보안 취약성 점검을 위한 전산망 안전진단 소프트웨어의 개발

홍기융, 박정호, 김병천, °김기현, 정현철, 이홍섭
한국정보보호센터

The Development of SecuDr for Automatic Diagnosis of Security Vulnerabilities in Computer & Network Systems

K. Y. Hong, C. H. Park, B. C. Kim, °K. H. Kim, H. C. Jung, H. S. Lee
Korea Information Security Agency

요약문

인터넷 및 정보통신망의 기술 추세에 편승하여 국·내외적으로 전산망 해킹과 역기능은 국가·사회적으로 매우 심각한 문제로 인식되고 있다. 국내의 경우 전산망 시스템 관리자 및 사용자의 부주의에 의한 전산망 보안 취약성이 해킹의 많은 원인을 제공하고 있는 실정이다. 또한 국제적으로 많은 보안도구들이 개발되어 있으나 국내의 경우 보급·운영되고 있는 국산주전산기에 대한 보안도구들의 호환성이 검증되지 않아 실무 적용에 어려움이 많다. 따라서 본 논문에서는 빈번하게 발생한 해킹 사례를 중심으로 시스템 관리자가 전산망 시스템 보안 문제점을 점검하고 조치할 수 있도록 하는 전산망 안전진단 소프트웨어 SecuDr를 소개한다. 개발된 SecuDr는 국산 주전산기인 타이컴 및 톨러런트와 UNIX를 운영체제로 하는 SUN, HP, IBM 등에서 동작가능하다.

Ⅰ. 서론

전세계는 정보화의 추진으로 인하여 문명의 발전을 거듭하고 있는 반면에 각종 역기능적인 측면 또한 증가 일로에 있다. 국내외적으로 인터넷을 기반으로 하는 각종 통신망의 상호연결은 물론 초고속정보통신망의 확충등 정보 통신기술의 급속한 발전으로 고도 정보사회로 진전하면서 개인정보 누설, 전산망 해킹 등과 같은 역기능 현상이 국가·사회적으로 매우 심각한 문제점으로 등장하고 있다.

국내에서 발생한 해킹 사례는 단순 침입, ID 도용, 자료 절취, 자료 변조 및 파괴 등이 있으며 시스템 관리자 및 사용자의 관리 부주의에 의한 보안 문제점들이 많은 원인을 제공한다. 외국의 해킹 실태는 국내에 비해 매우 심각한 실정이다[1]. 국가 중요 정보를 적국에 유출시켜서 안보상 큰 위협을 초래한 사례도 있으며 고도의 침해기술로 산업 정보를 유출하거나 개인정보를 침해하는 등의 사례로 인하여 각국은 매우 심각하게 대처하고 있는 실정이다. 특히, 외국의 해커가 타국의 전산망을 해킹하기 위하여 국내의 전산망을 중간 경유지로 선택하는 사례가 빈번해질 가능성이 있으므로 인터넷 해킹에 대한 대비책을 강구 후 접속·사용하여야 한다[1, 2, 3, 4].

해킹을 방지하기 위하여 인터넷상에는 COPS(Computer Oracle and Password System)[5], ISS (Internet Security Scanner)[6], SATAN(Security Administrator Tool for Analyzing Networks)[7] 등 많은 시스템 취약성 분석도구들이 있으나 국내 전산망 시스템 관리자의 경우 이들 보안 취약성 분석도구들에 대한 이해가 미비하거나 올바른 조치사항을 알지못해 취약성을 가진 시스템을 그대로 운영하고 있는 경우가 많다[2, 3, 4].

따라서 본 논문에서는 국내에서 발생한 해킹 사례가 더 이상 발생하지 않도록 하기 위하여 시스템에 내재된 보안 문제점을 점검하여 사전에 예방적인 조치사항을 취할 수 있도록 하는 전산망 안전진단 소프트웨어 SecuDr를 소개한다. 전산망 안전진단 소프트웨어를 개발하기 위하여 먼저 국내외 전산망 보안 및 해킹 실태를 분석하고 현재 개발된 관련 보안도구들을 고찰하여 국내에 우선적으로 필요한 보안기능 중심으로 전산망 안전진단 소프트웨어 개발 모델을 설정하였다.

개발된 SecuDr 소프트웨어는 국내에서 주로 운영되고 있는 타이컴, 톨러런트와 같은 국산 주전산기와 SUN, HP, IBM과 같은 UNIX 시스템의 운영체제별로 동작가능토록 구현하였다.

Ⅱ. 국내외 전산망 보안 및 해킹 실태 분석

1. 국내 전산망 해킹 및 역기능 실태

그 동안 국내에서 발생한 해킹사례의 대부분은 상용통신망에서 타인의 ID를 도용하거나 이들 업체를 해킹한 경우, 그리고 대학이나 연구소 등을 해킹하는 것이 주류를 이루고 있으며 대부분의 해커는 교육 수준이 낮으면서 컴퓨터에 집착·몰두한 10대~20대 청소년이나 호기심 많은 학생들에 의하여 행해지는 등 기술적 또는 동기면에서 볼 때는 다분히 단순 해커의 수준인 것으로 나타났다. 그러나 '95년 말 이후 '96년 초에 이르면서 악의성이 내재된 해킹 사례가 점차적으로 빈번해지고 있으며 현행 실정법에 의하여 처벌받을 수 있다는 사실을 모르고 있는 경향이 있는 등 범죄의식 또한 결여된 것으로 드러났다. 특히, 그동안 해킹 방지 기술을 연구하기 위한 대학내 동아리 활동으로 인식되어 왔던 학생들에 의하여 경쟁적이라 느껴질 정도의 해킹 행위가 이루어 진 것을 고려할 때 해커 및 해킹 행위에 대한 전반적인 점검이 필요한 때라고 느껴진다. 그동안 국내에서 발생한 대표적인 해킹 행위는 주로 단순 침입, ID 도용, 자료 절취, 자료 변조 및 파괴 등이었고 '95년 및 '96년에 발생한 해킹 사례를 살펴보면 다음과 같다.

가. '95년 해킹 사례 분석

'95년 한해 동안에 발생한 해킹 사례는 [표 1]과 같이 총 17건으로 대학·연구전산망 침입, PC 통신망 ID 도용 및 사기, 암호해독 등이다[1].

[표 1] '95년 국내 해킹 사례

일 자	사 례
'95. 1. 10.	홈뱅킹 이용 타인 예금 인출
'95. 2. 22.	대학 전산망에 해커 침입
'95. 3. 14.	모회사 제품 워드프로세서의 암호 해독
'95. 4. 8.	고교생이 ID 도용하여 사기 행위
'95. 4. 9.	PC 통신 ID 도둑 극성
'95. 6. 2.	고교생이 PC 통신으로 사기 행위
'95. 8. 7.	모대학 전산원 호스트 해킹
'95. 8. 9.	노래방 프로그램 암호 해독
'95. 8. 9.	외국 해커가 연구소 침입
'95. 8. 9.	모기업체 전산망 해킹 당함
'95. 8. 19.	통신 서비스 업체에 해커 침입
'95. 8. 20.	은행 신용카드의 비밀 암호체계 해독
'95. 9. 12.	상용 통신망에 해커 침입
'95. 9. 24.	교육 전산망 해킹한 해커 검거
'95. 10. 3.	삐삐 비밀번호 해킹
'95. 10. 12.	대학, 연구소 침투한 해커 검거
'95. 11. 18.	타인의 ID 도용하여 은행 서비스를 받음
총 계	17 건

이와 같이 '95년 분기별 해킹 사례를 살펴보면 3건(1/4분기), 3건(2/4분기), 8건(3/4분기), 3건(4/4분기)으로 학생들의 방학 및 휴가철이 포함된 3/4, 4/4분기에 발생빈도가 높은 것으로 나타나고 있다.

나. '96년 해킹 및 역기능 사례 분석

'96년(10월 현재)에 발생한 주요 해킹 및 역기능 사례는 [표 2]와 같이 총 9건으로 시스템에 직접적으로 피해를 입히는 등 악의적 해킹 사례가 증가하는 추세를 나타내고 있다[1].

[표 2] '96년 국내 해킹 및 역기능 사례

일 자	사 례
'96. 2. 1.	X통신업체 및 Y대학 해킹 당함
'96. 4. 16.	N기관 인터넷 해킹 : 비밀번호 파일 유출 (tftp의 사용으로 인함)
'96. 4. 19.	20대 국제해커 첫 적발 (일본 외무성등 세계 92곳 전산망 침투)
'96. 4. 26.	홈뱅킹·폰뱅킹 사고 (비밀번호 보안 허술)
'96. 4. 30.	개인 신상정보와 기업체 금융 거래 내역이 담긴 전산출력지 유출
'96. 5. 8.	K대학 학생에 의한 P대학 시스템 해킹
'96. 5. 21.	컴퓨터 조작 운전면허 부정 발급
'96. 6. 3.	인터넷에 북한 홈페이지 등장
'96. 9. 25.	K대학 학생 홈뱅킹 사기
총 계	9 건

'96년 분기별 해킹 사례를 살펴보면 1건(1/4분기), 7건(2/4분기), 1건(3/4분기)으로 향후 지속적으로 발생빈도가 높아질 것으로 우려된다.

2. 국외 전산망 해킹 실태

외국의 해킹 실태는 국내에 비하여 매우 심각한 실정이다. 국가 중요 정보를 적국에 유출시켜서 안보상 큰 위협을 초래한 사례도 있으며 고도의 침해기술로 산업정보를 유출하거나 개인정보를 침해하는 등의 사례로 인하여 각국은 매우 심각하게 대처하고 있는 실정이다. 최근에는 인터넷상에서의 해킹기술도 점차 고수준에 달하고 있어 인터넷 접속에 대한 각별한 보안 관리가 요구된다. 특히, 외국의 해커가 타국의 전산망을 해킹하기 위하여 국내의 전산망을 중간 경유지로 선택하는 사례가 빈번해질 가능성이 있으므로 인터넷 해킹에 대한 대비책을 강구한 후 접속·사용하여야 한다. 다음의 [표 3]에서는 국외 전산망 해킹 기술 및 방지 대책을 요약 제시하고 있다[1]

Ⅲ. 보안 도구

시스템 및 네트워크의 보안 취약성을 점검하고 보안수준을 높이기 위하여 사용되는 보안 도구들이 인터넷 상에 많이 공개되어 있다. 이 보안도구들은 그 기능에 따라 시스템에 대한 접근을 기록·제어하는 보안도구, 패스워드 파일의 보안관련도구, 시스템 내부 보안 점검도구, 원격 시스템의 보안 점검도구 등이 있다[2]. 그러나, 이러한 보안 도구들이 모든 보안 취약성을 점검해 주지 못하기 때문에 여러 도구들을 복합적으로 사용하는 것이 바람직하다.

[표 3] 국외 전산망 해킹 기술 및 방지 대책

전산망 해킹 기법	해킹 방지 대책
1. 패스워드 파일 불법 복제 및 유포, 해독(Cracking)	o Shadow 패스워드 파일 기법 o 랜덤 패스워드 사용
2. 패스워드 재시도 공격	o 시도횟수 제한 로그인 시스템 o 패스워드 Aging Scheme o One-Time Password o Challenge-Response Scheme
3. 트로이목마	o 시스템 실행 파일 점검 o Integrity 검증
4. 컴파일러(Compiler)에 의한 불법 명령어 삽입	o Certified Compiler S/W Installation
5. 프로토콜의 취약성을 이용한 신분위장 및 메시지 위조	o Version Up (Security Enhanced Version) S/W o PGP o PEM
6. tftp 프로토콜의 취약성을 이용한 비밀 파일의 불법 복제	o Secure Mode, tftp/tftpd 제거
7. 스니퍼(Sniffer)에 의한 패스워드 비밀성 침해	o 패스워드를 암호화하여 전송 o One-Time Password o Challenge-Response Scheme
8. 가로채기(Interception) 및 재전송(Replay)	o Timestamp 기법을 적용
9. 스푸핑(Spoofing)	o One-Time Password o Challenge-Response Scheme o Digital Signature o Secure Gateway
10. 비밀채널(Covert Channel)을 이용한 불법 정보 유출	o B2급 이상의 Secure System o Covert Channel 제거 기술 o Covert Channel 성능 제한 기술
11. Cascade 취약성을 이용한 불법 정보 유출	o Cascade Detection 기술 o Cascade Prevention 기술 o Cascade Correction 기술

1. COPS

COPS는 1991년 11월 Dan Farmer에 의해 만들어진 것으로 주목적은 보안 문제를 점검하고 제거하는 것이다. 시스템 관리자에게 침투자나 또는 바이러스 등에 대한 경보기능을 제공한다. COPS 소프트웨어 패키지는 UNIX 보안 영역에서 발생 가능한 문제점들을 각각 점검 확인하는 프로그램들로 구성된다. COPS가 점검하는 부분은 다음과 같다[1, 5]

- 파일, 디렉토리, 디바이스 등에 대한 접근허가권한
- 예측하기 쉬운 패스워드
- 패스워드 파일이나 그룹 파일에 대한 내용과 형식
- /etc/rc와 crontab에 의하여 실행되는 프로그램
- root-SUID 파일들의 존재여부와 그 파일들에 대한 기록권한 점검
- 중요한 파일들에 대한 CRC 점검
- 사용자들의 홈디렉토리와 주요 파일(.profile, .cshrc 등)에 대한 기록권한 점검

- anonymous ftp 점검
- 그 밖에 /etc/hosts.equiv 파일에 있는 '+'나 제한되지 않은 NFS export 등

2. ISS

ISS는 1993년 9월 Cristopher Klaus에 의해 작성된 것으로 원격 시스템에 대한 취약성을 점검하는 도구이다. 이 ISS는 시스템에 대하여 보안성을 다단계로 시험하는 기능을 가지고 있으며 보안 기능이 잘못 구성된 부분을 바로잡을 수 있도록 시스템 관리자에게 정보를 제공한다. ISS는 공개된 최초의 다단계 보안 스캐너(Multilevel Security Scanner)로 많은 UNIX 시스템상에서 쉽게 설치되고 호환성이 있도록 설계된 것이다. 실제로 인터넷 도메인에서 보안 기능이 잘못 구성된 많은 예가 제시되고 있으며 이러한 보안 허점들은 대부분 CERT나 CIAC advisories를 통하여 공표되었다. 이 ISS는 앞으로 많은 보완이 뒤따라야 할 것으로 보인다. ISS는 사용자나 관리자의 실수로 잘못 설정된 중요 파일들을 조사하여 그 이상여부를 알려준다. ISS는 자신의 계정이 없는 다른 시스템의 보안을 조사하는데 목적이 있는 것이 아니라, 자신의 시스템이 자신의 시스템에 계정이 없는 사람으로부터의 공격을 막을 수 있도록 도와주는데 그 목적이 있다. ISS의 주요 기능은 다음과 같다[1, 3, 6].

- guest, bbs, lp 등과 같은 필요없는 계정의 유무를 점검
- 각종 프로그램의 알려진 버그들을 점검
- NFS상에 export된 파일들의 제한사항을 점검
- 현재 사용중인 사용자들의 점검 등

3. SATAN

SATAN은 Dan Former와 Wietse Venema에 의하여 만들어진 것으로 1995년 4월에 최신 버전이 공개된 바 있다. 이 SATAN은 원격 시스템의 보안 취약성을 분석하는 툴이다. SATAN은 발견된 보안 취약성을 시스템 관리자에게 보고한다. SATAN이 실행되기 위해서는 Perl5 또는 그 이상, Netscape나 Mosaic과 같은 Web browser, UNIX 윈도우 환경을 요구한다.

이와 같은 SATAN의 핵심부는 추론 엔진(Inference Engine) 모듈이며 이 추론 엔진 모듈은 규칙 기반들로 구성된다. SATAN으로 부터의 공격을 막기 위하여 첫째로는 시스템을 정확하게 설치·구성하고, 둘째로는 모든 최신 patches를 설치하고, 셋째로는 시스템 사용을 모니터링하는 것이다. 이러한 방법을 통하여 SATAN을 이용한 공격으로부터 방어할 수 있다. 그러나, 불행하게도 SATAN의 공격을 완벽하게 막는 것은 어려운 것이 사실이다. SATAN의 주요 점검 항목은 다음과 같다[1, 3, 7].

- FTP 취약성
- 권한이 주어지지 않은 NFS 파일시스템 export(접근통제를 점검)
- portmap을 통한 NFS의 export(현재 export되어서 사용중인 호스트 점검)
- NIS의 패스워드 파일 접근
- REXD 액세스
- Sendmail 취약성
- TFTP를 이용한 비인가 파일 접근
- r-shell을 이용한 비인가 접근
- 제한이 없는 X 서버로의 접근
- 제한받지 않은 모델
- 쓰기권한이 있는 FTP의 홈 디렉토리

4. 기타 보안 소프트웨어 툴

위에서 언급한 COPS, ISS, SATAN 외에 TCP_Wrapper, Tiger, Crack. 등 많은 보안 소프트웨어 도구들이 있으며 [표 4]에서 이들 기타 보안 소프트웨어 도구들을 비교하였다.

[표 4] 기타 보안 소프트웨어 도구 비교

소프트웨어	기 능		
	예방	탐지(검색)	추적 및 복구(치료)
arpwatch		○	○
cops	○	○	
courtney		○	○
crack	○	○	
cracklib	○		
deslogin	○		
iss	○		
ipacl	○		
kerberos	○		
netlog		○	○
pgp	○		
pipem	○		
satan	○		
securscan	○		
tcpdump		○	○
tcpwrapper	○		○
tiger	○	○	○
tis	○	○	○
tripwire	○	○	○
traceroute			○
xinetd	○	○	○

< ○ : 기능이 있음을 나타냄 >

Ⅳ. 전산망 안전진단 소프트웨어 개발

1. 전산망 안전진단 소프트웨어의 모듈 설정

전산망 안전진단 소프트웨어는 전산망 해킹 및 컴퓨터 범죄 예방을 목적으로 UNIX 운영체제를 기반으로하는 워크스테이션급 이상의 중대형 컴퓨터 시스템에 대한 보안 취약성 분석 및 안전진단을 실행하도록 설계되었다.

전산망 안전진단 소프트웨어의 기능 모듈의 설정은 파일 및 디렉토리의 접근권한, setuid, setgid, 트로이목마 프로그램의 설치 등 시스템내의 보안 취약성 점검에 근간을 두었으며 패스워드 크래킹, 부팅 패스워드 변경, 단순파일전송프로토콜 공격 등 국내에서 발생한 해킹 사례를 중심으로 시스템 보안 점검 기능을 추가하였다. [표 5]는 전산망 안전진단 소프트웨어에서 설정한 기능 모듈을 나타내고 있다.

[표 5] 소프트웨어의 기능 설정

구 분	보안 취약성
국내 전산망 해킹 사례 분석	취약한 패스워드를 추정 시스템 부팅 패스워드를 설정 루트 권한 도용 단순파일전송프로토콜
시스템내의 보안 취약성 분석	파일, 디렉토리 접근 권한 setuid와 setgid 설정 파일전송프로토콜의 환경 설정 트로이 목마 프로그램의 설치

[표 5]에서 설정한 보안 취약성을 점검하기 위하여 그 특성에 따라 패스워드, 통신 프로토콜, 사용자, 그리고 시스템 관련 취약성 점검 기능으로 구분하였으며 [표 6]과 같이 세부적으로 10가지 기능의 안전진단 프로그램으로 구성하였다.

[표 6] 전산망 안전진단 소프트웨어의 기능 분류

구 분	기 능
패스워드 관련	• 패스워드 취약성 분석 및 점검 • 시스템 부팅 패스워드 점검 • 패스워드 파일 취약성 점검
통신프로토콜 관련	• 파일전송프로토콜 점검 • 단순파일전송프로토콜 점검
사용자 관련	• 사용자 홈 디렉토리 점검 • 사용자 홈 디렉토리내의 중요 파일 점검 • 사용자 그룹 점검
시스템 관련	• 시스템 관리자 환경 점검 • 시스템 관리자 권한으로 동작하는 프로그램 점검

2. 소프트웨어의 기능

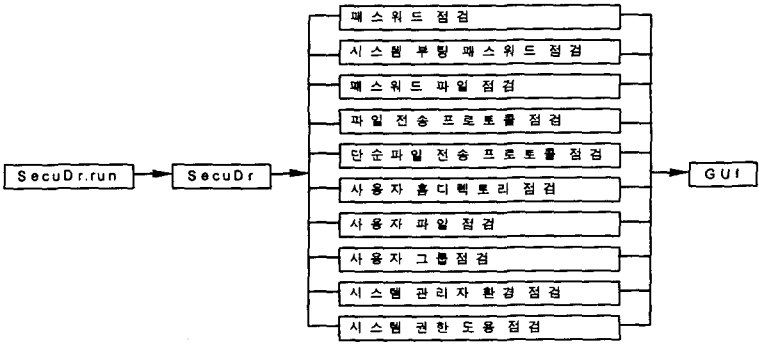
위에서 설정한 10가지 시스템 취약성 점검 기능을 수행하기 위하여 다음과 같이 세부 점검 항목을 설정하였다. 첫째, 패스워드 취약성 분석 및 점검에서는 패스워드가 없는 ID와 쉽게 추정이 가능한 패스워드를 점검한다. 둘째, 시스템 부팅 패스워드 점검에서는 시스템 부팅 패스워드가 설정되어 있는지를 점검한다. 셋째, 패스워드 파일 점검에서는 공백라인(blank line), 각 라인의 필드 수 오류, 패스워드 없는 ID, 중복된 ID, 영문자와 숫자 이외의 문자로 등록된 ID, 숫자로 되어 있지 않은 UID/GID, 루트가 아니면서 UID가 0인 ID, 그리고 잘못된 로그인 디렉토리를 점검한다. 넷째, 파일전송 프로토콜 점검에서는 /etc/ftpusers 파일, /etc/passwd 파일, ftp ID 의 홈디렉토리하의 ~ftp/etc/passwd 및 ~ftp/etc/group 파일과 루트의 해당 파일(/etc/passwd, /etc/group)과의 내용중복, 그리고 ftp 관련 중요 파일 및 디렉토리 접근허용모드를 점검한다. 다섯째, 단순파일전송프로토콜 점검에서는 단순파일전송프로토콜 서비스의 제공 여부를 점검한다. 여섯째, 사용자 홈 디렉토리 점검에서는 사용자 홈디렉토리가 디렉토리 모드인지 여부와 사용자 홈디렉토리의 접근허용 모드인지를 점검한다. 일곱째, 사용자 파일 점검에서는 사용자 홈디렉토리 내의 중요 파일(.rhosts, .profile, .login 등)의 접근허용모드를 점검한다. 여덟째, 사용자 그룹 파일 점검에서는 공백라인, 각 라인의 필드수 오류, 중복된 그룹, 영문자와 숫자 이외의 문자로 등록된 그룹, 그리고 숫자로 되어 있지 않은 그룹 ID를 점검한다. 아홉째, 시스템 관리자 환경 점검에서는 루트의 startup file(/.login, /.cshrc, /.profile 등)의 접근허용모드, 부적당한 umask의 설정, /.rhosts 파일에 루트가 아닌 entry의 존재 여부, /etc/hosts.equiv 파일내에 "+", 그리고 /bin, /etc 등 중요 디렉토리 및 파일이 루트 소유로 되어 있는지를 점검한다. 마지막으로 시스템 관리자 권한도용 점검에서는 setuid 및 setgid 설정 실행 파일들을 점검한다.

3. 소프트웨어의 개발

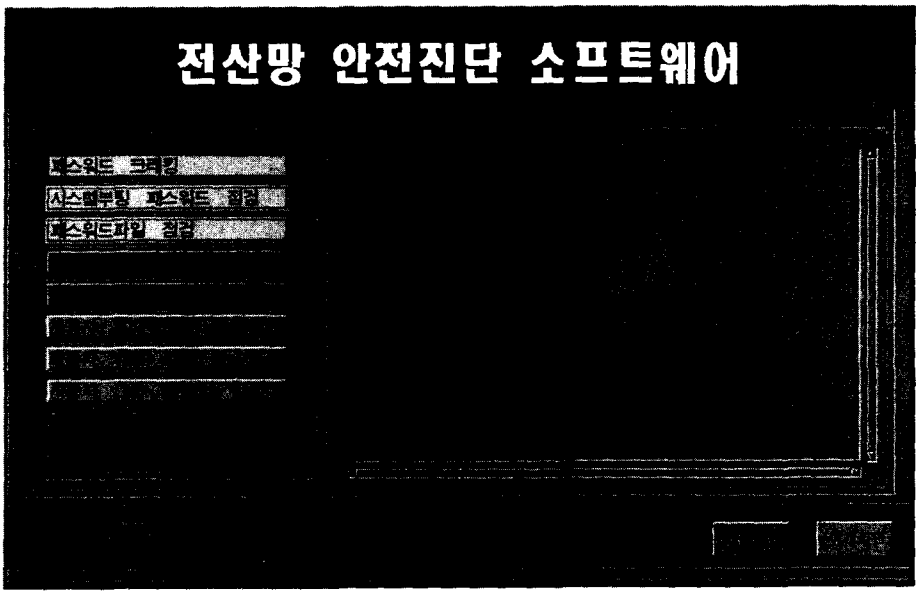
전산망 안전진단 소프트웨어는 UNIX 시스템 및 인터넷 보안취약성을 점검하기 위하여 개발하였으며 개발환경은 다음과 같다.

- 운영체제(O.S) : UNIX
- 하드웨어 : 워크스테이션급 이상의 중대형 컴퓨터시스템
- 쉘 명령어 환경 : C 쉘 또는 Bourne 쉘
- 프로그래밍 언어 : C 언어

전산망 안전진단 소프트웨어는 국내 전산망 환경을 고려하여 텍스트 모드와 윈도우 모드로 개발하였으며 (그림 1)에서는 윈도우 모드에서 소프트웨어의 동작 과정을 나타내고 있다. 먼저 텍스트 모드의 경우 사용자가 SecuDr.run을 수행하면 실제로 내부에서는 SecuDr 프로그램이 동작하며 SecuDr 프로그램은 총 10개의 모듈이 순서대로 진행되며 각 모듈별로 독립적으로 실행할 수도 있다. 원도우 모드일 경우 SecuDr.run을 수행하면 (그림 2)와 같이 안전진단 소프트웨어 화면을 구동하며 "안전진단 기능 선택" 항목을 선택하므로써 해당 기능 진단을 시작한다. 진단결과는 진단 결과 표시창(□)에 색깔별로 출력되며 세부내용 및 조치사항은 "안전진단 실행결과 메세지" 창에 한글로 출력된다.



(그림 1) 소프트웨어의 동작



(그림 2) 소프트웨어 동작화면

4. 호환성 시험

국내 전산망은 타이컴, 톨러런트 등 국산주전산기와 SUN, HP, IBM 등 다양한 UNIX 시스템으로 구성되어 있다. 본 논문에서는 개발한 전산망 안전진단 소프트웨어를 국산주전산기와 각종 UNIX 시스템에서 그 호환성을 검증하여 시스템 관리자들이 실무에 적용할 수 있도록 하였다. 개발한 전산망 안전진단 소프트웨어는 다음과 같은 UNIX 운영체제에서 호환성을 시험하였다.

- SUN OS 4.1.1
- SUN OS 4.1.3
- SUN Solaris 2.4
- SUN Solaris 2.5
- HP-UX 9.x
- HP-UX 10.x
- IBM AIX
- 주전산기 I(툴러런트) TX
- 주전산기 II(타이컴) UNIX SVR 3.2
- 주전산기 II(타이컴) UNIX SVR 4.2

5. 전산망 안전진단 소프트웨어의 기능 분석 및 비교

본 논문에서 개발한 전산망 안전진단 소프트웨어와 COPS, ISS, SATAN의 기능을 비교하면 [표 7]과 같다[1].

[표 7] COPS, ISS, SATAN, 및 전산망 안전진단 S/W의 비교

구 분		COPS	ISS	SATAN	SecuDr
1. Permission (write ability) 점검		○			○
2. /etc/rc* cron(tab) 점검		○			
3. CRC 점검		○			
4. .profile .cshrc 점검		○			○
5. /etc/passwd 점검		○			○
6. /etc/shadow 점검					○
7. /etc/group 점검		○			○
8. 패스워드 크래킹		○			○
9. 부팅 패스워드 점검					○
10. Anonymous FTP		○	○	○	○
11. Unrestricted TFTP		○		○	○
12. Miscellaneous root 점검		○			○
13. "+" in /etc/hosts.equiv		○			○
14. Ensuring root in /etc/ftpusers		○			○
15. Checking default logins (sync)			○		
16. Get pw via Ypx			○		
17. NIS password file access				○	
18. REXD access			○	○	
19. Sendmail 취약성		○	○	○	
20. Unrestricted NFS export				○	
21. Unrestricted X server access				○	
22 Unstricted modem				○	
23. Reports hosts available			○	○	
24. Establish OS type			○	○	
25. GUI			○	○	○
26. 운영체제/호환성	SUN OS/Solaris	○	○	○	○
	HP-UX	○	○	○	○
	IBM AIX	○	○	○	○
	TICOM UNIX SVR				○
	TOLERENT TX				○
27. 메모리		5 MB	272 KB	19 MB	6 MB

V. 결론

본 논문에서는 국내에서 발생한 해킹 사례를 중심으로 시스템 관리자 및 사용자 부실에 의하여 발생할 수 있는 보안 문제점을 점검하고 조치를 취할 수 있도록 하는 전산망 안전진단 소프트웨어를 제시하였다. 전산망 안전진단 소프트웨어는 국내 전산망 해킹 사례를 중심으로 패스워드 취약성, 시스템 부팅 패스워드, 패스워드 파일, 파일전송프로토콜, 단순파일전송프로토콜, 사용자 홈 디렉토리, 사용자 홈 디렉토리내의 중요 파일, 사용자 그룹, 시스템 관리자 환경, 그리고 시스템 관리자 권한으로 동작하는 프로그램의 점검 기능 등을 중심으로 구성·개발되었다. 또한 국내에서 운영되고 있는 각종 UNIX 시스템과의 호환성 검증을 위하여 SUN OS 4.1.1, SUN OS 4.1.3, SUN Solaris 2.4, SUN Solaris 2.5, HP-UX 9.x, HP-UX 10.x, IBM AIX, 그리고 국산 주전산기의 운영체제인 타이컴 UNIX SVR 3.2, 타이컴 UNIX SVR 4.2, 툴러런트 TX에서 그 기능을 시험하였다.

향후, 국내 전산망 환경에서 발생할 우려가 있는 보안 취약점들을 사전에 예방·진단할 수있도록 그 기능을 추가·보완할 예정이다.

참 고 문 헌

[1] 홍기용, "인터넷 발전과 보안", '96 정보보호 심포지움 자료집, pp. 121~166, 1996년 7월.
[2] 이재우외, *유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구*, 한국전산원, 1995년 12월.
[3] Derek Atkins et al., *Internet Security - Professional Reference*, Prentice-Hall, Inc., 1996.
[4] David A. Curry, *UNIX System Security*, Addison-Wesley Publishing Company, 1995.
[5] ftp://info.cert.org/pub/tools/cops/
[6] ftp://ftp.uunet.net/usenet/comp.sources.misc/volume39/iss/
[7] ftp://ftp.cerf.net/pub/software/unix/security/