특집기사

전산망 SECURITY

정 진 욱†

❖ 목 차 ❖

1. 서 론

현재 국내에서는 전산망의 확산과 컴퓨터 시스템의 보급 증대로 활발한 정보교환이 이루어지고 있다. 그러나, 전산망의 사용자 수가 확대됨에 따라 개인 정보의 불법 노출에 따른 프라이버시 침해 문제, 컴퓨터 바이러스 프로그램에 의한 전산망의 성능저하, 메시지 내용의 수정 및 변경에 따른 재산상의 피해 등 많은 문제들이 발생하고 있다. 따라서, 전산망에서의 정보보호 문제는 그 중요성이 더욱 제고되고 있다.

본 고에서는 이러한 전산망 보안에 관한 내용을 다음과 같이 살펴보았다. 2장은 ISO 7498-2에 기술된 OSI 통신 네트워크의 보안에 관한 구조를 기반으로 보안을 분석하였고, 3장은 인터네트 운영상의 보안대책을 보안도구를 통해 살펴보고, 4장은 OSI의 응용계층 서비스 중 전자우편 서비스를 지원하는 MHS(Message Handling System)를 보호하기 위해 제공되는 보안서비스와 MHS를 기반으로하는 EDI(Electronic Data Interchange)의 보안구조와 보안서비스를 분석하였다. 마지막으로, 5장에서는 인터네트의 대표적인 보안모델인 방화벽(Firewall)방식과 OSI보안구조에서 보안서비스의 중복성을 제거하자는 의미에서 제안된 SCSE (Secure Communication Service Element) 모델을 소개하였다.

2. OSI SECURITY

ISO는 컴퓨터 통신망의 기본구조를 OSI(Open Systems Interconnection)로 정의하고 표준안 ISO 7498에 그 기본모델을 보이고 있다. 기본모델에 덧붙여서 PART II 에서는 OSI에서의 보안구조를 정의함으로써, 개방형 시스템간의 통신을 위한 일반적인 보안관련 구조요소를 정의하고 있다. 즉, OSI 7498-2에서는, 안전한 통신을 가능하게 하고 보안에 일관된 원칙을 제공하기 위하여 용어의 정의, 보안서비스와 메카니즘 그리고 계층과의 관계, 보안서비스와 메카니즘의 계층에서 위치, 보안(보관)관리 등에 대하여 기술하고 있다. 따라서 본 절에서는 보안서비스와 메카니즘 그리고 이들 상호간의 관계를 살펴보기로 한다.

2.1 보안서비스

2.1.1 인증 서비스

이 서비스는 통신중인 동위실체(entity)상호간에 데이타의 근원지에 대한 인증을 제공한다.

(1) 동위 실체 인증

이 서비스는 통신실체간의 신원을 확인하기 위해 호의 설정 단계에서 제공한다. 이 서비스는 통신에 참여하는 실체가 인가되지 않은 이전 접속을 재사

†종신회원 : 성균관대 정보공학과 교수

용(replay)하거나 위장(masquerade)하지 않을 때에 신뢰성을 제공한다.

(2) 데이타 발신처 인증

이 서비스는 데이타의 근원지가 요청된 동위 실체라는 확증을 제공한다. 이 서비스는 데이타의 근원지에 대한 확증을 제공하지만 데이타 단위의 중복, 또는 변경에 대한 보호는 제공하지 않는다.

2.1.2 접근제어 서비스

이 서비스는 자원의 인가를 받지 않은 사용에 대한 보호를 제공한다. 이 서비스는 자원에 대한 모든 접근을 금지할 수도 있고 자원에 대한 특정한 조작(읽기, 쓰기, 지우기, 실행등)에 한해서 금지시킬 수도 있다. 접근제어는 다양한 보안 정책에 따르게 된다.

2.1.3 데이타 비밀보장 서비스

이 서비스는 인가받지 않은 제 3자의 의해 노출된 데이타의 보호를 제공한다. 이 서비스는 다음과 같이 몇 가지 경우로 나눌수 있다.

(1) 접속형(connection oriented)비밀보장

이 서비스는 네트워크내에서 이루어지는 접속형 통신의 모든 사용자 데이타의 비밀보장을 제공한다.

(2) 비접속형(connectionless)비밀보장

이 서비스는 네트워크내에서 이루어지는 비접속형 통신에서의 서비스 데이타 유니트(Service Data Unit)내의 모든 사용자 데이타의 비밀보장을 제공한다.

(3) 선택필드 비밀보장이 서비스는 접속형 또는 비접속형 통신에서

서비스 데이타 유니트내의 일부분의 데이타 비밀보장을 제공한다.

(4) 통신량 흐름 비밀보장

이 서비스는 통신량의 흐름의 관찰로부터 유래된 정보의 보호를 제공한다.

2.1.4 데이타의 무결성 서비스

이 서비스는 능동적 위협을 막는것으로 기술된 형태 중 하나를 취할 수 있다.

(1) 복구 접속형 무결성(connection integrity with recovery)

이 서비스는 네트워크내에서 이루어진 접속형 서비스의 모든 사용자 데이타의 무결성을 제공하며 데이타의 재사용이나 제거, 삽입, 변경을 검출한다. 무결성이 깨어졌을 경우 복구를 시도한다.

(2) 비복구 접속형 무결성(connection integrity without recovery)

이 서비스는 복구를 시도하지 않은 것을 제외하고는 복구 커넥션 무결성의 경우와 같다.

(3) 선택필드 접속형 무결성

이 서비스는 네트워크내에서 이루어지는 접속형 통신에서 사용자 데이타내에 선택된 필드의 무결성을 제공한다. 선택된 필드가 변경되거나 삽입, 삭제, 재사용되었는지를 검출한다.

(4) 비접속형 무결성

이 서비스는 네트워크내에서 이루어지는 비접속형 통신에서 사용자 데이타의 무결성을 제공하고 수신된 서비스 데이타 유니트가 변경되었는지를 검출한다. 또한 제한된 형태의 재사용 검출이 제공된다.

(5) 선택필드 비접속형 무결성

이 서비스는 네트워크내에서 이루어지는 비접속형 통신에서 서비스 데이타 유니트내의 선택된 필드의 무결성을 제공하고 선택된 필드가 변경되었는지를 검출한다.

2.1.5 부인불능(non-repudiation) 서비스

이 서비스는 다음 두 형태 중 하나 또는 둘 다 취할 수 있다.

(1) 발신 부인불능(non-repudiation with proof of origin)

데이타 수신자에게 데이타 발신처의 증명이 제공된다. 이 서비스는 발신자가 데이타나 그 내용을 보낸 사실을 거짓으로 부정하기 위한 시도를 봉쇄한다.

(2) 수신 부인불능(non-repudiation with proof of delivery)

데이타 발신자에게 데이타 배달 증명을 제공한다. 이것은 수신자가 데이타나 그 내용을 수신한 사실을 거짓으로 부정하기 위한 시도를 봉쇄한다.

2.2 보안 메카니즘

2.2.1 암호화

암호화는 데이타나 통신량 흐름 정보와 비밀보장을 제공할 수 있다. 암호화 알고리즘은 대칭(비밀키)방식과 비대칭(공개키)방식이 있다.

2.2.2 디지탈 서명

이 메카니즘은 다음의 두절차로 이루어진다.

- 데이타 단위에 서명하는 절차
- 서명된 데이타 단위의 검증 절차

서명과정은 서명자가 고유의 비밀정보를 사용하여 이루어진다. 두번째 과정은 공개적으로 이용가능한 절차와 정보를 사용한다. 그러나 이 절차로부터 서명자의 비밀정보를 추론할 수는 없다. 서명 메카니즘의 본질적인 특성은 서명이 서명자의 비밀정보를 사용하여야만 생성될 수 있다는 것이다. 그래서 서명이 검증되면 비밀정보의 유일한 소유자만이 서명을 만들 수 있다는 사실을 언제든지 제3자에게 입증할 수 있어야 한다.

2.2.3 접근제어 메카니즘

이 메카니즘은 실체의 접근 권리를 판단하고 보호하기 위해 실체의 자격이나 정보 또는 인증된 신원을 사용한다. 실체가 인가받지 않은 자원이나 부당한 형태로 인가된 자원을 사용하려고 한다면 접근제어 기능은 그 시도를 거절하고 경보발생과 보안감사일지에 그것을 기록하고 보고한다. 접근제어 메카니즘은 다음 내용 중 하나 또는 그 이상을 기반으로 한다.

(1) 동위 엔티티의 접근관리가 유지되는 접근제어정보 베이스

이 정보는 인가센터 또는 접근되는 엔티티에 의해 유지되며 접근제어 목록이나 계층적 및 분산구조의 매트릭스 형태일 수 있다. 이것은 동위 엔티티의 인증이 보장됨을 전제로 한다.

(2) 패스워드 같은 인증 정보

이것의 소유와 제시는 접근하는 실체의 인증 증거가 된다.

(3) 자격

이 정보의 소유 및 제시는 자격에 의해 정의된 자원이나 실체에 접근하는 권리의 증거이다. 자격을 위조할 수 없어야 하고 믿을만한 방법으로 전달되어야 한다.

(4) 보안 레이블

이것은 실체와 관련될 때 보통 보안정책에 따라 접근을 승인하거나 거절하기 위하여 사용된다.

(5) 시도된 접근시간

(6) 시도된 접근경로

(7) 접근구간

접근제어 메카니즘은 통신접속의 양쪽이나 중간 지점에 적용될 수 있다.

2.2.4 데이타 무결성 메카니즘

(1) 데이타 무결성의 두가지 형태

하나의 데이타 단위나 필드의 무결성과 데이타 단위 혹은 필드 스트림의 무결성으로 구분된다. 일반적으로 전자없이 후자의 규정이 비현실적일 지라도 이들 두 가지 무결성 서비스는 다른 메카니즘을 사용하여 제공된다.

(2) 무결성 판단 과정

하나의 데이타 단위에 대한 무결성 판단은 두 과정 즉, 송신 실체에서와 수신실체에서의 판단을 포함한다. 송신 실체는 데이타 자신으로 부터 함수를 적용하여 산출된 값을 데이타 단위에 추가한다. 이 값은 블럭검사부호나 암호 검사치와 같은 보조정보로서 그 자체가 암호화될 수도 있다.

수신자는 대응하는 값을 생성하여 데이타가 전송시 변경되었는지 판단하기 위해 수신한 값과 그 값을 비교한다. 이 메카니즘만으로는 한 데이타단위의 재사용을 보호하지는 못한다.

(3) 접속형 데이타 전송인 경우

데이타순서의 뒤바뀜, 손실, 재사용, 삽입, 변경을 막는 일련의 데이타 단위에 대한 무결성 보호는 순서번호, 시간, 날인, 암호연계(cryptographic

chaining)등을 필요로 한다.

2.2.5 인증 교환 메카니즘

(1)인증 교환에 적용되는 기술

① 패스워드와 같은 인증정보의 사용
송신실체에 의해 공급되고 수신실체에 의해 검사된다.

② 암호기술

③ 실체의 특성과 소유물의 이용

(2) 핸드셰이크(hand-shaking)프로토콜과의 결합

암호화 기술이 사용될 때 재사용을 막기 위해서는 핸드셰이크 프로토콜과 결합된다.

(3) 인증교환과 더불어 사용되는 기술

① 시간날인과 동기화된 클럭

② 2방향, 3방향 핸드 셰이크(일방향 또는 상호 인증)

③ 디지탈 서명과 공증 메카니즘에 의해 이루어지는 부인불능 서비스

2.2.6 통신량 삽입 메카니즘

이것은 통신량 분석에 대한 다양한 보급수단을 제공하기 위하여 사용되고 비밀보장 서비스에 의해 보급될 때 효과적이다.

2.2.7 경로선택 제어 메카니즘

경로는 실제 보안 서브네트워크, 중계, 링크만을 사용하기 위하여 사전배정에 의해 또는 동적으로 선택될 수 있다. 종단 시스템이 끊임없는 조작 공격을 검출한 경우, 다른 경로를 통한 접속을 설정하도록 네트워크 서비스 제공자에게 명령할 수 있다. 한편 보안 레이블을 수반하는 데이타는 서브네트워크, 중계, 링크를 통해 통과하도록 보안정책에 의해 강제될 수 있다. 또한 접속의 개시자나 비접속형 데이타 단위의 송신자는 특정 서브네트워크, 링크, 중계를 피하도록 경로 정보에 규정할 수 있다.

2.2.8 공증 메카니즘(notorization mechanism)

무결성, 발신처, 시간, 목적지와 같이 두 개 이상의 실체 사이에 전송된 데이타에 대한 공증 메카니즘의 규정에 의해 보증될 수 있다. 이 보증은 제 3자의 공증에 의해 제공되고 통신 실체에 의해 신뢰되며 검증할 수 있는 방법으로 요구된 보증을 제공하기 위하여 정보를 유지한다. 각 통신 인스탄스는 공증에 의해 제공되는 서비스에 적당한 디지탈 서명, 암호화, 무결성 메카니즘을 사용할 수 있다.

2.3 보안서비스와 메카니즘과의 관계

앞에서 기술된 보안서비스와 메카니즘의 관계는 <표 1>과 같이 정리할 수 있다.이 표에서 알 수 있듯이 정의된 14가지의 보안서비스는 중 11가지 서비스가 암호화 메카니즘을 근거로 하고 있으며 발신 부인불능 서비스도 디지탈서명 메카니즘과 데이타 무결성 메카니즘에 의존하고 있어 OSI의 보안서비스 접근 제어 서비스만을 제외하고는 모두 직접적으로 암호학의 응용범위에 속함을 알 수 있다.

<표 1> 보안서비스와 메카니즘과의 관계

메카니즘 / 서비스	암호화	디지탈 서명	접근 제어	데이타무결성	인증 교환	통신량 삽입	경로선택 제어	공증
동위엔티티인증	Y	Y	.	.	Y			.
데이타발신처인증	Y	Y	.	.	.	.		
접근제어서비스	.	.	Y	.	.	.		.
커넥션비밀보장	Y				.	.	Y	.
커넥션리스비밀보장	Y	.		.	.		Y	.
선택필드비밀보장	Y	.	.		.	.		.
통신량흐름비밀보장	Y	.		.	.	Y	Y	
복구커넥션무결성	Y	.		Y	.	.	.	.
비복구커넥션비밀보장	Y	.		Y	.	.	.	.
선택필드커넥션무결성	Y			Y	.	.		.
커넥션리스무결성	Y	Y	.	Y	.	.		.
선택필드커넥션리스 무결성	Y	Y	.	Y				.
발신부인불능		Y	.	Y				Y
수신부인불능	.	Y	.	Y	.			Y

(주) 이 메카니즘이 타당하지 않은 경우
Y 이 메카니즘이 다른 메카니즘과의 결합이 타당하다는 의미

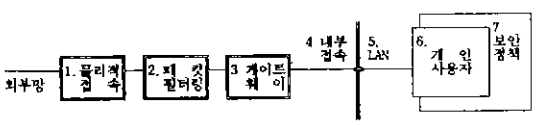
3. 인터네트의 SECURITY

인터네트(Internet)는 세계 최대의 네트워크로서, 미국방성에 의해 개발된 이기종간의 연결방법인 TCP/IP를 통신 프로토콜로서 사용한다. 여러 기종에서 손쉽게 이식하여 상호 연결이 용이하므로 꾸준하게 발전해온 인터네트는 개방형시스템 상호접속이 정착되기 전까지는 국제적인 현실표준으로서 지속적으로 발전되리라고 예측되고 있으며, 이의 표준화, 정책등은 IAB(Internet Activity Board)에서 조정하고 있다.

한편, 인터네트에서는 초기 R&D 환경에서 출발하였으므로 연구소나 대학등이 주된 가입기관이였고, 네트워크의 개방과 접속의 용이성으로 누구나 네트워크에 접속하기 쉬웠고, 네트워크 관련 정보나 프로그램 소스등이 개방되어 있기에 서독의 해커 간첩 사건,인터네트 Worm과 같은 크고 작은 보안 사고들을 겪어왔다. 따라서, 본 절에서는 인터네트의 보안 사고를 예방하고, 접근 제어 방식을 보안침해 모델과 보안도구를 중심으로 살펴보기로 한다.

3.1 보안 침해 모델

침입자는 시스템에 침입하여 불법적으로 관리자 권한을 취득한 후 시스템의 모든 정보를 없애버릴 수가 있으며 실제로 그러한 사건이 종종 발생되곤 한다. 이러한 시스템 침입을 예방하기 위해 많은 노력들이 이루어지고 있는데, 인터네트에 접속된 UNIX 시스템등의 호스트, 게이트웨이등에서의 보안위협요소들을 분석하여 적절한 예방(Prevention), 감시(Monitoring, Discovering a Break-in)등의 기능을 수행하는 연구개발이 많이 진행되고 있다.이러한 방법들의 접근을 다음 (그림1)과 같이 설명할 수 있으며, 이의 요약을 <표 2>에서 설명하고 있다.



(그림 1) 인터네트에서의 보안모델

<표 2> 보안모델 각 계층의 설명

7	보안문제의 정의와 적절한 보안정책 정의
6	보안정책에 의한 사용자 교육
5	내부 LAN에서의 보호
4	내부 LAN 세그먼트의 분리
3	외부로 부터 들어오는 트래픽을 게이트웨이에서 보안
2	외부로 부터 들어오는 트래픽을 라우터에서 필터링
1	모뎀이나 선에 물리적인 인터페이스에서의 보안

3.2 대표적인 보안 도구

이러한 보안침해에 관련하여 국내에서도 연구개발이 약간 진전되고 있으나 우선 해외 인터네트에서 널리 쓰이고 있는 보안 도구들을 중심으로 요약하여 <표 3>에 설명하고 있다.

<표 3> 인터네트 보안도구 요약표

분 야	제 품 명	설 명
인 증	npasswd	패스워드관리 정책을 강제화 가능, 길이 특정제한 등
	passwd+	추측하기 쉬운 패스워드의 삽입을 방지
	shadow	Shadow Passwd, 패스워드 파일의 패스워드를 일반사용자가 접근못 함
	passwd 2 1	기존의 기능에 aging expire 기능이 추가
	crack	패스워드 파일에서 사용자 패스워드를 알아내는 도구
	kerberos	LAN 환경에서의 주요 정보를 암호화 통신 인증하는 방법
시스템 점검 및 감시	aide	보안요소의 점검 및 체크
	COPS	시스템의 관한 모드의 체크, 보안구멍 체크 기능
	Tripwire	UNIX 화일시스템의 Integrity 를 체크하는 도구
	Swatch	syslog 도구등과 같이 시스템의 감시 도구
네트워크	tcp_wrapper	TCP/IP의 응용서비스에 대해 접근제어 인증, log, 릴정기능 제공
	SOCKS	TCP_Wrapper 와 유사한 기능을 하며, 접근제어 log등이 제공됨
	TCPDUMP	Ethernet 상의 트래픽 dump Traffic Tapping 가능
	nfswatch	NFS 트래픽 모니터링 도구

<표 3>은 인터네트에서의 보안관련 현황을 보안관련 프로토콜과 서비스 개발이라는 두 가지 관점에서 살펴본 것이다.

전세계적으로나 국내에서의 발전 및 확대추세에 미루어 보아, 아직 국내에서의 관련기술은 미흡하며 또한 국내에서도 학술연구전산망에서 보안침해 사고가 많이 발생하고 있으나 그에 대한 대책이 미비한 실정이므로, 이에 대한 관심과 연구개발 투자가 시급히 요청되고 있는 것이다.

4. MHS,EDI SECURITY

4.1 MHS의 개요

전자 메시지 통신 중에서도 개인간 메시지 통신은 컴퓨터네트워크에서 중요한 응용이며, OSI에서

는 MHS로 이런 응용을 지원하고 있다. MHS는 사용자들(사람과 컴퓨터 프로그램들)이 축적-전달(store-and-forward) 방식으로 메시지를 교환할 수 있게 한다. MHS의 구성요소 중, 메시지전송시스템(MTS)은 UA들과 MTS간에 프로브나 보고들 그리고 UA들간의 메시지를 전달해 주는 책임을 가진 응용 프로세스들의 집합이다. MTS는 하나 또는 그 이상의 메시지전송처리기(MTA)로 구성된 축적-전달용 통신네트워크 이다.

MHS 보안은 MTS(Message Transfer System)에서 발생될 수 있는 잠재적인 보안위협에 대처하기 위한 보안서비스로 설명한다. 그러므로, 본 절에서는 MHS 보안정책의 수립과정에서 고려되어야 하는 보안 위협요소들로부터 MHS 시스템을 보호하기 위해 제공되어야 할 보안서비스에 관하여 살펴 보았다.

4.2 MHS의 보안서비스

MHS 보안서비스들은 여러 개의 등급(Class)으로 나누어 지는데, 각 등급에 속한 보안 서비스들은 다음과 같다.

4.2.1 발신처 신분확인 보안서비스(Origin Authentication Security Service)

발신지 신분확인 보안서비스는 데이타의 발신처와 통신대등 실체의 신분 확인을 제공한다. MHS에서 일반적으로 신분확인 보안서비스들은 위장(Masquerade)의 위협으로부터 보호하기 위해서 제공되어질 수 있다. 이러한 위장의 위협을 방지하기 위해 제공되어지는 보안서비스들은 메세지 발신처 신분확인(Message Origin Authentication), 프로브 발신처 신분확인(Probe Origin Authentication), 리포트 발신처 신분확인(Report Origin Authentication), 안전한 접근 관리(Secure Access Management), 배달증명(Proof of Delivery), 제출증명(Proof of Submission) 서비스들이 있다.

가. 데이타 발신처 신분확인 보안서비스(Data Origin Authentication Security Service)

이 서비스는 모든 관계된 실체들(즉, MTAs or recipient MTS-user)에 대해서 메세지, 프로브, 리포트의 발신처에 대한 확증(corruption)을 제공한다. 하지만, 메세지, 프로브, 리포트의 중복(duplication)과 관련된 위협에 대해서는 보호할 수 없다.

- ▶ 메세지 발신처 신분확인 보안서비스(Message Origin Authentication Security Service)
- ▶ 프로브 발신처 신분확인 보안서비스(Probe Origin Authentication Security Service)
- ▶ 리포트 발신처 신분확인 보안서비스(Report Origin Authentication Security Service)

나. 제출증명 보안서비스(Proof of Submission Security Service)

이 서비스는 메세지가 수신자에게 배달되기 위해서 MTS가 확실하게 수신하였다는 사실을 메세지의 발신자에게 제공하고, 제출증명 서비스요소를 이용하여 제공되어질 수 있다.

다. 배달증명 보안서비스(Proof of Delivery Security Service)

이 서비스는 메세지가 의도한 수신자에게 배달되었다는 확신을 메세지의 발신자에게 제공하고, 배달 증명 서비스요소를 이용하여 제공되어질 수 있다.

4.2.2 안전한 접근 관리 보안서비스(Secure Access Management Security Service)

안전한 접근 관리 보안서비스는 자원(Resource)에 대한 불법적인 사용으로부터의 보호(Protection)와 관련되고, 대등실체 신분확인과 Security Context 보안서비스의 두개의 요소(Components)로 나누어 질 수 있다. 이 서비스는 위장, 정보의 누출, 그 밖의 위협으로부터 보호하기 위해서 제공되어진다.

가. 대등실체 신분확인 보안서비스(Peer Entity Authentication Security Service)

이 서비스는 연결확립시 연결하려는 실체의

identity를 확인하기 위해서 사용되어질 수 있고, 신분 확인교환 서비스요소에 의해서 제공되어진다.

나. 보안 문맥 보안서비스(Security Context Security Service)

이 서비스는 메세지와 관련된 Security Label을 참조함으로서 실체간의 메세지 전달의 범위를 제한하기 위하여 사용될 수 있고, 메세지와 Security Label의 관계를 제공하는 메세지 보안 레이블링 서비스요소와 매우 밀접하게 관계된다.

4.2.3 데이타 비밀성 보안서비스(Data Confidentiality Security Service)

이 서비스는 불법적인 누출로부터 데이타를 보호하기 위해서 제공 되어진다. 이러한 데이타 비밀성 보안서비스들은 MHS의 정보의 누출 위협(Leakage of Information Treats)으로부터 보호하기 위해서 제공 되어질 수 있으며, 이러한 정보의 누출 위협으로부터 보호하기 위해 제공 되어지는 보안서비스들은 연결 비밀성(Connection Confidentiality), 내용 비밀성(Content Confidentiality), 메세지 흐름 비밀성(Message Flow Confidentuality), 안전한 접근 관리(Secure Access Management)) 서비스들이 있다.

가. 연결 비밀성 보안서비스(Connection Confidentiality Security Service)

이 서비스는 사실상 MHS에서 제공되어지지 않지만, 하위 계층에서 이러한 보안서비스의 실행에 필요한 데이타가 대등실체 신분확인 보안서비스를 제공하기 위한 신분확인 교환 서비스요소 사용의 결과로서 제공되어질 수 있다.

나. 내용 비밀성 보안서비스(Content Confidentiality Security Service)

이 서비스는 메세지의 발신지와 수신자만이 메세지의 내용을 알 수 있다는 확신을 제공하고, 내용 비밀성 서비스요소와 메세지 인자 비밀성 서비스요소의 조합을 사용함으로써 제공되어질 수 있다.

다. 메세지 흐름 비밀성 보안서비스(Message Flow Confidentiality Security Service)

이 서비스는 메세지 흐름을 관찰함으로써 유추될 수 있는 정보의 보호를 제공한다. Double Enveloping Technique을 사용하여 완전한 메세지(봉투+메세지)를 다른 메세지의 내용이 되게함으로써, MTS의 임의의 부분(Part)으로부터 주소정보를 감추기 위해서 사용될 수 있고, Traffic padding과 함께 사용되어서 이 서비스를 제공할 수도 있다.

4.2.4 데이타 무결성 보안서비스(Data Integrity Security Service)

데이타 무결성 보안서비스는 MHS에 대해서 Active한 위협을 방지하기 위해서 제공 되어진다. 이러한 데이타 무결성 보안서비스들은 메세지 시퀀싱(Message Sequencing), 정보의 수정(Modification of Information)위협으로 부터 보호하기 위해 제공되어질 수 있으며, 이 서비스에는 연결 무결성(Connection Integrity), 내용 무결성(Content Integrity), 메세지 순서 무결성(Message Sequence Integrity) 서비스들이 있다.

가. 연결 무결성 안정성 서비스(Connection Integrity Security Service)

이 서비스는 사실상 MHS에서 제공되어지지 않지만, 하위 계층에서 이러한 보안서비스의 실행에 필요한 데이타가 대등실체 신분확인 보안서비스를 제공하기 위한 신분확인 교환 서비스요소 사용의 결과로서 제공되어질 수 있다.

나. 내용 무결성 보안서비스(Content Integrity Security Service)

이 서비스는 하나의 메세지에 대해서 메세지 내용의 무결성을 제공하고, 메세지 내용이 수정되었는지를 결정할 수 있는 형식(Form)을 갖고 있다. 이 서비스 역시 메세지 순서 무결성 보안서비스에 의해서 제공되어지는 메세지 재전송(Replay)에 대한 검출을 할 수 없다. 메세지 인자 무결성 서비스 요소 -어떤 경우에는 메세지 인자 비밀성 서비스요소- 와 내

용 무결성 서비스요소가 함께 메세지의 수신자에게 이 서비스를 제공하기위해 사용될 수 있다.

다. 메세지 순서 무결성 보안서비스(Message Sequence Integrity Service)

이 보안서비스는 메세지의 발신자와 수신자에게 순서화된 메세지를 제공하여 메시지 순서의 재배열에 대한 위협으로부터 보호된다. 이렇게 함으로써 메세지의 재전송(Replay)에 대한 위협으로부터 보호한다. 이 서비스는 메세지 순서 무결성 서비스요소와 메세지 인자 무결성 서비스요소의 조합을 이용하여 제공되어질 수 있다.

4.2.5 부인봉쇄 보안서비스(Non-repudiation Security Service)

부인봉쇄 보안서비스는 메세지가 제출, 전송, 배달된 후, 제삼자에게 그 메세지의 제출, 전송, 수신 사실에 대한 부인할 수 없는 증명을 제공한다. 이러한 부인봉쇄 보안서비스는 부인(Repudiation)의 위협으로부터 보호하기 위해서 제공되어지며, 제공되는 서비스는 발신처 부인봉쇄(Non-repudiation of Origin), 재출 부인봉쇄(Non-repudiation of Submission), 배달 부인봉쇄(Non-repudiation of Delivery) 서비스들이 있다.

가. 발신처 부인 봉쇄 보안서비스(Non-repudiation of Origin Security Service)

이 보안서비스는 메세지의 수신자(들)에게 메세지의 발신처, 그 내용, 관련된 보안 레이블(Label)에 대한 부인할 수 없는 증명을 제공한다. 이 서비스 역시 내용 무결성 보안서비스와 거의 유사하게 서비스요소(내용 무결성 서비스요소 + 메세지 인자 무결성 서비스요소 또는 메세지 인자 비밀성 서비스요소)의 두 개의 다른 조직을 이용하여 제공되어질 수 있다.

나. 제출부인봉쇄 보안서비스(Non-repudiation of Submission Security Service)

이 보안서비스는 메세지의 발신자에게 메세지가 원래 의도한 수신자에게 배달되기 위하여 MTS로 제출되었다는 부인할 수 없는 증명을 제공한다. 이 서비스는 제출증명 보안서비스를 제공하기 위해서 사용되어지는 제출증명 서비스요소를 이용하여 거의 유사한 방법으로 제공되어질 수 있다.

다. 배달 부인 봉쇄 보안서비스(Non-repudiation of Delivery Security Service)

이 보안서비스는 메세지의 발신자에게 메세지가 원래 의도한 수신자에게 배달되었다는 부인할 수 없는 증명을 제공하고, 배달 증명 보안서비스를 제공하기 위해서 사용되어지는 배달 증명 서비스요소를 이용하여 거의 유사한 방법으로 제공되어질 수 있다.

4.2.6 메세지 보안 레이블링 보안서비스(Message Security Labelling Security Service)

이 서비스는 보안 레이블이 MHS(MTAs과 MTS-user)의 모든 실체와 연계 되도록 해주고, 메세지 보안 레이블 서비스요소에 의해서 제공되어진다. 레이블의 무결성과 비밀성은 메세지 인자 무결성 서비스요소와 메세지 인자 비밀성 서비스요소에 의해서 제공되어진다.

4.2.7 보안 관리 서비스(Security Management Service)

MHS는 많은 보안 관리 서비스를 필요로 하지만, 여기서는 크리덴셜의 변경과 MTS-user 보안 레이블링의 등록에만 관계된다. 이러한 보안 관리 서비스는 위장(Masquerade), 정보의 누출(Leakage of Information) 그리고 그 밖의 위협들로 부터 보호하기 위해서 제공되어질 수 있고, 이러한 보안 관리 서비스에는 크리덴셜 변경 보안서비스, 등록 보안서비스, MS 등록 보안서비스들이 있다.

가. 크리덴셜 변경 보안서비스(Change Credentials Security Service)

이 보안서비스는 MHS에서 하나의 실체가 다른 실체가 갖고있는 것과 관계된 크리덴셜을 변경할 수 있도록 해주고, 크리덴셜 변경 서비스요소에 의해서 제공 되어진다.

나. 등록 보안서비스(Register Security Service)
이 보안서비스는 하나의 MTS-user에게 허용되어진 보안 레이블을 MTA에 등록할 수 있게 해주고, 등록 서비스요소에 의해서 제공되어진다.

다. MS 등록 보안서비스(MS-register Security Service)
이 보안서비스는 하나의 MS-user에게 허용되어진 보안 레이블을 확립할 수 있게 해준다.

4.3 MHS 보안서비스들의 사용

이상과 같이 설명한 MHS에 대한 위협요소들과 이러한 위협들로 부터 안전한 통신을 위한 서비스들을 <표 4>에 나타내었다.

<표 4> MHS 보안서비스의 사용

위협요소들		서비스
Masquerade	Impersonation and misuse of the MTS Falsely acknowledge receipt Falsely claim to originate a message Impersonation of an MTA to an MTS-user Implementation of an MTA to another MTA	Message origin authentication Probe origin authentication Secure access management Proof of delivery Message origin authentication Proof of submission Report origin authentication Secure access management Report origin authentication Secure access management
Message sequencing	Replay of message Re-ordering of messages Pre-play of message Delay of message	Message sequence integrity Message sequence integrity
Modification of information	Modification of message Destruction of message Corruption of routing and other management information	Connection integrity Content integrity Message sequence integrity
Message Loss		

4.4 EDI 의 개요

EDI란 컴퓨터 보급의 증가와 네트워크 확산에 의해 상호거래에 필요한 모든 데이타를 기업내 단말에서 통신회선을 통해 전자적으로 문서를 상호교환하도록 하는 시스템이다. 즉, EDI는 기업간 거래에 필요한 정형화된 자료를 규격화된 양식으로 네트워크를 통해 컴퓨터 또는 응용프로그램간에 데이타를 교환하는 것을 의미한다.

특히 무역, 유통, 운송 등 각 분야에서 EDI를 이용함에 있어서 반드시 해결해야 될 과제가 보안문제이다. 즉, 어떤 물량이 주문되었을 때, 그 주문에 대한 진위 여부의 확인이나 전달과정에서의 변조 및 누락이 없었는지, 또는 주문자가 나중에 주문사실을 부인하지 못하게 하는 조치라든가 중요한 거래 내용의 제 3자로의 누설 방지 등의 보안이 해결되지 않으면 EDI의 광범위한 이용은 불가능하게 될 것이다. 왜냐하면, EDI상에서 거래되는 모든 문서는 실제 각 기업의 이익과 바로 직결되는 중요한 서류들이기 때문이다. 따라서, 본 절에서는 EDI의 보안서비스와 그 서비스에 대한 메카니즘을 분석하였다.

4.5 EDI 보안서비스(Security Service)

4.5.1 발신처 인증(Origin Authentiction) 보안서비스

발신처 인증보안서비스는 데이타의 발신처와 통신대등실체의 인증을 제공한다. 일반적으로 EDI에서의 인증 보안서비스들은 위장(Masquerade)의 위협으로부터 보호하기 위해서 제공되어 질 수 있다. 이러한 위장의 위협을 방지하기 위해 제공되어지는 보안서비스들은 메시지 발신처 인증(Message Origin Authentication), 프로브 발신처 인증(Probe Origin Authentication), 리포트 발신처 인증(Report Origin Authentication), 안전한 접근 관리(Secure Access Management), 배달증명(Proof of Delivery), 제출증명(Proof of Submission) 서비스들이 있다.

4.5.2 안전한 접근 관리(Secure Access Management) 보안서비스

안전한 접근 관리 보안서비스는 자원에 대한 불법적인 사용으로 부터의 보호(Protection)와 관련되고, 대등실체 인증과 보안문맥(Security Context) 보안서비스의 두 개의 요소(Components)로 나누어 질 수 있다. 이 서비스는 위장, 정보의 누설, 그 밖의 위협으로 부터 보호하기 위해서 제공되어진다.

4.5.3 데이타 비밀성(Data Confidentiality) 보안서비스

이 서비스는 불법적인 누설로 부터 데이타를 보호하기 위해서 제공 되어진다. 이러한 데이타 비밀성 보안서비스들은 MHS의 정보누설 위협(Leakage of Information Treats)으로 부터 보호하기 위해서 제공되어질 수 있으며, 이러한 정보의 누설 위협으로 부터 보호하기 위해 제공되어지는 보안서비스들은 접속 비밀성(Connection Confidentiality), 내용 비밀성(Content Confidentiality), 메시지 흐름 비밀성(Message Flow Confidentiality), 안전한 접근 관리(Secure Access Management) 서비스들이 있다.

4.5.4 데이타 무결성(Data Integrity) 보안서비스

데이타 무결성 보안서비스는 MHS에 대해서 능동적인 위협을 방지하기 위해서 제공되어진다. 이러한 데이타 무결성 보안서비스들은 메시지 시퀀싱(Message Sequencing), 정보의 변경(Modification of Information)위협으로 부터 보호하기 위해 제공되어질 수 있으며, 이 서비스에는 접속 무결성(Connection Integrity), 내용 무결성(Content Integrity), 메시지 순서 무결성(Message Sequence Integrity) 서비스들이 있다.

4.5.5 부인불능 (Non-repudiation) 보안서비스

부인불능 보안서비스는 메시지가 제출, 전송, 배달된 후, 제삼자에게 그 메시지의 제출, 전송, 수신한 사실에 대한 부인할 수 없는 증명을 제공한다. 이러한 부인불능 보안서비스는 부인(Repudiation)의 위협으로 부터 보호하기 위해서 제공되어지며, 제공되는 서비스는 발신처 부인불능(Non-repudiation of Origin), 제출 부인불능(Non-repudiation of Submission), 배달 부인불능(Non-repudiation of Delivery) 서비스들이 있다.

4.5.6 메시지 보안 레이블링(Message Security Labelling) 보안서비스

이 서비스는 보안 레이블이 MHS(MTA들과 MTS사용자)의 모든 실체와 연계되도록 해주고, 메시지 보안 레이블 보안요소에 의해서 제공되어진다. 레이블의 무결성과 비밀성은 메시지 인자 무결성 보안요소와 메시지 인자 비밀성 보안요소에 의해서 제공되어진다.

4.5.7 보안 관리 서비스(Security Management Service)

EDI는 많은 보안 관리 서비스를 필요로 하지만, 여기서는 크리덴셜의 변경과 MTS사용자 보안 레이블링의 등록에만 관계된다. 이러한 보안 관리 서비스는 위장(Masquerade), 정보의 누설(Leakage of Information), 그리고 그 밖의 위협들로 부터 보호하기 위해서 제공되어질 수 있고, 이러한 보안관리 서비스에는 크리덴셜 변경 보안서비스, 등록 보안서비스, MS 등록 보안서비스들이 있다.

4.5.8 EDIM 책임 인증/부인불능(EDIM responsibility authentication/Non-Repudiation)

EDIMG 환경내에서 부인(Repudiation)에 대응하는 보호장치를 제공하는 서비스로, EDIM 책임 회송을 형식화(Formalizing)하는 것과 관계된다. 이러한 보안관련 서비스는 다음과 같다.

(1) EDI통지 증명/부인불능(Proof/Non-repudiation of EDI Notification)

(2) 검색 증명/부인불능(Proof/Non-repudiation of retrieval)

(3) 전송 증명/부인불능(Proof/Non-repudiation of transfer)

4.6 구현메카니즘

4.6.1 비밀보장 메카니즘

이 기능은 메시지의 불법 노출로 부터 데이타를 보호하기 위한 것으로 사용되는 암호 알고리즘은 처리 속도를 고려하여 본 고에서는 대칭키 암호시스템으로 가장 널리 알려진 DES(Data Encryption Standard) 알고리즘을 채택하였고, 자체 난수(random number)를 발생하여 이 난수

를 사용자키(UK)로 이용하도록 하였으며 메시지 전체를 암호화하게 된다.

DES와 같은 대칭키 시스템은 비밀키(사용자키)를 반드시 상대방도 가져야하므로 여기서는 키 관리를 간편하게 하기 위해 송신측에서 사용한 키를 수신측의 공개키를 사용하여 암호화시켜 전송하게 함으로서 수신측에서는 메시지를 암호화한 키를 알거나 보관할 필요가 없게 하였다. 즉, 사용자 키는 수신측 공개키에 의해 암호화되어 전송되며 수신측은 수신측의 비밀키를 이용하여 사용자키를 복호화한 후 이 키를 이용하여 메시지를 복호화하게 한다.

4.6.2 인증 및 무결성 서비스

발신처 인증 서비스는 메시지의 발신자로 부터 보내진다는 것을 보장할 수 있게 한다. 즉, 발신자는 자기만이 알고 있는 비밀키를 사용하여 암호화하는데 이 때 다른 어떤 사람도 발신자의 비밀키를 알 수 없다. 그리고 수신측에서는 공개키로서 복호화시킴으로 발신처를 증명할 수 있게 된다.

그리고 메시지 무결성 서비스는 발신자가 제출한 메시지가 수신자가 수신하기 전 불법 수정이나 변경이 없었다는 것을 보장하기 위한 것이다.
이 두 서비스는 X.509의 디지탈서명 메카니즘으로 해결할 수 있는데 이 때 암호화해야할 메시지의 길이(N)가 클 때 처리 시간이 많이 소요되므로 메시지 길이가 짧은 블럭단위의 길이로 hashing 함수를 수행하여야 하는데 X.509에서는 square-modular 방식을 제시하고 있으나 본 고에서는 32비트 머신상에서의 효율성과 안전성이 고려된 Rivest의 MD5 Message Digest 메카니즘을 사용하였고, 여기에 사용된 암호 알고리즘은 RSA알고리즘을 이용하였다.

먼저 송신측(A)에서 hashing 함수의 수행에 의해 얻어진 HV를 송신측의 비밀키 As로 서명된 정보(X=As(HV))를 메시지 헤더(header)에 부가하여 수신측에 보내면, 수신측(B)은 서명된 X를 송신측의 공개키 Ap로 복호화시켜 HV를 얻게 된다. 그 다음, 송신측으로 부터 수신된 메시지를 동일한 hashing 함수를 이용하여 HV'를 구하여 송신측으로 부터 수신된 HV의 값을 비교한다. 만약 이 값이 같다면 정당한 발신자에게서 온 것을 보장함과 동시에 변경없이 보내졌다는 것을 보장할 수 있게 된다.

4.6.3 수신내용 부인불능 메카니즘

일상적인 상거래시 성공적인 송신시에도 통신당사자의 부인에 따른 잠재적인 위협요소가 있다. 그 중 하나로서 청구서 및 대금지불 등과 같은 메시지를 받은 수신자가 수신 자체를 부인하고 미수신 claim을 제기하는 행위이다. 이런 위협을 메시지 발신자가 봉쇄하기 위한 것이 바로 수신내용 부인불능(Non-repudiation of receipt) 메카니즘이다. 이 메카니즘을 앞에서 설명한 디지탈서명 메카니즘과 메시지의 사본을 발신자에게 되돌려 보내는 행위를 함께 사용함으로써 해결할 수 있다.

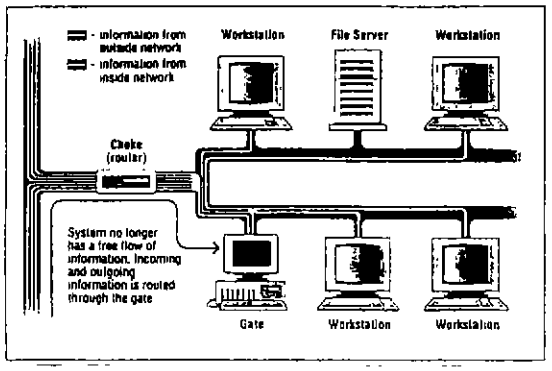
이 수신내용 부인불능은 디지탈서명을 하기 전 송신측의 EDIM(EDI Message) 내 Notification Request 필드에 PN 또는 NN을 요청하고 Notification Security 필드를 proof로 set시키는 제어과정을 먼저 거친 다음, 디지탈서명 과정을 거친다. 즉, 메시지 내용이 해싱 함수를 거친 후 그 값을 서명하여 자체 로그 화일(Audit)에 수록한 다음 수신측으로 전송한다.

수신측에서는 수신된 EDIM이 PN 또는 NN으로 set되어 있으면 EDIN을 생성하기 위해 메시지 내용을 해싱한 결과 값(CIC)을 수신측의 비밀키로 암호화하여 EDIN에 Bs(CIC)를 붙여 발신처로 보낸다. 발신측에서는 수신된 Bs(CIC)를 B측의 공개키로서 복호화시켜 이 메시지 내의 CIC와 이미 로그(Audit) 화일에 수록된 HV의 값을 비교하여 성공적으로 수행되었을 경우 수신측이 내용을 받았다는 것을 확인한 후 로그화일에 이 EDIN을 저장시켜 두고 나중에 문제가 발생시 수신자의 수신 사실에 대한 부인을 봉쇄하는 근거자료로 제시한다.

5. 모 델

5.1 인터네트 보안 모델

인터네트의 현실적인 보안대책인 방화벽시스템(Firewall System)은 인터네트에 접속한 가입기관의 내부도메인 네트워크를 보호하기위한 방법으로, 이는 외부네트워크와 접속하는 게이트웨이 시스템을 단지 하나만 두고 그 시스템에서 인증을 받아야만 내,외부로의 접근을 허용하는 시스템으로서, (그림 2)에서 보이는 모델이 기본적인 예이다.



(그림 2) Firewall 시스템 모델

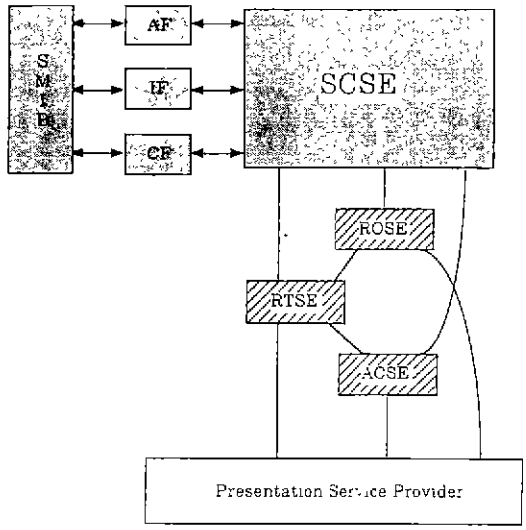
이러한 Firewall 시스템은 최근 활발하게 연구개발되고 있는 현실적인 보안대책의 하나로서 여러가지 제품들이 발표되고 있다.

5.2 개방형 환경안에서의 보안구조 모델

일본의 KOUJI NAKAO와 KENJI SUZUKI가 OSI응용계층에서 보안서비스를 제공하는 공통 응용서비스 요소인 SC서비스요소를 제안하고 보안서비스와 프로토콜을 정의하였다. 제안한 SCSE 보안모델은 (그림 3)과 같다. 이 모델은 어떠한 보안요구에 따라 AF, IF, CF 중 해당하는 Facility를 선택 호출하여 상호작용함으로써 보안서비스를 제공하게 된다. 또한 각 Facility들은 SMIB 내에 저장되어 있는 정보들을 사용하여 보안서비스들을 제공한다.

5.2.1 모델 분석

새로운 형태의 보안서비스요소인 SCSE를 OSI 7계층 중 응용계층에 둔 이유는 응용계층에서 모든 보안서비스들을 제공해 줄 수 있으며 몇몇 특정 서



(그림 3) SCSE 내부구조

비스는 그 성격상 응용계층에서만 제공가능하므로 현재 보안 표준화 동향을 분석해 볼 때 응용계층에 보안기능을 위치시키고 있다.

보안에 필요한 인증, 접근 제어, 무결성 등의 여러 보안 문제와 관련된 특정한 기능적 영역들은 포괄적이고 일관된 기술이 필요하다. 보안구조는 이러한 필요성을 만족시키기 위하여 연구되는 분야이다. 따라서 보안구조는 특정한 개방형 시스템 구조의 문맥에 각 영역의 기능들이 어떻게 적용될 수 있는가를 다루며 개방형 시스템의 보안에 대하여 통일된 관점 제공을 목적으로 개발되고 있다.

보안구조는 시스템과 시스템의 객체들을 보호하는 방법의 정의와 시스템간의 상호작용에 관련된다. 즉, 특정한 보안서비스를 제공하기 위한 서비스요소와 동작의 순서를 다룬다. 보안서비스는 시스템간에 교환되는 데이타, 시스템에 의해 관리되는 데이타, 그리고 시스템내의 통신되는 실체에 적용될 수 있다.

FTAM, VT, MOTIS 등과 같은 SASE(Specific ASE)들에서 요구하는 보안서비스들이 현재 OSI 보안 구조에서 제안된 두 세개의 일반적인 보안서비스로 제한되어 있으며, 이들이 각각의 SASE마다 구현되어 있음으로 인해서 보안서비스의 중복이 발생한다. 그래서 이런 중복성을 제거하

자는 의미에서 제안된 것이 SCSE 모델이었다. SCSE 모델은 응용계층에서 공통적으로 요구되는 보안서비스를 하나의 SCSE로 만들어 놓은 것이다. SCSE 모델은 공통적으로 요구되는 보안서비스를 제공하기 위한 세 개의 Facility, 즉, 인증서비스를 제공하는 AF(Authentication Facility), 데이타 무결성 서비스를 제공하는 IF(Integrity Facility), 그리고 데이타 비밀성 서비스를 제공하는 CF(Confidentiality Facility), 그리고 SMIB (Secure Management Information Base)로 구성된다. 각 구성요소에 대해 살펴보면 다음과 같다.

① AF(Authentication Facility)

접속지향 통신에서 통신관련자에 대한 인증을 하고 해당 통신에 참여할 자격을 검사하는 Facility이다. 동위실체의 신뢰성있는 접속의 확립이나 데이타전송의 과정에서 수행되는 동위실체 인증서비스를 제공해주는 부분으로서 식별검사나 암호화기능을 수행한다.

② IF(Integrity Facility)

전송되는 데이타의 무결성을 점검하는 무결성 서비스를 제공하는 Facility로서 메시지인증코드를 이용하여 무결성을 검사하고 데이타의 순서를 검사한다. 무결성은 내용의 무결성을 점검하는 내용 무결성(Content Integrity)과 전송되는 전문의 순서를 점검하는 순서무결성(Sequence Integrity)으로 나누어진다.

③ CF(Confidentiality Facility)

통신되는 데이타가 불법적으로 내용이 노출되는 것을 방지하는 데이타 비밀성 서비스를 제공하는 Facility로서 암호화 메카니즘을 사용하여 전송되는 데이타의 내용을 감출 수 있다.

④ SMIB(Secure Management Information Base)

각 Facility들이 각각의 해당되는 서비스를 제공하기 위해 사용하는 암호화알고리즘, 암호화동작모드, 암호화키, 초기벡터 등의 정보를 유지하기 위하여 로컬시스템에 SMIB(Secure Management Information Base)를 두어 사용하도록 구성하였다. SMIB에 저장된 정보들은 문맥(Context)단위로 처리되는데 이를 PRC(Protection Context)라 하며 각각의 PRC ID에 의하여 구분되고 관리된다. 이러한 정보들은 각 호스트에 있는 로컬 SMIB에 동일하게 저장되어야 하므로 OSI 보안관리 프로토콜 등에 의하여 관리되어야 한다.

6. 결 론

지금까지 개방형 환경에서의 보안에 대해 ISO 7498/2에서 정의된 전반적인 보안서비스와 메카니즘을 통해 살펴보았고, TCP/IP를 통신 프로토콜로 사용하는 인터네트(Internet)의 보안을 보안 침해모델과 방화벽(Firewall)이라는 보안도구를 통해 살펴보았다. 또한, OSI의 응용서비스 중 MHS의 보안과 MHS를 기반으로 하는 EDI의 보안도 살펴보았다.

또한, 최근, 음성,화상,비디오,텍스트 등 종합적으로 처리되고 전송되야 하는 멀티미디어에 대한 고속통신의 필요성이 대두되었다. 즉, 화상정보, HDTV, CAD/CAM, LAN간 통신, 대량의 화일전송을 만족시키는 서비스를 제공하는 광대역 ISDN(B-ISDN)과 광대역,저지연 스위칭과 멀티플렉싱 패킷 기술을 제공하는 ATM, 그리고 실제 물리적인 전송을 담당하는 기술인 SONET이다. 이러한 것들은 OSI 계층 개념과 완전히 일치하지는 않겠지만, ATM은 계층3와 계층2의 기능을 수행하고 SONET은 계층1의 기능을 수행한다고 볼 수 있다. B-ISDN에서 제공되는 서비스는 메시지 서비스, 대화형 서비스, 검색 서비스, 이용제어불능 서비스, 이용제어가능 분배 서비스로 분류할 수 있다. 이 때, 메시지 서비스는 OSI의 응용 서비스인 MHS와 같은 특징을 가지고 있으므로 이에 대한 보안서비스도 포함하고 있다.

이렇듯, 개방형 환경에서의 전산망 시큐리티에 대한 연구가 활발히 진행되고 있으며, 이와 아울러 정부에서 추진중인 초고속 정보통신망에서는 이전의 저속망에서의 보안특성과 다른 보안특성이 나타날 것으로 예상됨으로 이에 관한 사전연구가 필요할 것으로 추측된다.

참 고 문 헌

1. 정진욱," EDI시스템 시큐리티 선행기술 연구 ", 한국통신 최종연구 보고서, 1993.12
2. ISO, "ISO 498/2 Security Architecture,Information Processing System-Open system Interconnection Reference Model", 1984
3. "Information Processing System-Open System Interconnection REFERRENCE Model-Part 2: Security Architecture", ISO/DIS 7498-2,1987
4. KOUJI NAKAO and KENJI SUZUXI," Proposal on a Secure Communications Service Element(SCSE) in the OSI Application Layer", IEEE Journal on Selected Area in Communication, Vol.7,NO.J, May 1989
5. 임채호,변옥환," ISO 응용계층의 시큐리티 서비스 설계 및 구현 연구", 동계 컴퓨터 통신 워크샵, 1990
6. Simson Garfinkel and Gene Pafford, " Pratical UNIX Security", Prentice Hall, 1991
7. Daniel C. Lynch, Marshall T. Rose, " Internet SystemHandbook", Addison-Wesley, 1993.
8. CCITT Recommmendation X.400-X.430, " Data Communication Networks Message Handling Systems", 1989
9. CCITT Recommmendation X.435, "Message Handling Systems:EDI Messaging Systems", 1990.9
10. CCITT Recommmendation F.435, "Message Handling Systems:EDI Messaging Systems", 1990.9
11. Warwick Ford, "Computer Communication Security", Prentic Hall, 1994
12. 이필중, 정진욱, 박명순, 이재용, "전산망의 안전대책 개요", 정보통신보호학회지, 1권2호, 3호
13. 임채호, 한상철, 변옥환, "연구전산망 보안 가이드", 동계컴퓨터통신워크샵논문집
14. William Stallings, "ISDN and Broadband ISDN ", Macmillan,1992
15. 임채호, "인터네트보안", KRNET'93, 7. 1993, KTRC
16. 차경돈, 홍기웅, 김동규, "Secure MHS를 위한 부인봉쇄 서비스", 통신정보보호학술발표논문집 Vol.1, No.1, 1990

정 진 욱

성균관대학교 전기공학과 졸업
서울대학교 계산통계학과(전산학 박사)
한국과학기술 연구소 연구원
한국과학기술 연구원 시스템공학 연구소 데이타통신 실장
Maryland대학교 객원교수
(현) 성균관대학교 정보공학과 교수