정보보안 제품들에 대한 무결성 검증 도구 설계 및 구현

김태호*, 김창배*, 박성준*, 김창수*, 이선호**
*부경대학교 전자계산학과, **전산정보학과

The Design and Implementation of Integrity Verification tools for Information Security Products

Tae-Ho Kim*, Chang-Bae Kim*, Sung-Jun Park*, Chang-Soo Kim*, Sun-Ho Lee**
*Dept. of Computer Science, PuKyong Nat'l University
**Dept. of Computer Science and Information, PuKyong Nat'l University

요 약

현대 사회는 컴퓨터와 인터넷을 이용한 정보 교환이 필수적이다. 이러한 정보 교환은 기본적으로 해킹 및 불법적인 접근으로 보호되어야 하며, 이러한 불법적인 접근으로부터 정보를 보호하기 위해 정보보안 제품들이 많이 개발되어 있다. 본 연구에서는 기존의 개발된 보안 제품들이 UNIX 혹은 Windows 계열에서 개발되었다 할지라도 TCP/IP를 기반으로 하는 제품들에 대해서 내부적으로 전송되는 데이터들에 대해 보안 기능 및 무결성 기능을 실시간 및 자동으로 탐지하는 도구를 개발하는데 있다. 기존의 보안 제품들은 응용 계층 및 IP 계층에서 인증 및 보안 기능을 수행하는 제품들이 많이 개발되었는데, 본 연구에서는 응용계층과 IP 계층 모두에서 개발된 보안 제품들에 대해 자동으로 탐지하는 모듈을 Linux 환경에서 구현하였다. 그리고 관리자의 편리한 검증을 위해 다양한 인터페이스 환경을 제공하는 모듈을 추가하였다.

1. 서론

현재 보안 분야에서 공중망에 암호화와 인증 기능을 제공하여 사용하는 가상사설망(VPN)에 대한 많은 연구가 이루어지고 있다. 이러한 가상사설망 관련의 많은 제품들은 IETF에 의해 IP계층의 보안 표준으로 추천되는 IPsec 프로토콜을 사용하고 있다. IPsec 프로토콜은 사용자에 투명성을 제공하며 IP계층의 구현이므로 응용계층에서 구현되는 어플리케이션과의 호환성을 가지기 때문이다. 그러나 IPsec을 사용하여 무결성 기능을 제공하는 제품들이 정확한 기능을 하는지 검사하는 도구가 필요하다. 본 연구는 데이터 무결성을 검증하는 소프트웨어를 개발하고, IPsec을 적용한 후, 중간 호스트가 패킷을 변조하여 무결성 기능을 검증토록 하였다. 또한 패킷 변조위치를 조정함으로써 IP계층과 응용계층까지 무결성 검증기능을 확대하였다. 본 논문에서는 가상사설망을 구현하는 보안 프로토콜을 살펴보고, 실제 호스트간에 IPsec을 적용, 실시간으로 무결성을 검증하는 구현에 대해 살펴본다. 끝으로 결론 및 향후 연구과제에 대해 살펴본다.

2. 무결성 보안 제품 구현 방법

데이터 무결성 검증 도구의 개발을 위해 무결성 기능을 제공하는 보안 제품들의 계층별 구현 방법을 살펴보고, 특히 IP계층의 보안 프로토콜인 IPsec에 대한 전송 모드 및 처리 방법에 대해 기술한다.

2.1 가상사설망의 계층별 구현

가상사설망(VPN)은 구현 계층에 따라 링크계층, 네트워크계층, 응용계층에서 구현하는 방법으로 구분할 수 있다[1].

2.1.1 응용계층 구현

응용계층에서의 보안 제품 구현은 기본적으로 TCP/IP 계층에서의 전송 정보를 보호하거나, 위장 공격 등 데이터 그램의 전송 중에 일어나는 몇 가지 일반적인 네트워크 계층에 대한 공격의 보안 해결책이 없다. 이러한 문제점을 해결하기 위해 여러 가지 보안 기법들이 제시되고 있으나, 현재 IETF에서는 SOCKSv5[2]를 응용 계층의 가상사설망 보안 프로토콜로 추진하고 있다.

2.1.2 링크계층 구현

링크 계층에서 구현된 프로토콜은 비용 면에서 효율적이나 암호학적으로 확실하지 않아 다른 계층의 프로토콜과 함께 사용되는 터널의 종단에서만 인증이 제공되므로 위장공격이나 중도위협에 노출될 가능성이 크며 패킷 단위의 무결성이 보장되지 않으므로 DoS[3] 공격을 당할 수 있다. 링크계층의 구현 방법으로는 Microsoft의 「PPTP(Point to Point Tunneling Protocol)」, 이미 표준화가 이뤄진 「L2TP (Layer 2 Tunneling Protocol)」 등이 있다.

2.1.3 IP계층 구현

IP계층 보안 프로토콜은 단말 호스트간의 터널링 기능이 가능한 하위 계층에서 구현이 가능하며, 응용 소프트웨어의 수정 없이 IP 데이터그램의 페이로드(payload)에 전해지는 상위계층의 응용프로그램 데이터들을 보호할 수 있기 때문에 많이 사용된다. 계층별 분류를 도식화하면 그림 1과 같다.

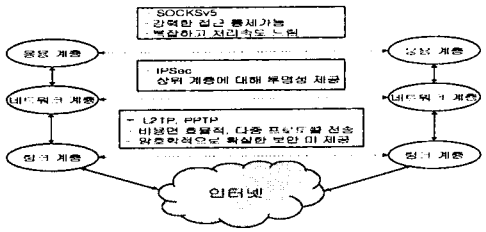

그림 1 가상사설망의 계층별 분류

2.2 IPsec

IPsec[4]은 TCP/IP 통신을 보호하기 위한 다목적 프로토콜이며, 호스트간의 트래픽을 보호하는데 적합하다. IPsec은 네트워크 계층의 가상사설망 구현을 위해서 무결성과 인증을 보장하는 인증헤더(Authentication Header)와 암호화된 캡슐화로 기밀성을 보장하는 ESP(Encapsulation Security Payload)를 사용한다. 인증 헤더는 패킷 안의 데이터를 검증 가능한 서명과 결합시켜 데이터 송신자의 신원을 확인하고 데이터가 변조되지 않았음을 검증할 수 있으며, ESP는 각 페이로드를 불법 해독할 수 없도록 한다. 또한 키 관리 메커니즘으로 다양한 방법이 사용될 수 있으며, IEFT의 제안에서는 ISAKMP[5]를 사용한다. 그림 2에서와 같이, IPsec은 Snooping 혹은 변조로부터 IP 패킷을 보호하기 위해 IP 프로토콜을 확장한다. IPsec은 새로운 IPv6의 한 부분으로 구현되고 현재의 IPv4에서도 동작할 수 있게 되었다.

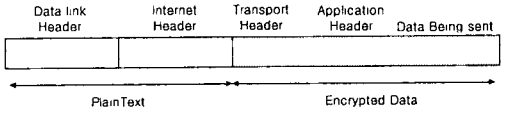

그림 2 IPsec 프로토콜의 기본 포맷

2.2.1 인증헤더

인증헤더(Authentication Header:AH)[6]는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하며 인증과 무결성을 보장한다. 기본적 개념은 IP 데이터그램 전체에 걸쳐 단방향 해쉬함수를 사용해서 인증 정보를 추가하여 보안을 제공한다. 인증헤더의 위치는 IPv6의 경우 Fregmentation과 End-to-End 뒤에, TCP 헤더 앞에 위치하고, IPv4에서는 IP헤더 바로 뒤에 위치한다(그림 3 참조). 인증헤더를 적용한 패킷의 처리는 목적지와 사용자 를 기초로 하여 SA (Security Association)를 선택하고 인증데이터를 처리 후 인증헤더를 추가하여 종료된다. 수신자는 목적지 주소 등을 이용, SA를 선택하고 무결성을 체크한다.

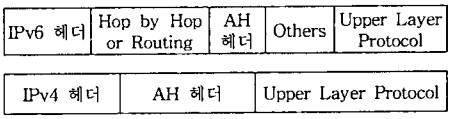

그림 3 IPv4와 IPv6에서의 인증헤더 위치

2.2.2 ESP(Encapsulation Security Payload)

ESP[7]는 암호화 기법을 사용, 데이터의 재전송 방지, 비밀성 제공한다. 기본 개념은 보호될 데이터를 암호화하여 ESP헤더의 데이터 영역에 삽입하고 IP헤더에 ESP헤더를 추가하는 것이다. 보호 영역이 트랜스포트 세그먼트나 IP 데이터그램 전체에 따라 트랜스포트 모드와 터널 모드로 나누어진다(그림 4 참조).

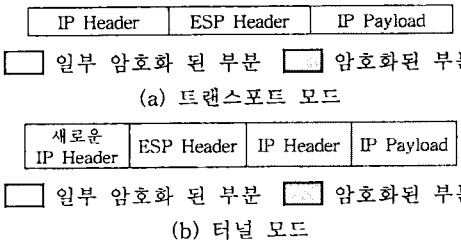

그림 4 ESP 모드의 두 가지 전송 모드

3. 무결성 검증 도구 구현환경 및 사용자 인터페이스

본 연구에서 구현하고자 하는 것은 IPsec이 적용

된 호스트간 전송 패킷을 게이트웨이에서 실시간으로 변조하고 수신측에서 변조를 확인하는 것이다. 게이트웨이에서는 IP계층까지만 통과하므로 패킷 변조를 위해 커널의 IP계층을 수정하였다. 또한 변조정보를 동적으로 선택할 수 있게 커널 모듈을 사용하였다.

3.1 라우터 기반의 무결성 검증 도구 구현

운영체제는 TCP/IP가 지원이 되며 소스가 공개되어 자유롭게 변경가능하고 안정적인 Linux(버젼 5.2 , 커널버젼 2.0.36)를 선택한다.

또한 두 컴퓨터 간 통신에 데이터 무결성을 보증하기 위해 IPsec표준안에 따른 구현인 FreeS/WAN[8]을 사용하여 VPN을 구성하고, 패킷을 변조하는 컴퓨터가 라우팅을 하도록 시스템을 구성한다. 데이터 무결성 검증 S/W를 개발하기 위한 테스트 환경 구성은 그림 5 과 같다.

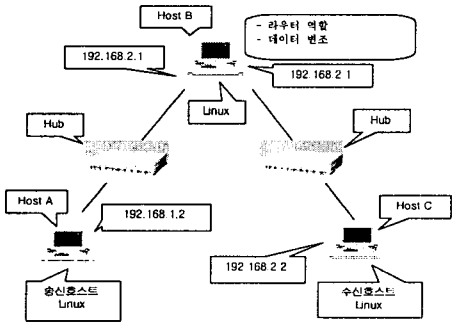

그림 5 데이터 무결성 검증 도구 개발 환경

Host B가 Gateway이어야만 하지만 Gateway의 설치가 비용면에서 힘들기 때문에 Host B에 두 개의 이더넷 카드를 설치하고 라우터 역할을 하도록 하였다.

3.2 IP 계층 패킷 모듈 수정 내용

그림 6에서 보듯이 NIC를 통해 수신된 패킷은 ip_input.c에서 목적지주소가 호스트 자신과 일치하면 상위계층으로 넘겨지고, 아닐 경우 ip_forward.c를 따라 ip_output.c로 보내져 다시 네트워크로 전송된다[9].

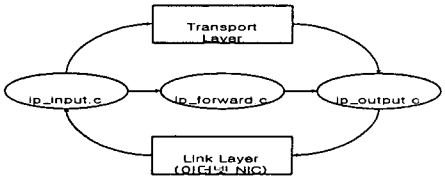

그림 6 IP계층에서의 패킷 처리 과정

본 연구에서는 패킷을 포워딩 시키는 ip_forward.c에 패킷 변조루틴을 추가한다. 본 연구의 구현은 크게 세 부분으로 나뉜다. 패킷 변조를 위한 커널 수정, 변조 정보의 동적 설정을 위한 커널 모듈 사용, 마지막으로 사용자 인터페이스를 구성하는 것이다(그림 7 참조).

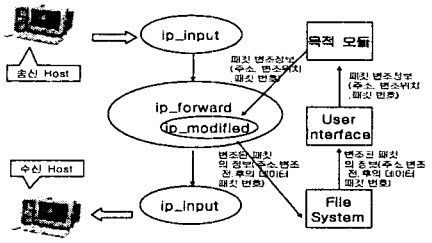

그림 7 패킷 변조를 위한 상세 모듈

3.2.1. Linux OS의 IP계층 수정

패킷을 변조하기 위해서 커널에 패킷 변조 루틴을 추가하고, 변조에 대한 정보를 동적으로 구성하기 위해서 변조에 대한 설정을 변경할 수 있는 루틴을 작성, 그 함수를 외부 커널 모듈이 참조할 수 있도록 심볼 테이블을 구성한다. 또한 변경된 패킷 정보를 외부 파일로 출력하기 위해 /proc 파일 시스템을 이용한다.

3.2.2 무결성 검사를 위한 환경 설정 모듈 추가

필요할 시에만 커널과 함께 수행되고 불필요할 때 제거되는 오브젝트 코드를 모듈이라 한다. 본 연구에서는 사용자가 동적으로 패킷 변조 정보를 입력하기 위한 특수장치를 설정하고 장치를 통해서 정보가 입력된 경우 정보를 처리하기 위해 목적 모듈을 사용한다.

3.3 사용자 인터페이스 및 구현 결과

사용자 인터페이스 프로그램을 수행했을 때 변조 정보를 변경하고자 하면 각 항목을 설정하여 수행할 수 있다. 각 항목에 대한 설명은 그림 8 과 같다.

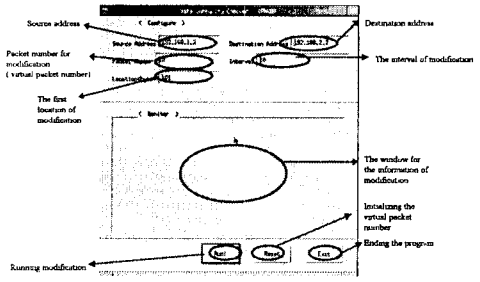

그림 8 패킷 변조를 위한 사용자 인터페이스

그림 5와 같은 구현 환경에서 실시간으로 전송되는 패킷을 변조한 경우, 게이트웨이에서 변경된 정보는 그림 9와 같다. 그림 9 는 192.168.1.2에서 192.168.2.2로의 패킷 중에서 가상 패킷 번호가 5이거나 간격이 5인 경우 패킷의 IP헤더 이후의 20번째 바이트에 1을 증가시키고 16bit 떨어진 곳에 1을 감소시킨다. 한편 응용 계층의 정보보호 무결성기능 검증할 때 그림 10 과 같은 TCP 체크섬[10]이 문제가 된다. 중간 게이트웨이에서는 상위 계층까지 가지 않고 IP계층까지만 통과하므로 TCP 체크섬을 다시 계산할 수 없어 응용 계층까지 갈 수 없게 되므로 무결성을 검증에는 부적합하다. 따라서 응용 계층의 무결성 검증 기능까지 확대하기 위해 패킷 변조 시 16비트 단위로 하여 두 개의 변조 위치를 설정하여 1증가, 1감소를 시킴으로써 패킷이 변조되었지만 TCP 체크섬에는 영향을 주지 않도록 하였다. 이 게이트웨이를 거친 패킷은 IP헤더를 제외한 데이터 영역이 변조되고, 변조 위치를 두 곳 설정함으로써 IPsec이 적용된 수신 호스트에서는 IPsec에 의해 변조되었음이 확인되고 응용계층에서의 구현은 TCP의 체크섬을 통과하여 변조되었음이 검출되었다.

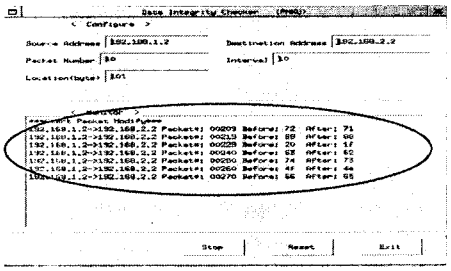

그림 9 패킷 변조 입출력 구성

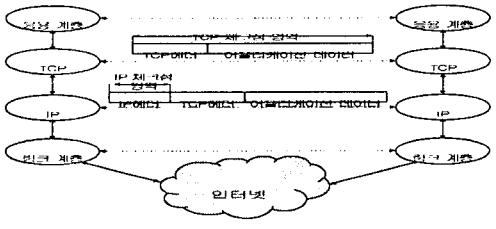

그림 10 계층별 체크섬 보호 영역

4. 결론

본 연구는 정보 보호 무결성을 지원하는 제품의 무결성 기능을 실시간으로 검사할 수 있는 검증도구의 구현을 목적으로 하였다. 구현을 위해 환경을 구성하고 IPsec을 적용한 가상사설망을 구성하였다. 또한 커널을 수정하고 목적 모듈을 사용하여 패킷을 변조하였다. 어떤 형태로 변조하더라도 변조된 패킷이 검출됨을 확인하였고, 변조 패킷의 위치를 조정하여 응용계층의 무결성 기능까지 검증할 수 있었다.

현재 보안도구 제품들을 평가하는 다양한 방법이 있지만, 본 연구에서 구현된 도구를 사용하여 무결성 기능을 충분히 검증할 수 있을 것이라고 생각한다. 본 연구에서는 정적 IP를 갖는 보안 도구를 대상으로 하였지만, 동적 IP를 갖는 Mobile IP까지 확장하는 것이 향후 연구과제로 계속 연구를 진행하고 있다.

[참고문헌]

[1] 한국정보보호 센터, "IP계층과 응용계층에서의 VPN 보안기술 표준(안)", November, 1998.

[2] [SOCKSv5] M.Leech, M.Ganis, Y.Lee, R.Kuris, D.Koblas, L.Jones SOCKS Protocol Version 5 , RFC 1928, March 1996.

[3] 정윤종, 한국정보보호 센터, "'98 해킹 사례 분석", 1999. 3.

[4] Naganand Doraswamy, Dan Harkins "IPSec", pp. 41-51

[5] [ISAKMP] D. Maughan, "Internet Security Association and Key Management Protocol", RFC 2408, November 1998

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

[7] [ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, November 1998.

[8] [FreeS/WAN] http://www.freeswan.org/ July 2000.

[9] R Magnus, U Kunitz, M Dziadzka, D Verworner, M Beck, H Böhme "Linux Kernel Internals" pp. 258-315

[10] R.Braden, D.Borman, C.Partridge Computing the Internet Checksum , RFC 1071, September 1998.