□ 기술해설 □

UNIX 시스템 보안

연세대학교 권태경* · 송주석**

목 차

1. 서 론

UNIX 시스템은 다중사용자 및 다중작업을 지원하는 컴퓨터 운영체제로서 1969년에 처음 소개된 이후 다양한 종류의 컴퓨터에서 널리 사용되고 있으며 또한 이들 사이에 공통된 작업환경을 제공해 주고 있다. 그러나 UNIX 시스템은 System V, BSD 등의 다양한 버전들로 서로 난립하게 되었으며, 이것은 사용자들에게 큰 부담이 되었다. 최근에는 이를 지각한 UNIX 시스템 개발자들에 의해서 표준화를 위한 활동이 활발히 이루어지고 있다. 한편 컴퓨터 및 네트워크 시스템의 보급이 활발해짐에 따라 제공되는 서비스의 다양화와 함께 이 서비스를 통해 유통되는 정보의 다양성과 중요성이 점점 증대되어 가고 있는 추세인데, 이와 병행하여 유통되는 정보에 대한 침해 위협 또한 더욱 가중되고 있다. 따라서 정보의 보안에 관한 연구는 이미 컴퓨터 및 통신학계의 주요 이슈가 된지 오래이며 주로 암호화기술을 근간으로 이루어져 왔다. 최근에는 선진국을 중심으로 기존의 컴퓨터 운영체제에 보안기능을 추가하는 보안 운영체제의 연구 및 개발이 활발하게 진행되고 있다. 특히 가장 폭넓은 사용자 및 사용영역을 갖고 있는 UNIX 시스템의 보안 기능 탑재는 앞으로 UNIX의 표준화 작업에 병행하여 더욱 체계적으로 이루어질 전망이다. 이미 미국 등지에서는 System V/MLS, SVR4.2 ES/MP, SunOS/MLS, Secure Xenix 등의 보안 UNIX가 상용화된 상태이며, 운영체제의 보안기능을 평가하기 위한 평가등급 표준안도 마련되어 있다. 특히 SVR4.2 ES 버전은 아직 미국내에서만 사용하도록 규정하고 있는데, 타이컴을 비롯한 여러 시스템에서 UNIX를 표준운영체제로 하는 우리나라에서도 UNIX 시스템 보안에 관한 기본적인 연구를 보다 활발히 진행하고 보안 UNIX 시스템의 개발 및 평가를 위한 방안을 서둘러 마련해야 하겠다.

본 논문에서는 이러한 시각에서 먼저 UNIX 시스템의 보안 연구개발 현황에 대해서 알아보고 운영체제의 보안에 대한 개요 및 UNIX 시스템 보안대책을 구체적으로 다루도록 한다. 특히 일

*준회원
**종신회원

반 UNIX 시스템의 운영자가 고려해야 할 사항들을 실질적인 관점에서 알아보도록 한다.

2. UNIX 시스템 보안 연구개발 현황

AT&T사의 System V 버전과 Berkeley대학의 BSD 버전으로 대표되는 UNIX 시스템은 주로 워크스테이션급의 컴퓨터를 중심으로 시장형성을 해왔으나 많은 종류의 버전들이 속속 등장하면서 호환성 등의 여러가지 문제점을 낳게 되었다. 한편 개인용 컴퓨터의 성능향상과 일관된 운영체제에 대한 요구는 UNIX의 표준화를 필요로 하게 되었고 특히 UNIX의 기존 시장에 도전하는 고성능 운영체제들이 IBM, Microsoft 사 등을 중심으로 발표되면서 기존 UNIX 연구그룹들은 UNIX의 표준화를 절실히 지향하게 되었다. 따라서 UNIX 시스템의 보안에 관한 연구도 UNIX의 표준화 동향과 맞추어 진행되고 있으며 미국 등지에서는 이미 상용화 단계에 이른 상태이다. 본 장에서는 UNIX의 보안 연구개발 현황을 연구그룹 및 제품을 중심으로 알아보도록 한다. 또한 UNIX 시스템에서 보안사고시 대응하기 위한 전담기관 및 조직에 대해서 알아보도록 한다.

2.1 UNIX 표준화와 보안 연구

현재 국제적으로 시장을 넓혀가고 있는 UNIX 운영체제에 대한 표준화 작업은 활발히 진행중이다. 세계 UNIX 시장의 구성은 (그림 1)과 같으며, 보안 UNIX를 요구하는 범위가 점차로 넓어지고 있다.

표준화 작업을 진행하는 대표적인 표준화 그룹으로는 IEEE의 POSIX, X/OPEN 그리고 OSF 등이 있다. 특히 최근에는 UI(Unix International)와 OSF로 크게 나누어져 연구를 진행해왔으나 AT&T사에서 독립한 USL을 중심으로 통합되고 있는 추세이다. OSF에서는 UNIX의 Secure Version을 개발하고 있으며, IEEE의 POSIX.6 Working Group에서는 4개의 보안소위원회(DAC, MAC, Privilege, Audit 그룹)를 구성하여 보안기능 표준화에 애를 쓰고 있다. X/OPEN에서도

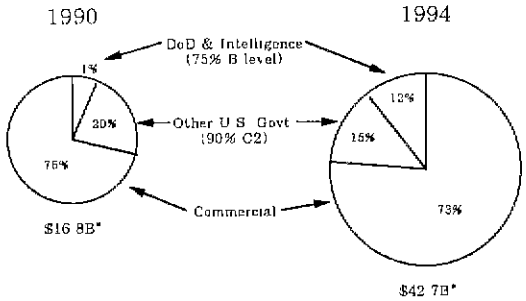


그림 1 세계 UNIX 시스템 시장 구성

이미 X/OPEN Security Guide를 발간한 바 있으며, NCSC(National Computer Security Center)에서도 Trusted UNIX 시스템을 개발하기 위한 Vendor들의 모임인 TRUSIX(Trusted UNIX Organizaiton)를 구성하여 진행중에 있으며, 이밖에도 OSF, AT&T (USL), SUN Microsystems, 그리고 Santa Cruz Inc.들은 각각 Secure UNIX Version을 표준화된 UNIX로 채택하고자 많은 노력을 기울이고 있다. 한편 UNIX의 다른 버전인 Xenix도 보안기능을 고려한 버전을 계속 개발중이며 Toronto 대학의 Secure TUNIS 등 학계에서도 다각적인 연구개발을 진행중이다.

2.2 보안 UNIX의 역사

본 장에서는 보안 UNIX 개발의 역사를 연도순으로 나열하며 알아보도록 한다. 초기에는 주로 미국내에서 개발되었으므로 각 기관에 대한 부연 설명을 생략하기로 한다.

◦ **1969** : UNIX 시스템이 처음 개발되었다. 이 시기에는 AT&T사에서만 사용되었고, 아직 보안에 관한 사항은 이슈가 되지 않았었다.

◦ **1970년대 초반** : UNIX가 학계를 중심으로 사용되기 시작했으며 역시 보안은 아직 이슈가 아니었다.

◦ **1970년대 중반** : 보안 UNIX가 처음 등장하였다. 그러나 성능 문제로 곧 사장되었다. 이 시기에 개발된 보안 UNIX에는 Mitre Secure UNIX, UCLA Secure UNIX, KSOS 등이 있다.

◦ **1970년대 후반** : UNIX가 본격적으로 상용화되었다. 가격과 생산성 문제로 보안 UNIX의

개발은 환영받지 못했다.

◦ **1983** : 보안 운영체제 평가기준으로 Orange Book이 발간되었다.

◦ **1984** : 미 국방성의 NCSC가 설립되었다.

◦ **1986** : UniForum에 의해 Security Working Group이 조직되었다.

◦ **1986년 12월** : Gould사의 UTX/32S가 NCSC에 의해 C2급으로 인정받았다.

◦ **1987년 7월** : NTISSP(National Telecommunications and Information Systems Security Poicy) No. 200에서는 미 연방정부 관련기관의 정보시스템을 위해 C2급의 운영체제를 요구하였다.

◦ **1987년 후반** : IEEE는 POSIX P1003.6 을 만들어 보안 표준화에 주력하게 되었다.

◦ **1988년 11월** : 인터네트 웜 사건은 UNIX의 약점들을 일시에 고발하게 되었다. 한편 X/Open에서는 보안 지침서(X/Open Security Guide)를 발간하였다. 또한 NCSC내의 소그룹인 TRUSIX는 X/Open 그룹과 정기적인 모임을 갖기로 합의하였다.

◦ **1989년** : AT&T의 USL은 표준 UNIX로 SVR4.0을 발표하였다.

◦ **1989년 10월** : AT&T사의 보안 UNIX인 System V/MLS는 NCSC로부터 B1급으로 판정을 받았다.

◦ **1991년** : USL의 보안 UNIX인 SVR4.1 ES가 발표되었다.

◦ **1993년** : SVR4.2 ES/MP가 발표되었고 B2 등급으로 인정받고 있다.

2.3 USL(UNIX System Laboratories)의 개발 현황

USL은 AT&T사의 연구소였으나 최근 분리되어 UI 및 OSF를 중심으로 진행되고 있는 UNIX의 표준화 작업을 적극적으로 추진하고 있다. 이미 SVR 4.x 및 SunOS 5.x 등은 UNIX 버전의 주류인 AT&T SVR 3.x 및 Berkeley 대학의 BSD 4.x의 기능을 통합하였고 표준 UNIX의 형태를 취하고 있다. USL에서 개발하여 이미 상용화되어 있는 SVR 4.1 및 SVR 4.2는

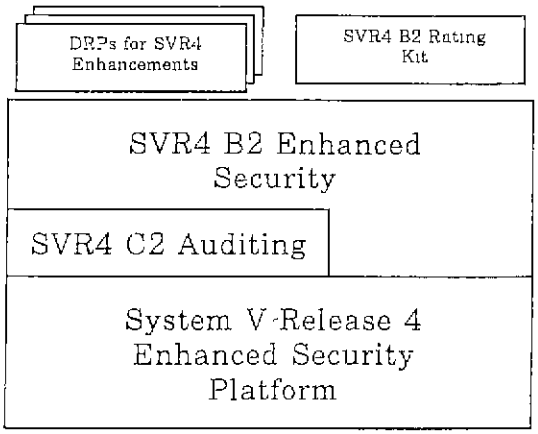


그림 2 SVR 4ES 개념도

ES(Enhanced Security) 및 MP(Multiple Processor) 버젼으로 미국내에서 폭넓게 사용되기 시작하고 있는 추세이다. 특히 1989년에 SVR 4.0을 표준 UNIX로 개발한 이래 1991년 개발된 SVR 4.1 및 최근 버전에 보안기능을 추가하므로써 본격적인 보안 UNIX의 개발을 진행중이다. USL에서 개발하는 보안 UNIX의 개념도는 (그림 2)와 같다.

SVR 4.2 ES/MP 등과 같은 보안 UNIX는 일반적으로 로그인시 다음과 같이 기존의 로그인 절차보다 두단계가 늘어난 절차를 거치게 된다.

```
login:
password:
group:
security level:
```

2.4 주요 보안 UNIX 제품

여기서 소개할 보안 UNIX는 이미 NCSC의 평가를 받았거나 현재 평가가 진행중인 대표적인 제품들로서 대부분 미국내에서만 사용되고 있다.

2.4.1 USL SVR 4.2 ES/MP

AT&T사에서 분리되어 표준 UNIX의 개발을 추진하는 USL의 SVR 4.2 ES/MP는 B2등급으로 인정받고 있다. SVR 4.2 ES/MP의 근간 버전인 SVR 4.0은 기존의 System V와 BSD의 표준으로서 확장된 네트워크 설비 및 가상 화일 시스템

설비 등을 포함한다.
개발회사 : Unix System Laboratories

2.4.2 AT&T System V/MLS

AT&T에서 다중사용자 및 다중작업을 위한 컴퓨터인 3B2/500과 3B2/600의 보안운영체제로서 개발한 System V/MLS는 1989년 NCSC로부터 B1등급을 판정받았다. System V/MLS는 TCSEC의 표준요구사항을 충실히 수용하였고 BLP 모델을 근간으로 설계되었다.
개발회사 : AT&T Federal System Div.
Greenboro, NC (800) 828-UNIX

2.4.3 SunOS MLS

상용 워크스테이션인 Sun-3과 Sun-4의 네트워크환경을 위해 개발된 SunOS MLS는 기존의 SunOS에 보안기능을 대폭적으로 추가한 운영체제이다. SunOS는 기본적으로 System V 및 4.2 BSD와 호환성을 갖는 표준 UNIX의 형태를 취하고 있으므로, 보안 기능이 추가된 SunOS MLS는 상용 보안 UNIX로서 많은 역할을 할 것으로 기대된다. SunOS MLS는 NCSC로부터 B1등급을 인정받고 있다.
개발회사 : Sun Microsystems, Inc.
2250 Garcia Avenue
Mountain View, CA 94043 (415)960-1300

2.4.4 Trusted Xenix

IBM PC AT를 위해 개발된 Secure Xenix의 다음 버전인 Trusted Xenix는 IBM PC AT 및 PS/2를 위한 보안 운영체제로서 Microsoft Xenix를 근간으로 System V와 호환성을 고려하여 개발되기는 했지만 운영체제 자체의 성능은 일반 UNIX만큼 강력하지는 못하다. 특히 AIX 개발에 주력하는 IBM은 B2급의 Trusted Xenix를 TIS사에 매각하였고, 현재는 판권을 가진 TIS사에서 개발되고 있다. Trusted Xenix는 NCSC의 B2급 후보로 지명되고 있다.
개발회사 : Trusted Infomation Systems, Inc.
3060 Washington Road
Glenwood, MD 21738 (301)854-6889

2.4.5 UTX/32S

Gould Computer Systems에서 Gould PowerNode 6000과 9000 시리즈의 수퍼미니컴퓨터를 위해서 개발한 범용 시분할시스템인 UTX/32S는 System V와 4.2 BSD를 근간으로 한다. UTX/32S는 이미 1986년 12월 C2급을 받았으나 최근에는 평가를 받은 기록이 없다. 현재는 Encore사에서 개발 및 판매 중이다.
개발회사 : Encore Computer Corp.
6901 W. Sunrise Boulevard
Ft. Lauderdale, FL 33313 (305)587-2900

2.5 운영체제 보안기능 평가기준

미국의 국방성에서는 이미 1983년에 TCSEC (Trusted Computer System Evaluation Criteria)이라는 운영체제의 보안기능 평가기준안을 마련하였고 이를 기준으로 기존의 운영체제 및 새로운 운영체제의 보안기능을 평가하고 보안등급을 부여하고 있다. 또한 유럽에서는 평가기준인 ITSEC(Information Technology Security Evaluation Criteria)을 영국, 독일, 프랑스, 네덜란드 등 4개국이 중심이 되어 발간하였다. TCSEC은 안전한 컴퓨터 시스템의 광범위한 이용을 촉진시키는 것을 목적으로하여 미 국방성의 연구소인 NCSC가 기존의 소프트웨어 도구와 Multics 운영체제를 기술적 기반으로 하여 발간한 안전한 컴퓨터 시스템 평가 기준이다. 표지색을 따라서 일명 Orange Book이라고도 불리운다. ITSEC은 평가등급이 매우 많은 반면 TCSEC은 등급은 간소화하였다. TCSEC의 평가등급을 상위등급부터 나열하면 A1, B3, B2, B1, C2, C1, D급 등의 7등급으로 나누어진다. 이중 D급은 보안기능이 전무한 경우이고 C1급에는 일반 UNIX가 포함되며 USL의 SVR 4.2 ES/MP는 B2급으로 인정되고 있다. 각 등급에 대해서는 간략히 요약하여 설명하도록 한다. (표 1)은 TCSEC으로 평가된 제품들을 등급별로 보여주고 있다.

2.5.1 A급

표 1 보안 평가를 받은 제품들

개발사 \ 등급	C2	B1	B2	B3	A1	승인 날짜
AT&T		SVR/MLS (UNIX)	SVR4.2			89/9 93/
BOEING		MLS LAN				
UNISYS	InfoGuard Security	OS1100 Security				87/8 89/8
CDC	NOS2 2					86/5
CAI	CA-TOP SECRET/MVS					
DEC	VMS			VMS50		86/7
DATA GENERAL Corporation	ACS/VS					88/12
Encore Computer System	UTX/32S					88/12
SUN		SunOS MLS				
Honeywell Information Inc			MULTICS		SCOMP	
IBM	RACF/MVS RACF/VM		Trusted XENIX			88/6 89/6
PRIME	PRIMOS					88/6
SKK	ACF2/MVS					
WANG	SVS/OS					
Hewlett Packard Company	MPE V/E					88/10

A1급을 초과하는 기능에 대한 규정은 아직 마련되어있지 않으며, A1급이 갖는 주요 기능은 B3급의 기능과 같다. 그러나 이를 보증할 수 있는 기능이 필요하다.

2.5.2 B급

B1, B2, B3 등의 세 등급으로 구분되며, C급의 기능을 포함하여 추가적으로 강제적 접근제어 기능을 구비한 시스템이다.

2.5.3 C급

C1, C2 등의 두 등급으로 구분되며 임의적 접근제어 기능을 구비한 시스템이다.

2.5.4 D급

보안기능을 구비하지 못한 시스템이다.

2.6 보안사고 응답기관

UNIX 시스템이 제공하는 기능 중 가장 중요한 것은 네트워크 기능라고 할 수 있다. 따라서 대부분의 보안사고는 네트워크를 통해서 발생하는 사례가 많다. 국내에서도 보안 침해 사례가 빈번하게 발생하고 있음에도 불구하고 적절하게 대응하지 못하고 있는 까닭은 보안사고에 대한 대응을 전담하는 전문기관이 없기 때문이라고도 할 수 있다. 본 장에서는 미국을 중심으로 활발히 활동하고 있는 보안사고 응답기관들에 대해서 알아보도록 한다.

2.6.1 CERT/CC

앞에서 간략히 언급한 바 있는 인터네크 웜 사건을 계기로, 미국 카네기멜룬대학의 Software Engineering 연구소 산하에 조직된 Computer Emergency Response Team/Coordination Center는 보안침해 사고가 접수될 때마다 즉각 전문가를 동원하여 문제를 해결하고 인터네트를 통해서 보안대책을 알리는 활동을 하고 있다. 인터네트를 통하여 CERT에 가입을 할 경우 UNIX 시스템을 포함하여 여러가지 시스템의 보안관련 정보를 접할 수 있다. CERT의 인터네트 주소는 다음과 같다.

- cert-advisory@cert.org
- cert-tools@cert.org

2.6.2 DDN SCC

DDN Security Coordination Center는 DDN 사용자를 위해서 운영되는 보안센터로서 CERT/CC와 유사한 역할을 담당하고 있다. 아래의 인터네트 주소로 Anonymous FTP를 통해서 정보를 얻을 수 있다.

- nic.ddn.mil

2.6.3 NIST CSRC

미국 정부기관들을 위한 정보처리 기술을 담당하는 NIST에 의해서 조직된 Computer Security Resources and Response Center는 바이러스에 대한 대응지침서를 발간하는 등 활발한 활동을 하고 있다. 아래의 인터네트 주소로 Anonymous FTP를 통해서 정보를 얻을 수 있다.

- csrc.ncsl.nist.gov

2.6.4 DOE CIAC

주로 미 에너지성 산하기관을 위해 발족된 Computer Incident Advisory Capability는 CERT와 유사한 활동을 하고 있다. CIAC의 인터네트 주소는 아래와 같다.

- ciac@tiger.llnl.gov

2.6.5 NASA CNSRT

Computer Network Security Response Team은 CERT와 연동하여 활동중이며 주로 NASA 관련 연구소를 위해서 활동을 하고 있다. CNSRT의 인터네트 주소는 아래와 같다.

- cnsrt@ames.arc.nasa.gov

3. 운영체제 보안의 개요

본 장에서는 보안운영체제의 개발을 위해서 필요한 기본적인 개념에 대해서 다루도록 한다. 다음에서 소개할 모델들을 기반으로 보안 UNIX들이 개발되고 있다.

3.1 보안 모델의 기본 개념

보안 모델이란 컴퓨터 시스템과 사용자의 보안 성질을 설명하는 추상적인 형태로서 모델의 설정과 접근 권한에 대한 제어가 핵심개념이 된다. 보안 모델은 컴퓨터 시스템을 구성하는 요소를 크게 주체와 객체로 나누어 제어 및 감시에 대한 능력을 추상적으로 설명하도록 한다. 여기서 주체란 사용자, 프로세스 등 능동적인 요소를 의미하며 객체란 화일, 프로그램 등 수동적인 요소를 의미한다. 보안 모델을 통해서 설명되는 보안시스템은 비밀성, 무결성, 가용성이 만족되어야 한다.

3.2 보안 모델의 종류

보안 모델은 크게 참조모니터 모델과 정보흐름 모델로 분류해 볼 수 있다.

3.2.1 참조모니터 모델

주체와 객체 사이에 모니터(Monitor)를 둠으로써 사용자의 객체 접근 요청을 받아서 필요한

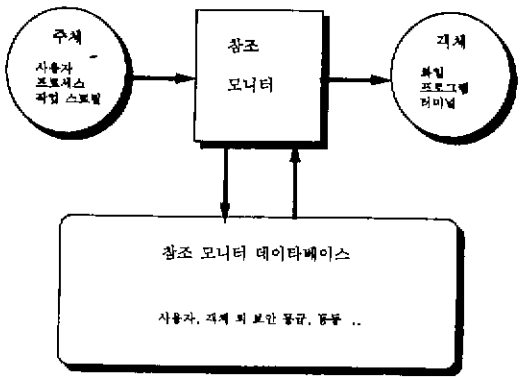


그림 3 참조모니터 모델

접근제어 정보를 참조하여 접근의 허용여부를 결정하는 모델이다. 이 모델은 (그림 3)과 같이 어떤 사용자와 어떤 객체 사이에서 단순히 접근의 허용 여부만을 결정하는 단일 레벨(Single-level) 보안 모델로 볼 수 있다. 접근제어를 위해서 데이타베이스의 보안등급을 참조하게 된다. 운영체제는 이와 같은 역할을 담당할 수 있으므로 본 모델의 적용에 적합하다고 할 수 있다.

3.2.2 정보흐름(Information Flow) 모델

수학적인 Lattice 개념을 기반으로 주로 다음과 같은 두가지 모델로 표현된다.

(1) 벨라파둘라(BLP) 모델

보안 시스템내에 허용되는 정보의 흐름을 설명하는 모델의 하나로 비밀성(Secrecy)를 중요시한 모델이다. 특히 System V/MLS와 같이 다중 레벨을 가지는 데이타를 처리하는 시스템을 설계할 때 기초가 된다.

(2) 비바 모델

벨라파둘라 모델과는 달리 데이타의 무결성(Integrity)을 중요시하는 모델로서 여기서는 주체와 객체에 대해서 무결성 레벨을 정의하고 있다.

3.3 운영체제 보안 정책

운영체제를 위한 보안 정책은 다음과 같은 보안 특성을 고려하여 구체적으로 수립되어야 하며, 수립된 정책을 기반으로 필요한 기술을 개발 및 적용하도록 해야 한다.

3.3.1 식별(Identification) 및 인증(Authentication)

운영체제의 모든 주체와 객체는 식별 즉, 신분확인 및 인증이 가능해야 한다.

3.3.2 의적 접근제어(DAC: Discretionary Access Control)

운영체제의 모든 객체는 소유권한을 가진 주체의 의도대로 접근제어가 가능해야 한다.

3.3.3 강제적 접근제어(MAC: Mandatory Access Control)

운영체제의 모든 객체는 보안등급에 의존하여 접근제어가 가능해야 한다.

3.3.4 감사(Auditing)

시스템에서 발생한 모든 사건은 추적 및 감시가 가능해야 한다.

3.3.5 안전한 통로(Trusted Path)

운영체제와 약속된 Trusted Path를 통한 안전한 통신이 가능해야 한다.

3.3.6 최소권한(Least Privilege)

운영자를 포함한 시스템의 모든 주체는 현재 필요한 권한 이상을 갖지 못하도록 규제 가능해야 한다. 최소권한을 위한 UNIX의 운영자 구성도는 (그림 4)와 같다.

3.4 운영체제 보안 기술

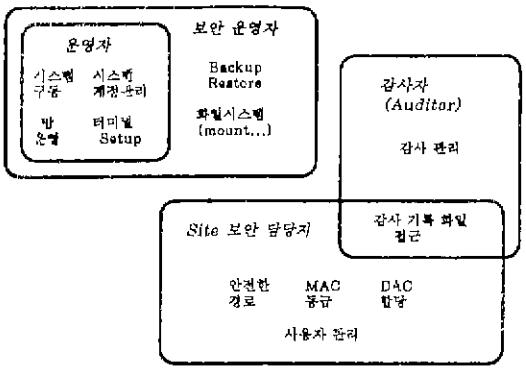


그림 4 운영자 최소권한 구성도

보안 운영체제의 개발을 위한 기술은 주로 암호기술 및 데이타베이스 관리 기술에 근간을 둔다. 앞서 설명한 보안 특성을 중심으로 필요한 보안 기술을 간략히 분류해 보도록 하며, UNIX와 관련된 기술은 다음장에서 설명하도록 한다. (표 2)에서는 앞서 설명한 정책과 기술을 통한 주요 보안기능을 사용자 관점에서 TCSEC 등급별로 설명하고 있다. 또한 (그림 5)에서는 보안 기능만을 추가하는 경우와 기능에 대한 보증을 할 경우에 드는 비용을 등급별로 비교하고 있다.

(1) 주체 및 객체의 Labeling
(2) 안전한 암호기술
(3) 패스워드 시스템을 비롯한 안전한 인증기술
(4) 임의적 접근제어를 위한 기술 (ACL, 모드 비트)
(5) 보안등급(Security Level) 관리 기술
(6) 기록(Log) 화일 관리
(7) 운영자 권한의 분산

표 2 등급별 주요 보안 기능

보안등급	주요사항	추가적인 보안 기능
A1	Verified design	
B3	Security domains	ACLs, enhanced trusted path, trusted recovery
B2	Structured	Least privilege, trusted path
B1	Labeled security	MAC
C2	Controlled access	Auditing
C1	Discretionary security	DAC, passwords
D	Minimal protection	

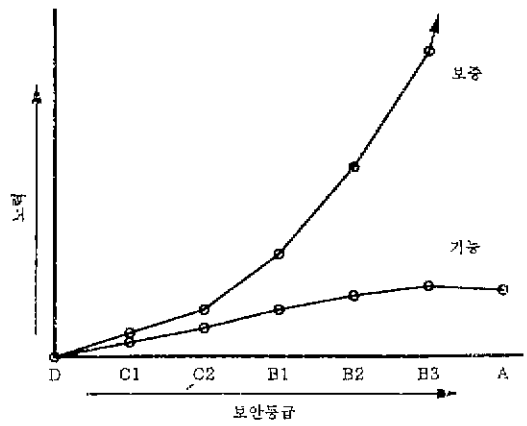


그림 5 보안 기능 · 보증의 비용 비교

(8) 사용자 그룹 관리

3.5 운영체제 보안을 위한 접근 방법

UNIX를 비롯한 기존의 운영체제들은 보안문제에 대한 고려없이 효율성과 편리성만을 중시하여 개발되어 왔다. 따라서 다수의 사용자와 다수의 자원에 대한 처리를 효율적이고 안전한 방법으로 하기 위하여 기존의 운영체제에 보안기능을 추가하는 방법이 제안되었고 이에 따라 1970년대에는 보안제품 연구개발이 기존 컴퓨터 시스템에 암호화, 접근제어, 감사 등의 보안기능을 하드웨어, 소프트웨어로 추가하는 방식으로 진행되었다. 그러나, 이러한 방식으로는 새로운 문제점(예, 트로이 목마, 신종 시스템 범죄)을 해결할 수 없다는 연구 결과와 함께 문제점 발생시 마다 보안 제품을 계속적으로 추가하는데 막대한 비용과 번거로움이 따르게 된다는 사실을 인식하여 미니급 이상의 컴퓨터 시스템에서는 1980년대부터 시스템 내부 커널(Kernel)에 보안기능을 탑재시키는 보안커널시스템 접근방법이 활발히 연구되었고, 주로 정부기관과 군기관에서는 이러한 보안 제품을 연구 개발하여 사용하고 있다. 최근 개발되는 보안 UNIX 시스템도

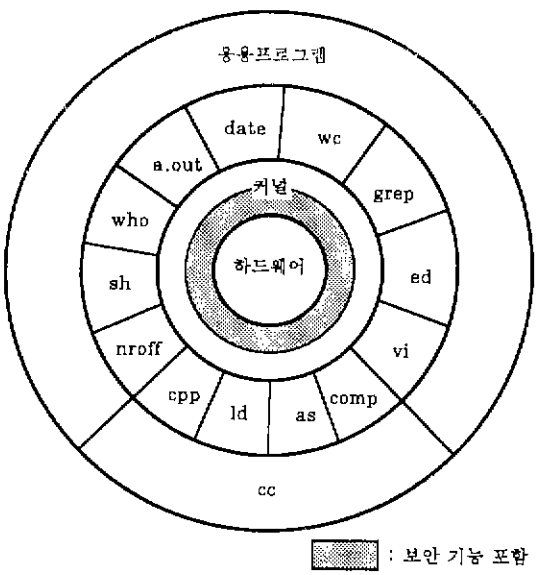


그림 6 UNIX의 보안커널시스템 접근

(그림 6)과 같이 보안커널시스템 접근방법을 지향하고 있다.

4. UNIX 시스템의 보안 대책

본 장에서는 기존의 UNIX 시스템을 중심으로 운영자가 고려해야 할 보안 대책에 대해서 알아보도록 한다.

4.1 사용자 계정(Account) 보안

UNIX 시스템 보안의 가장 중요한 부분은 사용자 계정 보안이다. 즉, 침입자가 시스템에 대한 접근을 가장 쉽게 할 수 있는 방법이 사용자의 계정을 확보하는 것이기 때문이다.

4.1.1 계정 관리 대책

(1) 사용자 계정의 특성

UNIX 시스템을 이용하는 모든 사용자는 계정을 갖게 된다. UNIX 시스템은 사용자의 이름 및 패스워드의 최대 길이를 8바이트크기로 인식하며 사용자는 사용자이름을 여러개 등록하므로써 다수의 계정을 이용할 수가 있다. 또한, UNIX 시스템은 사용자 관리를 일괄적이며 체계적으로 할 수 있도록 사용자그룹을 정의하도록 하는데, 일반적으로 System V 계열에서는 사용자의 그룹가입을 한개의 그룹으로만 제한 하는 반면 BSD 계열에서는 다수의 그룹에 대한 동시 가입을 허용한다.

(2) 수퍼유저 계정에 대한 보안 대책

UID 값을 0으로 갖는 수퍼유저는 UNIX 시스템의 모든 권한을 소유하게 되는 만큼 침입자들의 가장 큰 공격 대상이 된다. 따라서 이 계정은 철저히 보호되어야 하며 이에 대한 대책이 필요하다. UNIX 명령어 su는 단독적으로 사용될 경우, 패스워드 검사후 사용자의 UID를 수퍼유저의 UID 즉, 0으로 바꾸어주게 된다. 특히 이 su 명령을 사용하게 되는 경우 /usr/adm/messages 화일에 기록이 남게 되므로 시스템의 보안을 위해서 사용을 권장해야 하며, 사용시에는 반드시 /bin/su로 패스이름을 같이 입력하여 트로이목마를 예방하도록 해야 한다. BSD 계열의 새 버

전에서는 GID가 0인 wheel 그룹에 가입된 사용자에게만 su 명령을 사용할 수 있도록 제한하였고, su 명령의 새 버전중에는 wheel 그룹에 가입되어 있는 경우 사용자 자신의 패스워드를 입력하도록 허용하는 것도 있다.

다음과 같은 명령으로 불법적인 su 시도의 기록을 조회할 수 있다.

```
% grep BAD /usr/adm/messages
Oct 2 10:28:38 prose su: BAD SU intruder on
/dev/tty01
```

(3) 일반 계정에 대한 보안 대책

UNIX 시스템의 모든 계정은 외부세계와 시스템 내부를 연결해주는 통로역할을 담당하게 된다. 따라서 통로의 불법침입을 막을 수 있는 방법이 필요하다. 이에 대한 대책으로 우선 시스템 운영자는 다음과 같은 위험한 계정을 철저히 검색하여 제거 또는 감시관리를 하도록 해야 한다.

– 패스워드가 없는 계정

패스워드가 없는 계정은 다음과 같은 명령으로 쉽게 발견할 수 있으며 시스템 침입자에게는 가장 손쉬운 침투방법이 된다. 따라서 운영자는 미리 이런 계정을 발견하여 경고를 주어야 한다. 한편 최근의 UNIX 시스템은 수퍼유저만 읽고 쓸 수 있는 /etc/shadow 화일이나 /etc/security /passwd 화일에 패스워드 관련 정보를 분리 관리하도록 하여 보안 기능을 강화하고 있다.

```
% awk -F: 'length($2)<1 {print $1}' < /etc/
passwd
jssong
ktk
% grep 'jssong|ktk' /etc/passwd
jssong::102:10:Song JooSeok:/usr/prof/
jssong:/bin/csh
ktk::110:20:Kwon TaeKyoung:/usr/MS/netlab/
Ktk:/bin/csh
```

– Dormant 계정

사용자가 부재중이거나 거의 사용되지 않고 있는 계정에 대해서는 특별한 관리가 필요하다. 이러한 계정에 대한 감시 및 관리는 계정관리자의 몫이다.

– Default 계정/Open 계정

help, uucp, nuucp, ingres, system, mail, finger, who, telnet, open, guest, ftp 등의 Default 계정이나 Open 계정은 가급적이면 줄이도록 해야 하며 사용자영역(User Domain)을 구성해서 사용자의 추적이 가능하도록 해야한다.

(4) 사용자 계정의 감시

시스템 관리자는 주기적으로 계정보안을 위한 감시작업을 해야 한다. 최근 대부분의 UNIX 시스템은 이를 위한 기능으로 다음과 같은 화일과 명령어를 제공하고 있다.

– /usr/adm/lastlog

각 사용자가 로그인한 가장 최근의 시간을 기록한다.

– /etc/utmp

현제 로그인해 있는 사용자를 기록한다.

– who 명령어

utmp 화일의 내용을 출력한다.

– /usr/adm/wtmp(또는 /etc/wtmp)

각 사용자의 로그인 및 로그아웃 시간을 기록한다.

– last 명령어

wtmp 화일의 내용을 시간으로 정렬하여 출력한다.

– /usr/adm/acct(또는 /usr/adm/pacct)

시스템에서 수행되고 있는 명령어의 사용자 및 사용시간을 기록한다.

– lastcomm 명령어

acct 화일의 내용을 출력한다. (BSD 계열)

– acctcom 명령어

acct 화일의 내용을 출력한다. (System V 계열)

– sa 명령어

각 사용자 또는 프로세스의 시스템 점유율 및 사용량을 출력한다.

– ps 명령어

시스템에서 수행되고 있는 프로세스의 리스트를 출력한다.

4.1.2 패스워드 관리 대책

(1) 패스워드 암호화

UNIX 시스템에서 사용자 패스워드는 암호화되어 비교적 안전하게 관리되는데 패스워드의 암호화는 DES (Data Encryption Standard)에 기반을 둔 crypt(3) 함수를 이용해서 이루어진다.

UNIX crypt(3) 함수는 사용자가 입력한 8바이트 패스워드를 56비트크기의 키(각 캐릭터를 7비트 아스키코드로 인식)로 사용하여, 64비트의 0 블럭 즉 64자리의 이진수 0을 25번 반복하여 암호화한 후 11개의 문자스트링으로 바꾸어 /etc/passwd 화일에 기록한다. 패스워드 등록을 마친 후 사용자의 인증을 위해서 /bin/login 프로세스는 다시 같은 방법으로 입력되는 패스워드를 암호화하고 문자스트링으로 바꾸어 /etc/passwd 화일의 문자스트링과 비교하여 인증을 하게 된다.

(2) 패스워드 암호스트링의 보안 대책

/etc/passwd 화일은 공개화일이므로 이곳에 기록된 패스워드 암호스트링은 모두에게 공개될 수 있다. 따라서 crack 등의 소프트웨어적 공격에 민감해지게 되며 실제로 패스워드를 역으로 알아내어 침투하게 되는 사례가 빈번하다. 최근의 UNIX는 이에 대한 보안 대책으로 salt 비트와 쉐도우 패스워드화일을 제공하고 있다.

- Salt 비트

12비트의 숫자를 추가하여 DES 암호화 결과를 경우에 따라서 달라지게 만든다. 따라서 역으로 패스워드를 알아내기는 더욱 힘들어 진다.

- Shadow 패스워드화일

비공개화일인 /etc/shadow(또는/etc/security/passwd) 화일에 패스워드 암호스트링을 분리하여 기록한다. /etc/passwd 화일의 페스워드 영역은 *나 X로 대체하여 운영자권한으로만 쉐도우 패스워드화일을 참조 또는 변경할 수 있도록 한다.

(3) 패스워드 생성기

NCSC(National Computer Security Center)에서 권고하는 패스워드 생성기는 임의적인 값으로부터 안전하고 적당한 패스워드를 생성하도록 한다. 따라서 사용자가 임의로 선택한 패스워드보다 안전성이 높아지게 된다. 그러나 대부분의 UNIX는 기본적으로 이 기능을 지원하지 않으며 원하는 운영자는 인스톨해서 사용할 수 있다.

(4) 패스워드 에이징 (Aging)

사용자의 패스워드를 주기적으로 바꾸어 주는 것은 패스워드에 대한 좋은 보안 정책이라고 할 수 있다. 패스워드 에이징이란 각 패스워드에 생명주기(Life Time)를 할당하여 만기가 되면 사용자로 하여금 강제적으로 패스워드를 바꾸도록 하는 방법이다. SVR 4.x, SunOS 4.x, 4.3BSD-Reno, ULTRIX 4.x 등에서는 이와 같은 기능을 기본적으로 제공하고 있다. 다음은 SVR 4.0에서의 사용예이다.

```
# passwd -x maxdays -n mindays login_name
```
(사용자 패스워드의 생명주기를 결정한다.)
```
# passwd -f login_name
```
(사용자의 패스워드를 강제로 만기시킨다.)
```
# passwd -w numdays login_name
```
(사용자에게 패스워드 만기 경고를 줄 시간을 정한다.)
```
# passwd -s login_name
```
(사용자의 패스워드 에이징 정보를 출력한다.)

(5) passwd+/npasswd

사용자가 /usr/bin/passwd 대신에 passwd+나 npasswd를 이용할 경우 새롭게 설정되는 패스워드를 직접 /etc/passwd 화일에 저장하지 않고 패스워드의 내용에 대한 검사를 수행하게 된다. 이 경우 passwd+나 npasswd는 패스워드 검사를 위한 정보를 보유하게 되고 안전한 조건을 만족하지 않을 경우는 패스워드의 재설정을 요구하게 된다. 즉, 특수문자 등을 섞도록 하여 보다 안전한 패스워드의 설정을 유도한다.

(6) passwd 2.1

기존의 passwd 기능에 패스워드 에이징 기능을 탑재시킨 버젼이다. 운영자는 passwd 2.1을 인스톨하여 시스템의 보안을 강화하도록 해야 한다.

(7) crack

/etc/passwd 화일을 읽고 사용자의 패스워드를 추적하요 알아내는 도구이다. 이 도구가 침입자에 의해서 사용되지 않도록 쉐도우 패스워드 화일을 사용하도록 해야하며, 운영자는 정기적으로 이 도구를 이용하여 사용자의 위험한 패스워드에 대한 경고를 하도록 해야 한다.

(8) kerberos

UNIX 시스템으로 구성된 LAN 환경에서의 중요한 정보를 암호화하여 유통하고 또한 인증하도록 하는 광범위한 보안 도구이다. kerberos의 인증 프로토콜에 대해서는 이미 잘 알려져 있다.

4.2 화일 시스템 보안

UNIX 화일 시스템은 모든 화일과 디렉토리, 디바이스 등을 관리하며, 누가 무엇을 어떻게 접근하는가를 제어한다. 따라서 화일 시스템은 UNIX 시스템의 보안 기능을 위해서 가장 기본적인 도구가 된다. 화일 시스템의 보안을 위해서는 접근제어 정책을 잘 설정해야 하며 앞에서 설명한 바 있는 임의적 접근제어와 강제적 접근제어가 이에 해당된다.

4.2.1 임의적 접근제어 대책

UNIX 화일 시스템은 각 화일들의 소유자와 사용자 권한을 정의하고 제어할 수 있는 기능을 제공한다. C2급에서 요구되는 임의적 접근제어를 위해서는 ACL (Access Control List)을 이용하도록 해야한다. Multics에서 처음 소개된 ACL은 모드 비트를 다수의 사용자 영역에 대응시킬 수 있다. 즉 ACL은 화일에 대한 접근허가를 정밀하게 나열할 수 있도록 하므로 임의적 접근제어를 보장하게 된다. 다음은 ACL을 조회하는 명령의 예이다.

```
$ getacl test
# file  : 1   15897 Sep 20 21:18 test*
# owner : jssong
# group : netlab
user::rwx
user:ktk:rwx
user:jupiter:r-x
user:nyang:r-x
group::--x
group:prof:--x
other:---
```

4.2.2 강제적 접근제어 대책

강제적 접근제어를 위해서는 사용자의 각 계정 및 화일을 포함한 모든 자원에 Security Level이 할당되어야 하며 항시 Security Level을 참조하여 접근제어가 이루어져야 한다. 강제적 접근제어를 위한 Security Level은 다음과 같이 구성되는 것이 좋다.

Security Level (Sensitivity Level, Categoty Set)

4.2.3 화일 시스템 보안 대책

화일 시스템의 보안 문제를 검사하는 것은 UNIX 시스템 보안의 매우 중요한 부분이다. 주로 find 명령어 등을 이용하여 정기적으로 감시를 하고 검사해야 한다. find 명령어는 화일 시스템을 검색하기 위한 범용적 명령어이며 사용 형태는 다음과 같다.

```
$ find directories option
```

(1) SUID/SGID 화일 검색

```
# find / -type f -a -perm -4000 -print
```

(SUID 화일을 찾는다.)

```
# find / -type f -a -perm -2000 -print
```

(SGID 화일을 찾는다.)

(2) 디바이스 화일 검색

```
# find / \( -type b -o -type c \) -print
```

(3) 완전공개(World-writable) 화일 검색

```
# find / -perm -2 -print
```

(4) 미소유(Unowned) 화일 검색

이 명령의 옵션은 SVR 3.0 버전에서는 제공하지 않는다.

```
# find / -nouser -print
```

(5) .rhosts 화일 검색

```
# find home-directory -name .rhosts -print
# find home-directory -name .rhosts -exec rm -f {} \;
```

4.3 네트워크 보안

UNIX 시스템은 사용자들의 컴퓨터망 구성 요구에 상응하는 공통된 작업환경을 제공해 주며 관련된 편리 기능을 제공하는 네트워크 기반 운영체제이다. 따라서 UNIX 시스템을 이용하는 경우 자신의 컴퓨터를 통해서 연결된 다른 컴퓨터에 손쉽게 접근할 수 있으며 이로 인하여 여러가지 보안 문제를 발생시키게 된다. UNIX 시스템의 편리한 네트워크 기능 이면에 숨어 있는 보안 문제를 분석하고, 이에 대한 대책을 마련하는 것은 시스템의 보안 유지를 위해서 반드시

필요하다.

4.3.1 네트워크 관련 화일 관리

(1) /etc/hosts.equiv 화일

이 화일은 시스템 운영자가 사용자들을 위해서 안전한 호스트(Trusted Host)를 지정해주는데 사용된다. 이 화일을 통해서 안전한 호스트가 타인에게 공개될 경우 시스템에 대한 침해와 직결되므로 운영자는 안전한 호스트 지정을 신중하게 해야하며 가급적이면 사용을 피해야 한다.

(2) .rhosts 화일

이 화일은 일반 사용자가 자신의 안전한 호스트를 지정하는데 사용된다. 이 화일의 이용은 자제하도록 하는 것이 좋다.

(3) .netrc 화일

이 화일은 원격 호스트에 대한 ftp 명령을 수행할 경우 패스워드의 입력없이 로그인 할 수 있도록 하는데 사용된다. 이 화일에 대한 보안 대책 역시 사용을 자제하도록 하는 것이다.

(4) /etc/inetd.conf

이 화일 내용에서 정의한 서비스중 위험한 서비스를 리마크시켜서 사용하지 못하도록 하거나 서비스의 이용권한을 제한하여 시스템 보안을 고려하도록 해야 한다.

4.3.2 네트워크 서비스에 대한 보안 대책

UNIX 시스템이 제공하는 여러가지의 유용한 네트워크 서비스중 몇 가지는 그동안 보안상의 문제점이 다수 지적되었고 계속 수정되어 왔다.

(1) FTP(File Transfer Protocol)

1988년 이전에 만들어진 버전에는 침입자가 이 프로토콜을 통해서 시스템에 침입할 수 있는 오류가 있었으나 1988년 11월 발표된 버클리 버전부터 이 오류가 수정되었다. 따라서 시스템의 ftp 버전을 확인할 필요가 있다. 특별히 anonymous ftp 서비스를 위해서는 철저한 관리 및 운영을 해야 한다.

(2) TFTP(Trivial FTP)

tftp의 여러가지 버전은 보안상 문제점을 갖고 있는 것으로 지적되었으며 최근에는 문제점들을 보완한 버전들이 사용되고 있다. 다음의 예는 기존의 tftp를 이용해서 사용자 인증 과정 없이 원거리 호스트의 /etc/passwd 화일을 전송받아서 cracking 하는 예이다.

```
$ tftp
tftp> connect yourhost
tftp> get /etc/passwd tmp
Received nn bytes in nn seconds
tftp> quit
$crack < tmp
```

새 버전은 -s 또는 -r 옵션을 통하여 지정된 디렉토리에 대한 화일 전송을 제한할 수 있다.

(3) 전자우편(Electronic Mail)

몇몇 버전들은 보안상 문제점을 갖는 것으로 지적되었다. 실제로 전자우편이 갖는 오류는 1988년 Seely나 Spafford에 의한 인터네트 웜 사건에 이용되었다. 따라서 운영자는 전자우편의 버전 확인 및 신중한 설치를 고려해야 한다.

(4) Finger

fingerd에서도 오류가 발견되었고 역시 인터네트 웜 사건에 이용되었다. 다음과 같은 명령으로 버전을 확인한 후 1988년 11월 이전 버전이면 /etc/inetd.conf 화일을 통해서 fingerd의 수행을 미리 막아야 한다.

```
# strings /etc/fingerd
```

(5) NIS(Network Information Service)

NIS를 수행하는 경우에는 /etc/hosts.equiv, /etc/passwd, 서버의 passwd 화일 map에 대한 철저한 관리를 해야 한다.

(6) NFS(Network File System)

공개키 암호화 방식을 이용하여 보안기능을 고려한 Secure NFS가 SunOS 4.0에서 소개되었으나 키관리에 관한 문제점을 아직 해결하지 못한 것으로 지적되었다. NFS 서버는 /etc/exports 화일을 잘 관리하여 다음과 같이 everyone에게 EXPORT되는 경우가 없도록 해야한다.

```
$ showmount -e sapphire
export list for sapphire:
/usr/bin/X11            (everyone)
/usr/lib/X11            (everyone)
/usr/include/X11        (everyone)
```

4.3.3 네트워크 보안 감시 대책

네트워크 보안에 대한 감시 및 추적은 계정

및 화일시스템보다 더 어려운데 그 이유는 침입자의 침입방법이 훨씬 다양하기 때문이다. UNIX에서 사용되는 네트워크 감시를 위한 편리한 프로그램 및 설비를 소개하도록 한다.

(1) syslog 설비

이 설비는 명령어들에 대한 오류 메세지와 정보 메세지를 기록할 수 있도록 한다. 전형적으로 오류 메세지는 /usr/adm/messages 화일에 기록된다. syslog 설비를 위한 제어화일은 /etc/syslog.conf 화일이다.

(2) netstat 명령어

다양한 네트워크 테이블을 검사하는데 이용된다. -a 옵션을 줄 경우 현재의 모든 네트워크 연결의 리스트를 출력한다. -r 옵션을 줄 경우에는 라우팅 테이블의 내용 즉, 현재 알려진 모든 네트워크 루트를 출력한다.

(3) etherfind

etherfind 명령은 ethernet상의 모든 패킷을 읽어들인다. 일반적인 경우에는 ethernet 주소에 따라서 패킷을 filter하여 해당되는 패킷만 읽어들이지만, promiscuous 모드에서는 모든 패킷을 읽어들일 수 있다. 그러므로 사용자가 지정한 filter에 따라서 원하는 패킷을 읽어들이고 내용을 분석할 수 있다.

(4) TCP Wrapper

Wrapper의 기능은 크게 두가지로 나누어지는데 첫째, 인터네트 서비스에 대한 요구를 기록할 수 있고 둘째, UNIX 시스템에 대한 접근제어 메카니즘을 제공한다.

(5) Sniffer™/Lanalyzer™

패킷 수준에서의 네트워크 트래픽 감시는 Sniffer™, Lanalyzer™ 등의 상용 프로그램에 의해서 가능하다. 몇가지 UNIX 버전은 트래픽 감시 기능을 패키지로 제공하는데 여기에는 SunOS의 NIP(Network Interface Tap), ULTRIX 4.x의 Packetfilter, 4.3.BSD-Reno의 Berkeley Packet Filter 등이 있다.

(6) 방화벽(Firewall) 시스템

방화벽시스템은 인터네트에 접속한 가입기관의 내부 도메인 네트워크를 보호하기위한 방법으로, 외부네트워크와 접속하는 게이트웨이 시스템을 단지 하나만 두고 그 시스템에서 인증을

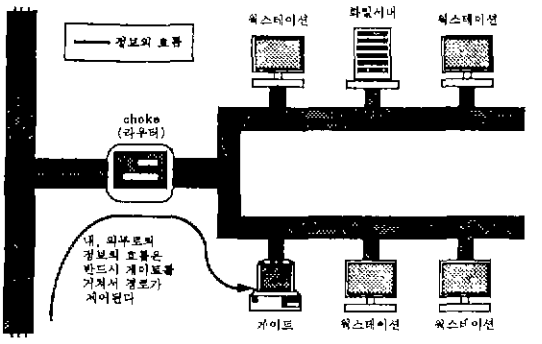


그림 7 방화벽 시스템

표 3 방화벽 시스템 제품들

제품명	기능	비고
InterLock (ANS CO+RE System)	telnet, ftp, SMTP Gateway, X-window, NNTP 응용 접근제어, logging, 사용자인증, 트래픽암호화 등	상용
Eagle Network Security Management System (Eagel Network Security)	시스템인증, monitoring, tracing, real time event reporting, audit log, 사용자인증 등	상용
Internet Firewall Toolkit (Trusted Information Systems)	ftp, telnet, rlogin, NNTP Proxy service, SMTP Gateway, 사용자인증, TCP 접근제어 등	공개
Texas TAMU (Texas TAMU Univ.)	router filtering, screen	공개
Karlbridge (Ohaio Univ.)	PC-based router filtering kit	공개

받아야만 내부 외부로의 접근을 허용하는 시스템이다.

(그림 7)이 보이는 방화벽 시스템은 내부 도메인의 전체적인 보안 관리 이외에 정보 흐름 제어, 경로 제어, 사용자 인증, 감사 기록 등의 기능을 수행한다.

방화벽 시스템을 구성하는 제품은 (표 3)과 같다.

5. 결 론

본 논문에서는 UNIX의 보안연구동향 및 보안운영체제의 기본 개념 그리고 UNIX의 보안기능 및 그 대책에 대해서 살펴보았다. 현재 일반적으로 사용되고 있는 UNIX 시스템인 SVR 4.0이나 BSD 4.3 그리고 SunOS 5.0 등은 TCSEC의 C1 또는 C2급에 해당되며 보안기능에 있어서는 극히 미약한 것으로 판단된다. 따라서 시스템 운영자는 세밀한 보안대책을 세우고 정

기적인 시스템 감시를 통하여 보안을 유지하도록 노력해야 하겠다. 한편 USL에서 개발된 SVR 4.2 ES/MP 등의 보안 UNIX는 ACL, 보안등급, 감사기능 등을 포함하여 B2급정도로 평가받고 있으며, 표준화된 보안기능을 탑재한 보안 UNIX 시스템들이 속속 등장할 전망이다.

기존의 운영체제 시장은 워크스테이션급에서 UNIX를 중심으로 대형 기종에서는 VM, MVS 등을 중심으로 그리고 소형 기종에서는 MS-DOS 등의 다양한 운영체제를 중심으로 편성되어 있었다. 그러나 하드웨어의 성능향상은 워크스테이션급과 소형 기종의 컴퓨터에 사용되는 운영체제의 시장충돌을 야기하게 되었고 기존의 UNIX 개발자들은 여러가지 버젼으로 나누어진 UNIX를 표준화시킬 필요성을 인식하게 되었다. 현재 표준화되고 있는 UNIX는 본 논문에서 살펴본 바와 같이 보안기능을 탑재하여 개발되고 있으며 곧 국내 사용자들도 보안 UNIX를 사용할 수 있게 될 것이다. 그러나 국내의 보안운영체제 연구는 아직 미흡한 실정이며 이들 상품에 대한 평가기준조차도 제대로 마련되어있지 않은 것으로 판단된다. 따라서 국내에서도 보안운영체제의 분석 및 평가를 위한, 나아가서는 개발을 위한 표준체계의 확립이 필요하다고 본다.

참고문헌

[1] Tom Duff, "Viral Attacks On UNIX System Security," USENIX-Winter 1989, pp. 165~171.

[2] Datapro, "An Overview of Secure UNIX," Datapro Reports, May 1990.

[3] Steve Bunch, "Security On UNIX Systems." UNIX Review, Vol. 10, No.3, pp. 39~48.

[4] Matthew S. Hecht, "Experience Adding C2 Security Features to UNIX," USENIX-Summer 1988, pp. 133~146.

[5] F.T. Grampp, R.H. Morris, "UNIX Operating System Security," AT&T Bell Lab. Technical Journal, Vol. 63, No. 8, Oct 1984, pp. 1649~1672.

[6] Mark Funkenhauser, R.C. Holt, "B1 TUNIS: A Kernel for a Secure UNIX System,".

[7] Robert Morris, Ken Thompson, "Password Security: A Case History," Communications of the ACM, Vol. 22, No. 11, Nov 1979, pp. 594~597.

[8] Department of Defense Computer Security Center, "TCSEC: Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, Dec 1985.

[9] David A. Curry, "UNIX System Security," Addison-Wesley, 1992.

[10] Simson Garfinkel, Gene Spafford, "Practical UNIX Security," O'Reilly&Associates Inc., 1991.

[11] Charles P. Pfleeger, "Security in Computing," Prentice Hall, 1989.

[12] Rik Farrow, "UNIX System Security by Rik Farrow," Addison-Wesley, 1991.

[13] John McLean, "The Specification and Modeling of Computer Security," IEEE Computer, Jan 1990, pp. 9~16.

[14] Neil A. Waldhart, "The Army Secure Operating System.".

[15] Roger R. Schell, "Security Kernel Design and Implementation: An Introduction," IEEE Computer, Jul 1983. pp. 14~22.

[16] Carl E. Landwehr, "The Best Available Technologies for Computer Security," IEEE Computer, Jul 1983, pp. 86~100.

[17] Guy-L. Grenier, Richard C. Holt, "Policy VS Mechanism in the Secure TUNIS Operating System,".

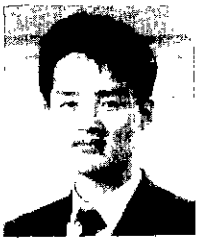
[18] Jerome H. Saltzer, "Protection and the Control of Information Sharing in Multics," Communications of the ACM, Vol. 17, No. 7, Jul 1974, pp. 388~402.

[19] M.S. Hecht, "UNIX without the Superuser.".

송 주 석

1976 서울대학교 전기공학과 (공학사)
1979 한국과학원 전기전자과 (석사)
1988 Univ. of California at Berkeley 전산과학과(박사)
1979 ~1982 한국전자통신연구소 전임연구원
1982 중앙전기주식회사 개발자문
1983 ~1985 Univ. of California at Berkeley Teaching Assistant
1985 ~1988 Electronic Research Lab Research Assistant
1989 ~1989 Naval Postgraduate School Assistant Professor
1989 ~1992 연세대학교 전산과학과 조교수
1992 ~현재 연세대학교 전산과학과 부교수
관심 분야 : B-ISDN, 컴퓨터 보안, 컴퓨터 네트워크, 프로토콜 엔지니어링

권 태 경



1992 연세대학교 전산과학과 (이학사)
1993 ~현재 연세대학교 전산과학과 석사과정
관심 분야 : ISDN, 컴퓨터 보안, 컴퓨터 네트워크, 암호학