제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

IPv4/IPv6 보안 패킷 분석기

권혁찬, 나재훈, 손승원
한국전자통신연구원 네트워크보안연구부
e-mail : hckwon@etri.re.kr

A Security Packet Analyzer in IPv4/IPv6 network

Hyeok-Chan Kwon, Jae-Hoon Nah, Sung-Won Sohn
Electronics and Telecommunications Research Institute

요 약

본 논문에서는 IP 보안(IPsec : IP Security)이 적용된 보안 패킷들을 네트워크 상에서 실시간으로 수집하여 분석해 주는 IP 보안 패킷 분석기를 설계 및 구현하였다. 본 패킷 분석기는 TCP, UDP, IP, ICMP 등의 일반 네트워크 패킷과 키 교환을 위한 IKE 패킷, 보안 통신을 위한 AH, ESP 패킷 등을 실시간으로 수집하고 분석하는 기능을 갖는다. 본 패킷 분석기는 현재의 IPv4 패킷 뿐 아니라, 차세대 인터넷인 IPv6 패킷에 대하여도 실시간 수집 및 분석 기능을 제공한다. 또한 본 분석기는 IPsec 엔진에 대한 보안성을 평가하기 위한 자동화된 평가기능도 제공해 준다. 개발한 패킷 분석기를 이용하여 ETRI 에서 개발한 통합 IPsec 엔진에 대한 보안성을 평가한 결과도 함께 보인다.

1. 서론

최근 인터넷의 폭발적인 발달과 더불어 인터넷 정보보호 서비스에 대한 요구가 매우 급증하는 실정이며, 관련 연구들이 매우 활발히 진행되고 있는 실정이다. IPsec(IP Security)은 Layer 3 즉, 네트워크 계층에서 보안서비스를 제공하기 위한 프로토콜로서 IETF Security Area 의 IPsec Working Group 을 중심으로 표준화가 진행 중이며, 현재 관련된 18 개의 RFC 작성이 완료된 상태이다[1-5]. 현재 IPsec 은 리눅스, FreeBSD, Window2000 등 여러 가지 플랫폼에서 구현되고 있으며, 리눅스 기반의 FreeS/WAN, FreeBSD 기반의 KAME 등 공개된 프로젝트도 다수 존재한다[6-8].

본 논문에서는 IP 보안(IPsec : IP Security)이 적용된 보안 패킷들을 네트워크 상에서 실시간으로 수집하여 분석해 주는 IP 보안 패킷 분석기를 설계 및 구현하였다. 본 패킷 분석기는 TCP, UDP, IP, ICMP 등의 네트워크 패킷과 키 교환을 위한 IKE 패킷, 보안 통신을 위한 AH, ESP 패킷 등에 대한 실시간 수집 및 분석 기능을 갖는다. 본 패킷 분석기는 현재의 IPv4 패킷 뿐 아니라, 차세대 인터넷인 IPv6 패킷에 대하여도 실시간 수집 및 분석 기능을 제공한다. 또한 본 분석기는 IPsec 엔진에 대한 보안성을 평가하기 위한 자동화된 평가기능도 제공해 준다.

본 논문의 구성은 다음과 같다. 2 장에서는 보안 패킷 분석기의 설계에 대한 내용을 기술한다. 3 장에서는 구현에 대한 내용과 실제 개발한 패킷 분석기를 이용하여 ETRI 에서 개발한 통합 IPsec 엔진에 대한 보안성 평가를 수행한 결과를 보인다. 마지막으로 4 장에서 결론을 맺는다.

2. IPv4/IPv6 보안 패킷 분석기의 설계

그림 1 은 보안 패킷 분석기의 기본 구조를 보여준다. 보안 패킷 분석기는 시스템을 총체적으로 제어하는 평가엔진 (Evaluation Engine), 시스템에 필요한 데이터를 관리하는 DBMS, 데이터를 수집하는 에이전트 (agent), 패킷 분석 및 보안성 평가를 위해 사용되는 모듈 (module) 그리고 패킷 분석 및 보안성 평가를 실행하기 위한 룰 해석기(rule interpreter)로 구성된다.

2.1 평가엔진(Evaluation Engine)

평가엔진은 그림 1 에서 볼 수 있듯이, System Configuration, Database Control, Rule Interpreter 로 구성된다.

System Configuration 은 세부적으로 Access Control, Agent Registration, Module Registration, Directory Setup 모듈로 나눌 수 있다.

Access Control 은 본 시스템 사용을 위한 사용자 인

증을 수행하는 부분이다. Agent Registration 에서는 에이전트 이름, 에이전트타입, 데이터베이스 이름, 현재 에이전트가 설치되어 있는 호스트 정보등을 등록한다. Module Registration 에서는 평가 룰에서 사용하게 될 각 모듈에 대한 정보를 등록하는 곳으로 모듈 이름, 모듈 설치 경로, 모듈에 대한 설명 등을 등록한다. Directory Setup 에서는 평가 룰 수행 시 사용되는 임시 데이터와 관리자가 임의적으로 만든 패킷 데이터가 저장될 Directory Path 를 정의한다.

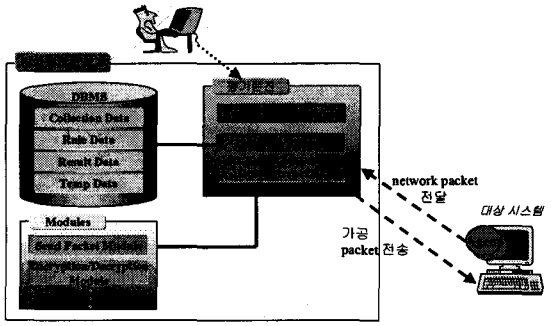

그림 1. 보안 패킷 분석기의 구조

그림 1 의 Database Control 은 DB 내의 테이블 생성, 데이터 추가, 수정, 삭제 등의 작업을 수행한다. 또한 평가 룰의 편집, 평가에 사용하기 위한 패킷 데이터 편집, 평가 결과의 검색 그리고 에이전트로부터 수신한 평가 결과 저장 및 검색 기능을 갖는다.

2.2 룰 해석기(Rule Interpreter)

평가 엔진내의 룰 해석기는 평가 룰을 DBMS 의 룰 데이터(Rule Data)로부터 순차적으로 읽은 다음, 수행 절차에 따라 명령을 해석하고 실행하는 기능을 갖는다. 룰 해석기는 Flow Control, Parser 그리고 External Interface 로 구성된다.

룰 해석기의 파서(parser)는 룰 데이터의 프로그램 필드에 저장되어 있는 평가 프로그램에 대한 문법검사를 수행 한 후 문법오류가 없으면 각 단어를 분리하여 흐름제어(Flow Control)로 보낸다. 흐름제어는 파서로부터 받은 각 단어에 할당되어 있는 제어명령을 수행하고, 명령수행 과정에 있는 함수들을 외부 인터페이스(External Interface)로 제공한다. 외부 인터페이스는 DB 조작, 에이전트와 모듈 제어, 룰 실행에 필요한 모듈과의 인터페이스를 제공하는 기능을 갖는다.

룰 해석기에서 처리 가능한 제어 명령으로는 IF 문, FOR 문, DO 문, BREAK 문, PRINT 문, COMMENT 문이 있다. 제어명령 이외의 평가 룰을 수행하는데 필요한 명령들은 모두 함수형태로 지원되며, 외부 인터페이스에 의해 수행된다. 외부 인터페이스에 의해 수행되는 함수는 표 1 과 같다.

MODULE 함수와 AGENT 함수의 파라미터로 사용되는 'command'에 포함되는 명령어로는 현재 sniffer 와 sndpkt 가 구현되어 있다. sniffer 는 주어진 룰에 맞는 packet 을 네트워크상에서 또는 타겟 호스트의 에이전트로부터 혹은 시스템 내부의 DB 로부터 스니핑하는 명령어이다. 현재 Sniffer 로 모니터링 할 수 있는 프로토콜로는 ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP 가 있다. Sndpkt 는 시스템 내에 저장된 패킷이나 현재 편집한 패킷을 Raw Socket 을 이용하여 목적 호스트로 전송하기 위한 명령어이다. 현재 Sndpkt 로 전송할 수 있는 프로토콜로는 ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP 가 있다.

표 1 외부 인터페이스 지원 함수

SQL(output DB, Query, input DB)
Input DB 로부터 Query 에 해당하는 SQL 질의를 실행하고 그 결과를 output DB 에 저장한다.
AGENT(command, START[or STOP])
Command 명령을 에이전트를 통해 실행시키거나 종료한다.
MODULE(command)
command 명령을 실행한다.
SAVE(filename, query, input DB)
InputDB 로부터 Query 에 해당하는 SQL 질의를 실행하고 그 결과를 그 결과를 패킷 전송용 데이터 타입으로 파일에 저장한다.

2.3 DBMS

보안 패킷 분석기에서 사용되는 DB 로는 Collection Data, Rule Data, Result Data, Temp Data 가 있다.

Collection Data 는 에이전트로부터 전송 받은 각종 프로토콜 데이터를 저장하는 곳이며, Ethernet, ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP 프로토콜에 대한 테이블을 보관, 관리한다. Rule Data 는 평가에 대한 룰을 저장하는 곳으로, Database Control 의 Rule DB Control 에 의해 평가 룰이 정의되거나 수정 및 삭제되며, 룰 해석기에 의해 평가 룰이 해석되고 수행되어 진다. Result Data 는 평가 룰이 수행된 결과를 저장하는 곳으로, Rule Interpreter 의 Flow Control 에 의해 저장되어 진다.

2.4 에이전트

에이전트는 대상 시스템에서 수행되며 네트웍 단자를 통해 송수신되는 패킷들을 보안 패킷 분석기로 전달하는 기능을 수행한다.

IP 보안 패킷 분석기는 START, STOP, HALT, RESUME 의 4 가지 명령을 에이전트에게 송신할 수 있는데 START 명령을 송신하는 경우에는 스니핑할 패킷을 선별하기 위한 option 값을 함께 전송할 수 있다. 각 명령 및 Option 값은 다음과 같이 정의된다.

START prot src ip1 dest ip2: 스니핑을 시작하라는 명령이며 스니핑을 위한 옵션으로 프로토콜(prot)과 패킷의 발신지(src), 패킷의 목적지(dest) 호스트를 지정할 수 있다. 옵션에서 지정한 조건에 맞는 패킷만 스니핑한다.

- STOP: 스니핑을 종료하고 시스템과의 접속을 해지하라는 명령.
- HALT: 스니핑을 일시 중지.
- RESUME: 스니핑을 계속 수행.

IP 보안 패킷 분석기과의 접속이 이루어지면 에이전트는 WAIT 상태에서 시스템으로부터의 명령을 기다린다. START 명령이 수신되면 상태를 ACTIVE 로 전이시키고 스니핑을 위한 준비 작업을 수행한다. 이는 PCAP 라이브러리를 초기화하는 작업을 포함한다. 에이전트가 ACTIVE 상태에서는 10ms 마다 PCAP 함수를 호출하여 패킷을 스니핑한다.

3. 구현

본 논문에서 제안한 IP 보안 패킷 분석기는 Windows 와 UNIX 환경에서 수행이 가능하며 Java 와 C 언어로 구현되었다. DB 는 my-sql 로 구현하였다. 그림 2 는 패킷 분석기의 메인 화면이다.

그림 2 에서 좌측의 세 개의 창은 등록된 에이전트, 모듈, 룰의 리스트를 tree 형식으로 보거나 선택할 수 있는 창이다. 우측 상단의 창은 실행 로그 파일이나 에이전트에서 오는 각 프로토콜의 수집데이터를 보여주는 창이다.창 하단의 log 는 log 기록보기를 선택하기 위한 버튼이며, Packet data 는 수집된 packet 전체를, ARP 는 수집된 packet 중 ARP 패킷만, AH 는 수집된 packet 중 AH packet 만 보기 위한 버튼이다. 나머지 IP, TCP, UDP, ICMP, ISAKMP 모두 동일한 방식으로 원하는 프로토콜 packet 만을 볼 수 있다. 이처럼 패킷을 각 필드별로 구분하여 보여줌으로 본 시스템은 IPsec 프로토콜 개발 시 디버깅 툴로도 사용이 가능하다. 우측 하단의 창은 에이전트에서 오는 패킷 데이터가 수집되는 과정을 보여주는 텍스트 영역이다.

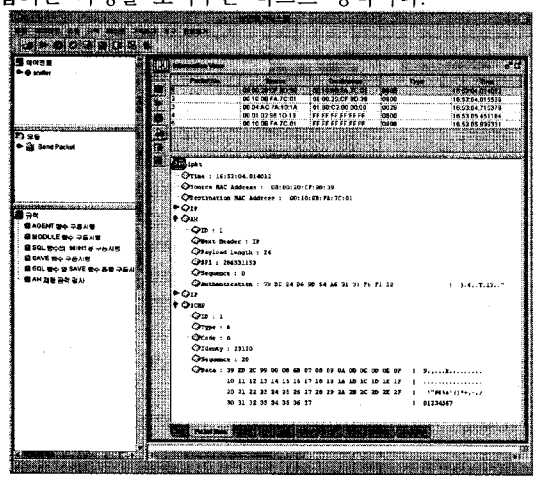

그림 2 스니핑된 AH 패킷

그림 2 의 '규칙' 메뉴는 룰을 입력, 수정, 선택, 삭제 할 때 사용된다. 그림 3 은 이미 입력된 룰 중 실행하고자 하는 하나의 룰을 선택하기 위한 윈도우 이다. 그림 3 에 기술된 룰의 의미는 다음과 같다. "목적 호스트로 전달되는 AH 가 적용된 ICMP 패킷을 스니핑하여 저장한 후 동일한 패킷을 재전송 하여보고 결과를 분석한다. 만약 재전송한 패킷에 대한 응답이 목적 호스트로부터 오게 된다면 '재현공격에 대한 가능성이 보임' 이라는 경고메시지를 출력하고, 응답이 오지 않는다면 '재현 공격에 대해 안전함'이라는 메시지를 출력한다." 그림 2 는 AH 가 적용된 ICMP 패킷을 목적호스트로부터 스니핑하는 단계에서 AH 패킷을 보여주는 윈도우이다. 그림 3 의 룰을 적용하여 ETRI 에서 개발한 통합 IPsec 엔진에 대하여 재현공격에 대한 위협을 테스트한 결과 안전하다는 결과가 나왔다. 실험 결과는 log 창을 통해 확인 할 수 있다.

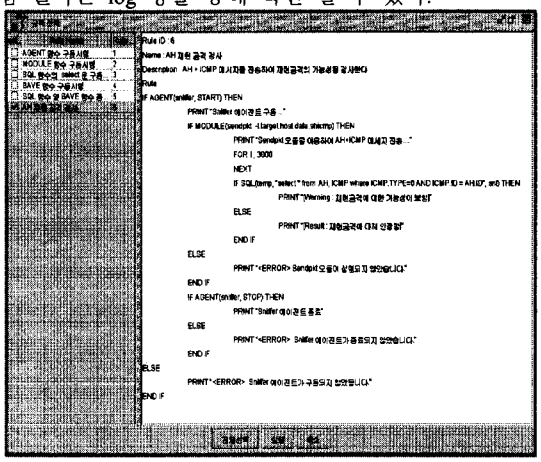

그림 3 룰 선택 화면

3.1 보안성 평가

IPsec 에서 제공하는 4 가지 보안성을 본 시스템을 이용하여 평가하는 방법을 요약하면 다음과 같다.

- 기밀성(confidentiality) : 전송중인 암호화된 ESP 패킷을 수집하여 메시지의 내용을 알아 볼 수 있는지 확인하고 임의의 키로 복호화 해본다.
- 원적지 인증(Data Origin Authentication) : 전송중인 AH 혹은 ESP 패킷을 실시간으로 수집한 후 수집한 패킷 헤더 내의 Source IP 주소를 변경하여 목적지로 전송하고, 그 결과를 분석한다.
- 접근 제어(Access Control) : 임의의 키(key)를 이용하여 AH 혹은 ESP 패킷을 구성하여 목적지로 전송하고, 그 결과를 분석한다.
- 비연결형 무결성(Connnectionless Integrity) : 수집한 패킷의 특정 필드를 변경한 후 ICV 값을 재계산하여 변조 한 후 전송하고, 그 결과를 분석한다.
- 재현공격 방어(Anti-replay) : 수집한 패킷을 복사하여 동일한 목적지로 전송하여 본다. 또는 수집된 패킷의 IPsec AH/ESP 헤더내의 SN(Sequence Number)값을 감시하여, 새로운 SN 을 생성하거나 수집한 SN 을 변경하여 전송하고, 그 결과를 분석한다.

실제 제안한 IP 보안 패킷 분석기를 이용하여 본 연구소에서 개발중인 통합 IPsec 엔진에 대한 보안성을 75 가지의 시험항목을 정의하여 평가하였다. 표 2 는 보안성 평가를 위해 정의한 시험항목의 일부이다.

평가 결과 C-ISCAP 은 총 72 가지의 보안성 평가 항목을 통과하였다.

표 2. 보안성 평가항목의 일부

1.	Detect modified ESP packet (Modification of IP src.)	
	H1 ==========> H2	ICMP Echo request (with AH, modification of IP src.)
	H1 <====X==== H2	No ICMP Echo reply (Drop packet)
2.	Inbound ESP packet with Fragmentation	
	(Authentication: HMAC-SHA1, Encryption: 3DES-CBC)	
	H1 ==========> H2	Send Fragmented TCP message
	(1^{st} /2^{nd} / 3^{rd} ... fragment)	(with ESP)
3.	Inbound Tunnel AH packet (Authentication: HMAC-MD5)	
	H1 ==> GW1 ==> GW2 ==> H2	ICMP Echo request
	|----------Tunnel----------|	(with tunnel AH)
	H1<== GW1<== GW2 <== H2	ICMP Echo reply
		(with Tunnel AH)
4.	Outbound AH+ESP packet with SA bundles	
	H1 ==> GW1 ==> GW2 ==> H2	ICMP Echo request
	|-Tunnel ESP -|	(with SA bundles)
	|------Transport AH ----------|	
	H2 <== GW1 <==== GW2 <== H1	ICMP Echo reply
	|-Tunnel ESP -|	(with SA bundles)
	|------Transport AH ----------|	
5.	Inbound AH+ESP (Policy=Drop)	
	H1 ======> H2	ICMP Echo request (with AH+ESP)
	H1 <==X == H2	No ICMP Echo reply (drop packet)

3.2 IPv6 패킷 분석기

본 패킷 분석기는 IPv6 패킷에 대해서도 패킷 분석 기능 및 트래픽 모니터링 등의 기능을 갖는다. 그림 4 는 IPv6 패킷 분석기에 의해 ESP 패킷이 스니핑된 화면을 텍스트 형태로 보여준다. 그림 5 는 IPv6 IPsec 통신 패킷의 트래픽을 실시간으로 모니터링 하는 화면 이다. 그림 5 에서 AH 가 적용된 패킷이 발생하고 있음을 확인할 수 있다.

4. 결론

본 논문에서는 IP 보안이 적용된 네트워크 상에서 전송되는 보안 packet 들을 실시간으로 스니핑하여 분석해 주는 IP 보안 패킷 분석기를 설계 및 구현하였다. 본 패킷 분석기는 보안 패킷을 스니핑하고 분석해 주는 기능 뿐 아니라 IPsec 엔진에 대한 보안성을 평가하기 위한 자동화된 평가기능도 제공해 주었다.

본 시스템은 다음과 같은 특징을 갖는다.

- 네트워크 상의 다양한 프로토콜들의 패킷을 수집하고 분석하는 기능을 갖는다.
- 에이전트를 사용하여 원거리 호스트에 대한 평가가 가능하다.
- 룰 기반으로 동작하므로 자동화된 보안성 평가가 가능하다.
- 룰에 대한 문법을 단순화 하여 손쉽게 룰을 정의할 수 있다.
- 평가 룰에 필요한 기능을 모듈로 관리하므로 확장이 용이하다.

현재 IPv6 네트워크 패킷에 대하여는 패킷 실시간 스니핑 및 분석 기능과 네트워크 트래픽 모니터링의 기능만이 구현되었다. 향후 IPv6 네트워크에 대한 보안성 평가 기능을 추가할 예정이다.

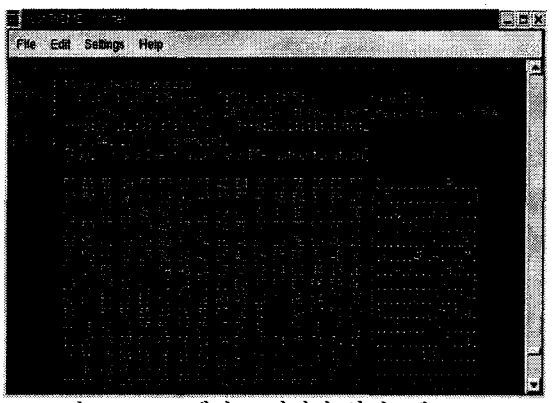

그림 4. IPv6 패킷 모니터링 화면 (텍스트 모드)

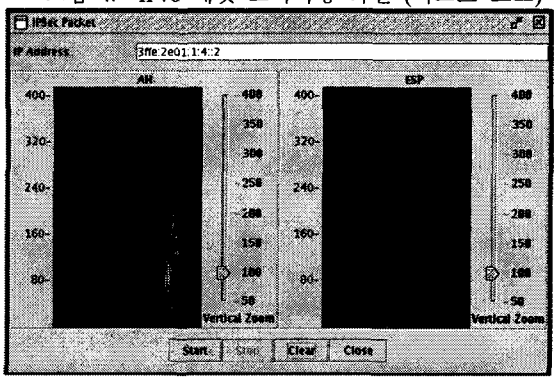

그림 5. IPv6 IPsec 트래픽 모니터링

참고문헌

[1] IETF, http://www.ietf.org
[2] S.Kent and R.Atkinson, Security Architecture for the Internet Protocol, RFC2401, Nov. 1998
[3] S.Kent and R.Atkinson, IP Authentication Header, RFC2402, Nov. 1998
[4] S.Kent and R.Atkinson, IP Encapsulating Security Payload, RFC2406, Nov. 1998
[5] D.Harkins, D.Correl, Internet Key Exchange, RFC2409, Nov. 1998
[6] USAGI Project, http://www.linux-ipv6.org/
[7] FreeS/WAN, http://www.ipv6.iabg.de/
[8] KAME, http://www.kame.net
[9] ISS, "Network and Host-based Vulnerability Assesment," http://documents.iss.net/ white_papers/nva.pdf
[10] J.H.Jeong, J.H.Nah, S.W.Sohn and J.T.Lee, "C-ISCAP: Controlled-Internet Secure Connectivity Assurance Platform," Proc. of the IEEE International Conference on Enterprise Information Systems(ICEIS2001), Vol. 2, pp.920-925, Setubal, Protugal
[11] ISS, 'Securing Operating Platforms: A solution for tightening system security," Jan. 1997