SSFNet을 이용한 보안전송 성능개선에 관한 연구

*류정은 **류동주 *이택희
*호남대학교 정보통신공학과
**전남대학교 정보보호협동과정

A Study on the Performance Improvement of the Security Transmission Using the SSFNet

*Jung-Eun, Ryu **Dong-Ju, Ryu *Taek-Hee, Lee
*Dept. of Information & Communication Engineering, Honam Univ.
**Interdisciplinary Program of Information Security, Chonnam Univ.
E-mail : *truenani@nate..com **ryu@gwangju.ac.kr

요 약

IPSec(Internet Protocol Security)은 IP(Internet Protocol)계층에서 패킷에 대해 무결성(Integrity), 기밀성(Confidentiality), 인증(Authentication), 접근제어(Access Control) 등의 보안 서비스를 제공하는 국제표준 프로토콜이다. 하지만 IPSec의 지나친 복잡성으로 시스템 구현이나 상호 호환의 어려움을 겪고 있는데, 이는 IKE의 복잡성에서 기인한다. 양단간의 신뢰성 있는 암호화키의 관리와 분배를 위해 사용되는 IKEv1(Internet Key Exchange Version 1)은 시스템의 복잡하고 DoS(Denial of Service) 공격에 취약하며 호스트에 *Multiple IP* 주소를 지원하지 않기 때문에 무선에서 사용이 불가능했다. 이를 극복하기 위해 개발된 것이 IKEv2 프로토콜로써 기존 IKE의 페이스 개념을 계승하고 있고 동일한 ISAKMP (Internet Security Association and Key Management Protocol) 메시지 포맷을 사용하고 있지만, 기본적으로 Phase 1에서 교환되어야 하는 기본 메시지 개수가 6개에서 4개로 줄어들었고 인증방식도 기본의 4가지 방식에서 2가지 방식으로 줄었다. 또한 DoS(Denial of Service) 공격에 잘 견디도록 설계되었다. 본 논문에서는 SSFNet(Scalable Simulation Framework Network Models)이라는 네트워크 보안 시뮬레이터를 이용하여 IKEv1과 IKEv2의 보안전송의 키 교환 지연값을 비교 분석하여 성능을 측정하고 그에 따른 문제점과 개선 방안에 대해 연구하였다.

ABSTRACT

IPsec(Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. IPSec is providing authentication, integrity and confidentiality security services. The specifications for Internet Key Exchange(IKEv1) were released to the world. Some criticisms of IKEv1 were that it was too complex and endeavored to define too much functionality in one place. Multiple options for multiple scenarios were built into the specification. The problem is that some of the included scenarios are rarely if ever encountered. For IPsec to work, the sending and receiving devices must share a Public Key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley(ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates. This thesis is a study on the performance improvement of the security transmission using the SSFNet(Scalable Simulation Framework Network Models)

키워드

IPv6, IPSec, IKEv1, IKEv2, SSFNet, ISAKMP/Oakley

I. 서 론

IPv6는 확장헤더에 IPSec 프로토콜을 탑재하는 것으로 보안문제 해결을 시도하고 있다. IPSec은 무

결성, 기밀성, 인증, 접근제어 등의 보안 서비스를 제공하며, 보안서비스가 IP 계층에서 제공됨으로서 기존의 응용 소프트웨어에 대한 변경을 요구하지 않아 일반 사용자에게는 투명한 상태로 처리되며, 응용계층 및 트랜스포트 계층의 모든 프로토콜에 공통된 정보보호 서비스를 제공 할 수 있다. IKE는 양단간의 신뢰성 있는 암호화키의 관리/분배를 위해 사용되며 IKEv2는 IKEv1이 가지고 있는 대부분의 특징과 속성들을 유지하면서 프로토콜을 단순화하였고, 효율성과 안전성, 강건성, 그리고 유연성을 증대시킬 수 있도록 설계되었다[1][11].

SSFNet은 실제 인터넷을 모델링하고 시뮬레이션하기 위해서 프로토콜들(IP, TCP, UDP, BGP4, OSFP 등)과 네트워크 구성 요소(Host, Router, Link, LAN 등)를 클래스로 구현한 자바 모델이다[5][13][14]. 본 논문에서는 SSFNet을 이용하여 IKEv1과 IKEv2의 보안전송을 시뮬레이션하고 그 결과로 키 교환 시 나타나는 지연시간을 측정하여 두 프로토콜간의 성능을 측정하고 그에 따른 문제점과 개선 방안에 대해 연구하였다.

Ⅱ. SSFNet의 개요

1. SSFNet

SSFNet(Scalable Simulation Framework Network Models)은 프로세스 기반 이산 사건 중심 시뮬레이션 커널(Process based Discrete Event-oriented Simulation Kernel)이다. 시뮬레이션 커널인 SSF의 소스는 공개되지 않았으나 그 중에서 네트워크 시뮬레이션을 지원하는 SSFNet은 라우터, 링크, 네트워크 인터페이스 카드 등 대부분의 인터넷 서브시스템들을 시뮬레이션 하는데 필요한 다양한 객체들이 Java로 구현되어 시뮬레이션 특성에 맞추어 그 특성을 변경 할 수 있다는 장점을 가지고 있다. 또한 SSFNet은 SSF를 기반으로 10만개 이상의 노드로 구성된 대규모 네트워크까지도 표현하도록 허용하고 있으며, 네트워크상의 실존하는 특정 행동을 따라 구현이 가능하다[6][8][13].

2. DML(Domain Modeling Language)

SSFNet에서 네트워크의 모델을 기술할 때 사용하는 언어인 DML은 단순한 문법을 가지고 있어 사용자가 손쉽게 특정 시나리오를 모델링할 수 있으나, 간단한 네트워크 모델을 구성하더라도 상당히 많은 양의 노력과 코딩이 필요하다는 단점을 가지고 있다[7][13].

[그림 1]은 하나의 네트워크가 있고 그 안에 두개의 호스트가 연결되어 있는 네트워크 구성을 나타낸다.

```
Net [
    host [ id 1 interface [ id 1 ] ]
    host [ id 2 interface [ id 1 ] ]
    link [ attach 1(1) attach 2(1) ]
]
```

[그림 1] DML Source Code

Ⅱ. IPSec의 개요

1. IPSec

IPSec의 보안기능은 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 확장 헤더를 기반으로 한다. AH 프로토콜은 IP 데이터그램에 대해 무결성(Integrity), 인증(Data Origin Authentication), 재전송 공격(Replay Attack) 방지 등과 같은 보안서비스를 제공하기 위해 사용되며 MD(Message Digest Algorithm)5, SHA(Secure Hash Algorithm)-1 등의 알고리즘을 사용한다. ESP 프로토콜은 IP 데이터그램에 3DES(Triple Data Encryption Standard), AES(Advanced Encryption Standard) 등의 알고리즘을 적용하여 기밀성(Confidentiality), 무결성(Integrity), 인증(Data Origin Authentication), 재전송 공격(Replay Attack) 방지 등과 같은 보안 서비스를 제공하기 위해 사용된다[2][3][4].

2. IKEv1 프로토콜

통신하는 두 호스트 사이의 키와 필요한 정보를 교환한다. 크게 두 단계로 이며, 첫 단계는 ISAKMP SA(Security Association)라고 불리는 키와 정보를 교환하는 단계이며 첫 단계에서 교환된 키와 정보에 의해 암호화된 상태에서 두 번째 IKE 단계가 수행된다. IKEv1은 DoS에 취약하고 지나치게 복잡하다는 점, 발생하지 않는 문제들에 대해서도 시나리오를 만들고, 그 시나리오를 해결하기 위해서 프로토콜의 디자인과정에서 정작 필요한 기능들은 없애고 기본 프로토콜만 복잡해지는 단점을 가지고 있다[5][11].

3. IKEv2 프로토콜 기술 연구 동향

Mobike WG(Mobile IKE Working Group)은 한 호스트가 다수의 IP를 소유하는 경우나 IPSec환경에서 로밍이나 단말의 이동성으로 인해 IP 주소의 변

경이 발생하는 경우, 이를 지원하기 위한 IKEv2 프로토콜을 확장하기 위해 구성되었다. Mobike는 다음 두 가지 경우를 지원, IKEv2를 확장하기 위한 IETF 워킹그룹이다[5][10].

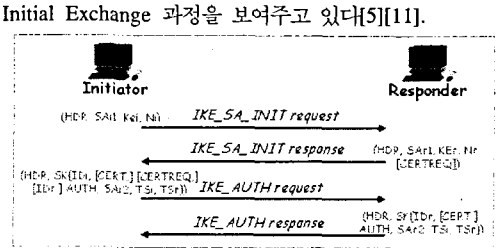
- 한 호스트당 multiple IP 주소가 존재
- IPSec환경에서 로밍이나 Mobility로 인한 IP주소 변경발생

현재 Mobike에서 연구 진행하는 것은 NAT(Network Address Translation)를 사용가능하게 하기 위한 방안에 대해서 초점이 맞추어져 있으며 키 인증과정에 대한 부분은 많은 검토대상으로 남아 있다. 무선 네트워크 설계 시 제안되어진 기본 설계는 VPN(Virtual Private Networks)이며 해당 노드와 서버간의 통신은 터널링 개념에서 시작된다[4][9].

4. IKEv2 프로토콜을 이용한 IPSec 동작원리

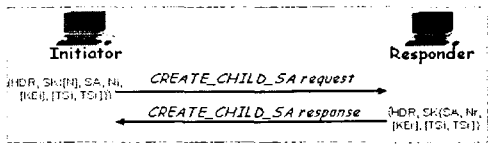
IKEv2 프로토콜은 기존의 IKEv1 프로토콜의 개념을 그대로 계승하면서 기능을 대폭 축약 설계한 것으로 기본 메시지 6개를 4개의 메시지 교환에 의해 통신쌍방의 인증된 보안 채널을 수립하였으며, 인증 방식도 4가지 방식에서 2가지(공개키, 사전공유 비밀키) 방식으로 줄였다. 또한 DoS(Denial of Service) 공격을 막기 위해 응답자로 하여금 쿠키로 응답하게 하여 합법적인 호스트에 대해서만 자원을 할당할 수 있게 한 키 관리 프로토콜이다[5][11].

IKEv2의 ID는 요청과 응답의 쌍으로 구성 되며 응답을 받지 못했을 때 요청 메시지는 재전송하거나 연결을 종료할 수 있다. 동작은 Initial Exchange 과정과 Subsequent Exchange 과정으로 이루어지며, 기본적으로 4개의 메시지 쌍으로 구성된다. Initial Exchange 과정은 IKE_SA_INIT와 IKE_AUTH으로 구성되는데, SA(Security Association) 설정이 끝나면, 상호 인증과 CHILD_SA를 설정한다. [그림 2]는 Initial Exchange 과정을 보여주고 있다[5][11].



[그림 2] Initial Exchange 과정(Phase 1)

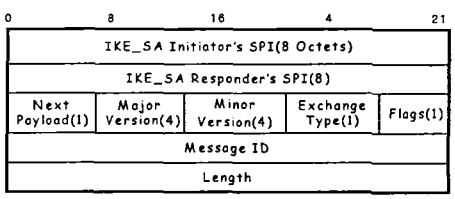
[그림 3]은 Subsequent Exchange 과정을 표현한 것으로 IKEv1의 Phase 2에 해당하는 Subsequent Exchange는 2개의 메시지 쌍으로 구성되며, CREATH_CHILD_SA는 SA를 재설정할 때 사용된다. 이외에 Informational Exchange 과정은 프로토콜 수행 중에 발생한 오류 정보 및 이벤트 탄생 정보 등을 교환할 때 사용된다[5][11].



[그림 3] Subsequent Exchange 과정(Phase 2)

IKE 메시지는 UDP 포트의 500번을 사용하며, UDP 헤더 바로 뒤에 IKE 메시지가 위치한다.

[그림 4]는 IKEv2 헤더의 포맷이다. IKE_SA Initiator's SPI는 SA를 식별하기 위해 선택한 랜덤한 값이며, Responder's SPI는 responder가 SA를 식별하기 위해 선택한 랜덤 값이다. Next Payload 헤더는 다음에 오는 페이로드 타입을 나타내며, Major Version과 Minor Version은 사용된 프로토콜의 버전이다. Exchange Type은 메시지 교환타입을 표시하고, Flags는 메시지에 셋팅된 특별한 선택사항을 표시하며, Message ID 필드는 잃어버린 패킷의 재전송을 제어하고 요청에 대한 응답 메시지의 매칭을 위해 사용된다. Length는 헤더와 이후의 페이로드 전체에 대한 길이이다[5][9][10][11].



[그림 4] IKE 헤더 포맷

Ⅳ. 실험 환경

1. 실험 모델

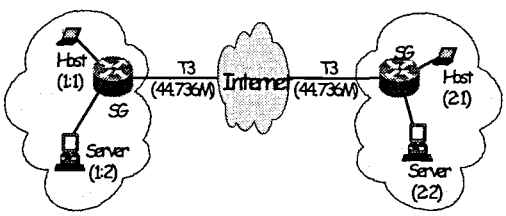
본 논문의 실험환경은 리눅스를 기반으로 구성되어져 있으며 자바를 이용한 시뮬레이션 네트워크인 SSFNET를 이용하였다. 또한 키의 측정치를 위하여 NIST(National Institute of Standards and Technology) 연구소에서 제작한 NIIST(NIST IPSec and IKE Simulation Tool)를 이용하여 키 관리와 교환에 대해 시뮬레이션 하였다. [표 1]은 실험환경 설정 부분이다.

[표 1] 실험 환경

Entity	Version or Sort
Linux Kernel	2.4.20-8
SSFNet	2.0
NIIST	v0.2.0b, v0.3.1b
IPSec Protocol	ESP(3DES)
Bandwidth	T3(44.736M)

IKEv1과 IKEv2는 같은 네트워크 환경에서 시뮬레이션 하였으며, 두개는 SG(Security Gateway) 역할을 하는 라우터를 사이에 두고 인터넷 부분에는 IPSec 패킷이 들어오면 그대로 Forwarding 해주는 역할을 하는 Native 라우터를 두는 네트워크를 구성했다. 두 호스트는 ESP 프로토콜을 사용하였고,, 두 SG간의 Bandwidth는 T3급인 44.736Mbps를 사용하였다.

[그림 5]는 실험 환경을 위해 구축된 가상 네트워크이다.



[그림 5] 네트워크 구성도

2. SSFNet 적용과정

시뮬레이션 과정은 크게 두 가지로 IKEv1을 이용해 전송했을 때와 IKEv2를 이용해 전송했을 때로 나눠진다. Java 기반으로 IPSec과 IKE 알고리즘을 만들고 DML로 이를 불러와 사용하는 형태로, IKEv1의 초기 값 설정은 [그림 6]과 같다.

```
ikeinit [
   timer_interval          2.0
   majorVersion            1
   minorVersion            0
   debug                   true
   trace                   true
   logfile                 "ike.log"
   p1_rekeying_mode        continuous
   global_default [
      rxt_maxcount              4
      rxt_min                 2.0
      rxt_max                64.0
      rtt_default             3.0
      replay                  true
      send_infoEx             true
   ]
```

[그림 6] IKEv1의 초기값 설정 부분

[그림 7]은 IKEv2의 초기 설정 값으로 IKEv1과 다르게 키의 Timeout 시간을 정의해주고 있으며, Router 설정부분에서 IKE Window Size 값을 1로 정의해서 실험했다.

```
ikeinit [
   slow_interval       1.0
   fast_interval       0.2
   majorVersion          1
   minorVersion          0
   debug                 true
   trace                 true
   logfile               "ike.log"
   ]
   dos                   false
   keepalive_timeout     75
   inactivity_timeout    75
]
```

[그림 7] IKEv2의 초기값 설정 부분

시뮬레이션을 실시하면 [그림 8]과 같은 IKE의 키를 초기화하는 과정의 Trace 파일을 볼 수 있다. 이 파일은 각각의 시간에 이루어지는 IPSec 보안전송을 보여준다.

```
@11.27101792: On 0:500,
[ikeSession] push(): Initial exchange: [INIT] Request
Sending Msg#3, src=0.0.0.17, peer=0.0.0.1, IC=-45526226, RC=-51682208
```

[그림 8] IKE.trace 파일의 내부

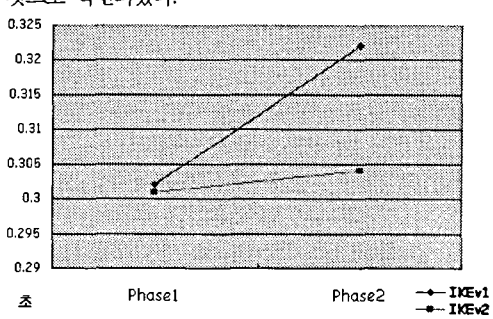
3. 결과 및 분석

[표 2]에서 보듯이 IKEv1rhk IKEv2의 과정으로 나뉘어서 실험을 수행하였고 그중 IPSec의 단계별 전송 지연시간을 살펴보면 Phase 1에서 IKEv1은 IKEv2에 비해 약 0.1초 정도 차이를 보였고, 키 교환(IKE)으로 실험한 경우 약 0.17정도의 지연시간을 확인하였다. 그러나 Phase 2과정에서는 두 개의 키 교환 과정과 전송과정은 큰 차이가 없는 것으로 확인하였다.

		Phase1	Phase2
IKEv1	IPSec	0.406	0.322
	IKE	0.502	0.302
IKEv2	IPSec	0.304	0.304
	IKE	0.333	0.301

[표 2] 시뮬레이션 결과

[표 2]를 [그림 9]의 그래프 형태로 비교 분석해 보면 단계별 시간 차이의 폭이 IKEv2가 훨씬 작은 것으로 확인되었다.



[그림 9] IPSec 보안전송 결과

Ⅳ. 결론 및 향후 과제

본 논문에서는 자바기반의 SSFNet을 이용하여 IKEv1과 IKEv2의 보안 전송의 차이점을 비교 분석하였다. 실험 결과에서 IKEv2의 지연시간이 IKEv1에 비해 짧아 빠른 핸드오프나 재전송시 유리 할 것으로 판단되었으며, 이를 통해 다양한 분야에서의 IPSec의 활용이 가능할 것으로 예상된다. 대표적인 활용분야는 여러 개의 주소를 가지고 이동해야 하는 MIPv6(Mobile Internet Protocol Version 6)라 볼 수 있고, IKEv2를 사용함으로서 위치 정보 유출 및 서비스 거부 등과 같은 공격을 막을 수 있을 것으로 예상된다.

향후 과제로는 SSFNet을 이용해 IKEv2를 모바일 노드에서 시뮬레이션을 수행할 예정이며, 그에 따른 실험 결과를 분석하여 더욱 효율적인 키를 분배과정을 연구할 필요성이 있다. 이를 토대로 무선 네트워크를 지원하는 NS(Network Simulator)-2를 이용, MIPv6노드에서의 IKEv2의 적극적 활용과 다양한 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998

[2] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, 1998

[3] S. Kent, R. Atkinson, "IP Encapsulationf Security Payload", RFC 2406, 1998

[4] Kent, Atkinson, "Security Architecture for IP", RFC 2401, Nov 1998

[5] Charlie Kaufman, "Internet Key Exchange (IKEv2) Protocol", IETF Internet Draft, draft-ietf-ipsec-ikev2-17.txt, September 2004

[6] 윤주범, 박응기, 임을규 "SSFNet을 이용한 네트워크 보안 시뮬레이션에서 동적 시뮬레이션 방법", 한국통신학회, 2004

[7] 윤주범, 임을규, 서정택, 이철원, "네트워크 시뮬레이션을 위한 언어 변환기 설계", 통신정보합동학술대회, 2003

[8] 이철원, 김동규, "네트워크 보안 시뮬레이션을 위한 SSF 설계", 한국정보보호학회, 2002

[9] 김진, 이상원, 최철준, 김광주, "IPSec용 차세대 키 관리 프로토콜의 동향 및 분석", 한국정보보호학회 하계, 2003

[10] 홍기훈, 정수환, 이계상, "IETF IPSEC 관련 그룹 및 MSEC 그룹 표준화 동향", 정보보호학회 춘계, 2004

[11] 최승복, 김해숙, "Specification Of IKEv2", Technical Report, 2003

[12] 박소희, 나재훈, 정교일, "IPv6 SEND 표준화 동향", IITA, 주간기술동향, 2004

[13] SSFNet 홈페이지 http://www.ssfnet.org/

[14] NIIST 홈페이지 http://www.antd.nist.gov/niist/

[15] 한국정보통신기술원, http://www.tta.or.kr/