特輯

UNIX 운영체제에서의 정보보호

趙 福 來
三 星 電 子 (株)

Ⅰ. 서론

국내 중형 컴퓨터 시장을 관찰하면 UNIX 운영체제의 시장점유율이 꾸준히 높아지고 응용분야도 넓어지는 것을 알 수 있다. 중형 컴퓨터란 개인용인 워크스테이션과 메인프레임 컴퓨터 사이의 중간 규모의 컴퓨터로서 작은 규모의 데이타처리나 워크스테이션 서버로 역할하는 컴퓨터를 가르킨다. 주전산기를 비롯하여 요즈음 출현하는 중형컴퓨터가 운영체제로 UNIX를 채택하는 이유는 운영체제의 소스코드를 저렴한 비용으로 도입할 수 있고, 바로 그 덕분에 높아진 시장점유율 비중에 힘입어 개방화 환경을 주도했기 때문이다. 따라서 신규업체에서 UNIX 운영체제를 선택함은 거의 필연적이었다.

원래의 UNIX 운영체제는 프로그래머의 생산성을 극대화하도록 개발되어 정보보호나 보안 측면에서는 부족한 환경을 가졌다. 프로그래머의 생산성은 기존 코드의 재사용 정도와 밀접한 관계가 있으므로, 서로의 파일을 공유하는 것을 규제하는 보안 특징은 거의 불필요한 것이었다. 그러나 UNIX 운영체제가 탄생지인 Bell 연구소로부터 외부의 대학이나 정부기관에 설치되면서 정보보안, 사생활 (privacy) 보호가 중요하게 되었다.

UNIX 운영체제가 세상에 퍼지면서 많은 특징들이 부가되었다. 이런 특징은 주로 원격 로그인, 전자우편, 파일전송, 넷워크 파일시스템 (NFS)등의 넷워크 연결성과 정보공유에 관련된 것이었다. 정보공유 특징은 각종 유틸리티의 폭발적인 증가를 가져왔고 동시에 여러가지 변종을 수반하여 정보보호가 용이한 환경으로 통제하는 것이 어렵게 되었다. 이런 추세는 마침내 1988년 미국에서 인터넷 웜 (Internet Worm)이라는 자기복제 프로그램이 넷워크 상을 돌아다니면서 자기 자신을 마구 복제하여 넷워크상의 수많은 컴퓨터가 일시적으로 기능을 상실하게 하는 사고를 낳았다.[1] 이 사건은 정보보호의 기능에 대해 주목하게 하였다.

미국 국방부는 오렌지북으로 통칭하는 비밀보장 컴퓨터 시스템 평가기준서(Trusted Computer System Evaluation Criteria, 이하 TCSEC)를 발표하고, 이에 근거한 등급이 정부기관의 기밀자료 처리용 컴퓨터에 필수 사항이 되었다. 민간 수요에서도 기밀보호능력은 대단히 중요한 특징으로 인식되었다. 그러나 원래의 UNIX 운영체제는 의미있는 등급을 받지 못했으므로 보안기능을 갖는 부가적인 패키지를 개발하는 것이 시급한 일이었다. 보안 패키지는 적절한 보안정책을 보조하고 침입이나 민감한 정보의 접근에 대한 일지를 남기는 기능을 제공하여 사후에 추적을 용이하게 하였다.

정보보호기능 측면에서 UNIX 운영체제는 등급이 없는 종래의 것과 (예를 들면 SVR 3.2, BSD 4.2) 운영체제의 핵심부분에 보안기능이 탑재된 최근의 것으로 (SVR 4.2나 이와 대등한 UNIX 운영체제) 나눌 수 있다. 보안기능이 탑재된 운영체제는 종래의 UNIX 운영체제가 지녔던 단순성을 넘어섰기 때문에 적절한 시스템 관리용 패키지의 도움을 받는 것이 필요하다. 이런 패키지는 운영체제와 묶여서 제공되기도 하는데, 개방 환경에 적응하기 위해서는 미들웨어로 제공하는 것이 바람직하다.

이 글에서는 종래의 UNIX 운영체제와 최신 운영체제의 기밀보장 기능, 시스템관리용 패키지에 대해 간략히 소개한다.

Ⅱ. 평범한 UNIX에서의 정보 보호

이러한 주제로는 참고문헌 [2,3] 에 잘 정리되어 있다.

1. 파일의 접근허가

UNIX 운영체제에서 시스템의 다운과 부트를 거쳐도 살아남는 (persistent) 자원은 파일시스템 인터페이스를 통하여 사용하게 된다. 파일 시스템의 각 파일들은 소유자, 그룹(owner, group)의 소유상황과 접근허가(access permission)를 포함하는 속성표를 가진다. 시스템의 자원을 사용하는 주체는 운영체제에서 사용자 번호와 1개이상의 사용자 그룹번호를 가진 프로세스로 표현된다. 파일의 허가방법은 사용주체별로 owner, group, other 로 구분되며 사용주체에 대해 독립적으로 읽기/ 쓰기/ 실행시키기 (read/ write/ execute)에 대해 표시되어 있다. 프로세스의 권한은 (privilege) 시스템관리자와 일반 사용자로 나뉘어 있다. 시스템 관리자 권한은 파일의 허가속성을 초월하므로 임의의 파일에 대해 읽기/쓰기가 가능하다. 다만 실행은 파일의 유형과 관계가 있으므로 초월하지 않는다. 일반 사용자에 대해서만 파일에 적힌 허용치 속성이 의미가 있고 다음과 같이 해석한다.

- 사용자 번호와 파일의 owner번호가 같을 경우
  : 파일의 속성중 owner에 해당하는 허가값을 하여 결정한다.
- 사용자가 가진 그룹번호중 한개가 파일의 group 번호와 같을 경우
  : 파일의 속성중 group에 해당하는 허가값을 사용하여 결정한다.
- 위의 두경우에 해당하지 않을 경우에는
  : 파일의 속성중 other에 해당하는 허가값을 사용하여 결정한다.

파일의 속성중 허가값은 소유자만이, 파일의 소유자 표시는 시스템 관리자만이 바꿀 수 있다. 파일의 유형은 맨처음 생성될 때 고정되어 바뀌지 않는다.

사용자가 불가피하게 시스템 관리자의 권한이 필요하게 되는 경우는 특정방법의 특정 기간에 대해서만 허락할 수 있도록 하고 있다. 특정 프로그램을 실행시키면 그 프로그램이 시스템관리자 권한을 가지게 하는 방법이다. 이런 것을 표시하는 파일 속성을 set-uid, set-gid라고 하며, 실행시에 파일의 owner, group과 동일한 권한을 가지게 된다. 이런 특징을 이용하는 것은 시스템 관리자만이 접근할 수 있는 각종 시스템 자원을 사용하는 프로그램들이다. 예를 들면 모든 사용자의 패스워드를 담는 파일은 특정한 방법으로만 변경이 되야하므로 보통 사용자는 접근을 제한하고 있는데, 사용자가 자신의 패스워드를 고치고자 한다면 불가피하게 그 파일을 수정할 수 있는 권한을 부여해야 한다. 그러므로 패스워드를 고치는 프로그램은 특정한 방법이 구체화된 것으로 생각할 수 있다.

파일의 허용속성은 디렉토리에 대해서는 별도의 의미를 가지는데 실행시키기는 탐색(search)허용, 즉 디렉토리 안의 파일들의 경로(path) 해석을 허용할 것인지를 나타낸다. 허용속성중 set-uid, set-gid중 other에 해당하는 것으로 sticky bit라고 하는데 디렉토리에 대해 이것이 설정되면 그 디렉토리 아래에 있는 파일들의 제거는 그 파일의 owner만이 가능하다. 만일 set-gid가 설정되면 디렉토리 아래에 생성되는 파일의 group 값을 디렉토리와 같게 하거나 사용자의 첫번째 group 번호로 붙이게 된다. (UNIX 운영체제마다 다름)

사용자가 파일을 생성할 때 매번 프로그램내에서 통제하지는 않으므로 (화면 출력을 파일로 만드는 경우) 사용자의 파일허용치 속성 설정 정책을 뒷받침하는 수단으로 umask라는 기능을 제공한다. 이것은 사용자가 파일을 생성할 때 디폴트 값을 가지도록 하는 것이다.

2. 파일이 아닌 자원의 사용

시스템의 모든 자원이 파일 시스템의 파일로 표시되는 것은 아니다. 이런 자원에 대해서는 각각 고유한 방법으로 제한과 보호를 하도록 되어 있다. 시스템 자원중 처리기의 사용시간, 메모리의 사용량, 생성할 수 있는 파일의 최대치를 제한하여 한 사용자가 시스템의 정상적인 운영을 손상시키지 못하도록 할 수 있다. 2프로세스간의 통신을 담당하는 메시지나 공유메모리는 자원의 허용 방법을 파일과 동일한 방법으로 정의하여 사용한다. 파일의 속성을 보여주는 명령에 대응되는 명령어를 별도로 준비하여 현재의 허용치를 볼 수 있도록 하여준다.

프로세스간이 통신의 일종인 signal의 접수는 owner가 같거나 보내는 쪽이 시스템 관리자 권한을 가질 때에만 허용하여 보통 사용자가 다른사용자의 작업을 방해하지 못하도록 보호를 한다. 또한 프로세스를 묶는 그룹개념이 있어서 어떤 단말기에서 기원

하는 모든 프로세스에 동일한 signal을 전달하는 기능이 제공되어 무의미한 프로세스의 실행을 막는 장치가 있다.

3. 패스워드 (password)

UNIX 운영체제에서 패스워드는 사용자가 컴퓨터와 접속을 시작하는 로그인 절차에서 반드시 필요한 것이다. 어느 사용자의 패스워드를 안다는 것은 그 사용자가 가지는 권한을 완전히 얻는 것이므로 패스워드의 보호는 보안의 핵심 사항이 되는 것이다. 사용자의 패스워드는 암호화하여 일반 사용자가 덧쓰는 것이 금지된 시스템 파일에 저장한다.

사용자가 기억할 수 있는 패스워드의 어휘수는 매우 제한되어 있다. 그러므로 아무리 정교한 암호화 기법을 사용하더라도 사용자가 선택할 법한 패스워드의 후보를 시험한다면 결국은 패스워드가 알려질 가능성은 대단히 높다. 패스워드의 유효성 시험을 제한하여 패스워드 누출을 지연시키는 것이 필요하다.

암호화된 패스워드를 감추어서 반드시 시스템에서 제공한 명령어 (login, su 명령어)만이 암호화된 패스워드를 접근하도록 한다. 이런 이유는 패스워드의 암호화 기법은 너무 많이 알려져서 패스워드를 추측하는 프로그램에 암호화된 패스워드를 입력하면 강력한 컴퓨터에서는 단시간에 패스워드를 알아낼 가능성이 많다. 또한 시스템에서 제공한 명령어는 계속되는 실패에 대해 기록을 남겨서 패스워드를 깨려는 행위에 대처할 수 있게 한다. (Shadow Password)

패스워드가 알려질 가능성은 패스워드의 사용기간에 비례하므로 정기적으로 패스워드를 바꾸는 것이 바람직하다. 그러므로 주기적으로 패스워드를 바꾸게 하며, 일단 변경된 패스워드를 어느 기간 내에는 바꾸지 못하게 막아서 사용자가 원래의 패스워드로 한번 더 바꾸는 것을 방지한다.

패스워드가 사전에 나오는 단어나 사용자 로그인 이름과 밀접한 관계가 있으면 추측하는 것이 용이하다. 그런데 패스워드를 추측하기 어려운 무의미한 글자의 나열로 만드는 것은 기억하기 어려울 뿐만 아니라 만들기도 어렵다. 이런 문제를 해결하기 위해 시스템 스스로 기억할 수 있는 - 대개 발음이 쉬운 - 무의미한 단어를 만들어 사용자가 선택하게 하는 기능을 제공하는 것도 있다.

시스템 관리자의 패스워드의 누출은 치명적인 위협이다. 그런데 직접 시스템 관리자의 패스워드를 알아내는 것은 어려우나, 시스템내의 사용자중 한사람의 패스워드를 알아낼 수 있는 확률은 매우 크다. 일단 시스템의 정상적인 연결이 가능해지면 시스템관리자의 패스워드를 알아냄이 없이도 시스템관리자와 동일한 권한을 행사할 방법을 강구할 가능성이 생기게 된다. 패스워드를 깨는 프로그램을 (Password Cracker)이용하여 패스워드의 견고성 시험을 하는것이 필요하다.

시스템 관리자의 권한을 얻기 위한 수단은 login 때부터 시스템 관리자로 로그인하는 압법과 일반사용자로 로그인하였다가 su 명령어를 이용하여 권한을 획득하는 방법이 있다. 대개는 su 명령어를 사용하는 것이 바람직한데 그 이유는 login은 로그인 절차를 위조하는 프로그램에 의해 부지불식간에 패스워드가 탄로날 가능성이 있으며, 두사람 이상의 시스템 관리자가 있는 경우에 실제의 사용자가 구분이 되지 않는 문제가 있다. su 명령어도 여러 사람이 모두 시스템 관리자 패스워드를 알아야 하므로 - 아무래도 비밀이 샐 가능성이 높다 - 자신의 패스워드를 쳐서 시스템 관리자 권한을 획득하도록 하는 것이 바람직하다. 직접적으로 시스템관리자로 로그인 하는 것은 보안을 위해 미리 지정된 단말기에서만 가능하도록 제한하는 기능이 대개의 UNIX 운영체제에 포함되어 있다.

4. 시스템 구동상태의 감시

간접적으로 시스템 정보 보안과 관련이 있는 것으로 시스템의 동작상태를 감시하는 명령이 있다. ps 명령어를 치면 시스템에서 구동중인 프로세스에 대한 기초적인 정보가 나타난다.

이 정보로 시스템의 보안 상태에 대해 간접적인 상태를 알수 있다. 넷워트가 연결된 시스템에서는 넷워크마다의 고유 명령어로서 시스템 사용현황을 보여주는 기능이 있다. 예를 들면 TCP/IP 넷워크에서는 netstat 명령어로 불법적인 연결을 상당수 발견하고 추적할 수 있다. 시스템 관리자는 몇몇 UNIX 운영체제에서는 의심스러운 프로세스에 대해 실행중인 프로세스의 이미지를 검사하는 방식으로(crash 명령) 거의 완전한 조사를 실시할 수 있다.

5. 시스템 로그

UNIX 운영체제는 사용자가 시스템에 연결된 상황을 기록하고 있다. 연결 시작, 종료 시각, 연결한 단말기나 넷워크 주소등을 기록하고 있어서 특정 시간

에 시스템을 사용하던 사용자의 명단을 작성할 수 있다. 프로세스 단위로 기록을 남기는 기능도 제공된다. 이 기록에는 사용자가 실행시킨 명령어와 명령시의 권한상태 실행시각, 종료시각, 시스템 자원사용량 등을 담고 있다. 이 기록은 보안 침해가 발생했을 때 추적의 실마리를 제공해준다.

시스템은 특권 상황의 변화를 반드시 콘솔에 표시하고 있다. 즉 시스템관리자로의 로그인 시도나 다른 사람의 권한을 이전받는 su 명령어의 시도는 그 결과와 함께 콘솔에 표시된다. 이런 표시는 하드카피를 가진 콘솔에서는 물리적인 침입이 없는한 보존이 되는 정보이다. 콘솔로의 출력과 동시에 이것을 파일로 만들어 손쉽게 조사할 수있다. 관심이 있는 사건만을 요약할 수 있다.

6. 넷워크에서의 고려사항들

TCP/IP 넷워크 기능은 UNIX 운영체제와 더불어 상승작용을 일으키며 발전했다. 사용자에게 넷워크에 투명한 자원접근을 허락하고자 시도하는 것들은 대개 보안 측면에서 위험성이 있다. 예를 들면 telnet은 항상 사용자에게 로그인하는 절차를 거쳐 사용자의 신원을 확인하지만 rlogin은 셋업 환경에 따라 이런 절차를 우회한다. 이런 우회는 신뢰가능한 호스트(trusted host)라는 전제가 반드시 필요하다. 이런 기본전제가 불확실한 넷워크 환경에서는 침입자가 신뢰가능한 호스트의 고장시에 이것을 흉내냄으로써 (spoofing) 보안이 무너지게 될 가능성이 있다. 반면 항상 패스워드를 묻는 절차를 가지는 것은 넷워크에서 통신 패킷을 도청함으로써 탄로가 날 가능성이 있다. 그러므로 넷워크에서의 보안은 일단 물리적인 보호가 없이는 근본적으로 불안하게 된다. (이점은 넷워크에만 적용되는 것은 아니나, 넷워크에서는 정보 누출시에 흔적을 발견하기 훨씬 어렵다.) 넷워크 자체의 보안은 운영체제만으로 해결되는 것이 아니고 넷워크 전용장비를 포함한 다른 차원의 문제이다.

넷워크 기능은 적절히 구성할 (configure) 때에는 비교적 정보보호가 가능하다. 적절한 구성은 정확한 사양이 없이 자연적으로 진화된 소프트웨어에서는 사실상 확인되기 어려운 일이다. 그러므로 오류아닌 오류가 발생할 가능성이 항상 있다. 넷워크에 참여하는 시스템들을 일관되게 제어하기 위한 패키지로 NIS (Network Information System)등을 사용하기도 한다. NIS가 주행중인 시스템은 패스워드등을 일관되게 관리하므로 NIS가 없을 때와는 정보 보안측면에서 시스템 파일들의 의미가 달라지게 된다. NIS는 충분한 훈련과 경험이 없으면 보안을 포함한 운영이 용이하지는 않으므로 기능의 제공을 위해 보안을 제쳐 놓는 경우가 많다. 넷워크 기능은 시스템 관리자가 복수화로 되는 것이 보통이므로 시스템 관리자들 사이의 원활한 의사소통을 지원하는 것이 필요하다. 간단히 말하면 이른바 적절히 구성하는 것은 정확한 훈련과 시행을 의미한다. 넷워크 기능은 침입에 대비한 보안확인 절차를 주기적으로 반복하는 것이 필요하다.

7. 모뎀과 원격단말

단말기의 통신선로가 모뎀(modem)을 이용한 전화선으로 구성된 것을 원격단말이라 하자. 원격단말은 물리적으로 보안이 보장되는 RS-232 선로를 물리적 특성이 불확실한 전화선으로 연결한 것이다. 그러므로 원격단말 기능에는 물리적인 보안기능을 보조하는 장치가 필요하다.

전화선이 통신장해로 선로가 끊길 때, 해당되는 연결을 반드시 제거하고 선로를 초기화시키는 데몬 프로세스의 보호가 필요하다. 이 데몬 프로세스는 원격단말에 대해 상황을 엄격히 해석하여 미리 지정된 시간동안 데이타를 주고받지 않으면 선로의 장애로 판단하는 것이 보통이다. 연결가능한 전화를 제한하여 아무나 시스템에 연결을 시도하는 것을 방지하는 수단으로 이른바 콜백(call-back)기능을 사용하는 것이 바람직하다. 사용이 허가된 곳의 전화번호를 기억하고 연결요청이 있으면 시스템으로 직접 로그인을 허용하는 것 대신에 시스템이 그 곳으로 전화를 다시 거는 방법이다. 이 방법으로 전화선의 물리적인 취약성을 극복하더라도, 여전히 보안에 위협이 되므로 원격단말을 통한 모든 연결은 시스템에 기록을 남기는 것이 필요하다. 원격단말을 허용하는 시스템에서는 더욱더 패스워드의 보안관리가 절대적이다.

8. 파일 시스템 점검

UNIX 운영체제에는 find라는 명령어가 있어서 파일시스템의 모든 파일을 차례로 순방하면서 시험할 수 있는 기능이 있다. 이 명령어는 시스템 보안에 위협이 되는 불법적이거나 무의미한 파일들을 찾는 목적으로 쓰인다. 불법적인 파일의 예로는 보안의 위협이 될 수있는 set-uid, set-gid된 것이나, 사용자 번

호가 등록되어 있지 않은 파일들이 있다. 또한 시스템 관리정책상 금지된 각종 초기화 파일을 찾아 내는데 사용된다.

시스템 명령어, 라이브러리등의 시스템 파일들에 대해서는 불법적인 변경사실을 파악하기 위해 주기적으로 전체 리스트를 만들어 변화가 있는가를 조사한다. 시스템 디렉토리는 반드시 시스템 관리자만이 변경가능한가를 검사해야 한다

파일시스템의 점검은 cron 데몬 프로세스에 의해 주기적으로 행해지며 그 결과는 시스템 관리자에게 보고된다. 파일시스템의 이상을 발견했을 때, 파일시스템의 복구를 위해 백업도 주기적으로 만든다.

Ⅲ. 보안 등급이 있는 UNIX 운영체제

정보보호의 등급을 논의하는 틀로 미국 국방부의 비밀보장 컴퓨터 시스템 평가서 (TCSEC)를 많이 사용한다.[4] 비밀보장 기능은 대개 운영체제 커널에 구현되므로 TCSEC에서 말하는 비밀보장은 보안이 가능한 운영체제 (secure OS)를 나타내는 것으로 해석한다. 앞 절에서 보였듯이 종래의 UNIX운영체제에서도 다수사용자(multiuser) 시스템으로 적절한 구성 유지만으로 나름대로 보안기능이 있다. 그런데도 별도의 보안기능 탑재가 요청되는 것을 이해하기 위해서는 TCSEC에서 제시한 평가기준의 의미를 아는 것이 긴요하다.

1. 보안의 근본 조건

TCSEC는 컴퓨터 보안의 근본 조건을 다음과 같이 말한다. 안전한 시스템은 특정한 보안장치를 통해 정보접근을 통제하여 인가된 주체 (사람이나 그를 대신하는 프로세스) 만이 정보에 대해 읽기/쓰기/만들기/없애기 정보접근 권한을 가진다. 안전한 시스템을 이루는 조건은 6가지가 있는데 항목중 네개는 정보접근 통제에 필요한 것을 다루며, 나머지 두개는 비밀보장 컴퓨터에 대한 신용보증을 다루고 있다.

항목 1. 보안정책 (Security Policy) :

시스템은 비밀취급(security clearance) 허가자에 한해서 민감한 정보 취급을 허용하는 위임보안정책과 (mandatory security policy) 임의로 선정된 자에게만 정보 취급을 허용하는 임의보안정책을(discretionary security policy) 시행할 수 있어야 한다.

항목 2. 표지 (Marking) :

위임보안정책에 따른 접근통제표(access control label)를 모든 정보객체에 붙일수 있어야 한다.

항목 3. 신원증명 (Identification) :

정보접근 주체가 구분되며 각각의 주체마다 인가된 비밀등급은 표시된다. 이것을 담는 정보는 안전하게 보관되야 한다.

항목 4. 책임 (Accountability) :

감사(audit)정보는 선택적으로 기록되고 변조로부터 보호되어 보안에 영향을 주는 행위는 책임자까지 추적할 수 있어야 한다.

항목 5. 보증 (Assurance) :

항목 1에서 항목 4까지의 조건이 시행되도록 하는 통제장치가 문서화되어 위의 항목들에 대한 구현이 충분한가를 독립적으로 검증할 수 있어야 한다.

항목 6. 끊임없는 보호 (Continuous Protection)

위의 다섯가지 항목이 하드웨어와 소프트웨어의 (비인가된) 변형에 대해서도 시스템의 수명이 다할 때까지 보호받아야 한다.

2. 보안 등급

위의 여섯가지 항목으로 평가하여 비밀보장등급은 4단계(division), 7등급으로 (class)으로 나눈다. 보장 능력이 약한 순서로 단계는 D, C, B, A로 되며 등급은 1, 2, 3의 번호로 나간다. D 단계는 최소보호(minimal protection)으로 표시되며 실제적인 의미 보다는 등급분류상 C, B, A의 어느 등급도 만족할 수 없음을 표시하는 것이다. A 단계는 B 단계의 최고등급이 입증되었음을 나타내는데 입증된 설계(verified design)로 표현되는 A1 등급 만이 있다. C, B 단계의 각 보안등급의 주요 특징을 하위단계에 없는 것만으로 요약하면 아래와 같다.

C1 등급, 임의보안 보호 (Discretionary Security Protection) : 보안정책으로 사용자가 특정한 사용자를 지정하여 정보공유를 통제하는 장치가 있고, 책임조건으로 패스워드로 신원증명(authen-ticate)하며, 보증조건으로는 (운영체제 안에 보안기능이 구현되었다면 운영체제가) 변형되지 않음과 시스템의 동작에 대한 설계문서와 동작을 설명하는 문서가 있어서 그 문서대로 동작해야하며, 별도의 문서로 시험방법와 기밀보장기능의 매뉴얼이 있어야 한다.

C2 등급, 통제된 접근 보호(Controlled Access

Protection) : 정보에 대한 접근 허용값이 인가된 자에 의해서만 지정되며 접근통제를 한사람 단위로 포함/배제하는 접근통제외에 저장장치가 재사용될 때에는 재사용전의 데이타를 파괴하며, 책임조건의 구현으로 피보호 정보에의 접근에 대한 감사기록의 생성, 유지와 변형방지및 부정접근방지 기능을 가져야한다.

B1 등급, 꼬리표 보안 보호(Labelled Security Protection) : 기밀등급을 표시하는 꼬리표를 지니며 이것으로 위임보안통제를 한다. 위임보안통제에서는 계층적 비밀서열로는 (hierarchical classification) 취급주체의 서열이 정보객체의 그것 이상이며, 비계층적 비밀범주로는 (non-hierarchical category) 취급주체의 여러 개의 비밀범주 중 하나가 정보객체의 비밀범주와 같아야 한다.

B2 등급, 구조화된 보호 (Structured Protection) : B1 등급의 형식화된 보안모형이 문서화되어야 하며 시스템 관리자에게 비밀보장 관리 기능이 제공되고 신원보증이 강화되어 비교적 침투가 어렵다. 간접적인 수단으로 시스템의 동작을 염탐하는 코버트통로(Covert Channel)에 대한 분석이 있어야 한다.

B3 등급, 보안 영역(Security Domain) : 보안등급이 달라질 때에 비밀보장통신로(Trusted Communicaion Path)로 연결되는 기능 등이 있어야 한다.

3. 보안 패키지

C2 등급의 보안기능은 주요 UNIX 운영체제에서 이미 지원하고 있다. C2 등급에서는 민간함 자원에 대한 감사자료의 생성과 임의접근 통제 일람표 (discretionary access control list) 기능의 지원으로 요약되고 있다. SVR 3.1, HP-UX, SUN OS 4.x, SCO XENIX 등에서 부가패키지로 제공하는 것으로 알려져 있다.[5,6,7]

B1 등급은 C2 등급의 접근통제방식의 차이가 주요한 것인데 이를 지원하는 것으로 SVR 3.1에 MLS라는 이름으로 제공하고 있다. B2 등급은 SVR 4.1 ES (Enhanced Security)에서 지원되고 있다. SVR 4.2에서도 포함되어 있다.[5,6]

주전산기 2호기에 대해서 살펴보면 1993년까지 제공하던 SVR 3.2계열에서는 C2 등급 보안패키지의 제공이 가능했었으나 실제로 이것을 개발하지는 않은 것으로 알려져 있다. 1994년부터 제공하게 될 SVR 4.2 에는 B2 등급의 보안기능이 지원된다.

Ⅳ. Administration Package

정보보안이 제공되는 UNIX 운영체제는 규모가 방대해지는 경향이 있다. 보안기능의 유지는 잡다한 일의 연속인 경우가 많다. 한사람이 두대 이상의 컴퓨터를 관리하는 경우도 흔해지고 있다. 또는 대형기종의 경우 여러사람이 시스템 한대를 관리해야 하는 경우도 있다. UNIX 운영체제에는 변종이 아직도 많으므로 서로간의 차이가 있을 수 있다. 또한 정보보안 기능을 이용해야 하는 조직에서는 UNIX 운영체제에 대한 경험이 적을 가능성이 있다. 이런 관리 운영환경을 향상시키기 위한 사용이 용이하며 이미 다른 기종에 사용중인 전문적인 운영관리지원 패키지 도움은 중요하다. 이는 운영체제가 정보보호를 위한 보안 기능이 부족하기 때문에 기능을 보완하려는 의미가 아니라 정보보호에 필요한 노동력이 많이 소요되므로 이를 자동화 한다는 개념으로 파악해야 한다.

대개의 관리운영 패키지에는 정보보호를 위한 수단으로 사용자의 신규등록과 사용중지, 저장된 정보의 백업, 보안기능의 관리등이 포함된다. 시스템의 상태를 모니터하고 사용현황을 보고하는 기능도 포함된다. 주전산기 2호기에의 이식 계획이 발표된 UNICENTER라는 패키지를 사례연구로 삼아 전문적인 시스템 관리 패키지의 기능을 살펴보기로 한다.[8] 이것은 다음의 5가지 분야로 기능이 구분된다.

- 보안,통제,감사 분야 (SCA)

SCA(Security Control and Audit,)는 운영체제에서 제공하는 파일접근허용이나 접근통제 리스트를 무시하고 사용자와 시스템의 자산사이의 관계형 DB를 구성하여 완전한 정책기반 보안관리시스템을 구축했다. 시스템의 자산이란 프로그램, 파일, 단말기와 패키지에서 사용하는 보안관련 명령을 포함한다. 관계형 DB에 보안사항을 저장 하였으므로 파일과 사용자 사이의 관계를 간편하게 조사하고 설정할 수 있다. 파일의 보안은 전반적인 정책으로 존재하므로 파일이 존재와는 상관없이 일관성 있는 접근통제를 이룰 수 있다. 모든 보안장치가 명령어에도 해당이 되므로 슈퍼유저의 특별기능은 통제된다. 접근방식은 읽기, 쓰기, 덧쓰기(update), 지우기(delete), 찾기로 구분된다. 패스워드를 명백한 것은 배제하며 필요시 기계가 패스워드를 생성해주며 패스워드 파일 자체를 파일시스템에서 없애버렸다. 일력 (calendar)

관리로 특정 사용자나 집단에 대해 지정된 시간에만 사용을 허락하도록 할 수 있다. 보안침해 사례뿐만 아니라 동작을 감사할 수 있다. 중요일이나 특정 프로세스와 사용자 계정은 차후에 검사와 평가를 위해 관련된 모든 일이 기록된다.

• 자동화된 스토리지 관리 (ASM)

ASM(Automated Storage Management,)은 디스크의 내용을 두벌이상으로 만드는 백업기능과 디스크의 내용을 다른 매체로 옮기는 아카이브(archive) 기능을 제공하는데 이것은 자동화되고 지능적으로 동작한다. 즉 백업은 하나의 파일에 대해 생성시간, 버전등에 따라 구분하여 여러벌의 백업을 구분하여 처리할 수 있으며 아카이브는 사용자는 눈치 못채게 스토리지의 여유공간에 따라 테이프와 디스크사이로 데이타를 옮기는 기능을 제공한다. ASM의 모티프 그래픽 환경으로 UNIX 운영체제의 파일시스템의 파일을 보여주고 파일의 위치에 대한 목록을 DB로 유지하고 이동을 제어하는 기능이 있다. 백업과 아카이브에서 사용하는 테이프에 대해 테이프에 저장된 데이타의 파기기한을 검사하는 기능이 있어서 보존 연한에 든 테이프에 실수나 고의로 덧쓰는 것을 방지한다.

• 자동화된 생산제어 (APC)

APC(Automated Production Control,)는 터미널을 통하지 않은 작업, 즉 백그라운드 작업을 관리한다. 시스템 콘솔 기능에 대해 각종 시스템 메시지의 표시과 보고기능에 대한 정책을 수립하여 중요한 정보를 쉽게 파악하도록한다. 스풀에 있는 각종 파일의 접근을 용이하게 하는 스풀 기능이 있다.

• 성능운영와 회계 PMA

PMA(Performance Management and Accounting,)는 처리기, 메모리와 입출력장치에 초점을 맞추어 세가지 다른 관점에서의 시스템 성능을 모니터한다. PMA는 회계기능으로 사용한 자원에 대한 비용을 시스템의 처리용량의 변화에 적응하며 변화시키는 기능이 있다. 자원의 사용이력을 수집 분석하여 성장추세를 요약하고 용량증가 계획을 세울 수 있도록 해준다.

• 데이타센터 행정 DCA

DCA(Data Center Administ-ration,)는 시스템 운영진에 필요한 업무 분장등의 행정을 제어하는 수단을 지원한다. 시스템운영중에 발생하는 각종 문제의 분류와 할당, 문제 해결 진척사항 관리를 자동화하도록 한다. 문제 해결의 진척에 따라 재할당, 문제의 위급성등을 상향조정하여 경각심을 높이는 기능등이 포함된다. 업무 분장및 문제해결 진척추적기능은 끊임없는 보안기능 유지에 필요한 요소이다.

Ⅴ. 소프트웨어 오류정정과 보안

일단 기밀보장 컴퓨터 시스템을 구성했더라도 이것을 위협하는 요소로 소프트웨어의 오류를 생각할 수 있다. 오류가 없는 소프트웨어는 없으므로 언젠가는 보안의 헛점이 발견되게 된다. 시스템에 이상이 발견될 때에는 즉각적으로 제작사에 연락을 위하는 것이 필요하다. (보안에 문제점이 발견될 때의 조치사항을 미리 준비해 두는 것이 좋다.) 침입자들 사이에도 정보를 교환하는 것이 보통이므로 자신과 비슷한 환경을 가진 곳에서의 문제점은 언제든지 가까운 시간에 발생할 가능성이 대단히 높다. 보안장치에 대한 정보에 귀를 기울이는 것이 중요하다. 정보입수 방법은 제작사에서 제공하는 소식지나 전자우편, 전자게시판을 이용하는 방법이 있다. 인터넷의 경우 CERT(Computer Emergency Res-ponse Team)에서 제공하는 경고나 주의를 전자우편이나 Usenet News를 통해서도 얻을 수 있다. 우선 comp.security.unix라는 뉴스 그룹을 구독할 것을 권장한다. 그 뉴스그룹에서는 여러기종을 사용하는 사람들의 문제 발생과 해결 경험을 나눌 수 있고, 최근의 잡지, 전자우편 목록등을 얻을 수 있다. CERT는 특정 운영체제에 대한 경고만을 내보내는 것이 아니라, (미국의 경우) 침입자를 발견했을때의 조치사항에 대해 조언을 해준다.

Ⅵ. 결론

UNIX 운영체제는 역사적인 특성으로 보안기능이 충분하지 않았으므로 적절한 보안정책을 세우고 운영체제에 포함된 정보보호 수단을 사용하여 시행하면 어느정도 시스템의 정보를 보호할 수 있었으나 규모와 유연성에서 제한적일 뿐만 아니라 완전하지 못하였다. 그런데도 UNIX 운영체제는 개방적인 특성으로 넓은 분야에서 채용되었다. 대다수가 UNIX가 운

영체제인 시스템으로 구성된 인터넷(Internet)은 시스템의 침입 시도를 왕성하게 하고, 그런 경험의 공유를 손쉽게 하였다. 즉 인터넷은 UNIX 운영체제가 가지던 보안의 헛점을 많이 노출시키는 역할과 동시에 대책을 논의하는 기구를 제공했었다. 이 단련기간을 통해 UNIX 운영체제의 정보보호 능력은 실제 사용에 크게 부족하지 않을 정도가 되었으나, 시스템 관리자의 막대한 유지 노력을 없앨 수는 없었다.

평범한 UNIX 운영체제로는 정보 보안의 원칙에 입각한 정보보호 체계를 만들 수 없었다. 그래서 처음에는 운영체제의 핵심적인 부분인 커널(kernel)에 충분한 구현없이 부가적인 패키지로 제공되는 것에 의존하였다. 즉 침입에 대한 추적기능에 노력을 기울이고, 시스템의 보안에 핵심을 이루는 패스워드의 관리를 철저히하는 방식이었다. 운영체제의 기술이 발전하고 또한 공공기관을 비롯한 수요처에서 보안시스템을 요청하게 되어 보다 발전된 정보보안 기능이 대개의 UNIX 운영체제에 탑재되고 있다.

1994년에는 주전산기 2호기(TICOM)에 이식될 예정인 UNIX SVR 4.2에는 정보보호기능이 기본커널에 탑재되어 있다. UNIX SVR 4.2 운영체제는 그 규모가 방대하여 시스템 관리가 점점 복잡해지며, 또한 주전산기의 성능 향상으로 더 많은 사용자를 지원하게 될 것이 명백하다. 주전산기에 전문적인 시스템 관리 패키지의 이식 노력이 발표되었다. 이런 패키지를 통하여 정보보호를 비롯한 제반 시스템 관리를 생산성과 신뢰성을 높일 뿐만 아니라 여러 기종이 운영되는 기관에서는 시스템 관리의 일관성을 제공하는 미들웨어로서 역할할 것을 기대하고 있다. 상용화된 많은 종류의 UNIX 운영체제중 SVR 4.2와 대등한 수준에 달하는 것으로 생각되는 것은 정보보안에 관한한 어느 운영체제에도 뒤지지 않는 것으로 평가할 수 있다.

이 글에서는 다루지 못했지만, 운영체제와 정보보안에 대한 표준 그룹에서 - POSIX 1003.6과 X/Open SWG - 표준안을 작성하면 정보보안에 관련된 소프트웨어의 이식성이 유지될 것으로 예상한다.

參 考 文 獻

[1] Seely, Donn. A Tour of the Worm, Dept. of Computer Science, Univ. of Utash, December, 1988.

[2] Curry, D., Improving the Security of Your UNIX System, SRI International Report ITSTD-721-FR-90-21, April 1990.

[3] Holbrook, P. and Reynolds, J., Site Security Handbook, RFC-1244, 1991.

[4] National Computer Security Center, "Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, CSC-STD-001-83, NCSC, December 1985.

[5] Unix System Laboratory, Audit Trail Administation UNIX SVR 4.2, UNIX Press.

[6] Unix System Laboratory, Design of Multiprocessing Security Features for UNIX SVR4 ES/MP, 1993, SVR4 ES/MP online document, 1993.

[7] Hewlett Packard, HP-UX System Security, 1991, Hewlett-Packard, HP-part no. B1862-90009.

[8] Computer Associates, CA-UNICENTER Systems Management Solution For The UNIX Environment - for HP-UX Systems.

筆 者 紹 介

趙 福 來

1959年 12月 6日生

1982年 2月 서울대학교 전자공학과 졸업(학사)

1984年 2月 KAIST 전기 및 전자공학과(석사)

1992年 2月 KAIST 전기 및 전자공학과(박사)

1989年 3月 ~ 현재 삼성전자(주) 근무

주관심 분야 : Unix OS, Mass Storage System