2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

NAT와 IPSec을 이용한 홈 네트워크 보안[1]

김홍철*, 송병욱, 박인성, 김상욱
경북대학교 컴퓨터과학과

e-mail:{hckim, bwsong, ispark, swkim}@woorisol.knu.ac.kr

Home Network Security using NAT and IPSec

Hong-Chul Kim*, Byung-Wook Song
In-Sung Park, Sang-Wook Kim

Dept. of Computer Science, Kyung-pook University

요약

최근 홈 네트워크를 구축할 수 있는 기반 전송기술이 급속도로 발전하고 있다. 또한, 이를 이용할 수 있는 고성능의 가전기기가 속속 개발됨에 따라 홈 네트워크가 대중화되고 있다. 이러한 상황에서 가장 중요한 이슈로 떠오르고 있는 것이 홈 네트워크 보안이다. NAT기술은 내부 네트워크를 외부로부터 은닉시키고 보호할 수 있는 새로운 기법을 제공한다는 점에서 최근 많은 관심을 받고 있다. 본 논문에서는 홈 네트워크 보안 시스템을 구현함에 있어 NAT기술과 범용 보안 메커니즘 IPSec을 적용하여 홈 네트워크를 인터넷과 같은 외부의 전산망에 존재하는 위험으로부터 안전하게 보호할 수 있는 기법을 제시한다.

1. 서론

최근 블루투스(Bluetooth), 하비(HAVi), 지니(Jini)등과 같은 유무선 기술이 발전함에 따라서 홈 네트워크를 실제로 구현하는 것이 가능해졌다[1]. 홈 네트워크는 가정에서 중요한 역할을 수행하는 내장 시스템, 멀티미디어 데이터 처리 및 서비스를 위한 셋탑박스 등과 같은 기기로 구성된 내부 네트워크이다. 이와 같은 기기들은 그 사용성을 극대화시키기 위해서 인터넷과 같은 기존의 외부 전산망과 연결되어 있다. 이미 기존의 전산망에서 가장 심각한 문제로 떠오른 것이 보안이며, 이는 홈 네트워크에서 더욱 심각하게 대두되고 있다. 하지만 현재 홈 네트워크를 위한 단순한 형태의 방화벽, 유해사이트 방지 소프트웨어가 상용화되어 있으나, 이들은 대부분 기존의 가정 내 컴퓨터를 대상으로 하고 있으며, 단편적인 보안기능만을 제공한다.

홈 네트워크를 외부 전산망에 존재하는 위험으로부터 보호하기 위해서는 보다 일반화되고 특화된 내부망 보호 메커니즘이 필요하다. NAT는 90년대 초반 IPv4가 지닌 부족한 인터넷 주소공간 문제를 일시적으로 해결하기 위한 임시 방편책으로 고안되었다. 그러나 최근에는 전혀 다른 분야, 즉 내부망 보안, 가상 서버, 가상 라우터 등과 같은 용도로 사용 가능하다는 것을 보여주고 있다. IPSec은 IP 수준에서 인증 및 암호화 기능을 제공해주는 IP 계층 수준의 범용 보안 메커니즘이다.

본 논문에서는 NAT와 IPSec 기술을 자세히 살펴보고, 홈 네트워크 방화벽 구현에서의 기술적용을 통해서 외부의 전산망 위험으로부터 홈 네트워크를 보호하는 방법을 제시한다.

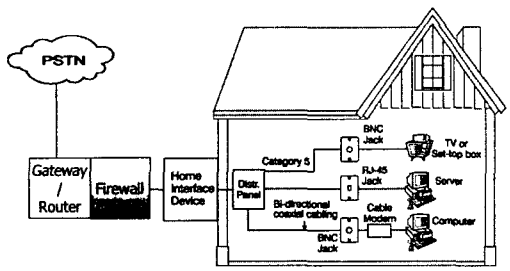
본 논문의 순서는 다음과 같다. 2장에서는 홈 네트워크 보안에 대해서 살펴본 다음, 3장에서 NAT기술, 4장에서는 IPSec을 자세히 설명한다. 5장에서는 NAT와 IPSec 기능을 내장한 방화벽 시스템을 통해서 홈 네트워크를 보호하는 기술을 제시한 다음, 6장에서 결론을 맺는다.

2. 홈 네트워크

최근 초고속 인터넷과 PC의 수요증가로 가정에

1. 본 연구는 정보통신연구진흥원이 지원하는 이동네트워크 정보보호기술개발 연구의 일부분임.

서 인터넷과 컴퓨터, 가전기기 등을 연결하는 홈 네트워크의 관심이 높아지고 있다. 특히 컴퓨터를 비롯한 인터넷, 파일, 프린터 공유는 물론 TV, 냉장고, 전자레인지 등에 연결해 모니터 앞에서 자유롭게 조절할 수 있고 외출 중 실내온도, 화재, 도난 등 집안을 제어할 수 있도록 해 주는 것이 바로 홈 네트워크이다. 이와 같은 홈 네트워크를 구성하는 가정에는 전체를 제어하는 홈 컨트롤 시스템과 같이 매우 중요한 기기를 포함하고 있다. 내부 또는 외부의 영향에 의해서 홈 컨트롤 시스템의 안전성에 문제가 생긴다면 매우 심각한 결과를 초래할 수도 있다. 즉, 홈 네트워크를 내부 및 외부의 전산망 위험으로부터 보호하는 것은 기존의 일반적인 전산망을 보호하는 것 보다 훨씬 중요하다.



(그림 1) 일반적인 홈 네트워크

2.1 홈 네트워크 보안

일반적인 유선 기반의 홈 네트워크는 (그림 1)과 같은 구조를 가진다. 내부망은 기존의 전화선, 이더넷 케이블 등과 같은 여러 가지의 기존 통신매체로 이루어져 있으며, 이것은 외부망과 연결되기 위해서 별도의 변환 장치를 필요로 하는데, 위 그림에서는 이를 Home Interface Device라고 표기하였다. 홈 네트워크를 위한 보안 시스템은 그 규모가 일반 네트워크에 비해서 작다. 따라서 방화벽 시스템과 같은 단일 시스템이 보안 관련 기능을 모두 내장하는 것이 보통이다. 홈 네트워크 보안에서는 크게 다음과 같은 사항들이 고려되어야 한다.

- 외부 전산망에 대한 안전한 접근
- 외부로부터의 접근에 대한 인증 및 접근제어
- 내부의 주요 기기에 대한 안전성 보장

2.1.1 외부 전산망에 대한 안전한 접근

가정 내부에서 PC 또는 이동 단말기를 통해서 외부망에 접속하는 경우 사용자의 개인정보 또는 내부망의 정보는 반드시 보호되어야 한다. 특히 최근 전자상거래나 인터넷을 통한 금전 서비스가 매우 보편화되고 있으므로 외부 전산망에 대한 안전한 접근은 매우 중요한 사항이다.

2.1.2 외부로부터의 접근에 대한 인증 및 접근제어

기존의 전산망과 마찬가지로 홈 네트워크에서 가장 위협이 되는 부분은 외부로부터의 악의적인 내부 네트워크 접속이다. 가정 내부의 중요 제어 시스템에 대한 적법한 접속 인증 및 불법적인 접근에 대한 처리는 홈 네트워크에 적용되는 방화벽 시스템이 갖추어야 하는 필수적인 기능이다.

2.1.3 내부의 주요 기기에 대한 안전성 보장

홈 네트워크는 매우 다양한 종류의 가전기기 및 그들을 제어하는 시스템으로 구성된다. 가정내의 전원 및 에너지를 제어하는 시스템, 멀티미디어 기기 제어를 위한 셋탑박스 등은 다른 기기들을 제어하거나 중요한 데이터를 내부 또는 외부로 전송하는 기능을 수행하므로, 이러한 기기에 대한 안전성 보장은 홈 네트워킹을 위해서 반드시 구현되어야 한다.

3. NAT (Network Address Translation)

NAT는 IP 주소를 다른 IP 주소로 변환하는 것을 의미한다. 90년대 초반 이 기술이 고안된 것은 IPv4가 지니고 있는 고질적인 문제, 즉 부족한 인터넷 주소공간에 대한 해결을 위한 것이었다. 이에 대한 임시 방편책은 내부의 전산망에 사설 IP 주소를 부여한 다음, 사설 IP를 지닌 내부의 호스트가 외부 인터넷에 접속을 할 경우에만 실제 IP 주소를 할당해주는 서버를 두는 것이다. 이 기술을 체계적으로 일반화한 것이 바로 NAT 기술이다. NAT는 내부의 *m*개 IP를 *n*개의 실제 IP(NAT-IP)로 변환하는 일반적인 모델(*m:n translation*)을 가지고 있다, 최근 많이 사용되고 있는 IP-masquerading은 *m:1* NAT 라고 할 수 있다.

3.1 NAT의 기본 원리

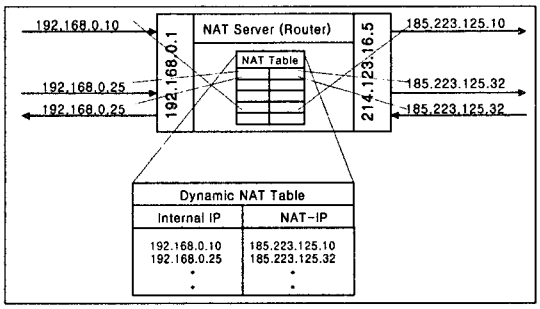
NAT는 IP 주소를 NAT-IP로 변환하는 방법에 따라서 정적 NAT와 동적 NAT로 분류된다[2]. 정적인 NAT는 변환되어야 하는 내부의 IP와 실제 NAT-IP 값이 이미 정해져 있는 것을 의미한다. 내부 IP주소의 수를 *m*, NAT-IP의 수를 *n*이라 하면 정적 NAT는 다음과 같은 매핑으로 표현된다.

m:n translation, m,n ≥ 1 and m = n (m,n ∈ N)
m: number of IPs that need to be translated
n: number of IPs available for translation

정적인 NAT는 변환되어야 하는 IP 주소의 개수와 NAT 서버가 보유하고 있는 NAT-IP의 개수가 동일한 경우에 보편적으로 적용되는 경우인데, 이것

은 동일한 클래스의 네트워크 주소간의 변환에 적당하다.

3.2 동적인 NAT 기술



(그림 2) 동적인 NAT의 내부 구조

동적인 NAT는 변환되어야 할 IP 주소의 개수가 NAT- IP의 개수보다 많은 경우 또는 그 개수가 일치하지만 정적인 매핑을 사용하는 것이 힘들 경우에 적용되는 NAT방식이며, 그 작동구조는 (그림 2)에 표현되어 있다[2]. 동적인 NAT에서의 내부 IP 주소와 NAT 서버의 NAT-IP간의 매핑은 다음과 같이 표현된다.

m:n translation, n ≥ 1 and m ≥ n (m,n ∈ N)

이 경우, 외부망과 통신할 수 있는 내부망의 호스트 수는 현재 NAT 서버가 보유하고 있는 사용 가능한 NAT-IP의 개수에 의해서 제한된다. 만일 사용 가능한 NAT-IP가 전혀 존재하지 않는 경우에는 해당 호스트에게 적절한 ICMP 메시지가 전송되어야 할 것이다(예: 'host unreachable' message). 동적인 NAT는 정적인 NAT에 비해서 그 구현이 훨씬 복잡해진다. 동적인 NAT는 현재 통신하고 있는 호스트뿐만 아니라, 현재의 TCP 연결에 대한 정보를 관리해야 한다. 동적인 NAT는 본 논문에서 적용하고 있는 것과 마찬가지로 내부 네트워크를 보호하는 용도로 사용될 수 있으며, 그 이외에도 부하 분산, 가상 서버, 가상 라우터, 방화벽 우회 라우팅 등과 같이 매우 다양한 방면에 사용될 수 있다.

이 외에도 NAPT라는 NAT의 변형된 기술도 있는데, 이것은 기존의 NAT가 IP 주소에 기반을 두고 매핑을 하는데 반해, TCP 및 UDP 연결의 포트번호도 매핑을 해 주는 기술이다. 가상 서버의 경우 이러한 NAPT를 이용하면 쉽게 구현된다.

4. IPSec

IPSec은 IP 프로토콜을 사용하는 모든 통신 프로토콜에 대해서 보안을 제공해주기 위해서 IETF가 제안한 보안 메커니즘이다. 현재 인터넷상에서 보안성있는 통신을 위해서는 해당 프로토콜 수준에서 서로 다른 도구를 사용한다.

- PGP: 메일 메시지의 암호화 및 복호화
- SSH: 원격 접속에 대한 인증 및 세션 암호화
- SSL/TLS: 안전한 소켓연결(Web)

이와 같은 방법은 해당 응용계층에서만 사용될 수 있으므로 범용성이 없다는 단점을 가지고 있다. IPSec은 이와 같은 범용적인 보안도구에 대한 필요성에 의해서 고안되었다. IP 프로토콜에 기반을 둔 프로토콜이라면 하위 프로토콜이나 상위 프로토콜이 무엇이라고 하더라도 모두 IPSec으로부터의 보안기능을 투명하게 제공받을 수 있다.

4.1 IPSec의 기능별 구성요소

IPSec은 다음과 같이 크게 3개의 프로토콜로 구성된다[3].

- ESP: 데이터의 인증 및 암호화
- AH : 데이터의 인증
- IKE: Internet Key 교환

4.1.1 ESP

ESP (Encapsulation Security Payload) 프로토콜은 IP 패킷의 암호화 및 인증 기능을 제공한다. ESP는 AH 프로토콜이 사용되지 않고 단독으로 사용될 수 있지만, ESP를 이용해서 암호화를 할 경우에는 반드시 인증 기능을 사용해야 한다[3].

현재 RFC 2406에서는 데이터 암호화 알고리즘으로 DES와 null encryption을 지원하고 있다. 또한 인증을 위한 알고리즘으로 keyed MD5와 keyed SHA를 지원한다. ESP가 적용된 IP 패킷은 ESP header와 trailer를 가지고 있으며, 그 위치는 IPSec이 운영되는 모드(전송모드, 터널모드)에 따라서 다르다.

4.1.2 AH

AH (Authentication Header)는 IP 패킷에 대한 인증 기능을 제공한다. 패킷에 대한 인증은 ESP를 이용하지 않고 AH 헤더를 IP 패킷의 헤더 뒷부분에 추가함으로써 구현할 수 있다[3]. 모든 IP 패킷은 헤더에 *next header* 필드를 가지고 있으며, 이것은 이후에 오는 데이터의 종류를 나타내므로, 어떠한 패킷이 AH가 추가된 패킷인지 일반적인 IP 패킷인지 식별할 수 있다. AH 헤더 역시 IPSec의 운영모드에 따라서 그 위치가 달라질 수 있다.

4.1.3 IKE

IKE (Internet Key Exchange)는 호스트간의 통신이 이루어지기 전에 필요한 사항들(인증 및 암호화에 사용되는 각 알고리즘, 키, 접속 유효기간)을 협상한 후 IPSec(ESP 또는 AH)을 설정한다. 이것은 IPSec 엔진을 가진 두 게이트웨이가 500번 포트를 이용해서 서로에게 패킷을 교환함으로써 이루어진다[3]. IKE는 매우 복잡한 프로토콜로서 크게 다음과 같은 하부 프로토콜을 가지고 있다.

- ISAKMP(RFC 2408)
- IPSec DOI for ISAKMP(RFC 2407)
- Oakley key determination protocol(RFC 2412)

IKE는 두 단계의 Phase를 거쳐서 완성된다. Phase 1은 두 게이트웨이가 양방향의 ISAKMP SA를 구성하며, 이것은 Phase 2에서의 IPSec SA를 구성하는데 사용된다. Phase 2는 ISAKMP SA를 이용하여 각각 단방향의 IPSec SA를 구축한다. 두 게이트웨이 사이에는 하나 이상의 IPSec SA가 존재할 수 있다.

5. NAT와 IPSec을 이용한 홈 네트워크 보호

홈 네트워크는 다수의 PC를 비롯하여 셋탑박스나 홈 컨트롤러와 같은 서버 시스템, 무선 단말기를 포함하고 있다. NAT를 이용하면 다음과 같이 홈 네트워크를 보호할 수 있다.

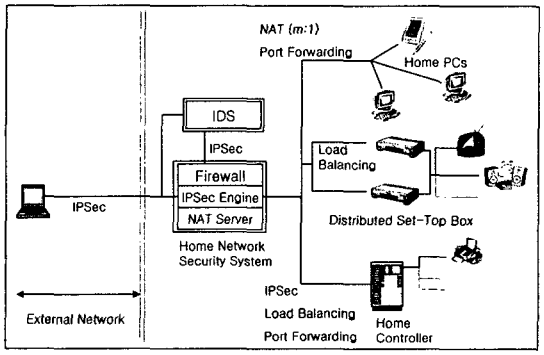
- m:1 NAT를 통한 홈 네트워크 내부정보 은닉
- 부하분산기능(Load Balancing)을 통한 서버의 과부하 해결 및 외부로부터의 DoS공격 방어
- 외부로부터의 안전한 내부 네트워크 엑세스

가정에서 외부 인터넷을 접근할 경우 NAT 서버는 NAPT또는 IP-masquerading 기능을 이용하여 공인 IP 주소를 가지지 않은 기기를 인터넷에 연결할 수 있다. 특히, 외부에서는 내부의 기기에 대한 정보를 얻을 수 없으며 오직 NAT 서버의 정보만을 알 수 있으므로, 홈 네트워크의 내부 전산망 정보를 외부에 노출시키지 않는다.

또한, NAT는 가상 서버기능 및 포트 포워딩 기능을 이용해서 외부에서 내부 서버로의 네트워크 패킷 부하를 분산시킬 수 있으며, 아울러 기존 전산망에서 심각한 문제가 되는 DoS공격을 방어할 수 있다.

외부에서 가정 내부로의 중요 데이터에 접근하는 경우, 악의를 가진 사용자에 의해서 그 정보가 유출될 수 있다. 이를 방지하기 위해서는 보통 방화벽을 설치하게 된다. 그러나 외부에서의 안전한 접속만을 허용하도록 방화벽을 설정하기란 매우 힘들다. NAT는 포트 포워딩을 이용하여 외부에서의 적법한 접속자가 방화벽을 통과하여 중요정보를 수집할 수 있도록 해 준다. 또한, IPSec을 이용하면 홈 컨트롤러와 보안서버 사이의 안전한 통신을 보장할 수 있으며, 외부에서 IPSec을 이용하여 홈 네트워크에 접근한 다음, NAT 서버의 포트 포워딩을 이용해서 안전하게 중요 시스템에 접속할 수 있다.

홈 네트워크 방화벽에서 NAT와 IPSec기술을 구현하여 홈 네트워크 보안체계를 구축하는 예가 (그림 3)에 나타나 있다.



(그림 3) NAT와 IPSec을 적용한 홈 네트워크 보안 시스템 구조

6. 결론

홈 네트워크는 PC를 비롯해서 셋탑박스, 홈 컨트롤러와 같은 중요 가전기기를 포함하고 있다. 홈 네트워크 보안 시스템에 NAT와 IPSec을 적용하면 홈 네트워크를 매우 안전하게 구축할 수 있다.

NAT는 내부의 네트워크 주소를 인터넷상의 공인 IP 주소로 변환 해줌으로써 내부의 전산망 정보를 은닉할 수 있는 기반 도구를 제공해 준다. 또한, 가상 서버 및 포트 포워딩 기술을 이용하여 외부로부터의 과중한 부하를 분산시킬 수 있으며, 현재로서는 별다른 해결책이 없는 DoS공격에 대비할 수 있도록 해 준다. IPSec은 IP 패킷을 네트워크 계층에서 상위 또는 하위 프로토콜에 투명하게 보안기능을 제공해주는 범용 보안 메커니즘이다. 이것은 기존의 모든 환경을 그대로 유지할 수 있다는 커다란 장점을 지니고 있다. IPSec을 이용하면 외부에서 홈 네트워크 내부의 서버 또는 보안 시스템에 안전하게 접속할 수 있으며 보안 시스템을 안전하게 운영할 수 있다.

참고문헌

[1] HomeAPI Specification, Version 0.98, HomeAPI Working Group, Aug. 1999.
[2] Michael Hasenstein, IP Address Translation, 1997, http://www.suse.de
[3] IPSec Information Center, http://www.freeswan.org/docs
[4] Linux Kernel Hacker Guide, http://redhat.com:8080/HyperNews/get/khg.html
[5] Load Distribution for Firewall-1, Check Point Software Technologies Ltd., seen at the 1997 CeBIT