IPv6 네트워크 계층의 보안성 평가를 위한 평가규칙 표기 언어 및 평가 수행기의 설계

권 혁 찬[†] · 김 상 춘[††]

요 약

현재 차세대 인터넷 IPv6 네트워크의 보안을 위한 IPsec(IP Security)의 구현에 대한 연구가 매우 활성화 되고 있는 추세이다. 그러나 현재 IPv6 네트워크 계층의 보안성을 평가하기 위한 자동화된 도구나 평가 방법론 등에 관한 연구는 매우 미진한 상황이다. 본 논문에서는 IPv6 기반 IPsec이 적용된 보안 시스템의 보안성을 평가하기 위해, 보안성 평가 항목을 정의할 수 있는 평가규칙표기언어를 설계하고 평가규칙표기언어를 이용하여 정의된 평가규칙을 해석하고 실행하기 위한 평가규칙 처리 도구를 제안한다. 평가규칙 처리도구는 사용자 인터페이스 부, 평가규칙 모듈 부, DBMS부로 구성되며 평가 대상 시스템에 탑재된 에이전트와의 협력을 통해 평가를 수행하는 구조를 갖는다.

A Design of SERDL(Security Evaluation Rule Description Language) and Rule Execution Engine for Evaluating Security of IPv6 Network

HyeokChan Kwon[†] · SangChoon Kim[††]

ABSTRACT

Recently, many projects have been actively implementing IPsec on the various Operating Systems for security of IPv6 network. But there is no existing tool that checks the IPsec-based systems, which provide IPsec services, work properly and provide their network security services well in the IPv6 network. In this paper, we design SERDL(Security Evaluation Rule Description Language) and rule execution tool for evaluating security of the IPv6 network, and we provide implementation details. The system is divided into following parts : User Interface part, Rule Execution Module part, DBMS part and agent that gathering information needed for security test.

키워드 : IPv6 네트워크(IPv6 network), 보안규칙표기언어(Security Evaluation Rule Description Language), 규칙처리기(Rule Execution Engine), IPsec

1. 서 론

현재 인터넷 주소의 고갈문제가 매우 심각한 문제로 대두되면서 IPv6를 도입하고자 하는 연구가 다각적으로 진행 중에 있다. 현재 IPv6 프로토콜에 대한 표준화는 IETF에 의해 이미 완료된 상태이며, 현재 많은 업체와 기관에서 IPv6 기능을 탑재한 통신 단말 및 운영체제를 개발 완료 하였거나 개발 중에 있다. 또한 시험망을 구축하여 운영하는 기관도 있다. 그러나 IPv6와 관련하여 더 많은 경험과 구현이 요구되고 있는 실정이다. 그 중 한가지 분야가 바로 보안 분야이다.

IPv6의 보안을 위해 제안된 프로토콜로 IPsec(IP Security)이 있다. IPsec은 네트워크 계층에서 기밀성과 인증 서비스를 제공하기 위하여 개발된 프로토콜로서 IETF의 차세대인터넷(IPng)인 IPv6 개발 노력의 일환으로 추진되고 있는 인터넷 보안 기술이다[1-3]. 현재 대다수의 IPsec구현은 IPv4에서 이루어지고 있으나 최근 IPv6도입의 필요성이 구체화되면서 IPv6에서의 IPsec구현에 대한 연구도 활성화 되고 있는 추세이다.

그러나 현재 IPv6 기반 IPsec 시스템에 대한 보안성을 평가하기 위한 자동화된 도구는 나와있지 않으며 이에 대한 보안평가 방법론 등에 관한 연구도 현재 미진한 상태이다.

본 논문은 IPv6 네트워크에서 정보보호 서비스를 제공하기 위해 IPsec 엔진을 탑재한 보안 시스템들 - 보안 호스트, 보안 게이트웨이 - 의 보안성을 평가하기 위한 방법에 대한 것으로, 보안평가 방법을 정의하기 위한 평가규칙표기언어를 설계하고 평가규칙표기언어를 이용하여 정의된 평

† 준 회 원 : 한국전자통신연구원 정보보호연구단 선임연구원
†† 종신회원 : 삼척대학교 정보통신공학과 교수
논문접수 : 2004년 1월 9일, 심사완료 : 2004년 6월 10일

가규칙을 해석하고 실행하기 위한 평가규칙 처리 도구를 제안한다. 본 시스템을 통해 평가 대상 시스템의 보안 위협 요소를 도출함으로 더욱 안전성을 보장하는 시스템을 개발할 수 있는 많은 장점을 제공할 수 있는 효과가 있다. 본 연구의 결과인 보안 평가규칙 처리 도구는 안전성을 고려한 IPv6 기반의 보안 시스템을 개발하는데 많은 도움을 줄 수 있을 것이며, 개발된 보안 시스템에 대한 신뢰성을 측정하기 위해서도 활용이 가능할 것이다.

본 논문에서 제안하는 보안성 평가 수행 절차는 크게 다음과 같은 단계로 이루어 진다. 보안 관리자가 평가규칙 표기 언어를 이용하여 보안평가규칙을 작성하거나 보안 관리자가 기존에 작성된 평가규칙을 불러온 후 필요하다면 평가규칙을 편집한 후, 평가규칙의 실행을 요구하는 1단계. 평가규칙 처리 모듈이 요구 받은 평가규칙의 문법을 검사하는 2단계. 평가규칙처리모듈의 규칙 실행기가 5개의 실행 유닛과 DBMS를 이용하여 요구된 평가규칙을 실행하는 3단계. 이 단계에서는 또한 평가를 수행하기 위해 평가 대상 서버에서 송수신되는 패킷을 실시간으로 평가서버로 전달해 주는 에이전트와 협력한다. 평가 결과를 DB에 저장하고 사용자에서 디스플레이 하는 4단계. 이렇게 총 네 개의 단계를 거쳐 보안 평가를 수행하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로서 IPv6, IPsec 그리고 네트워크 계층의 보안평가 연구에 대해 다룬다. 그리고 3장에서 설계한 평가규칙 표기언어에 대해 설명하며 4장에서 평가규칙 처리 도구에 대해 설명한다. 그리고 5장에서 개발한 평가규칙처리 도구 프로토타입을 이용하여 실제 보안성 평가를 수행한 사례를 소개하고 마지막 6장에서 결론을 맺는다.

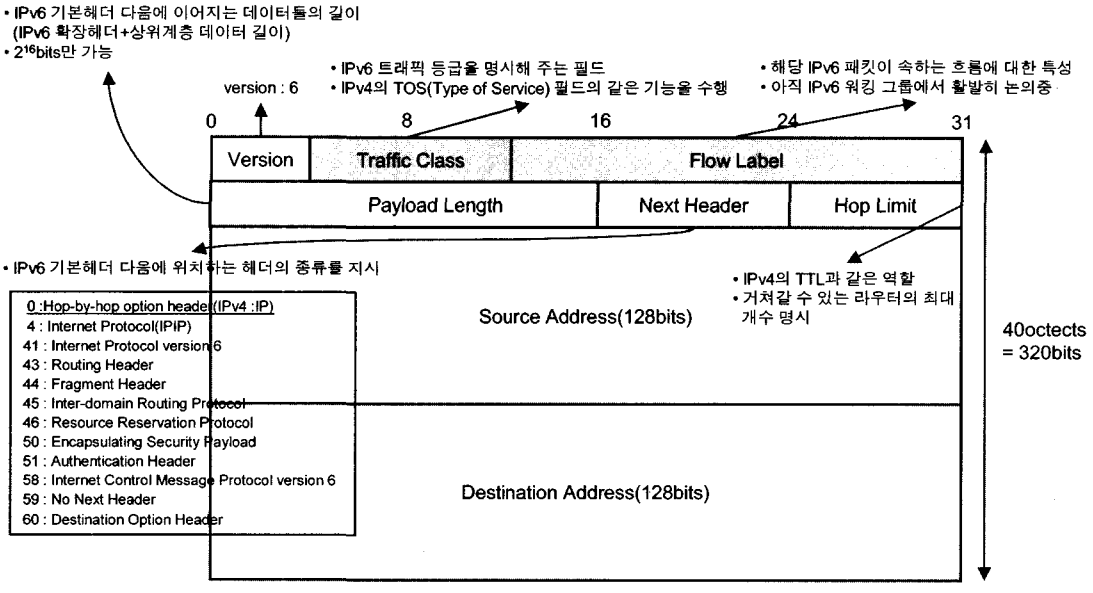
2. 관련 연구

2.1 IPv6 네트워크

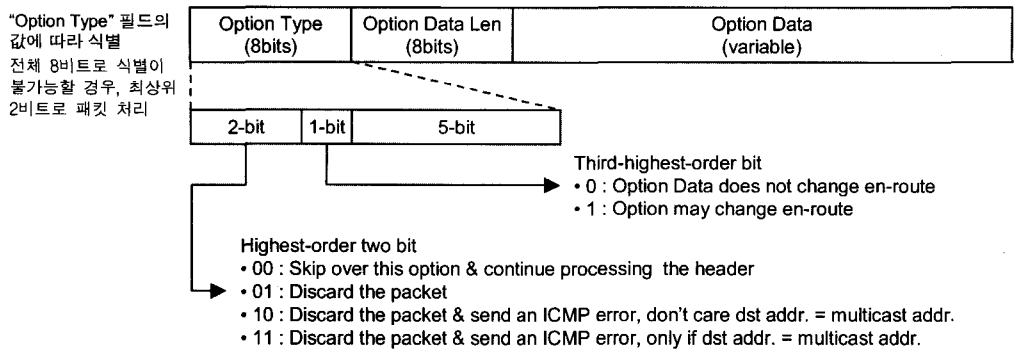
인터넷 주소의 고갈문제가 매우 심각한 문제로 대두되면서 IPv6를 도입하고자 하는 연구가 다각적으로 진행 중에 있다. 한국의 경우에도 정보통신부에서는 IPv6의 도입시기를 2002년부터 점차적으로 도입하여 2011년에서는 IPv6 순수망으로 완전 변환할 것으로 예측하며 이에 대비한 연구를 활성화 하고자 하고 있다[4-5].

IPv4와 비교하여 IPv6 네트워크의 특징은 다음과 같다[1].

- 확장된 주소 체계 및 공간 : 주소 공간을 32비트에서 128비트로 늘림
- 헤더 형식의 단순화 : 패킷 처리 비용을 줄이고 IPv6 헤더의 대역폭 비용을 제한하기 위해 일부 IPv4 헤더 필드가 삭제되거나 확장 헤더로 되어 선택적으로 사용하게 되었다. 주소 필드는 IPv4의 두 배인 40바이트로 확장되었지만, 전체 필드 수를 12개에서 8개로 단순화 시킴으로서 오히려 기본적인 처리 속도를 개선하는 효과를 갖는다. (그림 1)과 (그림 2)에서 IPv6 기본 헤더와 확장 헤더의 형식을 볼 수 있다.
- 확장 및 옵션에 대한 지원 향상 : IPv4 헤더의 옵션 필드에 사용되던 헤더들이 모두 확장헤더로 옮겨 짐.
- 플로우 레이블링 기능 : 송신자가 디폴트가 아닌 서비스 품질(QoS) 또는 실시간 서비스와 같은 특별 처리를 요청하는 특정 트래픽 플로우(flow)에 속하는 패킷을 레이블링(labeling)할 수 있다.
- 인증 및 사생활 보호 기능 : 인증, 데이터 무결성 및 데이터 기밀 유지를 지원하기 위해 확장 헤더를 규정하고 있다.



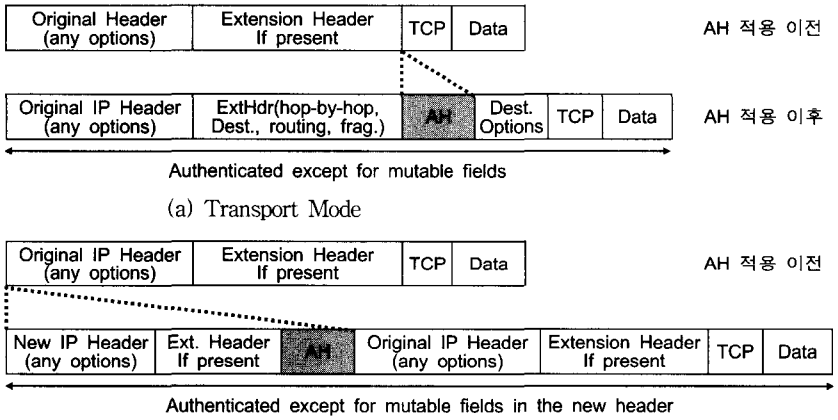
(그림 1) IPv6 기본헤더 형식



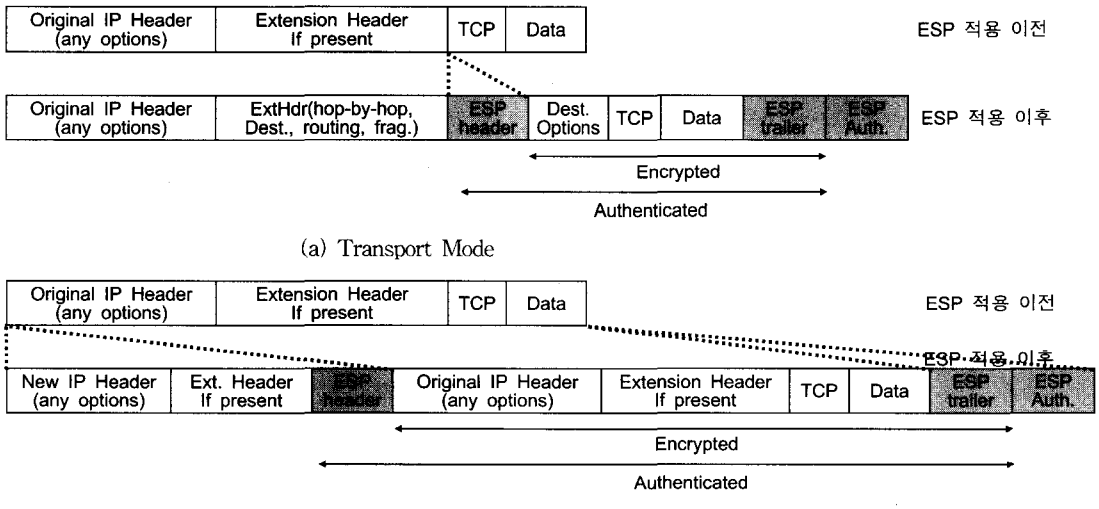
(그림 2) IPv6 확장헤더 형식

2.2 IPsec(IP Security)[2, 6, 7]

IPsec(IP Security)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 3) AH가 적용된 패킷



(그림 4) ESP가 적용된 패킷

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 3)과 (그림 4)는 original IPv6 패킷과 IPsec이 적용된 이후의 패킷의 형식을 보여준다.

2.3 관련 보안성 평가 도구

현재 IPv6 상의 일부 플랫폼에서 IPsec을 구현 중에 있으나 아직까지 IPsec 기반 시스템에 대한 보안성을 평가하기 위한 자동화된 도구는 나와있지 않다. 보안 호스트에 대한 보안 취약성 분석 툴로 ISS Internet Scanner, Cisco의 Cisco Scanner 그리고 LANguard network&port scanner등이 있으며, 이러한 툴들은 호스트나 네트워크에 대한 스캐닝을 통해 운영체제의 취약점을 도출하는 기능을 제공하며, 도출된 취약점을 참조하여 운영체제 패치 등의 작업을 하게 된다. 그러나 이러한 도구들은 IPsec이 탑재된 특정 호스트에 대한 보안성을 평가하는 기능은 제공해 주지 못하고 있는 실정이다[9-11]. 물론 운영체제 자체의 취약점 분석을 위해서는 네트워크 스캐닝 툴이 효율적일 수 있겠으나, 본 논문에서 대상으로 하는 layer 3에서의 보안성 평가는 네트워크 통신과 직접적으로 관련된 것이기 때문에 단순히 보안 스캐닝 방법을 통해서 수행할 수는 없는 것이다. 본 논문에서는 보안성 평가를 위해 실시간으로 전송되는 패킷을 수집하여 가공 후 재전송하는 방식을 제안하고 있으며, 이는 layer 3에서의 보안성 평가에 매우 적합한 방식이라 할 수 있겠다. 또한 본 논문에서 제안하는 방식들 즉, 설계한 보안평가규칙언어를 이용하여 평가규칙을 정의하는 방식, 평가규칙 처리도구를 이용하여 평가를 수행하는 방식, 평가 서버에 탑재된 에이전트와의 협력을 통한 평가방식 등은 기존의 방식과는 매우 다른 새로이 제안되는 방식이다. 이러한 방식의 장점은 결론 부분에 추가로 기술하였다. 또한 기존의 스캐닝 툴은 IPv4 기반으로 동작하는 반면 제안된 시스템은 IPv6 기반으로 동작한다는 것도 차이점이다. 향후 IPv6 망으로의 진화가 예상되며 이에 따른 요소 기술들이 활성화 될 것으로 기대되는 현재 분위기를 고려해 볼 때, IPv6 기반의 보안평가 기술도 큰 의미를 갖는 다고 볼 수 있다. 본 논문에서 제안한 평가 도구는 안전성을 고려한 IPv6 기반의 IPsec 시스템을 개발하는데 많은 도움을 줄 수 있을 것이며, 개발된 보안 호스트에 대한 신뢰성도 측정하기 위해서도 활용이 가능할 것이다.

3. 평가규칙 표기언어

본 장에서는 본 논문에서 설계한 보안성 평가규칙을 정의하기 위한 평가규칙 표기언어에 대해 기술한다. <표 1>은 평가규칙 표기언어의 주요 구문들을 보여준다. 각 구문을 설명하면 다음과 같다.

- RULE NAME 구문 : 규칙의 이름을 정의한다.
- DESCRIPTION 구문 : 규칙에 대한 설명을 기술한다.
- START_EVALUATION 구문 : 평가의 시작을 알리는 구문.
- END_EVALUATION 구문 : 평가의 끝을 알리는 구문.
- IF 구문 : IF 조건 구문.
- LOOP 구문 : 반복문 정의 구문. 반복문을 일정 시간동안 반복 할 수 있는 time 이라는 키워드도 정의 되었다. (예) LOOP time > 50ms : 50ms 동안 반복문 실행
- SAVE 구문 : DB에 저장된 패킷 중 조건에 맞는 패킷을 파일로 저장하거나 파일의 내용을 DB에 추가하기 위한 구문. 저장된 파일은 패킷 가공 및 전송에 사용될 수 있다.
- CAPTURE 구문 : 실시간으로 패킷을 수집하여 정의된 DB 또는 파일에 저장하기 위한 구문. CAPTURE 구문의 동작은 query에 정의된 target system의 주소에 탑재된 에이전트로 해당 명령을 전송하고 그 결과를 수신하여 저장하는 방법으로 동작하게 된다. CAPTURE 구문의 query에는 또한 수집할 패킷의 조건을 기술할 수 있다. query문에서 사용 가능한 현재 정의된 keyword는 다음과 같다.
  - ip_packet : IP packet 만을 수집
  - ip6 proto *protocol* : IP 헤더의 nexthdr 값이 *protocol*인 packet 만을 수집
  - ip6 protochain *protocol* : IP 헤더 chain 중에 *protocol*에 해당하는 packet 만을 수집
  - source_ip *source_address* : source IP가 *source_address*와 일치하는 packet 만을 수집
  - dest_ip *destination_address* : destination IP가 *destination_address*와 일치하는 packet 만을 수집
  - icmp_type *type* : ICMP 패킷 타입이 *type*과 일치하는 패킷만 수집
- SEND 구문 : filename에 저장된 패킷을 target 시스템으로 전송하기 위한 구문.
- EDIT_PACKET 구문 : fromfile에 저장된 패킷을 edit_option에 정의된 대로 가공하여 tofile로 저장하기 위한 구문.

〈표 1〉 평가규칙 표기언어의 주요 키워드

키 워 드	문 법
RULE_NAME	RULE_NAME : *strings*
DESCRIPTION	DESCRIPTION : *strings*
START_EVALUATION	START_EVALUATION
END_EVALUATION	END_EVALUATION
LOOP	LOOP *conditions* *statements ...* END LOOP

IF	IF conditions THEN
	statements..
	[ELSE]
	statements..
	ENDIF

conditions	*condition* {[AND | OR] *condition*}*
SAVE	SAVE (*filename, query, DBname*) SAVE (*DBname, query, filename*)
CAPTURE	CAPTURE (DBname, query) CAPTURE (filename, query)
SEND	SEND (filename, target)
EDIT_PACKET	EDIT_PACKET(fromfile, edit_option, tofile)
CHECK_PACKET	CHECK_PACKET(*filename, check_option*)
CHECK_FILE	CHECK_FILE(*filename*)
IPSEC_PROC	IPSEC_PROC(*fromfile, IPsec_option, tofile*)
BREAK	BREAK
PRINT	PRINT *display statement*
DELAY	DELAY *time*
COMMENT	// … or /* … */

- CHECK_PACKET 구문 : 패킷의 의미를 분석하기 위한 구문이다. 전달받은 패킷이 정상적으로 IPsec 처리가 되었는지 검사하거나 패킷을 가공하기 위한 패킷의 정보를 추출하기 위해 사용되는 구문이다.
- CHECK_FILE 구문 : filename에 해당하는 파일에 데이터가 저장되어 있는지 여부를 체크한다.
- IPSEC_PROC : IPsec 처리를 하기 위한 구문이다. fromfile에 있는 패킷에 대해 IPsec_option에 정의된 대로 IPsec처리하여 tofile로 저장하기 위한 구문이다.
- RECAL_ICV sa : 미리 정의된 SA를 이용하여 ICV 값을 재계산한다.
  - DECRYPT sa : 미리 정의된 SA를 이용하여 암호화된 패킷을 해독한다.
  - ENCRYPT sa : 미리 정의된 SA를 이용하여 패킷을 암호화 한다.

  SA값은 사용자가 임의로 설정해 놓은 값을 사용한다.
- BREAK : loop을 빠져 나가기 위한 구문
- PRINT 구문 : 메시지를 GUI로 디스플레이 하는 구문
- DELAY : time ms동안 시간 지연하고 동작을 정지한다.
- COMMENT : // 또는 /* 와 */ 을 사용하여 주석을 단다.

4. 평가규칙 처리 도구

4.1 기능 및 보안 요구사항

네트워크 계층 즉 layer 3에서 요구되는 보안 요구사항은 다음과 같다[2]. 아래의 다섯 가지 요구사항은 IETF 표준 문서인 RFC 2401,2402,2406을 참조하여 작성한 것이다.

- 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 폐기하여야 한다.

- 데이터 원적지 인증(data origin authentication)

서로를 직접 확인할 수 없는 인터넷상에서 상대에 대한 신뢰를 확보하기 위해 제공되는 서비스이다. 즉 패킷의 송신자를 인증하기 위한 것으로써 만약 공격자에 의해 패킷의 송신지 주소가 변경된 경우 이를 감지 할 수 있어야 하며 해당 패킷을 폐기하여야 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.

상기의 보안 요구사항을 만족하는지를 평가하기 위해 필요로 하는 기능 요구사항은 <표 2>와 같다.

〈표 2〉 보안 평가를 위한 기능 요구사항 항목

• IPsec 엔진에 대한 평가 기능

평가 대상	평 가 항 목	보 안 평 가 기 능
AH	재현공격 방어 기능 평가	AH 헤더 수집기능 / S/N 감시기능 / S/N 생성 및 변경기능 / 패킷 전송기능 / 결과 분석기능
	비연결형 무결성 기능 평가	AH 헤더 수집기능 / S/N 생성 및 변경기능 / SPI 변경기능 / ICV 계산 및 변경기능 / 패킷 전송기능 / 결과 분석기능
	원적지 인증 기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	접근 제어 기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
ESP	재현공격 방어 기능 평가	ESP 헤더 수집기능 / S/N 감시기능 / S/N 생성 및 변경기능/ 패킷 전송기능 / 결과 분석기능
	비연결형 무결성 기능 평가	ESP 헤더 수집기능 / S/N 생성 및 변경기능 / SPI 변경기능 / 패킷 전송기능 / 결과 분석기능
	원적지 인증 기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	접근 제어 기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	기밀성 기능 평가	ESP 패킷 수집기능 / 암/복호 기능 / 결과 분석기능
	제한된 트래픽 기밀성 기능 평가	ESP 패킷 수집기능 / 암/복호 기능 / 결과 분석기능

• 키 교환 블록 평가 기능

평 가 대 상	평 가 목 적	보 안 평 가 기 능
UDP/ISAKMP	Anti-Clogging (Denial of Service) 보호 기능 평가	ISAKMP Payload 수집기능 / ISAKMP Payload 생성기능 / 패킷 전송기능 / 결과 분석 기능
	Connection Hijacking 보호기능 평가	ISAKMP Payload 수집기능 / S/N 감시기능 / S/N 생성 및 변경기능 / 패킷 전송기능 / 결과 분석기능
	Man-in-the-Middle Attacks 보호기능 평가	ISAKMP Payload 수집기능 / ISAKMP Payload 생성기능 / 패킷 전송기능 / 결과 분석 기능
IP	IP spoofing 보호기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	Source Routing 보호기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	Land Attack 보호기능 평가	IP 헤더 수집기능 / IP 주소 및 port 변경기능 / 패킷 전송기능 / 결과 분석기능
ICMP	ICMP Bomb 보호기능 평가	ICMP 헤더 수집기능 / ICMP 헤더 생성기능 / 패킷 전송기능 / 결과 분석기능
	SmurfAttack 보호기능 평가	ICMP echo/reply 패킷 생성기능 / 패킷 전송기능 / 결과 분석기능

• 기타 평가 기능

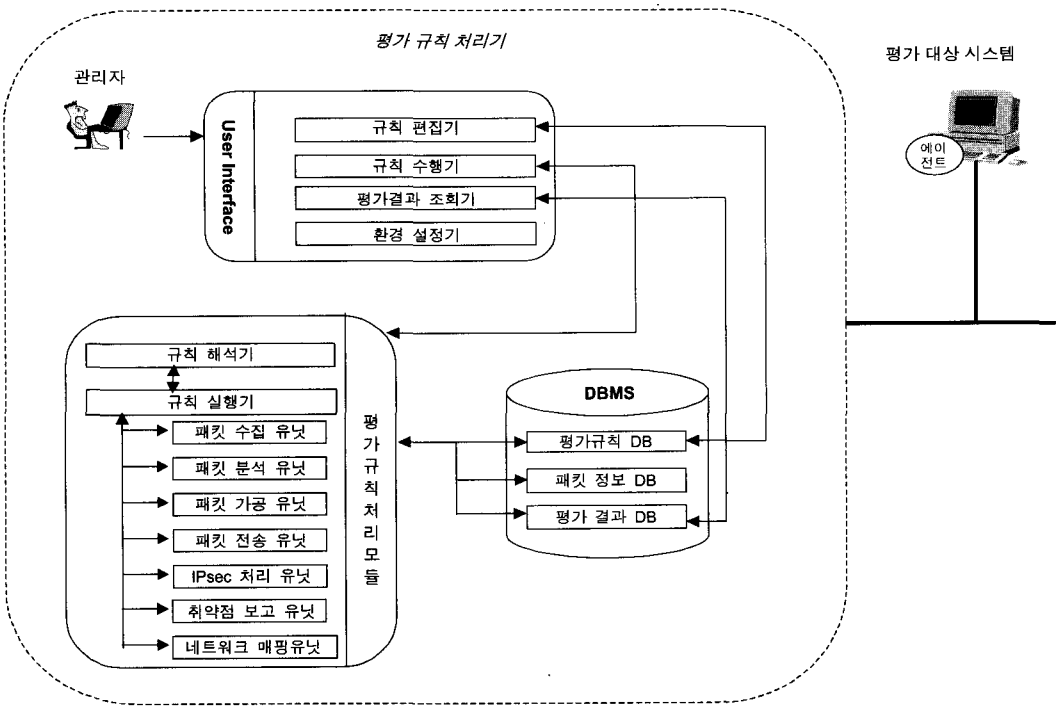
평 가 대 상	평 가 목 적	보 안 평 가 기 능
IP	IP spoofing 보호기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	Source Routing 보호기능 평가	IP 헤더 수집기능 / IP 주소 변경기능 / 패킷 전송기능 / 결과 분석기능
	Land Attack 보호기능 평가	IP 헤더 수집기능 / IP 주소 및 port 변경기능 / 패킷 전송기능 / 결과 분석기능
ICMP	ICMP Bomb 보호기능 평가	ICMP 헤더 수집기능 / ICMP 헤더 생성기능 / 패킷 전송기능 / 결과 분석기능
	Smurf Attack 보호기능 평가	ICMP echo/reply 패킷 생성기능 / 패킷 전송기능 / 결과 분석기능

4.2 전체 시스템 구조

본 절에서는 평가규칙표기언어로 정의된 평가규칙을 처리하기 위한 평가규칙처리 도구의 시스템 구조에 대해 설명한다. 평가규칙처리 도구의 전체적인 구성은 (그림 5)와 같다. 크게 사용자와 평가 시스템간의 인터페이스를 위한 사용자 인터페이스부와 평가규칙을 처리하는 평가규칙 모듈부 그리고 평가를 위한 각종 데이터를 저장하기 위한 DBMS 그리고 평가대상 시스템에 탑재된 에이전트부로 구성되어 진다.

평가 수행을 위한 절차는 크게 다음과 같은 단계로 이루어 진다.

- 1단계 : 보안 관리자가 평가규칙 표기 언어를 이용하여 보안평가규칙을 작성하거나 보안 관리자가 기존에 작성된 평가규칙을 불러온 후 필요하다면 평가규칙을 편집한 후, 평가규칙의 실행을 요구하는 단계.
- 2단계 : 평가규칙처리모듈이 요구 받은 평가규칙의 문법을 검사하는 파싱 단계.
- 3단계 : 평가규칙처리모듈의 규칙 실행기가 6개의 실행 유닛과 DBMS를 이용하여 요구된 평가규칙을 실행하는 단계. 이 단계에서 또한 평가를 수행하기 위해 평가대상 서버에서 송수신되는 패킷을 실시간으로 평가서버로 전달해 주는 에이전트와 협력한다.
- 4단계 : 규칙실행기의 취약점 보고 유닛을 이용하여 평가 결과를 DB에 저장하고 사용자에서 디스플레이 하는 단계.



(그림 5) 평가규칙처리 도구

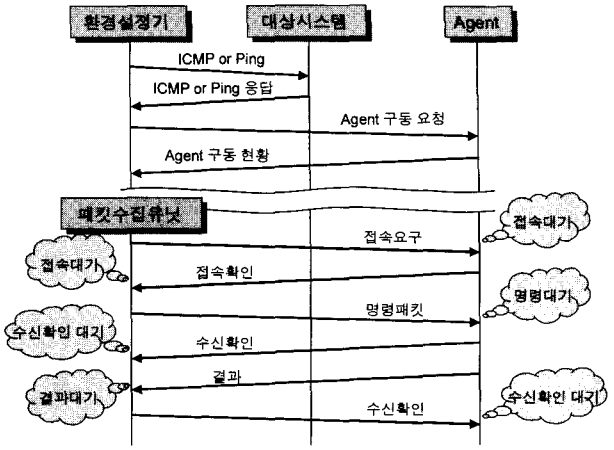
(그림 5)와 같은 구조에서 좀 더 자세한 보안 평가 과정을 기술하면 다음과 같다. 먼저 사용자는 규칙 편집기를 이용하여 평가규칙표기언어의 문법에 맞게 보안성 평가를 위한 규칙을 기술한다. 또는 기존에 저장된 규칙을 불러 올 수도 있다. 규칙의 편집이 완료되고 사용자가 평가규칙을 실행할 것을 평가 GUI를 통해 요구하면, 평가수행기는 이 명령을 받아 평가규칙처리모듈을 호출한다. 평가규칙처리모듈은 요구 받은 평가규칙을 해석하고 처리하는 기능을 갖는다.

평가규칙처리모듈의 각각의 구성요소의 기능은 다음과 같다.

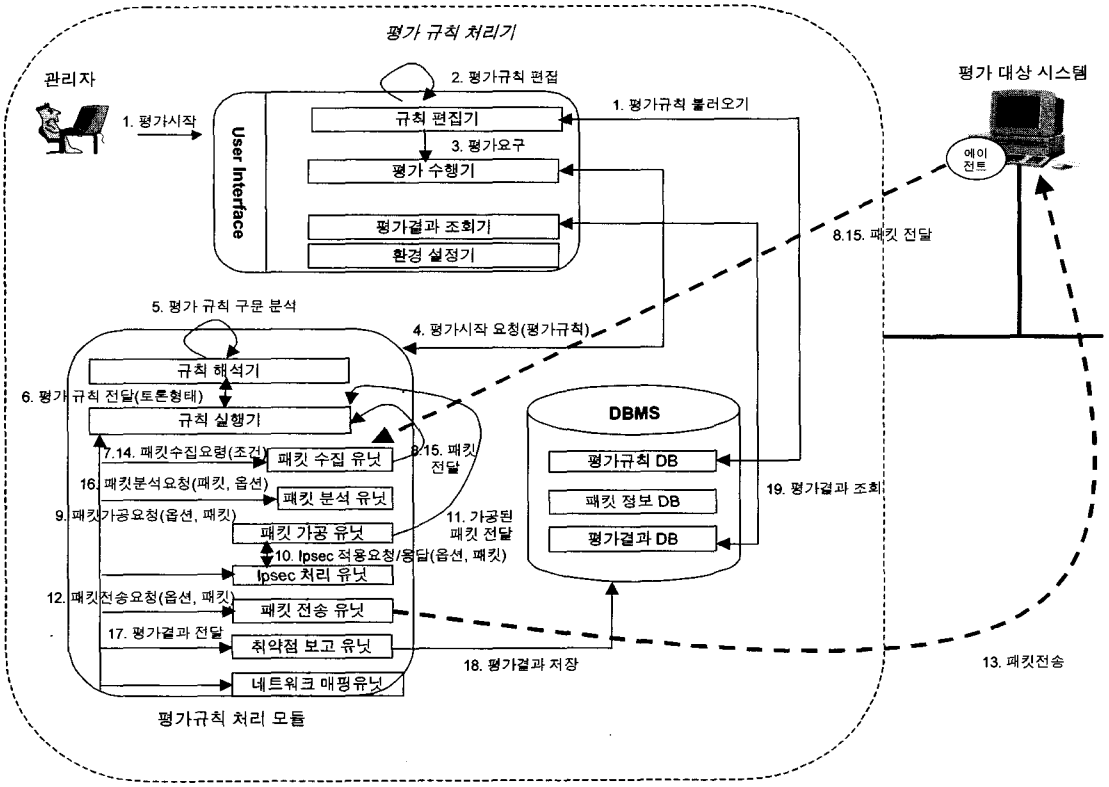
- **규칙해석기** : 사용자가 정의한 규칙이 문법에 맞는지 검사(parsing) 하고 문법에 맞다면 이 규칙을 토큰으로 분리하여 규칙실행기로 전달한다. 문법에 맞지 않는다면 문법 에러 메시지를 발생하여 사용자 인터페이스 모듈로 보낸다.
- **규칙실행기** : 토큰으로 분리되어 전달된 규칙을 실행하는 부분이다. 규칙실행기는 규칙실행 과정에서 필요에 따라 5개의 실행 유닛을 적절히 호출하여 수행한다. 5개의 실행 유닛을 설명하면 다음과 같다.
  - **패킷 수집 유닛** : 실시간으로 패킷을 수집하는 유닛이다. 보안 호스트의 패킷을 수신하기 위해 평가 대상인 보안 호스트에 패킷 스니핑 기능을 갖는 에이전트를 심어 놓는다. 이 에이전트는 자신이 탑재된 보안 호스트에서 송수신되는 패킷 중 패킷 수집 유닛에서 요구한 조건에 맞는 패킷만을 패킷 수집 유닛으로 실시간으로 전달하여 주게 된다. 패킷 수집 유닛은 전달받은 패킷을 규칙 실행기로 전달한다.
  - **패킷 분석 유닛** : 실시간으로 수집한 패킷을 분석하는 유닛이다. 수집한 패킷의 의미를 분석하여 이를 규칙실행기에게 알린다. 패킷 분석 유닛은 전달받은 패킷이 정상적으로 IPsec 처리가 되었는지 검사하거나 패킷을 가공하기 위한 패킷의 정보를 추출하기 위해 사용되는 기능이다.
  - **패킷 가공 유닛** : 패킷 가공 유닛은 보안성 평가를 위해 수집한 패킷을 주어진 규칙에 따라 가공하는 유닛이다. 패킷의 특정 필드의 값을 변경하는 등의 작업을 처리하며 IPsec 처리가 필요한 부분이 있다면 IPsec 처리 유닛의 도움을 받는다.
  - **패킷 전송 유닛** : 패킷 전송 유닛은 임의로 가공된 패킷을 평가 대상 보안 호스트에 전송하는 기능을 갖는다. 임의로 패킷을 전송하기 위해 raw socket을 사용한다. 규칙에 따라 패킷 전송 유닛에 의해 전송된 패킷에 대해 평가 대상 시스템이 반응을 보이는지의 여부는 패킷 수집 유닛과 패킷 분석 유닛에서 담당하게 된다.
  - **IPsec 처리 유닛** : 패킷을 가공하는 경우 IPsec 처리를 요하는 부분이 있는 경우 IPsec 처리 유닛이 이를 처리한다. 또는 패킷 분석 과정에서 IPsec 규격에 맞게 구성된 패킷인지를 분석하기 위해서도 IPsec 처리 유닛이 사용된다. IPsec 처리 유닛은 IPsec 처리를 위해 암복호화 기능과 해쉬함수 처리 기능을 갖는다.

또한 보안 관리자는 **환경설정기**를 이용하여 평가시스템의 각종 환경을 셋팅 할 수 있으며 현재 평가 대상 시스템의 네트워크가 정상적으로 동작하는지를 체크하고 해당 시스템에 에이전트를 탑재하는 기능도 갖는다. (그림 6)은 환경설정기에 의해 대상 시스템의 네트워크 상태를 체크하고 에이전트를 탑재하는 과정과 패킷 수집 유닛이 평가 대상 시스템에 탑재된 에이전트로부터 패킷을 전달받는 과정을 보인다. (그림 7)은 실제 평가가 수행되는 과정의 예를 도식화 한 그림이다.

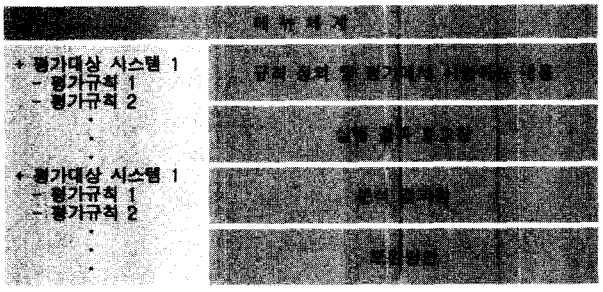
보안 관리자는 사용자 인터페이스의 **평가결과 조회기**를 이용하여 평가결과 DB에 저장된 평가 결과를 조회할 수 있다. (그림 8)는 평가 결과를 디스플레이하기 위해 디자인한 프레임 기반의 윈도우의 구성을 보여준다.



(그림 6) 에이전트 구동 및 패킷 수집 과정



(그림 7) 평가과정 예



(그림 8) 평가결과 디스플레이 윈도우

(그림 8)의 평가 결과 디스플레이 윈도우는 평가 결과를 일목요연하게 분석할 수 있는 체계로 구성되며 몇 개의 프레임 윈도우로 구성되어 각 프레임마다 고유한 결과 데이터를 보여 주도록 구성된다.

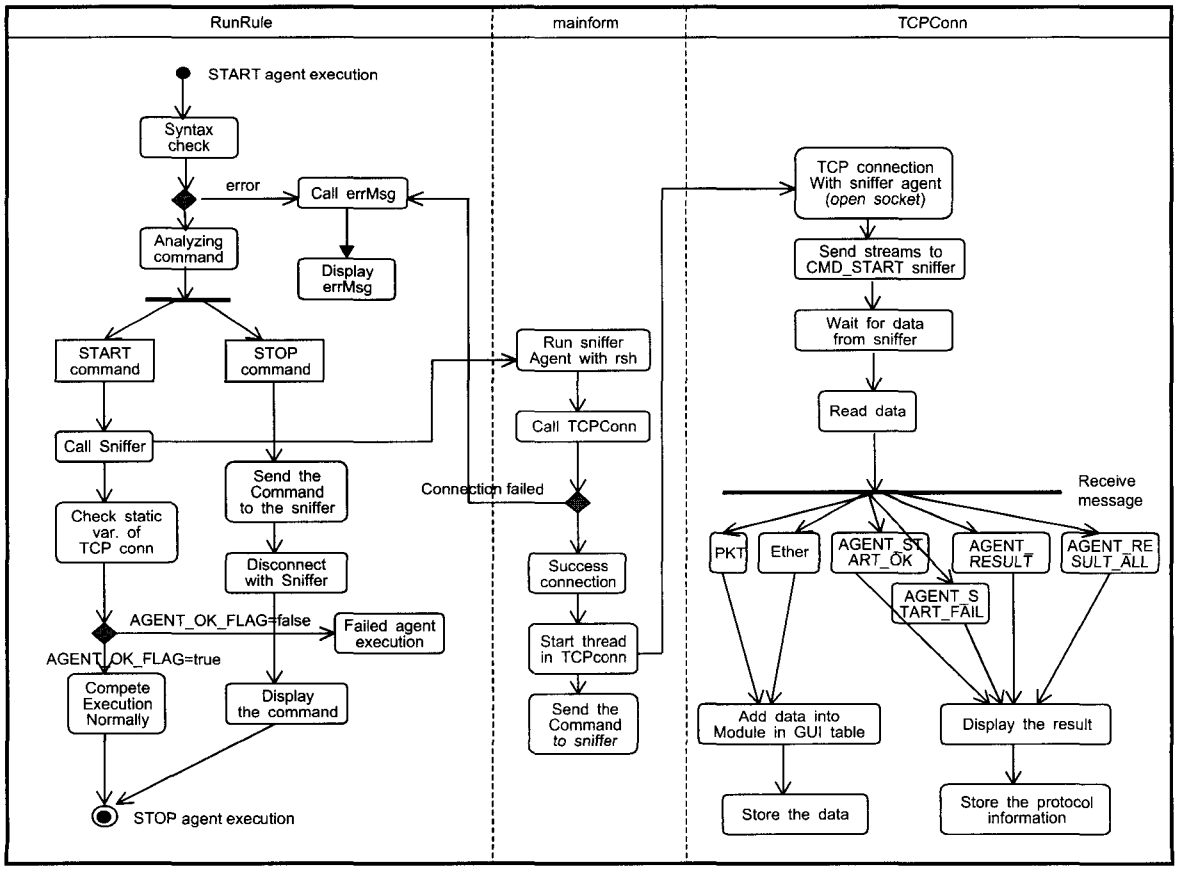
메뉴체계는 현재 활성화된 창에 따라서 메뉴가 동적으로 변화할 수 있도록 설계된다. 화면 왼쪽의 평가대상 시스템 목록은 Tree 형태로 디스플레이 되는 창으로 평가대상 시스템별로 평가결과를 볼 수 있는 화면을 제공한다. 기존에 시험이 완료된 평가 결과는 별도의 검색 기능을 통해서 관

리자가 엑세스 하는 것이 가능하다. 화면 오른쪽은 평가대상 시스템의 평가규칙을 클릭했을 때 활성화 되며 몇 개의 서브 프레임으로 구성된다. 규칙 정의 창은 시험된 규칙이 정하는 시험 방법 및 평가하는 취약성을 설명해 주는 부분으로 규칙 DB에 저장된 내용을 보여준다. 실행 결과 로그 창은 시험이 진행되는 동안의 에이전트가 전달한 로그를 보여준다. 분석 결과창은 평가규칙처리 도구가 해당 규칙을 평가한 최종 결과를 보여주는 창이다. 보완방안에서는 규칙 실행 결과로부터 얻어진 취약성 정도와 보완을 할 수 있는 방안을 디스플레이 한다. 특정 평가대상 시스템의 평가 실행 결과 및 분석 결과가 도착하였다는 신호를 보내주면 화면 좌측의 평가대상 시스템을 깜빡이게 하여 새로운 규칙 실행이 완료되었다는 표시를 해주고 사용자가 해당 규칙을 클릭하면 상세한 규칙 데이터를 디스플레이 하도록 한다.

4.3 보안 평가용 에이전트

보안 평가용 에이전트는 평가 대상 시스템에서 수행되며 네트웍 단자를 통해 송수신되는 패킷들을 평가시스템으로 전달하는 기능을 수행한다. 네트웍 접속 기능을 구분하여 보면 에이전트가 서버로 동작하고 평가시스템이 클라이언트로 동작하는 구조를 갖는다. 평가시스템과 에이전트사이의 통신은 TCP/IP를 이용하여 이루어 진다. 에이전트의 동작은 크게 다음과 같이 4개의 단계로 이루어진다.

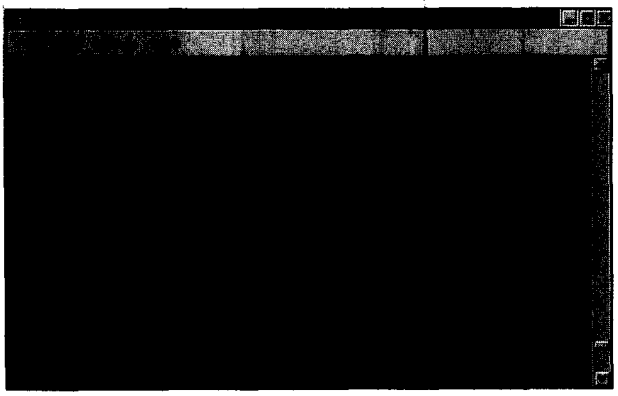
- 1단계 : 평가시스템으로부터의 접속 요구를 기다려 접속 요구를 수용하는 단계이다. 프로그램이 처음 실행되면 에이전트는 평가시스템이 세션을 열 수 있도록 소켓을 하나 생성하여 접속 요구상태로 대기시킨다.
- 2단계 : 평가 시스템과의 접속이 이루어 지면 에이전트는 평가시스템으로부터의 명령을 주기적으로 수신하여 패킷의 처리와 관련된 명령을 수행한다.
- 3단계 : 평가시스템으로부터 START 명령을 수신하면 패킷 스니핑을 개시한다. 스니핑을 위해 PCAP 라이브러리를 초기화하는 작업을 수행한 후에 평가시스템이 전달한 스니핑 옵션을 설정하여 지정된 패킷만 스니핑이 될 수 있도록 한다. 네트웍 단자에서 패킷이 스니핑 될 때마다 각 패킷 데이터는 평가시스템이 관리하기 용이한 구조로 변환되어 평가시스템에 전달되게 된다.
- 4단계 : 지속적으로 스니핑되는 패킷은 평가시스템으로부터 STOP 명령을 수신하면 스니핑을 멈추고 동작을 종료하게 된다.



(그림 9) 평가용 에이전트 동작과정

(그림 9)는 평가 대상 시스템에 탑재된 에이전트의 수행 과정을 도식화 한 것이다. 에이전트와 통신을 하게 되는 모듈은 평가규칙처리모듈이며, 평가규칙처리모듈은 에이전트에게 4가지 종류의 명령을 전달할 수 있다. 각각은 START (스니핑을 시작하라), STOP(스니핑을 중단하라), HALT(스니핑을 일시 중지하라), RESUME(스니핑을 재개하라)이다. START의 경우 옵션으로 프로토콜, source IP, destination ip를 query로서 줄 수 있다. 이 때 프로토콜을 옵션으로 주는 경우 IPv6 패킷 기본 헤더와 확장 헤더로 이루어진 header chain 중에서 해당 프로토콜을 찾는 기능도 제공한다.

(그림 10)은 평가용 에이전트 모듈이 실시간으로 스니핑한 ESP 적용 패킷의 내용을 텍스트 모드로 디스플레이 한 모습이다.



(그림 10) 실시간으로 스니핑한 패킷의 내용

4.4 데이터 베이스

규칙실행기에서 관리 되는 데이터베이스는 평가규칙 DB, 패킷정보 DB, 평가결과 DB로 구성된다. <표 3>에서는 평가규칙 DB의 구조를 보여준다. 평가규칙 DB는 평가에 대한 규칙을 저장하는 DB이다.

〈표 3〉 평가규칙 DB의 필드 구조

Field Name	Type	설 명
RULE_ID	INTEGER	평가규칙의 고유 ID
RULE_NAME	CHAR	평가규칙 이름
DESCRIPTION	CHAR	평가규칙에 대한 설명
RULE	MEDIUMTEXT	평가규칙표기 언어로 정의된 규칙
DateTime	DATE / TIME	평가규칙 날자 및 시간

본 규칙처리 도구는 데이터베이스 관리를 위해 JDBC를 이용한 관계형 데이터베이스 엑세스를 지원하며 다음과 같은 기본적인 기능을 수행하는 클래스를 별도로 구현하여 데이터베이스를 일관된 인터페이스를 통해서 엑세스 가능하도록 구현하였다.

Init(데이터 엑세스가 가능하도록 데이터 구조를 초기화 함), Open(DBMS에 접속), Close(DBMS 접속을 해제), Select (입력된 조건에 맞는 규칙을 검색), Update(선택된 규칙을 수정), Delete(특정 규칙을 삭제), Insert(새로운 규칙을 추가)

평가규칙을 설정하기 위한 알고리즘은 다음과 같다.

```
begin RSU module {
switch(func) {
                case SelectRule :
                        sRules = RuleDB.select(expr) ;
                if (sRules != 0) { DisplayRuleTitle() ; }
                break ;
        case NewRule :
                        if(CheckRuleSyntax(newRule) == OK) {
                                RuleDB.insert(newRule) ;
                        } else { DisplayErrMsg(badRuleSyntax) ; }
                break ;
        case UpdateRule :
                        if (CheckRuleSyntex(rule) == OK) {RuleDB.update(rule) ; }
                         else { DisplayErrMsg(badRuleSyntax) ; }
                        break ;
        case RemoveRule :  RuleDB.delete(rule) ;
                        break ;
        case DetailedInfo :
                DisplayDetailedRuleInfo(rule) ;
                break ;
        case ShowEnvVar :
                DisplayEnvVar() ;
                break ;
        case ChangeEnvVar :
                Update(envVar, newVal) ;
                break ;
        default :
                DisplayErrMsg(badCommand) ;
                break ;
        }
}
```

패킷 정보 DB는 에이전트로부터 전송 받은 각종 프로토콜 데이터를 저장하는 DB로서 각 프로토콜 별로 테이블을 생성하고 저장한다. 자동으로 생성되는 테이블은 Ethernet, ARP, IP, AH, ESP, TCP, UDP, ICMP, ISAKMP 이며 이 중 AH, ESP, ISAKMP에 대한 테이블의 구조를 <표 4>에서 볼 수 있다.

〈표 4〉 패킷 정보 DB의 필드 구조

• AH

Field Name	Type	설 명
ID	INTEGER	패킷에 대한 고유번호
LINKID	INTEGER	한 패킷내에서의 AH 순서번호
SERIAL	INTEGER	한 패킷내에서의 프로토콜 순서번호
NEXTHDR	CHAR	상위 계층 프로토콜의 유형
PAY_LEN	INTEGER	AH헤더의 전체길이
SPI	INTEGER	SA 식별자
SEQUENCE	INTEGER	단순 증가 카운터
AUTHENTICATION	MEDIUMTEXT	Authentication Data
TIME	VARCHAR	수행된 시간
RUNCOUNT	CHAR	수행 횟수

• ESP

Field Name	Type	설 명
ID	INTEGER	패킷에 대한 고유번호
SPI	INTEGER	SA 식별자
SEQUENCE	INTEGER	단순 증가 카운터
ENCRYPTION	MEDIUMTEXT	Encryption Data
TIME	VARCHAR	수행된 시간
RUNCOUNT	CHAR	수행 횟수

• ISAKMP

Field Name	Type	설 명
ID	INTEGER	패킷에 대한 고유번호
INIT_COOKIE	CHAR	SA을 시작한 Entity의 COOKIE
RESPOND_COOKIE	CHAR	SA에 응답하는 Entity의 COOKIE
NEXT_PAY	CHAR	메시지내의 첫번째 Payload의 타입
MAJ_VER	INTEGER	ISAKMP의 Major버전
MIN_VER	INTEGER	ISAKMP의 Minor버전
EXCHANGE_TYPE	CHAR	현재 사용되고 있는 Exchange타입
FLAGS	CHAR	Exchange에 대한 특정한 선택사항
MESSAGE_ID	INTEGER	메시지 식별자
TOTAL_LEN	INTEGER	헤더를 포함한 전체 Payload길이
ENCRYPTION	MEDIUMTEXT	Encryption된 데이터
TIME	VARCHAR	수행된 시간
RUNCOUNT	CHAR	수행 횟수

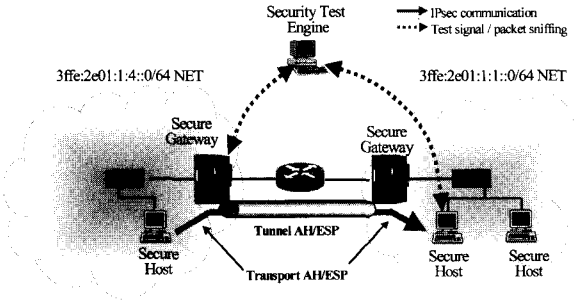
평가 결과 DB는 평가규칙이 수행된 결과를 저장하는 DB로서 평가규칙처리모듈의 규칙 실행기에 의해 데이터가 저장된다. 저장된 데이터는 User Interface의 평가 결과 조회기에 의해 보안 관리자에게 전달된다. <표 5>에서 평가 결과 DB의 구조를 볼 수 있다.

〈표 5〉 평가 결과 DB의 필드 구조

Field Name	Type	설 명
HOSTID	INTEGER	평가 대상 호스트 ID
IP	STRING	평가 대상 호스트 IP 주소
RULE_LIST	ARRAY of INTEGER	적용한 평가규칙 ID
RESULTS	ARRAY of CHAR	평가 결과
DateTime	ARRAY of DATE/TIME	각 평가규칙을 적용하여 평가를 수행한 날자 및 시간

5. 보안성 평가

현재는 보안평가규칙 처리 도구는 프로토타입이 개발된 상태이며, 몇가지 보안 평가 항목을 평가규칙언어를 이용하여 정의하고 테스트 해 보았다. 본 논문에서 제안한 보안성 평가 시스템과 에이전트에 탑재된 패킷 스니핑 모듈은 JAVA와 C를 통해 구현하였다. 데이터베이스는 JDBC를 이용하여 구현하였다. 평가를 위한 네트워크 환경은 (그림 11)과 같다.



(그림 11) 평가 환경

IPv6 네트워크에서 IPsec이 제공해야 하는 5가지 보안성을 평가 대상 네트워크에서 적절히 제공하는지를 평가 시스템을 통하여 평가하기 위한 방법을 요약하면 다음과 같다.

• 기밀성(confidentiality)

전송중인 IPsec ESP가 적용된 암호화된 패킷을 수집하여 임의의 키를 생성하여 복호화 해본다. 복호화된 패킷의 의미를 알 수 있는지 확인한다. 이 기능은 현재 구현되지 않았으며 테스트 방법을 설계 중에 있다.

• 원적지 인증(Data Origin Authentication)

전송중인 IPsec이 적용된 패킷을 실시간으로 수집한 후 수집한 패킷 헤더 내의 전송자의 IP 주소를 임의로 변경하여 목적지로 전송하고, 이 패킷을 받은 노드가 이에 대한 응답을 하는지 확인한다.

• 접근 제어(Access Control)

임의의 키(key)를 이용하여 AH 혹은 ESP 패킷을 구성하

여 목적지로 패킷들을 전송하여 접근 권한을 얻을 수 있는지 시도한다.

• 비연결형 무결성(Connnectionless Integrity)

네트워크 상에서 실시간으로 수집한 AH가 적용된 패킷의 특정 필드를 임의로 변경한 후 이 값을 기초로 ICV값을 재계산하여 변조하여 전송하고, 이에 대한 대상 노드의 응답이 있는지 확인한다. 또 한가지 방법으로 ESP암호화된 패킷을 실시간으로 수집한 후 임의로 패킷의 내용을 변조하여 수신호스트로 전송한다. 이 때 수신호스트에서 변조된 패킷을 정상적으로 폐기하는지 확인한다.

• 재현공격 방어(Anti-replay)

네트워크 상에서 실시간으로 수집한 패킷을 다시 동일한 목적지로 재전송하여 본다. 또는 수집된 패킷의 IPsec AH/ESP 헤더내의 SN(Sequence Number)값을 감시하여, 새로운 SN을 생성하거나 수집한 SN을 변경하여 재전송하고, 이에 대해 대상 노드의 응답이 있는지 확인한다.

본 논문에서는 이상의 5가지 기본적인 보안 서비스의 제공 및 IPsec의 정상동작을 테스트하기 위해 ETRI에서 개발중인 Universal IPv6 엔진을 대상으로 하여 몇 가지 보안 항목을 테스트 해 보았다. 그 중 비연결형 무결성 항목에 대한 평가를 소개하면 다음과 같다. (그림 12)와 (그림 13)은 각각 평가규칙 표기 언어를 이용하여 Connectionless Integrity 항목을 평가하기 위해 작성한 평가 아이템과 평가규칙언어로 작성한 평가규칙 내용을 보여준다.

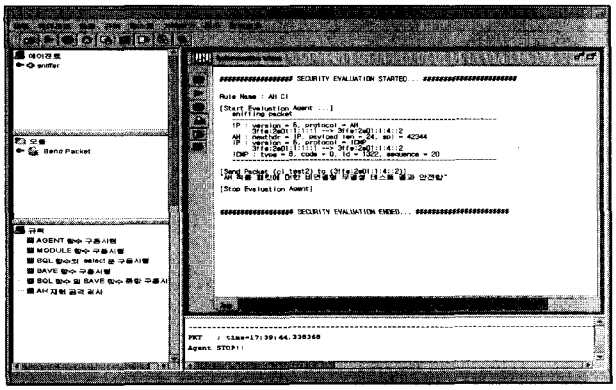
```
Test Item : AH Connectionless Integrity
Try
    H1 ==> SES ==> H2 ICMP Echo request (with AH, modification
    of ICV)
Result [PASSED]
    H1 <==X= H2 No ICMP Echo reply (Drop packet)
Result [FAILED]
    H1 <==== H2 ICMP Echo reply
```

(그림 12) 비연결형 무결성 평가 아이템

```
RULE_NAME : AH CI
DESCRYPTION : AH가 적용된 packet의 비연결형 무결성 평가
START_EVALUATION
    LOOP time < 300ms
        IF (CAPTURE (ci_test, ip6 protochain icmp and ah and icmp_type 8))
            IPSEC_PROC(ci_test, RECAL_ICV, ci_test2) ;
            BREAK ;
        ENDIF
    END LOOP

    IF (CHECK_FILE(ci_test2))
        SEND_PACKET(ci_test2, 3ffe : 2e01 : 1 : 4 : : 2) ;
    ELSEIF
        PRINT(테스트 수행 중 에러 발생함) ;
    ENDIF

    LOOP time < 30ms
        IF(CAPTURE (ci_result, ip6 protochain icmp and source_ip 3ffe : 2e01 : 1 : 4 : : 2 and icmp_type 0))
            PRINT(AH적용 패킷에 대한 비연결형 무결성을 제공하지 못함) ;
            BREAK
        ENDIF
    END LOOP
    IF NOT CHECK_FILE(ci_result)
        PRINT(AH적용 패킷에 대한 비연결형 무결성 테스트 결과 안전함) ;
    ENDIF

END_EVALUATION
```

(그림 13) Connectionless Integrity 평가규칙

(그림 13)의 평가규칙은 target 시스템으로 전송되는 AH가 적용된 ICMP packet을 실시간으로 스니핑하여 ICV값을 재계산한 후 target 시스템에 전송한 후 이에 대한 응답여부를 분석하여 Connectionless Integrity를 제공하는지의 여부를 평가하는 것이다. 응답여부를 분석하는 방법은 평가 대상 서버에 위치한 에이전트가 해당 서버에서 전송되는 패킷을 보안 평가 도구로 전달하고 보안 평가 도구는 이 패킷들을 분석하여 ICMP 패킷에 대한 응답 패킷이 있는지 판단하는 방법을 사용한다. (그림 13)에 정의된 규칙에서는 30ms간 ICMP 응답이 없으면 패킷이 폐기된 것으로 간주하도록 되어있음을 확인할 수 있다.



(그림 14) AH Connectionless Integrity 테스트 결과화면

(그림 14)는 (그림 13)에 정의된 규칙을 개발한 규칙 실행기 프로토타입을 이용하여 평가한 결과 화면을 보여준다. (그림 14)에서 볼 수 있듯이 평가결과는 AH가 적용된 패킷에 대한 비연결형 무결성을 제공하고 있다는 결과가 나왔다.

6. 결 론

본 논문은 IPv6 네트워크에서 정보보호 서비스를 제공하기 위해 IPsec 엔진을 탑재한 보안 호스트의 보안성을 평가하기 위한 방법에 대한 것으로, 보안평가 방법을 정의하기 위한 평가규칙표기언어를 설계하고 평가규칙표기언어를 이용하여 정의된 평가규칙을 해석하고 실행하기 위한 평가규칙 처리 도구를 제안하였다. 그리고 제안한 시스템의 프로토타입을 개발하여 일부 보안성 평가를 수행한 사례를 소개하였다.

본 시스템은 평가규칙표기언어를 통하여 보안성 평가규칙을 정의하고 정의된 규칙을 평가규칙 처리 도구에 의해 수행하는 구조를 갖는다. 평가규칙 표기언어는 매우 단순한 구조를 가짐으로 보안평가자가 손쉽게 평가규칙을 정의할 수 있는 장점을 갖는다. 또한 향후 추가적인 보안 취약점에 대한 평가를 수행하기 위해 정의된 규칙을 확장할 수 있는 확장성 또한 본 시스템의 장점이라고 볼 수 있다. 또한 평가용 에이전트를 두어서 실시간으로 패킷을 수집, 가공, 전송 하는 방식의 평가 방법 역시 새로운 방법이라고 볼 수 있다. 무엇보다도 기존의 네트워크 보안 스캐닝 도구가 제공하지 못하는 layer 3에서의 보안성 제공에 대한 평가를 수행한다는 점에서도 의의가 있다. 또한 IPv6 망에서 동작이 가능한 시스템으로 향후 IPv6 망으로의 진화과정에서 IPv6기반 시스템을 개발할 때 이에 대한 보안성 평가를 위한 도구로서 유용하게 사용이 가능할 것을 기대할 수 있다.

본 시스템의 프로토타입은 C, JAVA, JDBC를 이용하여 구현 하였으며, 평가용 에이전트의 패킷 캡쳐 모듈은 PCAP 라이브러리를 이용하여 구현하였다. 현재 평가규칙 표기언어를 이용하여 5가지 보안 요구사항을 기초로 몇 가지 평가규칙을 작성하여 라이브러리화 하는 작업이 진행 중에 있으며, 이 작업이 완료되면 보안 평가자는 라이브러리를 불러와서 평가를 수행할 수 있을 것이다. 현재 수집된 패킷 자체에 대한 분석 모듈과 IPsec 적용 모듈에 대한 구현이 진행 중에 있다.

본 시스템은 평가 대상 시스템의 보안 위협요소를 도출함으로 인해 더욱 안전성을 보장하는 보안 시스템을 개발할 수 있는 장점을 제공할 수 있는 효과가 있으며, 기 개발된 IPv6 네트워크 계층의 보안 서비스를 제공하는 서버에 대한 신뢰성을 측정하기 위해서도 활용이 가능할 것이다.

향후 연구과제로서 본 논문에서 평가 항목으로 제시한 5가지 요구사항에 대한 기능 확인 만으로 대상 시스템에 대한 보안성 평가가 충분한 지의 여부와 각각의 보안성 평가 방법에 대한 검증 작업이 필요하며, 이러한 작업은 시스템을 완성해 나가면서 수행할 예정이다.

참 고 문 헌

[1] S. Deering, R. Hinden, Internet Protocol, Version 6(IPv6) Specification, RFC2460, Dec., 1998.

[2] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC2401, Nov., 1998.

[3] N. Doraswamy and D. Harkins, IPsec : The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Prentice Hall, 1999.

[4] 정보통신부, http://www.mic.go.kr/.

[5] 권혁찬, 나재훈, 손승원, "IPv6 Security 동향", 주간기술동향, 1094호, 한국전자통신연구원, Sept., 2002.

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

[7] S. Kent and R. Atkinson, IP Encapsulating Security Payload, RFC2406, Nov., 1998.

[8] D. Harkins, D. Correl, Internet Key Exchange, RFC2409, Nov., 1998.

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

[10] Cisco Scanner, http://www.cisco.com/univercd/cc/td/doc/pcat/nssq.htm.

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

[12] A. Rubini, Linux Device Drivers, 1998, O'Reilly.

[13] S. Garfinkel and G. Spafford, Practical UNIX and Internet Security, 2nd edition, O'Reilly, 1996.

[14] M. Y. Lee, Internet Security Cryptographic principles, algorithms and protocols, WILEY, 2003.

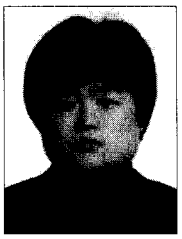
[15] H. C. Kwon, S. C. Kim, J. H. Nah, T. Y. Nam, S. W. Sohn, An Automatic Security Test Engine for IPv6 Network, Proc. of the International Workshop on Cryptology and Network Security(CNS'2003), pp.685-690, Miami, Florida, USA, Sept., 2003.

[16] J. S. Lee, S. C. Kim and S. W. Sohn. A Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management, pp.246-260, LNCS 2015, Dec., 2000.

[17] 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 ICEIS2001, Setubal, Protugal, Vol.2, pp.920-925.

권 혁 찬

e-mail : hckwon@etri.re.kr
1994년 서원대학교 전자계산학과 공학사
1996년 충남대학교 전산학과 이학석사
2001년 충남대학교 컴퓨터과학과 이학박사
2001년~현재 한국전자통신연구원 정보보호 연구단 선임연구원
관심분야 : Network Security, Mobile IPv6 Security, IPv6



김 상 춘

e-mail : kimsc@samcheok.ac.kr
1986년 한밭대학교 전자계산학과
1989년 청주대학교 전산학과 공학석사
1999년 충북대학교 컴퓨터과학과 이학박사
1983년~2001년 한국전자통신연구원 정보보호연구단 선임기술원
2001년~현재 삼척대학교 정보통신공학과 교수
관심분야 : Network Security, IP Security, Security Evaluation