□ 기술해설 □

인터넷 해킹 수법의 이해 및 대책

한국정보보호센터 신 훈*·임휘성·임채호

1. 서 론

인터넷 등 전산망에서의 해킹 등 침해사고는 지금까지 꾸준하게 증가되고 있으며, 시스템의 새로운 보안취약점들이 계속적으로 불법 해커들에의해 개발되어 그 수법들이 배포되고 있는 실정이다. 또한 해킹 등 침해사고의 경향도 단순한 호기심 차원을 떠나 경제적 이익을 노린 해킹과 무정부주의적인 사이버테러 식의 해킹, 기업스파이 해킹 등 다양해지고 있으며, 미국 국방성이 준비하고 있는 "정보전-방어"[1]와 같이 적성국가에 의한 국방전산망 등 국가기간전산망에 대한 불법적인 침입과 테러 등을 우려하기도 한다.

먼저 해킹 등 통신망과 컴퓨터에 대한 불법적인 비정상행위를 표 1과 같이 분류해 볼 수 있다. 인터넷 등의 전산망의 발전에 따라 시스템해킹, 무정부주의적 사이버테러, 바이러스 등이 급격하게 확산되고 있으며, 금융망을 위협하는 신용카드 불법 복제사기 등의 하드웨어 해킹, 전화교환기 및 이동통신, 위성통신에 대한 불법적인 도청과 과금조작 등이 우려되고 있다.

표 1 컴퓨터 비정상 불법 분야

비정상 분야	설 명	비 고
시스템 해킹	전산망·시스템 취약점 해킹	일반 해킹
하드웨어 해킹	상용시스템 하드웨어 락 해킹	신용카드 등
무정부주의 해킹	파괴·혼란을 노리는 공격	사이버테러
바이러스 해킹	웜, 바이러스 등 제작·배포	자료파괴, 동작정지
전화망 해킹	전화망 해킹 과금 조작, 파괴	프리킹 (Phreaking)

* 정회원

1) IW-D(Information Warfare-Defense), Nov/1996

여기에서는 시스템해킹 등 전산망에 관련되는 해킹 수법들과 대책을 논하고자 하는데, 우선 해커들을 불법적 해킹을 시도하는 그 동기에 따라 분류해 보고 최근 해킹 및 해커들의 변화를 살펴보고자 한다. 다음 표 2는 해커들을 추구하는 동기에 의해 분류해 본 것인데,

표 2 해커의 동기에 의한 분류

해커의 종류	동 기	비 고
단순 해커	호기심·영웅심리	대부분의 해커
내부 불순분자 해커	개인·집단의 이익과 동기	내부 직원
범죄적 해커	금전적 이익 추구	금융망 등 대상
테러리스트/그룹	개인, 그룹이 추구하는 이상	혼란·파괴 목적
기업체 고용 해커	기업 이익 추구	기업정보유출
국가 고용 해커	경쟁국 등 정보 유출	국가 이익추구

범죄적이며, 집단적인 불법행위를 일으킬 수 있는 해커들에 대한 분석과 대책이 매우 필요하며 단순 호기심에 의한 해커들도 지식을 깨우치면서 범죄적 양상으로 변해갈 수 있다는 점이 매우 우려되는 것이다. 특히 표 3에서 보이고 있는 미국방성이 규정한 미국내 주요기간망에 대한 위협에서는 보다 세분화하여 정치적 군사적인 동기까지도 예측하고 있는 실정이다.

최근 미국 등 선진국에서는 홈페이지 공격[2]

표 3 미국방성이 규정한 주요 위협

주요 위협 형태	증명된 사 례	알려진 사 례	2005년경 가능시례	2005년후 가능시례
조작 미숙 운영자	W			
일반 단순 해커	W			
조직 내부 불순분자	W			
단순 일반 범죄자	W			
조직적 범죄자	L		W	
정치 반대파에 의한 범죄		W		
테러리스트 그룹		L	W	
해외 국가 스피이	L		W	
진술·용병에 의한 수단		W		
의도적인 전술적 정보전			L	W
국가 안보 체제 파괴자				L

※W(Widespread)=광범위함, L(Limited)=제한됨

이 많았으며 유나보머(Una Bomber)와 유사하게 유나메일러(Una Mailer)가 등장하여 ISP를 공격[3]하거나, 주요 저명인사에 대한 공격[4], 신용카드회사 공격[5] 등이 이루어졌으며, 국내에서는 학생들의 단순한 해킹이 아닌 홈뱅킹 사기사건[6], 중고등학생들이 해킹에 심취하여 불법 침입을 시도하거나 PC통신 패스워드 및 ID 사기 사건 등을 일으키고 있다. 국내외적으로 해킹이 범죄화되고 연령이 어려지는 등 심각한 사회문제로 발전하고 있음을 알 수 있다.

최근 해커들에 의한 해킹사고 등에 관련하여 예전과는 다른 변화를 보자면 다음과 같다.

- -그룹화되고 있으며 지능화 되는 경향
- -공격 수법과 도구·방법론들이 우수해지고, 복잡해지며, 빨라지는 경향
- -공격 지식을 전문가와 초심자가 우수한 통신수단을 이용하여 서로 주고 받는 경향
- -보다 강력하고 범죄적 동기를 제공하고 있는 경향
- -국제적 피해 사례가 점점 확대되고 있는 경향
- -해커에 의해 개발된 새로운 취약점들이 늘고 있는 경향

그러므로 이젠 해커를 단순한 호기심에 의한 침입시도로 보기 어려워지고 있어 보다 적극적으로 대처해야할 필요성이 대두되고 있다.

이 논문에서는 기존에 자주 이용된 전형적인 해킹 수법들에 대해서는 간략하게 요약 설명하고자 하며 주로 최근 해외에서 자주 논의되고 있는 해킹 사례와 새로운 취약점들에 대해 살펴보고 사이버테러 등에 사용되는 수법인 서비스거부공격(Denial of Service Attack) 수법을 분석해 보고자 한다.

2. 기존의 해킹 수법의 이해 및 대책

2.1 해킹 수법 요약

지금까지 90년대 초반에 많이 이용되던 해킹 수법들은 이제 업체들의 수정판 배포 및 버전업과 시스템 관리 실무자들의 관심으로 취약점들이 많이 해소되기는 하였으나 여전히 해커지망생들에 의해 이용되고 있으며, 관심을 가지고 대처방법을 구현해야 한다. 대표적인 해킹 수법들을 이 시기의 미국 CERT에서 발표한 경향을 토대로 살펴보면,

- -Crack 을 이용한 패스워드 크래킹,
- -sendmail 취약점 공격,
- -패킷 스니퍼링(sniffering),
- -NFS, NIS 등 시스템 취약점 공격
- -tftp, ftp 공격, 시스템 남용 공격

등으로서 CERT, CIAC, 8LGM 등에서 지금까지 발표된 시스템 취약점 기술권고문들을 분석하고 데이터베이스화한 보고서[7]를 참고하기 바라며, 여기에서는 해킹 수법들을 그 형태에 따라 분류하고 그 대응 방안에 대한 요약표로서 설명을 대신하고 주요 해킹 수법과 대책들에 대한 설명을 하고자 한다.

2.2 주요 해킹 수법의 설명과 대책

○패킷 스니퍼링(Packet Sniffering)

누구나 쉽게 구할 수 있는 스니퍼는 LAN상

2) 미국 CIA, DOJ 홈페이 공격, 1996
3) 미국의 ISP 는 전자우편 공격으로 인터넷 서비스 중단으로 인한 피해가 매우 큰 시례가 있었음, 1996
4) 빌게이츠, 빌클린턴 등 사회정치적으로 유명인사에 대한 메일박스 공격, 1996
5) 크리스마스에 신용카드시스템을 공격 7 시간이나 정지시킨 사례, 1996
6) K대학 학부생의 인터넷 경유 홈뱅킹 시스템에 침입하여 불법 계좌이체를 시도, 1996
7) "정보시스템해킹현황 및 대응", 1996, 한국정보보호센터

표 4 해킹 수법의 분류 및 대책 요약

해킹 수법 분류	수법 설명	대표적인 수법	대책 요약
사 회 공 학	관리자를 속여 공격대상의 인증정보 등을 알아냄	전화 등을 통해 타인으로 위장 ID, 패스워드 알아냄	올바른 보안 정책과 방침 수립 운영
계 인 도 용	침입자가 정당한 사용자의 권한을 훔쳐 접근	-패킷 스니퍼 -패스워드 크랙	일회용패스워드, 새도우패스워드 등
신 뢰 성 위 장	정당한 호스트로 위장하여 인증없이 불법 접근	.rhosts, /etc/host.equiv 변조	시스템 변조 방지, 일일점검
취 약 성 공 격	운영체제, 응용프로그램 버그를 이용한 침입	sendmail, tftp, NFS, elm 등	버그 패치, 버전업, 올바른 시스템 구성
데 이 타 주 도 공 격	바이러스, 웜, 트로이목마 등 불법프로그램 이용	rootkit. Worm, AutoHack. ISS, SATAN 등	불법프로그램 감시, 불법 접근 차단
서 비 스 거 부 공 격	시스템의 정상적 서비스를 방해하는 공격	Mail Storm/Spam, Sync/Ping Flooding 등	불법 공격 감시 및 접속 끊기
구 조 적 문 제 공 격	시스템, 프로토콜의 구조적 결함을 이용한 공격	IP Spoofing	불법 공격 감시 및 접속 끊기

의 모든 패킷을 감시하고 유출할 수 있어 이를 이용하여 원격지 접속 시도시에 전달되는 사용자의 ID 와 패스워드를 알아낸다. 보통 이 프로그램은 정상적인 프로그램이름으로 설치되어 알아내기 어려우므로 LAN 인터페이스의 모드를 점검하여 스니퍼 설치 여부를 감지해내는 CPM 이라는 도구를 사용하여야 한다. 이 스니퍼의 공격을 차단하기 위해서는 일회용패스워드(One Time Password)를 사용하거나 통신중 암호화 전달하는 프로그램인 SSH("Secure Shell")이나 S-Telnet("Secure Telnet") 등을 사용하는 것이 좋다.

○sendmail 공격

전자우편 배달자 프로그램인 UNIX sendmail은 그 복잡한 구현과 setuid root 실행 모드로 인해 지금까지 수많은 버그들이 발표되었고 해커들이 손쉽게 이용하는 수법 중의 하나이다. 여기에는 패스워드를 크랙할 수 있도록 패스워드 파일을 카피하거나 root 쉘을 뺏는 버그들이 포함되어 있으며 버그가 패치된 최신 버전을 사용하는 것이 가장 바람직하다. 또한 root 실행이 아닌 일반권한으로 실행할 수 있는 방법들이 제공된다. smap 등과 같은 프락시를 이용하여 사용하는 것이 좋다.

○NFS 공격

NFS(Network File System) 공격은 주로 NFS 구성상의 문제로 인해 발생한다. /etc/exports 파일의 구성에서 자리수가 256자를 넘은 경우 누구나 그 시스템의 디스크를 마운트할 수 있으며, 쓰기 권한이 열린 경우라면 불법적으로 .rhosts를 만들거나 계정을 만들어 손쉽게 침입할 수 있게 된다. 정확한 NFS 구성을 하거나 NFS를 사용하지 않는 것이 좋다.

○IP Spoofing 공격

송수신자 간의 TCP 접속시 일어나는 3방향 접속(3 Way Handshake)시 필요한 순서번호(Sequence Number) 를 추측하여 불법접속을 만드는 방법이다. 이 방법은 현재까지

-Sequence number guessing
-SYN flooding
-Connection hijacking
-Connection killing by RST
-Connection killing by FIN
-SYN/RST generation
-killing the INETD
-TCP window spoofing

등으로 응용되어 TCP/IP 프로토콜의 기본 취약점을 공격해 왔는데, 일반적으로 IP spoofing이란 공격기법은 케빈미트닉이 사용한 방법을 의미하며 이 공격기법은 순서번호추측방식(Sequence Number Guessing) 기법이 함께 사용되는 고난도의 해킹기법을 말한다.

이 공격에 대해서는 방화벽 환경을 구성하여 패킷필터링시 외부에서 들어오는 패킷중에서

소스 IP의 주소가 내부망의 주소인 패킷을 걸러낼 수 있다. 이 경우에는 내부사용자의 내부 호스트에 대한 이러한 공격은 패킷 필터링으로 막을 수 없으므로 호스트 보안차원에서 TCP wapper의 설치와 rsh , rlogin 등의 인증없는 서비스를 사용치 않는 것이 요망된다. 그러나 여러종류의 IP spoofing은 TCP/IP의 설계 및 구현의 문제점에 기인한 것이므로 새로운 프로토콜을 사용하지 않는한 완벽한 보호대책은 어렵다. 다만 지속적인 보안관리 및 모니터링만이 최소한의 피해를 막을 수 있다고 할 수 있겠다.

○기타 수법

시스템 취약점 공격에 대한 대책은 주로 패치나 올바른 구성 및 운영을 통해 방지할 수 있으며 서비스거부 공격은 최근 나오는 경향이므로 3절에서 설명하고자 한다.

3. 최근 해킹 수법 동향과 대책

3.1 최근 해킹 수법 동향

앞절에서도 밝힌 바와 같이 해킹 수법은 점차 지능화·고도화·범죄화되고 있으며 시스템의 새로운 취약점들을 꾸준히 밝혀내고 분석해내고 있다. 미국의 CERT 팀을 위주로 공신력있는 기관에서는 매월 3, 4개씩의 취약점과 대책을 설명하는 권고문들을 발표하고 있으며 비공식기관이나 업체에서는 매주 3, 4개씩의 문제점들을 알아내고 있다. 여기에서는 주로 1996년도와 1997년도를 중심으로 해킹 수법 동향을 알아보기로 한다.

1996년과 1997년 미국 CERT의 동향요약을 보면 다음과 같은 해킹 경향을 보이고 있다.

- —NFS, NIS 취약점을 탐지하기 위해 자동탐색기(Scanning Tool)을 사용한다.
- —loadmodule과 rpc.ypupdate 를 이용하여 root 권한을 얻으려고 시도한다.
- —스니퍼, IP Spoofing 공격이 계속되고 있다.
- —sendmail 공격, 운영체제 상의 취약점을 지속적으로 시도한다.
- —리눅스 기계에 대한 공격이 많아지고, 메일폭탄공격이 나타나기 시작하고 있다.
- —WWW cgi-bin/phf 공격을 하고 있다.
- —서비스 거부 공격이 잦아지고 있다.

여기에서 WWW httpd, CGI 등의 취약점만을 살펴보고 주요 문제인 서비스거부공격에 대해 주로 알아 본다.

○WWW httpd, CGI 문제점

먼저 httpd nph-test-cgi 스크립트에서의 취약점[12]을 살펴보면, httpd에 포함되어 있는 nph-test-cgi 스크립트에서의 취약점 때문에 일반 사용자들이 볼 수 없도록 되어있는 파일목록을 볼 수 있게되는 문제점으로서 nph-test-cgi 스크립트는 웹서버의 환경에 대한 정보를 보여주도록 만들어 졌지만, 자료요구에 대해 너무 자세하게 보여주기 때문에 접근 권한에 상관없이 일반 사용자가 임의의 파일목록을 볼 수 있게 되는 것으로서 외부의 사용자가 시스템계정에 로긴하지 않고도 파일목록을 읽을 수 있다. 이를 방지하기 위해서는 nph-test-cgi 스크립트를 지우거나, 이 스크립트의 내용을 다음과 같이 수정한다.

```
echo QUERY-STRING = $QUERY-STRING
→echo QUERY-STRING = "$QUERY-STRING"
```

그밖에도 CA-96.06(Vulnerability in NCSA /Apache CGI example code, AUSCERT Advisory AA-96.01), 최근 발표된 SNI SA[8] (Vulnerabilities in the Apache httpd) httpd의 cookie 모듈의 취약점을 이용하여 원격지의 사용자가 시스템에 불법접근할 수 있도록 해준다.

3.2 서비스 거부공격과 대책

최근 한국정보보호센터에서는 해외에서 서비스거부공격 등에 의한 사이버테러 공격이 자주 나타남에 따라 특별보고서[9]를 만든바 있다. 여기에서 서비스거부공격 수법을 분류하고 해커들이 사용하는 주요 수법들에 대해 살펴보고자 한다.

8) Secure Networks Inc. 의 Security Advisory로서 1997년 1월 12일 발표됨, http : //www.certcc.or.kr/Advisory/etc/APACHE-MOD.advisory.1.13.97 참고

9) "서비스거부공격의 이해와 대책". 1997. 2, 한국정보보호센터

표 5 서비스거부공격 수법의 분류

공격근원	프로토콜	공격 대상 자원	공 격 수 법 명
내부 사용자의 공격	해당 없음	시스템	CPU 서비스거부공격
			메모리 서비스거부공격
			프로세스 서비스거부공격
			디스크 서비스거부공격
외부 사용자의 공격	TCP	응용프로그램·서비스	talk를 이용한 화면 서비스거부공격
			finger redirect 공격
			netcat을 이용한 공격
			DNS에 대한 공격
			syslog에 대한 공격
			linx를 이용한 httpd 공격
		네트워크·시스템	Inetd killing 공격
			Inetd Loop 공격
			TCP 접속 끊기 공격
			TCP window 크기 속이기 공격
			socket open/close flooding
			socket descriptor 과소비 공격
			SYN flooding 공격
	UDP	시스템	UDP bomb 공격
		네트워크·시스템	UDP flooding 공격
	ICMP	시스템	ICMP rediect 공격
		시스템	ICMP echo bomb 공격
		네트워크	ICMP bomb 공격
	SMTP	시스템	mail bomb 공격
			mail spam 공격

다음 표 5는 서비스거부공격들을 그 수법에 따라 분류하였는데, 시스템에 계정을 가지고 있는 내부 사용자가 공격할 수 있는 방법과 외부의 전산망 사용자가 공격할 수 있는 수법으로 크게 나누었고, 외부 전산망 사용자에 의한 공격은 공격에 이용하는 프로토콜에 의해 분류하여 보았다.

내부사용자에 의한 공격은 주로 시스템자원에 대한 공격으로서 시스템을 독점하여 과소비함으로써 서비스거부를 하게끔 하거나 과중한 서비스를 요청함으로써 일어난다. 여기에서는 네트워크 상에서의 주요 공격에 대해 알아 본다.

○ Finger Redirection 공격

fingerd 프로그램의 redirection 기능을 이용하여 공격자의 출발지 IP주소를 속여 서비스거부공격을 할 수 있는데, 다음을 보면,

```
% finger @system.two.com@system.one.com
[system.one.com]
[system.two.com]
Login   Name       TTY   Idle   When   Where
root    Operatior  p4    1      -- -   - -
```

finger는 system.one.com을 통하여 system.two.com으로 finger를 하게된다. system.two.com에서 보면 system.one.com이 finger하는 것 처럼되어 자신의 위치를 숨길 수가 있으며, 다음과 같이

```
% finger user@@@@@@@@@@@@@@@@
@@@@@@@@@host.we.attack
```

연속적인 "@" 표시는 host.we.attack을 계속하여 finger 하게 만들어 host.we.at tack 호스트가 in.fingerd 프로세스를 많이 만들어 내게 하여 네트워크서비스 부하를 높이는 finger bomb을 수행할 수 있다. tcpwrapper를 설치하여 finger 시도를 막거나, redirection을 제공하지 않는 fingerd 프로그램(GNU finger)를 사용하거나 inetd.conf 파일을 수정하여

finger 서비스를 제공하지않는다.

○ inetd 무한루프 공격

inetd 무한루프 공격은 SUN Solaris 시스템에서 inetd 구현상의 문제점에 기인한 것으로서 telnet 의 특정 포트에 접속한 후 "^]"를 연속적으로 반복하면 계속 inetd가 생성되고 결국 네트워크서비스가 느려지게 된다. 패치버젼을 가져다 설치해야 한다. 그밖에 리눅스에서는 inetd 프로세스를 불안전하게 하는 특정한 입력을 주어 프로세스를 정지시키기도 한다.

○ WWW 서버 공격

lynx를 이용하면 WWW 서버에 과도한 접속을 할 수 있으며 이를 이용하여 정상적인 WWW서비스를 방해할 수 있다. 네트워크 상의 공격을 모니터링하고 한 브라우저에서의 과도한 접속을 제한한다.

○ DNS 공격

도메인이름은 DNS-name-lookup( ) 함수를 통해 서버에 요청하므로 53번 포트에 계속적인 거짓 정보를 보내어 네임서버의 부하를 가중시키면 서버의 동작에 장애가 발생할 수 있으며, 임의의 도메인네임리스트를 만든 후 반복하여 질의함으로써 부하를 가중시키거나 53번 포트에 SYN Flooding 공격을 할 수 있다. 최신 DNS 버전을 패치하고, 네트워크의 상황을 모니터하여 탐지한다.

○ UDP Bomb 공격

UDP Bomb 공격은 정확하지 않은 UDP 헤더를 전송하여 목표 시스템을 reboot 시킬 수 있는데, 주로 SunOS 에서 나타날 수 있다. ip-options에 올바르지 않은 크기의 패킷을 넣어 보내게 되면 그 패킷을 받은 시스템의 동작이 정지되거나 재시동되는 것으로서 SUN 시스템의 패치로 설치하면 된다.

○ UDP 포트 서비스 거부 공격

간단한 출발지주소 spoofing을 이용하여 UDP를 이용하는 echo, time, daytime, chargen 등의 서비스들을 루프반복시켜 시스템의 부하를 크게 증가시킨다. 패킷의 내용에 상관없이 들어오는 패킷의 출발지 주소(Source Address)로 결과를 돌려주는 접속이 되면 서비스는 서로 패킷을 계속 주고 받아 서비스 거부를 일으키게된다. 그러므로 공격자는 출발지주소를 위장하여 공격대상 주소의 UDP 서비스 포트로 연결을 시도한다. 공격대상 호스트는 출발지주소의 호스트와 계속적으로 매우 많은 양의 패킷을 주고 받게 된다. 이 공격은 주로 chargen과 echo 서비스를 이용하므로 chargen, echo 서비스를 중지하거나 방화벽 또는 라우터에서 차단시킨다. 하지만 꼭 이러한 서비스를 이용해야하는 경우에는 방화벽 등에서 프락시를 사용하거나 echo, discard, chargen, daytime, time을 대신하는 riis 패키지[10] 사용하면 된다.

○ ICMP redirect 공격

특정 시스템에 ICMP redirect 패킷을 전송할 경우에 시스템이 정지하거나 재시동되는데, ICMP redirect 패킷은 일반적으로 라우터가 보내는 패킷으로서 호스트의 라우팅 테이블을 무효화 시키고 새로운 라우팅 경로를 알려주므로 공격자는 Paragon OS R1.4가 설치되어 있는 호스트에 ICMP redirect 패킷을 보내게 되면 운영체제의 구현상 문제로 인하여 이로한 취약점이 생기므로 라우터나 방화벽에서 ICMP 패킷을 막거나 패치된 운영체제를 설치한다.

○ ICMP bomb 공격

대상 시스템에 정당한 호스트로 가장한 ICMP Unreachable 패킷을 보내어 공격대상 호스트가 접속을 끊도록 만드는 공격으로서 라우터는 패킷이 목적호스트에 도착하지 못할 경우 상위 라우터에 ICMP Unreachable 패킷을 보내어 목적지로 접속이 불가능함을 됨을 이용하여 공격자는 대상시스템이 이미 가지고 있는 접속을 확인한 후 현재 접속한 클라이언트를 가장하여 공격대상 호스트에 ICMP Unreachable 패킷을 보낸다.

그 결과 공격대상 호스트는 ICMP Unreachable 패킷을 받고 클라이언트 호스트가 다운된 것으로 판단, 접속을 끊어버리게 된다. 라우터나 방화벽시스템에서 ICMP 패킷을 막아 공격에 대비한다.

---

10) tcp wrapper와 함께 사용할 수 있는 프로그램으로 상기 서비스들을 제공하면서 침입자의 공격시도(looping attack)를 막고 로그를 남길수 있는 프로그램이다. 이 프로그램은 다음에서 가져올 수 있다 : ftp : //ftp.fit.qut.edu.au/pub/security/riis.tar

○ ICMP ECHO Bomb 공격

이 공격은 인터넷상의 수많은 시스템에 대해 특정 크기의 ping을 목표 시스템에 보내는 것만으로 목표스템을 정지시키거나 재시동시킬 수 있는 공격으로서 수법이 매우 간단하며, 목표 시스템에 대해 IP 주소이외의 어떠한 정보도 알 필요가 없고, 다양한 시스템(모든 IP 장비)들이 공격에 취약할 수 있다는 점에서 매우 위험한 공격 방법이다. IP 환경의 모든 시스템과 장비들인 유닉스 시스템, NT 시스템, 네트웨어 시스템, TCP/IP를 사용하는 Windows 3.1 시스템, Windows '95 시스템, 침입차단시스템(Firewall), 라우터, 그리고 심지어는 네트워크 프린터에 이르는 모든 종류의 IP 장치들[11] 이 공격에 취약성을 가질 수 있다. 이 공격은 ICMP echo 패킷의 분해와 결합시 허용된 길이의 초과를 유도하고 재결합시 마지막 세그먼트를 오버플로우시키면 시스템에 따라 시스템 중단, 재시동, 커널 덤프 등 다양한 증상을 보이게 된다. 물론 대부분의 시스템에서는 이같은 패킷의 전송을 허용하지 않는다. 그러나 사용자는 자신이 수정한 버전의 프로그램과 커널을 사용할 수도 있으며, Windows '95나 Windows NT에서도 이러한 환경을 만들어 공격할 수 있다.

이 공격에 대한 해결책은 각 업체들이 제공하는 패치(patch)를 설치하는 방법 뿐이며, 그러나 패치를 구할 수 없는 시스템들에 대해서는 우선 라우터, TCPwrapper)나, 방화벽에서 ICMP echo를 차단하여 막을 수 있다.

○ Mail bomb 공격

대량의 전자우편을 임의의 수신자에게 보내 시스템의 전자우편 수신스풀(Spool)디스크를 모두 사용하게 함으로써 시스템을 정지시키는 공격으로서 임의의 사용자에게 다량의 메일을 한꺼번에 보낼 때 voodoo(unix), Upyours(pc)등의 프로그램을 사용하여 송신자의 전자우편주소를 속여 보낼 수 있다. 그리고 또한 대상 수신자의 전자우편 주소를 많은 수의 전자우편그룹(Mailing List)에 가입시킴으로써 많은 량의 메일을 받아보게할 수 있다. 이를 막기위해서는 시스템차원에서 특정사이트(불필요한 메일을 보내는 사이트)에서의 SMTP 포트의 사용을 막는 방법과 사용자 자신이 전자우편 수신시 필터링하는 방법이있다.

4. 해킹 방지 연구 개발 및 동향

4.1 국외 동향

해외에서는 해킹방지를 위한 연구개발과 관련제품들 중 전산망방화벽시스템(Firewall)에 대한 투자가 가장 많은 것으로 파악될 수 있다. 해킹방지에 직접관련되는 제품 분류들을 표 6에서 보이고 있다.

표 6 해킹 방지 관련 기술 분류

해킹 방지 관련 기술 분류	설 명	대표적 유관제품·활동 등
전산망방화벽	전산망 불법침입 방지	Firewall 시스템 다수
바이러스방지	바이러스 침투방지·예방	바이러스 백신, 스캐너
침입탐지기술	침입 실시간 확인	IDES, RealSecure, NetStalker 등
접근제어기술	사용자와 자원간 통제	Multilevel Secure OS
향상된 사용자 인증기술	강력한 사용자 신분 인증	SecureID(One Time Password)
취약성 점검·관리기술	취약점 점검·분석·관리	ISS Suite, SATAN, OmiGuard등
로그·감사평가	시스템 부당 사건 감시 등	Tripwire, MD5, …
보안 컨설팅	보안성 진단, 설계	CSI, NCSA, SRI 등
침입자 분석, 추적, 지원	침입흔적 분석, 추적 지원	CERT, CIAC, ASSIST 등

11) 이 취약성을 가질 수 있는 시스템들에 대한 상세한 목록은 다음의 문서를 참조하기 바란다 : http : //prospect.epresence.com/ping/index.html

4.2 국내 동향

국내에서 해킹방지 및 예방 관련 기술력은 그다지 높지 않고 지금까지의 연구개발도 미미

한 상태이므로 많은 분야에 대한 연구개발이 요구된다고 하겠다. 실제 해킹 사건을 겪으면서 CERT 활동이 일부 시작되었으며, 포항공대, SERI, 한국전산원 등에서의 연구개발이 일부 이루어졌다.

최근 한국정보보호센터에서는 그림 1에서 보이는 바와 같이 SecureDR 라는 프로그램의 개발과 보급을 통해 유닉스시스템의 보안 취약점들을 점검분석해낼 수 있는 제품을 개발하였으며, 한국정보보호센터의 CERTCC-KR 홈페이지를 통해 직접 온라인으로 자신의 취약점을 점검보고 받을 수 있는 그림 2와 같은 원격지 점검프로그램을 개발했다.

그림 1 전산망안전진단소프트웨어(Secure DR) 초기화면

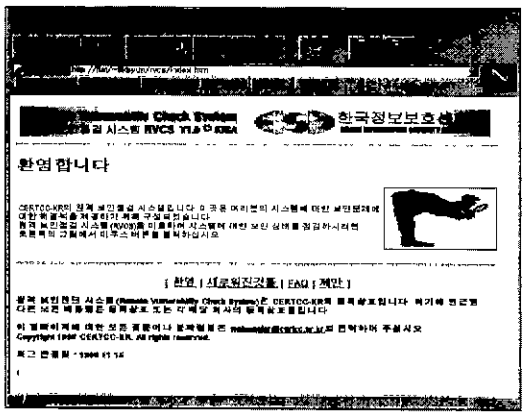

그림 2 원격보안진단시스템(RVCS) 초기화면

5. 결 론

현재 국내의 인터넷 등 전산망에서는 해킹 사건들이 끊임없이 발생하고 있으나 시스템관리자가 이를 간과하고 지나치거나 탐지하고도 보고하지 않는 경우가 허다한 것으로 보인다. 최근에도 해킹 사건이 지속적으로 발생하고 있는데, 국내 해커에 대한 대비책 뿐만 아니라 해외의 지능적 해커들의 불법침입이 매우 우려되므로 국내 통신망사업자, 기업 등에서 정보보호를 위해 많은 노력을 기울여야 할 때이다.

최근 국내에서의 전산망 해킹방지 관련 제품 동향은 주로 전산망 방화벽시스템의 보급과 연구개발에 초점이 맞추어져 있으며 해킹 방지와 직접적인 관련이 있지는 않지만 전산망을 이용한 온라인 상거래시스템의 연구개발도 많이 이루어지고 있지만 실질적인 시스템 침입방지를 위한 각종 연구개발과 제품의 발표는 매우 미흡한 것으로 보이므로 많은 국내 연구진들이 이 해킹방지기술분야에 대해 관심을 가져주길 바란다.

참고문헌

[1] 한국정보보호센터, "정보시스템 해킹 현황 및 대응", 1996.
[2] 한국정보보호센터, "정보보호현황", 1996
[3] 한국정보보호센터, "Firewall 시스템 총서", 1996.
[4] 한국정보보호센터, "온라인원격지보안분석 및 진단도구 개발", 1996.
[5] 한국정보보호센터, "정보보호총서", 1996
[6] Larry J. Hughes, Jr. "Actually Useful Internet Security Techniques", New Riders, 1995.
[7] Karanjit Siyan, "Internet FIrewalls and Network Security" New Riders, 1995.
[8] Larry J. Hughes et al., "Implementing Internet Security" New Riders, 1995.
[9] Garfinkel & Spafford, "Practical UNIX & Internet Security", 2nd Ed, O' Reilly Association, 1996.
[10] Hans Husman, "Introduction to Denial of Service", Feb 9, 1997.
[11] Bugtraq Mailing list archive http : // geek-girl.com/bugtraq/.

[12] ISS vulnerablity database http : // www.iss.net.
[13] Cert Summary ftp : //info.cert.org/ pub/cert-summaries/.
[14] Matt Bishop "UNIX Security Threats and Solutions" NETWORK '96, Nov 4, 1996.
[15] AUSCERT Advisory http : //www.auscert.org.
[16] CERT Advisory ftp : //info.cert.org/ pub/cert-advisories/.
[17] RSA OEM Product Lists, http : // www.rsa.com.
[18] Defense Science Board, "Report of the Defense Science Board Task Force on Information Warfare -Defense", Nov. 1996.
[19] William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addision-Wesley, 1994.
[20] Marcus J. Ranum, "A Taxonomy of Internet Attacks : You Can Expect", 1995.
[21] CERTCC-KR-TR-97001, "전산망 해킹 침해사고시 어떻게 처리하나", 1997-01-31.
[22] Dan Farmer, '시스템공격점검을 통한 보안 개선 방안", 1995.

신 훈

1992 한국항공대학교 전자계산학과 학사
1995 서강대학교 전자계산학과 석사
1995～1996 국방정보체계연구소 연구원
1996～현재 한국정보보호센터 기술대응팀 주임연구원

임 휘 성

1985 연세대학교 공과대학 전자공학과 학사
1987 연세대학교 공과대학 전자공학과 석사
1992～1996 한국 아이비엠 소프트웨이 연구소
1996～현재 한국정보보호센터 기술대응팀 선임연구원

임 채 호

1986 홍익대학교 전자계산학과 학사
1986～1991 시스템공학연구소 선임연구원
1991～1994 대전실업전문대학 교수
1990 건국대학교 전자계산학과 석사
1995 시스템공학연구소 초빙연구원
1996～현재 한국정보보호센터 기술대응팀 책임연구원