사용자를 위한 선택적인 서비스 지원의 가상사설망 구현

김정범 이윤정 이근호 이송희 김태윤
고려대학교 컴퓨터학과
{qston, genuine, root1004, fine, tykim}@netlab.korea.ac.kr

Implemention of Virtual Private Networks supporting User's choice service

Jeong-Beom Kim, Yun-Jung Ree, Keun-Ho Lee, Song-Hee Yi, Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

IETF에서 IPSec(Internet Protocol Security)[1]의 구조를 발표한 이래 IPSec을 이용한 많은 VPN(Virtual PrivateNetwork)[2][3]이 구축되어 왔다. 이렇게 구축된 VPN에서 사용되는 CG(CryptoGate) 혹은 SG(Security Gateway)는 각각의 망에서 게이트 역할을 한다. 하지만 이런 기존의 CG나 SG는 IPSec의 정책을 사용자가 선택하는 것이 아닌 망 관리자가 일방적으로 서비스하도록 설계되어있다. 이러한 점은 사용자가 자신의 데이터를 평가하여 자율적으로 그에 맞는 서비스를 이용하는 것이 아니므로 사용자가 사용하는 것을 꺼릴 수도 있다. 또한 게이트웨이에 자신의 키를 백업할 수 있도록 하여서 사용자가 다시 이 망에 접근할 경우 다시 키 협상을 하는 것이 아닌 백업해둔 키를 가지고 연결할 수 있도록 하였다. 본 논문은 VPN에서 이러한 점을 고려하여 CG를 설계함으로써 VPN 사용의 확장성을 해결한다.

1. 서론

재택 근무가 활발해지고 기업 외부와도 네트워크 구성이 필요하게 되는 등의 기업 네트워크가 점차 확대되어감에 따라 막대한 시설 투자가 필요하게 되었다. 네트워크의 확대와 함께 네트워크에 연결된 서로간에 안전한 통신을 하기 위해 사용해 오던 전용망에 투자해야 하는 비용과 그에 따른 운영과 관리가 커다란 문제가 되고 있다.

VPN(Virtual Private Network)이란 이런 문제들의 해결을 위한 방안으로, 기업의 네트워크를 구성할 때 전용 임대회선을 사용하는 것이 아니라 공용망인 인터넷망을 이용하는 연결망이다. VPN은 터널링이라는 기법을 사용하여 임대일 연결과 같은 터널을 형성하며 데이터 패킷들은 터널을 통해 안전하게 전달된다. 이러한 터널링을 구현하는 기술로는 PPTP(Point to Point Tunneling Protocol), VTP(Virtual Tunneling Protocol), L2F(Layer 2 Forwarding Protocol), L2TP(Layer 2 Tunneling Protocol), IPSec(IP Security Protocol) 등이 있다. 본 논문에서는 이러한 터널링 기법 중 IPSec으로 구현된 VPN의 환경을 기반으로 연구한다.

IPSec으로 구현된 VPN에서 사용되는 CG(CryptoGate)는 IPSec 정책의 모든 관리가 네트워크 관리자에 의해 결정된다. 이러한 경우 사용자는 자신이 원하는 IPSec 서비스들을 선택할 수 없게 된다. 이러한 점을 해결하기 위해서 본 논문은 IPSec 헤더의 TOS(Type Of Service)[4]부분과 패킷 분석기를 이용하여 사용자가 IPSec 서비스의 서비스 중 하나를 선택할 수 있도록 하였다. 이렇게 함으로써 사용자가 자신의 데이터 특성에 맞는 서비스를 선택할 수 있어 그 사용의 효율성을 높일 수 있도록 하였다.

그리고 요즘 연구가 한창인 키 백업 기술까지 사용자가 원할 경우 이용할 수 있도록 도입하여 구상 및 설계를 하였다.

2.관련연구

2.1 VPN(Virtual Private Network)[2][3]

가상 사설 네트워크(VPN)는 인터넷과 같은 공유 또는 공용 네트워크를 통한 연결을 포함하는 사설 네트워크의 확장이며 공유 또는 공용 인터네트워크를 통해 지점간 개인 링크 속성을 에뮬레이션하는 방법으로 두 컴퓨터간에 데이터 전송이 가능하다. 지점간 링크를 에뮬레이션하기 위해 데이터는 공유 또는 공용 인터네트워크를 통과하여 목적지에 도달할 수 있도록 라우팅 정보를 제공하는 헤더에 의해 캡슐화 된다. 개인 링크를 에뮬레이션하기 위해 전송되는 데이터는 암호화되어 기밀성이 유지되고 공유 또는 공용 네트워크에서 차단되는 패킷은 암호 키가 없으면 암호화될 수 없는데, 개인 데이터가 캡슐화되고 암호화되는 링크를 가상 사설 네트워크(VPN) 연결이라고 한다.

그림 1은 VPN의 논리적 개념을 나타낸다.

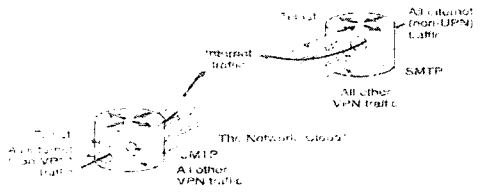

그림1.가상사설 네트워크(VPN)

VPN 연결은 사용자가 인터넷과 같은 공용 네트워크에서 제공하는 하위 구조를 사용하여 가정에서나 이동 중에도 회사 서버에 원격 액세스 연결을 할 수 있게 해 준다. 사용자의 입장에서 볼 때, VPN은 컴퓨터, VPN 클라이언트, 회사 서버인 VPN 서버간의 지점간 연결이며 공유 또는 공용 네트워크의 정확한 하부 구조는 논리적으로 전용 사설 링크를 통해 데이터를 보내는 것처럼 보다 안전하게 데이터를 전송할 수 있다. VPN 연결은 또한 회사가 인터넷과 같은 공용 인터네트워크를 통해 지리적으로 떨어져 있는 사무실이나 다른 회사와 보안이 유지되는 통신을 유지하면서 연결을 라우팅할 수 있게 해 준다. 원격 액세스 연결 및 라우팅 된 연결과 함께 VPN 연결을 통해 기업은 시외 전화나 구내 전화 전용 회선 또는 인터넷 서비스 제공자(ISP) 전용 회선을 사용할 수 있다.

2.2 IPSec(Internet Protocol Security)[1]

IPSec은 다음과 같은 보안 서비스를 제공한다. 이 서비스는 선택적이며 일반적으로 로컬 보안 정책은 이 서비스 중에서 하나나 그 이상의 서비스를 선택한다.

- 데이터의 비밀성 - IPSec의 송신자는 네트워크로 전송되기 전에 데이터를 암호화하여 보낸다.
- 데이터의 무결성 - IPSec 수신자가 보내는 데이터는 받는 사람의 데이터와 같다.
- 데이터의 인증 - IPSec의 수신자는 패킷을 보낸 송신자의 인증을 확인할 수 있다.
- 재사용성 방지 - IPSec 수신자는 재사용 공격을 방지할 수 있다.

IPSec 동작에는 세 가지 기본 구성요소가 필요하다. 즉, Security Association(SA)[5][6], Authentication Header(AH)[7], Encapsulating Security Payload(ESP)[8]가 IPSec 동작에 중요한 역할을 한다.

3. 본론

3.1 선택적인 서비스 지원을 위한 CG 메커니즘

앞에서 언급한 대로 IPSec 서비스는 네트워크 관리자가 일방적으로 사용자가 서비스하게끔 되어 있는 구조이다. 이런 문제를 해결하기 위한 방안으로 본 논문은 IP Header의 TOS(Type Of Service) 필드의 2비트를 이용한다. 2비트로 구분한 이유는 사용자가 원하는 보안 서비스를 받을 수 있게 하기 위함이며, KRH 서비스를 시행할 경우 오직 한 번의 패킷을 보냄으로써, 네트워크 리소스를 효과적으로 이용할 수 있기 때문이다.

TOS 설정에 따른 동작은 표1과 같다.

표 1 TOS 설정에 따른 서비스

1bit \ 2bit	0	1
0	일반 패킷	AH
1	ESP	AH+ESP(Backup)

표 1을 살펴보면, TOS의 맨 앞 비트는 사용자의 데이터에 대해 ESP 서비스를 요청할 때 설정하여 보내는 것이며 TOS의 두 번째 비트가 설정된 경우에는 자신의 데이터를 위해 AH 서비스를 요청할 때 설정하는 것이다.

이 표에서 중요한 점은 ESP와 AH를 같이 쓸 경우에만 사용자의 세션키가 백업된다. 이것은 KRA(Key Recovery Alliance)에서 발표한 KRH[9][10]에 대한 논문에 자세히 나와 있듯이, 키에 대한 정보를 AH와 함께 쓰지 않을 경우 변경 등과 같은 위험성 때문이다.

이러한 전체적인 구상도는 그림 2와 같다

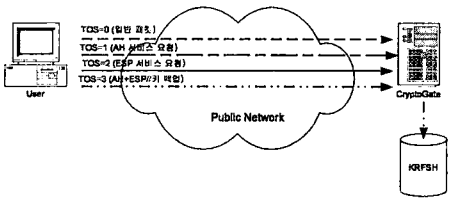

그림 2 제안한 사용자와 CG의 동작원리

제안한 CG를 사용하기 위한 사용자 인터페이스는 다음과 같다.

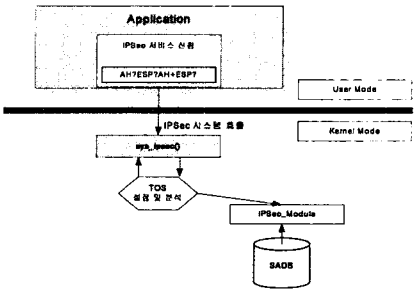

그림 3 사용자 인터페이스

그림3을 보면 사용자 응용계층에서 자신의 데이터에 맞는 서비스를 선택하게 되면 커널 영역에서는 IPsec 시스템 호출이 발생하게 된다. 시스템 호출에서는 표 1과 같은 서비스 테이블을 참조하여 IPSec 처리한 패킷을 전송하게 된다.

이렇게 전송된 패킷의 처리를 위한 CG의 내부 구성을 살펴보면 그림4와 같다.

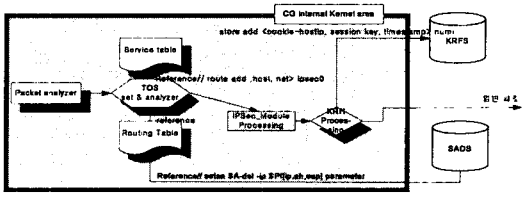

그림 4 CG 내부 커널 다이어그램

그림 4를 살펴보면 사용자측에서 IPSec 처리된 패킷이 들어오면 패킷 분석을 통해 서비스 테이블과 라우팅 테이블을 참조하여 TOS 설정 비트를 통한 서비스 처리를 해주게 된다. IPSec 모듈을 통과할 때 TOS 비트가 3일 경우 서비스 테이블을 참조하여 키 백업이라는 사용자의 요구에 따라 사용자의 쿠키 값과 만료시간, 세션키등을 외부 Storage인 KRFS(Key Recovery Field Storage)에 백업한다. 그리고 모든 패킷에 대한 서비스를 처리해준 후 일반 패킷을 목적지 호스트에 전송해주게 된다.

3.2 에러 처리를 위한 ICMP(Internet Control Message Protocol)[11]

본 장에서 필요한 에러 메시지 타입의 종류는 4가지가 있다. 이 4가지 종류로는 먼저 사용자에게 전송된 패킷이 CG 내부의 네트워크에 없는 경우, 둘째 서비스 테이블에 맞게 처리되지 않은 경우, 그리고 키 백업을 성당하게 요청하지 않은 경우 마지막으로 SADB(Security Association DataBase)에 사용자의 SA 협상 내용이 없는 경우이다.

이러한 에러를 처리하기 위한 ICMP 메시지 타입을 정리하면 표2와 같다.

표2. ICMP 에러 메시지 타입

type	code	Description
19		IPSec message
	0	라우팅 테이블 참조 에러
	1	서비스 테이블 참조 에러
	2	키 복구 에러
	3	SADB 참조에러

3.3 CG의 동작 결과

그림 5는 CG가 제대로 동작하는지를 알아보기 위하여 사용자측에서 전송하기 전의 패킷을 printk()함수를 써서 패킷을 스니핑한 결과이다.

```
receiving ESP packet (before sending 48):
 00 00 ff ff ff ff ff ff fe fe 00 00 00 00 08 06 00 01 08 00 06 04
00 01 fe fe 00 00 00 00 a3 98 00 01 00 00 00 00 00 00 a3 98 28
3c 01 02 02 04
```

그림5. 전송하기 전 패킷 내용

그 다음 목적지 CG의 NIC 모듈에 역시 printk() 함수를 써서 복호화하기 전의 암호화 패킷 내용과 복호화한 후의 패킷 내용을 스니핑 해서 보낸 패킷의 내용과 복호화 한 후의 패킷 내용이 같은지를 분석하였다.

```
receiving ESP packet (before decrypt):
 59 93 cf 5c 2c af 39 50 71 e0 67 90 19 ea ce df 17 d2 dd 3f 8e
d5 77 3f e8 aa f3 b5 3a 29 99 6a ff 41 a6 93 05 05 b0 b8 14 69 a6
b0 55 08 12 db
receiving ESP packet (after decrypt 48):
 00 00 ff ff ff ff ff ff fe fe 00 00 00 00 08 06 00 01 08 00 06 04
00 01 fe fe 00 00 00 00 a3 98 00 01 00 00 00 00 00 00 a3 98 28
3c 01 02 02 04
```

그림6. 복호화 되기 전· 후의 패킷 내용

그 결과 비교한 패킷의 내용이 같음을 분석하였고 패킷의 내용이 그림6처럼 암호화되어서 전송된다는 것을 알 수 있었다.

4. 결론 및 향후 연구 과제

본 논문에서는 기존의 IPSec에서 정책서버를 복잡성을 줄이고 사용자의 신뢰 확보와 안정성을 지원할 수 있는 IPSec을 제안한다. 임의대로 불필요한 보안 서비스를 정책적으로 시행하는 것보다는 사용자 자율성을 고려하여 자신의 전송할 데이터의 보안 등급을 결정하고 그에 따른 자신의 서비스를 선택할 수 있다. 또한 사용자의 세션키를 분실한 경우 백업해둔 키를 이용할 수 있어 사용자가 사용하기에 좀더 신뢰성이 있도록 하였다.

향후 연구 과제는 무선 환경 하에서 사용자의 신뢰성을 확보할 수 있는 캡슐화 방식의 키 복구 기반을 제공할 수 있는 IPSec을 구현하는 방법을 연구하고자 한다.

5. 참고 문헌

[1] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, NRL,

[2] Kosiur, D., "Building and Managing Virtual Private Networks?", John Wiley & Sons. 1998.

[3] http://www.freeswan.org/freeswan_trees/freeswan-1.8/doc/index

[4] Almquist, P., "Type of Service in the Internet Protocol suite", RFC 1349, July, 1992.

[5] Harkins, D., and Carrel, D., "The Internet Key Exchange (IKE)", November 1998, RFC 2409, available at http://www.cis.ohio-state,.edu/Service/rfc/rfc-text/rfc2409.txt.

[6] Maughan, D., chertler, M., Schneider M. and Tunner, J., "Internet Security Association and Key Management Protocol(ISAKMP)", RFC 2408, NRL, November 1998.

[7] Atkison, R., "IP Authentication Header", RFC 2402, NRL, November 1998.

[8] Atkison, R., "IP Encapsulation Security Payload", RFC2406, NRL, Npvember 1998.

[9] Gupta, S., "A Common Key Recovery Block Format: promoting Iteroperability between dissimilar key recovery schemes", KRA white-paper, 1998.

[10] Markham, T., and Wiliams, C., "Key Recovery Header for IPSec", draft Key Recovery Alliance Recommendation 2, Aprile 1998.

[11] Postel, J. B., "Internet Control Message Protocol", RFC 792,21, 1981.