□특집□

클라이언트/서버 환경에서의 정보 보안 기술

강 영 일†

◈ 목 차 ◈

1. 서 론

급변하는 컴퓨팅 환경에서 보안상의 문제는 그 중요성이 점점 강조되고 있다. 기업이나 관공서와 같은 공공 단체들도 기밀의 노출이나 자료의 변질 방지에 많은 노력을 하고 있다. 정보 통신 시스템의 광범위한 설치, 보존, 운영에서도 보안 문제가 크게 대두되고 있다. 전자결재나 송금 등의 통신에서 보안성과 함께 정확성도 중요한 요소이다. 이러한 정보 보안 문제는 다음과 같은 정보 통신 환경 변화 때문에 더욱 그 중요성이 강조되고 있다.

(1) 개인 휴대 단말 장치의 사용이 증가한다.
(2) 무선, 이동 통신의 사용이 증가한다.
(3) 원격 단말의 지원이 불가피하게 된다.
(4) 시스템들이 많은 플랫폼에 복잡하게 연결된다.
(5) 인터네트 사용을 공중망으로 해결함으로 공중망에 더욱 의존한다.
(6) 클라이언트/서버 환경이 증가한다.

보안 문제가 기술적인 문제 접근에서 이야기되어 왔으나 이제는 중요한 기업 전략의 일환으로 다루어지고 있다. 기업과 같은 환경에서 비밀 정보의 누설은 곧 기업의 생존과 직결되는 문제이기 때문이다. 보안 시스템에 대한 투자도 날로 증가되고 있음으로 보안 유지를 위한 비용도 증가되고 있다. 보안 문제는 아마추어 해커들의 영웅심이나 호기심의 충족에서 점차 여러 가지 불순한 목적과 동기로 위협받고 있다. 1990년 이후 보안 문제는 점차 전문적이고 지능적인 침입자로 인하여 문제가 되고 있다. 보안상의 문제점은 외부에 알려지지 않고 담당자들이 덮어두는 경우도 많다. 조직의 경영자는 신뢰성이나 고객의 보안 문제로 종종 심각한 침투 파괴 사실을 은폐하려고 한다. 이런 경우 침입자를 보호하고 문제의 근본적인 해결을 어렵게 하는 경우가 많다. 호스트를 중심으로 하는 과거의 업무 체계가 클라이언트/서버 환경으로 변화되면서 보안 문제는 좀더 어려운 문제가 되고 있다. 다수와 다수의 자유로운 연결은 클라이언트/서버 환경이 주는 장점이나 보안 문제는 증가한다. 이러한 관점에서 본고는

† 정회원 : 한국전자통신연구원 부설 정보통신연구관리단 기초전문위원

클라이언트/서버 환경에서 보안상의 문제를 조명하고 이를 해결하려는 여러 시도에 대하여 논하고자 한다.

2. 클라이언트/서버 시스템 보안 문제

주기적인 패스워드의 변경으로 클라이언트/서버 환경에서 보안성이 유지 될 수 있는가? Information Week의 Emst와 Young 클라이언트/서버 시스템의 대부분이 채용하고 있는 UNIX/ NT 사용 현황과 보안 문제를 다음과 같이 보고하고 있다. UNIX/NT 환경은 점차 확산되고 있고 내, 외부 조직에서 이에 접속하려는 기회도 증가하고 있다. 워크 스테이션, 미니급 컴퓨터, LAN 서버, 메인 후레임이 UNIX/NT 환경에 연결되어 사용되고 있다. 반면 UNIX/NT 에 대한 보안의식은 높지 못한 것으로 나타났다. 많은 수의 기업 조직에서 UNIX/NT 환경에서 운영되는 시스템이 호스트를 중심으로 하는 종래의 중앙 집중식 시스템과 동일한 정도의 보안 조치 속에 운영되고 있다. 클라이언트/서버 환경에서 운영되는 UNIX/NT 시스템이 더 높은 보안 대책이 필요하다. 많은 사용자가 UNIX/NT 시스템의 보안 시스템을 잘 이해하지 못하고 있다는 점도 Emst와 Young은 지적하고 있다. 회사와 같은 기업 조직에서 보안 정책이 확고히 되어 있지 않다. 또 보안성 점검도 주먹구구인 경우가 많다. 충분한 시간적인 여유라든가 예산상 보안 시스템의 구축에 드는 비용도 문제이다. 시스템 구축이후 보안 시스팀의 운영능력도 중요한 요소로 지적되고 있다. UNIX/NT의 보안을 관리하는 상용 소프트웨어는 이 경우 많은 도움이 될 수 있다. UNIX/NT 환경에서 지적되는 보안 관계 문제는 조직의 여러 계층 책임자에게 알려져야 한다. 조직의 중간 관리자 계층은 해당조직의 어느 자원이 민감한 비밀인가를 이해하고 있음으로 보안 시스템의 설정과 운영에 효과적인 대응을 할 수 때문이다. 조직의 구성원은 보안에 대한 교육을 받아야 하고 적절한 이행여부도 체크되어야 한다. 최고 경영층은 보안 관계 투자와 인력 배치에 대한 방안을 가지고 있어야 한다.

3. 새로운 위협

클라이언트/서버 시스템에서 보안 설정은 몇 가지 상황변화에 따른 대비가 필요하다고 생각된다. 최근의 경향은 노트북과 같은 휴대형 컴퓨터를 이용한 이동사용자가 증가하고 있다. 다수의 서버와 크라이언트가 지역적으로 멀리 떨어져 있을 수 있으며 통신상의 문제점도 고려되어야 한다. 이러한 복잡한 환경을 고려하여 기술과 대책이 다루어져야 한다. 상용적으로 나와 있는 방화벽, 바이러스 퇴치 소프트웨어, 정기적인 패스워드의 변경, 이더넷 네트워크 보안 관리 장치 등의 활용이 활발하게 진행되고 있다. 이전에는 높은 클래스로 분류되는 안전한 데이터 센터를 유지할 수 있었다. 그러나 정보 시스템의 복잡성 증가로 이러한 성역의 존재는 없어지고 있다. 새로운 환경에서 완벽한 방안을 찾는 것은 매우 어렵다. 클라이언트/서버 환경과 부합하는 몇 가지의 장치와 보호 방안을 복합적으로 사용하는 것이 좋다. 방화벽은 보안을 위하여 갖추어지는 필수품으로 인식되고 있으나 이 기술의 적용을 위한 자세한 연구가 필요하고 생각된다. 한가지 방안으로 모든 문제가 해결되지 못하기 때문에 사업환경에 맞는 다른 보안 대책도 추가하여야 한다. 클라이언트/서버 시스템에서 강력한 사용자 개인 식별 방안이 강구되어야 한다. 인가되지 않은 부정 사용자의 침투로 네트워크상의 여러 시스템이 공격당할 수 있기 때문이다. 보안 시스템을 구매하기 전에

어떠한 보안 정책을 갖느냐 하는 것이 결정되어야 한다. 보안 관리자는 자체 시스템의 보안성을 주기적으로 점검하고 현재의 상태를 파악하고 있어야 한다. 또 새로운 시스템의 도입으로 어떠한 변화가 이러 나는지 알고 있어야 한다. 그렇지 못하면 의미 있는 행동을 취할 수 없다. 가장 보호되어야할 자원이 무엇인지 인식하고 무엇을 위해 보안 활동을 하고 있는지를 알아야 한다. 사업수행의 목표를 감안한 보안대책이어야 한다. 기술적인 면에서만 보안 대책을 바라보면 효과적인 대응을 할 수 없다. 사용자들의 습관적인 경향도 고려하여야 한다. 어느 조직에서는 이동 데이터 통신기기의 사용을 가급적 제한하기도 한다. 은밀한 데이터는 통신 자체를 자제하기도 하는데 습관적인 행동에서 보안성을 추구하려는 사례이다.

그러나 수동적인 대책으로 업무가 제한된다면 사업의 목표 추구에 문제가 생긴다. 높은 보안성이 요구되는 경우 데이터 암호화로 대책을 강구하여야 한다. 암호화된 데이터는 접근하여 데이터를 얻어도 이를 복호화하는 것이 매우 어려움으로 높은 보안 대책이 될 수 있다. 그러나 복호화 과정에서 이러나는 문제를 방지할 수 있는 대책이 강구되어야 한다. 클라이언트/서버 환경과 다수의 데이터 베이스로 구성된 시스템을 위하여 어떠한 보안 조치가 필요한지 신중하게 생각하여야 한다. 사용자 인증은 아마도 가장 중요한 보안상의 요소중 하나일 것이다. 대부분의 경우 보안관리 시스템은 패스워드의 길이, 패스워드 변경의 빈도 등을 요구하기도 한다. 패스워드의 정기적인 변경은 사용자 인증을 바탕으로 하는 많은 보안 시스템에 도움을 줄 것이다. 일부의 전문가들은 다수의 서버로 구성된 클라이언트/서버 환경에서 보안관리 시스템의 중앙관리 경향을 예측하고 있다. 보안 관리를 하나의 믿을 수 있는 서버(Trusted Server)에 의지함으로 개별 사용자 인증이 손쉬워지기 때문이다. 이때 서버의 개념은 물리적으로 하나의 하드웨어에 국한되는 것은 아니다. 인증을 위한 메시지 교환은 공개키/비밀키 암호화 방식을 이용할 수 있다. 디지털 서명방식은 데이터의 부정한 변조를 방지하고 서명자의 부인 방지 기능을 갖는다. 암호화 과정은 더욱 복잡한 기술과 비용의 상승을 초래할 수 있다. 그러나 암호화는 안전성이 요구되는 패스워드의 분배 또는 송수신 과정에서 도청을 방지하는 유효한 방법이다.

4. 보안을 위한 시스템 고려사항

기업이나 기관에서 실제로 채택하는 보안 대책은 컴퓨팅 환경의 변화에 많이 영향을 받았다. 아마 보안 문제에 피해를 본 관리자도 많을 것이다. 이러한 피해는 금전적인 피해를 주기도 하고 또 다른 사업상 신뢰 문제도 발생할 것이다. 다음 <표 1>은 보안 문제와 이에 대한 해결 방안에 대해 보여준다.

<표 1> 보안 문제별 대책

보안 사항	보안 대책	기능
데이터의 변조, 누출,파손.	DES, RSA 암호화.	자료 암호화하고 필요시 복호.
사용자의 비인가 자료 접근.	접근 관리 S/W 채용.	사용자/관리자차별 접근제어.
사용자/사용자의 보안문제.	사용자인증/ ID카드 채용.	암호 S/W 혹은 ID카드 인증.
부정한 침입자의 자료접근.	방화벽 채용.	특정 통신 훨터링 혹은 차단.
서버O/S 시스템 침입.	O/S 툴에서 해결.	O/S 상에서 헛점을 봉쇄.

4.1 데이터의 변조, 누출, 파손 방지

보관 유지된 자료가 침입자 혹은 기타의 원인으로 변조 파괴되는 문제이며 많은 경우 도난 보다 훨씬 심각한 문제를 야기시킨다. 보안 관리 시스템은 이를 방지하고 점검하는 시스템을 유지해야할 것이다.

4.1.1 데이터 암호화

보안을 요하는 데이터를 암호화하는 것은 믿을 수 없는 네트워크 환경에서 비밀 유지에 도움을 준다. 악의적으로 혹은 우연한 기회에 네트워크에 들어온 침입자는 데이터가 암호화되었으면 변조를 쉽게 할 수 없다. 금전의 전자적 거래는 믿을 수 있는 네트워크 환경이라도 암호화하는 것이 필수적이다. 암호화하는 과정에서 알고리즘에 따라 누가 데이터를 입력하고 변경하였는지 알 수 있기 때문에 메시지 자체의 실명 식별 효과도 얻을 수 있다.

4.1.2 비밀키 암호

암호화하는 알고리즘은 여러 가지가 있다. 가장 많이 쓰이는 것으로 56비트, 128비트의 길이를 가지고 있는 DES 암호 알고리즘을 들 수 있다. 현재 56비트 키는 비밀을 유지하는 최소한도라고 볼 수 있다. 좀더 안전성을 추구하려면 128비트 키 방식을 사용하여야 할 것이다. DES는 미국의 국가 표준 암호 알고리즘으로서 하나의 키로 암호/복호를 수행함으로 대칭키(Symmetry Key) 방식이다. 그 동안 암호기술은 선진국의 전유물처럼 전적으로 의존해 왔으나 앞으로 국내기술을 기반으로한 데이터 암호화가 가능하리라 전망된다. 삼성 종합기술원, 퓨처시스템, 소프트포럼, 펜타컴퓨터, 켁신시스템 등 벤처기업들과 대기업들이 암호 알고리즘의 적극적인 개발에 나서고 있다고 한다(전자신문 '97.9.29). 데이터의 암호화는 전체 데이터에 대하여 하는 방법과 일부분을 하는 방법이 있는데 데이터를 처리하는 복잡성과 편이성에 따라 정해진다.

4.1.3 공개키 암호

공개키 암호의 알고리즘은 일방향 함수를 이용한다. 일방향 함수는 지수함수와 같이 역으로 함수를 푸는데 어려운 수학적인 특성을 이용한다. 개별적인 통신 개체는 공개키와 비밀키를 부여받는다. 공개키와 비밀키는 RSA[2]와 같은 암호 알고리즘에 의하여 생성시키는데 어느 일방을 알아도 나머지 키를 계산하는 것이 매우 어렵다. 메시지는 공개키에 의하여 암호화되고 통신 상대방에 보내진다. 그러므로 메시지를 송신할 개체는 공개키를 부여받아야 한다. 수신자는 암호화된 메시지를 비밀키를 이용하여 푼다. 이 비밀키는 수신자 이외의 개체에 알려져서는 안된다.

4.1.4 암호키 보내기

운영 시스템은 다른 개체의 공개키를 알고 시스템이 시작과정에서 모든 개체에게 자신의 공개키를 분배한다. 분배 과정에서 공개키는 암호화되어 분배되어야 한다. 그러므로 사용자가 운영체제 관리자와 같은 기능을 흉내내지 못하도록 한다. 이러한 기능은 사용자의 비밀키를 이용하여 암호화되어 전송하는데 비밀키의 개체만이 인증과정을 통과 할 수 있도록 하여 해결 될 수 있다.

4.2 사용자의 보안 문제 해결

4.2.1.인가 받지 않은 자료 접근

정당하고 등록된 사용자라도 접근이 허용되는 부분과 그렇지 않은 부분이 있다. 조직은 접근 허용과 범위에 대한 데이터 구분 방안을 가져야 한다. 비밀스러운 부분에 대한 일반 사용자의 접근이 허용되어서는 안된다. 클라이언트/서버 리소스 데이터의 접근은 공통된 보안상의 문제점이다.

일부 사용자에게 사용이 한정되어 있는 리소스 데이터는 누출되지 않도록 한다. 서버를 사용할 수 있는 권한은 운영 관리자 외에는 사용이 금지되어야 한다. 모든 사용자가 사용할 수 있는 자료 이외에는 접근이 제한되어 호기심 있는 사용자의 불법적인 해킹이 방지되어야 한다.

4.2.2. 사용자간의 보안

사용자 전원 개별적인 보안 유지가 보장되어야 한다. 사용자끼리의 개인 자료 유출이 많은 경우에 문제가 된다. 사용자 개개인은 한정된 범위내 리소스 접근이 허용되어 불법적 접근이 방지되어야 한다. 정당한 사용자가 자료를 사용한 후 혹은 사용 중에 다른 사용자가 이를 불법적으로 재사용할 수 있다. 네트워크 관리자는 한번 사용된 자료가 남아 침입자에게 재사용되는 가능성을 철저히 배제되도록 하여야 한다. 이것은 네트워크에 존재하는 기억 장치에 이미 사용된 정보가 남을 수 있다는 사실에 근거 한다. 개인 신상, 카드와 같은 토큰을 병용하는 것이 하나의 방법이다. 될 수록 사용자의 특징이 많이 인식되는 인증 시스템이 병용되어야 한다.

4.3 부정한 침입자의 자료접근

영업의 확장이나 업무의 증가, 지역적인 제한에서 벗어나기 위하여 서버가 넓은 공간에 위치하게 된다. 이러한 지역적인 분산에서 침입자는 더욱 용이해진 게이트웨이 접근이 가능해 진다. 원격에서 오는 접속에 보안조치는 몇 가지 유의할 점이 있다. 해커는 좀더 새로운 네트워크에 접근하여 영향을 주려하는 경향이 있는 반면 정보 침입자는 고가의 정보를 획득하려 한다.

4.3.1 사용자 인증 과정

로그인시 패스워드 점검은 정당하고 등록된 사용자인가 확인하는 과정이다. 침입의 목적으로 네트워크상의 접속 과정을 시뮬레이터등으로 도청을 하는 경우가 있다. 이 경우 침입자는 사용자에 대한 정보를 도용할 수 있다. 침입자는 분석한 사용자 정보를 이용하여 유용한 정보를 빼 갈 것이다. 다른 유형은 잘 알고 있는 패스워드 해킹 방식이다. 이러한 패스워드 공격(예: Dictionary Attack)은 패스워드의 구성을 이 공격에서 벗어나도록 함으로 피한다. 로그인 과정에서 3번 기회를 주고 실패하면 접속을 제한하는 방법을 흔히 쓴다. 접속 제한은 시스템 관리자만이 함으로 보안을 유지한다. 그러나 이러한 외부 침입은 보안 문제의 일단에 불과하다. 먼 곳에서 접속을 시도하는 침입자외에 내부의 불순하거나 호기심 많은 일부 사용자가 보안 문제를 야기시키는 경우가 많다. 보안 시스템 설계자는 모든 여러 상황에서 유기 되는 문제를 종합적으로 보아야 한다. 인간의 편의성과 의존성 추구면에서 패스워드 보안 문제를 이해 하여야 한다. 8 내지 9 단위 정도의 어려운 문자 조합을 4 내지 6주 정도의 주기로 바꾸어 사용하려면 복잡한 생활 속에서 단순한 문제는 아니다.

4.3.2. 방화벽

방화벽은 하나의 네트워크와 다른 네트워크의 정보 교환을 선별하여 교환 시켜주는 시스템이다. 네트워크 내부에서 보면 원하지 않는 데이터의 침입을 밖으로부터 차단하여 주는 역할을 한다. 간단히 말하면 방화벽은 접속을 제어해 준다. 이 시스템은 외부의 접속 요구에 대하여 어떤 포멧을 갖춘 접속은 허용하고 그렇지 못한 것은 접속을 거부한다. 효과적인 방화벽은 외부의 침입으로부터 네트워크에서 보관중인 자료를 보호하게 된다. 방화벽은 순수한 소프트웨어로 되어 프로그램 형태로 될 수 있고 또 하드웨어를 포함하기도 한

다. 기술적으로 보아 프로그램이 가능한 라우터는 방화벽의 역할을 할 수 있다. 라우터는 IP레벨에서 통신을 제어한다. IP레벨 제어는 방화벽으로 보아 일차적인 제어 관문이 될 수 있다. 새로운 제품으로 응용층을 기초로 통신을 제어하는 방화벽이 나오고 있는데 좀더 완전한 역할을 수행한다. 응용계층을 이용한 방화벽은 데이터 변환에 대한 해석에 있어 장점을 가지고 있다. 다른 하나의 방화벽 구축 방법은 컴퓨터를 방화벽 호스트로 사용하는 것이다. 이 경우 좀더 강력한 방화벽 역할을 수행 할 수 있다. 시장에 나와 있는 방화벽 제품은 프록시 서버와 패킷 휠터의 조합으로 이루어진다. 사용자에게 투명성은 방화벽 제품의 중요한 포인트이다.

4.4 클라이언트/서버 시스템 O/S

클라이언트/서버 O/S에서 해결 해야할 보안 시스템의 목표는 다음과 같이 정의할 수 있다.

(1) 하나의 서버가 다른 서버의 비밀스러운 부분에 접근하여 자료의 변경이나 누출이 되어서는 안된다.
(2) 인터 프로세스간 통신 보안이 지켜져야 한다.

보안 문제가 클라이언트/서버 환경에서는 좀더 심각한 것은 다수의 서버가 존재하고 서버간에 통신이 복잡하기 때문이다. 대부분의 클라이언트/서버 운영시스템은 서버간의 통신과 상호 연결에서 모듈성을 보장하여야 한다. 같은 노드에서 운영되는 서버와 다른 노드에 운영되는 서버간에 서로 통신이 필요하기 때문이다. 상호 통신 과정에서 도청(Eavesdropping), 메시지 재사용(Replaying of Message), 위장(Masquerading)이 보안 문제가 된다. 이러한 보안상의 문제를 해결 할 수 있는 운영 시스템의 설계는 여러 사항의 준비가 필요하다. 상호 통신 시스템에서 첫 번째 일은 명칭을 정하는 일이다. 운영 시스템은 명칭을 관리하는 운영 관리 시스템을 가지고 있다. 명칭 관리 시스템은 로칼 포트를 생성하고 원하는 태스크에 명칭을 알려준다. 이러한 시스템은 다음 특징을 가진다.

(1) 인터서버와 클라이언트/서버 통신 인터페이스를 분리한다.
(2) 네트워크 서버간에 메시지를 암호화한다. 이때 암호화 알고리즘은 공개키 시스템을 사용한다.
(3) 서버의 사인을 인증한다. 인증 경우와 명칭 확인을 요구할 경우에는 공개키/비밀키 쎌을 사용한다.
(4) 서버 상호간의 인증에도 공개키/비밀키 쎌을 사용한다.

이러한 보안 시스템 설계 사례는 Mach3.0 마이크로커널에 기초한 클라이언트/서버 운영 시스템 Masix[5][10]로 한다. Mach3.0은 포트를 기초로 강력한 태스크간 통신을 지원하고 있다. Masix는 다수의 서버를 지원하고 각 노드에 위치한 스테이션을 DGL(Distributed Generic Layer)상에서 인식한다. 네트워크에 있는 개체간 통신 관리는 GNS (Genenric Network Server)가 한다. 명칭 관리는 ACS(Administration Configuration Server)를 통하여 하는데 모든 네트워크에 사용되는 태스크의 명칭 프로토콜을 수행한다. 또 ACS는 하나의 개체 로칼 포트(Proxy port)를 생성시켜 원격 접속 처리를 수행한다.

4.4.1 통신 접속의 분리

서버들의 상호 통신연결은 두 가지로 구분되는데

(1) 크라이언트의 연결요청을 접수하기 위한 통신 연결은 통신 포트를 통하여 한다. 이 통신 포트는 ACS의 요청에 의하여 준비된다.
(2) 다른 서버의 요청에 의한 통신 연결은 역시 통신 포트를 통하는데 ACS의 요청에 의하

여 이루어지는 점은 동일하나 ACS는 과정에 인증을 통하여 서버를 확인한다는 점이 다르다. ACS는 이 과정을 통하여 크라이언트와 서버의 통신 요청을 구분 처리한다. 이 분리 기능은 서버통신에 있어 원격 서버의 부정한 통신 요구로부터 포트를 보호한다.

4.4.2 메시지 암호화

운영 시스템에서 사용하는 메시지를 암호화하는 데는 RSA[2] 방식을 이용한다. 이 방법은 메시지 통신 개체들이 먼저 비밀키에 대한 정보가 없어도 공개키로 메시지를 암호화하는데 문제가 없기 때문에 크라이언트/서버 환경에 적합한 시스템이다. RSA는 안전성이 증명되고 널리 사용되는 암호 시스템이다. 매우 큰 정수의 소인수 분해가 어렵다는 사실과 지수함수의 일방향 성질에 근거하여 MIT대 암호 학자 3인 (Rivest, Shamir, and Adleman)이 설계한 것이다. 암호화 과정은 A 가 B에게 암호문을 보낸다고 할 때 다음과 같다[12].

A 와 B 의 공개키를 각각 $E_A=\{n_A,\ e_A\}$, $E_B=\{n_b,\ e_B\}$라 하고 비밀키를 각각 $D_A=\{p_A,\ q_A,\ d_A\}, D_B=\{p_B,\ q_B,\ d_B\}$ 라 한다. 이때 p와 q는 소인수로서 키 생성에만 사용된다.

(1) A는 보내고자 하는 메세지 m_A를 자신의 비밀키를 이용하여 $m_A \equiv m^{d_A} \pmod{n_A}$를 계산한다.

(2) 그것을 B 의 공개키를 이용하여

$c_A \equiv m_A^{e_B} \pmod{n_B}$ 를 계산한다.

(3) c_A를 B 에게 전송한다.

(4) B 는 수신한 c_A를 자신의 비밀키와 A의 공개키를 사용하여

$$m_A \equiv ((c_A^{d_B} \bmod n_B)^{e_A}) \bmod n_A$$

메세지를 복호화 한다.

이때 A의 비밀키는 A 이외의 사람이 알 수 없으므로 A의 신원 확인이 가능하다. RSA 암호 시스템은 많은 전문가들에게 암호 시스템의 대명사로 불리고 있다.

4.4.3 태스크 메시지 교환

태스크 A 와 B 쌍방이 안전한 방법으로 메시지를 송 수신하는 과정을 설명한다.

(1) A는 B의 의사 포트에 메시지를 보낸다.

(2) 메시지를 수신 받는 의사 포트 GNS_a는 메시지를 B에 대신하여 받는다. 의사 포트는 GNS_b의 공개키 pwb_{R_b}와 자신의 비밀키를 이용하여 이를 암호화한다. 이 것을 GNS_b에게 보낸다.

(3) 암호화된 메시지를 GNS_b는 A의 공개키 pwb_{R_a}와 자신의 비밀키 $\sec_{R_b}$를 이용하여 복호화하여 B에게 보낸다.

(4) B가 A에게 역으로 메시지를 보내는 경우는 위 과정을 역순으로 수행한다.

4.4.4 서버 인증

Masix의 초기화에서 개별적인 서버와 DGL 서버는 ACS에 같이 등록된다. 그러나 유사 프로세스는 등록되어서는 안된다. 만약에 등록이 되면 이후 서버로 인정이 되어 우선권을 갖게된다. 우선권을 갖게 되면 시스템 정보에 접속될 수 있고 다른 시스템 상태를 바꿀 수 있게 된다. 등록이 필요한 사용자는 포트를 등록할 때 쓸 명칭 코드를 ACS에 보내야 한다. ACS는 프로세서 서버에게 포트의 소유자를 찾을 수 있도록 요청한다. 소유자를 찾게 되면 이 소유자의 코드를 이용하

여 암호키를 생성한다. 만약 이 암호키가 ACS의 인증을 받지 못하면 등록을 요청한 프로세스는 정당한 서버의 자격이 없다고 판단된다. 이 경우 등록은 취소된다. ACS는 요청된 암호를 되돌리고 이 키의 소유여부가 정당한 서버로서 인정되는 증명으로 사용한다.

4.4.5 국부 서버의 인증

암호키를 인증 프로토콜에 사용하는 것은 위에서 설명한 바와 같고 ACS에 의하여 준비된 암호키가 인증에 사용된다. 로칼 서버가 A 와 B 라면 상호 인증은 다음과 같은 과정을 거친다. C_k (.....)를 k 키로 암호화한 메시지로 표시한다.

(1) A는 메시지(A, B)를 ACS_a에게 보낸다.

(2) ACS_a는 $\sec_a$와 $\sec_b$를 사용하여 새로운 비밀키와 공개키 셀($\sec_{ab}$, pub_{ab})를 생성하고 이 키는 단지 A와 B의 상호 메시지 교환에만 사용한다. ACS_a는 A에게 메시지(B, $\sec_{ab}$, $C_{\sec_b}$($\sec_{ab}$, pub_{ab}, A)를 보낸다.

(3) A는 $\sec_{ab}$, pub_{ab}를 보관하고 B에게 $C_{\sec_b}$ ($\sec_{ab}$, pub_{ab}, A)를 보낸다.

(4) B가 자신의 비밀키로 암호를 풀 수 있기 때문에 $\sec_{ab}$, pub_{ab}를 추출한다. 이제 A와 B 만이 이 키 셀의 사본을 갖게 되고 이를 소유했는지 여부가 상호 자격을 인증을 할때 증표로 사용된다.

$\sec_{ab}$, pub_{ab}를 갖지 않은 프로세스는 인증받지 못하는 프로세스가 된다. 그러나 재사용(Reuse) 공격은 가능하기 때문에 타임 스탬프와 같은 정보의 추가로 문제를 해결한다.

4.4.6 원격 서버의 상호 인증

A와 B가 서로 다른 노드에 있을 경우 키 셀 ($\sec_{ab}$, pub_{ab})의 분배는 더욱 복잡하여 진다. 다른 노드의 ACS가 분리된 명칭 관리를 하고 있기 때문이다.

(1) A 는 ACS_a에게 메시지 (A, B)를 보낸다.

(2) ACS_a는 ACS_b에게 메시지(A, B, $\sec_a$)를 보내야 하지만 서로 원격에 위치함으로 GNS_a가 메시지를 의사 포트로서 받게 된다.

(3) GNS_a는 GNS_b에게 메시지 C_{pubGNS_b}(A, B, $\sec_a$)를 보낸다.

(4) GNS_b는 $\sec GNS_b$를 이용하여 복호화 하고 ACS_b에게 메시지 (A, B, $\sec_a$)를 보낸다.

(5) ACS_b는 $\sec_a$와 $\sec_b$를 근거로 하나의 새로운 키 셀($\sec_{ab}$, pub_{ab})을 생성하여 그리고 이를 ACS_a에게 메시지(A, B, $C_{\sec_b}$ ($\sec_{ab}$, pub_{ab}, A)) 를 보낸다. ACS_a가 원격이므로 GNS_b가 의사 포트로 대신하여 메시지를 받는다.

(6) GNS_b는 메시지 C_{pubGNS_a}(A, B, $C_{\sec_b}$ ($\sec_{ab}$, pub_{ab} , A))를 GNS_a에게 보낸다.

(7) GNS_a는 $\sec GNS_a$를 이용하여 복호화하고 메시지 (A, B, $\sec_{ab}$, pub_{ab}, $C_{\sec_b}$ ($\sec_{ab}$, pub_{ab}, A))를 ACS_a에게 보낸다.

(8) ACS_a는 A에게 메시지 (A, B, $\sec_{ab}$, pub_{ab}, $C_{\sec_b}$($\sec_{ab}$, pub_{ab}, A))를 보낸다.

(9) A는 $\sec_{ab}$, pub_{ab}를 보관하고 B에게 메시지 $C_{\sec_b}$($\sec_{ab}$, pub_{ab}, A)를 보낸다.

(10) B만이 이 메시지를 자신의 비밀키로 $\sec_{ab}$, pub_{ab}을 추출할 수 있으며 A와 B는

서로 이 키 쌀을 공유하게 되므로 서로 상대방을 인증할 수 있게 된다.

다수의 서버로 구성된 클라이언트/서버 환경에서 보안성이 보장된 상호 통신이 필요하다. MASIX 운영 시스템에서 채용한 GNS(Generic Network Server)에 의한 해결 방법이 예시되었다. 이 방법은 상호 통신의 인증 과정과 암호화를 통하여 안전성을 추구한다. 이 메커니즘은 공개키와 비밀키의 암호 알고리즘에 의하여 이루어진다. 특히 이 메커니즘은 서로 원격으로 위치하여 분산 인증 프로토콜을 수행함으로 원격으로부터 오는 태스크도 동질성을 보장하고 있다.

4.5 유지 보수

아는 것이 힘이다! 대부분의 정보 관리 책임자들은 패스워드를 모르는 사용자는 시스템에 접근하기 어렵고 방화벽과 같은 보안시스템이 침입을 막아 준다고 믿고 있다. 그러나 방화벽을 비롯한 모든 보안 방지 시스템은 결국 고개 넘기 퀴즈 풀이와 같은 원리이며 완벽하기엔 한계점이 있다. 물리적인 보안과 함께 완벽한 소프트 설계를 갖추었다 해도 불법적인 침입이 가능하다. 침입자는 시스템을 무력화 하기 위하여 여러 가지 방법을 동원 할 수 있다. 보안 시스템 설계에서 유의 해야할 점은 설계에 레이어 개념을 도입하는 일이다. 패스워드와 인증 과정은 하나의 레이어에 불과하고 여기에 보충된 보안 레이어의 설치가 필요하다. 물론 다층 구조의 보안 시스템이 사용자 편에서는 편의상 하나의 레이어 처럼 느껴져야 한다. 하나의 방안은 조직에서 사용하는 네트워크 기억 장치들이 여러 개의 보안 영역으로 나누는 방법이 있다. 일반적인 자료 저장과 비밀 자료의 저장을 구분하고 전용 서버도 아예 구분하는 방법이 좋다. 전용 터미털을 구분 설치하고 여기에 물리적으로 접근을 통제한다면 더욱 보안성이 강해 질 것이다. 다음 레이어는 원격 접속시 원격접속 프로그램을 사용하는 방법이다. 이 프로그램은 전용의 네트워크 게이트웨이 "Hand shake" 루틴을 사용하여 접속이 가능하게 한다. 대부분의 경우 외부에서 침투하여 보안이 문제되는 것이 드물고 내부의 문제점이 더욱 심각하다. 중요한 것은 보안 시스템의 지속적인 점검과 사용 현황을 파악하는 일이다. 아주 안전하게 시스템 설계가 된 시스템이라고 해도 사용자와 운용 시스템의 사용 현황이 기록 유지되어야 할 것이다. 기록 유지는 보안상의 허점을 발견한다던가 잘못된 행위가 일어나고 있다는 사실을 알려준다. 한두번의 점검으로 부족하며 지속적이고 일상적인 점검과 유지 보수가 필요하다.

5. 결 론

컴퓨터 이용 환경의 변화는 앞으로 닥치는 보안 문제와 직결된다. 이용 환경의 변화를 예측하고 보안 대책을 강구하는 것이 순서일 것이다. 경제 사회적인 환경 변화도 보안 문제를 예상할 수 있는 하나의 요소가 될 것이다. 요즈음 부각되는 지적재산(Intellectual Property)의 가치 증대와 전자화폐(E-cash)는 정보화 사회의 진전으로 문제는 더욱 심화될 것이다. 보안 문제의 어려움은 대부분의 사람들이 잘 모르고 있다는 사실이다. 보안 문제를 경제적으로 계량화하는 연구도 가치 있는 일이다. 보안 대책의 수행은 항상 비용의 증가를 가져온다. 보안 문제 해결을 위하여 투자를 결정하는 일이 쉽지 않기 때문이다.

참고문헌

[1] W. Diffie and Hellman. "New Direction in Cryptography", IEEE Transactions on Information Theory, IT-22, pp.644-654, 1976.

[2] R. Rivest, A.Shamir and L. Adleman. "Method of Obtaining Digital Signatures and Public Key Cryptosystems", Communications Of the ACM, 21(2), pp:120-126, 1978.

[3] M. Accetta, R. Baron, W. Bolosky, D. Gould, R. Rashid, A. Tevanian and M. Young. "MACH: New Kernel Foundation For UNIX Development", In Proceedings of The Usenix 1986 Summer Conference, June 1986.

[4] T.R.Rao and K.Y.Nam, "Private Algebraic Code Encryptions" IEEE Transactionson Information Theory, Vol.35, No.4, pp:829-833, Jul. 1989.

[5] R.Card, E. Commelin, S. Dayras, and F. Mevel, "The MASIX Multi-Server Operating System", In OSF Workshop on Microkernal Technology for Distributed System, Jun. 1993.

[6] Tsutomu Matsumoto, "Incidence Structure for Key Sharing". ASIACRYPT pp:298-297, Nov. 1994.

[7] J. Stevenson and D. Julin, "MACH-US: UNIX of Generic OS Object Servers", In Proceedings of the 1995 Usenix Confcrence, Jan. 1995.

[8] F. Mevel and J. Simon, "Building a Distributed Generic Layer for Multiple Personality Support on Top of the Microkernel", In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications. pp:636-644, Nov. 1995.

[9] Hidenory Kuwakado, Kenji Koyama, "A New RSA-type Scheme Based on Singular Cubic Curves", In Proceedings of Korea-Japan Joint Workshop on Information Security and Cryptology:4.5.1-4.5.8, 1995.

[10] Franck Mevel and Jullien Simmon, "Secure Communication Services in The Masix Distributed Operating System", In Proceedings of the IASTED International Conference, (240-049), pp:5-8, Jan, 1996.

[11] Janet G. Butler. Securing, "The Enterprise Network", Pub. of Computer Technology Research Corp. Chap.3, pp:45-63, 1997.

[12] 한국전자통신연구원, "현대암호학", pp:129-132, 1978.

강 영 일

1966년 서울대학교 공과대학 전기공학과 (공학사)
1989년 Fairleigh Dickinson University 전기과 (공학석사)
1996년 고려대학교 전산과학과 (이학박사)

1979년-현재 한국전자통신연구원 책임기술원
1996년-현재 정보통신연구관리단 기초전문위원 파견
관심분야 : 코딩이론과 알고리즘