《主 題》

인터넷의 보안

임찬순, 임채호, 변옥환
(시스템 공학 연구소)

□차 례□

Ⅰ. 개요

인터넷은 전세계 150여 개국 6천만 명 이상의 사용자가 활동하고있는 Network of Networks로서 최근에는 특히 Web과 전자 거래 등 상용화 서비스의 확산과 더불어 급속도로 그 규모가 확장되고 있다.

이러한 인터넷의 확산과 더불어 전세계적으로 대학, 연구소, 관공서 그리고 기업체들이 기관이나 조직간의 정보 교류의 중요성이 부각되고 있으며 외부에 공개할 자료와 보안을 유지할 자료의 구분의 필요성이 그 어느 때 보다 증대하고 있다.

인터넷은 유닉스 호스트와 TCP/IP 프로토콜 중심의 개방형 구조를 가지고 있으며 또한 많은 유틸리티들을 사용하고 있는데, 특히 이들은 정보 보안에 많은 취약성을 가지고 있다.

인터넷에서 제공하는 서비스(FTP, Telnet, DNS, SMTP, NFS 등)가 근본적으로 가지는 보안에 대한 취약성과 잘못된 시스템 구성, 접근 제어 등에 기인하여 인터넷에서 제공하는 서비스 중 약 5백여개가 거의 주요 공략 대상이 되고 있다. 따라서 보안에 대한 시스템 관리자의 역할이 매우 중요하며, 불법 침입에 대한 예방적 차원, 방어적 차원, 사후 조치 차원의 대책과 좀 더 실용적인 보안 연구가 절실히 필요한 시기이다.

국내에도 95년을 전후하여 CERT-KR 발족을 선두로 서울 지방 검찰청 컴퓨터 범죄 수사 센터, 경찰청 해커 수사대 가동, 그리고 금년 3월중 발족되는 정보보호 센터의 활동을 계기로 불법 침입 등의 보안 사고에 대한 대응 방안 및 연구가 활성화되리라 예상된다.

본 고에서는 인터넷에서 보안 현황, 문제점 그리고 대응 방안을 중심으로 기술하고자 한다. 먼저 2 장에서는 인터넷에서 보안 문제가 발생하는 원인과 보안 사건의 예를 보이고, 3장에서는 이러한 인터넷 상의 보안 문제를 해결하기 위한 보안 대책에 대하여 기술한다. 특히 현재 가장 중요하다고 생각되는 적극적 방어 대책인 방화벽 시스템(firewall system)에 대하여 비교적 자세히 기술한다. 4장에서는 인터넷 보안 사고 처리 방법에 대하여 기술하고, 5장에서는 인터넷 보안 연구 활동 현황에 대하여 고찰하고, 마지막으로 6 장에서 결론을 맺는다.

Ⅱ. 인터넷 보안의 취약점

본 장에서는 인터넷에서의 보안 상의 구조적 그리고 시스템 차원의 취약점을 검토하고, 이로 인하여 발생한 여러 보안 관련 사건들을 조사 기술한다.

2.1 인터넷 보안 문제점

인터넷은 다음과 같은 특성으로 인하여 전산망의 침입자들에게 매우 취약한 면을 보여주고 있다.

- 개방성 : 인터넷은 상호 정보 교환을 대화형으로 빠르고 원활하게 제공하여 전세계 어디서나 다양한 정보를 자유롭게 전달하므로 침입자들이 쉽게 침입할 수 있는 기회를 제공한다. 예를 들어 대부분의 호스트에는 guest, sonnim 등과 같은 계정을 만들어서 제한된 범위에서 자기 시스템을 사용할 수 있도록 하고 있는데, 이러한 계정이 침입자 들의 침입 도구로서 이용되기도 한다.
- UNIX, TCP/IP의 소스 개방 : IBM/SNA와 같은 업체의 독자 프로토콜은 개발 업체만이 소스를 독점하고 있으므로 해당 프로토콜을 사용하는 전산망에는 보안에 대하여 큰 문제점이 존재하지 않는다. 반면에 TCP/IP 프로토콜이나 UNIX 시스템의 소스는 많은 학교와 연구소에서 소스를 소유하고 있으며, 또한 이를 분석하여 계속 성능이 개선되고 있다. 그러나, 침입자들은 공개된 소스를 분석하여 이들의 취약성, 버그 등을 발견하여 침입하는데 사용하고 있다.
- 침입자들의 상호 정보 교환 용이성:인터넷에서는 감일이라는 것이 불가능할 정도로 많은 수의 전자 게시판(BBS)과 온라인 정보 교환을 위한 방법들이 제공되므로 침입자의 침입 방법이 손쉽고 은밀하게 교환되어 이를 바탕으로 하여 새로운 침입자가 양산되고 있는 실정이다. BBS의 여러 게시판, IRC(Internet Relay Chatting), 전자 우편과 뉴스 그룹을 통한 정보의 전달은 순식간에 방송되듯이 많은 인터넷 사용자와 침입자에게 알려진다. 또한 어떤 싸이트에서 정상적인 관리자들을 위하여 개방한 경고성 자료 문서들이 오히려 침입자에게 도움을 주는 경우도 있다.

위와 같은 취약성을 이용하여 불법 침입자는 단순한 호기심에 의해 다른 기관의 시스템을 불법으로 침투하기도 하지만 범죄적인 동기에 의해 불법 침입하여 시스템을 불법 사용하거나 파괴하기도 한다. 그러나 불법 침입이 호기심에 의한 것인지 아니면 범죄적인 동기에 의한 것인지를 판단할 방법이 전혀 없으므로 모든 침입은 범죄적인 동기에 의한 침입자로 가정하여야 한다. 이런 침입자들이 일으킬 수 있는 위험 요소에는 다음과 같은 것이 있다.

- 악의적 목적에 의한 불법 접근과 비인가된 시스템 사용
- 악의적 목적에 의한 정보의 열람, 파괴 및 변조
- 악의적 목적에 의한 시스템 정상 서비스 방해

위의 위협 요소로 볼 때, 다음과 같은 보안(Security)의 본래 목표를 인터넷에서의 보안 목표에 적용할 수 있다.

- 정보의 비밀성(Information Confidentiality)
- 정보의 무결성(Information Integrity)
- 정보의 가용성(Information Availability)
- 부인 봉쇄(Non-Repudiation)
- 서비스 기록(Service Auditing)

2.2 인터넷 보안 취약점 분석

인터넷은 전술한 바와 같은 구조적 문제점들에 의해 시스템 자체에 늑히 다음과 같은 대표적인 취약점을 이용하여 불법 침입자들은 불법 침입을 시도하고 있다.

2.2.1 NFS 취약점

NFS는 네트워크를 통하여 여러 시스템들이 파일 시스템을 공유함으로써 여러 파일 시스템을 로컬 디스크처럼 사용할 수 있게 한다. 즉, 여러 대의 NFS 클라이언트 들이 큰 용량의 디스크를 가진 NFS 서버의 파일 시스템을 운영 체제나 아키텍쳐에 상관없이 쓸 수 있다. 다음은 NFS와 연관된 파일들이다.

- /etc/exports : 클라이언트에게 export할 디렉토리와 옵션 등록
- /etc/xtab : 현재 export하고 있는 디렉토리, 파일 시스템과 export 시의 옵션 /etc/fstab : 부팅 시 자동적으로 마운트할 로컬 혹은 리모트 파일 시스템 등록
- /etc/mtab : 현재 마운트된 디렉토리에 대한 정보
- /etc/netgroup : 네트워크 상의 호스트 그룹 정의

이러한 NFS는 사용자에게 많은 이익을 제공하지만 다음과 같은 보안 취약점을 가지고 있다.

- /etc/exports 파일에서 주어진 옵션의 길이가 256자를 초과한 경우 옵션이 없는 것과 똑같은 상태가 되어 연결된 모든 호스트가 접근할 수 있다.

• rpc.mountd에 -n옵션을 붙여서 사용할 때, 허가 받지 않은 시스템이 정상적인 시스템과 NFS 서버 사이의 파일 핸들을 알고 있다면 아무 제약없이 NFS 서버를 사용할 수 있다.

이러한 문제점을 해결하기 위하여 /etc/exports 파일에 옵션을 최대한 사용하여 접근을 제한하고, export할 호스트의 수를 최대한 제한하고, export할 파일 시스템을 최대한 줄인다.

그리고, rpc.mountd에 -n옵션은 SunOS 3.0 이전 버전을 사용하는 호스트가 NFS 클라이언트가 될 수 있도록 하기 위한 것이므로 해당 호스트의 버전을 업그레이드하여 -n 옵션을 사용하지 않도록 한다.

2.2.2 NIS 취약점

NIS는 SUN에서 개발한 소프트웨어로서 SUN 시스템으로 이루어진 서브 네트워크를 효율적으로 관리할 수 있도록 한다. 중요한 시스템 파일들(예) /etc/passwd, /etc/groups, /etc/hosts, /etc/netgroups, /etc/ethers …)을 네트워크를 통하여 공유함으로써 서브 네트워크에 연결된 시스템들의 시스템 관리자와 사용자에게 일관된 환경을 제공한다. 이 때, NIS 서버와 클라이언트 간에는 RPC를 사용하여 구현된다.

NIS는 도메인 이름이 일치할 경우 어떤 호스트의 요청에 대하여서도 NIS를 통하여 공유되는 패스워드나 그룹 등에 관한 파일들(NIS 맵)을 넘겨주게 된다. 이렇게 유출된 NIS 맵에 대하여 crack 등의 소프트웨어를 사용하여 일반 사용자나 루트의 패스워드를 알아낼 수 있다.

이러한 문제를 해결하는 방법은 도메인 이름을 어렵게 하거나, DES rpc를 사용하여 NIS를 사용하거나, 접근 제어가 가능한 portmap을 사용하여 NIS맵이 외부로 유출되지 않도록 한다.

2.2.3 Sendmail 취약점

Sendmail은 대상 시스템 내에 계정이 없더라도 대상 시스템에 메일을 보내어 원하는 명령을 수행할 수 있으므로 잘못된 sendmail의 사용은 심각한 문제를 야기시킬 수 있다. 다음은 sendmail의 대표적인 버그를 설명한 것이다.

Sendmail은 setuid를 가지고 있으며, 잘못 전달된 메일을 루트의 권한으로 /var/tmp/dead.letter에 쓴다. /var/tmp 디렉토리는 아무나 파일을 작성할 수 있으므로 다른 일반 사용자의 패스워드를 알아낸 불법 침입자가 /var/tmp/dead.letter에 /.rhost 파일을 symbolic link로 연결한 뒤, 자신의 호스트 이름을 넣은 잘못된 메일을 보내게 되면 시스템은 /.rhost 파일에 불법 침입자의 시스템을 넣게 된다. 이렇게 되면 불법 침입자는 자신의 호스트에서 루트로서 해당 시스템에 rlogin 한다면 해당 시스템에서 루트의 권한을 사용할 수 있다.

Sendmail의 이러한 문제점은 특별한 해결할 방법이 없고 새로운 패치가 나오는 대로 즉각 시스템에 설치하는 것이 최상의 방법이다.

2.2.4 기타 취약점

- 공개된 계정이나 패스워드 없는 계정을 사용하여 침입한다.
- 호스트의 /etc/passwd 화일을 입수하여 그 계정의 패스워드를 알아내어 침입하다.
- 네트워크 응용 프로그램의 버그, 보안 취약점을 공략한다.
- 시스템이나 네트워크의 잘못된 구성을 이용하여 침입한다.
- 네트워크 상의 트래픽을 받아 분석 후 침입한다.
- 침입 후 불법으로 관리자 계정을 얻기 위해 불법 프로그램을 설치, 실행한다.
- 침입 후 다음의 침입을 위해 불법 프로그램을 설치한다.
- 침입 후 시스템 파일 등을 열람, 변조, 훼손한다.

국내 각 기관의 관리자들은 이러한 수법들에 대하여 충분히 대처하고 있지 못하다. 따라서 현재 국내에서 활동하는 침입자들은 인터넷에 가입된 기관이면 어떠한 기관이라 할지라도 침입할 수 있다는 자신감을 가지고 있을 정도이다. 이러한 사례들은 인터넷의 팽창과 비례하여 발생되고 있으며 전산망 등 정보화 사회에 진입할 수록 피할 수 없는 현상이라고 볼 수 있다.

2.3 인터넷 보안 사건

인터넷 보안 관련 사건으로 전세계의 이목을 집중시킨 사건에는 다음과 같은 것들이 있다.

- 서독 스파이 해킹 사건 : 1987년 서독의 해커들이 서방국의 기밀 정보를 빼내 KGB로 넘긴 사건으로서 인터넷에 접속된 주요 군사 기지, 첨단 산업 및 국방 관련 개발 업체들의 시스템에 침

입, 대표적인 군사 프로젝트의 정보와 첨단 개발 정보 등을 빼내 KGB에 돈이나 마약 등을 받고 팔아 넘긴 사건. 이 사건의 해결은 우연히 이들의 행위를 발견한 미국의 한 네트워크 관리자가 1년 반이나 감시 추적하여 해결하였다. 최종 검거 단계에서는 위장된 군사 프로젝트 네트워크를 만들고 이들을 유인하여 체포 하는 방법을 사용하였다.

- 인터네트 웜 사건 : 바이러스에 7500여대의 컴퓨터가 감염되어 동시에 정지한 사건으로 코넬 대학의 대학원생이 finger 등을 이용하여 상대편 시스템의 문제점을 알아내고 자신의 웜 프로그램을 상대편 시스템에 복사한 후 전자우편의 취약점을 이용하여 이 웜을 컴파일하면서 시스템에 부하를 거는 프로그램을 사용하여 발생한 사건이다.
- 죤 메카트닉 사건 : 2,3년간 타인을 위조하여 정보를 팔거나 돈을 빼낸 사건으로서 1995년 FBI에 의해 체포되었는데, 여기에는 산디에고 슈퍼컴퓨터 센터에 근무하는 컴퓨터 보안 전문가인 일본계 미국인 Tsutomu Shinomura 가 계획적으로 만든 부비트랩에 걸려 이에 단서가 됨으로써 잡히게 되었다.
- 씨티은행 침입 사건 : 러시아 해커가 씨티 은행의 계좌를 불법 인출한 사건으로서 시티 은행 망에 침입한 해커가 공모자의 타행 계좌로 불법적인 인출을 시도하여 수백만 달러를 송금한 사건으로 FBI의 추적 끝에 체포되었다.

그 밖에 뉴욕시의 414 번가에 사는 일단의 해커들이 뉴욕 암 센터를 해킹하고 자신의 침입 흔적을 지우려고 하다가 환자들의 모든 암 치료 정보까지 지워버려 정문화까지 열린 사건이 있었으며, NASA에서 Worms Against Nuclear Killers(WANK) worm 프로그램은 NASA 네트워크 내의 많은 컴퓨터를 감염시켰으며, 시스템 불법 침입으로 3명의 호주 해커들이 구속 당한 것, 2명의 해커들이 네바다의 많은 컴퓨터에 불법 침입하였다가 구속 당한 사례 등이 있다.

이러한 침입자들이 저지르는 사건은 외국에서 뿐만 아니라 최근 국내의 인터네트에서도 급격하게 증가되고 있는 추세이다. 다만 현재 인터네트에서의 침입자들의 수준이 평균적으로 그다지 높지는 않지만, 호기심에서 불법 침입을 즐기는 침입자들의 숫자가 기하급수적으로 증가한다는데 문제가 있으며, 이들이 점점 고난도의 기술을 습득하면 할수록 범죄로 악용할 우려가 있다. 최근 국내에서 발생한 인터넷 보안 사건들로는 다음과 같은 것들이 있다.

- 영국 청소년 원자력 연구소 침입 사건/1994
- 유럽 암 연구센 터 해킹 사건, CDK/1994
- 천리안 홈 뱅킹 사건/1995
- 서강대 / 한남대 전산망 서버 침입 사건/1994
- 서울대 전산망 정보 서버 침입 및 파괴 사건/1995
- 해외 침입자의 원자력 연구소, 선경 침입 및 경로 이용/1995
- 한국 전산원, 한국통신 연구센터 침입 사건/1995
- 서울대 침입 해커 추적/1995
- 지방 대학 해커 검거/1995

III. 인터넷 보안 대책

2장에서 기술한 바와 같이 불법 침입자들로 인하여 발생한 수많은 보안 사건들로부터 자원을 보호하기 위하여 보안 대책을 세울 필요성이 제기된다.

보안 대책에는 먼저 침입자들이 이용하는 인터넷 상의 취약성을 분석하여 이를 자동 복구 혹은 시스템 관리자에게 알려주는 예방 대책, 침입자들이 시스템에 접근하지 못하도록 막는 방어 대책, 마지막으로 시스템에 침입한 침입자를 탐지하여 역추적하는 사후 대책이 있다. 본 장에서는 위의 보안 대책 각각에 대하여 자세히 기술하도록 한다.

3.1 예방 대책

본 절에서는 인터넷에 존재하는 중요한 자원에 대한 위협과 불법 사용 등을 예방하기 위하여 자원이 가지고 있는 보안 취약성을 분석하고 이를 자동 복구 혹은 관리자에게 통보하는 도구들에 대하여 기술한다. 먼저 이들 도구들에게 요구되는 기능은 다음과 같다.

- 시스템 보안 취약점 점검
- 원격지 취약점 점검
- 원격지 대상 시스템 및 전산망 전체에 대한 점검
- 보안 취약점 자동 복구 혹은 통보 및 패치 기능

3.1.1 SATAN(System Administrator Tool for Analyzing Networks)

SATAN은 네트워크를 통하여 리모트 시스템의 보안 상태를 검사하여 그 결과를 데이터베이스에 저장

하여 HTML 브라우저를 사용하여 보여준다. 결과 보고서는 해당 시스템이 가지는 보안 취약점, 이에 대한 이유 및 해결 방안을 포함하고 있다. SATAN이 검사하는 보안 검사 사항으로는 sendmail 취약점, FTP 취약점, TFTP 취약점, 잘못된 NFS exports, NIS 패스워드 파일 접근, REXD 접근, 제한 받지 않은 X서버 접근 등이 있다. 그림 1은 SATAN의 초기 화면이다.

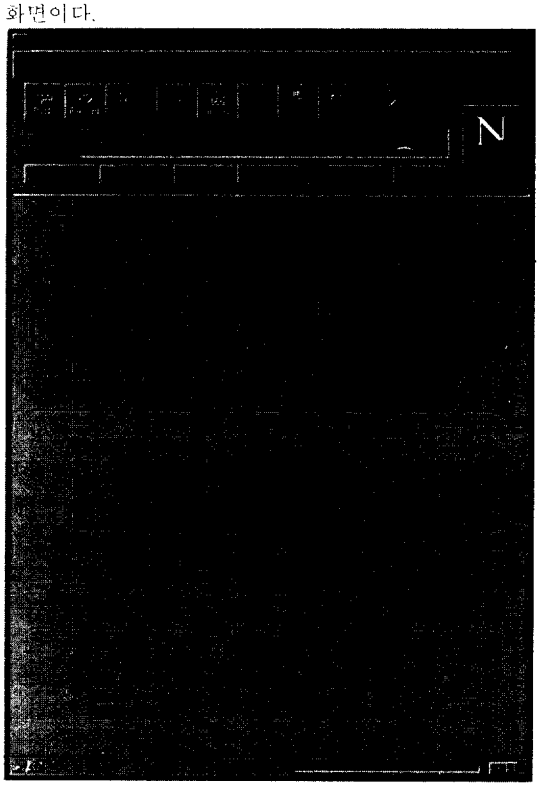

그림 1. SATAN의 초기 화면

3.1.2 ISS(Internet Security Scanner)

ISS는 여러 종류의 보안 취약점을 검사하여 사용자나 시스템 관리자의 실수로 인하여 잘못 설정된 사항을 보고한다. ISS는 SATAN과 같이 리모트 시스템의 보안 취약성을 검사하는 것이 아니라 외부의 불법 침입자로부터 자신의 시스템을 보호하기 위하여 자신의 시스템을 검사한다. ISS는 /etc/passwd 파일을 검사하여 패스워드 없는 사용자의 존재 유무, 2.3 절에서 기술한 여러 프로그램들이나 시스템의 버그, 현재 사용자 등을 검사한다.

3.1.3 Tcpwrapper

네트워크 서비스(ex). telnet, finger, rlogin, rsh …) 에 대한 로그 파일(서비스 요청 호스트 이름과 서비스 이름 기록)을 만들어서 몇 가지 부가적인 보안 검사를 하는 도구이다. Tcpwrapper는 그 크기도 작을 뿐만 아니라 시스템에 존재하는 소프트웨어나 구성 파일을수정할 필요가 없으며, 클라이언트와 서버 어플리케이션 사이의 실질적인 통신에 부하를 주지 않는다. Tcpwrapper은 inetd 데몬이 네트워크 서비스 요청에 해당하는 서비스 데몬을 호출하기 전에 tcpd 라는 데몬을 먼저 구동 시켜 네트워크 서비스에 대한 로그를 작성한 뒤에 해당 서비스 데몬을 호출하도록 한다.

3.1.4 COPS (Computer Oracle and Password System)

전반적인 보안 문제를 검사한다. 자동적으로 보안 취약점을 검사해주지만 문제를 자동 해결해주지는 못한다.

3.1.5 crack

표준 유닉스의 8자 DES password를 찾기(풀기) 위해 만들어 졌다. 이 프로그램을 이용하여 제대로 만들어지지 않은 사용자의 패스워드를 찾아 고침으로써 침입자의 패스워드 공격을 미리 방지할 수 있다.

3.1.6 Tripwire

여러 가지 signature routine을 사용하여 시스템의 중요 파일들에 대하여 signature를 만들어 중요 파일의 변조 여부를 검사할 수 있다.

3.1.7 Swatch

로그 파일에 있는 정보를 이용하여 사용자가 정의한 특별한 형태의 라인을 찾아 각각에 해당되는 행동을 취할 수 있게 하는 도구이다. 즉, 해커의 침입에 대하여 즉각적인 행동을 취할 수 있어 시스템의 보안에 중요한 역할을 수행한다.

3.1.8 MD5 (New Message Digest Algorithm)

파일의 지문(파일을 식별할 수 있는 기호)을 만드는 프로그램으로 중요 파일에 대하여 지문을 만들어 중요 파일을 검사할 수 있다.

3.1.9 CPM (Check in Promiscuous Mode)

LAN 상의 promiscuous mode(LAN 라인 상의 모든 패킷을 볼 수 있는 상태)에 있는 호스트를 검사한다.

3.1.10 LSOF (LiSt Open Files)

Open된 파일의 목록을 보여주는 프로그램으로 시스템에서 필요한 파일 이외의 파일이 open되어 있는지를 점사한다.

3.1.11 Sniffer

네트워크 상에서 돌아 다니는 패킷을 모두 가로채는 프로그램이다. 일반적으로 목적지가 자신의 호스트가 아닌 패킷은 볼 수가 없는데, 이 프로그램은 자신이 볼 수 없는 패킷까지 모두 가로챈다. 따라서 침입자들에게 악용되는 경우가 있다.

3.1.12 Traceroute

현재 시스템에서 다른 어떤 시스템으로의 패킷의 IP 경로를 추적하는 프로그램이다.

3.2 방어 대책(Firewall system)

본 절에서는 침입자의 침입으로부터 자원을 보호할 수 있는 방화벽 시스템에 대하여 기술한다. 먼저 방화벽 시스템에게 요구되는 주요 기능은 다음과 같다.

- 패킷 필터링 기능
- 응용 계층 게이트웨이 기능
- 안전한 사용자 인증 기능
- 사건 및 접속 기록 기능
- 편리한 사용자 인터페이스

방화벽 시스템이 없는 환경에서는 전산망의 보안은 전적으로 호스트 시스템의 보안에 의존하게 되며, 망에 연결된 모든 호스트가 일정하게 역할을 분담하여야 한다. 그러나, 망이 커질수록 보안의 통제는 매우 어려워지며 잘못된 구성, 부적절한 패스워드 등이 원인이 되어 쉽게 전산망 보안이 무너지게 된다. 따라서 방화벽의 짙은 방법은 전산망 전체의 보안 수준을 높이며 불법 침입자의 침입 시 적절히 대처할 수 있다. 방화벽 시스템은 한 도메인 내의 네트워크 보안을 위한 최선의 해결책을 제공한다. 물론 방화벽 시스템을 구현하는 것이 침입자의 침입을 완전히 막는다고는 할 수 없지만 가장 효과적이고 비용이 비교적으로 저렴하게 드는 방법이다.

본 절에서는 방화벽 시스템의 기본 원리와 이의 구현 및 원리, 방화벽 시스템 제품들에 대하여 기술한다.

3.2.1 방화벽 시스템의 기본 개념

방화벽의 원래 의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는 것이다. 이러한 의미를 인터넷에 적용하면 방화벽 시스템은 네트워크의 보안 사고나 문제가 더 이상 확대되는 것을 막고 격리하려는 것이다. 즉, 어떤 기관 내부의 네트워크를 보호하기 위해 외부에서의 불법적인 트래픽 유입을 막고, 허가되고 인증된 트래픽만을 허용하려는 적극적인 방어대책이다. 이의 정당성은 다음 정리에서 찾아볼 수 있다.

- 정리A. 우수한 방법론에 의해 만들어진 프로그램이라 할지라도 결국 사람에 의해 만들어졌으므로 버그가 있기 마련이며, 이 버그는 결국 보안 취약점이 된다.
- 정리B. 프로그램을 실행시키지 않으면 보안 문제는 없다.
- 정리C. 모든 컴퓨터는 많은 프로그램을 실행한다.
- 정리D. 만약 보안 문제를 최소화하려면 컴퓨터는 최소한의 프로그램을 실행하여야 할 것이다.

A,B,C 정리에 대한 반론이 없다면 현재 사용되고 있는 모든 컴퓨터는 보안 문제를 거의 피할 수 없다. 그러나, D 정리에 의해 하나의 시스템이 외부와 내부와의 트래픽에서 불순한 의도의 트래픽을 걸러줄 수 있다면 내부에 존재하는 대다수의 시스템은 안전을 보장 받을 수 있다.

방화벽 시스템의 기본 목표는 네트워크 사용자에게 투명성(transparent)을 보장하지 않아 약간의 제약을 주더라도 위험 지대를 줄이려는 적극적인 보안 대책을 제공하는 것이다.

3.2.2 방화벽 시스템

방화벽 시스템에 대한 각종 토론이 이루어지는 그 곳에서는 방화벽 시스템에 대한 다음과 같은 일반적인 용어 정의 및 개념을 도출하였다.

A. 스크린 라우터(Screen Router)

거의 대부분의 기관이 인터넷에 접속할 경우 일반적으로 인터넷 패킷을 전달하고 경로 배정(Routing)을 담당하는 라우터(Router)라는 장비를 사용하게 된다. 이러한 라우터는 패킷의 헤더 내용을 보고 필터링(스크린) 할 수 있는 능력을 가지고 있다. 즉, 네트워크 수준의 IP 데이타그램에서는 출발지 주소 및 목적지 주소에 의한 스크린, TCP 수준의 패킷에서는

네트워크 응용 프로그램을 판단케 해 주는 포트 번호에 의한 스크린, 프로토콜별 스크린 등의 기능을 제공한다. 이러한 기능을 가진 스크린 라우터 만을 사용하여서도 어느 정도 수준의 보안 접근 제어를 통한 방화벽 시스템 환경을 구축할 수 있으나, 라우터에서 구현된 펌웨어의 수준으로는 제한점이 많고 복잡한 정책을 구현하기 어려우므로 보통 스크린 라우터와 다음의 베스천 호스트를 함께 운영한다.

B. 베스천 호스트(Bastion Hosts)

베스천 호스트는 방화벽 시스템이 가지는 기능 중 가장 중요한 기능을 제공하게 된다.

원래 베스천은 중세 성곽의 가장 중요한 수비 부분을 의미하는데, 방화벽 시스템 관리자가 중점 관리하게 될 시스템이다. 따라서 베스천 호스트는 방화벽 시스템의 중요 기능인 접근 제어 및 응용 시스템 게이트웨이로서 가상 서버(Proxy Server)의 설치, 인증, 로그 등을 담당하게 된다. 그러므로 베스천 호스트는 외부의 침입자가 주로 노리는 시스템이 되므로 일반 사용자의 계정을 만들지 않고 해킹의 대상이 될 어떠한 조건도 두지 않는 가장 완벽한 시스템으로서 운영되어야 한다. 보통 판매되는 방화벽 시스템은 이러한 베스천 호스트를 제공하는 것이라고 볼 수 있다. 그림 2는 스크린 게이트웨이와 베스천 호스트의 인터넷상의 위치를 보여준다.

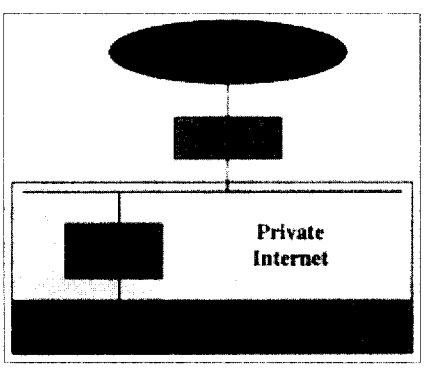

그림 2. 스크린 라우터와 베스천 호스트의 위치

C. 이중 네트워크 호스트(Dual-Homed Hosts)

이중 네트워크(외부 네트워크와 내부 네트워크) 호스트는 2개 이상의 네트워크에 동시에 접속된 호스트를 말하며 보통 게이트웨이 호스트라고 말하는 시스템으로서 외부 네트워크와 내부 네트워크 간의 유일한 패스를 제공한다. 즉 동적인 경로 배정과 경로 정보 전달을 배제하여 모든 내.외부 트래픽이 이 호스트를 통과하도록 함으로써 베스천 호스트의 기능을 여기에 구현한 것이다.

D. 스크린 호스트 게이트웨이(Screen Host Gateway)

스크린 호스트 게이트웨이를 내부 네트워크에 두어 스크린 라우터가 내부로 들어가는 모든 트래픽을 전부 스크린 호스트에게만 전달되도록 한다. 또한 스크린 라우터는 내부에서 외부로 가는 모든 트래픽에 대해서도 스크린 호스트에서 출발한 트래픽만 허용하고 나머지는 거부하게 된다. 따라서 외부와 내부 네트워크 사이의 경로는 외부 네트워크 - 스크린 라우터 - 스크린 호스트 - 내부 네트워크 이외의 경로는 결코 허용하지 않게 된다. 즉 베스천 호스트, 이중 네트워크 호스트의 개념을 합친 형태의 시스템이다.

E. 스크린 서브네트(Screen Subnet)

스크린 서브네트는 일명 DMZ(DeMiliterization Zone)를 외부 네트워크와 내부 네트워크 사이에 두는 것으로서 완충 지역 개념의 서브네트를 운영하는 것이다. 여기에 스크린 라우터를 두어 이 완충 지역을 곧장 통과 못하게 하지만 외부 네트워크는 물론 내부 네트워크에서도 이 스크린 서브네트에 접근할 수 있다. 특히 어떤 기관에서 외부로 공개할 정보 서버(Information Server), 즉 익명FTP서버, 고퍼(Gopher) 서버, 월드와이드웹(WWW)서버 등을 여기에 운영하면 된다.

F. 응용 계층 게이트웨이(Application Level Gateway)

응용 계층 서비스들은 중간전달(Store-and-Forward) 방법을 쓰는 경우가 많은데, 이는 게이트웨이에서 수행할 작업과 동일하다. 게이트웨이는 송신자 응용 서비스가 보내는 각종 정보를 그대로 전달한다. 사실 이 게이트웨이에서는 보안을 위한 특별한 서비스가 제공된다.

예를 들어 내부와 외부간의 모든 응용 수준의 트래픽에 대해 로그 기록이나, Telnet 나 FTP 등에서 사용자 인증을 할 경우 보다 우수한 방법을 사용한 변경된 인증 방법을 이용한다든가 하는 것이다. 이 응용 계층의 게이트웨이 기능은 가상 서버(Proxy Server)라는 인터넷의 클라이언트/서버 개념에서 나온 서버 기능을 제공하게 된다. 예를 들어 외부의 전자 우편 클라이언트가 내부의 어떤 호스트내 전자우편 서버와 접속 맺기를 원한다면 중간에 가상 서버가

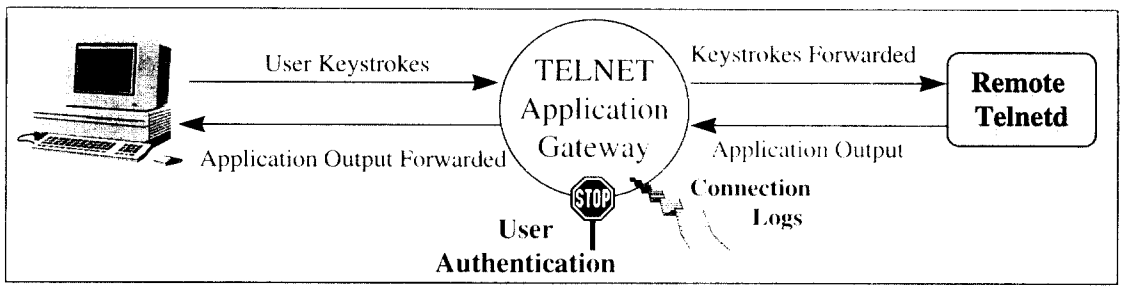

그림 3. 응용 계층 게이트웨이의 구조

이를 받아 다시 내부의 서버에게 전달하는 방식이 된다. 그림 3은 응용 계층 게이트웨이의 구조이다.

G. 방화벽 시스템의 사용자 인증 시스템

방화벽 시스템은 한 기관의 네트워크 전체를 보호해야 하므로 일반적으로 유닉스 시스템에서 사용되는 단순한 패스워드 기법으로 사용자를 인증하는 방법을 사용하지는 않는다. 보다 우수한 인증 시스템으로서 일회용 패스워드(One Time Password)를 보통 채택하고 있다. 즉 매번 사용자가 로그인을 시도할 때 마다 매번 새로운 패스워드를 이용하는 것인데, 이는 침입자들이 최근 이용하고 있는 sniffer에 의한 패킷 가로채기를 통해 시스템의 사용자 ID와 패스워드를 알아내서 침입하는 것을 근본적으로 막아주게 된다. 일회용 패스워드 시스템의 동작은 Challenge-Response 개념으로 그림 4와 같이 동작하는데, 이를 보자면,

1. 사용자는 자신이 로그인하려는 시스템으로부터 Challenge로서 난수(Random Number)를 받는다.
2. 사용자는 자신이 가지고 있는 계산기 형태 크기의 HHA(Hand Held Authenticator)로 Challenge와 자신의 ID를 입력한다.
3. HHA는 시스템이 가지고 있는 알고리즘과 동일한 알고리즘에 따라 일회용 패스워드를 반환한다.
4. 사용자는 HHA가 반환한 일회용 패스워드로 시스템에 로그인한다.

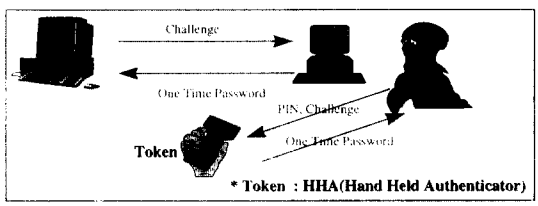

그림 4. 일회용 패스워드 시스템

H. 암호 장비(Encryption Devices)

암호 장비는 어떤 기관의 네트워크가 인터네트를 통해 여러 지역으로 분산되어 있을 경우 적당하다. 즉 본사 네트워크가 방화벽 시스템을 구축하여 보호되고 있을 때 지역적으로 떨어진 지점 네트워크도 본사 네트워크처럼 보호되어야 한다. 이 경우 본사와 지점 네트워크 간 인터넷으로 연결되었다면 안전을 보장하기 어려우므로 두 지점을 암호 장비를 이용하여 가상 사설 링크(VPL, Virtual Private Link)로 만들어 운영함으로써 두개의 네트워크를 하나의 안전한 네트워크로 만든다.

3.2.3 방화벽 시스템의 구현 예

그림 5는 예제로 구성한 방화벽 시스템을 보여주고 있다. 외부 인터넷과는 스크린 라우터로 연결하며 외부 인터넷과의 인접점에는 스크린 서브네트가 구성되어 하나의 완충지대를 만들며 여기에 외부에 공개하는 FTP서버, WWW 서버를 운영할 수 있다. 그리고 내부로 들어가는 모든 트래픽은 배스천 호스트를 거쳐야 하며 배스천 호스트에서는 허용된 네트워크 응용별로 가상 서버를 운영하고 있다.

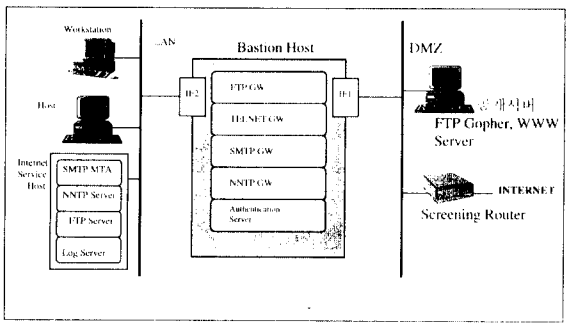

그림 5. 방화벽 시스템 구성 사례

3.2.4 도입시 고려 사항

먼저 보안 정책을 수립하고 이에 맞는 방화벽 시스템을 구축해야 한다. 상용화된 시스템을 구매할 경우 고려해야 할 사항은 다음과 같다.

1. 방화벽이 수립된 전산망 보안 정책에 대한 지원 여부, 보안 정책 변경에 대한 적용 유연성 여부, 필터링 기술 채택 여부, 다어얼업 등의 지원 여부, 새로운 사용자 인증 시스템 지원 여부 등을 다각적으로 고려
2. FTP, Telnet, HTTP 등을 기본적으로 지원하는 proxy 서버가 있고 사용자 인증 시스템을 갖고 있는지 여부와 함께 외부 공개 서버와 내부망 사용 가능 서버를 구분, 서로 분리할 수 있어야 함
3. 규칙을 정의하는 언어가 사용자에게 쉬워야 하며, GUI 화면으로 지원
4. 방화벽 시스템의 일반 규정이 적용하지 않는 규칙은 거절
5. 방화벽이 전산망에 있는 트래픽을 로깅해야 하고, 향후 전산망 보안 정책 수립에 필요한 통계 자료를 추출할 수 있어야 함
6. 방화벽이 보완된 OS로 운영되고 있는가 여부와 TCP/IP 상의 서비스들을 어느 정도 지원하고 있는지 여부를 따져야 함. 그리고 TCP, UDP, RCP를 기반으로 하는 응용시스템까지 지원할 수 있는가를 파악
7. 방화벽이 암호화된 기능을 지원하는 가를 파악

3.3 사후 대책

사후 대책으로는 기존의 자원을 보호한다는 소극적인 개념에서 나아가 시스템에 침입한 침입자를 탐지 추적하여 침입자의 실제 근원지를 알아내어 침입자의 신원을 밝힐 수 있는 적극적인 보안 개념이다. 침입자 역추적 시스템에서 요구되는 기능으로는 다음과 같은 것이 있다.

- 실시간 사건 기록 기능
- 실시간 침입 탐지 기능
- 불법 사용자 역추적 프로토콜
- 역침입 기능을 응용한 역추적 기능

침입자 역추적 시스템은 보안 사고 사후 처리의 기본 기술로서 침입자를 근본적으로 제거할 수 있는 기술이지만 현재 이에 대한 드래프트(draft) 표준만이 제시되어 있을 뿐이며 실제 이를 구현한 시스템은 존재하지 않는다. 현재 이쪽 분야에서 가장 심도있게 연구 되고 있는 부분은 불법 침입자 탐지 기능 쪽이다.

3.3.1 USTAT(State Transition Analysis Tools for UNIX)

USTAT 시스템은 UNIX 환경하에서 실시간 침입 탐지 도구로서 Philip A. Porras가 개발한 STAT의 일반적인 설계 기법을 UNIX환경에서 적용하여 구현한 것이다. STAT는 컴퓨터 침입을 표현하기 위한 새로운 접근 방법으로 침입 과정을 상태 변화의 순서로 나타내고 있다. 즉 어떤 침입을 성공적으로 달성하는데 필요한 과정을 초기 상태에서 목표 상태에 도달하기까지의 단계들을 컴퓨터 사용 측면에서 표현한 것이다. 그림 6과 같이 USTAT는 시스템의 감사 추적(audit trail)은 SUN OS의 C2 Basic Security 모듈을 이용하여 수집된 감사 데이타를 이용하여 침입을 탐지한다.

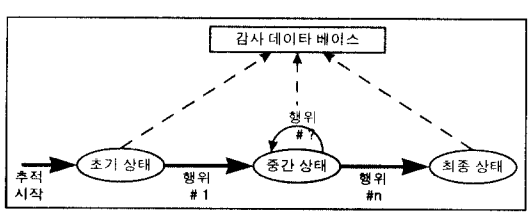

그림 6. USTAT의 상태 천이도

3.3.2 IDES(Intrusion Detection Expert System)

SRI international에서 개발된 IDES는 불법적인 행위를 찾아내기 위해 복잡한 통계 방법과 알려진 수

법, 시스템 취약성, 그리고 각 기관의 보안 정책을 내재한 전문가 시스템을 사용하는 포괄적인 전문가 시스템이다. IDES는 현재 행위가 과거 또는 받아들일 수 있는 행위에 대하여 현재의 행위가 합법적인지를 판단하기 위하여 사용자, 리모트 호스트, 타겟 호스트로 정의된 profile을 사용한다.

IDES는 타겟 시스템을 모니터하여 profile을 적절히 수정하여 사용자의 행동 유형을 학습한다. 또한, IDES는 의심스러운 행위를 기술할 수 있는 전문가 시스템을 포함한다.

3.3.3 침입자 추적 기술

침입자가 탐지된 경우에 이를 추적하기 위한 시스템으로 지금까지 이 분야의 연구가 거의 없었다. 이는 추적이라는 단어에서 알 수 있듯이 추적을 수행하다 보면 다른 관리 영역의 시스템을 조사하여야 하는 경우가 빈번히 발생하게 되는데 이는 또 다른 privacy 침해가 되기 때문이다.

본 고에서는 자신의 시스템에 로그인하여 사용하고 있는 사용자를 식별할 수 있는 identification 프로토콜을 사용한 간단한 역추적 방법에 대하여 설명한다. Identification 프로토콜에서는 그림 7과 같이 쌍방 간의 TCP 포트 번호가 제공되면 서버 시스템 상에 해당 connection의 소유자를 알려주는 문자열을 되돌려 준다.

이 프로토콜은 TCP 상에서 구축된 connection-oriented 응용 프로토콜로서 서버는 TCP 포트 113 번을 계속 검색하다가 TCP connection이 설정되면 관련된 connection을 나타내는 정보를 읽어 들인다. 만일 읽어 들인 내용이 정확한 경우 서버는 해당 connection에 대한 시스템 사용자 ID를 클라이언트에 보낸다. 이 프로토콜을 사용하여 불법 침입자를 추적하기 위해서는 모든 시스템들이 연결되어 있어야 하는데, 이 상황에서 불법 침입자가 연결을 끊거나 로그 아웃을 하면 추적이 불가능하고, 추적 시 각 시스템의 관리자 간에 협조가 기밀하게 이루어져야만 한다.

이러한 불법 침입자 역추적 시스템은 추적의 오버헤드를 고려하여 설계하여야 하며, 나쁜 의도를 가진 사용자가 다른 시스템의 일반 사용자에 대한 정보를 얻어낼 수 있는 단점을 가지고 있다.

3.4 인터넷 응용 보안

본 절에서는 인터넷을 이용하는 사용자 측면에서 이들이 인터넷을 이용하기 위해 사용하는 응용 서비스에서의 보안을 다룬다. 특히 사용자들이 요구하는 프라이버시 문제라든가 정보 보호 등의 요구사항을 지원하는 대표적 보안 응용 시스템에 대해 알아본다.

3.4.1 PGP(Pretty Good Privacy)

본 소절에서는 전자우편의 보안을 위한 방법으로서 PGP방법에 대해 설명한다. Phil R. Zimmerman이 세계적인 공개용 도구로서 개발한 것인데, PGP 를이용하여,

- 파일의 암호화 및 저장
- 전자우편을 특정인 만을 위해 송신
- 전자우편/파일에 전자 서명
- 문서의 변조 방지 메카니즘
- 키 관리 기능

등을 제공하는데, 이 시스템의 특징은 다음과 같다.

- 세션마다 키 교환을 이용한 블럭 암호
- RSA* 공개키 방식의 암호 기법
- IDEA 블럭 암호화
- MD5(Message Digest 5) 인증 기법
- 분산된 키 관리 기능
- 전자우편 보안에 적합

PGP가 위와 같은 기능을 제공하지만 미국이 보안 관련 제품의 해외 수출을 통제하고 있기 때문에 PGP의 여러 버전 중에서 라이센스 문제가 없는 것만 국내에서 이용할 수 있다. 국내에서는 2.6ui 나 2.6i 버전이며, 다음 Anonymous FTP Sites 에서 가져올 수 있다.

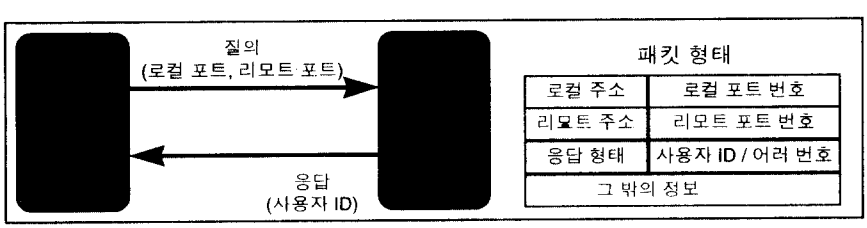

그림 7. Identification 프로토콜

- ftp://what.snu.ac.kr/pub/pgp/2.6.i/
- ftp://venus.etri.re.kr/pub/pgp-elm/pgp-cookies.tar.gz
- ftp://juno.kaist.ac.kr/pub/security/pgp/

또한 국내에서는 개인의 사생활 보호를 위해 필요하다면 암호화하여 메세지를 전달할 수 있도록 되어 있지만 국가 보안상 적극적인 활용은 국가 기간 전산망 등에만 허용되고 있는데, 일단 메세지의 변조 유무, 전자 서명 등은 사용할 수 있다.

3.4.2 SSH(Secure Shell)

Secure Shell은 pgp 와 마찬가지로 공개키 방식의 암호 방식을 이용하여 원격지 시스템에 접근하고 메세지를 암호화하여 전송을 할 수 있는 시스템이다. 그러므로 LAN 상에서 다른 시스템으로 로그인할 때 sniffer에 의해 도청 당하는 것을 막을 수 있다. 이 시스템은 다른 네트워크 응용 프로그램과 마찬가지로 Client/Server 형태로 동작하며 서버 쪽에는 sshd라는 서버 프로세스가 항상 실행되고 있어야 한다. ssh-keygen을 통해 키를 생성하고 마치 rlogin 처럼 사용한다.

3.4.3 WWW 보안

WWW 환경에서 알려진 보안상의 문제점은 클라이언트와 서버 양쪽에서 발생할 수 있다. 클라이언트에서는 엉뚱한 서버로부터 데이타를 받아 잘못된 해석을 할 수 있으며 서버에서는 데이타의 변조, 파괴, 사용자 인증, 접근 제어 등이 있을 수 있다. 따라서 이를 방지하기 위하여 인증/비밀/무결성 서비스가 필요하다. 현재 나와 있는 방법으로서 HTTP Proxy 를 사용하여 URL/Language 필터링을 하거나, 새로운 HTTP 보안 프로토콜이 표준화 되기까지 기다려야 할 것이다.

먼저 EIT(Enterprise Information Technologies)에서 제안한 SHTTP(Secure HTTP)는 PEM, PGP 등에서 이용하는 암호 메세지 형식을 이용한 End-to-End Secure Transaction을 제공한다. SHTTP의 기능은 메세지 보호를 위해 signature, authentication, encryption을 제공하며, 여러 환경의 키 관리 기법과 Challenge-Response 방법의 인증 전송 방법이 제공된다. SHTTP의 형태는 헤더에서 다음 필드의 값에 따라 결정된다.

- Content-Privacy-Domain : PEM, PGP, PKCS-7
- Content-Transfer-Encoding : 7BIT, 8BIT, BASE64
- Content-Type : application/http(MIME)
- Prearranged-Key-Info : Inbabd, Kerberos and Outband
- MAC-Info : Message Authenticity Check

Netscape사가 제안하고 있는 SSL(Secure Socket Layer)방법은 네트워크 응용마다 공통적으로 요구되고 있는 보안 서비스를 네트워크 응용 계층 바로 아래에 한 계층을 더 두는 것으로 encryption, Server Authen.(Always)/Client Authen.(Optional), Message Integrity(MAC) 등이 제공되며 다음과 같은 절차를 거친다.

- Connection Phase : 키 협상, 보안 협상
- Authentication Phase : Certificate 교환

현재 EIT의 SHTTP와 Netscape의 SSL을 통합한 새로운 표준이 제안되고 있으며, 이의 표준화를 위한 IETF wtg(WWW Transation Working Group)이 활동 중에 있다.

3.4.4 Kerberos

Kerberos는 MIT Athena 프로젝트에서 개발한 네트워크 인증 시스템으로서 인터넷 응용 시스템이 공동으로 사용할 수 있는 인증 메카니즘을 제공한다. 현재 버전 5까지 나와 있으며, DES(Data Encryption Standard)방식의 비밀 키 암호 방법과 Global Clock을 이용한다.

IV. 인터넷 보안 사고 처리

인터넷 보안 사고 처리를 위한 국제적인 사고 응답팀(IRT, Incident Response Team)들이 있는데 이들은 보안 사고 예방 활동으로서 보안 사고에 대한 진단 문서나 관련 정보

교환 및 배포, 홍보, 세미나 등을 개최하고, 보안 사고 사후 활동으로서 보안 사고의 접수, 이의 진단, 및 추적과 관련 기관별 협조 등의 활동을 하고 있다.

FIRST(Forum of Incident Response Team)는 세계 각국의 IRT 들과 관련 기관들의 보안사고 응답을 위해 만든 협의회이다. 이 FIRST는 회원제로 운영되고 있으며, 회원 상호간 보안 사고 및 보안 관련 정보 교환이 주된 목적이다. 매년 1 회의 워크샵과 총회를 가지고 있으며, 1995년도 워크샵이 독일에서 개최되었으며, 한국도 CERT-KOREA라는 이름으로 가입할 예정이다. 대표적인 가입 기관은 다음과 같고 FIRST

의 WWW 홈페이지의 URL은 http://first.org/first이다.

- CERT(Computer Emergency Response Team),
- CIAC/DOE(Computer Incident Advisory Capability/Department of Energency)
- DoD(Department of Defence), US Airforce, US Navy, NASA
- Sun Micro Systems, MCI, Sprint
- CERT-NL, CERT-IT, CERT-DFN, …등등의 유럽 국가 CERT

CERT(Computer Emergency Response Team)는 일련의 해킹에 의한 보안 사고를 국제적으로 처리하고 이의 예방 정보들을 미리 전세계적으로 알리기 위한 조직으로서 1989년 미국방성의 지원으로 카네기 멜런 대학 내 소프트웨어 연구소 산하에 만들어 졌으며, 미국방성은 매년 수백만불의 예산지원을 하고 있다. 세계 각국의 여러 CERT 들의 URL은 표 1과 같다.

CERT이름	U R L	REMARK
AUSCERT	http://www.auscert.org.au	호 주
DFN-CERT	http://www.cert.dfn.de/eng	독 일
CERT-NL	http://www.nic.surfnet.nl/surfnet/security/cert-nl.html	네덜란드
SWITCH-CERT	http://www.first.org/first/switch.html	스위스
PCERT	http://www.cs.purdue.edu/pcert/pcert.html	Purdue대학

표 1 : 여러 CERT들의 URL

최근 국내의 인터네트에 대한 보안은 일단 드러난 활동으로서 KIS그룹(Korea Internet Security-Group)과 한국 CERT (CERT-Korea)의 발족이다.

KIS 그룹은 몇 년 전부터 KNC/SG-INET 산하의 보안 그룹을 확대 개편하여 최근 활동을 개시한 연구회이다. KIS-Group 은 국내 인터네트 보안 분야의 기술 발전을 위하여 회원간 정보교환 및 세미나 등을 통해 상호 기술력 배양이 그 목적으로 구성되었다. KIS 그룹은 회원에 대한 자격 제한은 없으며 누구나 회원이 될 수 있다. majordomo@cert-kr.or.kr로 본분에 "subscribe security"라고 메일을 보내면 되고 통신 수단은 전자 우편을 통해 이루어진다. 그리고, 매 짝수 달 첫째 수요일에 정기적으로 회의 및 세미나를 개최한다.

한국 CERT(CERT-KR : "써트 코리아"로 발음)는 KNC 산하의 조직으로서 최근 발족되었고, 6월 1일부터 공식 활동에 들어가게 되는 보안 사고 응답 센터 기능을 하게 된다.

주로 CERT-KR은

- 국내 인터네트 보안 사고의 접수 및 해결 지원
- 국제적인 보안사고 해결 업무
- 인터네트 보안 관련 컨설팅
- 인터네트 보안 관련 R&D 지원

등의 기능을 수행하는데, 시스템 공학 연구소에 그 사무국을 두고 활동하고 있다. 한국 CERT 는 국내 인터네트 상에서 온라인으로 서비스를 지원하고 있는데, 주요 서비스는 다음과 같으며, 그림 8은 CERT-Korea WWW 홈페이지이다.

- www.cert-kr.or.kr　한국 CERT WWW 서버,
- ftp.cert-kr.or.kr　한국 CERT Anonymous FTP 서버,

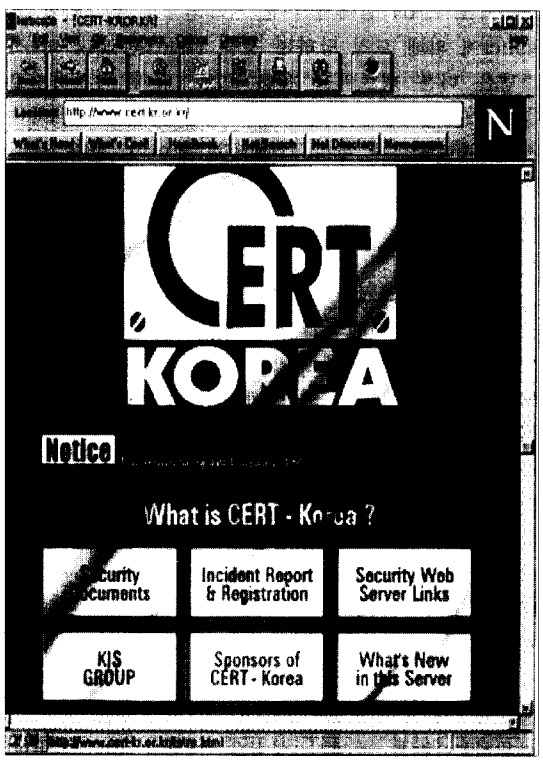

그림 8. CERT-Korea WWW 홈페이지

1995년 3월부터 12월까지 CERT-Korea에 접수된 사건은 보누 26건으로 학교 12건, 연구소 7건, 회사 7건이 각각 접수되었다. 이중 9건이 국제 협력으로 처리되었다. 그러나, 일반적으로 발생한 사건의 약 5% 만이 보고되는 현황을 감안할 때 실제적으로 발생한 보안 사고는 약 500건을 넘을 것으로 추산된다. 보안

사건 접수나 문의사항은 www.cert-kr.or.kr의 Web 페이지를 이용하거나, staff@cert-kr.or.kr로 전자우편을 보내면 된다.

V. 인터넷 보안 연구 활동 현황

본 장에서는 국내외에서 현재 수행 중인 인터넷 보안 연구 현황, 보안 사고 처리 및 인터넷 보안의 미래에 대하여 기술한다.

5.1 국내외 보안 연구 활동 현황

5.1.1 국외 동향

군사 및 특수 목적의 보안뿐만 아니라 사용 보안 기술 수준이 탁월하고, 특히 미국은 전산망 보안에 대한 기술력을 선세계적으로 주도권을 잡고 있는데, RSA라는 우수한 공개키 방식의 알고리즘을 기반으로 한 다양한 사용 제품들이 존재한다.

망 응용 공통 보안 서비스 라이브러리는 MIT에서 개발한 Kerberos를 기반으로 하여 DEC에서 제안한 공개키 방식의 DASS(Distributed Application Security Service)가 제안되었고, 최근에는 IETF의 GSS-API(Generic Security Service API)가 Kerberos 기반의 비밀 키 방법과 X.509 방식의 공개 키 방법을 혼용하여 업계 표준이 작성되고 있다.

예방 차원의 보안 취약성 분석 진단을 위한 다양한 도구들이 개발되고 있다. 특히 앞에서 설명한 SATAN, ISS, COPS와 같은 시스템은 리모트의 시스템의 취약성을 검사하거나, 로컬 시스템의 취약점을 분석해낸다. 또한 자동 복구를 위한 Secure__Sun__Check는 썬 워크스테이션용 SunOS 4.X 버전의 14 항목의 보안 문제점을 분석하여 자동 복구한다. 그러나 이 시스템의 기능은 매우 미약하고 하나의 시스템만을 대상으로 하므로 그 효용성이 상당히 낮다. 그러나, 그 밖에 제품 개발이나 연구가 거의 시도되고 있지 않다. 방어 차원의 방화벽 시스템은 TIS, CheckPoint 사의 제품들이 뛰어난 수준의 성능과 기능을 가진 방화벽 시스템 제품들을 발표하였으며, 그 외의 40여 업체의 제품이 발표 중이다.

방화벽 시스템의 핵심 기술인 사용자 인증 및 접근 제어는 라우터를 제공하는 통신 업체와 스마트 카드 방식의 토큰을 이용한 제품들이 발표되고 있으며, 매우 우수한 성능을 보이고 있다.

사후 처리 차원의 실시간 탐지 기술은 몇몇 사용 제품이 있지만 아직 연구 개발 수준이며, 실시간 역추적 기술은 IETF 보안 분야에서 프로토콜을 제안한 적이 있지만 더 이상 연구 개발이 진행되고 있지 않다.

5.1.2 국내 동향

전반적으로 군사 및 특수 목적의 암호 알고리즘 및 암호 장비 기술에 대하여 높은 수준을 가지고 있는 것으로 보이지만 전산망, 시스템 보안 기술 및 상용 보안 기술 수준은 현저히 낮은 편이다. 따라서 최근 사용 및 전산망 보안 시스템의 수입이 급증하고 있는 추세이다.

5.2 IETF(Internet Engineering Task Force) Security Area

Security Area 의장은 Jeffrey Schiller(jis@mit.edu)로서 IETF/Security Area의 각 Working Group들의 현황은http://www.ietf.cnri.reston.va.us/html.charters/wg-dir.html/Security__Area에 자세히 기술되어 있으며, 현재 다음과 같은 보안 관련 그룹들이 활동 중이다.

5.2.1 Authenticated Firewall Traversal (aft) Working Group

WG Mail: aft@unify.com

To Join: aft-request@ unify.com

이 그룹은 방화벽 시스템에서 인증을 위하여 응용계층에서 TCP, UDP를 지원하는 프로토콜을 연구한다. 상호 연관성(interoperability)을 높이기 위하여 일반적인 인증 프레임워크를 사용한 기반 인증 기술도 제안하고 있다.

5.2.2 Common Authentication Technology (cat)

WG Mail: cat-ietf@mit.edu

To Join: cat-ietf-request@mit.edu

이 그룹은 지정된 특정 보안 메카니즘에 따라 호출자(caller)를 캡슐화하여 다양한 프로토콜에 대한 강력한 인증을 제공한다. 호출자의 프로토콜 내에 보안 데이터 요소를 합치는 작업에서 보안 구현 작업을 분리함으로써 보다 보안 지향적으로 일관적이고 모듈화된 보안 접근 방법을 연구하고 있다.

5.2.3 Domain Name System Security (dnssec)

WG Mail: dns-security@tis.com

To Join: dns-security-request@tis.com

이 그룹에서는 DNS에 대한 인증 받지 않은 데이터 변경을 막는 연구를 수행하고 있다.

즉, 무결성 데이터와 인증 능력을 전자 서명 방법을 사용하여 DNS 프로토콜에 첨가한다.

5.2.4 IP Security Protocol (ipsec)

WG Mail: ipsec@ans.net

To Join: ipsec-request@ans.net

이 그룹에서는 IP의 클라이언트 프로토콜의 방어 메카니즘을 개발하고 있다. 네트워크 계층의 보안 프로토콜은 인증, 무결성, 접근 제어 등을 유연하게 지원하는 암호화를 지원하는 것이다. 이를 위하여 설정된 IP Authentication Header와 IP Encapsulation Security Payload의 포맷은 암호화 알고리즘에 무관하게 구성된다.

5.2.5 One Time Password Authentication (otp)

WG Mail: ietf-otp@bellcore.com

To Join: ietf-otp-request@bellcore.com

일회용 패스워드 시스템인 벨코어 S/KEY 시스템과 이와 연관된 패키지(ex)logdeamon, NRL OPIE …) 등을 사용하여 일회용 패스워드를 위한 표준 RFC를 작성한다.

작성된 표준 RFC는 일회용 패스워드 인증 기술을 개발하는 여러 개발자들 간의 상호 호환성을 높이고, 인터넷의 보안 위험을 감소시킬 것이다.

5.2.6 Privacy-Enhanced Electronic Mail (pem)

WG Mail: pem-dev@tis.com

To Join: pem-dev-request@tis.com

이 그룹은 RFC 822 메시지를 무결성, 데이타 발생지 인증 등을 제공하는 형태로 변경하는 작업을 수행하고 있다.

5.2.7 Public-kry Infrastructure (pkix)

WG Mail: ietf-pkix@tandem.com,

To Join: listserv@tandem.com

이 그룹은 X.509를 기반으로 PKI를 지원하기 위하여 필요한 인터넷 표준을 개발한다.

이 PKI는 인터넷 상의 많은 응용 프로그램에서 X.509의 사용을 통하여 상호증명 및 상호운 용성을 높일 수 있다.

5.2.8 Web Transaction Security (wts)

WGMail : www-security@nsmx.rutgers.edu,

To Join: www-security-request@nsmx.rutgers.edu

Web 트랜잭션에서의 보안 서비스 제공을 위한 스펙과 요구 사항을 개발한다. 이들 작업은 병렬적이고 HTTP working group과 독립적으로 진행된다.

5.3 초고속 정보 통신 망의 보안

인터넷은 향후 초고속 정보 통신망(Information Superhighway)의 주도적인 근간 망을 제공할 가능성이 매우 크다. 미국의 주도로 세계 각국이 앞 다투어 인터넷에 대한 프로젝트를 진행하며, 세계적인 정보 통신망 구축이 준비되고 있다. 이러한 배경에서 국내에서도 정부의 주도로 프로젝트 창출과 연구 개발이 시도되고 있는 것이다. 하지만 최근 국내외에서 발생되고 있는 일련의 전산망 보안 침해 사고들은 초고속 정보 통신망에서도 필수적으로 미리 준비해야 할 문제임은 틀림이 없을 것이다. 미국에서 고려하고 있는 초고속 정보 통신망에서의 보안은 다음과 같다.

- 디지탈 서명과 같은 보다 우수한 서명 방법 제공.
- 온라인 디지탈 무비에서 저작권 보호를 위한 기법 제공.
- 상업 서비스에 새로운 방법 : 신용 카드 회사 등에서 매우 필수적인 방법이 필요할 것이다.
- 초고속 정보 통신망에서 보안 서비스 자체가 서비스 기능.

현재도 인터넷 등에서 많은 해커들의 불법 침입과 행동으로 인한 피해가 흔히 발생하고 있는데 초고속 정보 통신 망에서도 같은 문제에 직면하게 될 것이다. 이때의 보안 관련 이슈를 다음과 같이 고려할 수 있겠다.

- 물리적 보안(Physical Security) : 물리적인 회선 보호를 위한 방안
- 인식(Identification) : 사용자, 접점 등의 확인
- 인증(Authentication) : 발신자 인증, 인증 정보의 보호 등
- 접근 제어(Access Control) : 초고속 정보 통신망의 모든 자원의 보호
- 무결성(Integrity) : 메세지 무결성과 초고속 정보 통신망 내 소프트웨어 무결성
- 감사(Auditing) : 충분한 사건의 기록, 감사 분석

도구의 개발과 응용망 보안 관리(Network Security management) : 서비스 거부 관리, 혼잡 제어(Congestion Control), 네트워크 보안사건 기록 수집 및 분석 등

VI. 결론

전세계적으로 인터넷의 열풍이 확산되는 것과 함께 국내에서도 인터넷을 기반으로 한 초고속 정보 통신망 구축이 활발히 진행되고 있다.

이러한 상황에서 보안 관련 기술들은 국내에서도 다른 기술들 보다 우선적으로 연구 개발되어야 할 분야 중 하나이다. 아무리 정보 통신 서비스를 위한 여러 기술들이 잘 개발되어 사용자들의 호응을 받더라도 자신이 사용하는 시스템이 불법 사용자들에게 취약성을 보이고, 이로 인하여 보안 사고를 겪게 된다면 사용자들에게 외면 당하기 때문이다. 또한 보안 관련 기술 및 여러 제품들은 대부분 자국 내에서만 사용 가능하고 외국으로는 유출을 금지하고 있으므로 보안 관련 기술 및 제품들을 국산화하여 적용하는 것은 매우 중요하다 할 수 있다.

이러한 보안 기술에 대한 국내 연구 개발 적용과 더불어 언터넷을 위한 보안 프로그램 및 관련 보안 도구들을 모아 우리가 벽돌을 한장 한장 쌓아 높은 담장을 만들어 간다는 마음 자세로 불법 침입에 대한 예방, 방어, 사후 처리 차원의 대책으로 적극 대응해 나간다면, 현재 발생하고 있는 전산망 시스템에 대한 불법 침해 사례는 대폭 줄어들 것이라고 사료된다.

인터넷을 근간으로 한 초고속 정보 통신 망 활성화의 성패가 현명한 보안 대책 및 관련 기술 개발에 달려 있다고 볼 때, 각 기관들의 보안 전문 요원 양성과 더불어 정부의 적극적인 연구 개발 투자 및 관심이 매우 중요하다고 볼 수 있겠다.

다음은 보안 관련 기술로서 앞으로 연구 개발 되어야 할 대표적인 분야이다.

- 해킹 관련 보안 도구 개발
- 전자 우편 보안 기술 개발
- 전산망 방화벽 시스템 개발
- 인증 기법의 개발(Kerberos, CAT 등), 패스워드 시스템
- 인터넷 온라인 캐쉬(NetCash, Cybercash 등) 보안 시스템
- WWW 보안 기술
- Auditing, 접근 제어 등의 기술
- Trusted System 기술
- PEM 등에서 활용하는 인정서 기법에 기초한 공증 서비스

VII. 참고 문헌

[1] Danny Smith, "Forming Incident Response Team", AUSCERT, 1995

[2] Fredric J. Cooper, Implmenting Internet Security, New Rider Publishing, 1995

[3] Karanjit Siyan, Internet Firewalls and Network Security, New Rider Publishing, 1995

[4] Marcus J. Ranum, "A Taxonomy of Internet Attacks: You Can Expect", 1995

[5] Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: Private Communication in a Public World, Prentice-Hall, 1995

[6] N. Derek, UNIX Security A Practical Tutorial, Mc Grow-Hill, 1993

[7] Security+ for UNIX, 포항공대전산소, 1995

[8] Simson Garfinkel and Gene Spafford, Practical UNIX Security, OReilly & Association, 1991

[9] Simson Garfinkel, PGP:Pretty Good Privacy, OReilly & Association, 1995

[10] UNIX Computer Security Check Lists, AUSCERT, 1994

[11] William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addision-Wesley, 1994

[12] William Stalling, Protect Your Privacy: The PGP User's Guide, Prentice-Hall, 1995

[13] 이희조 외, 인터네트, 유닉스 보안, NETSEC-KR'95, 1995.6

[14] 관리자를 위한 인터네트 보안지침서 Version 1.1 - 1.5, 한국 과학 기술 연구원 시스템 공학 연구소, 1995

변 옥 환

- 1986년 2월:서울대학교 공과대학 컴퓨터공학과 학사과정졸업
- 1979년 한국항공대학교 정보통신공학과 졸업(공학사)
- 1985년 인하대학교 대학원 전자공학과 졸업 (공학석사)
- 1993년 경희대학교 대학원 전자공학과 졸업 (공학박사)
- 1978년 - 현재 시스템 공학 연구소 책임 연구원 (연구전산망 개발실장)
- 1983년 - 1984년 미국 OSM corp. 방문 연구원
- 1995년 - 현재 한국통신정보보호학회 이사
- 주요 관심 분야 : 정보통신망 보안, 관리, 망 설계 및 서비스

임 채 호

- 1986년 홍익대학교 전산학과 졸업 (공학사)
- 1991년 건국대학교 대학원 전자계산학과 졸업 (공학석사)
- 1995년 홍익대학교 대학원 전자계산학과 박사과정 수료
- 1985년 8월 - 1992년 8월 시스템 공학 연구소 선임 연구원
- 1992년 9월 - 1995년 1월 대전 실업 전문 대학 전자계산학과 교수
- 1995년 2월 - 현재 시스템 공학 연구소 선임 연구원
- 주요 관심 분야 : 컴퓨터 통신, 컴퓨터 통신 보안, 운영체제 보안, 분산 시스템

임 찬 순

- 1994년 중앙대학교 전자계산학과 졸업(공학사)
- 1996년 중앙대학교 대학원 컴퓨터공학과 졸업(공학석사)
- 1996년 - 현재 시스템 공학 연구소 연구원
- 주요 관심 분야 : 정보통신망 보안, 운영체제 보안, 망 관리