通信情報保護學會誌
第6卷 第3號, 1996. 9

네트워크 시스템의 보안 관리

Security Management on a Network System

박 태 규*, 강 창 구**, 김 대 호**

요 약

본 논문에서는 OSI에서 규정하는 네트워크 관리 기능별 5개 영역 중 보안 관리 기능의 정의, 보안 관리 작업의 이점, 보안 관리 수행 절차, 공중 데이터 망에 연결시 유용한 보안 유지 사항, 보안 관리 도구의 예, 보안 사건의 보고와 OSI에서 수행하고 있는 표준화 작업 내용으로서 네트워크 관리 프레임워크, JTC1/SC21의 OSI 관리 내용 개요를 소개한다.

1. 서 론

네트워크 보안 관리란 데이터 네트워크에 연결된 장치 내에 저장된 중요한 정보에 대한 접근점(Access Point)을 통제함으로써 그 정보를 안전하게 보호함을 의미한다. 중요한 정보라 함은 어떤 조직에서 안전하기를 원하는 데이터로서 이를테면 급여, 고객 계정, 연구·개발 일정 등에 관련된 것일 수 있다. 네트워크 보안 관리는 네트워크 관리자로 하여금 다음과 같은 방법에 의해서 중요한 정보를 보호하도록 할 수 있다[1].

- 조직의 내부 및 외부 사용자에 의한 호스트와 네트워크 장치에의 접근 제한
- 보안 위반 시도나 실행에 대해 관리자에 통보

보안 관리는 일반적으로 다음과 같은 단계로 구성된다.

- 보호될 중요 정보의 식별
- 접근점의 파악
- 접근점의 안전화
- 안전한 접근점의 유지관리

이러한 형태의 보안 관리는 운영체제 또는 물리적 보안과 혼동되어서는 안된다. 보안 관리에 의한 보호는 네트워크 호스트 및 장치를 통하여 데이터 네트워크내의 접근점을 통제하도록 함으로써 실행된다. 접근점은 소프트웨어 서비스, 하드웨어 구성요소, 네트워크 미디어를 의미할 수 있다. 한편, 운영체제 보안은 파일, 디렉토리, 프로그램 등의 보호를 의미하며, 물리적 보안은 전산실 출입문 잠금, 카드출입 시스템 설치, 키보드 잠금 등을 의미한다. 그러나, 후자는 여기서 언급하는 보안 관리의 일부가 아닐지라도, 이러한 것들을 빼고는 보안

* 한서대학교 전산정보학과 교수
** 한국전자통신연구소 책임연구원

관리는 의미가 없다. 적절히 설치하고 관리함으로써, 보안 관리는 데이터 네트워크를 통한 비인가자를 호스트에 접근함을 막을 수 있다. 그러나, 비인가자가 컴퓨터에 들어올 수 있고, 중요 정보를 저장하고 있는 디스크 드라이버를 제거할 수 있다면, 그 데이터는 결코 안전하지 않다. 본 논문에서는 보안 관리의 이점을 설명한 후, 보안 관리를 수행함에 있어 필요한 4단계 활동을 논하고, 3가지 보안 관리 도구를 단순한 것부터 발전된 것까지를 소개하고자 하며, 사건 보고 기능으로부터 보안 사건 내용을 얻을 수 있는 감사 추적의 이점을 논하고자 한다. 또한 OSI에서 수행하고 있는 보안 관리의 표준화 활동 내용을 소개하고자 한다.

2. 네트워크 보안 관리

2.1 보안 관리의 이점

데이터 네트워크에 호스트를 연결하는 사용자의 주 관심사는 호스트에 존재하는 중요 정보에 대한 보안성의 결여 문제이다. 이러한 문제를 피하기 위해, 호스트에서 처리하는 중요한 정보는 네트워크 접근을 모두 불가능하게 하고, 이동이 가능한 매체(즉, 자기 테이프, 광디스크 등)를 통하여 정보를 전달할 수 있다. 이런 방식으로는 호스트의 물리적 보안 접근이 가능한 사람만이 중요 정보를 다룰 수 있다. 그러나, 이러한 방법은 안전할지라도 매우 비효율적이다. 적절히 설치되고 유지 관리되는 보안 관리는 네트워크에서 더욱 실제적이고, 효율적이며 보안성 확보에 대한 대안을 제공할 수 있어야만 한다. 따라서 중요 정보에 대한 실질적이며 확신할 수 있는 안전성을 구축함이 보안 관리의 주 이점이다. 어떤 조직의 사설 데이터 네트워크가 공중 데이터 네트워크에 연결되고, 급여 정보를 저장하고 있는 그 조직의 컴퓨터가 네트워크에 연결되어 있어 어떤 사용자의 요구에 따라 급여에 관한 정보를 제공한다고 가정해 보자. 쉽게 알 수 있듯이 무제한 접근의 결과로 그 조직의 혼란을 야기할 수 있다. 보안 관리의 결여로 발생할 수 있는 혼란의 결과는 1988년 11월에 인터네트 벌레(Internet Worm)가 나타났을 때 크게 보여주었다[1]. 사용자 서비스로 보안성을 확보하지 못하고 인터네트를 통해 호스트에 있는 정보를 얻을 수 있게 됨으로써, 이 벌레는 컴퓨터 네트워크에 있는 수천 대의 컴퓨터를 계속 침투하였다. 이 벌레가 사용한 방법은 "sendmail"이라는 UNIX 서비스로 컴퓨터에 연결하고, shell을 생성(spawn)하고, 자신을 수행시켰다. "sendmail"의 다른 개정판(version) 조차도 어떠한 보안 검토도 없이 프로그램 디버그 모드의 하나로 그 벌레의 접근을 허용하였다. 이 벌레는 또한 호스트에 대한 권한을 얻기 위해서 "finger"라 불리는 또 다른 UNIX 서비스를 사용하였다. 이러한 "sendmail"과 "finger"공격은 어떠한 네트워크 접근점에서의 보안 취약성을 찾아내는 벌레의 예들이다. 흥미롭게도 벌레가 호스트에 로그인 하기 위해서 사용한 가장 성공적인 방법은 단순히 호스트 보안의 약점인 일반적인 패스워드를 사용했다는 것이다. 그 벌레는 파일 시스템을 파괴하고, 데이터를 망가뜨리고, 다른 여러 가지 악의 있는 행위를 수행할 수가 있었다. 다행스럽게도 의도적인 것은 아니었지만, 그 벌레 자체를 여러 번 복제하였기 때문에 프로세서의 지나친 부담(load)으로 그 행위는 정지되었다. 또 다른 허술한 보안 관리로 인해 조직에 피해를 끼친 실제 예는 뻐꾸기 알(Cuckoo's Egg) 등에 소개되고 있다.

2.2 보안 관리의 수행 단계

효과적인 보안 관리는 네트워크 관리자로 하여금, 중요 정보에 대한 보안 요구와 사용자 업무 수행에 따른 정보에의 사용자 접근 요구와의 균형을 맞출 필요가 있다. 이러한 네트워크 관리는 ① 중요 정보의 식별 ② 접근점의 파악 ③ 접근 점의 안전화 ④ 안전한 접근점의 유지관리의 4단계로 나타낼 수 있다. 호스트 컴퓨터에 중요한 정보인 급여 데이터가 저장되어 있다고 가정하자. 접근점은 원격 로그인과 파일 전송이며, 관리자는 시스템 콘솔에서 인가자에게만 접근을 허가함으로써 안전화한다. 모니터 시스템은 비인가 된 로그인 시도를 로깅(logging) 함으로써 보안유지를 확인한다. 각 사용자 계정에 대해 로그인 시 패스워드를 확인하는 것만으로 보안성은 충분치 못하다.

2.2.1 중요 정보의 식별

보안 관리를 실행함에 있어 첫 번째 단계로서 네트워크에 연결된 어떤 호스트가 중요 정보를 갖고 있는지를 판단하는 것이다. 대부분의 조직은 어떤 정보가 중요한가에 대한 분류 정책을 일반적으로 갖고 있다. 즉, 계정, 재정, 고객, 판매, 기술, 고용자 정보 등의 정보로, 얼핏보기에 이 절차는 단순해 보이지만, 어떤 정보가 중요한지는 환경에 따라 다를 수 있으며, 어떤 호스트에 중요한 정보가 존재하는지를 찾는 것은 매우 어려운 일일 수 있다.

2.2.2 접근점 파악

어떤 정보가 중요한지를 파악하고, 그 정보가 어디에 위치해 있는지를 파악한 후, 네트워크 사용자가 어떻게 그 정보에 접근하는지를 알 필요가 있다. 이 절차는 각 소프트웨어가 네트워크를 통해서 어떤 서비스를 제공하는지를 검사할 필요가 있다. 데이터 네트워크에 있는 많은 컴퓨터들은 사용자에 의한 원격 로그인을 제공한다. 만일 이러한 로그인 기능이 유일한 사용자를 식별하지 못하고, 시스템 내에서 인가된 구역에만 갈 수 있도록 제한하지 못한다면, 우리는 안전의 필요에 따라 이러한 접근점을 검사하기를 원할 것이다. 또한 많은 컴퓨터들은 데이터 네트워크를 통해서 파일 전송을 수행할 수 있다. 원격 로그인 기능과 같이, 사용자를 유일하게 식별하지 못한다면, 이 사용은 제한되어야만 한다. 보안 관리 조사를 필요로 하는 파일전송 서비스의 한 예는 FTP(File Transfer Protocol)에서의 "anonymous" 로그인 이다. FTP는 TCP/IP의 파일 전송 프로토콜로서 사용자 이름인 "anonymous"로, 로그인 시 사용자 패스워드를 어떠한 것을 입력해도 무방하도록 되어있다. 이 방식은 공개 소프트웨어 및 문서 등을 배포하는데 사용된다. 어떤 컴퓨터가 FTP 서비스로서 "anonymous" 로그인을 제공하는 경우 이 컴퓨터의 네트워크 관리자는 어떤 정보가 접근 가능한 디렉토리에 포함되어 있는지를 주의 깊게 조사해야만 한다. 그리고, E-mail, 원격 프로세스 수행, 파일 및 디렉토리 서버, 네임서버 등 또한 보안 관리를 사용하여 안전하게 유지되도록 컴퓨터에 접근점을 부여할 수 있다. 예로, UNIX 운영체제인 컴퓨터에서 이 컴퓨터에 의해 제공되는 서비스는 "/etc/service" 파일이 존재하며, 이 파일은 네트워크 트랜스포트 프로토콜에 의한 사용을 위하여 서비스 포트에 응용프로그램 이름을 매핑시킨다. 유사하게, 많은 PC들은 컴퓨터가 제공할 수 있는 서비스를 나열하는 파일이나 응용프로그램을 갖는다. 많은 컴퓨터 시스템들은 네트워크 관리 프로토콜을

통해 중요치 않은 정보를 제공하는 것 같이 보인다. 그러나, 좀더 자세히 그 정보를 살펴보면 제한 접근이 필요함을 발견 할 것이다. 즉, 네트워크 주소, 이름, 운영체제, 운영시간 등. 그러나 네트워크 관리 프로토콜을 운영하고 있는 컴퓨터가 고객을 위해 새로운 관리 운영체제를 시험한다고 가정해 보자, 경쟁 사에 의해 조회될 때 응답된 운영체제의 개정판 번호가 아직도 공개되지 않은 것일 수도 있을 것이다. 이 정보의 누출은 비록 적지만 경쟁사의 제품 판매에 영향을 줄 수도 있다. 사용자로 하여금 네트워크 미디어를 통과할 때 패킷을 모니터 하도록 하는 기능은 중요 정보에 대한 또 다른 접근점이 된다. 때로는 프로토콜 분석기나 호스트 컴퓨터에 대해 기능시험을 위해 수행된다. 이때 네트워크 관리자는 사용자도 이런 행위를 할 수 있고, 패킷을 모을 수 있으며, 패스워드나 다른 중요 정보를 찾아낼 수 있음을 알아야만 한다. 또 다른 데이터 망에서 중요 정보를 담고 있는 간과하기 쉬운 장소는 네트워크 관리 시스템 자체이다. 네트워크 관리 시스템은 사용자로 하여금 네트워크 자체에서, 관계 데이터 베이스 내에서부터 중요한 정보를 발견할 수 있는 많은 방법들을 준다. 데이터 네트워크에 대한 접근점이 판명되면, 우리는 네트워크 관리 시스템을 고려해야 한다. 그 방법을 다음절에서 설명하기로 한다. 많은 조직에서는 그들의 모든 네트워크 장치와 호스트에 대한 보안 사항을 표준화하기 위해서 실제적으로 장비에 맡기고 있다. 이러한 네트워크 보안 표준은 중요 정보에의 여러 가지 접근 방법을 다루는 규칙으로서 제공된다.

2.2.3 접근점 안전화

보안 관리의 다음 단계는 필요한 보안 기법[1,2,3]을 적용하는 것이다. 보안은 데이터 네트워크의 여러 계층에서 적용될 수 있다. 즉, 데이터 링크 수준에서 암호화가 가능하며, 네트워크 장비는 패킷 필터에 바탕을 두고 트래픽 흐름을 안전화 할 수 있다. 또한 모든 호스트에서 정보에 대한 각 접근점과 관련된 서비스를 가질 수 있으며, 중요 정보에 접근하도록 하는 각 서비스는 호스트 인증(Host Authentication), 사용자 인증, 키 인증 등의 상이한 보안 기법을 제공할 수 있다.

① 암호화

LAN 또는 WAN을 지나가는 중요 정보를 암호화함으로써 비인가 접근을 막을 수 있다. 암호화는 이 경우에 코드화(encode)를 의미하며, 암호장비는 전송되는 정보를 스크램블 하거나 코드화하기 위한 알고리즘을 사용한다. 정보가 전달되면 수신 측에서 알고리즘의 역 수행으로 원래의 정보를 얻을 수 있게 된다. 암호화는 위성과 무선링크로 데이터 전송 시에 매우 유용한데, 이 경우에는 공중에서 인가되든 안되든 누구든지 신호를 수신할 수 있어 취약해 지기 때문이다. 암호와의 주 이점은 단지 인가된 사람, 즉, 암호화 키에 접근할 수 있는 사람만이 중요 데이터에 접근할 수 있다는 점이다. 그러나 그 방법은 절대 안전한 것은 아니다. 암호화된 데이터를 연구하는 사람은 대단히 복잡한 키도 깰 수 있기 때문이다. 예로, 많은 기관에서 사용되는 DES와 장비들은 최근 깨질 위기에 놓여 있다. 이러한 가능성 때문에 사용자들은 정기적으로 키를 바꾸길 원할 것이다. 이렇게 함은 암호화를 수행하는 각 장비에 새로운 키(또는 하드웨어, 소프트웨어)의 물리적 전송을 의미한다. 키의 물리적 전송은 시간 및 자원의 낭비일 수 있으나, 이는 키를 전송하는 가장 안전한 방법이다. 비록 암호장

비가 유지관리가 어렵다 해도 많은 조직은 중요 정보를 안전화 하기 위해서 이 방법 사용을 선호한다.

② 패킷 필터링

라우터나 브리지 같은 많은 네트워크 장비들은 네트워크나 MAC(Media Access Control) 주소에 기반을 둔 패킷 필터링을 수행할 수 있다. 패킷 필터링은 패킷이 중요 정보를 발생시키는 접근점에 도달하기 전에 불안전한 호스트 컴퓨터에 또는 호스트 컴퓨터로부터의 패킷을 정지시킨다. 이 방법이 방화벽(Firewall) 구성하는 기능의 한 원리이다. 그러나, 이 방법이 보안에 도움을 제공할 지라도 몇 가지 문제를 갖고 있다. 첫째로, 각 네트워크 장치 내에 패킷 필터를 구성할 필요가 있다. 이는 새로운 주소나 주소의 변경시 그 필터들을 바꿔줄 필요가 있다. 두 번째로, 필터를 사용함으로써, 불안전한 호스트 컴퓨터가 사용자에게 통보없이 주소를 변경한다면 동작이 되지 않는다. 예로, MAC 주소에 기반을 둔 세그먼트간에 패킷을 필터링하는 Ethernet 브리지를 고려해보자. 이제 MAC 주소는 일반적으로 Ethernet 인터페이스의 ROM 칩에 설정된다. 그러므로 불안전한 호스트 컴퓨터상의 인터페이스 보드가 변경되면, 새로운 보드는 같은 MAC 주소를 갖지 않을 것이다. 이것은 결과적으로 더 이상 불안전한 호스트 컴퓨터에 또는 호스트 컴퓨터로부터 더 이상의 정보를 멈추게 하지 못한다. 이 문제는 악의있는 사용자뿐만 아니라, 새 보드가 새로운 MAC 주소를 갖고 있음을 인식하지 못하고서 결함이 발견되거나 또는 업그레이드를 목적으로 인터페이스를 변경하는 네트워크 관리자에 의해서 발생될 수 있다. 어떤 호스트 컴퓨터는 이러한 문제를 피하기 위해서 사용자들이 자신의 MAC 주소를 셋업하도록 소프트웨어 구성 파라미터를 제공하기도 한다.

③ 호스트 컴퓨터 인증

호스트 인증 방법은 발원지(Source) 호스트 ID에 근거한 서비스에 접근을 허가하는 것으로, 이 호스트 ID는 IP, DECnet, X.25 또는 앞 절에서 언급한 MAC 주소에 의해서 사용되는 것과 같은 일반적으로 네트워크 주소이다. 많은 컴퓨터 서비스들이 호스트 인증기법을 사용한다. 일반적인 예로 시리얼 연결을 통해 X.25를 거쳐 통신하는 컴퓨터는 발원지 X.121 주소에 기반을 둔 호출을 받거나 거절을 결정할 것이다. 아니면, 하나의 컴퓨터는 모든 가능한 발원지 네트워크 주소의 일부에 혹은 한 서비스에 접근함을 허락하지 않을 수도 있다. 왜냐하면, 호스트 인증은 네트워크 주소에 기반을 두고 있기 때문이다. 많은 네트워크 장비들 또한 이러한 일을 수행하는데 도울 수 있다. 토큰링 브리지는 접근 제한을 셋업함으로써 어떤 발원지 시스템만이 브리지의 다른 편에 있는 컴퓨터에 자료를 전송할 수 있게 할 수 있다. 비록 사용자들이 호스트를 안전하게 하기 위한 한 가지 방법으로 이것에 전적으로 의존할 필요가 없을지라도 패킷 필터 역시 호스트 인증을 수행함에 도움을 줄 수 있다. 다른 예로, 중앙 네트워크 관리 시스템은 네트워크 운영자들이 사용할 수 있도록 큰 칼라 디스플레이를 갖고 있다. 비록 네트워크 관리 시스템상에 많은 일들이 데이터 네트워크 상의 여러 컴퓨터에서 수행될지라도, 각 네트워크 관리 프로세스는 그 결과를 중앙 시스

템의 디스플레이에 결과를 보여줄 수 있다. 중앙 시스템은 디스플레이를 사용하고자 하는 컴퓨터가 인증된 호스트인지를 확인하기 위해 호스트 인증을 사용할 수 있다. 널리 알려진 X11 윈도우 시스템이 이 방법을 사용한다. 이 경우에 X 서버는 호스트 이름을 사용하며, 이 호스트 이름은 네트워크 주소로 변환되어 컴퓨터로 하여금 국지(local) 디스플레이에 접근하도록 인가한다. PC 파일 서버는 종종 어떤 컴퓨터를 파일 시스템에 접근토록 허가할 것인가를 결정하기 위해 호스트 인증을 사용한다. 예를들어, 디스크 없는 PC가 전원이 켜지면 사용가능한 어떤 파일 서버에 파일 시스템을 요구할 수 있다. 만일 특정 서버가 중요 정보를 갖고 있다면, 우리는 모든 PC들이 이 파일 시스템을 사용토록 하지는 않을 것이다. 우리는 네트워크 주소로 식별된 인가된 PC로부터만 파일 시스템에 접근하도록 허가함으로써 이것을 실현할 수 있다. 호스트 인증은 어떤 접근점의 보안을 제공하기에 유용하지만 완전하지는 않다. 만일 한 컴퓨터 상의 어떤 서비스가 중요 정보에 접근한다면, 단지 발원지 호스트의 ID를 아는 것 만으로는 정보를 제공받기에는 충분한 자격이 되지 못한다. 또한 다음 예를 고려해 보자. 호스트 "trust"는 사원들에게 사내용으로 프로그램을 복사할 수 있도록 하는 서비스를 제공한다고 가정하자. 이 프로그램을 보호하기 위해 "trust"는 단지 호스트 "innocent" 만이 그 프로그램에 접근할 수 있도록 호스트 이름을 사용한다. 그러나 한 사용자가 개인용으로 "trust"에서 그 프로그램을 복사하기로 한다고 가정하자. 이렇게 하기 위해서 그 사용자는 "innocent"를 끄고, 그 컴퓨터를 "innocent"와 같은 주소를 갖는 "devious"로 재구성할 수 있다. 그리고는, "devious"가 "trust"에서 프로그램에 접근했을 때, 이것을 허락할 것이다. 왜냐하면 "trust"는 "devious"가 "innocent"라고 생각하기 때문이다. 또 다른 예로, 호스트 "master"는 사용자들이 개발중인 소프트웨어를 원격으로 수행토록 허락하는 서비스를 제공한다고 가정하자. "master"에 있는 소프트웨어는 그 조직내의 누구와도 공유되지 못하므로, 우리는 호스트 "servant"에 있는 사용자만이 그 프로그램을 수행할 수 있도록 하는 호스트 인증 방법을 사용할 수 있다. "servant"의 시스템 관리자는 우리가 오로지 새로운 소프트웨어에 접근할 수 있는 인가된 사람이라고 확신하여 "servant"에 계정을 갖도록 했다고 가정하자. 그러나 우리는 "servant"에 로그인하는 정당한 사용자는 "master"에서 그 소프트웨어를 실행시킬 수 있음을 알 것이다. 따라서 우리는 다음 단계로 "master"에서 그 소프트웨어에 대해 보안성을 높이기 위해 사용자 인증을 채용해야 할 것이다.

④ 사용자 인증

사용자 인증은 서비스에 대해서 사용자 접근을 허가하기 전에 각 사용자를 식별할 수 있는 서비스를 통해서 접근점을 안전하게 하는 또 다른 방법을 제공한다. 사용자 인증은 각 서비스들이 정확한 사용자를 식별할 수 있도록 하기 때문에, 호스트 인증보다는 어떠한 서비스에 대해 미세한 수준의 제어가 가능하다. 사용자를 구별하는데 사용되는 일반적인 방법은 패스워드이다. 그러나, 패스워드가 효과적일지라도 완벽하지는 않으며, 우리가 바라는 만큼 항상 안전하지는 않다. 패스워드 사용에 따른 한

가지 문제점은 몇몇 네트워크 서비스들이 패스워드를 발원지 호스트에서 목적지 호스트에 전송함에 있어 평문 그대로 사용한다는 것이다. 평문의 사용은 단지 패킷을 잡아 봄으로써 패스워드를 누구나 발견할 수 있게 된다. 이 문제에 대한 일반적인 해결방법은 암호화된 패스워드를 보내는 것이다. 그러나, 이 방법은 암호화 키가 깨지면(복잡한 키를 깨는데 오랜 시간이 소요될지라도) 이 방법도 깨지게 된다. 패스워드를 채용함에 또 다른 문제점은 사용자들이 기억하기 쉽게 만드는 경향이라는 점이다. 따라서 쉽게 발견될 수 있음을 의미한다. 일반적으로 자주 사용되는 패스워드는 반복 시도를 통해서 쉽게 발견될 수 있는 일반 단어들이다. 대안으로 임의로 패스워드를 생성하거나 특수문자 또는 숫자를 포함시킴으로써 일반 단어가 아닌 패스워드를 제공하는 것이다. 그러나 이렇게 함으로써 기억하기에 어려워 결과적으로 사용자들이 보통 호스트 근처에 기록을 해 놓게 된다. 이러한 단점에도 불구하고, 패스워드는 아직도 사용자를 식별하는데 자주 사용된다. 관리자들은 단순히 이들의 취약성을 인식하고 그 취약성으로부터 보호할 필요가 있다. "master"와 "servant"를 사용해서 우리의 예를 들어 보자면, 우리가 어떻게 보안 관리를 더욱 효과적으로 설치할 수 있을지를 생각해 보자. "master"에 있는 소프트웨어를 접근하기 위해서 "servant"에 계정을 갖도록 허가 하기 보다는, "master"에 정당한 계정을 갖는 사용자에게만 접근하도록 하는 서비스를 우리는 사용할 수 있다. 이러한 환경하에서, "master"에 있는 소프트웨어를 실행시키기 위해서 사용자는 우선 인증된 호스트에서 시작해야 하며, 그 다음에 유일한 패스워드를 넣어야만 한다. 다른 예로, "snoopy"라는 컴퓨터는 사용자가 어떤 조직의 고객 정보 데이터 베이스를 접근하도록 하는 서비스를 제공한다 하자. 그 조직의 고객 서비스 부서에서 일하는 사람들만이 이 중요 정보에 접근이 인증된다. 따라서, 고객 서비스 대행 업체가 고객에 관한 정보를 필요로 할 때, 그들은 "snoopy"에 연결되는 자신의 PC에서 프로그램을 사용한다. 그러나, "snoopy"가 대행 업체에게 정보를 주기 전에, 데이터 베이스 프로그램을 그 대행 업체에 데이터 베이스를 사용하는 인증으로서 사용자를 식별하는 패스워드를 요구한다. 그리하여, 고객 서비스 대행 업체의 책상에 있는 모든 사용자들이 고객에 관한 정보를 얻을 수 없도록 할 수 있다. 비록 사용자 인증이 호스트 인증만을 수행 했을 때 보다 일반적으로 더 효과적일 지라도 이 방법은 한가지 분명한 관점을 갖고 있다. 거의 모든 사용자 인증 방법은 컴퓨터의 정확한 구성에 달려 있다. 분명 컴퓨터가 서비스를 위해서 사용자 인증을 제공한다면 모든 사용자를 위해서 똑 같이 패스워드를 만든다면 원하는 보안은 실현 될 수 없다. 호스트 인증과 사용자 인증을 함께 적용하면 한 방법만을 사용하는 것보다 접근점을 안전하게 하는데 더욱 효과적인 수단을 제공할 수 있다. 다시 "snoopy"의 예로 돌아가서 우리가 사용할려고 했던 방법은 패스워드를 통해서 각 사용자 인증을 하는 것이었다. 그러나 이것이 우리가 원하는 모든 보안을 제공하겠는가? PC 데이터 베이스 접근을 위한 계정의 패스워드를 갖는 각 사용자는 "snoopy"로부터 중요 정보에 접근할 수가 있다. 보안성을 높이기 위해서 우리는 이러

한 서비스에 대해 호스트 인증과 사용자 인증 모두를 적용하기를 원한다. 이 2계층(two-layered) 접근 방법은 서비스를 요청하는 사용자는 인증된 호스트에서만 들어올 수 있고 그들은 인증된 사용자임을 확인 할 것이다.

⑤ 키 인증

키 인증 시스템은 도착지(Destination) 대상 호스트에서만 의존하지 않는 방법으로 호스트 인증과 사용자 인증 둘 모두를 실현하는 수단을 제공한다. 키 인증은 키 서버라는 네트워크에 연결된 호스트를 할당 함으로써 이루어 진다. 키 서버는 인증된 사용자에게 키 발급을 해줄 책임을 지고 있다. 어떤 서비스가 요청 될 때 발원지 컴퓨터가 키를 키 서버에 요청한다. 그때 서버는 사용자로 하여금 인증을 위한 패스워드를 치도록 한다. 이제 키 서버는 발원지 컴퓨터와 그 서비스를 요청하는 사용자 모두를 식별 할 수 있게 된다. 이 자료와 키 서버내에 존재 하는 보안 규칙에 기반을 두고 서버는 유효한 키를 발급할 것이다. 이 시스템은 목적지 컴퓨터에서는 접근 요구가 유효한 키와 일치 할 때만 그 서비스를 허락하기 때문에 일을 계속 한다. 어떤 키 인증 서버에서는 유효한 키를 일정 시간 경과 후(8시간 정도)에 무효화 시키는데, 이것은 사용자의 세션을 멈추게 하는 결과를 가질 수 있다. 그러나, 이는 또한 하나의 유효 키가 무한정 접근을 허락하지 않음을 보장한다. 우리가 알 수 있듯이, 키 서버가 사용자를 인증하고 서비스에 접근을 허락하기 때문에, 엄격한 물리적 보안하에 있도록 할 필요가 있다. 키 인증을 사용하는 원격 로그인을 위한 요청 예는 다음과 같이 동작할 것이다.

1. 발원지 컴퓨터는 목적지 컴퓨터에게 원격 로그인 서비스를 요청한다.
2. 원격 로그인 프로세스는 사용자가 목적지 컴퓨터에 로그인 하도록 허락해 주는 키를 키 서버에게 요청한다.
3. 커 서버는 발원지 컴퓨터를 유효화(Validate)하고 그 사용자가 목적지 컴퓨터의 원격 로그인을 사용토록 인증됨을 보장해준다.
4. 모든 확인이 끝나면, 키 서버는 목적지 컴퓨터에 원격 로그인을 위한 유효한 키를 발원지 컴퓨터에게 발급해 준다.
5. 발원지 컴퓨터는 유효한 키를 갖고 목적지 컴퓨터에 원격 로그인 서비스를 요청한다.

키 인증 방법에서, 키 서버는 데이터 네트워크 서비스에 대한 접근점 보안을 관리함에 있어 중요시 해야 한다. 키 서버가 정확히 구성되고, 관리 되는 것 또한 실로 중요하다. 그러나, 키 인증을 위해서 발원지 컴퓨터 상의 각 서비스는 트랜잭션 시작점에 키 서버에게 키를 반드시 요청해야만 한다. 더욱이 목적지 컴퓨터상의 서비스는 각 요청이 유효한 키에 의해 수행될 때만 서비스를 위한 요청을 수락해야만 한다. 이는 우리가 키 서버를 단순히 설치할 수 없고, 키 인증을 사용하여 시작할 수 없음을 뜻한다. 여러분의 모든 응용 프로그램과 서비스는 또한 키 서버를 사용하도록 변경 되어야만 한다. 키 인증을 위해서 최근 MIT의 "Kerberos" 서비스를 UNIX 컴퓨터에 널리 보급하고 있다. 오늘날 많은 컴퓨터 업체들이 몇몇 형태의 키 인증 시스템을 제공하고 있다.

2.2.4 안전한 접근점의 유지관리

네트워크 접근점을 효율적으로 안전하게 하기 위한 마지막 단계로서 유지관리를 들 수 있다. 앞에서 언급한 바 있는 데이터 네트워크에 대한 보안 대책은 안전하게 최선의 상태로 유지하는 일은 조직으로 하여금 시간과 자원을 필요로하는 어려운 일이다. 그러나, 설사 잘 계획되고 잘 구축이 되었다 할지라도 보안 시스템이 완전하게 유지되고, 수정되도록함도 불가피하게 필요하다. 유지관리에 대한 핵심은 잠재적이거나 실제 보안 침투를 실행시키는 것이다. 이 경우에 네트워크 보안을 감사할 책임이 있는 관리자에 의해 실시될 수 있다. 예로서, 그들은 감사를 위한 근거로서 잠재적인 네트워크 접근점의 네트워크 관리자 문서와 필요한 보안사항을 사용할 수도 있다. 어렵게도 오늘날 시중에 있는 네트워크 소프트웨어에 관련된 최신 자료들의 유지는 또 다른 큰 일이다. 따라서, 이런 경우에는 때때로 감사인이 하고자 하는 가장 좋은 방법은 보안 관리 중요 사항과 이에 대한 조직의 지침을 이해하는 것이다. 다른 상황에서 네트워크 관리자는 분명하게 알려진 보안문제의 확인을 위해서 호스트 상에 관련 프로그램을 설치할 수도 있다. 간단한 프로그램으로 패스워드를 시도 하거나 임의로 암호화 키를 가지고 보안 침투를 시도할 수도 있다. 더욱 정교한 프로그램으로 여러 방법을 이용하여 컴퓨터 네트워크에 공격을 수행해 볼 수 있다. 이 두 경우에 각 프로그램은 네트워크 관리자에게 보안 침투에서의 성공 또는 실패를 통보할 수 있다. 이러한 접근 방법의 장점은 비인가자에 의한 침투나 접근점에 발견된 문제가 관리자로 하여금 해당 접근점을 막을 수 있다는 점이다. 또 다른 방법은 취약점을 찾기 위해 포상 또는 현상금을 거는 방법이다. 여기에서 보안을 보장하기 위해 제안된 어떤 방법도 적절한 유지관리가 불가능 할 것이다. 감사는 매일 수행될 수 있으며, 보안성을 시험하는 프로그램은 모든 가능한 허점을 확인할 수는 없다. 네트워크 관리자는 적합한 보안대책을 이해하고, 조직을 위해 필요한 노력을 경주할 필요가 있다.

2.3 공중 네트워크에의 연결

2.2절에서 호스트에 대한 서비스로서 보안 관리를 어떻게 실행할 것인가를 다루었다. 데이터 네트워크을 공중 네트워크에 연결하지 않는 조직은 앞서 설명한 단계로서도 조직에서 필요한 보안을 제공함을 알 수 있을 것이다. 그러나, 공중 네트워크에 연결되는 데이터 네트워크을 갖는 조직에 대해서는 좀 다른 보안 관리 방법을 실행할 필요가 있다. 다음의 3가지 형태의 접근방법이 공중 데이터 네트워크에서부터 그 조직의 데이터 네트워크에 이르기까지 적용이 가능하다.

① 접근 불허
② 접근 완전 개방
③ 제한적 접근

공중 데이터 네트워크 상에서 어떠한 원격 로그인 접근을 허용하지 않는 사설 데이터 네트워크는 단순히 전자우편을 보내고 받는 수단으로서만 공중 네트워크에 연결하여 사용할 것이다. 예를 들어, 단지 모뎀을 통해서 몇 시간 동안만 공중 데이터 네트워크에 우편을 보내고, 접수할 목적으로 연결된다. 공중 데이터 네트워크와의 모든 거래(Transaction)는 그 조직의 데이터 네트워크내에서부터 제한될 것이다. 이 방법에 있어서 그 조직은 어떠한 접근

점이 존재하지 않기 때문에 공중 데이터 네트워크에 대한 접근점을 찾을 필요가 없다. 반대로, 그 조직이 자신의 컴퓨터와 공중 데이터 네트워크 사이에서 어떤 거래에 대한 어떠한 제한도 가하지 않는다면, 모든 보안 관리는 그 조직내의 각 개인 컴퓨터까지에 존재해야만 한다. 이러한 구성에서, 그 조직은 중요 정보를 허용하기 전에 호스트 인증과 사용자 인증을 컴퓨터가 수행하고 있는한 어떤 데이터든 그 네트워크로 들어갈 수 있도록 허락할 수도 있다. 그러나, 그 조직의 대부분의 컴퓨터에 호스트 또는 사용자 인증을 수행하지 않고 공중 네트워크에 있는 어떤 서비스에 접근하기를 원하고, 어떤 서비스를 공중 네트워크에 제공하기를 원한다면, 분명 공중 네트워크에의 개방 자체는 보안 위험에 노출될 것이다. 제한적 접근 방법으로 이러한 경우의 보안사항을 도울 수 있다. 제한적 접근을 허용함은 그 조직의 네트워크과 공중 네트워크 사이에서 일부 호스트만이 서비스를 제공하기 위한 인증을 수행함을 의미한다. 이러한 일반적인 각본은 네트워크 관리자가 공중 데이터 네트워크에 서비스를 제공하는 모든 컴퓨터를 통제할 수 있도록하여, 공중 네트워크에서 제한적 서비스가 가능토록하며, 그 조직의 접근점을 좀 더 안전하게 할 수 있도록 한다. 예로서, 어떤 조직이 자신의 데이터 네트워크에 "wideopen"이라는 컴퓨터를 갖고 있고, 이 컴퓨터는 그 조직내의 물리적인 네트워크 세그먼트에 있는 호스트라하자. 사용자의 보안 셋업은 조직내의 데이터 네트워크에 해당하는 어떠한 데이터도 우선 "wideopen"에 보내진다. 사용자는 이 "wideopen"에 대해 어떤 서비스를 허용토록 결정하기 위해 몇 단계를 수행하길 바랄 것이다. 종종, 그러한 서비스들은 공중 네트워크 사용자로 하여금 그 조직의 데이터 네트워크에 들어가기 전에 우선 멈춤지로서 또한, 사용자는 공중 데이터 네트워크와 그 조직에 "wideopen"이 전자우편 중계기(relay)로서 행동하도록 허락하길 원할 것이다. 그러나, 어떠한 원격 로그인이나 파일 전송을 허락하고 싶지는 않을 것이다. 이러한 기법들을 사용하여, 사용자는 조직이 공중 데이터 네트워크의 비인가된 사용자에 중요 정보를 노출할 것이라는 두려움 없이 공중 네트워크을 사용할 수 있다.

2.4 네트워크 보안 관리 도구

앞서 보았듯이 보안 관리는 네트워크 관리자로 하여금 호스트와 네트워크 자원에 대해 사용자 접근을 제한케함으로써 그리고, 보안 침투나 시도에 대해 그 관리자에게 보고케 함으로써 중요 정보를 보호하도록 할 수 있다. 네트워크 관리 시스템에서의 보안 관리는 소프트웨어 도구를 사용함으로써 실행된다. 이것이 어떻게 잘 수행되느냐는 관리자가 사용 가능한 도구의 기능에 달려있다. 다음에 3가지 보안 관리 도구의 예를 살펴보고자 한다.

2.4.1 단순한 도구

네트워크 관리 시스템상에서 보안 관리를 위한 단순도구는 보안대책이 어디에 존재하는가를 보여줄 수 있다. 그림 형태의 네트워크 지도에서의 입력에 따라, 이 도구는 사용자가 선택하는 어떠한 장치나 호스트에 적용가능한 모든 보안대책을 스크린에 보여줄 수 있다. 추가적으로 어떤 사용자나 네트워크 주소를 제한하도록 네트워크내에서 모든 위치를 변경할 수 있도록 해 줄 수 있다. 그 도구는 구성 데이터 베이스(Configuration Database)에 질의(query)해서, 필요한 정보를 스크린에 보여준

다. 이 보안 관리 도구는 이미 네트워크 관리 시스템에서 제공하는 구성 관리 정보를 사용하여, 네트워크에서 복잡한 연결 또는 접근 가능한 문제를 해결하는게 매우 유용할 수 있다.

2.4.2 복잡한 도구

좀더 개선된 도구는 중요 정보에 대한 접근점을 관찰하는 실시간 응용프로그램을 갖도록 설계될수 있다. 가능성 있는 보안문제가 발생하는 즉시, 이 응용프로그램은 그림으로된 네트워크 지도에 있는 영향을 받는 호스트나 네트워크 장비의 색깔을 변경시킬 수 있다. 또는 다른 사건들로 인해 색깔에 혼동이 생길 때는 관심을 끌도록 다른 방법으로 발견사실을 보고할 수 있도록 하거나, 시스템 벨을 울리거나, 자동적으로 네트워크 관리 시스템 상에서 수행되는 윈도우에 발견 사실을 로깅하도록 설계할 수 있다. 예로, 그러한 응용 프로그램은 어떠한 사용자가 컴퓨터에 원격로그인을 여러번 실패 했을 때 보고할 수 있다. 이 보고는 그 사건을 보고함에 있어 컴퓨터의 성능에 따라 2가지 방법으로 실행될 수 있다. 만일 실패한 로그인 시도에 관심을 갖는 네트워크 관리 시스템에 사건을 보고할 수 있다면, 이는 바람직하다. 그렇지 않으면, 보안 관리 응용프로그램이 실패한 원격 로그인 시도에 관하여 컴퓨터의 로그인 화일을 체크하기 위한 기능을 가질 필요가 있다(대부분의 컴퓨터는 추후 조사를 위해서 파일에 실패한 로그인 시도를 저장할 것이다). 그러나 이 방법은 보안 관리 응용프로그램으로 하여금 특정 파일 형식 만을 따르도록 하고 있다. 이 프로그램은 어떤 특정 서비스에의 사용자 접근 시도에 대해 거부함을 반복적으로 보고함과 같이, 좀더 유용한 정보를 제공토록 더 개량될 수 있다. 이러한 도구는 중요 정보에의 접근점을 갖는 서비스에 대해 비인자된 사용자 또는 호스트의 접근시도시 사용자에서 알리도록 설계할 수도 있다. 이렇게 함으로써, 이 도구는 호스트의 구성을 다시하도록 도와 줄 수 있다. 이 도구는 보안이 적용되는 호스트나 장치에 대해 질의를 우선 필요로 할 것이며, 적절한 정보를 위하여 사용자에게 질의를 할 것이다. 예로, 보안을 네트워크 주소별로 제한 적용할 때는 리피터, 브리지, 전단 프로세서(Front-End-Proccessor), 라우터에 적용되기 때문에 매우 방대하다. 더욱이 각 장비 제작업자에 따라 보안 응용이 완전히 상이할 수 있다.

2.4.3 발전된 도구

발전된 보안 관리 도구는 복잡한 도구보다 더 개량되어, 보안관련 사항에 관하여 사용자에게 안내하기 위해 모아놓은 관련 교통 패턴 데이터를 사용한다. 더 완전한 보안 관리는 단순도구와 복잡한 도구에서 언급한 기능 뿐만아니라 이러한 기능도 필요로 한다. 개선된 도구는 사용자가 컴퓨터 혹은 장치에 설치코자 하는 보안 형태를 검사하여, 그 설치에 대한 가능한 반향으로 경고를 줄 것이다. 이 도구는 어떻게 보안대책이 네트워크에 영향을 끼쳤는지를 분석하기 위하여, 역사 자료와 함께 사용자로부터 입력을 받아 사용할 것이다. 예로, 우리가 데이터 네트워크의 두 지역 "chaos"와 "ordered"간의 모든 교통을 멈추게 하는 호스트 인증기법을 설치할 것이다. 이 도구는 사용자에게, 계획된 보안이 데이터 네트워크상의 교통을 85%를 멈추게 했다고 알려줄 것이다. 이제 이 비율은 당신이 원하는 결과일 수 있을 것이다. 다른 한편으로, 이 결과는 시스템 또는 기법 설계상의 실수 일 수도 있다. 어쨌든, 개

선된 도구는 당신의 노력을 재요구하거나 존재할 수 있는 구성상의 실수를 경고할 것이다.

2.5 보안 사건 보고

실시간 응용프로그램과 같이 보안 정보를 종합하고, 보고하는 감사 추적은 보안 관리를 수행할 때 중요하다. 감사 추적을 할 수 있도록 도와주는 응용프로그램으로, 사용자는 접근점이 위협받을 때의 패턴을 결정하여 비인가된 접근을 멈추게 할 수 있다. 또한 실시간 응용프로그램으로 그 데이터로부터 구성의 실수 결과로인한 비인가 요청을 찾아낼 수 있도록 도와줄 수 있다. 예로, 사용자가 다음 상황에 처해 있다고 가정해 보자. 매일 오후 2:00경에 공중 데이터 네트워크으로부터 원격 로그인을 위해 비인가된 요청이 일어나고 있다. 이 정보로부터 사용자는 발원지 컴퓨터를 파악할 수는 있지만, 특정 사용자를 알 수는 없다. 이 발원지 컴퓨터는 외부 회사의 것이며, 또한 네트워크내의 목적지 컴퓨터가 항상 같음을 알 수 있을 것이다. 그 목적지 컴퓨터인 "Lotsainfo"는 분류된 정보에 관한 문서를 갖고 있으며, 매일 조직의 뉴스를 종합하여 종업원에게 제공되는 서비스의 일부이다. 사용자의 첫 행동은 오후 2:00에 시스템에 관한 행위를 관찰하도록 요구하는 내용의 전자우편을 발원지 시스템의 관리자에게 보내는 것일게다. 그러나, 이 시스템은 약 200여 사용자를 갖고 있다. 즉, 모든 원격 로그인 시도의 발생을 관찰하는 것도 어려울 수 있다. 며칠 후 발원지 시스템의 관리자가 여러분에게 오후 2:00경에 어떤 별다른 행위를 하지 않았음을 알린다. 그러나, 매일 종합보고를 생산하는 사용자의 보안 관리 응용프로그램은 매일 "Lotsainfo"에 대한 원격 로그인 요청을 계속 보여준다.

3. OSI 보안 관리 표준화

네트워크 관리(Network Management)를 위한 OSI 기반 프로토콜 표준화는 OSI 기반 네트워크의 보안 보호(Security Protection)를 지원한다. 네트워크 관리를 보호하기 위해 필요한 보안기술들은 성숙되고 있으며, 제품에 실용화되고 있는 상황이다. 이 분야의 성숙으로 때로는 광범위한 보안 기술 가운데에서 어떤 기술 요소를 선택해야 하는가의 어려움에 봉착하게되며, 보안 대책을 네트워크의 각 계층에 위치시킴에 있어서도 많은 선택들이 존재할 수 있다[2]. 네트워크 관리 프로토콜은 시스템, 네트워크, 네트워크 요소를 관리하기 위한 수단을 제공한다. 이 프로토콜은 구성관리(Configuration Management), 계정관리(Accounting Management) 및 사건 로깅(Event Logging)과 같은 관리 기능들을 지원하며, 네트워크의 문제의 진단을 돕기 위한 편의를 제공해준다. 네트워크 관리 프로토콜은 그 자체가 응용 프로토콜이며, 이 프로토콜은 다른 응용 프로그램과 같은 방법으로 하위 계층 통신 기능을 이용한다. 개방형 시스템 네트워크 관리 표준으로 OSI 관리를 위한 국제 표준에서는 CMIP(Common Management Information Protocol)를 정의하고 있다. 여기에서는 OSI 네트워크 관리 표준의 보안 측면을 다루고자 한다. 이 주제는 두 가지 서로 상이한 측면을 같이 다룬다.

- 보안 서비스 규정에 대한 네트워크 관리 프로토콜에 의한 지원(보안의 관리로 알려짐)
- 네트워크 관리 통신을 보호하기 위한 수단(관리의 보안으로 알려짐)

다음에서는 OSI 관리 구조와 표준에 대한 개요와 OSI 관리의 보안 측면(보안 경고 보고, 감사 추적 기능, 접근 제어, CMIP 보안을 포함)을 다루기로 한다.

3.1 OSI 네트워크 관리 프레임워크

OSI 관리 표준은 ISO/IEC JTC1/SC21 소위원회에서 ITU와 공동으로 개발되었다. 이 표준은 CMIP 규격에 덧붙여 몇몇 네트워크 관리 프레임워크를 포함하고 있다. 그 개요를 살펴보면 다음과 같다. 첫 번째 OSI 관리 표준[4]은 1989년에 발간되었으며, OSI를 위한 관리 프레임워크를 정의(ISO/IEC 7498-4)[5]하고 있다. 여기에서는 2가지 형태의 관리를 구분하고 있는데, 하나는 OSI 시스템 관리로, 일반적인 시스템의 관리를 지원하고 있다. 다른 하나는 OSI 계층 관리로 특별한 OSI 계층 개체(Entity)의 관리에 관계하고 있다. 관리 프레임워크는 5가지의 관리 기능별 영역인 구성관리(Configuration Management), 결함관리(Fault Management), 계정관리(Accounting Management), 성능관리(Performance Management) 및 보안 관리(Security Management)를 정의하고 있다. 관리 프레임워크는 후에 시스템 관리 개요(ISO/IEC 10040)[9]에 의해 확장되었다. 이 표준은 OSI 관리 표준에 사용되는 용어를 정의하고, 기본적인 OSI 관리의 개념을 설명하며, 여러 가지 표준간의 관계를 기술하고, 이러한 표준에 관한 적합성을 위한 규칙을 설정하고 있다. OSI 관리 표준은 객체 지향 모델링 기법을 채용하고 있다. 관리될 대상 자원은 관리 대상 객체(managed object)로서 모델링된다. 관리 대상 객체는 그들이 받아들이는 행동과 그들이 내보내는 통보, 그들이 볼 수 있는 속성, 그들이 보여주는 행위에 의해 특징 지워진다. 실제의 네트워크에서 관리 대상 객체의 범주는 가상적으로 무한정이며, 관리 대상 객체의 정의는 다른 조직에 의해 만들어 질 수 있다. 관리 대상 객체는 봉쇄(Containment)에 근거하여 계층적으로 조정된다. 예로서, 하나의 파일은 여러 개의 레코드들을 포함할 수 있으며, 이 레코드들은 여러 개의 필드를 포함할 수 있다. 각 시스템을 위한 봉쇄 트리는 맨 위(top)에 시스템 관리 대상 객체를 갖는다. 완전한 정보 모델은 관리 정보의 구조 표준(ISO/IEC 10165)[11]에 설명되어 있으며, 관리 정보 모델, 관리 정보의 정의, 관리 대상 객체의 정의를 위한 지침, 일반 관리 정보 등과 같은 여러 개의 부분들을 포함하고 있다. 더욱 발전된 표준으로서 ISO/IEC 10164[10]는 앞서 언급한 5가지 관리 기능별 영역에서의 여러 가지 관리 기능을 정의하고 있다. 한편, OSI의 구조적인 프레임워크는 관리하는 시스템과 관리되는 대상 시스템으로 구성되며 1개 이상의 관리 대상 객체를 포함한다. 두 시스템간에는 CMIP 응용 계층 프로토콜을 통하여 통신한다. CMIP는 ISO/IEC 9596[12]에 나타나 있다. CMIP에 의하여 제공되는 서비스는 CMIS (Common Management Information Service)로 알려져 있으며 ISO/IEC 9595[13]에 기술되어 있다. CMIP는 원격 운영 모델을 채용하고 있는 요청/응답 프로토콜이다. 그 서비스에는 2가지 형태가 제공된다.

- 관리 대상 객체에 의해 생성된 사건 통보의 전달(M-EVENT-REPORT 서비스)
- 관리하는 시스템에 의하여 호출되고, 관리 대상 객체에서 목표하는 동작의 전달

후자의 동작은 다음을 포함한다.

- M-GET : 관리 대상객체의 속성 값에 따른 정보를 얻어옴
- M-SET : 1개 이상의 관리 대상 객체의 1개 이상의 속성 값을 변경
- M-CREATE : 관리 대상 객체의 인스탄스(Instance)를 생성함
- M-DELETE : 환경으로부터 1개 이상의 관리 대상 객체를 제거함
- M-ACTION : 관리 대상 객체의 부분으로서 명시된 사전 정의된 행동 절차를 호출함
- M-CANCELGET : 긴 GET 동작의 연산을 중지함

3.2 JTC1/SC21 WG4[2]에서의 OSI 관리

OSI 관리 표준은 "보안의 관리(Management of Security)"나 "관리의 보안(Security of Management)"을 구별하여 언급하지는 않고 있다. 그러나, 그 표준들은 이 두 가지에 다 해당되는 요소들을 갖고 있다. "보안의 관리"를 지원하기 위하여 보안 경보 보고 기능, 보안 감사 추적 기능 등 2가지의 중요한 보안기능이 보안 관리 영역에서 정의되고 있다. "관리의 보안"을 지원하기 위하여 접근 제어 모델과 접근 제어 정보 정의 지원이 제공된다. 또한 규약이 CMIP 프로토콜에서 제한된 보안 기능을 위해서 만들어 진다. 한편, OSI 시스템 관리를 위한 ISO 프로젝트 10164에서는 다음과 같은 주요 보안 주제를 다루고 있다.

- DIS 10164-8 : 보안 감사 추적 기능 (Security Audit Trail Function)[18]
- CD 10164-7 : 보안 경고 보고 기능 (Security Alarm Reporting Function)[17]
- DIS 10164-9 : 접근 제어를 위한 객체 및 속성(Objects and Attributes for Access Control)[19]

3.2.1 보안 감사 추적 기능 (DIS 10164-8 : Security Audit Trail Function)

이 권고안은 보안 감사 추적 기능을 정의한다. 보안 감사 추적 기능은 중앙 집중형 또는 분산형 관리 환경에서 응용 프로세서에 의해 사용될 수 있는 시스템 관리 기능이며, 이 관리 환경에서는 시스템 관리를 목적으로 정보와 명령을 주고 받게 된다. 보안 감사 추적은 어떤 네트워크를 안전하게 함에 중요한 역할을 수행한다. 이 표준화 권고안에서는 다음과 같은 내용을 담고있다.

- 보안 감사 추적 보고 기능을 지원하기 위해서 필요한 서비스 정의를 위한 사용자 요구사항을 설정
- 보안 감사 추적 보고 기능에 의해 제공되는 서비스를 정의
- 그 서비스를 제공하기 위해 필요한 프로토콜 설정
- 그 서비스와 관리 통보와의 관계를 정의
- 적합성 요구사항(Conformance requirement) 설정

3.2.2 보안 경고 보고 기능 (CD 10164-7 : Security Alarm Reporting Function)

이 권고안은 보안 경보 보고 기능을 정의한다. 인증, 접근 제어, 비밀성, 무결성의 보안 서비스 모두에 발생될 보안 위협으로부터 보호할 목표를 갖고 있다. 그러나 이러한 서비스들은 항상 완전하게 제기능을 할 것으로 생각할 필요는 없다. 거기에는 적절치 못하거나 보호

메카니즘이 오동작 하거나, 예외적으로 교묘하거나 고질적인 공격 또는 메카니즘을 극복할 수 없는 환경(예로, 패스워드 분실 등) 때문에 항상 보안상 위험이 발생될 우려가 있다. 따라서 보안 위협이나 의심스러운 일이 발견될 때 이러한 사실들을 운영자나 관리자, 관리 책임자에게 보고를 할 필요가 있다. 이러한 보안 경보를 통해서 의심스러운 사용자에 대한 감시와 권한의 취소 또는 더욱 강한 보안 메카니즘을 호출하거나 결함이 발생한 네트워크 또는 시스템 요소를 수리하는 등의 후속 조치를 할 수 있게 해준다. 보안 경보는 원칙적으로 어떠한 네트워크이나 시스템 요소에 의해서 발견될 수 있는 보안 관련 사건에 의해 야기될 수 있다. 관리 모델에서는 사건을 발견하는 요소가 관리 대상 객체가 된다. 보안 경보는 M-EVENT- REPORT를 통해서 관리하는 시스템에 조언을 주게된다. 보안 경보 보고 기능 표준(ISO/IEC 10164-7)에서 M-EVENT-REPORT 호출시 전달되는 정보를 기술하고 있다. 교환시에 사용되는 축약 구문(Abstract Syntax)은 관리 대상 정보 정의(ISO/IEC 10165-2)[20]에서 기술하고 있다. 보안 경보 보고에서 전달되는 인수는 다음의 3가지의 범주로 나눌 수 있다.

- M-EVENT-REPORT에 공통되는 인수는 ISO/IEC 9595에서 정의하고 있다(즉, invoke identifier, mode, managed object class, managed object instance, event type, event time, current time).
- 관리 정보에 공통되는 인수는 ISO/IEC 10164에서 정의하고 있다(즉, notification identifier, correlated notifications, additional information, additional text).
- 보안 경보에 해당되는 인수(즉, 보안 경보 원인, 보안 경보 심각도, 보안 경보 발견자, 서비스 제공자).

여기에서, 사건 형태와 보안 경보 원인을 합치면 경보의 이유가 된다. 보안 경보 원인에 대한 해당되는 옵션과 사건 형태의 가능한 값은 무결성 위반, 동작상의 위반, 물리적인 위반, 보안 서비스 혹은 메카니즘 위반, 시간 영역 위반 등 이다. 보안 경보 심각도(Severity) 인수는 initiating 관리 대상 객체에 의하여 인지된 경보의 중요도를 나타낸다. 가능한 값들은 Indeterminate, Critical, Major, Minor, Warning 등이다. 보안 경보 발견자 인수는 경보 조건을 발견한 실체를 나타낸다. 서비스 사용자 인수는 서비스를 요청한 실체가 경보를 발생시킴을 나타낸다. 서비스 제공자 인수는 경보를 발생토록 유도한 서비스를 제공하는 실체를 나타낸다. 그 표준들은 이상과 같이 나타낸 값의 의미 이상을 설명하지 않고 있다. 따라서, 이러한 필드의 상세한 설명은 경보를 발생하는 관리 대상 객체 클래스의 표시자(Specifier)에게 또는 지역 보안 정책(Local security policy)에 맡기고 있다. 또한, 보안 경보 보고 기능은 중앙 집중형 또는 분산형 관리 환경에서 응용 프로세서에 의해 사용될 수 있는 시스템 관리 기능이며, 이 관리 환경에서는 시스템 관리를 목적으로 정보를 주고받게 된다. 이 표준안은 ISO 7498-4[5]에 의해 정의된 응용 계층에 위치하며, ISO/IEC 9594에 의해 제공되는 모델에 따라 정의된다. 시스템 관리 기능의 역할은 CCITT 권고안 X.700(ISO/IEC 10040)[10]에 기술되어 있다. 시스템 관리 기능에 의해 정의되는 보안 경보 통보(Security alarm notification)는 운영상의 조건, 서비스의 질, 보안에 관한 정보를 제공한다. 보안 관련 사건은 곧 보안 규약에 관계된 것이다. 보안 정책은

보안 관련 사건이 발생했을 때마다 취해야할 행동을 결정하게 된다. 예로서, 보안 정책은 보안 관련 사건이 발생했을 때, 보안 경보 보고가 이루어지도록 하고, 보안 감사 추적에 사건 레코드가 만들어지며, 문턱 값을 증가시키고, 혹은 그 사건을 무시하거나 이러한 행위를 통해 적절한 조치를 취하도록 규정한다. 이 표준안은 보안 경보 보고에만 관련된다. 이 표준화 권고안에서는 다음과 같은 내용을 담고 있다.

- 보안 감사 추적 보고 기능을 지원하기 위해서 필요한 서비스 정의를 위한 사용자 요구사항을 설정
- 보안 감사 추적 보고 기능에 의해 제공되는 서비스를 정의
- 그 서비스를 제공하기 위해 필요한 프로토콜 설정
- 그 서비스와 관리 통보와의 관계 정의
- 적합성(Conformance) 요구사항 설정

3.2.3 접근 제어를 위한 객체 및 속성 (DIS 10164-9 : Objects and attributes for access control)

이 표준화는 OSI 관리 서비스와 프로토콜을 사용하는 접근 제어 규약에 적용할 수 있는 규격이다. 이 규격은 다음과 같은 내용을 담고 있다.

- OSI 관리 서비스와 프로토콜을 사용하는 접근 제어 규약을 위한 사용자 요구사항 설정
- OSI 관리 서비스와 프로토콜을 사용하는 관리 응용에 사용하기 위한 ISO/IEC 10181-3에서 정의한 전반적 접근 제어 모델의 해석 및 적용
- 접근 제어를 위한 절차 정의
- 시스템 관리를 위한 관리 대상 객체 클래스 및 속성 형태 정의
- 시스템 관리를 위한 접근 제어 정보의 교환에 필요한 프로토콜의 설정
- CMIP를 사용하는 관리에서 접근 제어 인수의 ASN(Abstract Syntax Notation) 규정
- 접근 제어를 지원하기 위한 인정 요구사항 규정

한편, 관리 자원의 접근제어에 대한 네트워크 관리는 자체적인 접근제어 요구사항을 가지고 있다. 누가 관리 행위를 호출하는지, 누가 관리 정보를 만들고 삭제하고 수정하고 혹은 읽을 수 있는지를 제어함이 필요하다. 그러한 접근 제어는 네트워크 관리 프로토콜을 사용하는 어떠한 네트워크에서도 중요하다. 왜냐하면, 네트워크 관리 자원에 대한 위협은 전체 네트워크에 대한 위협과 다를 바 없기 때문이다. 이러한 형태의 접근 제어가 ISO/IEC 10164-9(Object and Attributes for Access Control)[19]에서 설명된다. 이 표준은 시스템간에 접근제어 정보의 통신을 지원하기 위한 필요한 정보 객체 정의와 아울러 접근 제어 모델을 제시하고 있다. 접근제어 프레임워크 표준에 용어 및 개념적 모델이 ISO/IEC 10181-3[23]에서 설명되고 있다. 여러 가지 접근 제어 정책이 포함되어 있으며 여러 가지 접근 제어 메카니즘(접근 제어 리스트, capabilities, 보안 레이블, 내용 기반 제어 등을 포함)이 사용될 수 있다. 접근 제어 결정은 M-GET 또는 M-SET과 같은 관리 연산의 호출에 적용된다. 발원자(Initiator)는 관리하는 시스템(혹은 관리하는 사용자)이 되며 대상자(target)는 관리 대상 시스템의 정보자원이 된다. 서로 다른 대

상자 단위(target granularity)도 가능하다. 즉, 대상자는 관리 대상 객체, 관리 대상 객체의 속성, 관리 대상 객체의 속성 값 또는 관리 대상 객체의 행위일 수 있다. 따라서, 사용자가 어떤 관리 정보를 어떤 목적을 위해서 접근할 수 있는지에 대해서 세세한 부분에 이르기까지 제어할 수 있다. 접근요청을 허락할 것인지 거부할 것인지에 대한 결정은 접근 제어 규칙에 근거한다. 접근 제어 규칙은 관리 정보 사항으로서 표현될 수 있으며, CMIP 프로토콜을 사용하여 다루어질 수 있다(예, 읽기 또는 수정). Global rule, Item rule, Default rule 등 3가지의 서로 다른 형태의 접근제어 규칙이 구별화 된다. 여러 가지 규칙이 특정 접근 요청에 적용될 때는 서로 다른 형태의 규칙이 다음과 같은 순서를 갖게 된다.

(1) 접근을 거부하는 Global rule
(2) 접근을 거부하는 Item rule
(3) 접근을 허가하는 Global rule
(4) 접근을 허가하는 Item rule
(5) default rule

접근 제어 규칙은 보안 정책이 요구하는 실제의 어떠한 결정 과정에 근거할 수 있다. 규칙에 대한 하나의 규격은 Access permission, Initiator list, Target list, Scheduling conditions, State conditions, Authentication context 등과 같은 여러 개의 요소를 포함할 수 있다. 접근 제어 결정 절차는 다음과 같다. 첫째, 접근 요청과 함께 제출된 어떠한 접근 제어 정보(예로 제출된 접근제어 certificate 혹은 token)는 정당화될 필요가 있다. 발원자와 대상자에 적용하는 모든 접근 규칙은 그들의 global/item /default 표시에 따라 식별되고 그룹화 된다. 그리고 이러한 규칙들은 제한 조건(constraint)을 고려하여 적용된다. 규칙을 적용하는 방법은 사용되는 특정 접근 제어 메카니즘에 달려 있다. 접근 제어 리스트 메카니즘에 있어서는, 발원자의 식별은 적용 가능한 접근제어 리스트와 비교된다. Capability 메카니즘에 있어서는 발원자에 의해서 제출된 capability는 규칙에서 나타난 capability와 비교된다. label-based 메카니즘에 있어서는 발원자와 관련된 레이블은 규칙에 의해서 인식된 레이블 집합들과 비교된다. 문맥 기반 확인(Context-based check)은, 예로서 스케쥴링 조건, 상태 조건 혹은 인증 레이블 또한 적용될 필요가 있다. 접근 결정 후에 다른 행위가 일어날 필요가 있다. 결정을 내리기 위해서 사용된 정보는 임시로 똑 같은 발원자를 포함해서 향후에 결정을 위해서 저장된다. 대상자와 관련된 접근 제어 정보는 수정될 필요가 있다(예로서 관리 동작이 관리 대상 객체가 만들어지거나 삭제되어야 한다면). 보안 정책에 따라서 보안 경보 보고 혹은 보안 감사 추적 통보를 만들 필요가 또한 있을 것이다. 거부될 접근 사건에 있어서 발원자에게 응답하는 방법에는 여러 가지가 있다. 보안 정책은 접근 거부 오류 표시, 무응답, 거짓 응답(즉, 접근이 허용되는 발원자에게 나타난다), 혹은 응용관련 중지 등과 같은 형태의 응답을 규정할 수 있다. 위의 절차를 지원하기 위하여 원격으로 접근제어 결정을 내리는데 사용된 저장 정보를 관리할 필요가 있다(예로 생성, 수정). 이런 목적을 위해서 표준에서는 몇 가지 관리 대상 객체 클래스와 속성 형태 정의를 지원하고 있다. 이러한 정의는 ISO/IEC 10164-1[10]에서 정의된 절차를 이용하여 원격으로 접근제어가 다루어질 수 있도록 할 수 있다.

3.2.4 CMIP 보안

CMIP 프로토콜 사양은 최소한의 보안 특성을 포함한다. 사실 내장된 보안 특성은 오직 관련된 동작 호출과 함께 접근제어 허가권(certificate)을 나르기 위한 규정뿐이다. 아무런 특정한 허가권 형식도 강제적은 아니다. 그러나 유럽의 ECMA 그룹의 작업에 근거한 가능한 허가권 정의는 ISO/IEC 10164-9[19]에 첨부되어 있다. 이것은 CMIP 통신이 보호될 수 없음을 의미할 필요는 없다. 그 이유는 보안에 대하여, OSI 모듈화 접근 방법은 다른 곳에 추가되어 보호될 수 있도록 하기 때문이다. CMIP 세션의 전체적 데이터 무결성 및 비밀성은 종단 시스템 수준의 보안 서비스를 이용하여 제공될 수 있다. 더 많은 종합적 응용계층의 보안 서비스는 일반적인 상위 계층 보안 기능을 이용하여 추가될 수 있다.

4. 결 론

많은 조직들이 그들의 데이터 네트워크를 안전하게 관리하기 위한 노력에도 불구하고 단편적인 접근 방법만을 이용해 오고 있다. 네트워크는 더욱 분산되고 복잡해지는 경향이며, 이에 따른 보안관리도 점점 어려워지고 있는 추세이다. 아울러 네트워크 관리를 보호하기 위해 필요한 보안기술들은 성숙되고 있다. 이제까지 네트워크 관리 환경에서의 보안 관리의 이점 및 보안 서비스인 인증, 비밀성, 무결성, 접근제어 등에 초점을 맞추어 그 내용을 살펴보고, 아울러 최근의 표준화 활동, 소요 보안기술, 네트워크 관리 통신을 보호하기 위한 표준화 요소 등을 알아보았다. 네트워크 관리를 위한 OSI 기반 프로토콜 표준화는 OSI 기반 네트워크의 보안 보호를 지원한다. 네트워크 관리 프로토콜은 시스템, 네트워크, 네트워크 요소를 관리하기 위한 수단을 제공한다. 이 프로토콜은 구성관리, 계정 관리 및 사건 로깅과 같은 관리 기능들을 지원하며, 네트워크의 문제의 진단을 돕기 위한 편의를 제공해 준다. 네트워크 보안 관리는 기술적, 관리적, 물리적 대책 등이 함께 인식되고, 구현될 때 비로소 그 조직의 중요정보를 안전하게 유지 관리 할 수 있을 것이다.

참 고 문 헌

[1] Allan Leinwand & Karen Fang, Network Management - a Practical Perspective, Addison - Wesley, 1993

[2] Warwick Ford, "Security Techniques for Network Management," IEEE, 1992

[3] Warwick Ford, Computer Communications Security : Principles, Standard Protocols and Techniques, Prentice Hall, 1994.

[4] ISO/IEC 7498-2, Information Processing System - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture, 1989.

[5] ISO/IEC 7498-4, Information Processing System - Open Systems Interconnection - Basic Reference Model - Part 4 : Management framework, 1989.

[6] ITU-T X.800, Data Communication Networks : Open Systems Interconnection (OSI) : Security, Structure and Applications, 1991.

[7] ITU-T X.402, Data Communication Networks : Message Handling Systems : Overall Architecture, 1992. 9.

[8] ITU-T X.435, Data Communication

Networks : Message Handling Systems : Electronic Data Interchange Message System, 1991.

[9] ISO/IEC 10040: Information Technology - Open System Interconnection - System Management Overview (Also ITU-T Recommendation X.701)

[10] ISO/IEC 10164-1: Information Technology - Open System Interconnection - Systems Management: Object Management Function(Also ITU-T Recommendation X.730)

[11] ISO/IEC 10165-1: Information Technology - Open System Interconnection - Structure of Management Information: Management Information Model(Also ITU-T Recommendation X.720)

[12] ISO/IEC 9596: Information Technology - Open System Interconnection - Common Management Information Protocol Specification(Also ITU-T Recommendation X.711)

[13] ISO/IEC 9595: Information Technology - Open System Interconnection - Common Management Information Service Definition(Also ITU-T Recommendation X.710)

[14] ISO/IEC 10164-4: Information Technology - Open System Interconnection - Systems Management: Alarm Reporting Function (Also ITU-T Recommendation X.733)

[15] ISO/IEC 10164-5: Information Technology - Open System Interconnection - Systems Management: Event Report Management Function (Also ITU-T Recommendation X.734)

[16] ISO/IEC 10164-6: Information Technology - Open System Interconnection - Systems Management: Log Control Function (Also ITU-T Recommendation X.735)

[17] ISO/IEC 10164-7: Information Technology - Open System Interconnection - Systems Management: Security Alarm Reporting Function (Also ITU-T Recommendation X.736)

[18] ISO/IEC 10164-8: Information Technology - Open System Interconnection - Systems Management: Security Audit Trail Function (Also ITU-T Recommendation X.740)

[19] ISO/IEC 10164-9: Information Technology - Open System Interconnection - Systems Management: Object and Attributes for Access Control (Also ITU-T Recommendation X.741)

[20] ISO/IEC 10165-2: Information Technology - Open System Interconnection - Structure of Management Information: Definition of Management Information (Also ITU-T Recommendation X.721)

[21] ISO/IEC 10165-4: Information Technology - Open System Interconnection - Structure of Management Information: Guidelines for the Definition of Managed Objects (Also ITU-T Recommendation X.722)

[22] ISO/IEC 10165-5: Information Technology - Open System Interconnection - Structure of Management Information: Generic Management Information (Also ITU-T Recommendation X.723)

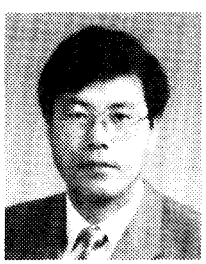
[23] ISO/IEC 10181-3: Information Technology - Security Frameworks in Open Systems - Access Control Framework (Also ITU-T Recommendation X.812)(Draft)

□ 著者紹介

박 태 규

1980년 10월 경북대학교 전자공학과(전산전공) 공학사
1981년 2월 ~ 1982년 12월 한국국방연구원 전산센터 연구원
1982년 12월 ~ 1992년 2월 한국전자통신연구소 선임연구원
1989년 8월 충남대학교 대학원 전산학과 이학석사
1996년 2월 성균관대학교 대학원 정보공학과 공학박사
1992년 3월 ~ 현재 한서대학교 전산정보학과 부교수

※ 관심 분야 : 컴퓨터 · 네트워크 보안, 병렬 암호화



강 창 구

1979년 2월 한국항공대학 항공전자공학과 공학사
1986년 2월 충남대학교 대학원 전자공학과 공학석사
1993년 8월 충남대학교 대학원 전자공학과 공학박사
1979년 ~ 1982년 한국공군 기술장교
1987년 ~ 현재 한국전자통신연구소 책임연구원, 부호4 실장

※ 관심 분야: 부호이론, 통신 프로토콜, 통신 및 컴퓨터 보안, 정보보호 서비스 및 메카니즘

김 대 호

1977년 한양대학교 전자공학과 공학사
1984년 한양대학교 산업대학원 전자공학과 석사
1993년 Univ. of Maryland at College Park
Dept. of Computer Science Visiting Scholar
1977년 ~ 현재 한국전자통신연구소 책임연구원, 부호기술연구 부장

※ 관심 분야: 전송분야, 통신 및 컴퓨터 보안