特輯

국내외 Internet 보안 대책

윤기송, 변옥환
시스템 工學 硏究所

Ⅰ. 개요

요즈음 국내 연구 및 기술 개발그룹에서의 인터네트에대한 이용 열기와 관심이 매우 뜨겁게 달아 오르고 있다. TCP/IP라는 통신프로토콜을 이용하는 인터네트는 그 규모가 전세계 1만 7천개 이상의 네트워크와 여기에 속한 200만대 이상의 컴퓨터가 상호 연동되어 구성되는 글로벌 네트워크이다. 현재 연구 및 기술개발과 관련한 2천만명이상의 이용자가 세계 도처에 산재해 있는 컴퓨팅 및 다양한 정보자원을 자유롭게 활용하고 있다. 이들중 대부분은 무료로 이용할 수 있는 리소스이며, 현재 전자우편등의 서비스를 상호 교환할 수 있는 나라는 세계 137개국에 달하고 있다.

인터네트가 이와같이 활성화 되는것은 정보 리소스 및 네트워크의 개방과 접속의 용이성에 따라 세계 도처의 누구나 네트워크에 접속할 수 있다는 것에 기인하지만, 또한 이러한 특성 때문에 서독의 해커 간첩사건, 인터네트 Worm 사건, 그리고 해커가 침입하여 시스템의 하드 디스크를 모두 지워버린 행위등 국내외적으로 크고 작은 보안사건이 급증하고 있다. 시스템에 침입하는 침입자는 업체가 제작하여 판매할때 시스템이 가진 Security Hole을 찾아 침입하여 관리자의 특권을 얻은후 피해를 주는데 인터네트 가입기관의 증가 및 서비스의 다양화 추세에 비례하여 침입자의 기술 수준 및 행위도 더욱 다양해지고 있는 실정이다.

본고에서는 인터네트 보안사고를 검토하고 이에대한 해외 인터네트 보안센터 및 보안 연구개발 현황을 분석하며, 또한 실제 적용하고있는 네트워크 보안 방안 및 보안도구의 종류를 소개함으로서 앞으로 국내 학술연구전산망그룹의 핵심 문제로 대두될 Internet Security 대책의 진전에 도움이 될수 있도록 하고자 한다.

Ⅱ. 보안사고

1. 시스템 침입자

시스템 침입자란,

"불법적으로 어떤 기관의 전산망이나, 시스템에 침입하여 허가되지 않는 작업을 실행하는 사람"

이라고 정의를 내려 볼 수 있으며 이러한 침입자가 보통 시스템에 어떤 종류의 손해를 입히는 것이다. 흔히 해커(Hacker)와 크랙커(Cracker) 혹은, 침입자(Intruder)를 구별하기도 하는데, 해커는 시스템에 악의적인 손해를 입히려고 하지는 않는성격을 가진다. 하지만 보통 해커라고 할지라도 악의없이 불법적인 침입과 허가되지 않는 일을 하기도 하며 또한 실수로 손해를 입히는 일을 저지르기도 한다. 만약 이러한 손해가 치명적이지 않을수도 있지만 또한 그렇지 않을수도 있어서 시스템이나 전산망의 관리자는 이러한 문제에 대해서 쉽게 용납하지는 않을 것이므로 함께 시스템 침입자로 보는것이 일반적이다.

해커란 컴퓨터 시스템의 상세한 내부를 알고 싶어하는, 그리고 보통 이론적인 프로그램보다 즐기는 프로그램을 작성하기 좋아하는 청소년들이라고 보았을 때 이들은 단순히 다른 시스템에 침입한다는 것은 잠시 책을 빌려 본다든가, 차를 빌려타보는 호기심과 탐구심인지도 모른다. 책에는 보다 많은 원하는 정보를 알 수 있으며, 차를 빌려타보는 행위는 그 차의 성능을 알고 싶은 단순한 욕망일 수 있는 것이며, 또

그러한 행위는 나중에 책주인에게는 보다 나은 가치의 정보를 돌려줄 수도 있으며 또한 차주인에게는 차의 성능을 시험하여 그 차의 문제점을 알려 줄수 도 있는 것이다.

그런데 침입자(Cracker)는 정말 고의적으로 손해를 입히려는 목적을 가지고 침입하는 경우로 구분되어야 겠다. 예를 들어 해커와 같은 식으로 침입했다가 관리자들에게 들켜 시스템을 사용할 수 있도록 간청하였으나 거절당했을때의 감정으로 손해를 입히려고 한다든가, 혹은 그 기관의 경쟁회사나, 경쟁 연구그룹이 몰래 정보를 빼기위해 침입하거나, 또는 그 회사에게 해고당한 사람이 복수를 위해, 경쟁기관으로 옮긴 사람이 그 회사의 기밀 정보를 가져가기 위해서등과 같은 많은 사례들을 볼 수 있다.

국내의 경우 악의적인 목적을 가지고 침입을 시도하는 사례는 거의 발견된 바 없으며 단지 한두건에 이르는 것으로 보인다.

대개 자기 실력을 과시하려는 해커들의 영웅심리나, 실제 그 시스템의 보안 상태를 점검하려는 그룹들도 있다. 하지만 해커나 침입자나 대부분 침입에 성공한 후 다시 그 시스템에 손쉽게 접근하기 위해 불법적인 뒷문 (Backdoor)을 만들어 두게 되고 관리자는 자신의 시스템을 선의의 인증된 사용자들이 안심하게 시스템을 사용할 수 있도록 서비스하기 위해 일단 불법적인 침입과 허가되지 않은 작업을 막으려고 할 것이다.

아직까지 대부분의 국내 시스템 관리자는 해커나 침입자들의 침입기술을 따라가지 못하고 있으며 시스템의 어떤 비정상적인 운영도 해커나 침입자의 증거나 증상의 조치로 눈치채지 못하는 경우가 허다한 것이다. 이는 사무실의 어떤 직원이 밤마다 누가 그 사무실에 침입하여 서랍도 열어보고 금고의 돈을 빼내가고 있는 사실을 전혀 모르고 지내는 경우와 마찬가지인 것이다. 물론 밤마다 사무실에 침입하는 사람은 복사 열쇠나 만능열쇠를 가지고 있는 것이다. 그런데 어느날 출근했을때 금고문이 열려있다든가, 서랍문이 열려있다든가 하는 침입자의 실수나 이제 그 사무실에서 흥미를 못느꼈을때 해둔 상태를 보고 사건을 깨닫는 일들이 생기는 것이다.

가능한 시스템 침입자가 들어올 여지를 막는것이 가장 중요하며 침입자의 발견과 손해나 사고를 겪었을 때 이에 대처하는 절차를 미리 수립해두고, 대처능력을 개발해야 할 것이다.

2. 국내외 보안사고 사례

인터네트에서의 보안 침해사고는 대부분 시스템 침입자(Cracker)에 의한 것이다. 미국 인터네트에서 발생하기 시작한 해커에 의한 불법침입은 공중 통신망을 이용한 PC통신에서 비롯되었고 애초의 인터네트에는 국방관련한 기관이 함께 접속되어 있었으므로 군사기밀, 중요한 정보가 유출되는 사태가 발생하였다. 특히 KGB의 금전지원을 받는 서독의 청소년 해커그룹에의한 미국 군사기지 정보 불법 접근 및 정보의 유출사건은 인터네트의 보안문제가 국제화되는 것을 알려주는 중요한 사건이었다. 이러한 사건은 유럽에서는 EU 국제통신망을 이용한 보안침해사건들을 통해서도 보고된 바 있으며 이러한 영향은 국내에서도 국제 Leased Line이 미국 인터네트와 연결된 시점부터 국내의 해커(침입자)들이 출현하게 된 배경이 되었다. 여기에서는 국내외 보안침해 사례들을 분석하여 국내 보안사고 처리를 위한 기초적인 이해를 돕고자 한다.

1) Internet Worm 사건

1988년 11월 2일 코넬대학 대학원생인 Robert T. Moriss는 네트워크를 통해 상대편 UNIX(Berkeley) 시스템에 자신의 프로그램을 전송한후 시스템을 정지시키는 프로그램(일명 Internet Worm)을 개발한후 실행하여 6,000여대 이상의 인터네트 호스트를 일시 정지시켰다.

다만 Virus와는 달리 시스템의 정보를 파괴하지는 않았으며, UNIX 시스템의 네트워크 보안 취약점을 이용하여 자신의 프로그램을 상대편으로 감염시키는 이른바 Worm의 역할을 하였는데, 6,000여대의 컴퓨터를 하루밤새 일시 정지시켰으므로 그 놀라움은 매우 컸다고 볼 수 있겠다. 감염된 시스템은 사용자나 시스템화일이 파괴당하지는 않고 Worm 프로그램을 계속 복제하고 또 Compile함으로서, 즉 자신의 프로세스를 계속 증가하여 결국 시스템이 동작을 멈추게 된다. Worm 프로그램이 이용한 UNIX 시스템의 보안 취약 요소는,

①Fingerd의 보안구멍 (Security Hole) : argument size를 체크하지 않는것을 이용하여 buffer를 overflow 시킨다.

②Sendmail의 DEBUG 옵션을 이용한 Worm 프로그램의 전송 : SMTP인 Sendmail이 프로토콜을 시도할때 대신 DEBUG 옵션으로 별도의 Worm 프로그램을 전송하는 shell script를 수행한다.

③사용자의 account, passwd 이용 : 네트워크를

통해 시스템 사용자의 계정을 알아낸후 passwd를 공략함으로서 상대편 시스템을 감염시킨다.

으로서 이를 막기 위해서는 보안구멍이 제거된 새로운 시스템 프로그램으로 Version Up 하고 사용자의 패스워드를 보안성있게 유지하는 방안을 마련한다.

2) Cuckoo's Egg

Cuckoo's Egg(뻐꾸기 알)은 서독의 해커들을 추적한 시스템 관리자가 쓴 책자의 이름이다. 클리포드 스톨은 이 해커들이 다른 시스템에 불법적으로 액세스하고 불법적으로 정보를 빼내가는 것을 마치 뻐꾸기가 자신의 알을 다른 새의 둥지에서 부화시키는것을 연상하여 이러한 책이름을 고안 하였다. 이 관리자는 일년반에 걸친 추적끝에 서독 해커들이라는 사실을 알게되었고 해커들이 전세계 300여기관을 불법적인 접근을 시도하고 군사기밀정보를 탈취한다는 사실을 알게되었는데, NSA, CIA등에서 결국 이 해커들이 구 소련 KGB의 자금지원을 받는 서독 해커임을 밝혀 서독에서 기소되었다.

자신의 시스템에 불법침입한 침입자들이 서독의 어느 대학으로부터 시작되며 이것은 또 어느해커의 집에서 PC를 통해 시작된다는 사실을 알게되기 까지 그 해커들이 침입을 시도하는 시스템의 관리자, 전화회사의 교환원, 전화회사의 기술자, 국제 통신회선 담당자까지 협조하면서 추적하는것을 보면, 네트워크를 통한 보안 협조체제의 중요성을 깨닫게 하는 것이다.

3) 기타 해외 보안 사건

그밖에도 NASA에서의 Worms Against Nuclear Killers(WANK) worm 프로그램은 NASA 네트워크내의 많은 컴퓨터를 감염하였으며, 또 시스템 불법침입으로 3명의 호주 해커들이 구속당한 것, 2명의 해커들이 덴마크의 많은 컴퓨터에 불법침입하였다가 구속당한 사례등을 보아서 알수 있지만 현재에도 해외 인터네트에는 수많은 해커들이 아직도 해킹의 즐거움(?)을 노리고 있는 것으로 보고되고 있으며 매우 우려할만한 사실이다.

4) 국내 사례

국내 슈퍼컴퓨터가 91년도에 집중적인 침해를 당했었는데, 전단의 게이트웨이 워크스테이션들의 Public User-id를 이용 접속한다음 Trojan Horse 프로그램 등으로 수퍼 사용자권한을 획득하고 수퍼컴퓨터에 rlogin 할 수 있는 상태를 만든 다음,

-일반계정의 패스워드를 바꾸거나,

-Trojan Horse 프로그램을 만들고,

-Su, login등의 대치,

-시스템관리자 권한으로 shutdown 한일

등등의 행동을 하였다. 이후 시스템 관리자들은 수퍼컴퓨터에서의 위의 문제점들을 해결 조치하고 수퍼컴퓨터 보안기능을 강화 하였다.

그리고 1992년 7월 모 대학에 일단의 침입자들은 외부 Internet과 접속된 그 대학의 LAN Segment 내의 6대의 Sun 워크스테이션들을 불법 접근하여 화일시스템의 내용을 지우는 행위를 저질렀는데, 관리자 권한을 가지고 모든 화일 시스템을 지우는 행위도 있었으며 일부를 지우는 행위도 있었다. 관리자는 추후 Backup Tape로 이용 복구하였으나 3주전의 Backup Tape를 이용해야하는 경우도 있었으므로 3주간의 작업이나 정보는 고스란이 잃어버리는 결과가 되었다. 이후 관리자는 패스워드를 Crack을 이용 변경하고, 관리자의 패스워드 변경, COPS를 이용한 SUID 프로그램의 색출, 그리고 Backup 회수를 늘리는 조치를 취하였다. 그밖에도 모 기관의 연구센터에서도 불법침입자가 디스크의 화일시스템을 지우는 행위를 하였으며, 모대학의 네트워크 정보 서버시스템도 불법 접근하여 화일시스템 일부를 지웠다. 이러한 행위들은 단순한 해커의 활동에서 최근에 보안사고로서 리포트되고있는 내용을 볼때 침입자 (Intruder가 아닌, Cracker)로서 악의적인 활동을 벌이고 있음을 알수 있다. 보통 사용자의 계정을 훔친다음 Backdoor, Trojan Horse등의 해킹 프로그램 기술로서 관리자 권한을 획득하고 눈에띄지 않는 장소에 사용자의 계정과 패스워드를 저장해두고 지속적인 활동을 하려고 한다.

3. 불법 프로그램

컴퓨터 시스템에 불법 침입하는 프로그램의 종류를 보자면 다음과 같이 분류할 수 있다.

1) Back door : 불법 액세스를 가능케 하는 프로그램,
2) Logic Bombs: 어떤 조건에 맞으면 실행하는 프로그램,
3) Virus: 시스템 프로그램을 변경하거나, 자신을 복사하는것,
4) Worms: 네트워크를 통해 전파되어 감염하는 프로그램,
5)Trojan horse: 시스템 프로그램처럼 수행하나 다른 일을 하는것,

6) Bacteria: 컴퓨터 시스템을 정지하기 위해 자신을 복사하는것.

보통 침입자들이 불법 액세스를 위해 많이 쓰이는 불법 프로그램은 Back door, Trojan Horse 프로그램으로서 주로 다음을 주의한다.

1) login, telnetd, ftpd, rshd의 교체,
2) .rhost를 이용,
3) /etc/fstab에서 NFS를 이용,
4) sendmail 프로그램에서 불법 액세스,
5) /etc/passwd, /etc/groupdm를 이용,
6) /dev/kmem, 혹은 디바이스 화일의 권한 변경,
7) SUID 프로그램,
8) /etc/inetd.conf를 변경 리모트 불법 액세스

4. 보안사고의 대응

1) 기본 대처 상황

앞에서 기술한 여러 형태의 유사한 침해사례에 대응하기위해 현재 침입을 당하고 있는것을 알았을 때, 혹은 침입의 흔적을 발견했을 때 어떻게 해야 할 지 보통 시스템 관리자는 당황하게 된다. 이럴 경우를 대비하여 사실 이경우의 절차를 정책으로 미리 세워두는 것이 필요한 것은 당연하다. 아뭏든 이 경우 주의해야 할 점으로서 당황하지말고,

- o 정말 침해당한 것인지 의심해 보고,
- o 실제 화일이 손상을 입었나를 확인하고,
- o 증거물을 확득하고 보관할 필요성을 체크하며,
- o 가능한 빨리 복구하여 정상화 해야하는가?,
- o 화일의 변경유무를 다시 확인할 필요성이 있는가?,
- o 내부나 외부 사람이 이 일을 알아도 되는가?,
- o 다시 발생 가능한 일인가?,
- o 문서화 작업,
- o 즉시 log를 만드는 것등의 제반 대처를 해야 한다.

2) 침입자의 발견

침입자를 발견하기 위해서는 관리자가 침입자의 활동을 직접 모니터링할 수도 있으며, security hole, /etc/passwd등의 시스템 화일이 변경된 것을 확인하거나, 다른 지역의 관리자로 부터의 통지를 받아 알 수도 있다.

3) 해커 발견후 조처

침입자를 발견한 후 관리자의 조치는 상황을 보며 판단하는 것이 좋은데 네트워크를 통해 들어온 침입자를 역추적 하기 위해 finger, who, netstat등의 명령을 통해 알아보고, 상대 시스템의 정보를 알아낸 후 상대 시스템 관리자의 협조를 요청한다.

①침입자의 침입방법 분석

이를 위해서는 UNIX의 log 화일을 분석해야 하는데, 주로

- o 비정상적인 시간대의 login과,
- o 의심스러운 su 명령,
- o 낯설은 시스템으로부터의 login등을 우선 체크한다.

하지만 교묘한 침입자는 대부분 이러한 시스템 log 화일이나, 자신의 사용 흔적을 지워 보통의 정상 상태로 만들어 두는 예가 많다. 이것이 어려울 경우 아예 log 화일 전체를 없애 버리기도 한다.

② 침입자의 시스템 불법 정리

침입자를 몰아내고 여러 분석을 마친 후 침입자가 만들어둔 여러가지 불법 작업들을 정리해야 하는데, 먼저 새로운 계정을 만든경우에는 /etc/passwd화일을 원래대로 복구해야 한다. 특히 UID가 0인경우, passwd가 없는 경우등을 검사한다. 그리고 침입자들이 만들어 둔 불법 바이러스 프로그램등을 없애기 위해 SUID, SGID 프로그램등을 색출하고 화일과 디렉토리등의 권한 모드의 변경 유무 체크, backup과 비교 Integrity체크를 시도한다. 그리고 감추어진 화일과 디렉토리들을 찾기 위해 /etc/fsck를 이용하거나, /usr/bin/cat-v등을 이용한다.

Ⅲ. 인터네트의 보안활동

인터네트 보안에 관한 활동은 각 기관별 보안센타 활동과 IETF 보안, 표준화 활동의 두가지로 대별 할 수 있다.

1. 보안센타 활동

인터네트 관련 미국의 주요 기관의 보안센터(CERT, NIST, DOD, DOE등)에서는 보안침해사례의 수집, 분석 및 배포를 통하여 보안침해를 방지 및 최소화하는 활동이 활발히 진행중이다. 특히, 전세계 100개국이상이 인터넷에 연동되어있고, 서독 스파이사건에서 보듯이 보안침해는 전세계를 무대로 발생할 수 있으므로 FIRST(The Forum of Incident Response and Security Teams)와같은 보안을위한 국제적인 조직을 통하여 보안기술 및 정보 교류등이 활성화 되고 있다.

1) CERT/CC(Computer Emergency Response Team / Coordination Center)

1988년 11월 발생한 Internet Worm 사건이후 미국은 인터네트 보안을 위하여 체계적인 인터네트 보안 전담기구인 CERT/CC를 카네기 멜론대학 소프트웨어 공학연구소에 만들었다. CERT는 총 14명으로 구성되어있으며 DARPA로부터 예산지원을 받고 있다.

주요 구성 그룹으로는 Incident Response 그룹, 보안 연구그룹, 보안 툴 개발 그룹, 교육훈련그룹등이 있다.

주요 활동 내용 :

o Incident Response 활동을 통하여 타 기관에 대한 보안기술지원 및 Vendor와 보안전문가와의 긴밀한 협조관계 유지

o 보안 침해사고 접수 처리 활동을 통하여 보안 데이타베이스를 구축하고 인터네트 일반 사용자에게 제공

o FIRST 활동을 통하여 타 국가 및 타 기관의 보안센타와 보안관련 정보 공유, 보안사고 방지 및 대책 마련을 위한 기술협력, 보안사고 해결을위한 국제적 협조체제 구축

o IETF 보안 표준화 활동 (RFC 1281 "GUIDE LINES FOR THE SECURE OPERATION OF THE INTERNET")

필요한 정보는 mail to cert@cert.org 혹은 anonymous ftp cert.org로 거져올수 있다.

2) FIRST(The Forum of Incident Response and Security Teams)

FIRST는 컴퓨터 보안 침해 문제를 해결하고 보안사고를 방지하기위해 정부, 학술기관, 일반기업체 및 학교등 각종 단체에서 자발적으로 모인 국제조직으로서 현재의 가입기관은 아래와 같다.(7개국, 33개기관)

CERT	Apple CORE	U.S.Sprint
SUN	DEC	EDS
US Navy	Motorola	TRW
DDN	CCTA(영국)	NASA Goddard
SERT(호주)	USN	Micro-Bit Virus Center(독일)
Penn Sachs	GE	DFN(독일)
Goldman,Sachs	West Inghouse	NORDUNet(스웨덴)
Renater(프랑스)	USAF	NIST
DOD	SBA	NASA Ames
DRA(영국)	DOW USA	DOE
Purdue	Unisys	SURFNet(네델란드)

FIRST 의 목표

o 보안사고의 효율적인 방지 및 감시, 사고후 원상회복등에 필요한 기술 및 정보의 교류

o 보안사고의 위협 및 출현등을 신속히 전파할 수 있는 방안 마련

o FIRST의 연구활동에 필요한 사항 제공

o 기타 보안정보의 공유

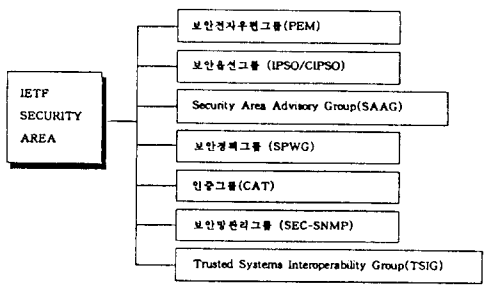
FIRST의 가입은 전체 가입기관의 2/3이상의 동의를 얻어야하며 탈퇴는 임의로 할 수 있으며 본부는 NIST에 있다. 또한 매년 보안교육 및 홍보를 위하여 Incident Handling Workshop을 개최하고 있다. 관련정보는 first.org를 통하여 anonymous ftp로 가져올 수 있다.

3)기타

그외 CERT/CC와 유사한 기관으로 다음과 같은것들이 있다.

- o DDN SCC : 미국방성 네트워크 Security Coordination Center (anonymous ftp nic.ddu.mil)
- o NIST CRSC : 미 표준기술국 Computer Security Resources and Response Center (anonymous ftp csrc.ncsl.nist.gov)
- o DOE CIAC : 미 에너지성 Computer Incident Advisory Capability (mail to ciac@tiger.llnl.gov)
- o NASA CNSRT : 미항공우주국 Computer Network Security Response Team (mail to cnsrt@ames.arc.nasa.gov)

2. IETF 보안 표준화 활동



1) 보안 전자우편 그룹 (PEM)

Private Enhanced Mail(PEM)은 일반 인터네트 전자우편에 무결성, 기밀성, 송신자 인증등의 보

안기능을 제공하는 프로토콜이다. PEM은 DES(대칭적 암호기법)및 RSA(비대칭적 암호기법)을 표준 암호화 기법으로 권고하고 있다. (RFC 1421~1424)

PEM 의 절차

①수신자의 증명서를 가져와서 수신자를 확인하고 공개키를 알아낸다

②Data Encryption Key(DEK)생성

③표준 메세지 형태로 변화시킨후 암호화를 하고 Message Integrity Check(MIC)를 계산한다

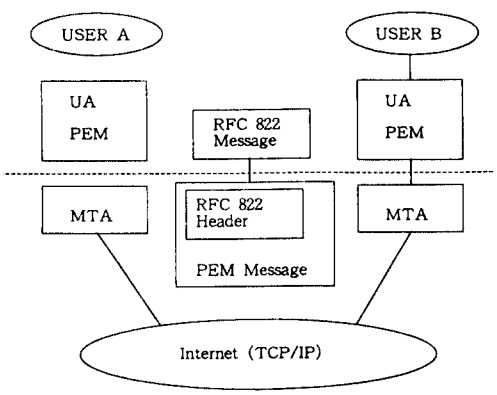
④송신자의 비밀키로 MIC 암호화, 수신자의 공개키로 DEK를 암호화

⑤PEM 헤더 생성

⑥수신자는 PEM 메세지의 증명서 확인, 송신자 공개키 추출

⑦ DEK 복호화, 무결성 확인

⑧ 원 메세지 생성



2) IP 보안 옵션 그룹 (IPSO/CIPSO)

(Internet Protocol Security Option / Common IPSO)

데이타 비밀등급과 사용자 및 사이트의 비밀 취급인가 수준을 나타내는 레이블링 방식을 통하여 네트워크상의 정보 흐름을 제어할 수 있다. RFC 1108은 미국내의 보안분야에서만 통용되도록 설계된 프로토콜로서 현재 두가지 옵션을 제공하고있다.

o DOD Basic Security Option :

Unclassified, Confidential, Secret, Top Secret의 4가지 분류와 관련 DOD Authority 플래그로서 IP Datagram이 레이블되며 이를 통하여 엑세스 제어가 이루어진다.

o DOD Extended Security Option :

보안 카테고리나 Release Marking과 같은 부가정보들을 처리할 수 있도록 한다.

CIPSO는 다른 정부기관들과 민간기업을 대상으로 하는 IPSO이다.

3) IETF SAAG 그룹

인터네트에서 사용되는 새로운 프로토콜, 서비스를 개발하는 워킹그룹으로 구성되어있고 주요 워킹그룹으로는 전자우편 서비스의 확장, 네트워크 데이타베이스, 네트워크 뉴스 프로토콜, 네트워크 팩스, 네트워크 프린팅, 가상터미널, 접속지향 IP, 동적 호스트 구성, ATM상의 IP, Apple Talk IP, FDDI IP, 라우터 요구사항 디렉토리, MHS, OSI 네트워크 운영, ODA, IP 시큐리티 옵션, 인증기술, 보안전자우편, 망관리 보안, 오디오, 비디오, 분산화일시스템 등이 있다.

4) 보안정책 그룹 (SPWG/ SSPWG)

인터네트 보안정책을 만드는 그룹으로 다음과 같은 보안정책을 제시하고 있다.

o 각 사용자는 보안정책을 이해하고 따라야 한다.

o 각 사용자는 보안 메카니즘과 절차를 사용해야 한다.

o 시스템, 서비스 제공자는 보안을 유지해야 한다.

o 업체와 시스템 개발자는 보안 기능을 제공해야 한다.

o 사용자, 업체, 시스템 제공자는 보안을위해 상호 협조해야 한다.

o 인터네트 보안 프로토콜의 개발은 지속적으로이루어 져야 한다.

o 인터네트에서의 개발시 반드시 보안을 고려해야 한다.

5) 인증 그룹 (CAT)

한 사용자의 신분을 타 시스템에서 그 신분을 확인하게하는 사용자 인증의 방법으로서 Kerberos와 X.509 공개키 방식을 사용하는 DEC의 DASS(Distributed Authentication Security Service)가 있다. 이 그룹에서는 서로다른 키 방식을 사용하더라도 인증 서비스는 같다는 점에서 응용 프로그램들이 어떤 방식에서도 동작하는 공통의 인터페이스를 제공하기위한 작업을 하고 있다. GSS-API(General Security Services Application Program Interface)로서, GSS-API base application GSS-API, C언어 bindings, kerberos Version 5 가 검토중에 있다.

6) 보안 망관리 그룹 (Sec-Snmp)

SNMP(Simple Network Management Protocol)

는 인터네트에서의 장비들을 제어하는 프로토콜이다. 한 Request에 대 해 서 MIB(Management Information Base)를 근거로 응답하게 된다. 불법 Request를 방지하기 위하여 Secure SNMP는 보안 Wrapper를 제공한다. Wrapper는 Request 및 Response 할수 있는 시스템들을 지정한다. 이를 위하여 대칭적 키 암호를 사용한다 (MD5, RFC 1321). 기밀성 (Confidentiality)이 Option으로 주어지며, DES가 이용된다. Secure SNMP에대한 자세한 내용은 Proposed Standard로 발표될 예정이다.

7) TSIG (Trusted Systems Interoperability Group)

o 신뢰성 있는 시스템간에 상호 연동에대한 분야를 개발

o 상호연동사양을 개발

o 분산시스템에서의 인증방법 개발

Ⅳ. 네트워크 보안 방안

1. 방화벽(Firewall) 시스템 보안 방안

방화벽 시스템은 인터네트에 접속된 가입기관의 내부 네트워크 도메인내에 속한 여러 리소스를 보호하기위한 대응방안으로서, 외부 네트워크와 접속하는 게이트웨이 시스템을 두고 그 시스템에서 인증(Authentication)을 받아 내부, 외부로의 트래픽 접근을 허용하는 시스템으로서 최근 활발히 연구개발되고 있는 현실적인 보안 대책중 하나이다. 방화벽 시스템은 주로 외부(external) 시스템 개념이 주종을 이루고 있으나 최근에는 내부 (Internal) 방화벽 개념도 많은 관심을 모으고 있다.

1) 내부 방화벽

모든 시스템을 하나의 LAN으로 연결하지 말고, 작은 여러개의 LAN으로 구성하여 게이트웨이나 라우터를 이용하여 상호 연결하고 다음과같이 조치한다.

o 각각의 LAN마다 NIS 서버를 둔다(즉, 전체 NIS 서버를 두지 않음)

o 다른 LAN의 시스템을 신뢰하지 않는다.

o 여러 LAN에서 복수개의 계정을 가진 사용자는 서로 다른 패스워드를 가져야 하며 LAN간에는 rhost를 허용하지 않으며, 또한 LAN을 경유한 접근이 있을 경우 인증 방법이 있어야 한다.

o 게이트웨이는 최대 수준의 log를 하며, 보안기능을 최대화하고, 가능한 사용자 계정을 두지 않는다.

그리고 이러한 Internal Firewall 시스템을 사용하였을 경우의 장점은 다음과 같다.

o LAN의 물리적인 고장의 파급을 최소화한다.

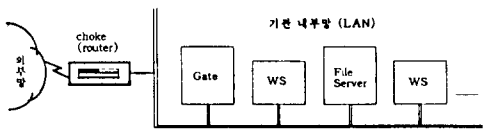
o LAN에서의 시스템 수가 적으므로 고장의 위험을 최소화 한다.

o Flooding 공격에 영향 받는 시스템의 수를 최소화 한다.

o 특정 시스템의 공격에대한 방벽을 만들 수 있다.

2) 외부 방화벽

외부 방화벽 시스템의 일반적 구성 형태는 그림과 같은데 여기에서 choke와 Gate는 같은 하나의 컴퓨터 일수도 있고 또한 Gate는 프로토콜별로 여러개의 컴퓨터가 될수도 있다.



o 게이트웨이 시스템은 내부와 외부 네트워크 사이의 데이터를 패스한다.

o Choke는 외부에서 들어오는 패킷의 목적지 호스트가 게이트웨이가 아니면 접속을 거부한다.

o 내부 네트워크의 호스트 이름, 어드레스, 라우팅 정보는 외부로 발행하지 않음으로서 외부에서 내부의 어느 호스트라도 직접 접근하지 못한다.

o 내부 호스트로 접근하려는 외부의 사용자는 게이트웨이 시스템에 계정이 있어야하며, 인증을 받아야만 내부 시스템에 접근할 수 있다.

o 게이트웨이 시스템은 Dynamic Routing을 실행하지 않으며, Static 라우팅만이 제공된다.

o 게이트웨이 시스템은 일반 사용자 계정을 가지고 있지 않으며, 단지 root, 그리고 외부에서 내부 도메인으로 접근이 허용된 사용자 계정만이 있다.

o 게이트웨이 시스템은 해커의 표적이 되는 시스템 유틸리티들을 삭제하고, Trojan Horse, Backoor의 표적이 되지 않도록 권한 조정과 보안 환경을 극대화한 시스템이다.

3) 방화벽 시스템 환경에서의 Name 서비스

Gate의 구축시에도 기관 자신의 Domain Name 서비스는 지속적으로 제공되어야 한다. 특히 전자우편 서버를 위한 서비스를 위해서도 도메인 네임 서비스를 지원해야하는데, 보통 Gate 시스템이 전자우편

서버 기능을 함께 지원한다. 이럴 경우 그 서버는 내부의 특정 호스트로 전달해야 할 전자우편을 받아 넘겨주어야 한다. 이를 위한 도메인 네임 서비스의 예를 들기 위해 예제 도메인을 example.re.kr로 두고, Gate 시스템이 gate.example.re.kr, 내부에서 전자우편을 받을 호스트를 inside.example.re.kr로 가정한다. 이럴경우 내부 호스트에대한 MX 레코드의 값은,

inside.example.re.kr IN HINFO NEXT MACH
: 604800
inside.example.re.kr IN MX 10 gate.example.re.kr
: 604800

으로 지정하면 된다.

4) 방화벽 환경에서의 전자우편 서비스

전자우편 서비스는 외부로 나가는 모든 전자우편이 Gate 에서 나가는 것처럼 하기위해,

o 전자우편 헤더의 From: , To: , Cc: 들은 user@inside.example.re.kr에서,

user@example.re.kr로 바뀌어져야하며,

o Gate로 들어오는 모든 전자우편들은 내부의 정확한 전자우편정보를 위해 alias를 가지고 있어야 하는 것이다.

o 또한 내부의 호스트에서의 전자우편들은 모두 Gate로 전달되도록 구성해야 하며, Gate에서 헤더가 다시 작성되어 외부로 전달되게끔 한다.

이와같이 구성한 경우의 장점은 다음과 같다.

o 단지 하나의 서버만이 복잡한 전자우편 구성을 가지면 된다.

o 단지 하나의 서버만이 사용자의 완전한 alias를 가지면 된다.

o 내부 사용자의 전자우편 환경의 변화가 있다면 하나의 서버에서만 그것을 수정하면되고 외부의 사용자는 그 변화를 몰라도 된다.

o 사용자의 계정에 대해 Alias를 자유롭게 사용할 수 있다.

o 퇴직한 사용자의 전자우편 forward를 위해 계정을 남겨둘 필요없이 해결할 수 있다.

5) 방화벽 환경에서의 Netnews 서비스

Gate 시스템을 news 서버로서 구성하는 것이 좋은 방법이다.

o 모든 외부로 나가는 뉴스 기사들의 Path:, From: 등에는 gate의 이름만이 보이도록 지정하는데, B 뉴스시스템의 경우 이렇게 간단히 Configuration을 고칠 수 있다.

o 내부에서는 간단하게 NNTP와 rrn 으로 뉴스를 볼 수 있다.

o 뉴스의 spool 디렉토리 (/usr/spool/news)는 NFS로 내부 호스트에게 Export 한다.

6) 방화벽 시스템 환경에서의 FTP 서비스

Anonymous FTP의 경우에는 gate 에서 이를 구성하고, 내부 사용자는 NFS로 접근할수있도록 한다. 그리고 내부 사용자가 외부 호스트와 FTP 하고자 할 경우에는 Gate에 패스워드가 *인 ftpout등의 특정계정을 하나 마련하고 그 계정의 /etc/passwd 엔트리의 마지막 쉘 정의 부분을 /usr/ucb/ftp로 지정한다. 또한 그 계정의 HOME 디렉토리는 root 소유로 하며, 권한 모드는 755로 조정하며, root 소유의 ~ftpout/.rhosts 만들어 ftpout 계정을 쓸 수 있도록 허가된 내부사용자의 리스트를 저장하고 내부에서,

% rlogin gate.example.co.kr -l ftpout

를 통해 ftp 할 수 있도록 한다. 그리고 syslog 등을 통해 모든 ftpout에대해 로그를 만드는것이 중요하며, 내부 사용자는 전송된 화일을 NFS를 통해 접근한다.

7) 현존 방화벽 시스템 현황

기술한 Firewall 시스템은 현재 Internet상의 현실적인 보안대책중 하나로서 다음 표와 같은 무료로 공개된 혹은 상용제품들이 발표되어 활용되고 있다.

표 Firewall 시스템 현황

제품명	개발기관	형태	기 능
InterLock	ANS CO+RE Systems, Inc.	상용	TELNET, FTP, SMTP Gateway, X-Window, NNTP 등을 제공에서, Logging, 사용자인증, 보안에 필요한것
Eagle Network Security Management System	Eagle Network Security	상용	시스템 인증, Monitoring & Tracing, Real Time Event Reporting, Audit Log, 사용자 인증등
Internet Firewall Toolkit	Trusted Information Systems	공개	FTP, TELNET, rlogin, NNTP Proxy 서버스, SMTP Gateway, 사용자 인증, TCP 접근제어
Texas TAMU	Texas TAMU Univ	공개	하우의 방화벽, 스크린
Karlbridge	Ohaio Univ.	공개	PC-Based 하우의 방화벽 키트
Cisco's	CISCO, Inc.	상용	CISCO 하우터의 액세스 리스트를 통한 방화벽

2. 인터네트 보안도구

보안상의 취약점을 가지고 있는 인터네트 그룹의 보안관련 기관들은 시큐리티 구현에 필요한 문서, 도

구, 아이디어들을 개발 보급하고 있는데 여기에서는 크게 시스템 레벨과 네트워크 레벨에서의 시큐리티 강화 도구들에대한 현황을 분석 정리한다.

1) 시스템 레벨

① 인증서명 관련

명 칭	기 능
npasswd	◦ UNIX의 보통 passwd 대신 사용가능 프로그램 ◦ Password 정책에 정의된 구성에따라 사용자에게 특정 패스워드 사용토록 강제함 ◦ Password aging 기능이나 expiring check 기능 없음
passwd+	◦ 시스템의 /bin/passwd와 교체 사용 가능 ◦ 사용자가 추측하기 쉬운 패스워드 사용하는것 방지
shadow	◦ encrypt 되어진 사용자 패스워드를 보지 못하게 함 ◦ C2 Security 레벨 ◦ crack등에의한 패스워드 유출 가능성 줄임
passwd 2.1	◦ 사용자가 패스워드를 새로 갱신할때마다 사전에 crack 당할지 여부를 판단하여 좋은 패스워드 사용하도록 강제 ◦ Password aging, expiring 기능 추가
crack	◦ passwd 화일의 DES 방식으로 암호화된 field를 여러가지 규칙 및 사전 대입식을 통해 역으로 풀어내는 Tool
KC(Killer Crack)	◦ crack 3.0의 대체 Tool
UFC-crypt	◦ crack이나 KC의 암호 해독시간을 보다 빠르게 하기위한 crack 4.1의 보완 Tool

② 암호화 관련

명 칭	기 능
kerberos	◦ client와 server사이에 password등의 정보들을 암호화하여 인증, 상호정보교환
louko_des	◦ DES 패키지로서 kerberos의 인증 서버에 사용시 적합
des_dist	◦ louk0_des의 신 버전
cbw	◦ Single UNIX crypt(3)에의해 암호화된 메세지를 복호화하기위한 상호 문답식 세트
hill	◦ Hill-cipher를 이용한 암호화 프로그램 ◦ 이용자가 키를 주어 ASCII 모드의 cipher text를 만들때 사용
des	◦ 화일 암호화 tool ◦ kerberos des 패키지에 상응하는 기능 갖도록 구현
karn	◦ DES tool

③ 모니터링, 화일시스템 점검 관련

명 칭	기 능
miro	◦ cops, audit 등과같이 보안 체한요소들을 정의하고 체크하는 tool ◦ 보안정책의 확장이나 수정에 용이
cops	◦ 보안상의 문제를 자동으로 검토하고 체크하여 경고를 보고 해주는 tool ◦ MIT에서 제작된 Rule-Based Security check system인 kuang expert system이 포함되어 있음
KUANG	◦ 보호 메카니즘을 사용자가 일관성있게 사용하는가를 체크하는 tool ◦ Hack등의 공격자의 입장에서본 UNIX 보호 기법 이용
Tripwire	◦ UNIX 시스템의 화일 변경 상태를 감시하는 tool
Watcher	◦ 시스템을 감시하기위한 Monitoring 프로그램
fsh	◦ /usr/local/bin에 설치되어 사용자의 shell account를 close off 하는데 사용됨
syslogd	◦ syslog library나 syslog daemon이 없는 경우 사용 가능
Swatch	◦ syslog와 같은 logging 기능 수행 ◦ 편리한 사용위해 telnetd나 ftpd와 같은 프로그램들 수정
sundiag	◦ SUN O/S 하드웨어 diagnostic 프로그램

④ 네트워크 관련

명 칭	기 능
tcp_wrapper	◦ TCP/IP의 응용서비스에대한 접근제어, 인증, 로그, 함정기능 제공
SOCKS	◦ TCP_Wrapper와 유사한 기능을 하며 접근제어, 로그등 제공
netstat	◦ local 호스트의 네트워크 상태 및 정보제공
log/tcp(tcpd)	◦ 호스트로 연결 시도하는 모든 활동을 로깅 ◦ 호스트 이름이나 어드레스의 속임수도 점검
TCPDUMP	◦ Ethernet상의 트래픽 dump, 트래픽 Tapping 가능
tcpwr.shar	◦ Finger, FTP, TFTP, TELNET, RLOGIN, RSH, EXEC, TALK등 IP 네트워크 서비스에 관계된것 모니터링
Xinetd	◦ inetd와 대체 사용가능하며 logging 및 접근제어
ftpd-5.177	◦ 기존의 ftpdfmf 개량하여 security기능을 향상시킨 tool
tamu	◦ 강력한 bridging filter 패키지
netlog-1.02	◦ 침입을 발견해내는 유용한 프로그램들로 구성
traceroute	◦ 패킷이 route 될때 routing path의 추적 가능
nfswatch	◦ NFS 트래픽 모니터링 도구
securelib	◦ 인증되지않은 액세스에대한 RPC daemon들 보호
etherfind	◦ ethernet 상의 패킷들을 찾는데 사용
rpcinfo	◦ RPC 정보들 보고

V. 결언

최근 국내에서도 부각되고있는 인터네트의 보안문제는 첫째, 교육.연구기관들 사이의 자유로운 연구 및 기술 정보교환을위한 전산망의 개방화 추구, 둘째, 전산망이 채택하는 네트워크 프로토콜인 TCP/IP 및 대다수 기관의 UNIX 기종의 보안 취약점, 셋째, 해외 인터네트로부터 보안 침해기술이 자유롭게 유입되는등 보안에대한 기본적인 취약한 배경에 기인하고 있다.

글로벌 네트워크인 인터네트의 보안사고는 세계 도처에서 급증하고 있으며 우리나라도 몇년전부터 이러한 보안침해사건이 점점 빈발하고 있다. 금년중 국내 인터네트 상용화 서비스가 확산되면 불특정 다수의 가입자에 의한 보안 침해 가능성은 더욱더 높아질것으로 사료된다.

해외에서는 본고에서 소개한 바와같은 보안사고등에 대비하여 미국의 카네기 멜론대학의 CERT/CC등의 보안사고 응답센터의 구축, 인터네트를 위해 각종 기술 지원 및 연구개발을 담당하는 그룹인 IETF에서의 Security 관련 기술개발, 그리고 주요 기관들의 Firewall 시스템 구축과 공개 소프트웨어 개발보급등 보안사고를 사전에 방지하고, 사고발생시 피해를 최소한으로 줄이기 위한 부분에 많은 노력을 기울이고 있다.

국내에서도 학술연구전산망 참여집단에서 대학 및 연구소의 전문가를 중심으로 보안관련 워킹그룹을 결성하여 일부 활동을 하고 있고, 관련학회 및 전산망 전담기관에서도 나름대로 많은 노력을 기울이고 있으나, 특히 앞으로 급증할 불특정다수의 해커들에 의한 피해를 체계적으로 방지하고 효과적으로 대응하기에는 많은 무리가 있는것 같다.

앞으로 초고속 국가기간망 구축시에도 보안문제는 주요 사안으로 등장할 것으로 보이므로 범 국가적인 차원에서의 종합적 보안대책 및 동분야에 대한 연구 및 기술개발의 적극적 투자가 시급히 요망된다고 본다. 현실적으로 시급한 관련 프로그램 및 보안 지침서의 개발과 아울러 전산망 보안센터의 구축, 전문가 양성, 그리고 IETF와 같은 국내 Security WG의 보다 적극적인 활동에의한 기술지원등은 국내 인터네트 발전 및 활성화를위해 적극 추진해야할 최소한의 현안 사항이라 할 수 있을 것이다.

參 考 文 獻

[1] Garfinkel & Spafford, Practical UNIX Security, O'Reilly & Associate, Inc., 1992.

[2] RFC1244, Site Security Handbook.

[3] RFC1281, Guidelines for Secure Operation of the Internet.

[4] Steve Crocker, Ocerview of Internet Security Development, INET'93, June 1993.

[5] Stephen T. Kent, An Overview of Internet Privacy Enhanced Mail, INET'93, June 1993.

[6] Richard D. Pethia, Kenneth R. Van Wyk, Computer Emergancy Response-An International Problem, CERT/CC SEI CMU, 1990.

[7] Marcus J. Ranum, A Network Firewall, Digital Equipment Corp., 1992.

[8] Wietse Venema, TCP WRAPPER : Network Monitoring, Access Control and Booby Traps, UNIX Security Symposium III, Sept. 1992.

[9] ANS CO+RE, Inc., InterLock-The Key to Network Security, May 1993.

[10] TSIG, Trusted Realm Environment Exchange Serveice.

[11] TSIG, Trusted Systems Interoperability Group : FAQ with Answers, Jan. 1994.

[12] TIS, Internet Firewalls Frequently Asked Questions, March 1994.

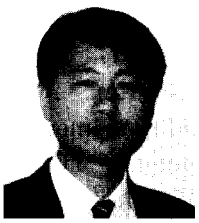
[13] 시스템공학연구소, "Workstation security Guide Summary", 1993.

[14] 정윤종, 김재우, 변옥환, 임채호, "Privacy Enhanced Mail For KREONet", JW-ISC, 1993.

[15] 박형우, 윤기송, 임채호, 변옥환, "연구전산망 보안센타 구축연구", 한국통신정보보호학회, 1993. 11.

[16] 정진욱, "Internet Security", 산학연저널, 1994. 4.

筆 者 紹 介

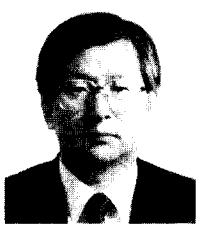


윤 기 송

1957年 9月 19日生
1984年 2月 부산대학교 조선공학과 (학사)
1988年 NewYork CITY UNIV. 전산학(석사)
1993年 NewYork CITY UNIV. 전산학(박사)

1993年 6月 ~ 현재 시스템공학연구소 연구전산망개발실 선임연구원

주관심 분야 : 컴퓨터네트워크, 네트워크 보안, 병렬알고리즘



변 옥 환

1953年 8月 28日生
1979年 한국항공대학교 통신공학 (학사)
1985年 인하대학교 전자공학 (석사)
1993年 경희대학교 전자공학 (박사)

1978年 9月 ~ 1983年 12月 KIST 전산개발센터 연구원
1983年 12月 ~ 1984年 12月 미국 OSM Computer Corp. 연구원
1985年 3月 ~ 1988年 2月 KIST 시스템공학센터 선임연구원
1988年 3月 ~ 1994年 ~ 현재 시스템공학연구소 연구전산망개발실장/책임연구원

주관심 분야 : Network Management & Security, 전산망 설계 구축