通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

정보보호시스템의 보안기능 통합평가 도구

이 경 현*, 박 영 호*, 조 현 호*, 김 창 수*, 노 병 규**

요 약

본 연구에서는 정보보호시스템의 신분확인 기능과 데이터 무결성 기능 그리고 네트워크 취약성 평가를 수행할 수 있는 정보보호시스템의 보안기능 통합 평가 도구를 개발하였다. 개발된 도구는 독립적으로 수행되어온 평가기능들을 통합, 개선함으로써 네트워크를 통해 연결되어 있는 시스템의 안전성을 총체적으로 평가할 수 있으며, 또한 네트워크의 보호를 목표로 개발된 침입차단시스템의 구성상의 취약성이나 IPSec이나 SSL을 적용하여 가상사설망(VPN)을 구현한 제품들에서 제공하는 무결성을 검증하기 위한 자동화된 도구로서 활용될 수 있다.

Ⅰ. 서 론

네트워크 기술의 발전과 인터넷의 급속한 확장으로 네트워크의 활용 영역을 다양한 분야로 확대시키려는 노력이 증가함에 따라 이를 불법적으로 이용하려는 악의적인 침입자들도 증가하고 있는 추세이다. 이로 인해 다양한 서비스를 위해 사용되는 인터넷에서 직면하는 가장 중요한 문제로 개인정보의 보안과 암호화의 필요성을 함께 지적하고 있다. 이러한 정보보호의 개념 및 기술을 통해 허가된 사용자들에게 올바른 서비스를 제공하기 위한 신분확인 기능과 네트워크 상에서 데이터의 기밀성과 인증, 데이터 무결성에 대한 검증이 필수적으로 요구되는 현실이다.

이처럼 정보보호에 대한 필요성이 대두됨으로써, 대부분 보안 전문가들은 외부 네트워크 즉, 인터넷을 통한 침입으로부터 내부 네트워크를 보호하기 위한 수단으로 침입차단시스템(Firewall)의 설치를 권장하고 있다. 또한 외부 네트워크와의 정보 교환에 대한 요구와 재택 근무의 증가로 인해 네트워크의 범위가 점차 확대됨에 따라 상호간에 안전한 통신을 위해 공중망 환경에서의 보안에 대한 취약성을 개선하여 사설망과 같은 환경을 구성하는 가상사설망(Virtual Private Network)의 개념이 제안되고 있다. 그러나 이들 보안제품에 대한 안전성을 소프트웨어공학 측면에서의 보안성 추정 모형[1, 2]이나 정보보호시스템의 평가기준들을 공개하고 있으나 보안제품들의 보안기능을 다각적인 시각에서 통합적으로 평가할 수 있는 도구는 사실상 전무한 실정이다. 따라서 본 연구에서는 개별적으로 수행되어온 네트워크 위협 유형 및 침입차단시스템의 취약성 평가, 신분확인 기능 평가와 전송데이터의 무결성 검정기능을 통합적으로 수행할 수 있는 보안기능 평가 도구를 개발하였다.

II장에서 현재 보편적으로 사용되고 있는 정보보호시스템의 보안기능과 시스템의 취약성에 대해 살펴보고, III장에서는 개발된 보안기능 평가도구의 구성 및 동작원리에 대해서 설명한다. 마지막으로 IV장에서는 향후과제에 대해서 논의한 뒤 결론을 맺도록 한다.

Ⅱ. 정보보호시스템의 보안기능 및 취약성

2.1 침입차단시스템

현재와 같이 네트워크의 규모가 방대해진 현실에서 많은 수의 시스템 각각을 일일이 점검하고 거기에 맞는 보안 대책을 마련하여 적용하는 것은 쉬운 일이 아니다. 따라서, 이러한 문제점을 해결하기 위해서 내부 네트워크와 외부 네트워크의 연결점에서 내부 네트워크 상의 시스템들을 보호할 수 있는 네

* 부경대학교 (pyhoya@mail1.pknu.ac.kr)
** 한국정보보호센터

트워크 구성 요소가 필요하게 되었고, 이러한 기능을 담당하는 시스템이 바로 침입차단시스템이다.

2.1.1 침입차단시스템의 기능

침입차단시스템은 일반적으로 패킷 필터링(Packet filtering)과 사용자 인증에 기반을 두고 외부로부터의 침입을 차단하게 된다. 허용된 네트워크 사용자들에게는 원하는 서비스를 제공하면서 허용되지 않은 사용자들에게는 서비스를 차단하고, 해당 서비스의 허용 또는 실패에 대해 기록하게 된다.

패킷 필터링 시스템은 네트워크 계층과 전송계층에서 유입되는 패킷의 허용 여부를 결정하는 기능을 한다. 이 때 패킷의 허용 여부는 관리자에 의해 명시되는 접근제어규칙(Access control rule)에 기반을 두고 이루어지므로 올바른 접근제어규칙의 설정이 중요하다고 할 수 있다.

프록시 서버는 TCP/IP 응용 계층(Application layer)에서 트래픽을 가로채어 검사한다. 프록시 서버의 목적은 인터넷에 접속하려고 하는 사용자의 신분을 파악하고 권한이 있을 경우 접속을 허락하도록 하는 것이다. 사용자가 외부 또는 내부 네트워크상의 호스트나 서비스에 직접 접속하지 않고 프록시(Proxy) 시스템이 모든 접속을 중간에서 처리하며, 이때 모든 접속은 프록시 시스템의 보안 기능에 의해 제어되기 때문에 허가되지 않은 사용자나 호스트, 명령어들의 접근이나 수행을 막을 수 있다.

2.1.2 침입차단시스템의 취약성

침입차단시스템의 사용은 내부 네트워크를 외부 네트워크로부터 보호해주는 이점을 제공해 준다. 하지만 이러한 침입차단시스템에도 다음과 같은 몇 가지 취약성이 존재한다[3, 4].

- 시스템 내부의 결함
- 시스템 운영자의 관리 소홀
- 내부사용자에 의한 공격 및 정보 유출

2.2 신분확인 시스템

신분확인이란 서버와 클라이언트 사이의 정보교환에서 사용자의 실제 신원을 확인하는 과정을 의미한다. 신분확인의 목적은 사용자에 대한 신분 보장을 제공하는 것이며, 신분위장 및 재전송 공격들의 위협으로부터 시스템을 보호할 수 있어야 한다. 클라이언트/서버 환경에서 사용자의 신분을 확인하기 위한 다양한 방법들이 있지만 구현상의 이유 등으로 인해 사용자만이 알고 있는 패스워드의 전달을 이용한 방법이 일반적으로 사용되고 있다.

2.2.1 패스워드 전달을 이용한 신분확인

일반적으로 UNIX계열 시스템은 사용자의 패스워드를 /etc/passwd 혹은 /etc/shadow 파일에 암호 알고리즘으로 암호화해서 저장한다. 비록 패스워드를 암호화된 형태로 안전하게 보관하지만 패스워드를 이용한 신분확인 시스템은 다음과 같은 취약성을 가지게 된다[5, 6].

- 패스워드 도청(eavesdropping)
- 패스워드 추측(guessing)
- 패스워드 재연(replay)
- 부적절한 패스워드의 사용
  - 사용자의 이름 또는 그 이름을 변형하거나 반복한 형태들
  - abcdef, abcd1234 혹은 AAAA와 같은 문자의 연속이나 반복
  - 좋아하는 사람이나 가족들의 이름
  - 간단한 형태의 사전단어
  - 위와 같은 형태의 조합 등

2.2.2 일회용 패스워드를 이용한 신분확인

일반적인 패스워드 시스템은 매번 같은 패스워드를 사용하는 정적인 특성으로 인해 사용자의 신분확인정보를 재연(Replay)할 가능성이 존재하게 된다. 이런 문제의 해결방안으로 일회용 패스워드(One-time password)처럼, 로그인마다 패스워드가 자동으로 변경됨으로써 패스워드의 도난이나 분실로 인한 재연공격을 막기 위한 다양한 방안들이 사용되고 있다.

단순한 패스워드 사용방식을 개선한 일회용 패스워드 기법은 사용자만이 알고있는 비밀문구(pass-phrase)로부터 일련의 일회용 패스워드들을 생성하는데 수행되는 일 방향 함수(one-way function)의 계산능력을 이용한다. 이러한 방식을 사용하는 대표적인 신분확인 기법으로 S/Key[7]가 있다.

S/Key는 클라이언트나 서버 양쪽 모두 안전한 일 방향 해쉬함수(One-way hash function)를 사용하지만 다음과 같은 취약성을 가지게 된다[8].

- 신분확인을 위한 패스워드만 보호
- 해쉬함수에 기반 하는 시큐리티
- 사전 공격(Dictionary Attack)에 대한 취약성

따라서 S/Key의 안전성은 전적으로 사용자에 의해 선택된 비밀문구와 S/Key 계산에 사용되는 해쉬함수의 안전성에 의존하므로 사용되는 패스워드 단어에 대한 통계적 임의성 평가와 해쉬함수에 대한 충돌회피성 등을 검정하여야 한다. 또한 S/Key를 계산하기 위해 원격지의 S/Key 계산기를 사용한다면, 스니핑과 같은 방법으로 전송되는 사용자의 비밀문구가 노출될 수 있다. 비밀문구의 노출은 곧 S/Key의 위협으로 직결되므로, S/Key의 계산은 반드시 로컬 시스템에서 하도록 해야 한다.

2.3 가상사설망(Virtual Private Network)

공중망 환경에서 상호간의 안전한 통신을 위해 암호화와 인증 기능을 제공하기 위한 가상사설망에 대한 많은 연구가 이루어지고 있다. 가상사설망의 구현은 IETF에서 제안하는 IP계층에서의 보안 프로토콜인 IPSec[9]을 이용한 구현과 SOCKSv5[10]를 사용한 응용계층에서의 구현으로 구분할 수 있으며[11], 가상사설망과 관련된 대부분의 제품들이 IPSec에 기반을 두고 개발되고 있다.

IETF에서 제안하는 IPsec은 IP 계층에서의 보안 프로토콜로 네트워크 계층에서 인증(Authentication)과 기밀성(Confidentiality) 그리고 무결성(Integrity)을 제공한다[9]. IPSec은 단말호스트간의 터널링(Tunneling) 기능이 가능한 하위 계층에서 구현이 가능하며, 응용 소프트웨어의 수정 없이 IP 데이터그램의 페이로드로 전해지는 상위계층의 응용프로그램의 데이터그램을 보호할 수 있기 때문에 많이 사용된다.

가상사설망의 사용에 따른 문제점으로는 공중망의 사용에 있어서 어떻게 전용선에서와 같은 QoS(Quality of Service)와 보안 기능을 사용자에게 투명하게 제공해 줄 수 있는가 하는 것이다. 보안에 관해서는 현재 개발자들이 각기 프로토콜을 설계하여 사용하고 있으나 가상사설망이 공중망의 사용을 전제로 하고 있으므로 호환성의 문제를 고려해야 한다.

Ⅲ. 정보보호시스템 보안기능 통합 평가도구

본 연구에서 개발한 정보보호시스템 통합평가 도구는 신분확인기능 평가와 네트워크 취약성 평가 그리고 데이터 무결성 평가로 구분된다. 신분확인기능 평가에서는 사용자의 신분확인을 위해 사용되는 패스워드에 대한 평가를 통해 해당 시스템의 취약한 패스워드와 S/Key 패스워드의 동작상의 취약성을 평가한다. 네트워크 취약성 평가에서는 침입차단시스템의 응용서비스별 보안기능을 평가함으로써 침입차단시스템의 구성상의 취약성 및 오용여부를 평가하고, 포트스캐닝과 SYN flood를 이용해서 네트워크 공격에 대한 취약성을 평가한다. 데이터 무결성 기능 평가에서는 가상사설망이 적용된 환경에서 전송되는 패킷의 변조 여부를 IP계층과 응용계층으로 구분하여 검사하도록 한다.

신분확인기능 평가와 침입차단시스템의 취약성 평가를 위해 TIS의 FWTK(Firewall Tool Kit)를 사용하여 평가환경을 구축하였고, 데이터 무결성 평가를 위해 공개용 IPSec 제품인 FreeS/Wan과 SSL을 사용하여 평가환경을 구축하였다.

3.1 신분확인기능 평가

신분확인기능 평가는 telnet, ftp, http 서비스를 사용하여 시스템의 로그인에 사용되는 패스워드와 관련된 평가를 수행한다. 이때 평가대상이 되는 패스워드는 일반적인 패스워드와 일회용 패스워드인 S/Key 패스워드로 구분할 수 있다. 표 1은 신분확인기능 평가항목을 요약하여 보여준다.

〔표 1〕 신분확인기능 평가 항목

평가구분	평가항목
패스워드 시스템 평가	무효한 패스워드 평가
	특수문자 포함 패스워드 평가
	패스워드 길이제한 평가
	패스워드 추측 평가
S/Key 동작 평가	S/Key 반복수 평가
	S/Key 임의단어 평가

telnet이나 ftp의 경우는 대상시스템에 로그인을 위해 사용자의 ID와 패스워드를 요구하게 되며, http의 경우 사용자의 신분확인을 필요로 하는 특정 디렉토리별로 정의된 신분확인 기능을 평가하게 되는데, http 프로토콜은 사용자의 인증을 위한 방법으로 기본인증(Basic authentication)과 MD5 다이제스트 인증(Digest authentication)을 제공한다[12, 13].

본 연구에서는 각 평가모듈별을 통해 반복적으로 생성된 패스워드를 온라인상에서 직접 평가 대상시스템의 로그인을 위해 사용함으로써 평가를 수행한다.

3.1.1 UNIX 패스워드 및 S/Key 패스워드 평가

패스워드 평가에서는 무효한 패스워드(invalid password) 평가, 특수문자 패스워드 평가, 패스워드 추측 평가 그리고 패스워드 길이제한 평가로 구성된다.

- 무효한 패스워드(Invalid Password) 평가

무효한 패스워드 평가는 사용자가 입력한 유효한 패스워드의 변형을 통해 무효한 패스워드를 자동으로 생성하여 목표 시스템에 반복적으로 접속을 시도함으로써 평가하게된다.

- 특수문자 패스워드 평가

유효한 패스워드를 일반적인 특수문자와 조합하여 패스워드 테스트를 수행한다. 테스트를 수행하기 위해 유효한 패스워드를 입력하고, 패스워드 테스트에 사용될 특수문자를 선택한다.

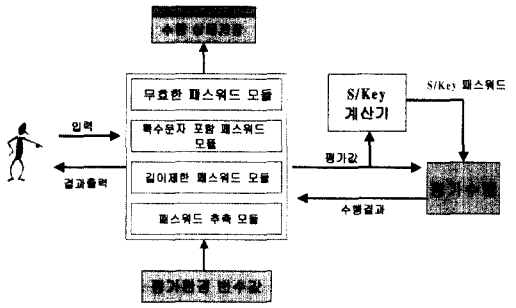
- 패스워드 추측(Password guess) 평가

패스워드 추측 평가는 패스워드로 사용 가능한 모든 문자들의 조합을 이용해서 임의의 패스워드를 만드는 방법과 패스워드 사전(password dictionary)을 이용하여 온라인(on-line)상에서 직접 생성된 패스워드를 평가하는 방법으로 나뉜다.

- 패스워드 길이제한 평가

모든 가능한 문자의 조합으로 생성되는 패스워드의 길이를 제한해서 평가하는 방법이다. 최소 길이와 최대 길이로 지정된 길이의 모든 패스워드를 생성하여 평가하도록 한다. 패스워드의 최소 길이는 4자 이상이어야 하고 최대 길이는 8자 이하이다.

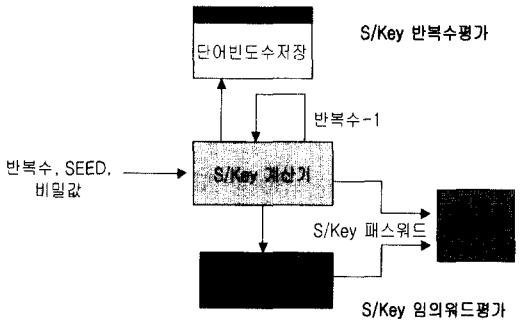
S/Key 패스워드 평가에서는 각 평가모듈별로 생성된 패스워드를 S/Key 패스워드를 계산하기 위한 비밀문구로 사용한다. 이때 S/Key 패스워드를 계산하기 위한 해쉬함수로서 MD4와 MD5를 선택적으로 사용할 수 있도록 하였다. 평가 수행과정은 그림 1과 같다.



〔그림 1〕 패스워드 평가 시스템 모듈 구성도

3.1.2 S/Key 동작 평가

S/Key 동작 평가에서는 S/Key 신분확인 메커니즘과 관련해서 S/Key 생성을 위한 반복수와 S/Key 일회용 패스워드를 구성하는 단어들에 대한 평가를 수행한다.



〔그림 2〕 S/Key 동작평가 모듈 구성도

S/Key 반복수 평가를 통해 시스템의 해쉬함수의 반복횟수가 올바르게 동작하는지 여부를 평가한다. 입력된 반복수를 0까지 1씩 감소시키면서 해당 반복수를 이용해 생성된 S/Key를 사용하여 시스템에 접속함으로써 평가를 수행한다. 이때 S/Key 패스워드로 사용된 단어들을 카운트하여 S/Key 단어사전에서 사용된 단어들의 출현빈도를 기록하여 단어들의 통계적 임의성을 평가하도록 하였다.

그리고 S/Key 임의워드 평가를 통해 실제로 계산된 S/Key 패스워드의 단어들을 단어사전에 없는 패스워드 단어로 변경하여 시스템에 접속을 시도함으로써 평가를 수행하도록 하였다. 그림 2는 S/Key 동작평가 모듈의 구성을 보여준다.

3.2 네트워크 취약성 평가

네트워크 취약성 평가는 침입차단시스템 프록시 서버의 취약성 평가와 네트워크 공격 취약성 평가로 나누어진다. 표 2는 네트워크 취약성 평가 항목을 요약해서 보여주고 있다.

〔표 2〕 네트워크 취약성 평가 항목

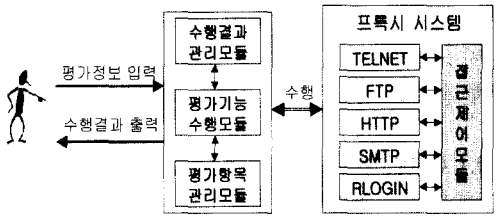
평가구분	평가동작	평가항목
프록시 시스템 평가	telnet	파일전송 허용 여부
	ftp	파일전송, 생성/삭제
	http	URL 제한, Java/ActiveX제한
	smtp	메일크기, 메일개수, 첨부파일 제한
	rlogin	기본항목 평가
네트워크 위협 평가	portscan	시스템의 listening 포트 검색
	SYNflood	SYNflooding 공격에 대한 평가

3.2.1 침입차단시스템 취약성 평가

침입차단시스템은 시스템을 설치할 때 발생할 수 있는 구성상의 취약성과 시스템에서 운용되는 프로그램의 취약성으로 인한 시스템 자체의 취약성을 가질수 있다. 현재 국내에서는 한국정보보호센터에서 침입차단시스템에 대한 평가를 담당하고 있으며, 본 연구에서는 한국정보보호센터에서 침입차단시스템의 평가요소로 제시한 평가항목에 대해 자동화된 평가를 수행할 수 있도록 하였다.

침입차단시스템 평가는 telnet, ftp, rlogin, http, smtp 각각의 서비스에 대해 침입차단시스템의 프록시 서버를 경유해서 목표 시스템에 접속했을 때 프록시 서버의 각 서비스별로 설정된 동작을 평가함으로써 시스템에서 발생할 수 있는 구성상의 취약성 및 오용 가능성을 평가한다. 사용자는 원하는 서비스를 선택하고 평가에 필요한 값들을 설정하여 해당 시스템에 접속함으로써 평가를 수행하게 된다. 침입차단시스템 취약성 평가 기능의 시험평가를 위해 TIS사의 FWTK(Firewall Toolkit)을 설치하여 평가를 수행하였다.

각 서비스의 공통 평가항목으로 연결제한 개수 평가항목을 설정하여 제한된 개수를 초과하는 접속에 대한 제한 여부를 평가하고, 타임아웃(time out)을 설정하여 아무런 입력 없이 지정된 시간이 경과한 후의 연결 종료 여부를 평가한다. 그림 3은 프록시 시스템 평가를 위한 시스템 구성을 보여주고 있다.



〔그림 3〕 프록시 시스템 평가 구성도

3.2.2 네트워크 공격 취약성 평가

네트워크를 통한 공격에 대한 취약성평가는 포트스캔(Portscan)과 SYNflood공격에 대한 평가로 구성된다. 포트스캔을 수행해서 대상 시스템에서 현재 동작중이거나 대기(listening)상태에 있는 포트들을 검색한다. 포트스캐닝 자체는 시스템에 직접적인 공격을 행하지는 않지만 해킹의 초기단계에서 시스템에서 실행중인 특정서비스와 같은 정보를 얻기 위해 우선적으로 행해지는 기법이다.

포트스캔 평가를 통해 해당 시스템에 실행중인 포트를 검색하고, DoS(Denial of Service)의 일종인 SYNflood를 이용해서 실제 해당 시스템의 특정 포트로 사용자가 입력한 수만큼의 SYN 패킷을 전송하여 공격을 수행함으로써 해당 공격에 대한 감지와 차단 여부 및 backlog queue의 설정을 파악할 수 있도록 한다. SYNflood 공격을 수행 후, 해당 시스템으로의 접속 가능여부를 조사함으로써 네트워크를 통한 공격의 취약성을 평가한다.

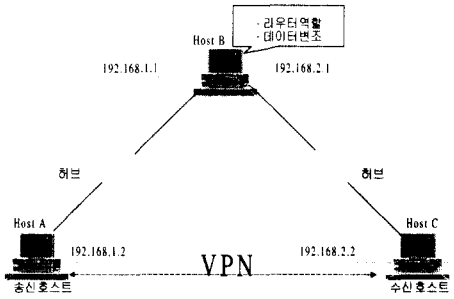
3.3 전송 데이터의 무결성 평가

본 절에서는 전송데이터의 무결성을 평가하기 위해 VPN을 구성하는 방법 중 IP 계층에서의 무결성을 제공하기 위해 국제 표준으로 자리잡고 있는 IPsec을 적용한 시스템에 대한 무결성 평가와 응용계층에서의 무결성을 제공하는 시스템들에 대해 평

가를 수행하였다.

시험평가는 공개용 IPSec 제품인 FreeS/Wan과 OpenSSL을 설치하여 평가를 수행하였으며, 전송 데이터의 무결성을 검증하기 위한 평가환경으로 다음 사항을 구현하여 평가하였다.

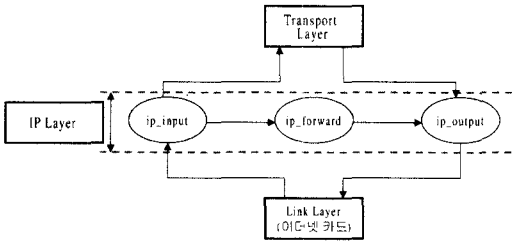
- 데이터 무결성을 보장하기 위한 제품들이 설치된 환경 하에서의 데이터 통신의 무결성을 검증하기 위해서 라우터의 커널을 수정하여 패킷 변조 기능을 커널에 포함시킨다.
- 패킷 변조에 대한 정보를 사용자 입력을 통해 동적으로 설정하고 변경된 패킷에 대한 정보를 보여주기 위해 커널과 사용자간에 정보를 주고받을 수 있도록 한다.
- 응용 계층에서의 무결성 검증을 위해서는 패킷이 변조된 경우라도 트랜스포트 계층의 검사합(Check-sum)을 통과하여야 함으로 이 경우에 변경된 패킷의 내용에 따라 검사합을 재 계산하도록 한다.



〔그림 4〕 전송데이터 무결성 평가 환경 구성

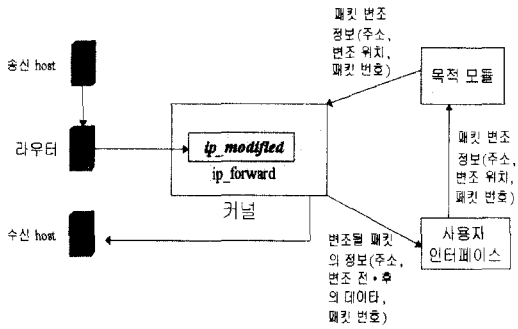
전송데이터의 무결성을 검증하기 위한 테스트 환경은 그림 4와 같다. 그림에서처럼 Host A와 Host C간의 통신은 IPSec이나 SSL을 적용하여 무결성을 보장한다. 데이터 무결성을 탐지하기 위해 역시 Linux를 사용하여 VPN을 구현해 보았다. Host A와 C 간에 통신을 할 때 Host B를 경유하도록 하기 위해서 Host B가 라우터 역할을 하도록 하는 가상 네트워크를 구성하였다.

그림 5는 라우터의 IP계층에서의 패킷 처리 과정을 보여주고 있다. 무결성 검사를 위해 그림 6과 같이 라우터의 커널의 ip_forward에 패킷을 변조하기 위한 루틴을 추가하여 입력받은 정보를 이용해서 라우터를 통과하는 패킷을 변조하고 수신측에서 변조 여부를 확인하는 방법으로 평가를 수행하였다.



〔그림 5〕 라우터의 패킷 처리 과정

변조를 위해 입력되는 정보로 변조를 위한 가상의 패킷 번호와 변조 위치 그리고 변조를 위한 간격을 입력하도록 하였다.



〔그림 6〕 무결성 평가 모듈 구성

Ⅳ. 결론 및 향후과제

최근 네트워크의 발전으로 인해 네트워크가 정보수집의 중요한 수단이 되는 동시에 이를 악용하는 사례가 늘어나고 있으며, 실제로 이러한 침해 사고들이 여러 언론 매체를 통해 보도되고 있다.

이는 알려진 취약점에 대한 패치를 실시하지 않거나 또는 잠재적인 취약점이 존재하는 불필요한 서비스를 실행시키는 것과 같은 관리상의 소홀함이나 미숙함이 주요 원인이 되고 있으며, 또한 사용자들은 공격자들에 의해 크랙 당하기 쉬운 취약한 패스워드를 무분별하게 사용함으로써 공격자들에게 공격의 수단을 제공해 주기도 한다.

이러한 추세에 맞추어 침입차단시스템, 그리고 가상사설망과 같은 여러 보안 강화 제품들이 쏟아져 나오고 있으나 이들에 대한 보안 수준을 다각적인 시각에서 평가할 도구는 사실상 전무한 실정이다.

따라서 본 연구에서는 사용자 신분확인 기능과 취약성 평가 그리고 무결성을 평가기능을 통합, 개선함으로써 총체적이며 자동화된 평가를 수행하기 위한 정보보호시스템 보안기능 통합평가 도구를 개발하였다.

본 연구에서 개발된 통합평가 도구를 사용함으로써, 관리자들은 시스템의 취약성과 다양한 위협 요소들을 사전에 평가하고 분석함으로써 외부로부터의 불법적인 침입에 대한 허점을 미연에 방지할 수 있는 관리 도구로서 그 역할을 수행할 수 있을 것으로 판단된다.

한편 본 연구에서 개발된 소프트웨어는 정보보호 시스템의 네트워크 상에서의 종합적인 보안기능 평가를 수행할 수 있는지의 판단에 초점을 맞추어 개발되었으며, 본 평가도구의 각 평가항목에 대한 시험평가를 일부 제품에 대해서만 실시하였으므로 향후 여러 보안제품에 대한 시험평가를 통해 본 개발 도구의 기능을 수정 보완한다면 추후 개발될 정보보호 제품의 안전성 및 취약성 평가를 위한 도구로서 적절히 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 고정호, 김경렬, 이강수, "정보보호 제품 및 시스템의 보안성 측정 모델", 제10회 정보보호와 암호화에 관한 학술대회, WISC 98', p.450-462, 1998

[2] 장화식, 이경현, "암호 모듈 및 정보보호시스템의 보안성 추정 모형", 1999 한국멀티미디어학회 추계학술발표 논문집 p.59-63, 1998

[3] 한국전산원 표준본부, "방화벽 시스템의 구축과 운용", 1996.

[4] "네트워크 취약성 분석 및 평가 S/W 개발", 한국정보보호센터 시험평가 99-5 최종연구보고서, 1999.

[5] Walter Belgers, "UNIX Password Security", 1993. Preprint, http://andercheran.aiind.upv.es/toni/unix/index_en.html

[6] Simpson Garfinkel, Gene Spafford, "Practical Unix and Internet Security 2nd Edtion", O'Reily & Associates, Inc

[7] N. Haller, "The S/Key One-time Password System", Proceedings of the ISOC Symposium on Network and Distributed System Security, 1994.

[8] "정보보호시스템 신분확인기능 평가 S/W 개발", 한국정보보호센터 시험평가 99-3 최종연구보고서, 1999.

[9] Naganand Doraswamy, Dan Harkins, "IPSec: The New Security Standard for the Internet, Intranet and Virual Private Networks", Prentice Hall PTR, 1999.

[10] M. Leech, M. Genis, Y. Lee, R. Kuris, D. Koblas, L. Jones, "SOCKS Protocol Version 5", RFC 1928, March, 1996.

[11] "정보보호시스템 무결성 기능 평가 S/W 개발", 한국정보보호센터 시험평가 99-4 최종연구보고서, 1999.

[12] Berouz A. Forouzan, "TCP/IP Protocol Suit", McGrawHill, 1998.

[13] J. Frank, P. Hallam-Barker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June, 1999.

〈著者紹介〉

이 경 현 (Kyung-Hyune Rhee) 정회원

1982년 : 경북대학교 수학교육과 졸업
1985년 : 한국과학기술원 석사
1992년 : 한국과학기술원 박사
1982년~1993년 3월 : 한국전자통신연구소 선임연구원
1993년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 부교수
관심분야 : 암호학, 정보보호, 네트워크 보안

김 창 수 (Chang-Su Kim)

1984년 2월 : 울산공과대학교 전자계산학과 졸업
1986년 2월 : 중앙대학교 전자계산학과 석사
1991년 2월 : 중앙대학교 전자계산학과 박사
1992년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 부교수
관심분야 : 실시간 운영체제, VPN구현, 보안S/W, GIS/GPS

노 병 규 (Byung-Gyu No)

1991년 : 충남대학교 대학원
1988년~1997년 : 한국전자통신연구소 선임연구원
1997년~현재 : 한국정보보호센터 평가2팀장
관심분야 : 침입탐지시스템, 침입차단시스템, 시스템평가, 정보보호

박 영 호 (Young-Ho Park)

학생회원

2000년 2월 : 부경대학교 전자계산학과 졸업
2000년 3월~현재 : 부경대학교 전자계산학과 석사과정
관심분야 : 정보보호, 네트워크 보안

조 현 호 (Hyun-Ho Cho)

1997년 2월 : 부경대학교 전자계산학과 졸업
2000년 3월~현재 : 부경대학교 전자계산학과 석사과정
관심분야 : 정보보호, 네트워크 보안