

# IPSec을 적용한 가상사설망의 성능개선을 위한 동적 키 재생성 주기 변경 프로토콜

\*한종훈, 이정우, 박성한  
한양대학교 컴퓨터공학과

e-mail : {\*jhhan, jwlee, shpark}@cse.hanyang.ac.kr

## Dynamic Key Lifetime Change Protocol for Performance Improvement of Virtual Private Networks using IPSec

\*Jong Hoon HAN, Jung Woo LEE, Sung Han PARK  
Department of Computer Science & Engineering Hanyang University

### Abstract

In this paper, we propose a dynamic key lifetime change protocol for performance enhancement of virtual private networks using IPSec. The proposed protocol changes the key lifetime according to the number of secure tunnels. The proposed protocol is implemented with Linux 2.4.18 and FreeS/WAN 1.99. The system employing our proposed protocol performs better than the original version in terms of network performance and security.

### I. 서론

공중망을 이용하여 Virtual Private Network (VPN)을 구축하기 위해서는 네트워크 계층에서의 보안이 필수적인데 IETF의 네트워크 계층 보안 프로토콜 표준이 바로 IPSec이다[1]. IPSec Gateway를 사용하여 VPN을 구성 할 경우 각 Gateway간에 터널링 방식으로 암호화 된 데이터를 전송하게 되는데, 이 가상의 보안터널을 맺기 위해 키를 협상하고 전송하는 프로토

콜이 Internet Key Exchange (IKE)이다[2]. IKE에서는 암호 키의 노출을 막기 위해 주기적으로 암호 키를 재생성하게 되는데, 이는 계산집중적인 방식으로 이루어져 있어서 네트워크 성능을 저하시키는 주요 요인 중 하나이다. 이 키 재생성 주기에 대한 기존 연구가 충분하지 않아서 네트워크 관리자가 임의로 설정해서 사용하는 문제가 있고, 또한 망의 트래픽 상황에 관계 없이 하나의 값으로 고정되어 있어서 비효율적이다. 따라서 본 논문에서는 보안터널 수에 따른 적절한 키 재생성 주기를 결정하고, 그 결과를 이용하여 각 터널의 트래픽 상황을 모니터링 하여 동적으로 키 재생성 주기를 변경하는 방법을 제안한다.

### II. IPSec

IPSec은 IP datagram을 위한 상호운용 가능한 암호 기반의 고품질 보안을 제공하도록 설계되었다. IPSec에서는 이러한 목표들이 Authentication Header (AH)와 Encapsulating Security Payload (ESP)의 두 가지 트래픽 보안 프로토콜, 키를 협상하고 관리하는 IKE 프로토콜의 사용을 통해 총족된다[3].

## 2.1 AH

AH 프로토콜은 무결성, 데이터 근원 인증, 재전송 공격 방지 서비스를 제공한다. 그러나 AH는 자신이 보호하는 패킷을 암호화하지 않으며, 따라서 어떠한 기밀성 서비스도 제공하지 않는다. IPSec 처리에 의해 AH가 들어가는 위치와 보호의 범위는 운용방법에 따라 달라진다. 먼저 트랜스포트 모드에서 AH 프로토콜로 인증하는 경우에는 원래의 IP 헤더의 일부 필드(TTL등 전송 중에 달라질 수 있는 필드)를 제외한 전체 범위가 된다. 터널 모드에서 AH 프로토콜을 적용할 때의 헤더 구조는 그림 1과 같다.

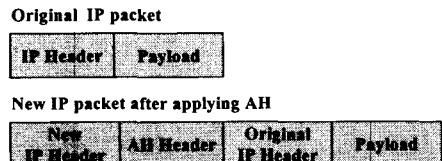


그림 1 터널모드 AH 구조

## 2.2 ESP

ESP는 데이터 기밀성, 데이터 근원 인증, 무결성, 재전송 공격 방지 서비스, 제한된 트래픽 흐름 기밀성을 제공한다. 기밀성 서비스는 패킷을 암호화하기 위한 암호알고리즘을 사용함으로써 제공된다. 트래픽 흐름 기밀성은 터널 모드에서만 제공된다. 터널 모드에서 ESP 프로토콜을 적용하는 경우 패킷의 구조는 그림 2와 같다.

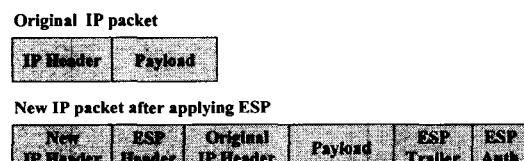


그림 2 터널모드 ESP 구조

## 2.3 IKE

IKE는 Security Association (SA)의 수립을 위하여

인증된 키 자료를 보호된 방식으로 협상하고 제공하는 프로토콜이다. IKE는 ISAKMP, Oakley, SKEME의 관련 부분을 결합한 프로토콜이다. IKE는 2단계 SA 수립과정을 보호하기 위한 1단계 교환과 실제 데이터를 보호하기 위한 IPSec SA를 수립하는 2단계 교환으로 구성된다.

## III. 키 재생성 주기

IPSec을 적용한 보안게이트웨이를 이용하여 VPN을 적용할 경우 가장 큰 문제는 네트워크 성능의 저하이다. 네트워크 성능 저하의 주요 요인 중 하나로 키 재생성을 들 수 있다. IPSec은 암호화키의 노출을 막기 위해 주기적으로 키를 재생성 한다. 키의 재생성은 매우 복잡한 연산을 필요로 하므로 키를 자주 생성하면 네트워크 성능이 급격히 저하된다. 그러나 네트워크 성능만을 고려하여 키 재생성 주기를 너무 길게 하면 키가 노출될 가능성이 높아진다. 따라서 네트워크 성능과 보안성을 고려한 적절한 키 재생성 주기의 결정이 필요하다. 또한 보안 터널 수에 따른 고려가 필요하다. 이 키 재생성 주기는 모든 VPN에 적용할 수 있는 일반화된 값이 존재하지 않는다. VPN 게이트웨이의 수, 각 게이트웨이의 연산 능력, 설치된 곳의 인터넷 망 상태 등 여러 가지 요인이 복합적으로 작용하기 때문이다. 그러나 실험을 통한 예시를 참조하여 설정에 맞게 적용 할 수 있을 것으로 사료된다.

### 3.1 테스트 베드 환경

본 논문에서는 Red Hat Linux 8 (kernel 2.4.18-14)를 OS로 하고 IPSec 공개구현 프로젝트인 FreeS/WAN 1.99를 설치하여 보안게이트웨이를 구성하였다. 하드웨어 사양은 펜티엄-3 700Mhz CPU, 256M 메모리이다. 각 게이트웨이는 직접 연결하고 여기에 네트워크 성능 분석기인 SmartBits 200을 사용하여 측정하였다. AH, ESP를 적용하고 MD5, 3DES를 사용하였고, 인증방식으로 digital signature(RSA public key)를, 옵션으로 PFS를 사용하였다.

### 3.2 측정 결과

표 1 보안터널수와 키 재생성 주기에 따른 네트워크 처리율 (Mbps)

터널수 키주기(s)	1	10	30	50	80
1800/450	31.9809	30.5413	28.9677	28.5021	27.9623
1800/225	31.9784	30.4608	28.8945	28.2581	27.8885
800/200	31.9794	30.4183	28.5761	27.8137	24.6521
800/100	31.9548	30.4006	28.8701	27.7892	24.0967
400/100	31.7657	30.3137	28.4087	27.8031	23.8297
400/50	31.6135	30.3218	27.8885	27.3085	23.0585
200/50	31.6045	30.2474	27.6738	24.0541	22.7711
200/25	31.6039	30.2359	27.3843	23.0713	21.7789
100/25	31.6041	30.2383	27.2209	23.0713	21.5332
50/25	31.6029	30.2554	27.3117	23.4558	20.9233
30/15	31.6021	28.6921	24.6692	21.7961	18.7401

보안터널이 1개인 경우 키 재생성 주기를 짧게 하여도 네트워크 성능에는 큰 변화가 없는 것을 알 수 있다. 그러나 보안터널이 80개인 경우에는 키 재생성 주기가 네트워크 성능에 큰 영향을 미치고 있다. 또한 보안터널 수에 따라 급격히 네트워크 성능이 저하되는 구간이 있음을 알 수 있다. 이에 따라 이 구간보다 조금 긴 키 재생성주기를 선택하면 보안성과 네트워크 성능 사이에서 적절한 키 재생성 주기를 결정할 수 있다.

#### IV. 키 재생성 주기의 동적 변경

VPN에서 모든 게이트웨이가 동시에 송수신을 하는 경우는 거의 없다. 망의 용도에 따라 다르지만 가능한 모든 연결의 90%정도가 사용될 수도 있고 20~30%만이 사용될 수도 있다. 그럼에도 불구하고 기존 방식에서는 VPN에 고정된 한 개의 키 재생성 주기만이 허용되기 때문에 가장 큰 값을 선택하거나 혹은 평균을 내서 사용할 수밖에 없다. 이는 매우 비효율적이므로 본 논문에서는 트래픽 상황에 따라 동적으로 적절하게 키 재생성 주기를 변화시키는 프로토콜을 제안한다. 동작 방법은 그림 3과 같다.

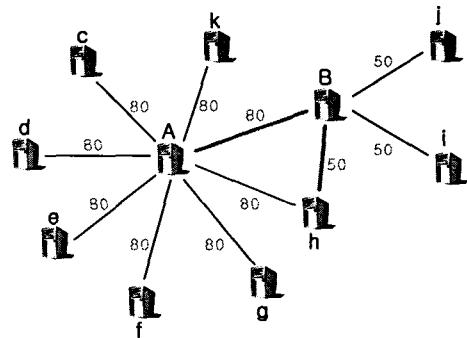


그림 3 보안 터널 수에 따른 키 재생성 주기의 동적 변경

보안터널 수가 10, 30, 50, 80, 120개일 때 각각에 적절한 키 재생성 주기를 결정했다고 가정한다. 망 전체에 보안게이트웨이(SG)가 11개가 존재하고 SG 하나 당 10개의 보안터널을 사용한다고 가정하면 SG 하나의 최대 연결 가능한 터널 수는 100개이므로 120개에 맞는 키 재생성 주기가 사용되어야 한다. 그러나 제안하는 방법에서는 A-B, B-h간 연결이 없는 경우 A는 80, B는 30개에 맞는 키 재생성 주기를 사용하게 된다. A-B간 터널이 활성화 되면 A는 80개, B는 30개에 맞는 키 재생성 주기를 제안하게 되는데 이렇게 상충하는 경우에는 긴 것을 채택한다. 그리고 B-h간 연결이 활성화되면 B는 50개, h는 30개를 제안하고 50개가 채택된다. 이후 B는 i와 j에게 키 재생성 주기를 50으로 변경하라는 메시지를 보내서 변경을 완료한다.

본 논문에서는 동적 키 재생성 주기 변경을 위해 그림 3과 같은 구조를 제안한다.

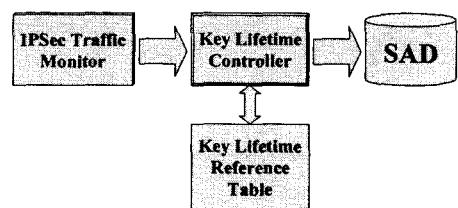


그림 4 동적 키 재생성 주기 변경 프로토콜

IPSec peer간 통신을 위해서는 암호화 알고리즘, 운영모드, 암호 키, 키의 수명 등에 대한 합의가 필요하는데 이것을 IPSec에서는 SA라고 하며 SA의 뜻을 SA database (SAD)라고 한다. SAD내에서 SA는 Security Parameter Index (SPI), 송/수신지 IP 주소에

의해서 고유하게 식별된다. IPSec Traffic Monitor에게 송수신중인 보안터널 수를 보고 받은 Key Lifetime Controller는 Key Lifetime Reference Table에서 터널 수에 해당하는 키 재생성 주기를 가져와서 SAD내 SA의 값을 변경한다.

## V. 제안한 프로토콜의 구현

FreeS/WAN은 리눅스에서 IPSec 프로토콜을 구현하는 공개 프로젝트 중의 하나이다. FreeS/WAN에서는 KLIPS라는 리눅스 커널 모듈과 Pluto라는 커널 밖에서 동작하는 데몬(daemon) 두 개의 구조로서 구현하고 있다.

KLIPS는 리눅스 커널 속에서 실제 IPSec packet의 처리, 암호화, 패킷 인증 값 계산, outgoing packet에 대해 ESP 헤더와 AH 헤더 생성, incoming packet에 대해 헤더의 해석을 처리한다. Pluto는 KLIPS와 달리, 리눅스 커널 속에서 동작하는 것이 아니라 데몬(daemon)프로그램으로 커널 밖에서 동작한다. IKE 프로토콜을 구현으로 phase 1 ISAKMP SA의 생성, 호스트간 인증과 다른 게이트웨이와의 협상을 처리하고 IPSec SA를 생성한 후 관련 파라미터를 리눅스 커널 속에서 동작하는 KLIPS에 전달하는 역할을 한다. Pluto안에 IPSec Traffic Monitor와 Key Lifetime Controller를 구현하였다.

IPSec Traffic Monitor는 /proc/net/ipsec\_eroute의 보안 터널별 통과한 패킷수를 참조하여 활성화된 터널의 수를 체크한다. 그림4는 ipsec\_eroute의 예제이다.

251	192.168.1.2/32	->	192.168.2.2/32	=> tun0x14b0@
0	192.168.1.3/32	->	192.168.2.3/32	=> tun0x14b2@
1910	192.168.1.4/32	->	192.168.2.4/32	=> tun0x14b4@
47	192.168.1.5/32	->	192.168.2.5/32	=> tun0x14ac@
115	192.168.1.6/32	->	192.168.2.6/32	=> tun0x14ae@
0	192.168.1.7/32	->	192.168.2.7/32	=> tun0x14a6@
196	192.168.1.8/32	->	192.168.2.8/32	=> tun0x14a8@
468	192.168.1.9/32	->	192.168.2.11/32	=> tun0x14a@

그림 4 /proc/net/ipsec\_eroute

첫 번째 열이 통과한 패킷의 개수이고, 순서대로 송신 IP, 수신 IP, SA의 식별자이다. 식별자 뒤에는 수신

게이트웨이 IP가 붙는다. 각 터널별로 통과한 패킷수를 주기적으로 저장하여서 터널의 활성화 여부를 결정하고 Key Lifetime Controller에 보고한다.

FreeS/WAN에서 SAD는 KLIPS에 구현되어 있는데 Pluto의 값을 참조한다. 이 값은 state 구조체 안에 connection 구조체가 포함된 이중 구조체의 형식으로 구현되어 있다. 그림5는 connection 구조체의 일부이다.

```
struct connection {
    char *name;
    lset_t policy;
    time_t sa_ike_life_seconds;           ①
    time_t sa_ipsec_life_seconds;         ②
    time_t sa_rekey_margin;
    :
};
```

그림 5 connection 구조체

①, ②가 키 재생성 주기를 나타낸다. Key Lifetime Controller는 터널 수를 보고 받아 Key Lifetime Reference Table의 값을 가져온 뒤 SAD의 ①, ② 값을 변경한다.

## VI. 결론

본 논문에서는 IPSec을 적용한 VPN의 트래픽 상황에 따른 키 재생성 주기의 예를 제시하고 이를 바탕으로 동적으로 키 재생성 주기를 변화시키는 프로토콜을 제안한다. VPN의 최초 설치 시 측정을 통하여 적절한 키 재생성 주기를 결정하면, 이후 제안한 프로토콜을 사용하여 트래픽 상황에 따라 효율적으로 키 재생성 주기를 변화시킴으로써 네트워크 성능과 보안성을 개선할 수 있다.

## References

- [1] Roger Younglove, "IP security: what makes it work?", *Computing & Control Engineering Journal*, Vol 12, Issue 1, Feb 2001.
- [2] R. Perlman, C. Kaufman, "Key exchange in IPSec: analysis of IKE", *Internet Computing, IEEE*, Vol 4, Issue 6, Nov/Dec 2000.
- [3] Carlton R. Davis, "IPSec : Securing VPNs", *McGraw-Hill*, July 2001.