IPv4 및 IPv6 보안 패킷 분석기의 설계 및 구현

(A Design and Implementation of IPv4/IPv6 Security Packet Analyzer)

조 진 기*, 김 상 춘**, 이 상 호***
(Jin-Ki Cho · Sang-Choon Kim · Sang-Ho Lee)

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. 본 분석기의 목적은 IP 계층의 보안을 위해 IPsec엔진을 구현하고 탑재한 보안 호스트가 관련 표준에 적합하게 IPsec을 구현하였는지의 여부를 분석하기 위한 목적과, 해당 보안 호스트가 요구되는 보안성을 실제 제공하는지를 자동화된 방법으로 평가하기 위한 목적이다. 본 논문에서는 개발한 패킷 분석기를 이용하여 실제 IPsec엔진이 탑재된 보안 호스트에 대해 보안성을 평가한 결과도 함께 보인다.

Abstract In this paper, we design and implement real time IP security packet analyzer on IPv4 and IPv6 network. This packet analyzer sniffs and analyzes the packets generated by the protocols that are used by IPsec, IKE, IPv4 and IPv6 such as AH, ESP, ISAKMP, IP, ICMP and so on. The purpose of this analyzer is to check current security status of the network automatically. In this paper we provide implementation details and the examples of security evaluation by using our security packet analyzer system.

Key Words : IP 보안(IPsec), 보안패킷(Security Packet), 보안평가(Security Evaluation)

1. 서 론

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 Area의 IPsec Working Group을 중심으로 표준화가 진행 중이며, 현재 관련된 18개의 RFC 작성이 완료된 상태이다[1][2][3][4][5]. 현재 IPsec은 리눅스, FreeBSD, Window2000 등 여러 가지 플랫폼에서 구현되고 있으며, 리눅스 기반의 FreeS/WAN, FreeBSD 기반의 KAME 등 공개된 프로젝트도 다수 존재한다[6][7][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,

* 부산경상대학 멀티미디어컴퓨터과
** 삼척대학교 정보통신공학과
*** 충북대학교 전기전자컴퓨터공학부

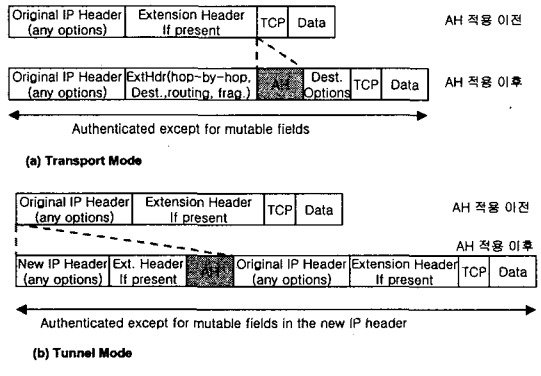
차세대 인터넷인 IPv6 패킷에 대하여도 실시간 수집 및 분석 기능을 제공한다. 또한 본 분석기는 IPsec 엔진에 대한 보안성을 평가하기 위한 자동화된 평가기능도 제공해 준다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 IPsec 소개, IP 계층의 보안 요구사항 그리고 기존의 패킷분석기에 대한 소개에 대한 내용을 기술한다. 3장에서는 보안 패킷 분석기의 설계에 대한 내용을 기술하며, 4장에서는 구현 및 실제 개발한 패킷 분석기를 이용하여 IPsec엔진이 탑재된 보안 호스트에 대해 보안성을 평가한 결과를 보인다. 마지막으로 5장에서 결론을 맺는다

2. 관련연구

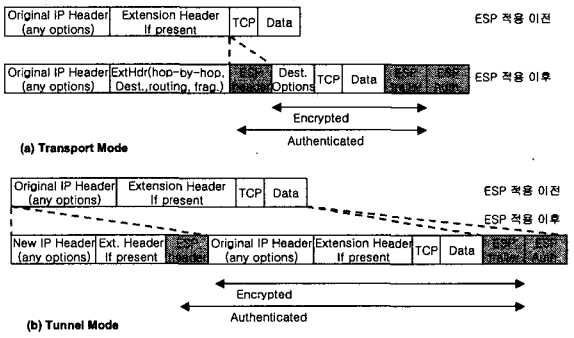
2.1 IPsec(IP Security)

IPsec(IP Security)[1][2]은 네트워크 계층에서 기밀성과 인증 서비스를 제공하기 위하여 개발된 프로토콜로서 IETF의 차세대인터넷(IPng)인 IPv6 개발 노력의 일환으로 추진되고 있는 인터넷 보안 기술이다. 현재 대다수의 IPsec구현은 IPv4에서 이루어지고 있으나 최근 IPv6도입의 필요성이 구체화되면서 IPv6에서의 IPsec구현에 대한 연구도 활성화 되고 있는 추세이다. 실제 IPv6 규격에 정의된 확장헤더에는 IPsec 프로토콜에 사용되는 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 헤더가 포함되어 있다.



<그림 1> AH 적용 패킷
<Fig. 1> AH packet

IPsec 엔진은 IP계층에서의 정보보호 서비스를 제공하기 위해 커널에 탑재되어 수행되며, Outbound 패킷의 경우 패킷을 암호화하고 인증 값을 계산하여 추가하는 등의 방법으로 패킷을 재구성하여 Ethernet 계층으로 내려 보내는 기능을 가지며, Inbound packet의 경우 암호화된 패킷을 복호화하고 인증 값을 검증하여 상위계층으로 올려 보내는 기능을 갖는다. <그림 1>과 <그림 2>는 original IP 패킷과 IPsec이 적용된 이후의 패킷의 형식을 보여준다. 각각은 IPv6 패킷을 예로 하여 작성한 그림이다.



<그림 2> ESP 적용 패킷
<Fig. 2> ESP packet

2.2 IP 계층의 보안 요구사항

IP 계층 즉 network layer에서 요구되는 5가지 보안 요구사항은 다음과 같다[2].

* 기밀성(confidentiality)
  메시지를 암호화하여 키를 가진 합법적인 사람을 제외하고는 중간에 불법적인 도청자가 메시지의 내용을 알아볼 수 없도록 하는 서비스이다.
* 비연결형 무결성(Connectionless integrity)
  메시지 변조를 할 수 없도록 하는 것으로 송신자가 메시지를 특정 수신자에게 전송할 경우 제3자가 불법적인 도청을 통해 전송한 메시지를 중간에서 가로챈 후 메시지를 변조하여 수신자에게 전송할 수 없도록 하는 서비스이다. 만약 공격자에 의해 메시지가 변조 되었다면 수신자 측에서는 이를 감지할 수 있어야 하며 해당 패킷을 폐기 하여야 한다.
* 데이터 원적지 인증(data origin authentication)
  서로를 직접 확인할 수 없는 인터넷상에서 상대에 대한 신뢰를 확보하기 위해 제공되는 서

비스이다. 즉 패킷의 송신자를 인증하기 위한 것으로써 만약 공격자에 의해 패킷의 송신지 주소가 변경된 경우 이를 감지 할 수 있어야 하며 해당 패킷을 폐기 하여야 한다.

* 접근 제어(access control)
  불법적인 제3자의 접근을 완전히 차단하거나, 서로 다른 중요도를 가지는 정보 및 시스템에 대해서 접근 권한을 달리 부여하여 정보를 보호하는 서비스이다.
* 재현공격방지 (Anti-replay)
  한 번 사용된 메시지를 다시 사용할 수 없도록 하는 서비스로써, 송신자가 수신자에게 보낸 메시지를 중간에서 제3자가 가로채고 있다가 메시지 수신이 일단 완료된 후에 가로챈 메시지를 다시 보내 공격하는 것을 막는 서비스이다.

2.2 보안패킷분석기 관련 기존연구

현재 유닉스의 TCPdump를 통해 IP packet을 실시간으로 capture 하여 볼 수 있다. 그러나 이 도구는 단지 IP 계층의 일반 패킷에 대한 간략한 정보만을 보여주며 IP 보안을 위한 패킷인 AH, ESP, ISAKMP등의 패킷을 구분하여 보여주지는 못하고 있다. 본 패킷 분석기는 각종 IP 계층의 보안 패킷을 수집하는 기능을 가지며 각각의 필드를 분류하여 사용자에게 display하는 구조를 갖는다. 또한 본 보안패킷분석기는 실시간으로 수집한 보안 패킷을 가공 및 전송한 후 대상 시스템에서 발생하는 패킷을 분석하여 대상 시스템이 적절한 보안 서비스를 제공하는지 평가하는 기능도 추가로 제공하고 있다.

보안 호스트에 대한 보안 취약성 분석 툴로 ISS Internet Scanner, Cisco의 Cisco Scanner 그리고 LANguard network&port scanner등이 있다[9][10][11]. 이러한 툴들은 호스트에 대한 스캐닝을 통해 운영체제의 취약점을 도출하고, 도출된 취약점을 참조하여 운영체제 패치 등의 작업을 하기 위한 도구이다. 그러나 이러한 도구들은 IPsec이 탑재된 특정 호스트에 대한 보안성을 평가하는 기능은 전혀 제공하지 못하고 있다. 물론 운영체제 자체의 취약점 분석을 위해서는 네트워크 스캐닝 툴이 효율적일 수 있겠으나, 본 논문에서 대상으로 하는 IP 계층에서의 보안성 평가는 네트워킹과 직접적으로 관련된 것이기 때문에 단순히 보안 스캐닝 방법을 통해서 수행할 수는 없는 것이다[12]. 또한 본 논문에서 제안하는 보안평가 방식 즉, 실시간으로 패킷을 수집, 가공, 재전송 그리고 분석을 통한 방법은 기존에 시도되지 않은 새로운 방법이라고 볼 수 있다.

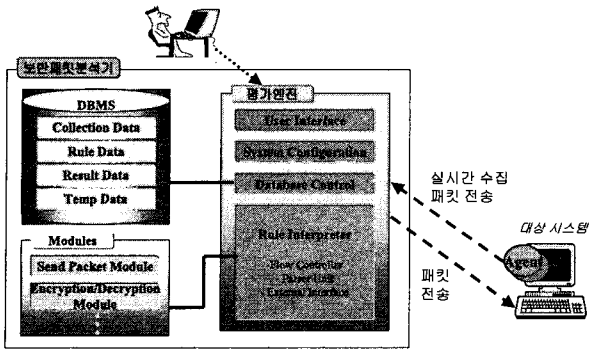
3. 보안패킷분석기의 설계

<그림 3>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.

3.1 패킷수집용 에이전트

패킷 수집용 에이전트는 실질적으로 대상시스템에서 네트워크 단자를 통해 송수신되는 패킷을 주어진 조건에 따라 실시간으로 수집하여 보안 패킷 분석기로 전달하는 역할을 수행한다. 보안 패킷 분석기는 START, STOP, HALT, RESUME의 4가지 명령을 에이전트에게 송신할 수 있으며, 수집할 패킷을 선별하기 위한 option 값을 함께 전송할 수 있다. 각 명령의 의미는 다음과 같다.

- PING : 에이전트와의 통신상태 점검
- START : 패킷 수집을 시작하라는 명령. option 정보도 함께 전송한다.
- STOP: 패킷 수집을 종료하고 시스템과의 접속을 해지하라는 명령.
- HALT: 패킷 수집을 일시 중지.
- RESUME: 패킷 수집을 계속 수행.
- OPT : Option 값 변경. option 정보를 새로이 전송한다.



<그림 3> 보안 패킷 분석기의 구조

<Fig. 3> Architecture of Security Packet Analyzer

패킷 수집을 위한 option 값은 다음과 같이 정의된다.

- ip_packet : IP packet 전체를 수집
- src ip1 dst ip2 : 수집할 packet의 source IP와 destination IP 지정. all로 지정도 가능함.
- ip6 proto protocol : IP 헤더의 nexthdr 값이 protocol인 packet 만을 수집
- ip6 protochain protocol : IP 헤더 chain 중에 protocol에 해당하는 packet 만을 수집
- source_ip source_address : source IP가 source_address와 일치하는 packet 만을 수집
- dest_ip destination_address: : destination IP가 destination_address와 일치하는 packet 만 수집
- icmp_type type : ICMP 패킷 타입이 type과 일치하는 패킷만 수집

IP 보안 패킷 분석기과의 접속이 이루어지면 에이전트는 WAIT 상태에서 시스템으로부터의 명령을 기다린다. START 명령이 수신되면 상태를 ACTIVE로 전이시키고 패킷 스니핑을 위한 준비 작업을 수행한다. 이는 PCAP 라이브러리를 초기화하는 작업을 포함한다. 에이전트가 ACTIVE 상태에서는 7ms 마다 PCAP 함수를 호출하여 패킷을 스니핑한다.

3.2 평가엔진

평가엔진은 <그림 3>에서 볼 수 있듯이, User Interface, System Configuration, Database Control, Rule Interpreter로 구성된다.

User Interface는 사용자와의 interface를 담당하며, 실시간으로 수집된 패킷을 분석하여 별도의 GUI 화면으로 구성하여 사용자에게 display 해주는 기능도 처리한다. 4장의 <그림 4>에서 실시간으로 수집한 패킷에 대한 display window를 볼 수 있다.

System Configuration은 세부적으로 Access Control, Agent Registration, Module Registration, Directory Setup 모듈로 나눌 수 있다. Access Control은 본 시스템 사용을 위한 사용자 인증을 수행하는 부분이다. Agent Registration에서는 에이전트 이름, 에이전트타입, 데이터베이스 이름, 현재 에이전트가 설치되어 있는 호스트 정보 등을 등록한다. Module Registration에서는 평가 룰에서 사용하게 될 각 모듈에 대한 정보를 등록하는 곳으로 모듈 이름, 모듈 설치 경로, 모듈에 대한 설명 등을 등록한다. Directory Setup에서는 평가 룰 수행 시 사용되는 임시 데이터와 관리자가 임의적으로 만든 패킷 데이터가 저장될 Directory Path를 정의한다.

<그림 3>의 Database Control은 DB내의 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. 실시간으로 에이전트로부터 전송 받은 패킷은 사용자의 설정에 따라 수신과 동시에 GUI로 display 되거나 바로 DB로 저장된다. 두 가지 모두의 경우도 가능하다. <그림 3>의 Rule Interpreter에 대한 내용은 3.3절에서 기술한다.

3.3 룰 해석기

평가 엔진내의 룰 해석기는 평가 룰을 DBMS의 룰 데이터(Rule Data)로부터 순차적으로 읽은 다음, 수행절차에 따라 명령을 해석하고 실행하는 기능을 갖는다. 실질적으로 대상 시스템에 대한 보안성 평가를 수행하는 객체가 룰 해석기이다.

룰 해석기는 Flow Control, Parser 그리고 External Interface로 구성된다. 룰 해석기의 파서(parser)는 룰 데이터의 프로그램 필드에 저장되어 있는 평가 프로그램에 대한 문법검사를 수행 한 후 문법

오류가 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 DB조작, 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.

표 1. 외부인터페이스
Table 1. External Interface

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

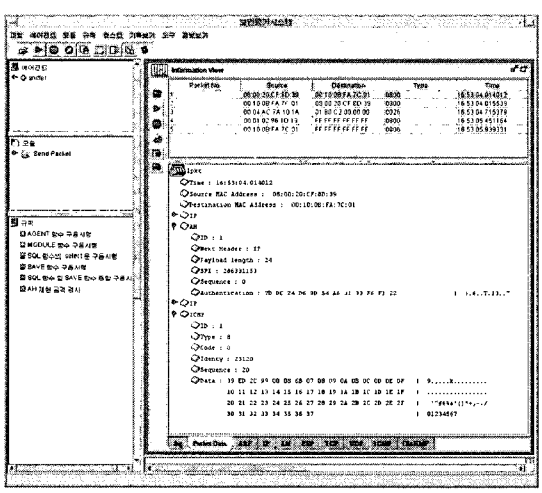
<표 1>의 MODULE 함수와 AGENT 함수의 파라미터로 사용되는 'command'에 포함되는 명령어로는 현재 sniffer와 sndpkt가 구현되어 있다. sniffer는 주어진 룰에 맞는 packet을 네트워크상에서 또는 타겟 호스트의 에이전트로부터 혹은 시스템 내부의 DB로부터 스니핑하는 명령어이다. 현재 Sniffer로 모니터링 할 수 있는 프로토콜로는 ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP가 있다. Sndpkt는 시스템 내에 저장된 패킷이나 현재 편집한 패킷을 Raw Socket을 이용하여 목적 호스트로 전송하기 위한 명령어이다. 현재 Sndpkt로 전송할 수 있는 프로토콜로는 ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP가 있다.

3.4 DBMS

보안 패킷 분석기에서 사용되는 DB로는 Collection Data, Rule Data, Result Data, Temp Data 가 있다. Collection Data는 에이전트로부터 전송 받은 각종 프로토콜 데이터를 저장하는 곳이며, Ethernet, ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP 프로토콜에 대한 테이블을 보관, 관리한다. Rule Data는 평가에 대한 룰을 저장하는 곳으로, Database Control의 Rule DB Control에 의해 평가 룰이 정의되거나 수정 및 삭제되며, 룰 해석기에 의해 평가 룰이 해석되고 수행되어진다. Result Data는 평가 룰이 수행된 결과를 저장하는 곳으로, Rule Interpreter의 Flow Control에 의해 저장되어진다.

4. 구 현

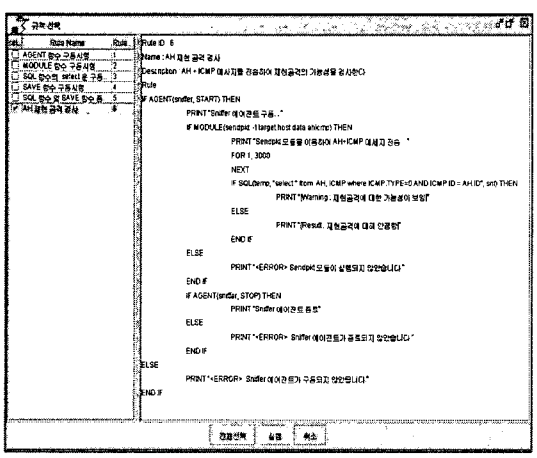
본 논문에서 제안한 IP 보안 패킷 분석기는 Windows와 UNIX 환경에서 수행이 가능하며 Java와 C언어로 구현되었다. DB는 my-sql로 구현하였다. <그림 4>는 패킷 분석기의 메인 화면이다.



<그림 4> 실시간으로 수집된 AH 패킷 (IPv4)
<Fig. 4> Collected IPv4 AH packet

<그림 4>에서 좌측의 세 개의 창은 등록된 에

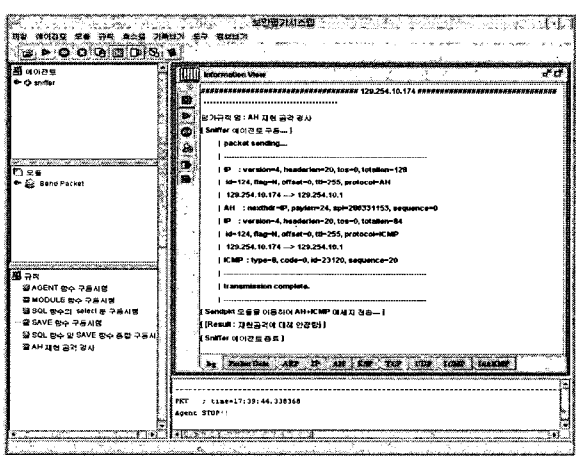
이전트, 모듈, 룰의 리스트를 tree형식으로 보거나 선택할 수 있는 창이다. 우측 상단의 창은 실행 로그 파일이나 에이전트에서 오는 각 프로토콜의 수집데이터를 보여주는 창이다.창 하단의 log 는 log 기록보기를 선택하기 위한 버튼이며, Packet data는 수집된 packet 전체를, ARP는 수집된 packet중 ARP 패킷만, AH는 수집된 packet중 AH packet만 보기 위한 버튼이다. 나머지 IP, TCP, UDP, ICMP, ISAKMP모두 동일한 방식으로 원하는 프로토콜 packet만을 볼 수 있다. 이처럼 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 4>의 '규칙' 메뉴는 룰을 입력, 수정, 선택, 삭제 할 때 사용된다.



<그림 5> 샘플 룰
<Fig. 5> Sample Rule

본 시스템은 2장에서 언급된 IP 계층에서의 5가지 보안 요구사항을 대상 시스템이 만족하는 지를 평가하기 위해 각각에 대한 보안평가 룰을 정의하여 라이브러리 형태로 제공한다. 각각의 보안성 평가방법을 요약하면 다음과 같다.

- 기밀성(confidentiality) : 전송중인 암호화된 ESP 패킷을 수집하여 메시지의 내용을 알아볼 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 ICV값을 재 계산하여 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 SN을 생성하거나 수집한 SN을 변경하여 전송하고, 그 결과를 분석한다.



<그림 6> 평가결과 log
<Fig. 6> Evaluation Log

한가지 예로 <그림 5>의 경우에는 재현공격방지 기능에 대한 평가 룰을 보여준다. <그림 5>에 정의된 룰을 간단히 요약하면 다음과 같다.

시스템 구성 :
호스트 A-게이트웨이 A-게이트웨이 B-호스트 B

항목 1 : Tunnel AH의 재현공격방지 기능 테스트 룰 :
절차 1. 호스트 A에서 Tunnel AH가 적용된 ICMP 패킷을 생성하여 호스트 B로 전송한다.

절차 2. 보안패킷분석기는 이 패킷을 실시간으로 sniffing하여 보관한다.

결과 3. 호스트 B는 이에 대한 ICMP 응답 패킷을 호스트 A에게 전송한다.

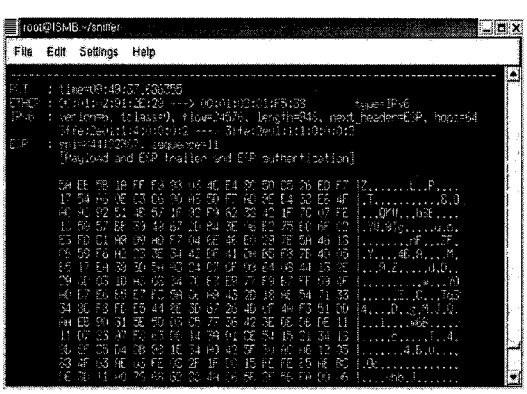
절차 4. 보안패킷분석기는 절차 2에서 수집한 동일한 패킷을 호스트 B에게 전달한다. 이때 원적지의 주소는 원 패킷과 동일하게 호스트 A이다.

절차 5. 보안패킷분석기는 에이전트로부터 실시간으로 전달되는 패킷을 분석하여 호스트 B가 재전송한 패킷에 대한 응답 패킷을 호스트 A로 보내는지를 확인한다.

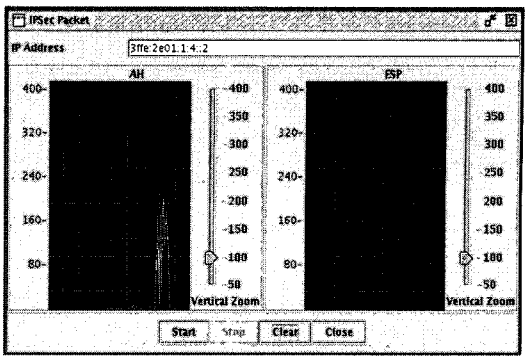
절차 6. 만약 호스트 B가 응답패킷을 보냈다면, 재현공격방지 기능에 취약성이 있음을 보고한다.

<그림 6>에서는 <그림 5>에 정의된 룰을 입력으로 하여 보안패킷분석기 시스템이 대상 시스템의 재현공격방지 기능을 테스트한 결과를 보여준다. 테스트 결과 재현공격 방지 기능을 제공하는 것으로 평가되었다. 평가한 대상 시스템은 리눅스 기반으로 본 기관에서 개발이 진행 중인 IPv4/IPv6 IPsec 통합 시스템이다.

또한, 본 연구에서는 시스템에 IPsec의 기능이 정확히 구현되었는지를 분석하기 위해 40여 가지의 시험 항목을 정의하여 테스트를 진행 중에 있다. <표 2>는 정의한 시험항목의 일부를 보여준다.



<그림 7> IPv6 패킷 모니터링
<Fig. 7> IPv6 Packet Monitoring



<그림 8> IPv6 IPsec 트래픽 모니터링
<Fig. 8> Traffic Monitoring of IPv6 IPsec packet

본 패킷 분석기는 IPv6 패킷에 대해서도 패킷 분석기능 및 트래픽 모니터링 등의 기능을 갖는다. <그림 7>은 IPv6 패킷 분석기에 의해 수집된 ESP패킷을 텍스트 형태로 보여준다. <그림 8>은 IPv6 IPsec 통신 패킷의 트래픽을 실시간으로 모니터링 하는 화면이다. <그림 8>에서 AH가 적용된 패킷의 발생 정도를 확인할 수 있다.

표 2. IPsec 구현정확성에 대한 평가항목의 일부
Table 2. A Part of Evaluation Item

1. Inbound ESP packet with Fragmentation (Authentication: HMAC-SHA1, Encryption: 3DES-CBC) H1 ====> H2 Send Fragmented TCP message (applying ESP)
2. Inbound Tunnel AH packet (Authentication: HMAC-MD5) H1 => GW1 => GW2 => H2 |-Tunnel-| H1<= GW1<= GW2 <= H2 ICMP Echo request (Applying tunnel AH between GW 1 and 2) ICMP Echo reply (Applying tunnel AH between GW 2 and 1)
3. Inbound AH+ESP (Policy=Drop) H1 => H2 ICMP Echo request (with AH+ESP)

```
H1 <= X = H2
      No ICMP Echo reply  (drop packet)

4 Detect modified AH packet
 (Modification of IP dst.)
 H1  ==> H2   ICMP Echo request
          (with AH, modification of IP dst.)
 H <=X= H2  No ICMP Echo reply

5. Outbound AH+ESP packet with SA bundles
 H1 => GW1 => GW2 => H2
       |- ESP SA-|
  |------AH SA---------|
 H2 <== GW1 <== GW2 <== H1
       |-ESP SA-|
  |------AH SA---------|

  ICMP Echo request (with SA bundles)
  ICMP Echo reply (with SA bundles)
```

5. 결 론

본 논문에서는 IPsec엔진의 보안성을 평가하기 위한 자동화된 규칙기반 보안평가시스템을 설계 및 구현 하였다. 제안하는 보안평가시스템은 ETRI에서 개발중인 C-ISCAP (Controlled Internet Security Connectivity Assurance Platform)이라고 명명한 통합 IPsec엔진에 대한 보안성을 평가하고 디버깅하기 위한 목적으로 개발되었으나, 독립적으로 존재하는 평가시스템으로 C-ISCAP 뿐 아니라 기타 현재 개발중인 IPsec엔진에 대해서도 아무런 변경 없이 평가를 수행할 수 있다.

본 평가시스템은 다음과 같은 특징을 갖는다.

- 네트워크 상의 다양한 프로토콜들의 패킷을 수집하고 분석하는 기능을 갖는다.
- 에이전트를 사용하여 원거리 호스트에 대한 평가가 가능하다.
- 규칙기반으로 동작하므로 자동화된 보안성 평가가 가능하다.
- 규칙에 대한 문법을 단순화 하여 손쉽게 규칙을 정의할 수 있다.
- 평가규칙에 필요한 기능을 모듈로 관리하므로 확장이 용이하다.

본 논문에서 제안하는 보안평가 방식 즉, 실시간으로 패킷을 수집, 가공, 재전송 그리고 분석을 통한 방법은 기존에 시도되지 않은 새로운 방법이라고 볼 수 있다.

현재 보안평가시스템은 100% 자동화 되지는 않았으며 일부 수동 작업이 필요하며, 계속 보완해 나갈 예정이다. 향후 과제로서 보안평가시스템의 규칙을 추가하여 다양한 방식의 보안성 평가가 가능하도록 확장하는 작업이 필요하다. 현재 평가시스템은 Java와 DBMS를 이용하여 구현되어서 규칙을 수행하는 시간이 오래 걸리므로 평가 대상 호스트와의 연결이 끊어지는 현상이 종종 발생한다. 이러한 속도문제를 해결하기 위한 연구도 현재 진행중이다. 또한 기타의 개발된 다른 IPsec 엔진에 대한 테스트를 수행하는 작업도 현재 진행중이다.

참 고 문 헌

[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," ISS, ISS Internet Scanner, http://www.iss.net/

[10] Cisco Scanner, http://www.cisco.com/en/US/products/sw/secursw/ps2134/tsd_products_support_eol_series_home.html

[11] LANguard Network&Port scanner, http://www.gfi.com/languard/lanscan.htm

[12] 정한열, "효율적인 네트워크 보안시스템 구축에 관한 연구", 한국컴퓨터정보학회논문지, 제3권 4호, pp.120-125 , 1998.

조 진 기 (Jin-Ki Cho)

- 정회원
- 1986년2월 : 충북대학교 계산통계학과 (이학사)
- 1988년 2월 : 숭실대학교 전자계산학과 (공학석사)
- 1998년 8월 : 충북대학교 전자계산학과 (박사수료)
- 1991년 8월 ~ 현재 : 부산경상대학 멀티미디어컴퓨터과 조교수
- 관심분야 : 정보보호, 프로토콜 엔지니어링, 컴퓨터네트워크

김 상 춘 (Sang-Choon Kim)

- 정회원
- 1986년 8월 : 한밭대학교 전자계산학과 (이학사)
- 1989년 2월 : 청주대학교 전자계산학과 (이학석사)
- 1999년 8월 : 충북대학교 전자계산학과 (이학박사)
- 2001년 2월 ~ 현재 : 삼척대학교 정보통신학과 조교수
- 관심분야 : 네트워크 보안, 정보보호

이 상 호 (Sang-Ho Lee)

- 정회원
- 1976년 2월 : 숭실대학교 전자계산학과 (공학사)
- 1981년 2월 : 숭실대학교 전자계산학과 (공학석사)
- 1989년 2월 : 숭실대학교 전자계산학과 (공학박사)
- 1982년 2월 ~ 현재 : 충북대학교 전가전자컴퓨터공학부 교수
- 관심분야 : 네트워크보안, 프로토콜엔지니어링, 네트워크구조