정보보호 서비스를 위한 보안평가 시스템 설계

김상춘°* 현정식** 이종태* 손승원*
*한국전자통신연구원 정보보호기술연구본부 정보보호응용연구부
** 청주대학교 전자계산학과

Design of the Security Evaluation System for Internet Secure Connectivity Assurance Platform

Sang-choon Kim°*, Jeung-sik Hyun**, Jong-tai Lee*
*Information Security Technology Division, ETRI
**Dept. of Computer Science, Chongju University

요 약

인터넷의 발달로 정보보호에 대한 인식이 증가하면서 정보보호 서비스를 제공하기 위한 연구 및 개발의 필요성이 증가하고 있다. 정보보호 서비스를 제공하기 위하여 개발되고 있는 시스템은 일반적인 시스템보다 보안성 유지의 필요성이 훨씬 중요하기 때문에 이러한 시스템의 안전성을 평가하는 기술은 매우 중요하다. 그러나 아직까지 정보보호 서비스를 제공하는 시스템에 대한 안전성을 평가하는 기술이나 연구는 전무한 실정이다. 본 논문에서는 IP 레벨에서의 정보보호 서비스를 제공하기 위하여 개발되고 있는 인터넷 패킷보호 보증플랫폼에 대한 보안성을 평가하는 시스템을 설계하기 위하여 이 시스템에서 제공하는 정보보호 서비스와 이러한 서비스가 정상적으로 제공되고 있는 지를 평가하기 위한 보안평가 시스템을 설계한다.

I. 서론

1. 개요

인터넷과 WWW 의 이용이 폭발적으로 증가하면서 정보보호 서비스에 대한 많은 연구가 진행되어 왔다. 지금까지 인터넷 응용분야에 대표적인 정보보호 메커니즘으로는 전자우편 부문에 PGP, PEM, S-MIME, 네트워크 관리 부문에 SNMP 보안, 웹 부문에 S-HTTP, SSL/TLS 와 SOCKS 등을 들 수 있다. IETF 에서는 TCP/IP 네트워크를 대상으로 전송 계층과 네트워크 계층에 표준 정보보호 메커니즘을 제공하고자 노력을 계속하고 있다.

IPsec 은 IP 계층에서 정보보호 서비스를 제공한다. TCP/IP 를 이용하는 모든 통신은 반드

시 IP 계층을 거쳐가야 하기 때문에 IPsec 은 응용프로그램이 TCP 또는 UDP 를 사용하여도 이들에게 정보보호 서비스를 제공한다. 즉 IPsec 의 정보보호 서비스를 사용하기 위하여 응용프로그램들을 변경할 사항이 전혀 없다는 것이다.

정보보호 서비스를 제공하기 위하여 개발되는 시스템은 일반적인 시스템 보다 보안성 유지가 매우 중요하기 때문에 이를 위해서는 시스템에 대한 보안성 평가가 필요하다. 보안성 평가를 위해서는 많은 종류의 보안성 시험과 분석이 요구된다. 보안평가 시스템은 보안성 시험을 통해 보안상의 문제점을 찾아내고, 이를 바탕으로 보안 상태를 향상시킬 수 있도록 보안상 문제점을 해결할 수 있는 방법을 제시해 주는 시스템이다. 또한 정보보호 서비스를 제공하는 시스템의 보안 상태를 분석하여 시스템 전체의 보안 상태를 평가하고 이에 대한 해결책을 제시함으로써 불법적인 행동이 발생하기 전에 시스템의 보안 수준을 높여줄 수 있는 시스템이다[1].

2. 보안평가 시스템 연구의 필요성

정보보호 서비스를 제공하는 시스템에 대한 보안성 평가를 해주는 정형화되고 표준화된 기술은 아직 없다. 다만 일부 개발 업체마다 독자적인 기능을 갖는 호스트 및 네트워크의 취약성을 분석해 주는 툴을 개발하고 있다. 현재 sscan, SATAN [2], SAINT, ISS 등의 해킹 툴을 사용하여 시스템 및 네트워크의 취약점을 분석하는 방법이 널리 사용되고 있으나 각각의 툴을 하나로 통합하여 사용하기가 불편하고 각각의 보안상 취약점을 통합 분석한 종합적인 분석 결과를 얻어내기 힘들며 새로운 취약점이 알려질 때마다 각각의 툴들을 따로 업데이트 해야 하는 단점이 있다.

또한 정보보호 서비스를 제공하는 시스템의 보안성을 분석해주기 위하여 개발된 시스템은 전무한 실정이다. 따라서 이러한 시스템의 보안성 분석을 위한 보안평가 시스템에 대한 보다 심화된 연구와 개발이 필요하다.

본 논문에서는 이러한 연구의 일환으로 인터넷에서의 공격 방법에 대해 분석하고, 이러한 인터넷 공격 방법에 대응하기 위해 개발하고 있는 시스템 중 IP 레벨에서의 정보보호 서비스를 제공하는 인터넷 패킷보호 보증플랫폼의 시스템 형상과 제공되는 정보보호 서비스를 알아보고, 인터넷 패킷보호 보증플랫폼의 보안성을 평가하기 위한 보안평가 시스템을 설계한다[3] ~ [6].

II. 인터넷에서의 공격 방법

이 절에서는 인터넷 공격 방법 중 IP 레벨에서의 공격 방법에 대하여 기술한다.

1. Sniffer

Sniffer 는 최근 널리 쓰이고 있는 침해 기술로서 tcpdump, snoop, sniffer 등과 같은 네트워크 모니터링 툴을 이용해 네트워크 내에 돌아다니는 패킷의 내용을 분석해 정보를 알아

내는 기술이다. 이 기술은 네트워크에 연동돼 있는 호스트뿐만 아니라 외부에서 내부 네트워크로 접속하는 모든 호스트가 공격 대상이 되므로 주의해야 한다. 이를 위해 해커는 먼저 자신의 시스템이나 보안 취약점을 가지고 있는 시스템에 침입하여 루트(Root) 권한을 획득 한 후에 이 시스템에 다시 로그인 하기 위해 백도어(Backdoor)를 설치한 후 그 시스템이 속해 있는 네트워크 상의 모든 ftp, telnet 그리고 rlogin 세션의 처음 128 개의 문자를 가로챌 수 있는 네트워크 모니터링 툴을 설치해 실행한다. 이 패킷 스니퍼링은 일종의 엿보기이다.

2. Packet Spoofing

Packet Spoofing 은 인터넷 프로토콜인 TCP/IP 의 구조적 결함, 즉 TCP 시퀀스번호, 소스 라우팅, 소스 주소를 이용한 인증(Authentication) 메커니즘 등을 이용한 기술로써 인증 기능을 가지고 있는 시스템에 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 기술이다. 즉, 이 기술은 자신이 침투하고자 하는 컴퓨터를 무력화하기 위해 자신이 그 컴퓨터인 것처럼 가장하는 것이다. 아무리 보안이 잘 되어있는 컴퓨터라도 자기자신을 경계하지는 않기 때문이다. 이러한 기술은 NASA 나 미 국방부까지 뚫을 수 있는 최고의 기술이다.

3. 서비스 거부 공격(Denial of Service Attack)

서비스 거부 공격이라 함은 일반적으로 공격자의 컴퓨터로부터 표적 시스템과 그 시스템이 속한 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 표적 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하도록 하게 하는 기술을 말한다. 분산 서비스 거부 공격이라 함은 많은 수의 호스트들에 패킷을 범람시킬 수 있는 DoS 공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표 시스템(네트워크)에 대하여 일제히 데이터 패킷을 범람(Overflow)시켜서 그 표적 시스템 또는 네트워크의 성능저하 및 시스템 마비를 일으키는 기술이다.

4. Session Hijacking

Hijacking 이란 침입자가 이미 인증 받은 사용자의 세션을 빼앗는 것을 의미한다. 침입자가 Hijacking 에 성공하게 되면 타겟이 된 인증 사용자가 가지고 있던 모든 특권을 활용할 수 있다. CERT(Computer Emergency Response Team)에 의해 문서화된 유일한 Hijacking 은 서버 호스트에서 Hijacking 소프트웨어를 실행해 터미널을 Hijacking 하는 것이다. 이런 유형의 Hijacking 은 Hijacking 소프트웨어를 설치하기 위해 침입자가 Root 를 가지고 서버에 접근해야 한다. 속임수 차단, 패킷 필터링, 사용자 인증 같은 여러 가지 방어를 같이 사용하면 인증되지 않은 접근이나 불법 운용을 방지 할 수 있다.

5. Replay Attack

Replay Attack 은 이용자가 제대로 맞는지를 확인하는 과정에서 서버 시스템은 이용자 사

이에 전자서명과 같은 암호화한 데이터를 주고 받는다. 그 도중에 제3자인 해커가 네트워크 상에 전송되고 있는 데이터를 복사해 뒀다가 나중에 이를 그대로 서버에 전송해서 합법적 이용자를 가장하여 침입하는 기술이다.

6. CGI Attack

각종 CGI 구현 시 또는 웹 서버 환경 설정에서의 오류를 이용하여 시스템에 접근하여 내부 명령을 임의로 실행하는 기술을 말하며 최근 들어 인터넷 이용이 크게 늘면서 많이 사용되는 침해 기술이다. 이를 방지하기 위해서는 보안 기능을 보완하는 최신 버전의 프로그램이 사용될 수 있도록 시스템 관리자가 관리를 해야 한다.

위와 같은 정보 유출 및 침해에 대하여 효과적으로 대응하기 위한 기술 개발이 시급한 실정이며 이와 관련한 기술에 대한 표준화 작업 및 제품 개발이 활발하게 이루어 지고 있다.

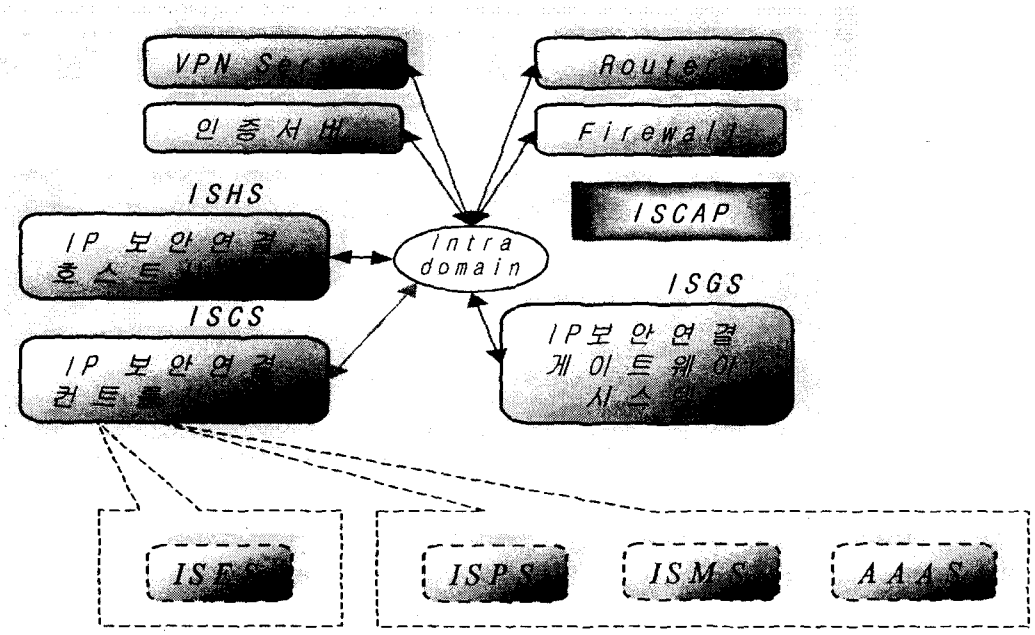
III. 인터넷 패킷보호 보증플랫폼

인터넷 패킷보호 보증 플랫폼(ISCAP : Internet Secure Connectivity Assurance Platform)은 IP 레벨 보안 서비스를 제공하는 시스템이다. 즉 기존의 응용 레벨의 인터넷 서비스의 변경 없이 IP 레벨에서의 정보보호 서비스를 제공한다. IPv4/IPv6 를 지원하는 IPsec Engine은 IP 레벨에서 기밀성(confidentiality), 무결성(integrity), 데이터 인증(data authentication), 접근 제어(access control), Anti-replay 서비스 등을 응용레벨 인터넷 서비스에 제공한다. 이는 IP 계층에서 정보보호 서비스를 제공하므로 상위 레벨 프로토콜 및 프로그램을 수정할 필요가 없다. 각 서브시스템은 인터넷에 접속되며 인터넷을 통해 IP 패킷 형태로 상호간에 정보를 교환한다.

ISCAP 의 각 서브시스템은 공개키 기반 시스템(PKI: Public Key Infrastructure)에서 제공하는 CA (Certification Authority)와 연동을 통하여 공개 키 인증에 관한 정보를 교환하며, IPsec 을 지원하는 VPN 서버, 라우터, 방화벽 시스템과의 연동을 통하여 정보보호 서비스를 제공한다[7] ~ [29].

1. 시스템 형상

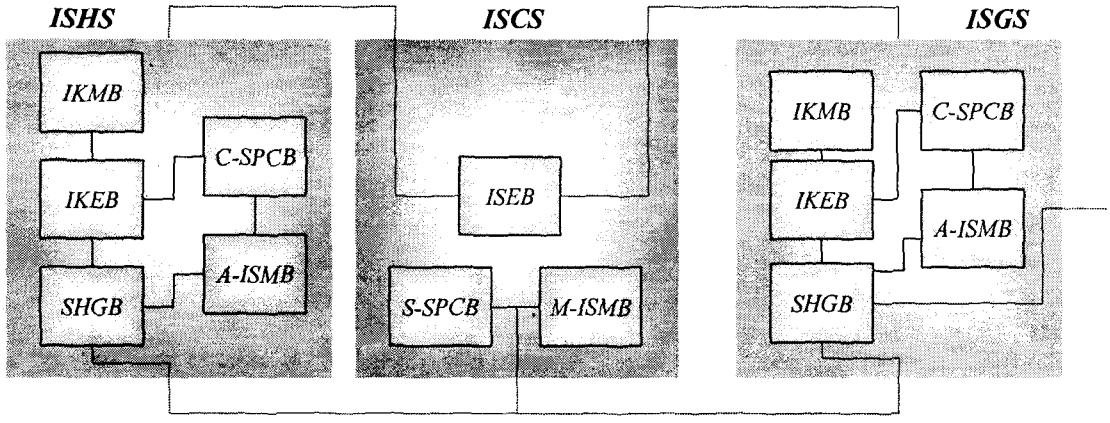
ISCAP 시스템에서 제공할 기능들을 그룹화하여 [그림 1]과 같이 IP 보안 보안연결 호스트 시스템(ISHS : IP Secure connectivity Host System), IP 보안연결 게이트웨이 시스템(ISGS : IP Secure connectivity Gateway System), IP 보안연결 콘트롤 시스템(ISCS : IP Security Control System) 등 3 개의 서브시스템으로 구성되며, 각 서브시스템은 인터넷에 접속되어 인터넷을 통해 IP 패킷 형태로 상호간의 정보를 교환한다. 이러한 형상 구성도는 [그림 1]과 같다.



[그림 1] 인터넷 패킷보호 보증플랫폼(ISCAP) 형상 구성도

2. 서브 시스템과 블록 연관도

ISCAP 시스템은 3 개의 서브 시스템과 여러 블록으로 구성되며 서브 시스템과 블록의 연관도는 [그림 2]와 같다.



[그림 2] ISCAP 각 서브 시스템과 블록의 연관도

3. 서브 시스템의 기능

ISCAP를 구성하는 각 서브시스템의 기능은 다음과 같다.

가. IP 보안연결 호스트 서브시스템(ISHS: IP Secure connectivity Host System)

ISHS 는 호스트에서 송/수신되는 데이터의 기밀성, 무결성, 접근 제어, IP 데이터그램에 대한 발신지 인증, 선택적인 Anti-Replay 서비스 등의 정보보호 서비스를 제공한다.

나. IP 보안연결 게이트웨이 서브시스템(ISGS: IP Secure connectivity Gateway System)

ISGS 는 게이트웨이에서 송/수신되는 데이터의 기밀성, 무결성, 접근제어, IP 데이터그램에 대한 발신지 인증, 선택적인 Anti-Replay 서비스 등의 정보보호 서비스를 제공한다.

다. 보안기반규칙 제어 서브시스템(ISCS: IP Security Control System)

ISCS 는 ISCAP 내의 보안상 취약점 분석과 감사 이벤트 처리, 시스템 및 IP 데이터의 모니터링을 통하여 보안상 문제점을 찾아내고 이를 운용자에게 보고함으로써 보안 관리자가 문제점을 해결할 수 있도록 서비스를 제공한다.

4. 인터넷 패킷보증 플랫폼에서의 정보보호 서비스

인터넷 패킷보증 플랫폼에서는 IP 레벨 정보보호 서비스를 제공한다. 따라서 IP 계층에서 정보보호 서비스를 제공하므로 상위 레벨 프로토콜 및 프로그램은 수정할 필요가 없다.

IP 레벨에서 IPv4/IPv6 를 지원하는 IPsec Engine 은 다음과 같은 정보보호 서비스를 응용 레벨 인터넷 서비스에 제공한다.

가. 기밀성(confidentiality)

메시지를 암호화하여 키를 가진 합법적인 사람을 제외하고는 중간에 불법적인 도청자가 메시지의 내용을 알아볼 수 없도록 하는 서비스이다.

나. 무결성(integrity)

메시지 변조를 할 수 없도록 하는 것으로 송신자가 메시지를 특정 수신자에게 전송할 경우 제 3 자가 불법적인 도청을 통해 전송한 메시지를 중간에서 가로챈 후 메시지를 변조하여 수신자에게 전송할 수 없도록 하는 서비스이다.

다. 데이터인증(data authentication)

서로를 직접 확인할 수 없는 인터넷상에서 상대에 대한 신뢰를 확보하기 위해 제공되는 서비스이다.

라. 접근 제어(access control)

불법적인 제3자의 접근을 완전히 차단하거나, 서로 다른 중요도를 가지는 정보 및 시스템에 대해서 접근 권한을 달리 부여하여 정보를 보호하는 서비스이다.

마. Anti-replay

한 번 사용된 메시지를 다시 사용할 수 없도록 하는 서비스로써, 송신자가 수신자에게 보낸 메시지를 중간에서 제 3 자가 가로채고 있다가 메시지 수신이 일단 완료된 후에 가로챈 메시지를 다시 보내 공격하는 것을 막는 서비스이다.

IV. 보안평가 시스템 설계

이 절에서는 3 절에서 분석한 인터넷 패킷보호 보증플랫폼에서의 보안성을 평가하여 보안상의 위협을 도출하고, 이를 관리자에게 알려줄 수 있고, 확장성을 갖는 보안평가 시스템을 설계하기 위하여 기능 요구 사항들을 도출하고 이를 충족시키기 위한 보안평가 시스템을 설계한다.

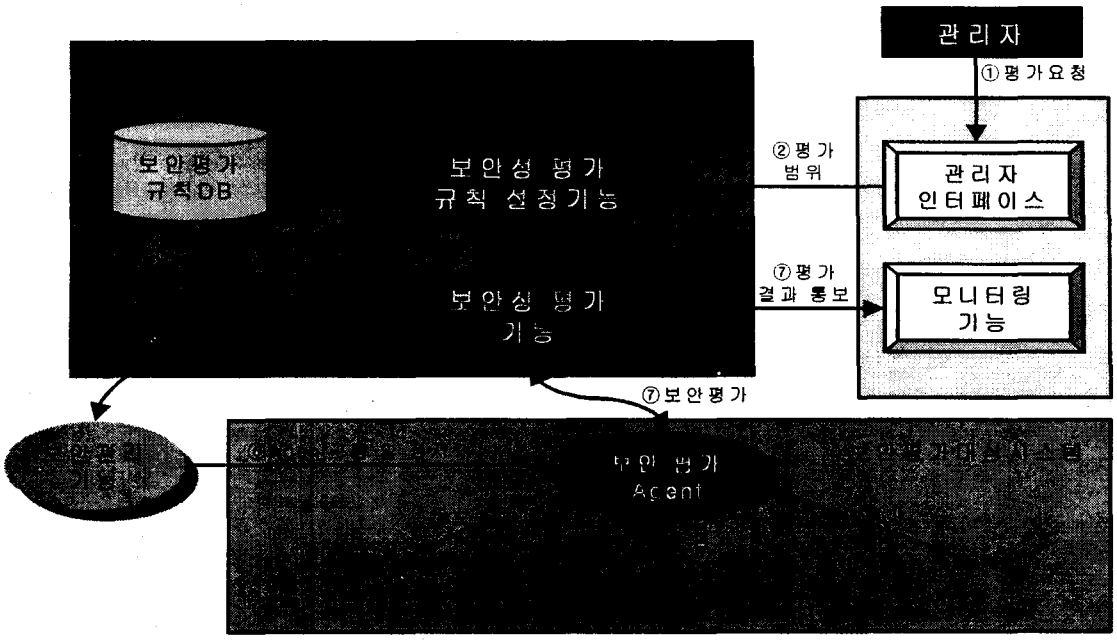
1. 보안평가 시스템에 대한 기능 요구사항

본 논문에서 설계하는 인터넷 패킷보호 보증플랫폼에서의 보안평가 시스템에 대한 기능요구사항은 다음과 같다.

- ISCAP 의 안전성 분석이 가능해야 한다.
- Linux 또는 Solaris 운영체제에서 보안평가 기능을 수행할 수 있어야 한다.
- 평가 룰 데이터베이스의 보안평가 룰을 사용한 룰 기반의 보안평가가 가능해야 한다.
- 보안평가 룰 관리 기능, 즉 룰의 추가, 삭제, 변경 등이 가능해야 한다.
- 관리자 툴을 사용한 중앙 집중식 관리를 제공해야 한다.
- GUI 를 이용한 ISCAP 의 취약점 상황 디스플레이가 가능해야 한다.
- Security Hole 발견 시 찾은 과정을 리포트하는 기능을 수행할 수 있어야 한다.
- 보안평가 후 시스템 설정 수정 권유를 할 수 있어야 한다.
- 에이전트를 이용한 특정 호스트의 low level 수준에서의 보안성 분석을 할 수 있어야 한다.
- 시스템의 버그 패치 여부를 확인할 수 있어야 한다.
- 특정 서브넷의 보안성 평가를 할 수 있어야 한다.
- 포트 스캐닝을 통한 네트워크 취약점을 분석할 수 있어야 한다.
- 각 서브넷의 모든 평가 정보를 수집해 전체 도메인의 보안성을 평가할 수 있어야 한다.
- 평가 기능을 모듈화하여 손쉽게 업그레이드할 수 있도록 하여야 한다.
- 지정한 시간에 자동으로 수행이 가능해야 한다.

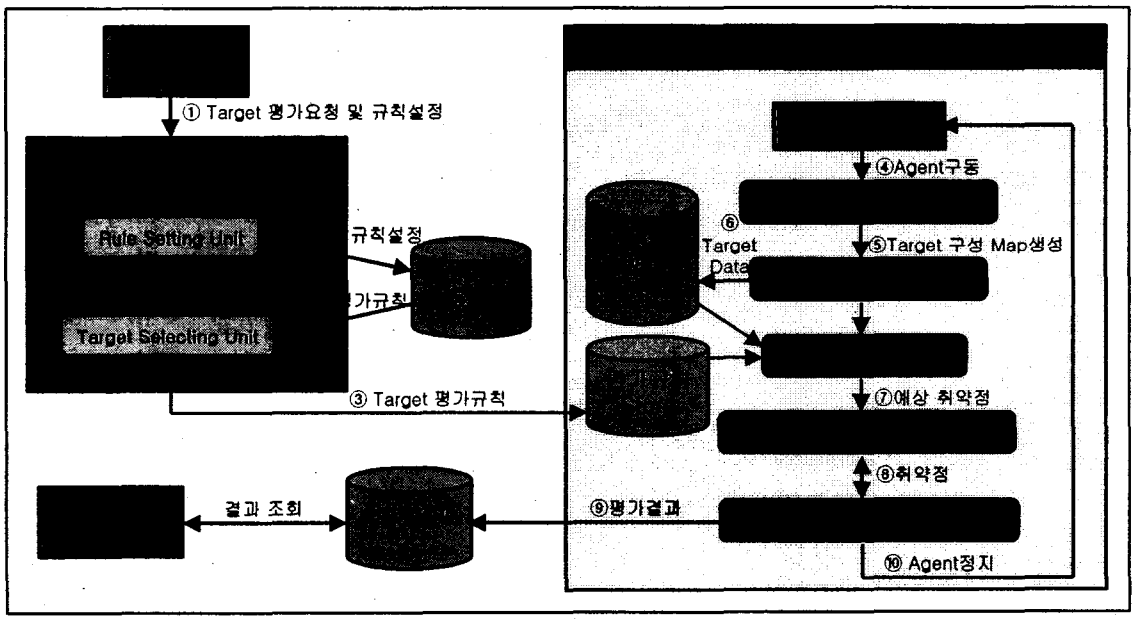
2. 보안평가 시스템의 구조 및 기능 흐름도

위의 기능 요구사항을 만족시키기 위하여 본 논문에서 제안하는 보안평가 시스템의 구조 및 기능 흐름도는 [그림 3]과 같다.



[그림 3] 보안평가 시스템의 구조 및 기능 흐름도

이러한 보안평가 시스템을 구성하는 블록의 내부 구조 및 흐름도는 [그림 4]와 같다.



[그림 4] 보안평가 시스템의 블록 내부 구조 및 흐름도

블록을 구성하는 각 요소들에 대한 세부 기능에 대한 정의는 다음과 같다.

가. 규칙제어 모듈(Rule Control Module ; RCM)

관리자가 GUI 를 통해 보안평가 환경을 설정하거나, 보안규칙 DB 의 보안평가 규칙을 관리하거나, 관리자가 설정한 보안평가 범위 및 대상에 해당하는 보안평가 규칙을 설정하여 주는 기능을 하는 모듈로서, GUI 와 보안평가 규칙 DB, 규칙 평가 모듈과 연동한다.

나. 규칙 평가 모듈(Rule Evaluation Module ; REM)

평가대상군의 네트워크 연결 현황을 파악하고, 평가대상군으로부터 평가에 필요한 데이터를 수집하여, 분석한 후 예상취약점을 도출하는 기능과 도출된 예상 취약점을 평가하여 취약점을 확인하는 기능을 하는 모듈로서, 평과 결과를 평과 결과 DB에 저장하고 GUI 를 통해 관리자에게 알려주는 기능을 포함한다. 또한 규칙제어 모듈, 평과 결과 DB 및 GUI 와 연동한다.

3. 보안평가 시스템의 수행 절차

보안평가 시스템의 처리절차는 다음과 같다.

<평가요청 수행 절차>

[관리자 -> GUI] 관리자가 GUI 를 통해 평가 대상 및 규칙을 설정한다.

<RCM 수행 절차>

[단계 1] GUI 를 통해 관리자가 설정한 평가 대상 및 규칙을 보안평가규칙 DB에 저장한다.

[단계 2] 보안평가규칙 DB 로부터 관리자가 요청한 평가 대상에 대한 규칙을 수집하여 평가규칙 Data Store 에 저장한다.

<REM 수행절차>

[단계 1] 보안평가 Agent 을 구동한다.

[단계 2] 평가 대상 네트워크 구성도를 생성한다.

[단계 3] [단계 2]에서 생성된 평가 대상에 관련된 Data 를 수집하여 평가 대상 Data Store 에 저장한다.

[단계 4] 평가규칙 데이터 Store 에 저장된 규칙을 평가 대상 Data Store 에 저장된 데이터에 적용하여 평가한다.

[단계 5] 평가한 결과를 통해 예상 취약점을 도출한다.

[단계 6] 도출된 예상 취약점에 대하여 평가 대상에 직접 취약점을 확인한다.

[단계 7] 발견된 취약점의 평가 결과를 평가결과 DB에 저장하고 결과를 출력한다.

[단계 8] 보안평가 Agent 을 정지한다.

<기타 수행절차>

[단계] 관리자는 필요할 때 언제든지 GUI 를 통해 평가결과 DB를 검색한다.

V. 결론

본 논문에서는 IP 레벨에서의 인터넷 공격 방법에 대하여 분석하고, 이러한 공격에 대처하는 서비스를 제공하기 위한 인터넷 패킷보호 보증플랫폼에 대한 시스템과 제공하는 정보보호 서비스에 대하여 분석하였다. 또한 ISCAP 이 제공하는 정보보호 서비스에 대한 보안성을 평가하기 위한 시스템에 대한 요구사항을 도출하고, 이를 충족하는 보안평가 시스템을 설계하였다.

제안한 보안평가 시스템은 인터넷 패킷보호 보증플랫폼에서 제공하는 정보보호 서비스에 대한 보안성을 평가하기 위한 기술들을 정의하고, 정의한 기술들을 이용하여 ISCAP 의 보안성을 평가하여 그 결과를 저장하고, 관리자가 필요시 그 결과를 참조할 수 있는 기능을 가지고 있다.

또한 ISCAP 에서 기밀성, 무결성, 데이터 인증, 접근제어, Anti-replay 등의 정보보호 서비스를 제공하기 위한 프로토콜들의 보안성을 평가하기 위한 기술을 제안하였다.

앞으로 IP 레벨에서의 정보보호 서비스를 제공하기 위하여 개발되는 시스템에 대한 보안성을 평가해 주는 확장성을 고려한 보안평가 시스템에 대한 많은 연구가 필요하다.

참고문헌

[1] 이재승, 김상춘, 이종태, 김경범, 손승원, "대규모 네트워크 환경하에서의 침해사고 예방을 위한 보안평가 시스템 설계", 제12회 정보보호와 암호에 관한 학술대회(WISC 2000), pp. 160 ~ 176

[2] Larry J. Hughes, Jr., *Actually Useful Internet Security Techniques*, New Riders Publishing, 1995

[3] 이재승, 김상춘, 김경범, 손승원, " 대규모 네트워크 보안성 분석 자동화를 위한 보안평가 시스템의 설계", 제 5 회 통신소프트웨어 학술대회 COMSW2000(The 5th Conference on Communication Software), pp. 172 ~ 176

[4] ISS, "Network and Host-based Vulnerability Assessment," http://documents.iss.net/whitepapers/nva.pdf

[5] Vulnerability Testing, http://esperosun.chungnam.ac.kr/~jmkim/firewall/vulnerability/vul00.html

[6] 한국전산원, " 정보시스템 보안을 위한 위험분석 소프트웨어 개발 보고서" , 1997

[7] IETF RFC1828, " IP Authentication using Keyed MD5"

[8] IETF RFC1829, " The ESP DES-CBC Transform"

[9] IETF RFC 2085 HMAC-MD5, " IP Authentication with Replay Prevention"

[10] IETF RFC2104 HMAC, " Keyed-Hashing for Message Authentication"

[11] IETF RFC2401, " Security Architecture for the Internet Protocol"

[12] IETF RFC2402, " IP Authentication Header(AH)"
[13] IETF RFC2403, " The Use of HMAC-MD5-96 within ESP and AH"
[14] IETF RFC2404, " The Use of HMAC-SHA-1-96 within ESP and AH"
[15] IETF RFC2405, " The ESP DES-CBC Cipher Algorithm With Explicit IV"
[16] IETF RFC2406, " IP Encapsulating Security Payload(ESP)"
[17] IETF RFC2407, " The Internet IP Security Domain of Interpretation for ISAKMP"
[18] IETF RFC2408, " ISAKMP"
[19] IETF RFC2409, " The Internet Key Exchange(IKE)"
[20] IETF RFC2410, " The NULL Encryption Algorithm and Its Use With IPsec"
[21] IETF RFC2411, " IP Security Document Roadmap"
[22] IETF RFC2412, " The OAKLEY Key Determination Protocol"
[23] IETF RFC2451, " The ESP CBC-Mode Cipher Algorithms"
[24] IETF Internet-Draft, " Security Policy System"
[25] IETF Internet-Draft, " Security Policy Protocol"
[26] IETF Internet-Draft, " Policy Framework for IP Security"
[27] IETF Internet-Draft, " IPsec Policy Schema"
[28] IETF Internet-Draft, " IPsec Policy Discovery Protocol requirements"
[29] IETF Internet-Draft, " Security Policy Specification language"