IPSec과 SSL의 성능평가를 위한 분석※

박유라*, 이경배*, 이혜민*, 이광우**, 이근우**, 김승주*, 원동호*
*성균관대학교 정보통신공학부
**성균관대학교 대학원 컴퓨터공학과
e-mail : yuraloen@nate.com

Analysis for Performance Evaluation of IPSec and SSL

Yura Park*, Kyungbae Lee*, Hyemin Lee*,
Kwangwoo Lee**, Keunwoo Rhee**, Seungjoo Kim*, Dongho Won*
*School of information & Communication Engineering,
Sungkyunkwan University
**Dept. of Computer Engineering, Graduate School,
Sungkyunkwan University

요 약

인터넷의 발달은 우리 생활에 많은 변화를 가져왔다. 이제는 단순한 통신뿐만 아니라 금융, 경제 분야에 이르기까지 다양한 범위의 활동들이 네트워크에서 이루어지고 있으며 그에 따라 정보보호의 중요성도 증가했다. 네트워크 상에서의 정보보호를 위해 현재 대표적으로 VPN 시장에서는 IPSec 기반의 VPN과 SSL 기반의 VPN이 경쟁을 하고 있다. 이에 본 논문에서는 IPSec과 SSL 프로토콜의 성능을 비교하고 다양한 관점에서 성능을 평가한 사례들을 분석한다. 그리고 이를 통해 IPSec과 SSL 프로토콜의 대한 성능평가 도구의 연구 필요성을 제시한다.

Ⅰ. 서 론

정보통신 기술의 발달로 인터넷이 급속히 보급되었다. 인터넷을 통한 정보의 접근 및 공유 범위가 넓어지면서 해킹, 바이러스, 개인정보 유출 등의 피해가 급증하여 이러한 문제들을 방지하고 통제하기 위한 네트워크 보안의 중요성이 함께 증가되고 있다.

네트워크 환경에서 정보를 보호하기 위해서는 사용자 인증(user authentication), 데이터 무결성(data integrity) 및 기밀성(confidentiality)을 보장해야 한다. 현재까지 네트워크 보안을 위한 다양한 프로토콜과 도구들이 개발되었다.

본 논문에서는 네트워크 보안을 위한 다양한 프로토콜 중에서 현재 널리 연구되고 있는 IPSec과 SSL 프로토콜을 분석하고 이들의 특성을 비교한다. 그리고 IPSec과 SSL의 성능평가 사례들을 분석하여 앞으로의 연구 방향을 제시하고자 한다. 2장에서는 IPSec과 SSL 프로토콜에 대해 설명하고, 3장에서는 IPSec과 SSL의 특성을 비교하고 성능을 평가한 내용을 분석하여 4장에서 결론을 도출한다.

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음

Ⅱ. IPSec 과 SSL

1. IPSec

1995년에 등장한 IPsec(IP Security)은 IETF의 IPSec Working Group에 의해 정의된 프로토콜로서 응용 계층과는 무관하게 IP 계층에서 보안 서비스를 제공하기 위한 프로토콜이다.

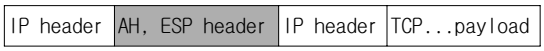
가. IPSec 보안 프로토콜과 알고리즘

AH(Authentication Header) 프로토콜은 패킷의 무결성 서비스와 송신자 인증서비스를 제공하고, ESP(Encapsulating Security Payload)는 무결성 및 인증서비스 외에 기밀성 서비스를 추가로 제공한다.

나. IPSec의 동작 모드

AH 프로토콜과 ESP 프로토콜은 헤더의 위치에 따라 두 가지 모드로 나눠진다.

(a) 전송 모드



(b) 터널 모드

(그림 1)

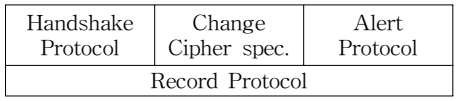
전송 모드는 종단 대 종단에 위치한 두 호스트 간에 이용되며 IP 패킷의 페이로드, 즉 TCP와 UDP 같은 상위계층 프로토콜 데이터만을 보호하게 된다. 이 경우 패킷 헤더는 보호 영역 밖이므로 송신자와 수신자 주소가 노출되어 트래픽 흐름이 노출될 수 있다. 하지만 터널 모드의 경우는 패킷의 전체가 보호 영역 안에 놓이므로 트래픽 흐름의 기밀성도 유지할 수 있게 된다. 보안 통신의 한 쪽이 호스트가 아닌 라우터인 경우는 반드시 터널 모드를 적용해야 한다. 터널 모드는 호스트와 호스트 사이에도 적용할 수 있다[1].

2. SSL

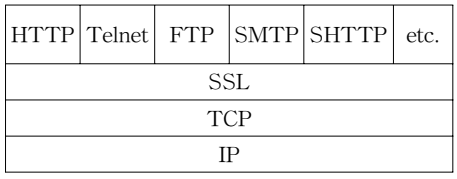
SSL은 네트워크 내에서 메시지 전송의 안전을 보장하기 위해 넷스케이프사에 의해 만들어진 프로토콜이다. 현재 많은 브라우저 프로그램들이 SSL을 지원하고 있다.

가. SSL 구조

SSL은 전송계층과 응용계층 사이에 위치하며, 그 구조와 위치는 다음과 같다.

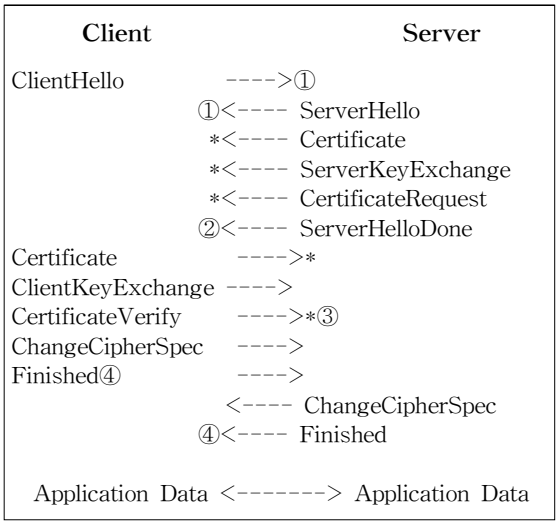


(그림 2) SSL의 구조



(그림 3) SSL의 위치

나. SSL 동작



* : Option

(그림 4) SSL 동작 과정

① 프로토콜 버전, 세션 ID, Cipher suite, 압축 method 등의 보안 파라미터를 협상하고 random값을 교환한다.

② 선택적으로 서버의 인증서를 전송하고 클라이언트의 인증서를 요청한다. Handshake에서 생성된 모든 데이터를 사용하여 클라이언트는 세션을 위한 premaster secret을 생성하고 이를 서버의 공개키를 사용하여 암호화하여 서버에게 전송한다.

③ 서버가 인증서를 요청하면 클라이언트의 인증서를 응답으로 전송한다. 클라이언트와 서버는 master secret을 사용하여 세션동안에 교환될 정보의 암호화와 복호화 및 무결성에 사용될 대칭키인 세션키를 생성한다.

④ 앞으로 교환할 데이터는 세션키에 의해 암호화 될 것이라는 메시지를 주고받는다. Change cipher suite과 finish 메시지 교환으로 handshake 과정을 마친다. handshake가 종료되면 클라이언트와 서버는 세션키를 사용하여 데이터를 암호화·복호화 및 송·수신 하며 데이터의 무결성을 검사한다[2].

Ⅲ. IPSec과 SSL 성능평가 사례 분석

본 장에서는 2장에서 살펴본 IPSec과 SSL 프로토콜을 기반으로 내용상의 비교표를 작성한다. 그리고 이 두 프로토콜의 성능을 여러 가지 관점에서 평가한 사례들을 분석한다.

1. IPSec과 SSL의 특성 분석

IPSec과 SSL 프로토콜의 내용을 통해 두 프로토콜의 구별되는 특성을 찾을 수 있다. IPSec은 소켓 기반의 보안인 SSL과 달리 IP계층에서 암호와와 인증을 수행하기 때문에 응용프로그램에 대해 투명하다. 따라서 IPSec은 SSL에 비해 방화벽과 무선 네트워크에 유리하다. 그러나 SSL이 IPSec보다 더 긴 HMAC을 사용하기 때문에 무결성 측면에서 더욱 강하다. 또한 원격 접근시 IPSec은 서버와 사전 키 공유를 한 별도의 클라이언트용 소프트웨어가 필요하지만 SSL 프로토콜은 웹브라우저에 기본적으로 탑재되어 있어 그 사용이 편리하다. 이러한 특성들을 <표 1>에 정리했다.

<표 1> IPSec과 SSL 비교

Function	IPSec	SSL
Configuration	어려움	쉬움
Client Authentication	필수	선택
Pre-Shared Key	있음	없음
Interoperability Problem	있음	없음
TCP Application Support	전체	일부
Throughput Rate	높음	높음
Handshake Time	느림	빠름

2. 전송 속도(Transfer speed) 비교

동일 환경에서 IPSec과 SSL이 사용하는 압축 알고리즘(compression algorithm)들의 전송 속도(transfer speed)를 100Mbps 네트워크와 1000Mbps 네트워크의 조건에서 평가한 사례를 비교한다[3]. IPSec에서는 압축 프로토콜인 IPComp[4]를 통해 압축 기능을 사용할 수 있으며, SSL에서는 SSL Record Protocol[5][6]을 통해 압축 기능을 사용할 수 있다.

가. IPSec

IPSec의 각 압축 알고리즘에서의 전송 속도 테스트 결과는 <표 2>과 같다.

<표 2> IPSec의 압축 알고리즘에 따른 전송 속도

압축 알고리즘	시간(Sec)
No Algorithm	2
3DES-SHA-1	12
3DES-MD5	10.5
3DES-SHA-1-DEFLATE	8.4
3DES-MD5-DEFLATE	7.8
AES-128-SHA-1	5.7
AES-128-SHA-1	4.5

나. SSL

SSL의 각 압축 알고리즘에서의 전송 속도 테스트 결과는 <표 3>와 같다.

<표 3> SSL의 압축 알고리즘에 따른 전송 속도

압축 알고리즘	시간(Sec)
No Akgorithm	2
3DES-EDE-CBC-SHA	9.8
DES-CBC-SHA	5.5
RC4-128-SHA	3.8
RC4-128-MD5	3.4
EXP-RC2-CBC-MD5	3.9

SSL은 RC4-128-MD5를 사용한 경우 가장 빠른 처리속도를 보였으며, 같은 환경 하에서 3DES 사용시 <표 2>와 같이 IPSec보다 더 나은 성능을 보여줬다.

3. 프로세서와 메모리 사용도 비교

프로세서와 메모리의 사용도를 비교하기 위해

① 프로토콜 미사용(No security)
② IPSec without offload
③ IPSec with offload
④ SSL

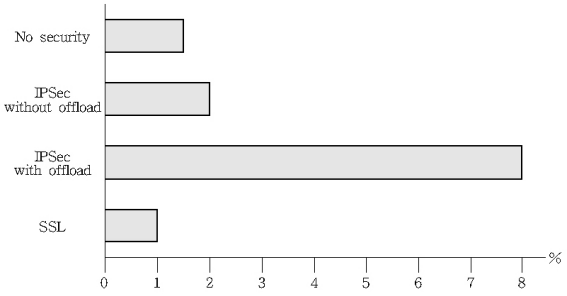
의 4가지 조건 하에서

ⓐ CPU 사용률
ⓑ 프로세서 큐 길이
ⓒ 초당 사용된 메모리 페이지

의 3가지 항목을 비교한 결과를 분석한다[7][8].

가. CPU 사용률

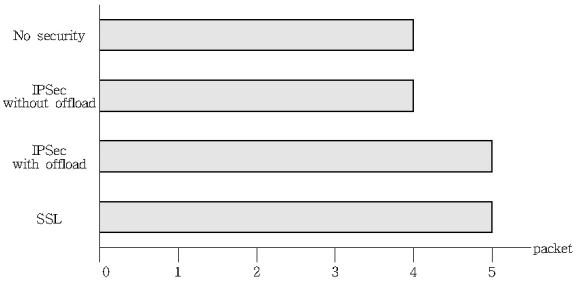
CPU 사용률의 측정 결과값은 (그림 5)에서와 같이 SSL이 가장 낮은 것으로 나타났다. offload를 사용하지 않은 IPSec은 프로토콜 미사용 상태와 비슷한 값을 보였으며, offload를 사용한 IPSec의 측정값은 다른 경우의 4배가 넘는 값을 나타냈다. 이를 통해 CPU 사용률의 측면에서는 IPSec보다 상위 계층의 프로토콜인 SSL이 효율적임을 알 수 있다.



(그림 5) CPU 사용률

나. 프로세서 큐 길이

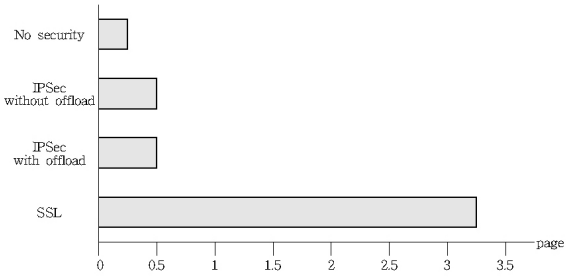
프로세서 큐 길이는 프로세서 대기 열에 있는 thread 수를 의미한다. (그림 6)에서 알 수 있듯이 모든 경우가 비슷한 값을 보였으며, offload를 사용한 IPSec과 SSL이 다른 경우보다 더 높은 값을 가지는 것을 알 수 있다.



(그림 6) 프로세서 큐 길이

다. 초당 사용된 메모리 페이지

초당 사용된 메모리 페이지는 시스템에 의해 디스크에서 읽거나 디스크로 쓴 메모리 페이지의 초당 평균값이다. 메모리 페이지는 (그림 7)처럼 SSL이 가장 많은 양을 사용하는 것을 알 수 있으며, IPSec 프로토콜의 메모리 페이지 사용량은 offload 여부에 관계없는 값을 보였다.



(그림 7) 초당 사용된 메모리 페이지

전체적으로 IPSec이나 SSL 프로토콜을 사용하는 것이 사용하지 않은 것 보다 메모리 페이지를 많이 사용함을 알 수 있다.

Ⅳ. 결 론

본 논문은 네트워크 보안 분야에서 사용빈도가 높은 IPSec과 SSL의 특성을 분석하고 여러 관점에서 실시한 성능평가 결과를 비교했다. 이를 통해 IPSec과 SSL의 장·단점이 환경 조건에 따라 다름을 확인했다. 그러므로 다양한 네트워크 환경에 적합한 프로토콜을 선택할 수 있도록 복합적이고 신뢰할 수 있는 성능평가 도구에 대한 연구가 이루어져야 한다.

참고문헌

[1] 이계상, “IPsec 표준화동향”, 동의대학교, 2000년

[2] 김소진, 신성환, 박지환, “SSL/TLS와 WTLS 의 프로토콜 취약성 분석”, 한국멀티미디어학회지 제5권 제3호, 2001년 9월, pp. 75～76

[3] AbdelNasir Alshamsi, Takamichi Saito, “A Technical Comparison of IPSec and SSL”, 9th International Conference on Advanced Information Networking and Application (AINA '05) Volume2, pp. 8～10

[4] A. Shacham, B. Monsour, R. Pereira. M. Thomas, “IP Payload Compression Protocol (IPCOMP)”, RFC 2393, Dec. 1998.

[5] William Stallings, “Cryptography and Network Security, Principles and Practices” 3rd Edition, International Edition, Prentice Hall

[6] William Stallings, “Network Security Essentials, Applications and Standards” 2nd Edition, Prentice Hall

[7] Jalal Raissi, “.NET Security : IPSec vs. SSL”, Proceedings of the IEEE SoutheastCon 2004 in Greenboro, pp. 8～9

[8] Jalal Raissi, “IPSec Offload Performance”, Proceedings of the IEEE SoutheastCon 2004 in Greenboro, p. 5