가능한 DSTM 메커니즘[5]과 Teredo 메커니즘[6]에 대해서만 공격 실험을 실시한다. 실험을 위해 사용된 모든 시스템들에는 Fedora Core 3(커널 버전 2.6.x) 배포판[7]이 설치되어 있다.

DSTM 메커니즘은 ENST Bretagne에서 구현한 DSTM 4.0[8]을 이용하여 그림 3과 같이 구성할 수 있다.

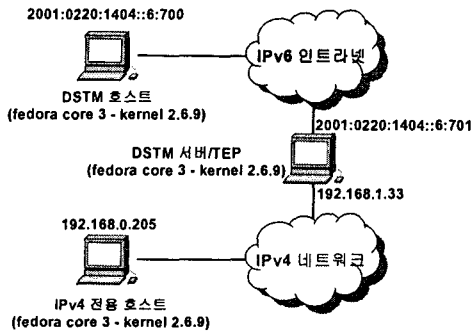

그림 3. DSTM 메커니즘 기반 IPv4/IPv6 혼재 네트워크 구성도

그림 3에서 보이는 바와 같이 DSTM 메커니즘은 DSTM 호스트, DSTM 서버, 그리고 TEP(Tunnel End Point)로 구성할 수 있으며, DSTM 호스트와 DSTM 서버는 동일한 인트라넷에 속해 있어야 한다. 본 실험에서는 DSTM 서버와 DSTM TEP를 하나의 시스템에 구축하였으나 실제로는 별도의 시스템으로 운영된다. 그림 3과 같이 구축된 DSTM 메커니즘에서 DSTM 호스트가 DSTM 서버에 서비스를 요청하면, DSTM 서버는 DSTM 호스트와 TEP 사이에 동적으로 터널링을 설정하여 DSTM 호스트와 IPv4 네트워크에 존재하는 IPv4 전용 호스트 간에 DSTM TEP를 이용하여 통신이 가능하도록 한다.

Teredo 메커니즘은 Rémi Denis-Courmont가 구현한 Miredo 0.8[9]을 이용하여 그림 4와 같이 구성할 수 있다.

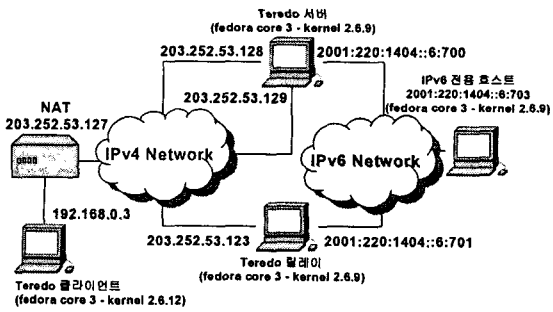

그림 4. Teredo 메커니즘 기반 IPv4/IPv6 혼재 네트워크 구성도

그림 4에서 보이는 바와 같이 Teredo 메커니즘은 Teredo 클라이언트, Teredo 서버, 그리고 Teredo 릴레이로 구성할 수 있다. Teredo 서버와 Teredo 릴레이는 IPv4 네트워크와 IPv6 네트워크의 경계지점에 위치하며, Teredo 서버는 NAT의 동작방식을 구분하기 위해 2개의 공인 IPv4 주소를 갖는다. IPv4 네트워크의 NAT 내부에 위치하는 Teredo 클라이언트에서 Teredo

서버에 서비스를 요청할 때 최초 패킷은 Teredo 서버와 터널링을 구성하여 전송하고, 이후 패킷은 Teredo 릴레이와 터널링을 구성하여 IPv6 전용 호스트와 IPv6 통신을 한다.

III. 공격 실험

본 장에서는 2장에서 설명한 IPv4/IPv6 혼재 네트워크 실험망에 구축한 듀얼 스택과 두 개의 터널링 메커니즘(DSTM 및 Teredo 메커니즘)에서 실시한 공격 실험 내용을 설명하도록 한다.

3.1 듀얼스택 메커니즘 기반 공격 실험

듀얼스택에서 실시한 공격 실험의 전제조건은 아래와 같다.

- IPv4와 IPv6 통신 모두 지원
- IPv4는 IPSec(ESP 확장헤더)을 이용하여 보안 통신
- IPv6는 IPSec(ESP 확장헤더)을 이용하지 않는 일반 통신

위와 같이 구성된 IPv4/IPv6 혼재 네트워크에서 사용자 또는 호스트는 IPSec 통신설정에 대한 오판을 함으로써 IPv6 네트워크 기반은 일반 통신을 실시할 가능성이 존재한다. 다시 말하면, 그림 2와 같은 네트워크 환경에서 호스트 A가 호스트 B로 'SSRC_hacking'이란 문자열을 IPSec 통신으로 오판하여 전송하였을 경우, 그림 5와 같이 IPv6 네트워크에서는 해당 통신 내용을 확인할 수 있다.

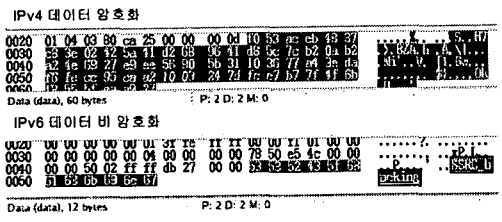

그림 5. 듀얼스택 메커니즘에서 패킷 도청 결과

3.2 터널링 메커니즘 기반 공격 실험

DSTM에서 실시한 공격 실험의 전제조건은 아래와 같다.

- 공격자는 DSTM 호스트와 DSTM 서버 사이에 위치함
- DSTM 호스트가 DSTM 서버로 전송하는 서비스요청 메시지에는 어떠한 보안인증도 실시하지 않음

DSTM 메커니즘은 DSTM 서버가 터널링 서비스를 요청하는 IPv6 호스트에게 IPv4 주소를 자동 할당하여 터널링을 지원하는 메커니즘이기 때문에, 그림 6에서 보이는 바와 같이 공격자가 DSTM 클라이언트가 DSTM 서버로 보내는 서비스 요청 패킷을 위조하여 다량의 DSTM 서비스를 요청하면, DSTM 서버가 관리하는 IPv4 주소가 고갈됨으로써 DSTM 서버에 대한 서비스거부 공격이 가능하다.

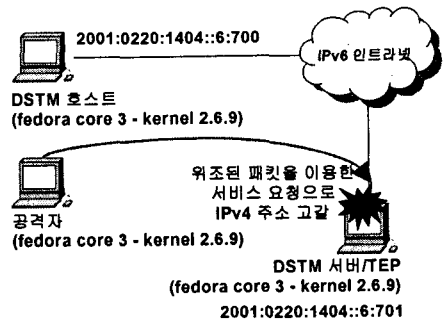

그림 6. DSTM 메커니즘에서 공격 실험 구성도

DSTM 서버에 대한 서비스거부 공격이 성공하게 되면, IPv4 주소 할당이 이루어지지 않아 정상적인 DSTM 호스트가 서비스를 받지 못하고 DSTM 서버에게 서비스 요청만 하고 있음을 그림 7과 같이 확인할 수 있다.

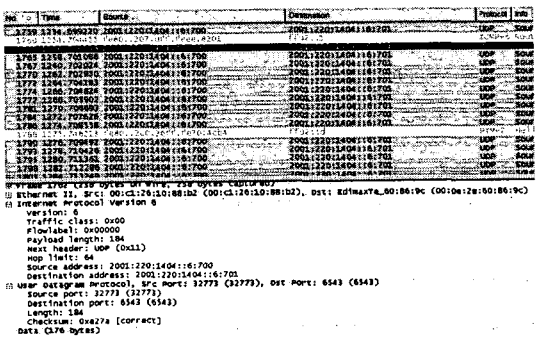

그림 7. DSTM 메커니즘에서 서비스거부 공격 결과 (Ethereal 이용)

Teredo에서 실시한 공격 실험의 전제조건은 아래와 같다

- 최초 패킷이 전송되기 전에는 Teredo 서버와 Teredo 클라이언트는 Teredo 릴레이 주소를 알 수 없음
- 사전에 공격자는 Teredo 릴레이를 공격하여 동작 불능 상태로 만듦

Teredo 클라이언트는 Teredo 릴레이가 자신의 주소를 전송하면 그때부터 Teredo 릴레이를 인식하여 Teredo 릴레이를 이용한 전송을 실시

하게 되는데, 그림 8과 같이 공격자가 Teredo 릴레이로 위장을 하여 Teredo 서버에 위장된 주소를 전송하면, Teredo 서버는 Teredo 클라이언트에게 위장된 공격자의 IPv4 주소를 알려주게 되고, Teredo 클라이언트는 위장된 Teredo 릴레이를 통하여 터널링 기반 통신을 하게 됨으로써, 공격자는 패킷의 내용을 확인할 수 있다.

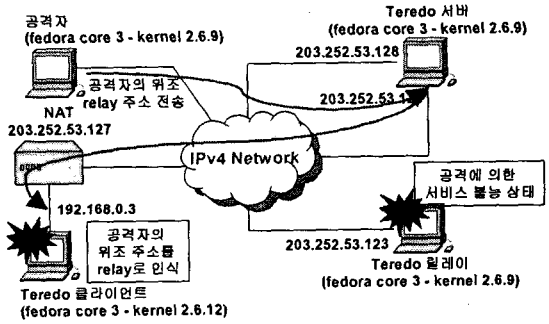

그림 8. Teredo 메커니즘에서 공격 실험 구성도

이와 같은 공격 과정을 보다 자세히 살펴보면, Teredo 릴레이로 위장된 공격자의 IPv4 주소를 Teredo 클라이언트에 알려주는 것을 그림 9에서 확인할 수 있다.

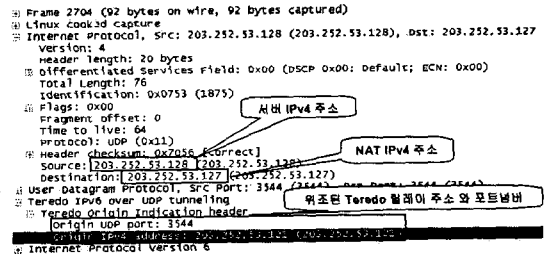

그림 9. Teredo 서버가 Teredo 클라이언트에게 Teredo 릴레이로 위장한 공격자의 IPv4 주소를 알려주는 패킷

Teredo 서버로부터 위장된 Teredo 릴레이 주소를 받은 Teredo 클라이언트가 공격자에게 통신 트래픽을 전송하는 것을 그림 10에서 확인할 수 있다.

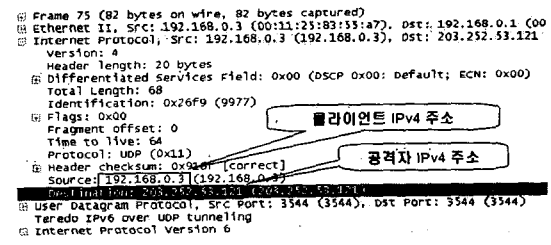

그림 10. Teredo 클라이언트가 위장된 Teredo 릴레이 주소로 패킷 전송

이와 같은 공격 실험은 IPv4/IPv6 혼재 네트워크가 존재하는 동안 계속적인 연구가 필요하며, 구체적인 실험 결과에 기반하여 듀얼스택 메커니즘과 터널링 메커니즘에서 예상되는 보안 취약점과 공격 양상에 대응할 수 있는 보안 기술을 개발할 수 있다.

IV. 결론

본 논문에서는 듀얼스택 메커니즘과 두 개의 터널링 메커니즘(DSTM, Teredo)을 이용하여 IPv4/IPv6 혼재 네트워크 실험망을 구축하는 과정을 보이고, 기존에 제시된 보안 취약점을 구축된 실험망에 직접 적용함으로써 구체적인 실험 결과를 제시하였다. 본 논문은 지금까지 이론으로만 연구된 보안 취약점을 직접 적용하고 확인함으로써 보안 실무자들에게 적합한 실무 중심의 연구 내용을 제공하고자 하였으며, 이러한 결과는 보안 기술을 개발하는데 중요한 자료로 이용될 수 있다. 향후에는 이러한 공격들에 대응할 수 있는 보안기술 및 보안시스템을 구현하고자 한다.

[참고문헌]

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

[2] M. Tatipamula, P. Grossetete, and H. Esaki, "IPv6 Integration and Coexistence Strategies for Next-Generation Networks," IEEE Communication Magazine, Vol. 42, Issue 1, Page 88-96, Jan. 2004.

[3] S. Hagen, IPv6 Essentials, O'Reilly, Jul. 2002.

[4] VSIX Internet Protocol Version 6, http://www.vsix.net/ipv6intro/ipv6Introduction/passive_linux_01.jsp.

[5] J. Bound, L. Toutain, and JL. Richier, Dual Stack IPv6 Dominant Transition Mechanism, Internet-Draft, Oct. 2005.

[6] C. Huitema, Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), RFC 4380, Feb. 2006.

[7] Fedora Project, http://fedora.redhat.com.

[8] DSTM: Dual Stack Transition Mechanism, http://www.ipv6.rennes.enst-bretagne.fr/dstm/index.html.

[9] Miredo Teredo for Linux and BSD, http://www.simphalempin.com/dev/miredo.