通信情報保護學會誌
第3卷 第3號, 1993. 9

근거리 전산 통신망(LAN)의 SECURITY에 관한 小考

차오길* · 김진원* · 김화수**

1. 序 論

컴퓨터 기술과 통신 기술의 결합으로서 현재 많은 각광을 받고 있는 통신망 중의 하나가 LAN이다.

이러한 LAN에 컴퓨터 시스템을 접속하는 대학교, 연구소, 기업들이 급속도로 증가하고 있는 추세인데, 이러한 이유는 컴퓨터 보급의 신속한 확대로 인하여 지리적으로 분산되어 있는 시스템을 효율적으로 이용하기 위한 것이다.

또한 LAN에서 제공되고 있는 서비스도 매우 다양해지고 있다. 그러나 LAN에서의 맹점은 정보의 내용 변경, 불법 유출, 순서 변경, 송·수신과 미확인 컴퓨터 바이러스 등의 위협을 내포하고 있다는 것이다.

이렇게 LAN이 SECURITY측면에서 취약점을 갖는 이유는 LAN은 개방형 구조를 갖기 때문이다.

최근에는 이러한 LAN의 불법적인 사용을 막기 위하여 여러 가지 SECURITY에 대한 새로운 제도와 절차가 마련 중이며 기술적인 SECURITY 시스템 구축의 필요성이 대두되고 있는 실정이다.

본 연구의 제2장에서는 LAN에 대한 일반적인 사항, 즉 LAN의 출현 배경, LAN의 분류, LAN 특성 및 응용 분야들을 고찰하였으며, 제3장에서는 LAN SECURITY의 문제점 및 대책으로써 LAN SECURITY 시스템에서 요구하는 필수 기능이 무엇인가를 고찰하고, 현재의 LAN SECURITY의 문제점을 기술적인 측면과 관리적인 측면으로 고찰하였다. 또한, 기술된 각종 문제점에 대한 LAN SECURITY 대책을 일반적인 사항과 LAN의 신뢰성(reliability) 향상 측면에서 제시하였으며, 제4장에서는 결론을 맺었다.

2. LAN의 概要

2.1. LAN의 출현 배경

LAN의 정의는 여러학자들에 의해 서로 다르게 정의되고 있으나, 일반적으로 "다수의 독립된 컴퓨터 시스템간에 상호 통신이 가능하도록 하는 통신 네트워크이다."라고 정의한다.

정보사회에서 통신 매체의 세 단계를 살펴보면, 제1단계는 각종 미디어 그 자체의 개발이고, 제2단계는 통신망 기술의 개발이며, 제3단계는 통신망에서 사용하는 소프트웨어의 개발이다.

LAN의 출현은 위의 세 단계중에서 제2단계에 해당된다.

초기에 컴퓨터가 개발된 이래 컴퓨터의 용도는 데이타 처리에 중점을 두어 왔으나 1980년대에 들어와서는 컴퓨터 연산능력의 제한, 컴퓨터 자원의 한정성 등의 난점을 해결하기 위하여 컴퓨터들간의

* 국방대학원 석사과정(전산학)
** 국방대학원 조교수(전산학)

상호 연결 필요성이 매우 고조되었다. 이와 더불어 컴퓨터 하드웨어 가격의 하락 및 컴퓨터와 통신 기술의 접목 시도, 그리고 비전문가로 하여금 컴퓨터를 이용하여 각종 정보를 처리하는 욕구가 증대됨에 따라 보다 효율적이고 조직적이며 신뢰성 있게 정보의 상호 교환을 목표로 등장한 것이 바로 LAN이다.

2.2. LAN의 분류

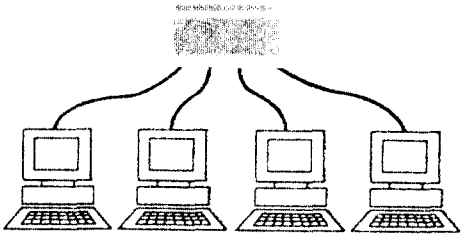
LAN이란 정보 통신의 발전에 따라 출현한 정보망의 한 형태로서 큰 건물과 제한된 지역내의 여러 건물들을 연결하여 정보를 고속으로 전송할 수 있게 하는 소단위의 고도 정보 통신망을 말한다. LAN은 아래와 같이 전송 매체, 전송 방식, 토폴로지, 엑세스 방식 등에 따라 다양하게 분류된다.

◦ 전송 매체에 의한 분류 : 전송 매체란 LAN에서 사용되는 물리적인 채널로써 대역폭에 따라 통신 용량이 제한되므로 이의 선택은 매우 중요한 의미를 갖는다. LAN에 이용되는 통신 매체로는 전화선(twisted pair), 동축케이블(coaxial cable), 광섬유(optical fiber)등이 있다.

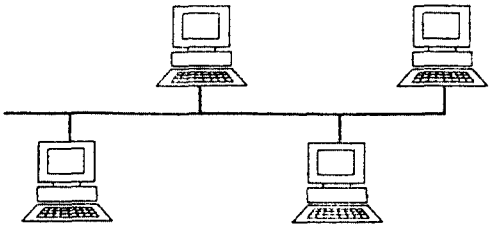
◦ 전송 방식에 의한 분류 : 실제로 채널에서 데이타가 전송되는 방법은 두 가지가 있는데, 즉, 직류 신호에 의한 베이스밴드(baseband) 방식과 직류 신호를 교류 신호로 변조한 후 전송하는 브로드밴드(broadband) 방식이 있다.

◦ 토폴로지에 의한 분류 : 토폴로지란 네트워크에 있어서 노드들의 물리적 또는 논리적 배치를 말하며, 네트워크의 특성을 결정하는데 많은 영향을 준다. LAN에서 사용되는 토폴로지의 형태는 일반적으로 그림 1과 같이 성(star)형, 버스(bus)형, 링(ring)형 등이 있다.

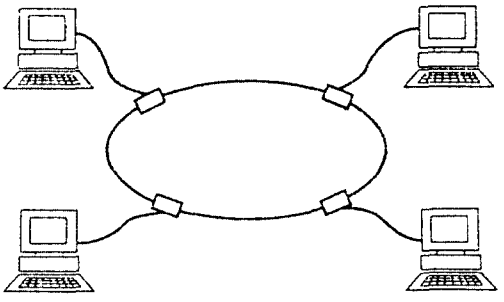
◦ 엑세스 방식에 의한 분류 : LAN의 특징 중의 하나는 채널을 공동으로 이용한다는 점으로 각 이용자가 공동 채널을 어떤 방법으로 분배하여 이용할 것인가가 LAN의 성능을 좌우하는 중요한 문제이다. 엑세스 방식에는 CSMA/CD(Carrier Sense Multiple Access/Collision Detection), 토큰 패싱(token passing), 슬롯 링(slotted ring)등이 있다.



성(star)형



버스(bus)형



링(ring)형

그림 1. 토폴로지의 종류

2.3. LAN의 특성 및 응용 분야

LAN의 특성을 살펴보면 (i) LAN은 통신망의 일종으로서 데이타의 비트(bit)들을 하나의 부착된 장비에서 또다른 장비로 옮기는 기능을 갖고 있다. (ii) LAN은 지역적(local area)인 곳에서 활용하는 통신망으로써 즉, 대부분의 경우에는 건물 내에서의 통신을 말하나 근거리 지역에 위치한 여러 건물들

간에 LAN을 통해서 각종 정보를 송·수신하는 특징이 있다. (iii) LAN은 다양한 종류의 정보(화상, TEXT, 그래픽 데이타 등)를 하나의 통신망상에서 송·수신할 수 있다.

LAN의 효과를 살펴보면 (i) 정보 자원을 공유할 수 있고, (ii) 정보의 실시간 처리 및 정보 자원의 일관성 있는 처리가 가능하며, (iii) 공통 회선을 설치하여 사용함으로써 케이블의 배선 비용 감소 및 정보처리 시스템 비용의 절감을 가져올 수 있고, (iv) 서로 다른 인터페이스의 접속을 가능케 함으로써 프로토콜 변환 기능의 제공과 이기종간의 통신을 가능하게 하며, (v) 임의의 터미널간에 N : N 통신이 가능함으로써 실질적인 분산처리 시스템이 실현될 수 있다.

LAN의 응용 분야를 살펴보면 (i) 최근 대부분의 회사내에서는 사무자동화의 필요성이 급격히 요망되고 있기 때문에 다양한 종류의 기기들과 그래픽 형태들을 지원하기 위해 전자우편, 전자게시판, 광파일, 원격회의, 화상정보처리 등의 업무를 지원하는 분야에 LAN을 응용하고 있으며, (ii) 공장에서는 효율적인 생산관리와 제품을 생산하고 판매하는 전체 공정과정을 자동화하기 위하여 모든 건물을 연결하는 수단으로써 LAN을 사용한다. 또한 (iii) LAN을 이용하여 데이타 처리에 사용하는 터미날이나 컴퓨터 기기들을 효율적으로 연결함으로써 상호간에 자원을 공유하고 공동의 정보를 검색하는데 응용되기도 한다.

3. LAN SECURITY 問題點 및 對策

3.1. LAN SECURITY 시스템의 필수 기능

LAN SECURITY에서 제공하여야 할 SECURITY 요구 기능을 살펴보면 다음과 같다.

첫째 : 무결성(integrity)을 보장하여야 한다. 여기에서 무결성이란 인가된 자(authorized member)만 화일 자료를 사용함으로써 기록된 화일의 재생, 삭제, 변경 등으로 부터 SECURITY를 보장하는 것이다. 즉, 비인가자에게는 화일에 대한 접근을 엄격히 제한하는 것이다. 특히, 인가자라 할지라도 화일을 재생하거나 삭제 또는 변경하는 등의 권한을 통제할 수 있는 기능이 제공되어야 한다. 이러한 통제방법은 암호화를 이용한 데이타 비밀 유지 서비스의 자동 효과로써 실현할 수 있다.

무결성에는 크게 두가지로 분류하는데 첫째는 내용 무결성이며, 둘째는 순서 무결성이다. 내용 무결성이란 전송되는 각각의 메시지에 대해 특정한 값을 첨부하여 전송하면 수신자는 이 메시지를 확인함으로써 무결성을 제고한다. 또한 순서 무결성이란 송신되는 메시지에 일련의 순서를 부여하여 전송할 시 외부의 공격이 탐지됨으로써 무결성을 제공할 수 있다.

둘째 : 인증성(authenticity)을 제공하여야 한다.

LAN을 사용할 시에는 여러 가지 방법으로 사용자들을 확인할 필요성이 대두된다. 인증성에는 반드시 사용자만이 인증 대상이 되는 것이 아니고 컴퓨터 시스템 및 각종 응용프로그램 등도 포함될 수 있다. 이러한 대상들이 실체를 가장해서 LAN에 침입하는 경우를 대비하여 정확하게 인증대상을 확인하는 기능이 제공되어야 한다.

특히 데이타 송신후 암호화된 데이타 영역에 송신측 주소의 복사본을 포함시켜 암호화하여 송신하면 수신측은 이를 복호화한 후 주소를 확인함으로써 실현할 수 있다.

셋째 : 가용성(availability)을 보장하여야 한다.

LAN에 연결된 시스템이나 시스템 내부에 있는 자료들은 인가된 사용자에게는 즉시 효과적으로 이용되도록 하여야 한다.

즉, 인가된 사용자에게 효과적으로 이용되도록 데이타의 백업(backup), 중복성(redundancy)유지, 물리적 위협으로부터 SECURITY를 유지시킴으로써 가용성을 보장할 수 있는 기능이 제공되어야 한다.

넷째 : 비밀성(confidentiality)을 보장할 수 있는 기능을 제공하여야 한다.

LAN에서의 SECURITY 시스템은 LAN 시스템에 대한 비인가자와 불법 침입자의 접근을 제어하고, 비밀 자료의 비밀성이 노출되지 않도록 인가된 자에게만 접근 가능하도록 해야 한다.

다섯째 : 이용성(usability)을 극대화할 수 있도록 하여야 한다.

즉 LAN에서 SECURITY(예를 들면 '비밀성')에 비중을 많이 두면 중요한 정보를 암호화해야 하는데, 그러한 경우 성능 및 가용성 등이 저하될 수 있으므로 SECURITY 뿐만 아니라 전체적인 시스템 성능과의 조화를 이룰 수 있는 기능을 제공하도록 노력해야 한다.

3.2. 제도적 측면에서의 LAN SECURITY 고찰

LAN SECURITY에 관한 연구는 이미 오래전부터 선진국에서 시작되었으나 아직 상용화 단계에 이르지 못하고 있는 실정이다.

선진국에서는 LAN SECURITY에 관련된 제품이 개발되었는데, 이러한 제품은 기존의 컴퓨터 SECURITY 시스템에 추가적인 기능이 부여된 것이다. 그러나, 이러한 기법으로는 LAN SECURITY를 근본적으로 해결할 수 없고, 필요한 기능을 자주 추가하는데 소요되는 경비의 증가로 인하여 현재는 시스템 내부에 SECURITY 기능을 탑재시키는 SECURITY kernel 시스템 기법이 활발히 연구되고 있는 실정이다.

IEEE에서는 LAN의 SECURITY 필요성을 인식하여 1988년에 LAN에 대한 SECURITY 프로토콜 표준화를 추진하여 IEEE 802.10을 구성하고 연구를 시작하였다. IEEE 802.10 표준안은 4개 분야로 연구가 진행 중이며 (i) SILS(Standard for Interoperable LAN Security) 모델, (ii) SDE(Secure Data Exchange) 프로토콜, (iii) 키 관리 프로토콜 및 (iv) 시스템 SECURITY 관리 프로토콜이 있다. IEEE 802.10 프로토콜의 구조 및 특성은 참고문헌 [8]을 참고하기 바란다.

미국에서 수행중인 SDNS(Secure Data Network System)라는 프로젝트는 분산 네트워크 SECURITY 기능을 구현하기 위한 프로젝트로써 정부와 기업체들이 공동으로 수행하며 OSI 네트워크 모델에 근거를 둔 네트워크 사용자의 데이타를 SECURITY 하기 위한 SECURITY 관련 서비스와 프로토콜 그리고 액세스 제어 기법 등이 포함된다. 그러나 여기에는 암호 알고리즘이 포함되어 있지 않다.

유럽 국가들도 통신망 환경에서의 보안에 대해 지대한 관심을 나타내고 있다. 대표적인 예로는 EUROPEAN COMPUTER MANUFACTURES ASSOCIATION의 컴퓨터 보안 모델을 들 수 있는데, 1986년부터 개방형 시스템에서의 보안과 관련된 프로토콜을 개발하고 표준화하기 위한 SECURITY의 골격 구축 작업을 시작하였다. 일본의 경우도 통신망 SECURITY에 관련하여 많은 투자를 하고 있으며, 특히 89년에 발표한 SECURE COMMUNICATIONS SERVICE ELEMENT 프로토콜이 대표적인 결과이다.

그러나, 국내 LAN SECURITY에 대한 구체적인 방안은 현재 제시되지 않고 있으며, 한국통신 정보보호학회가 『산학연의 SECURITY 암호와 표준화에 대한 연구』 활성화를 위해 주도적인 노력을 하고 있는 실정이다.

국내 정보 SECURITY 기술 관련 표준화는 현재 공업진흥청에서 DES 암호알고리즘 등 몇가지에 불과하며 아직 초보 단계에 이르고 있으며, 한국전산원에서는 LAN을 포함한 네트워크 SECURITY 기술 표준화를 위해 패스워드 활용 표준을 고시할 예정이고, 국내 실정에 적합한 네트워크 SECURITY 평가기준을 작성 중에 있다.

체신부에서는 『정보통신설비에 관한 안전 신뢰성 기준』을 고시로 제정 및 시행되었으며, 『전산망의 안전, 신뢰성 기술』은 고시된 상태에 놓여 있다.

그리고 전산망의 기능 유지와 SECURITY를 위한 기준을 정해 전산망 운용자와 이용자가 전산망의 안전 및 신뢰성 향상을 도모하고 정보 통신의 건전한 발전에 기여할 수 있는 지침을 제공하기 위해서 그 기준을 마련 중에 있다. 이렇게 국내에서도 과거보다는 통신망 환경에서의 보안 문제에 대한 인식이 높아지고 있는 추세이며, 또한 보안 문제에 대한 부단한 연구와 개발이 학계를 중심으로 산업계로 널리 확산되어 가고 있는 추세이다.

3.3. LAN SECURITY 시스템의 문제점

대부분의 LAN에서는 SECURITY의 필요성과 중요성은 인식하고 있으나, 실질적으로 기술적인 SECURITY 기능은 없는 상태로 운용되고 있다.

여기에서는 LAN의 기술적인 SECURITY를 달성하기 위해서 요구되는 SECURITY의 항목을 조사한 후 현재 운용중인 LAN의 기술적인 SECURITY상의 문제점을 고찰 해보도록 한다.

◦ 신분 확인 기능의 불안정 : LAN에서는 통신관련자들의 신분을 확인하고 해당 통신에 참여할 자격 유무를 검사해야 한다. 즉 통신 당사자간의 신분 확인(entity authentication)과 자격 유무의 점검 및 데이타 발신처의 신분 확인(data origin authentication)과 자격 유무를 점검하여 액세스를 요구할 때마다 액세스하는 주체가 요구하는 주체를 식별할 수 있어야 비인가자의 접근에 대처할 수 있는 인증이 확보된다. 그러나 현재 대부분의 LAN에서는 이러한 것을 충분히 제공하지 못하고 있는 실정이다.

이러한 문제점은 LAN의 속성상 모든 노드가 주소를 이용함으로써 다른 모든 노드에게 메시지를 송신할 수 있기 때문에 정당하지 못한 비인가자의 자원 이용이라는 중요한 문제점으로 대두된다.

◦ 액세스 제어 기능 : 정당한 사용자가 LAN에서 지원되는 자원을 사용하는가를 검사하는 기능이다. 즉, 비인가자가 어떠한 화일에 접근하여 고의로 메시지를 수정, 삭제, 추가 등의 행위를 할 수 없도록 상세한 액세스 제어기법을 제공해야 하나 실제적으로는 완벽한 액세스 제어기법이 제공되지 못하고 있는 실정이다. LAN의 속성상 메시지가 전송되는 모든 다른 노드에서는 메시지를 액세스 할 수 있으므로 메시지의 수정, 삭제, 추가 등의 권한이 없는 자에게 정보를 노출시킬 문제점이 야기된다.

◦ 자동 감사 기능의 미비 : 최근 컴퓨터와 통신이 결합된 기술인 통신망에 대한 의존도가 높아지면서 LAN 시스템을 불법적으로 액세스 하려는 의도 또는 일단 액세스하여 불법적으로 시스템 내부의 화일을 수정, 삭제, 추가 등의 행위를 하였을시 LAN SECURITY를 담당하는 운용자가 그러한 행위 전 혹은 행위 후에 나타나는 기록 정보를 자동으로 감사하는 기능이 매우 미흡한 실정이다.

◦ SECURITY 통신 장비 미비 : LAN망을 통하여 정보를 이용할 때 전송 중인 정보가 불법 침입자에 의해 도청, 변조되는 것을 방지하기 위하여 암호화에 의한 SECURITY 프로토콜의 표준화 및 SECURITY 통신 장비가 개발, 활용되어야 한다.

◦ 디지탈 서명 기능 미비 : 디지탈 서명 기능이란 문서 상에서 이루어지는 서명(signature)을 전자적으로(elctronically) 수행하는 것을 말한다.

LAN을 이용한 문서 송·수신시 문서 수신자는 수신된 메시지로부터 메시지의 무결성과 해당 메시지가 누구로부터 전송되었는지를 증명하고 싶어한다. 이러한 문제점을 디지탈 서명기법으로 해결할 수 있다. 디지탈 서명(digital signature)은 암호화 시스템을 이용한 보안 기법으로서 종이 문서에 사용하는 인감도장 같은 역할을 한다.

디지탈 서명 시스템에 포함하여야 할 사항을 살펴보면, (i) 서명문을 통해 수신자는 송신자 식별이 가능해야 하며, (ii) 수신자는 서명문을 통해 메시지의 무결성을 검증할 수 있어야 하고, (iii) 전송중인 메시지에 대한 비밀을 유지할 수 있으며, (iv) 송·수신자간에 분쟁 발생시 심판자가 분쟁을 해결할 수 있어야 한다. 이러한 디지탈 서명 시스템은 많은 이론적인 연구와 부분적인 구현은 이루어지고 있으나 현재까지 실용화가 안된 실정이다.

◦ SECURITY 응용 소프트웨어 개발 미비 : LAN상에서 사용되는 데이타 베이스 관리 시스템(DBMS), 메시지 핸들링 시스템(MHS), 전자게시판 시스템(BBS), 화상정보처리 시스템 등과 같은 각종 응용 소프트웨어는 SECURITY 기능이 당연히 제공되어야 하나, 현재 기존의 LAN에서 활용하고 있는 각종 응용 소프트웨어는 이러한 SECURITY 기능을 보유하고 있지 않기 때문에 여러가지 문제점이 발생된다. 예를 들면, 현재의 메시지 핸들링 시스템에서는 평문 메시지는 송·수신할 수 있으나 대외비 이상의 비밀 메시지는 송·수신이 곤란한 실정이다.

◦ 주소 공간 속성 및 지리적 분산으로 인한 문제점 : LAN에서는 주소 공간의 속성상 주소 관리를 이용한 명확한 제어가 어려우며 비인가자가 마치 인가자인 것처럼 자원을 이용할 수 있기 때문에 위험이 따른다. 또한 LAN은 지리적으로 분산되어 있기 때문에 메시지를 수정, 추가, 삭제 등의 권한을 갖지 않는 자에게 도청 등으로 인한 정보 노출 위험성이 상존한다.

◦ 통신 회선의 신뢰성 유지 미보장 : LAN상에서

의 주요한 SECURITY 유형 중에 하나인 통신 회선의 신뢰성 유지는 매우 중요한 부분이다. 왜냐하면 통신 회선의 신뢰성을 유지하기 위해서는 (i) 적정 전송 회선을 선택하고, (ii) 표준 통신 장비의 사용 및, (iii) 전송 오류에 대한 검출과 적정 절차 등 종합적인 회선관리등이 필요하기 때문이다. 만약에 이러한 조치가 이루어지지 않았을 경우, (i) 승인받지 않은 메시지가 송·수신될 위험성, (ii) 전송 과정에서 메시지의 유실, 변경 또는 중복, (iii) 바이러스가 침입할 위험성, (iv) LAN의 장애, (v) LAN상의 메시지 지연 등의 문제점이 야기될 수 있다.

관리적인 SECURITY의 문제점은 LAN에서만 적용되는 것이 아니고 일반적으로 모든 컴퓨터 시스템에 적용된다고 볼 수 있다. 본 연구에서는 기술적인 LAN SECURITY의 문제점을 중점적으로 살펴보고 해결 방향을 제시하고자 하는 것이다. 그러므로 간략히 관리적인 측면에서의 SECURITY 방법을 살펴보면 LAN과 관련된 주요 시설에 대한 화재 및 수해와 불법 침입 등에 의한 물적, 인적 재해를 사전에 예방하기 위하여 LAN이 설치된 주요 장소에 대해서는 안정성을 가장 중요하게 고려해야만 할 것이다.

3.4. LAN SECURITY 대책

현재의 LAN SECURITY 문제점들은 기술적인 측면과 관리적인 측면으로 분류하여 고찰하였으나, 본 연구에서는 먼저 기술적인 측면의 문제점에 대한 해결책을 제시한다.

첫째 : 데이타의 변경, 추가 등을 monitoring 할 수 있는 자동 감사 기능 시스템을 개발하고 적극 활용하여 데이타의 피해가 발생하는 경우 신속하게 조치할 수 있도록 해야 한다.

둘째 : 디지탈 서명 시스템을 개발하여 종이 문서에 사용하고 있는 인감도장 같은 역할을 담당하게 함으로써 기존 LAN SECURITY의 최대 문제점인 송·수신자가 메시지 송·수신시 발생되는 문제점들을 해결하기 위한 암호 시스템을 적극 개발하여 활용할 수 있어야 한다.

셋째 : 각종 LAN 응용 소프트웨어를 개발할 때 SECURITY 기능을 부가하여 제공할 수 있는 암호 시스템을 적극 개발하여 활용하여야 한다.

넷째 : 주요 정보의 안전과 신뢰성을 확보하기 위한 파일 액세스 제어 기법, 패스워드 관리 및 바이러스 대책 등에 대한 강력한 기법이 제공되어야 한다. 액세스할 때의 정당성을 제공하기 위한 액세스 제어 기법에서는 (i) 모든 주체에 대한 액세스 권한을 임무에 맞도록 최소화하고, (ii) SECURITY 메카니즘이 편리하게 사용할 수 있도록 하며, (iii) SECURITY 메카니즘의 간소화, (iv) 사용되는 메카니즘이 개방(open)되게 설계되어야 할 것이다. 또한 바이러스 대책으로는 LAN에 접속된 PC들의 안전을 위하여 file server내에 SITELOCK과 같은 프로그램을 상주시켜 LAN상에서 PC들간에 교환되는 바이러스를 체크하여 경고 조치 시킬 수 있다.

다섯째 : LAN 하드웨어의 신뢰성을 향상시키기 위해서 CUP 및 통신 제어 장치의 백업을 준비하며, 중요한 회선은 복수화, 우회 회선 설치 등 주요 화일에 대한 이중화를 고려할 수 있다.

여섯째 : LAN 소프트웨어의 신뢰성을 향상시키기 위해서는 LAN 소프트웨어를 개발하기에 앞서 신뢰도를 고려한 설계 기법 및 표준화를 통해 이룩할 수 있다. 즉, 네트워크의 구성이 완벽하다 할지라도 컴퓨터 네트워크의 여러 단계에서 SECURITY가 보장되기 위해서는 OSI 표준 모델에서의 SECURITY에 대한 연구가 있어야 한다. 또한 프로그램 작성 및 테스트 단계 등에서 소프트웨어의 신뢰성이 향상되어야 할 것이다.

일곱째 : LAN 운용시 신뢰성을 향상시키기 위해서는 자동화 및 간략화를 꾀하고, LAN의 부하 상태를 감시 및 제어하고 장애가 있는 곳을 검출 할 수 있는 SNMP(Simple Network Management Protocol) 기능을 강화시켜야 한다. 또한, 대외적으로 중요하거나 비밀성이 있는 자료에 대해서는 LAN 망에서 승인없이 공개되지 않도록 보호하고, 모든 메시지에 대한 지연, 유실, 중복이 없도록 하며, 바이러스가 LAN 망에서 통용되지 않도록 지속적인 조치와 통제를 하며, LAN의 신뢰성 향상을 위하여 이중 토폴로지를 구성하여 사용중인 망이 두절 되었을 시 다른 망이 이용될 수 있어야 한다.

여덟째 : 데이타 보호 및 부정사용 방지로 인한 LAN의 신뢰성 향상을 위해서는 액세스 권한 즉, 사용자 확인을 위한 패스워드 또는 자격 확인 기능 등을 강화해야 하고, 각종 자원에 대한 액세스 제어 기능을 강화함으로써 LAN 특성 중에 하나인 주소 관리를 이용한 명확한 제어 문제를 해결하여야 한다. 또한 데이타 누설을 방지하기 위하여 중요한 정보 및 화일은 암호화 기능을 설정하고, 암호화일은 반드시 타인이 액세스해도 내용을 알 수 없게 코드 형태로 두고 비인가자에게 사용자 번호 및 패스워드 등을 접근할 수 없도록 조치를 취하여야 한다.

아홉째 : LAN의 속성상 메시지 송·수신시 정당하지 못한 비인가자가 자원을 이용하고 메시지를 수정하는 것을 방지하기 위하여 데이타 발신처 인증, 무결성 데이타 비밀 유지등의 서비스를 제공해야 한다. 또한 LAN은 지리적으로 분산되어 있기 때문에 도청 등으로 부터의 정보 누출을 방지하기 위하여 무연결 데이타 무결성 및 데이타 비밀 유지 등의 서비스를 제공하여야 한다. 다음으로 관리적인 측면에서의 문제점을 해결하기 위해서는 SECURITY 책임자를 반드시 지정하여 운영하고, 전산 기록 매체에 대한 관리 및 입출력 관리 기록 그리고 패스워드 운용 대책 등 LAN에 관련된 각종 제도와 규정에 관한 세부 내용이 수립되어야 한다. 이러한 사항은 일부는 충족되고 있는 실정이나 현실성이 없는 부분이 아직도 많은 실정이다.

지금까지의 LAN SECURITY에 대한 기술적인 문제점 및 대책을 요약하면 표 1과 같다.

표 1. LAN SECURITY에 대한 기술적인 문제점 및 대책 요약

문 제 점	대 책
신분확인 기능의 불안정	사용자 확인을 위한 자격확인 기능(패스워드) 강화, 자원에 대한 엑세스 제어기능 및 주소관리기능 강화
엑세스 제어기능의 불안정	주요 정보의 안전과 신뢰성을 확보하기 위한 화일 엑세스 제어기법 등의 제공
자동 감사기능의 미비	자동감사기능 시스템을 개발하여 데이타 변경 및 추가시 신속하게 monitoring
SECURITY용 통신 장비 및 응용 S/W 개발 미비	LAN용 H/W의 신뢰성 향상을 위한 통신 제어장치의 이중화와 SECURITY 기능을 갖는 암호시스템 개발 활용
디지탈 서명기능의 미비	메시지 송·수신시 신분 확인이 가능하도록 디지탈 서명 시스템 개발 활용
통신회선의 신뢰성유지 미보장	중요한 통신회선은 이중화 및 복선화하여 LAN상에서 교환되는 정보의 신뢰성 향상

4. 結 論

본 연구에서는 근거리 전산 통신망(LAN)의 SECURITY에 대한 고찰을 기술하였다. 그 중에서도 LAN에 관한 일반적인 사항, LAN SECURITY 시스템에서 필수적으로 요구하는 기능, 제도적인 측면에서의 LAN SECURITY를 위주로 고찰하였다. 또한 기존 LAN SECURITY 시스템의 문제점을 기술적인 측면 및 관리적인 측면으로 분류하여 종합하였고 문제점에 대한 대책을 제시하였다.

기존 LAN SECURITY의 기술적인 측면에서의 문제점은 (i) 신분 확인 기능의 불안정 (ii) 액세스 제어 기능의 불안정 (iii) 자동 감사 기능의 미비 (iv) SECURITY 통신장비 미비 (v) 디지탈 서명 기능 미비 (vi) SECURITY 응용 소프트웨어 개발 미비 (vii) 통신 회선의 신뢰성 유지 미보장 등을 설명하였다.

이러한 LAN SECURITY의 문제점을 해결하기 위한 대책을 제 3 장의 '라' 항에 기술하였다. 앞으로 점점 복잡하고 다양해지는 현시점에서 LAN의 활용은 더욱 급증하는 추세를 보일 것이다. 이러한 LAN 상에서 SECURITY 기능의 제공없이 효용성이 많이 감소될 것이며, 따라서, 통신망에 관련된 SECURITY에 대한 관심과 연구가 더욱 활발히 이루어져야

할 것이다.

참 고 문 헌

1. 정보통신시대, 1993년 3월호.

2. 한국과학기술원 경영 과학회, 컴퓨터 범죄와 정보 시스템 보안, 1988.

3. 정보통신 진흥협회, 정보통신 안전체계연구, 1989.

4. 컴퓨터 매거진, 1993년 6월호.

5. 정보통신시대, 1993년 8월호.

6. 경영과 컴퓨터, 1993년 8월호.

7. 남길현, "암호시스템을 이용한 디지탈 서명 시스템", 통신정보보호학회지, 제 1 권, 제 1 호, 1991.

8. 유황빈, 이재광, "IEEE 802 구조에서의 정보보호 모델분석", 통신정보보호학회지 제 3 권, 제 1 호, 1993.

9. Bransted, K. Dennis, "Consideration for Security in the OSI Architecture", IEEE Network Magazine, 1987.

10. D.E. Denning, "Cryptography and Data Security", Addison Wesley, 1982.

11. Fred Piper, "Digital Signatures", Proceedings of the 7th International Conference and Exhibition on Informationn Security, 1991, 5.

□ 著者紹介

차 오 길

1987년 3월 : 해군사관학교 졸업(이학사)
1992년 2월~현재 : 국방대학원 석사과정(전산학)

김 진 원

1984년 2월 : 동국대학교 졸업(공학사)
1992년 2월~현재 : 국방대학원 석사과정(전산학)

김 화 수

1976년 3월 : 해군사관학교 졸업(이학사)
1984년 7월 : U.S. Naval Postgraduate School(美 해군대학원) 전산학 석사
1990년 8월 : Case Western Reserve University 전산학 박사
1991년 6월~현재 : 국방대학원 조교수(전산학)