스토리지 서비스를 위한 IPSec 프로토콜 성능 평가[1)]

황종모° 류준길 박찬익
포항공과대학교 컴퓨터공학과
{koyangee°, lancer, cipark}@postech.ac.kr

Performance Evaluation of IPSec Protocol for Storage Service

Jongmo Hwang° Junkil Ryu Chanik Park
Dept. Computer Science & Engineering, Pohang University of Science and Technology

요 약

최근 급격히 증가하는 정보량으로 인해서 기업체뿐만 아니라 개인들을 위한 스토리지 수요도 폭발적으로 증가하고 있다. 이에 따라 네트워크를 통한 스토리지 서비스 수요도 점차 증가하고 있다. 기업체의 패쇄적인, 파이버 채널을 이용한 SAN은 설치 및 유지비용 등의 문제로 인해서 개인 사용자 및 소규모 사업자들에게 네트워크 스토리지를 위한 가능한 솔루션이 아니다. 이와 관련하여 IP 네트워크를 이용한 네트워크 스토리지가 많이 소개되고 있으나 IP 네트워크를 이용한 네트워크 스토리지는 외부에 의해 데이터가 변조되거나 중요한 데이터가 유출되는 등의 보안상의 문제점을 안고 있다. 이러한 네트워크 스토리지의 보안상 문제점을 해결하기 위한 기술 중 하나가 IPSec 프로토콜이다. IPSec 프로토콜은 IP 계층에서 네트워크를 통해 전송되는 패킷들을 암호화함으로써 안전한 통신을 보장하는 프로토콜이다.

본 논문은 유무선 네트워크 환경에서 IPSec이 지원하는 여러 알고리즘을 이용하여 IPSec의 성능을 측정하고 분석하여, IPSec이 네트워크 스토리지의 보안에 적합한지를 알아본다. 특히 IPSec은 IPv6에서는 필수 기능으로 도입되기 때문에 네트워크 스토리지를 위해서 IPSec의 성능을 평가해보는 것은 의미가 있다고 생각한다.

1. 서론

기업을 포함한 많은 기관들이 스토리지 장치들이 직접적으로 연결되고 애플리케이션 서버에 의해 제어되는 DAS(Direct Attached Storage)에서 컴퓨팅 시스템과 소프트웨어가 LAN을 통해 파일서버 스토리지에 있는 데이터에 접근할 수 있는 네트워크 스토리지로 이행하고 있다. 특히 iSCSI[1]는 IETF에서 개발한 IP에 기초한 스토리지 네트워킹 프로토콜로써 이더넷이 전 세계적으로 구축되어 있기 때문에, 고비용의 복잡한 파이버 채널 SAN 없이도 네트워크 스토리지의 유연한 데이터 관리 성능을 충분히 활용할 수 있다는 장점이 있다. 하지만 iSCSI와 같은 이더넷 기반의 네트워크 스토리지들은 서비스 거부(DoS), 제3자(man-in-middle), 변조(spoofing) 등의 공격을 받을 수 있기 때문에 네트워크를 통한 데이터 전송 시의 보안이 매우 중요한 관건이다. 2004년도에 발표된 CSI/FBI 보고서[2]에 따르면 네트워크 보안을 위해 데이터 전송 시에 데이터를 암호화하는 보안 기술을 사용하고 있다고 대답한 응답자가 전체의 64%를 차지하였다. 이러한 보안 기술 중 하나가 IPSec(IP Security) 프로토콜인데, IPSec 프로토콜(이하 IPSec)은 IP 계층의 보안 프로토콜로써 전송되는 패킷을 암호화하여 IP 및 상위 계층(TCP, UDP, ICMP 등)의 보안을 제공한다.

본 논문에서는 다양한 네트워크 환경에서 IPSec에서 제공하는 여러 가지 알고리즘을 이용해 IPSec의 성능을 평가하고 분석함으로써 IPSec이 네트워크 스토리지 환경에서 적용가능한지를 평가해보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 IPSec에 대해 설명, 3장에서는 IPSec 성능 테스트를 위한 실험환경을 기술, 4장에서는 실험 결과 및 분석, 5장에서는 관련연구에 대해 설명을 하고 6장에서는 결론을 내린다.

2. IPSec

IPSec은 IP계층에서 데이터 보호 서비스를 제공하기 위한 프로토콜로서 다음과 같은 특징을 가지고 있다.

- 기밀성 : 데이터를 암호화하여 정보의 기밀성 유지
- 무결성 : MD5/SHA1과 같은 해시 알고리즘을 이용해 정보가 변조되지 않았음을 입증
- 인증 : 개인 또는 어플리케이션에 대한 신분 입증
- 재전송 방지 : 한 번만 수행되어야 하는 트랜잭션이 여러 번 반복 수행되는 것을 방지

IPSec의 구조는 기능적으로 아래와 같이 구분된다.

- 보안 프로토콜
  - AH : 인증 알고리즘을 이용하여 IP 데이터그램의 무결성, 인증 서비스 및 재전송 방지 기능을 제공한다. [3]
  - ESP : 암호화 알고리즘을 이용하여 IP 데이터그램에 대한 기밀성, 무결성, 인증 서비스 및 재전송 방지 기능을 제공한다. [4]
- SA (Security Association) : 데이터 송수신자간에 사전에 사용할 암호 알고리즘, 키 교환 방법, 키 교환 주기 등에 대한 합의를 담당한다.
- Internet Key Exchange (IKE) : 두 종단간의 신뢰성 있는 암호화 키 교환을 담당한다. [5]

IPSec의 동작모드로는 트랜스포트 모드와 터널 모드가 있고, 그림 1에서 알 수 있듯이 트랜스포트 모드에서는 데이터만을 암호화하며, 터널 모드에서는 헤더와 데이터 모두를 암호화하여 송신한다.

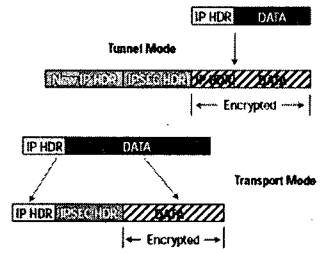

그림 1. IPSec 트랜스포트 모드와 터널 모드

1) 본 연구는 한국과학재단 특정 기초연구과제의 지원을 받아 수행하였음.

IPSec을 구현한 공개 프로젝트로는 Linux IPv4 상에서 IPSec을 구현한 FreeS/WAN, FreeBSD와 NetBSD 상에서 IPv6과 IPSec을 구현한 KAME, 4.4BSD-Lite 상에서 IPv6와 IPSec을 구현한 NRL 등이 있으며, OpenBSD는 자체적으로 IPSec을 제공하고 있다.

IPSec은 IP 기반의 모든 응용에 공통 보안 서비스를 제공할 수 있는 장점이 있는 반면, 커널 수준에서 구현되어야 하고 네트워크 성능을 저하시키는 단점이 있다. IPSec은 IPv4에서는 선택사항으로 구현되지만, IPv6에서는 필수기능으로 권고하고 있으며, 확장 헤더에 IPSec에서 사용되는 AH와 ESP 헤더를 기본적으로 포함하고 있기 때문에 IPv6가 대중화되기 전에 IPSec의 성능 개선이 선행되어야 할 것이다.

3. 실험 환경

IPSec 성능을 평가하기 위해 두 대의 머신이 아래와 같은 환경으로 구성되어 있다.

- CPU : Pentium 4 2.80GHz
- Memory : 512 MB
- OS : RedHat 9 (리눅스 커널 2.4.20-8)
- IPSec : Super FreeS/WAN 1.99.8 [6]
- Network benchmark : iperf 1.7.0 [7]

Super FreeS/WAN은 IPsec을 위해 사용할 수 있는 AES, BLOWFISH 등의 암호화 알고리즘과 X.509 디지털 인증 등과 같이 FreeS/WAN에서 지원하지 않는 기능들을 제공하기 위해 FreeS/WAN을 패치한 버전이다. 추가된 알고리즘들은 모듈로 제공이 된다.

iperf는 클라이언트/서버 환경의 프로그램으로써, iperf 클라이언트에서 IP 패킷을 일정량 생산하여 상대편 iperf 서버로 전송한 후 전송된 패킷의 양과 전송이 완료된 시간을 이용하여 네트워크 성능을 측정하는 툴이다.

IPSec 성능 평가는 1000Mbps, 100Mbps, 그리고 무선 네트워크 상에서 이루어졌으며, 무선 네트워크 환경은 그림 2에서 보는바와 같이 Intel 2011B Access point를 통해 802.11b 통신을 하도록 구성하였다.

그림 2. IPSec 테스트를 위한 무선 네트워크 환경

두 대의 머신은 ESP 터널모드로 구성이 되어 있으며, IKE는 3DES-MD5 알고리즘을 사용하였다. ESP는 암호 알고리즘으로는 3DES, AES, BLOWFISH를, 인증 알고리즘으로는 MD5, SHA1을 사용하여 성능을 비교하였다.

4. 실험 결과

4.1. iSCSI 상에서의 IPSec 성능

표 1은 1000 Mbps 환경에서 IPSec을 구동시켰을 때의 iSCSI 성능을 나타내고 있다. 실험에서 사용한 디스크 I/O 벤치마크 툴은 본 연구실에서 개발한 iogen을 사용하였다. iogen은 SCSI generic 인터페이스를 사용하여 디스크 I/O 명령을 발생, 디스크 성능을 측정하는 툴이다. WRITE 명령어, READ 명령어, 그리고 READ/WRITE 명령어를 1:1의 비율로 보냈을 때의 성능을 각각 측정하였으며, 3DES-MD5 알고리즘에 대해서만 측정을 하였다.

- const : 특정 블록에서만 READ 또는 WRITE 수행
- seq : 순차적으로 READ 또는 WRITE 수행
- MBPS : 네트워크 성능 (MegaByte per sec)
- IOPS : I/O 성능 (Input Output per sec)
- RT (Response Time) : 반응 시간

표 1. iSCSI 상에서의 IPSec 성능

패턴		Without IPSec			With IPSec		
		MBPS	IOPS	RT (msec)	MBPS	IOPS	RT (msec)
WRITE	const	54.49	217.96	58.11	5.22	20.86	708.47
WRITE	seq	28.04	112.16	123.48	5.13	20.53	721.01
READ	const	47.7	190.8	68.34	5.08	20.32	725.75
READ	seq	19.2	76.78	184.89	5.08	20.33	724.51
R/W	const	48.77	195.1	66.32	5.15	20.59	718.33

실험 결과에서 알 수 있듯이, iSCSI 상에서의 IPSec 성능이 최악의 경우 10%도 못 미치는 것을 알 수 있다.

IPSec의 성능이 저조한 이유를 좀 더 자세히 분석하기 위해 IPSec만의 성능을 1000 Mbps, 100 Mbps, 무선 네트워크 환경에서 IPSec에서 지원하는 여러 알고리즘을 이용해 테스트해 보았다 (성능 측정은 iperf를 사용함).

4.2. 1000 Mbps IPSec 성능

표 2는 1000 Mbps 네트워크상에서의 IPSec 성능을 나타내고 있다. 표 2에서 알 수 있듯이 네트워크 대역폭이 충분해 IPSec 성능이 CPU 성능 및 알고리즘에 큰 영향을 받는다. 모든 알고리즘의 CPU 점유율이 99% 이상 것도 이러한 이유 때문이다. 네트워크 대역폭이 충분하고 동일한 CPU에서 수행되기 때문에 알고리즘에 따른 성능도 크게 차이가 난다. SHA1보다는 MD5 해쉬 알고리즘이 더 좋은 성능을 나타내고, 암호화 알고리즘의 경우 AES, BLOWFISH, 3DES의 순으로 성능이 좋게 나타났다.

표 2. 1000 Mbps IPSec 성능

알고리즘	네트워크 성능 (Mbps)	평균 CPU 점유율 (%)
IPSec 사용 안 함	774	36.7
3DES-MD5	96	99.8
3DES-SHA1	86	99.9
AES-MD5	282	99.6
AES-SHA1	196	99.6
BLOWFISH-MD5	233	99.7
BLOWFISH-SHA1	163	99.5

4.3. 100 Mbps IPSec 성능

표 3은 100 Mbps 네트워크상에서의 IPSec 성능을 나타내고 있다. CPU 점유율은 1000 Mbps 환경에 비해 훨씬 감소했는데, 3DES-SHA1이 99.8%로 가장 높았고, AES-MD5가 37.4%로 가장 낮았다. 이는 네트워크 대역폭이 낮아지면서 네트워크에 병목현상이 생겨 IPSec 처리율 또한 낮아졌기 때문으로 해석할 수 있다. 3DES 알고리즘을 대체할 암호화 알고리즘이라고 일컬어지는 AES는 CPU 점유율로 보았을 때 3DES의 37% 수준으로, 3DES에 비해서 성능이 훨씬 좋은 것을 알 수 있다.

표 3. 100 Mbps IPSec 성능

알고리즘	네트워크 성능 (Mbps)	평균 CPU 점유율 (%)
IPSec 사용 안 함	94.1	9.7
3DES-MD5	73.7	94.2
3DES-SHA1	85.1	99.8
AES-MD5	89.6	37.4
AES-SHA1	89.5	50.5
BLOWFISH-MD5	90.6	44.2
BLOWFISH-SHA1	90.6	57.5

4.4. 무선 네트워크 IPSec 성능

표 4는 무선 네트워크상에서의 IPSec 성능을 나타내고 있다. 무선 네트워크 환경에서는 네트워크 대역폭이 5.28Mbps로 매우 낮기 때문에, IPSec 성능이 CPU 보다는 네트워크에 큰 영향을 받는다. 따라서 어떤 알고리즘을 사용하든 네트워크 성능 및 평균 CPU 점유율은 크게 차이가 나지 않고, 대부분이 IPSec을 사용하지 않았을 때와 비슷한 성능을 보이고 있다. 네트워크에 병목현상이 발생하기 때문에 CPU 점유율 또한 매우 낮은 것을 볼 수 있다.

여기서 알 수 있는 것 중 하나는 현재 사용되고 있는 무선 환경에서 VPN을 위해서 IPSec을 이용하는 것이 가능한 솔루션이라는 점이다.

표 1. 무선 네트워크 IPSec 성능

알고리즘	네트워크 성능 (Mbps)	평균 CPU 점유율 (%)
IPSec 사용 안 함	5.28	1.0
3DES-MD5	4.69	6.6
3DES-SHA1	4.99	6.7
AES-MD5	5.11	3.5
AES-SHA1	4.87	3.3
BLOWFISH-MD5	4.89	3.5
BLOWFISH-SHA1	5.03	3.7

그림 3은 위 실험 결과들을 그래프로 나타낸 것이다.

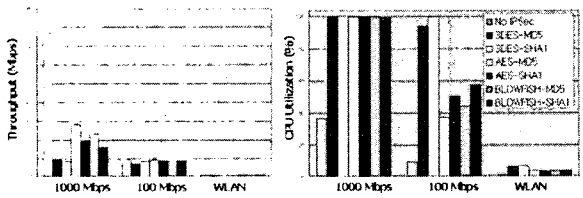

그림 3. IPSec 네트워크 성능(좌), IPSec CPU 점유율(우)

실험 결과에서 알 수 있듯이, 네트워크 대역폭이 높을수록 IPSec의 성능은 CPU 성능 및 알고리즘의 성능에 큰 영향을 받게 된다. 현재 IPSec에서 지원하는 알고리즘 중 AES의 성능이 가장 좋은데, iSCSI 상에서 IPSec 성능을 테스트한 3DES-MD5 보다 약 2.5배 성능이 향상되었다. 즉, iSCSI 상에서 AES 알고리즘을 선택하면 최고 13 MBPS 정도의 성능을 보일 수 있는데, 이는 네트워크 스토리지에 적용할 여지가 있음을 보여준다.

특히 암호화 키 사이즈로 보았을 때, 현재 안전한 암호 알고리즘은 80bit 정도이며 무어의 법칙을 적용했을 때 18개월에 1bit씩 증가하는 것을 감안하면 AES는 128bit로써 향후 20 ~ 30년은 안전하게 사용할 수 있기 때문에[8] IPSec의 성능을 보완해주며 안전하게 적용할 수 있는 알고리즘이라 할 수 있다.

하지만, 비록 1000 Mbps 환경에서의 네트워크 성능이 무선 네트워크나 100 Mbps 환경에서의 네트워크 성능보다 훨씬 좋지만, IPSec을 사용하지 않았을 때와 비교하면 IPSec이 성능면에서 많은 문제점이 있다는 것을 알 수 있다. 즉, 무선 네트워크나 100 Mbps 환경에서는 IPSec을 사용하지 않았을 때와 비교했을 때 88%~96%의 성능을 나타냈지만, 1000 Mbps 환경에서는 11%~36%의 상대적으로 나쁜 성능을 보이고 있다.

5. 관련 연구

5.1. SSL (Secure Socket Layer)

SSL[9]은 넷스케이프사가 개발한 프로토콜로써, IP 계층에서 작동하는 IPSec과는 달리, 응용 프로토콜(HTTP, Telnet, NNTP, FTP등)과 전송 프로토콜(TCP/IP등) 사이에서 정보보호를 제공한다. SSL은 종단간 보안을 구현하는데 적합하며, IPSec에서 제공하는 기밀성, 무결성, 인증 서비스 및 재전송 방지 기능을 모두 제공하여 IPSec과 함께 가장 널리 쓰이는 보안 프로토콜 중 하나이다.

SSL은 IPSec에 비해 사용하기가 쉽고, 성능이 더 좋은 장점이 있다. 하지만, IPSec은 IP를 사용하는 애플리케이션이라면 소스 코드의 변화 없이 사용 가능하지만 SSL을 사용하기 위해서는 애플리케이션이 SSL을 지원하도록 구현되어야 한다. 또한 SSL은 UDP를 지원하지 않기 때문에 보안성 면에서는 IPSec보다 떨어진다.

5.2. 보안 가속기

보안 프로토콜의 성능을 개선하기 위해 커널 또는 애플리케이션에서 담당하던 보안 프로토콜의 처리를 하드웨어에서 처리해주는 보안 가속기(Security Accelerator)가 Motorola, Hifn, Broadcom, Cavium, Securealink 등의 회사에서 개발되어 상용화되었다. 보안 가속기는 하드웨어 내부적으로 암호화, 인증 등의 처리를 수행하며, IPSec을 지원한다.

5.3. Fast IPSec

"Fast IPSec"[10]은 IPSec의 성능을 향상시키기 위한 목적으로 IPSec 처리 시 보안 가속기를 사용할 수 있도록 KAME IPSec을 보완한 프로토콜로써 FreeBSD용으로 구현되어 있다. "Fast IPSec"의 성능은 Pentium 4 2.53 GHz 머신에서 3DES-SHA1 알고리즘을 이용했을 때 최대 218 Mbps가 나왔는데, 이는 본 논문에서 실험한 결과의 약 2.5배 성능이다.

리눅스의 경우, IPSec 성능 향상을 목적으로 커널 버전 2.5.47 이후부터는 KAME/*BSD 모델을 새로운 IP 스택으로 도입하였다. 하지만 "Fast IPSec" 프로토콜이 구현되어 있지는 않다.

6. 결론

본 논문에서는 IPSec의 성능을 측정하여 IPSec이 네트워크 스토리지에 적용 가능한지에 대해 분석해보았다. IPSec은 기가비트 이더넷 환경에서는 네트워크 대역폭에 훨씬 못 미치는 성능을 보이며, CPU 성능과 인증/암호 알고리즘에 큰 영향을 받는다. 하지만, AES와 같이 다른 암호 알고리즘에 비해 성능이 뛰어난 알고리즘과 향후 과제로 상고 있는 보안 가속기를 이용한 고성능 IPSec 처리 시스템을 적용한다면 충분히 네트워크 스토리지에 적용할 수 있을 것이다.

참고 문헌

[1] Julian Satran, Kalman Meth, Costa Sapuntzakis, Mallikarjun Chadalapaka, Efri Zeidner, "iSCSI draft"

[2] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, "2004 CSI/FBI Computer Crime and Security Survey"

[3] S. Kent, R. Atkinson, "IP Authentication Header(AH)

[4] S. Kent, R. Atkinson, "IP Encapsulating Security Payload(ESP)"

[5] D. Harkins, D. Carrel, "The Internet Key Exchange(IKE)"

[6] http://www.freeswan.ca/

[7] http://dast.nlanr.net/Projects/Iperf/

[8] Albert Levi, "Overview of Cryptography", http://people.sabanciuniv.edu/levi/

[9] Alan O. Freier, Philip Karlton and Paul C. Kocher, "The SSL Protocol"

[10] Samuel J. Leffler, "Fast IPSec: A High-Performance IPSec Implementation", USENIX Proceedings of BSDCon'03