IPSec 및 ISAKMP 프로토콜 분석 도구 설계 및 구현

현정식 이태희 이석희 조 상

청주대학교 전자계산학과

Design and Implementation of IPSec and ISKAMP Protocol Analyzer

Jeung-Sik Hyun[0] Tae-Hee Lee Seok-Hee Lee Sang Cho
Dept. of Computer Science, Chongju University

요 약

IPSec은 IETF에 의해 IP 레이어 보안을 위한 개방형 구조로 설계된 것으로 인터넷에서의 정보 보호를 대표한다. 그리고 ISKMP는 인터넷에서 요구되는 정보보호를 설정하기 위한 인증, 키 관리 및 보안협상등을 담당하는 프로토콜로써 IPSec으로 보다 체계화된 인터넷 정보보호를 제공하기 위해 포함되어야 하는 IKE에서 사용하는 프로토콜이다. 이러한 IPSec을 이용한 보안 시스템을 개발하기 위해서는 시스템에서 사용하고 있는 프로토콜들에 대한 평가 방법도 같이 제시되어야 하나, 기존의 프로토콜 분석 도구들은 IPSec에서 제공하고 있는 프로토콜들을 분석 있지 못할 뿐만 아니라, 개발단계에서의 구현 평가를 하지 못한다. 본 논문에서는 IPSec을 구현하는데 필요한 AH 및 ESP 프로토콜과 ISAKMP 프로토콜을 실시간으로 분석하고, 이들 프로토콜들이 얼마나 잘 구현되었는지를 평가할 수 있는 프로토콜 분석 도구를 설계하고 구현하였다.

1. 서론

최근 인터넷과 WWW(World Wide Web)의 이용이 폭발적으로 증가하면서 인터넷 정보보호 프로토콜에 대한 많은 연구가 진행되어 왔다. 그 중 가장 대표적인 IPSec은 IP 레이어 레벨의 보안 서비스를 제공하므로 기존의 보안 프로토콜보다 다양한 응용 프로그램에 적용될 수 있다는 장점을 가지고 있다. 현재 IPSec 아키텍처는 RFC2401을 비롯한 18개의 RFC로 작성되어 있으며, AH(Authentication Header)와 ESP (Encapsulation Security Payload)의 두 가지 확장헤더와 IKE(internet Key Exchange)를 정의하고 있다. 현재 AH, ESP와 IKE는 대부분의 플랫폼에서 프로토타입으로 구현되었고 WINDOWS 2000에서도 구현되었으나 아직 완전하다고 볼 수 없다 [1].

IPSec을 이용한 보안 시스템이 얼마나 잘 구현되었는지 평가할 수 있는 방법은 시스템에서 사용하는 프로토콜을 분석함으로써 알 수 있다. 프로토콜 분석은 각 프로토콜이 교환하는 패킷들을 캡처하여 분석하고, RFC에서 제시된 사항과 얼마나 일치하는지 판단할 수 있어야 하며, 특정 패킷에 대한 응답이 적절한지를 종합적으로 평가할 수 있어야 한다.

2. 프로토콜 분석 도구의 설계

네트워크상의 프로토콜을 분석할 수 있는 도구로는 tcpdump, snoop, sniffer등이 있으나 이들은 아직 IPSec에서 사용하고 있는 프로토콜들을 지원하고 있지 않으며, 단순한 네트워크 모니터링 기능을 수행할 뿐 프로토콜에 대해 전반적인 평가는 불가능하다.

그림1은 프로토콜 분석도구의 시스템 형상을 나타낸 것이다. 우선 네트워크 상의 패킷들을 tcpdump에서 사용하고 있는 것과 같은

libpcap[2]에 의해 캡쳐하고, 캡쳐한 패킷들을 프로토콜 별로 나누어 화면에 출력한다.

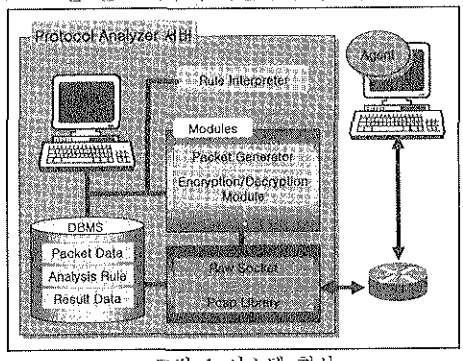

그림 1 시스템 형상

그리고 캡쳐된 패킷을 데이터베이스에 저장하고 저장된 패킷을 읽어 프로토콜 분석규칙에 의해 분석한다. 분석결과로 규칙수행 로그를 저장하고 차후에 새로운 분석결과와 비교할 수 있게 한다.

이 시스템은 IPSec에서 사용하는 AH[3], ESP[4], ISAKMP[5-6] 프로토콜도 모니터링할 수 있을 뿐만 아니라 기존의 프로토콜도 모니터링 할 수 있다. 그리고 IPSec이 제공하고 있는 정보보호 서비스에 대해 사용자가 정의한 분석규칙으로 프로토콜을 분석하고 시험할 수 있다. 그리고 프로토콜 분석시 필요한 기능들은 모듈단위로 등록하여 손쉽게 사용 할 수 있다. 프로토콜 분석에 필요한 부가적인 기능으로, 사용자가 프로토콜 분석 및 시험에 필요한 패킷을 프로토콜별로 만들 수 있고, 만들어진 패킷을 Raw Socket[2]을 통해 네트워크로 전송할 수 있다. 패킷을 송수신하는 기능은 모듈로써 등록되어 있는 기본 기능이다.

마지막으로 원거리의 시스템들은 에이전트를 이용하여 패킷을 수집하고, 평가할 있으며, 에이전트가 설치된 다수의 시스템을 순차적으로 평가 할 수도 있다.

3. 프로토콜 분석도구의 구현

IPSec 및 ISAKMP 프로토콜 분석 도구의 구현 환경은 다음과 같다.

- OS : Solaris 7 (Sun Ultra Sparc)
- GUI : Java
- DBMS : MySQL

그 외에 libpcap을 사용하여 패킷을 캡쳐하고, Raw Socket을 사용하여 패킷을 전송하는 모듈은 C언어로 작성하였다.

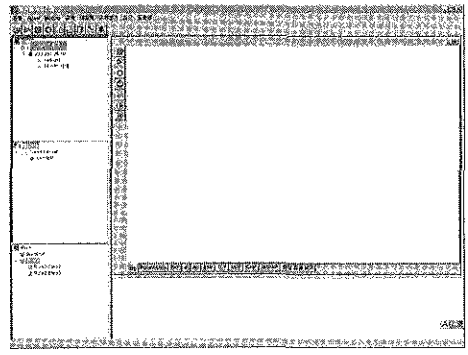

그림 2 메인화면

그림2는 프로토콜 분석도구의 메인화면을 나타낸 것으로 에이전트 설치현황과 모듈 및 분석규칙 등록현황을 한눈에 볼 수 있다. 각 사항에 대해서는 추가, 삭제, 변경이 가능하다. 프로토콜에 대한 분석은 규칙을 수행 시킴으로써 시작할 수 있다. 메인화면의 규칙수행 버튼을 클릭하면 평가를 수행할 시스템을 선택하고, 적용될 규칙을 선택하게 된다.

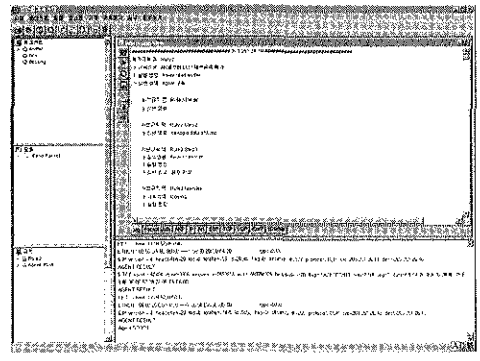

그림 3 분석규칙 수행화면

그림3은 분석규칙을 수행시켜 패킷을 실시간으로 캡쳐하고, 프로토콜을 분석하는 화면 나타낸 것이다. 그냥 단순히 패킷만을 캡쳐하여 보고자 할 경우에는 분석규칙에 패킷수집과 관련된 모듈만 동작시키면 된다.

그림4는 분석규칙에 의해 캡쳐된 패킷들을 프로토콜별로 분류하여 보여주고 있는 화면이다. 프로토콜별 세부사항은 화면의 항목들을 마우스로 클릭함으로써 데이터부분까지 상세히 볼 수 있다.

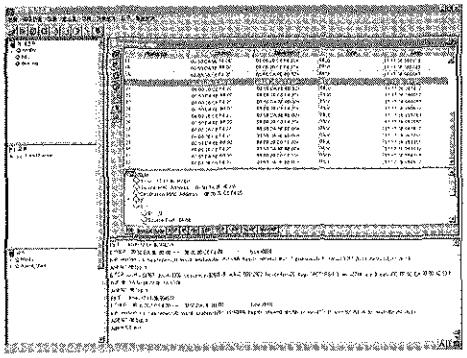

그림 4 패킷 캡처화면

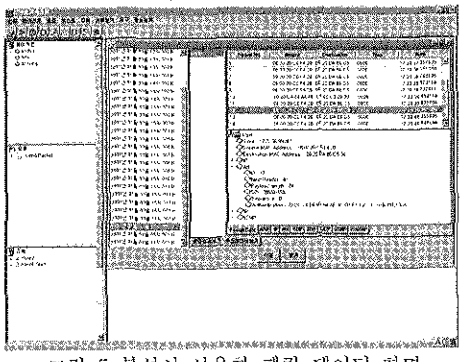

그림 5 분석시 사용한 패킷 데이터 화면

그림6은 프로토콜 분석시 사용한 패킷 데이터 들을 보여주는 화면으로써 수행날짜별로 저장되어 있는 분석결과 로그와 링크되어 있다. 그러므로 사용자는 분석결과 로그의 수행날짜를 클릭하고 수집데이터보기 탭을 클릭하면 분석결과 로그에서 보여주고 있는 패킷 데이터를 볼 수 있다.

그림7은 사용자가 프로토콜 분석 및 시험에 사용할 패킷을 생성하거나 삭제, 변경하는 화면을 나타낸 것이다.

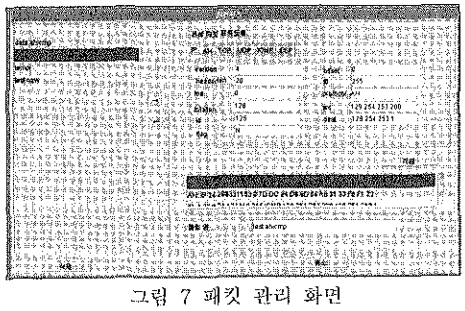

그림 7 패킷 관리 화면

4. 결론

현재 구현된 프로토콜 분석 도구는 다음과 같은 장점을 가지고 있다.

- ARP, IP, TCP, UDP, ICMP 및 AH, ESP, ISKMP 프로토콜의 패킷 내용들을 모니터링 할 수 있다.
- 규칙 기반 분석을 수행하므로 보다 자유로운 프로토콜 평가가 가능하다.
- 에이전트에 의해 패킷을 수집할 수 있으므로 원거리의 시스템도 평가할 수 있다.
- 분석에 필요한 기능들을 모듈단위로 관리할 수 있으므로 확장이 용이하다.

그러나 보다 완성도 높은 보안 시스템을 개발하는데 사용하기 위해서는 다음과 같은 사항들이 개선되고 추가되어야 할 것이다.

- 분석에 따른 실시간 패킷 응답 속도의 증가
- Decryption기능으로 추가하여 암호화된 패킷 분석 기능
- Encryption기능으로 가상적인 암호화 패킷 전송 기능
- 가상적인 패킷으로 프로토콜을 구현하여 통신하는 기능

5. 참고 문헌

[1]. 이종태, 손승원, " 인터넷 정보보호 IPSec 기술" , 한국통신학회논문지 '99-2 Vol.24 No.2A

[2]. W. Richard Stevens, " Unix Network Programming" , Volume 1

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

[4]. S. Kent, R. Atkinson, "IP Encapsulation Security Payload", RFC 2406, November, 1998.

[5]. H. Harney, C. Muckenhirn, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[6]. D. Maughan, M. Schertler, M. Schneider, and J. Turner "Internet Security Association and Key Management Protocol", RFC 2408, November 1998.

현 정 식(Jeung-Sik Hyun)

1999년 2월 : 청주대학교 컴퓨터정보학과 졸업

1999년 3월~현재 : 청주대학교 산업학원경영대학원 전자계산학과 재학중