□ 기술해설 □

초고속정보통신기반 구축에 따른 시스템 및 네트워크 시큐리티

성균관대학교 정진욱*

목 차

1. 서 론

정보화사회의 가장 큰 특징중의 하나는 정보의 고집적화와 고집적화된 정보의 고속 유통에 있다. 정보저장장치의 대용량화 추세는 앞으로 더욱 가속화가 예상되며 정보를 저장하고 처리하는 모든 기기들은 통신회선을 통하여 상호연결되고 광섬유를 이용하는 정보 전송속도 또한 기가 bps급이 일반화 될 것으로 예측된다. 국가안보를 비롯한 모든 국가운영을 위한 중요정보들로부터 개인생활을 영위하는데 필요한 정보까지 그러한 저장용기에 저장되고 전국을 상호연결하고 있는 네트워크에 의해 끊임없이 접근되고 유통될 것이다.

이러한 정보의 고밀도화 고집적화 그리고 네트워크를 통한 쉬운 접근등은 우리생활에 엄청난 변화를 가져와 21세기 우리의 생활을 윤택하게 하고 우리의 국가경쟁력을 한차원 높이게 될 것이며 선진복지국가로 가는 필수적인 요건이 될 것이다. 산업혁명이 인간생활의 변화에 미쳤던 것보다 더 큰 정보화 혁명이 서서히 시작되고 있으며 초고속 정보통신망은 정보화혁명을 이루는 기반 구조로서 정보화 혁명의 성패를 가름하는 중요한 요인중의 하나가 될 것이다.

그러나 우리는 여기서 간과할 수 없는 사실 하나에 주목할 필요가 있다. 깨끗하고 편리한 에너지인 가스를 잘못 다스렸을 경우에 오는 엄청난 피해, 대규모 교통수단에서 안전이 무시되었을 경우에 오는 인명손실 등 모든 문명은 양면성을 가지고 있다는 사실이다. 고속화와 대규모화는 그 안전이 무시되었을 경우 그 피해 또한 대규모화한다는 사실에 주목하여야 할 것이다. 근년에 우리가 겪은 여러 가지 재난을 미루어 생각한다면 정보화 사회에서의 안전 혹은 보안이 유지되지 못했을 경우 우리가 입게될 손해는 엄청난 것임을 알 수 있을 것이다.

전산망에서 안전 혹은 보안이 유지되어야 할 자원에는 하드웨어적인 자원과 소프트웨어적인 자원이 있다. 하드웨어적인 자원은 주로 컴퓨터 자체나 통신설비중 물리적인 자원이 되며 물리적인 자원의 안전 문제는 가시적이므로 문제 자체가 명확하여 이에 대처하기 위한 방안도 비교적 단순하게 된다. 예를 들어 지진 홍수 등의 자연재해나 화재, 불법침입, 온습도 등 급격한 변화에 대응하는 방법 등이 이에 속할 것이다.

*종신회원

이들은 전산망과 직접적인 관계가 없이도 이미 명확한 규정에 의해 안전대책이 시행되고 있다.

이러한 물리적인 전산망 자원의 안전 문제도 매우 중요하지만 여기서는 전산망의 소프트웨어적인 자원의 보안 문제에 대해 중점적으로 생각해 보고자 한다. 사실 정보화가 진행될수록 소프트웨어적인 성격의 정보자원의 중요성이 더욱 크게 될 것이 틀림 없는 것이기 때문이다.

소프트웨어적인 성격의 전산망 자원에는 데이타, 파일, 시스템프로그램, 응용프로그램, 여러 가지 서류 등이 있으며 이들은 저장매체의 하드웨어적인 안전성이 유지되고 있다 하더라도 소프트웨어적으로 얼마든지 유해를 당할 가능성을 내포하고 있다. 소프트웨어적인 전산망 자원들은 다음과 같은 특성을 갖고 있다.

소프트웨어적인 전산망 자원들은 물리적인 접근없이도 얼마든지 그 내용에 접근할 수 있다. 즉 통신망을 통해 자원이 물리적으로 저장되어 있는 매체로부터 멀리 떨어져 있는 곳에서도 불법복사, 내용변조, 내용파괴 등의 행위가 가능하다.

소프트웨어적인 전산망 자원들은 훔쳐간 뒤에도 원형이 그대로 보존되어 있기 때문에 도난당한 후에도 도난 당한 사실을 알기가 어려워 그 피해가 지속적이 될 가능성이 있다.

소프트웨어적인 전산망 자원들은 종이에 기록된 문서가 변조되었을 때 비교적 쉽게 변조사실을 알 수 있는데 비해 컴퓨터 기록매체에 기록되어 있기 때문에 변조사실을 발견하는 일 또한 쉽지 않다. 따라서 그 피해가 지속될 가능성이 있다.

소프트웨어적인 전산망 자원들은 고집적화 고용량화 되어있고 보통 고속 통신회선으로 연결되어 있기 때문에 종이로 된 정보보다 훨씬 많은 양의 정보를 짧은 시간에 훔쳐가거나 변조 혹은 훼손시킬 수 있다.

문자정보들은 대화형 통신이 아니라 일괄통신의 형태를 취하며 음성통신처럼 사람이 직접 정보의 송수신자가 아니므로 통신상대방 상호간에 상대가 적당한 통신상대자인지를 확인하기 위해서는 별도의 장치를 필요로 한다.

위와 같은 여러 가지 특성 때문에 정보통신망에서의 시큐리티 문제는 복잡한 양상을 띠게 된다. 뿐만 아니라 정보통신망은 앞으로 더욱 개방적이고 이용과 편의 위주로 운영되어야 할 것이나 개방성이나 이용자편의성 등은 안전성과 정면으로 대치되는 개념이어서 어려움을 더하게 된다.

시큐리티 문제는 시스템 시큐리티와 네트워크 시큐리티로 나뉘어 진다. 그러나 O·S 시큐리티 문제를 제외한 시스템 시큐리티 문제는 모두 네트워크 시큐리티 문제와 유사한 특성을 갖는다. 따라서 본고에서는 네트워크 시큐리티 문제를 중심으로 하여 이야기를 전개하고자 한다. O·S 시큐리티 문제도 매우 중요하고 광범위한 기술적인 내용을 포함하므로 별도의 기회에 논의되어도 좋을 것이다. 네트워크 시큐리티에 대하여도 여러 가지 접근방법이 있을 수 있겠으나 국제표준기구(ISO)에 의해 국제표준으로 채택되고 또한 가장 널리 받아 들여지고 있는 OSI 네트워크 보안구조 모델을 통하여 그 체계적인 접근 방법을 살펴보고 어떠한 것들이 있는지 살펴보기로 하겠다.

2. OSI 보안 구조

OSI망 구조는 지금까지 개발된 어떠한 망구조 모델보다 체계적이고 합리적이며 가장 광범위한 지지를 얻고 있는 망구조 모델이다. ISO에서는 이러한 OSI망 구조의 부속서로서 보안구조(ISO 7498-2)를 세계표준으로 채택하고 관련된 표준안을 계속하여 개발하고 있는 상태로 모든 네트워크 보안의 기준이 될 것으로 보인다.

OSI 시큐리티 구조는 세 가지의 기본 개념으로 구성된다.

① 시큐리티 위협 : 어떤 기관이 소유하고 있는 정보의 시큐리티를 위태롭게 하는 행위

② 시큐리티 메카니즘 : 시큐리티 위협을 발견해 내거나 예방하거나 혹은 위협으로부터 회복하기 위하여 고안된 통신기법(메카니즘)

③ 시큐리티 서비스 : 기관이 데이타 처리시

표 1 Key OSI Security Standards

ISO 7498-2	OSI Basic Reference Model-Part 2. Security Architecture
ISO 8649 AM1	Service Definition for the Association Control Service Element- Amendment 1 : Authentication during Association Control Establishment
ISO 8650 AM1	Protocol Specification for the Association Control Service Element- Amendment 1 : Authentication during Association Control Establishment
ISO 9160	Data Encipherment -Physical Layer Interoperability Requirements
DIS 9796	Security Techniques : Digital Signature Scheme Giving Messange Recovery
ISO 9797	Data Cryptographic Techniqures : Data Integrity Mechanism Using a Cryptograhic Check *Function Employing a Block Cipher Algorithm*
DIS 9798-1	Security Techniqures : Entity Authentication Mechanisms-Part 1 : General Model
CD 9798-2	Security Techniqures : Entity Authentication Mechanisms-Part 2. Entity Authentication Using Symmetric Techniqures
CD 9798-3	Security Techniqures : Entity Authentication Mechanisms-Part 3 : Entity Authentication Using Public Key Algorithms
DIS 10116	Mode Of Operation for an n-Bit Block Cipher
CD 10181-1	Security Framworks-Part 1 : Overview
CD 10181-3	Part 3 : Access Control
CD 10181-4	Part 4 : Non-repudiation
CD 10181-5	Part 5 : Integrity
CD 10181-6	Part 6 : Confidentiality
CD 10181-7	Part 7. Security Audit Framework
DIS 10736	Transport Layer Security Protocol
CD 10745	OSI Upper Layers Security Model

스템이나 정보전송 시큐리티를 강화하기 위한 통신 서비스, 이 서비스들은 시큐리티 위협에 대한 대항 수단이다

그러면 시큐리티 위협, 시큐리티 메카니즘, 시큐리티 서비스의 순서대로 그 내용을 살펴보기로 한다.

2.1 시큐리티 위협

2.1.1 시큐리티 요구 조건

시큐리티 위협을 이해하기 위해서는 시큐리티 요구 조건을 먼저 살펴보아야 한다.

컴퓨터와 네트워크 시큐리티는 다음과 같은 세 가지 요구조건을 생각해 볼 수 있다.

① 비밀성(Secrecy) : 컴퓨터 시스템내의 정보는 오직 인가 받은자 만이 접근(access)할 수 있도록 보장되어야 한다. 접근에는 읽기와 인쇄하기 등이 포함되며 어떤 정보의 존재 사실 자체도 노출되어서는 안된다.

② 무결성(Integrity) : 컴퓨터 시스템 자산(assets)은 오직 인가 받은자 만이 내용을 수정할 수 있도록 보장되어야 한다. 수정에는 써 넣기, 내용변경하기, 지우기, 새로 만들어 넣기 등이 포함 된다.

③ 가용성(Availability) : 컴퓨터 시스템 자산은 오직 인가 받은 사람만이 사용할 수 있도록 그리고 언제나 사용가능하도록 보장되어야 한다.

2.1.2 위협의 형태

정상적인 정보의 흐름을 방해하는 몇 가지 형태의 위협요소들이 있다.

정상적인 정보의 흐름이란 정보가 정당한 송신자로부터 정당한 수신자까지 도청이나 변조 등 어떠한 방해도 받지 않고 정확하게 전송되는 경우를 말한다.

위협의 형태는 다음의 네 가지로 분류된다.

① 흐름차단(Interruption) : 시스템의 일부가 파괴되거나 사용할 수 없게 된 상태이다. 이는 시큐리티 요구조건 중 가용성에 대한 위협이다. 실제 예로는 하드디스크의 파괴, 통신회선의 절단 파일관리 시스템의 무력화 등이 여기에 속한다.

② 가로채기(Interception) : 인가받지 않은 제3자가 컴퓨터 자원을 액세스하는 경우이다. 이는 시큐리티 요구조건 중 비밀성(Secrecy)에 관한 위협이다. 인가받지 않은 자란 사람일 수도 있으나 프로그램이나 다른 컴퓨터일 수도 있다.

③ 변조(Modification) : 인가받지 않은자가 자원에 액세스할 뿐만 아니라 내용을 고치기까지 하는 경우이다. 이는 시큐리티 요구조건 중 무결성(Integrity)에 대한 위협이다. 데이타파일의 값을 바꾸거나

프로그램이 다르게 동작하도록 프로그램을 수정하거나 네트워크에 전송중인 메시지의 내용을 변조하는 경우이다.

④ 위조(Fabrication) : 인가받지 않은 자가 시스템에 위조물(counterfeit object)을 삽입하는 경우이다. 이 역시 시큐리티 위협요소 중 무결성(Integrity)에 대한 위협이다. 네트워크에서 가짜의 메시지를 삽입하는 경우 그리고 파일에 가짜 레코드를 추가하는 경우 등이다.

2.1.2.1 수동적인 위협

수동적인 위협은 전송중인 정보를 중간에서 도청하는 것이다. 여기에도 다시 두가지 형태가 있는데 메시지의 내용을 도청하는 것과 트래픽을 분석하는 것이 그것이다. 트래픽 분석이란 메시지의 내용이 아니라 트래픽 자체를 분석함으로써 통신하는 호스트의 위치나 메시지의 길이, 메시지 발생의 빈도 등을 확인함으로써 어떤 사실을 유추해 내고자 하는 것이다. 수동적인 위협은 감지하기가 매우 어려우며 메시지를 암호화 함으로써 방어할 수 있다.

2.1.2.2 능동적 위협

능동적인 위협은 데이터를 변조하거나 가짜 데이터를 만드는 행위를 말한다. 능동적 위협은 다시 가장(masquerade), 재연(reply), 메시지의 변조(modification of message), 서비스의 거절(denial of service)등 네 가지로 구분된다.

- 가장(masquerade) : 어떤 실체가 다른 실체인척 행동하는 것이다. 가장은 보통 남의 인증절차를 절취하였다가 자신이 마치 인증받은 그 사람인 것처럼 행동함으로서 그 사람의 권리를 행사하고자 하는 것이다.
- 재연(reply) : 정상적인 메시지를 도청하여 두었다가 재전송하여 이득을 취하는 행위 이다. 예를 들어 정상적인 지불명령을 도청하여 두었다가 다시 재전송 함으로서 두 번 지불받게 하는 행위 등이 여기에 속한다.
- 메시지의 변조(modification of message) : 합법적인 메시지를 변경하거나 지연시키거나 순서를 바꿔치기 함으로써 불법적인 이득을 취하고자 하는 행위이다.
- 서비스의 거절(denial of service) : 통신시설 등의 정상적인 이용을 방해하는 행위 이다. 예를 들어 공격자는 특정 목적지로 가는 모든 메시지를 지워 버리는 행위가 여기에 속한다. 때로는 모든 네트워크에 대해 공격이 이루어지기도 하고 네트워크에 쓸데 없는 메시지를 대량 투입함으로서 네트워크의 성능을 떨어 뜨리기도 한다.

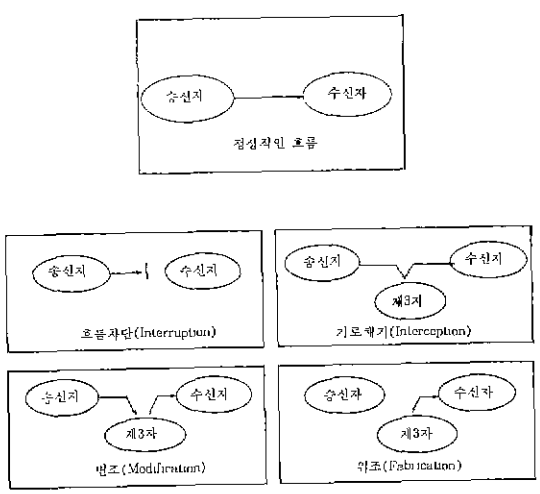
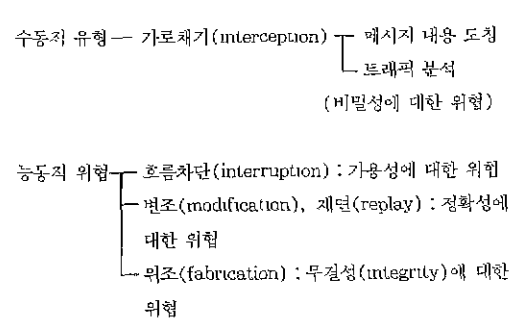


그림 1 시큐리티 유형의 네 가지 형태



〈능동적, 수동적 위협의 분류〉

2.2 시큐리티 메카니즘(Security Mechanism)

시큐리티 메카니즘은 OSI의 특정 계층에서 실현되는 것과 특정 계층과 상관없이 이루어지는 두 가지 종류가 있다. 이들을 차례로 살펴보기로 한다.

2.2.1 암호화

컴퓨터 시큐리티에서 가장 큰 역할을 하는 것이 암호화이다. 암호화란 인식가능한 메시지를 바꾸어 주는 프로세스(process)이다. 암호화에는 암호화와 복호화에 동일한 키(key)를 사용하는 전통적인(conventional) 암호화 방법과 암호화와 복호화에 서로 다른 키를 사용하는 공개 키 (public key)암호화 방법이 있다. 공개키 암호화 방법에서는 한쌍 두 개의 키중 하나는 공개하기 때문에 이러한 이름으로 불리운다. 키중 하나를 공개하지만 공개된 키로부터 비밀키를 유추하는 것은 수학적으로 불가능에 가깝다. 공개 키 방식은 관리해야 할 키의 갯수가 전통적인 암호화 방법에 비해 적어지는 이점이 있으나 연산 소요시간이 많이 걸리는 단점이 있다. 그러나 점차 연산속도가 개선되는 알고리즘이 등장하고 비강도(strength of secrecy)가 높기 때문에 많이 쓰이게 될 것으로 보이며 공개 키 방식의 암호화는 디지탈 서명(digital signature)에도 이용이 가능하다. 공개 키 암호화에도 몇 가지 방식이 있으나 RSA 방법이 보편화되어 있다.

2.2.2 트래픽 패딩(Traffic Padding)

링크 암호화, 패킷 헤더의 암호화 등을 이용하여 어느 정도의 트래픽 분석 위협으로부터 방어가 가능하나 트레픽의 양을 분석하는 위협으로부터 방어하기 위해서는 다른 방법이 필요하다. 트래픽 패딩은 정상적인 메시지흐름이 멈추었을 때 가짜 암호메시지를 계속 내보냄으로서 트래픽의 양을 분석하는 공격으로부터 방어하고자 하는 수단이다.

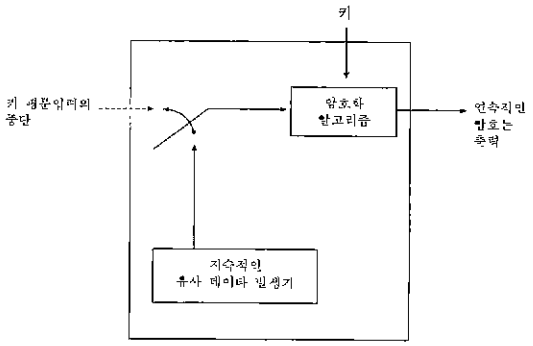


그림 3 트래픽 패딩 암호화 장치

2.2.3 인증교환(Authentication Exchange)

메시지의 암호화에 의해서도 서로 상대방이 정당한 상대방인지 인증할 수 있으나 MAC (Message-Authentication Code)을 사용하는 방법도 많이 이용된다. MAC을 이용함으로서 수신자를 메시지가 전송중에 변경되지 않았음을 확인할 수 있으며 메시지가 정당한 상대방으로부터 온 것임도 확인할 수 있다. 메시지가 순서번호를 갖고 있다면 메시지가 올바른 순서로 도착한 것도 확인이 가능하다.

2.2.4 디지탈 서명

인증교환은 제3자의 공격으로부터 메시지를

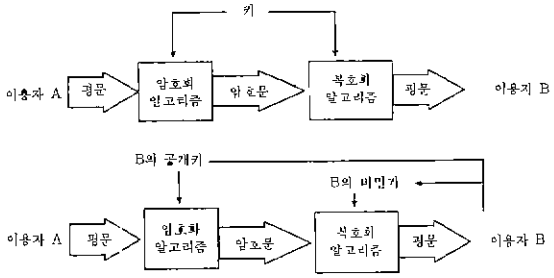


그림 2 전통적 암호화(상)와 공개 키 암호화(하) 방식

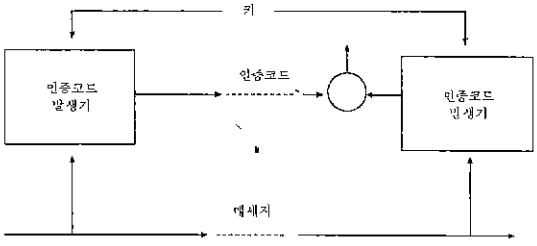


그림 4 메세지 인증 방법

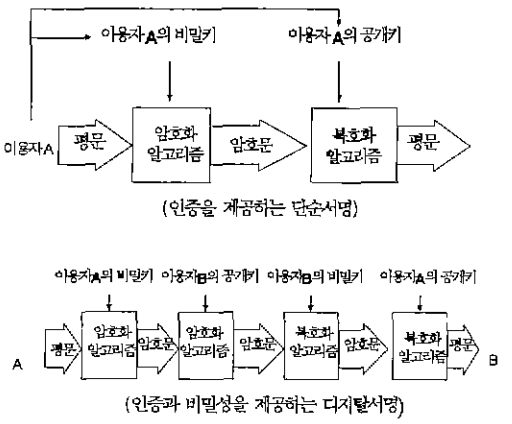


그림 5 공개키를 이용하는 직접 서명방식

보호할 수는 있으나 통신 당사자들이 거짓 메시지를 만들거나 (수신자) 메시지 발신사실을 부인(발신자)하는 등의 행위로부터 발생하는 문제는 여전히 남게 된다. 이러한 통신 당사자들의 부정한 행위로부터 방어하는 수단이 디지탈 서명이다. 디지탈 서명은 서명자와 서명시간이 검증가능해야 하고 서명당시 메시지의 내용을 인증할 수 있어야 하며 추후 법적인 문제가 발생하였을 때 제3자에 의해 확인가능해야 한다. 디지탈 서명방식에는 통신당사자들이 직접 서명하고 확인하는 직접 서명방식과 중재자의 역할을 하는 제3자를 두는 중재자 서명방식이 있다. 직접서명방식은 공개 키 시스템을 이용하는 것이 일반적이며 중재자 서명방식은 직접서명방식에서 송신자가 키를 분실하여 키의 취득자가 메시지를 보냈음을 주장하는 것을 방지할 수 있다. 중재자 디지탈 서명방식에서는 전송되는 메시지가 우선 중재자에게 가서 내용과 발신처를 확인한 후 발신시간을 명기하여 수신자에게 보냄으로써 그러한 단점을 보완할 수 있다.

2.2.5 접근제어(Access Control)

접근제어는 특정 시스템이나 특정 자원에 오직 인가 받은자 만이 접근할 수 있도록 제어하는 것이다.

보통 컴퓨터에서 주로 적용되어 왔으나 네트워크에서도 필요한 메카니즘이다. 이용자(사람)를 제한하는 경우에는 지금까지 패스워드가 주로 이용되어 왔으나 단순한 패스워드 이용은 많은 문제점이 있다. 액세스하는 주체를 Subject, 액세스 대상이 되는 객체를 Object로 하여 액세스 매트릭스를 이용하는 방법이 많이 쓰인다.

2.2.6 데이타 무결성(Data Integrity)

인증은 통신하는 당사자들이 상호간에 정확한가 하는 관점이지만 무결성(integrity)은 실제 데이타의 정확성 보장을 의미한다. 기술적으로 에러제어와도 유사하다. 데이타무결성은 모든 통신프로토콜에서 중요한 의미를 가지며 따라서 모든 프로토콜은 무결성을 보장하기 위한 메카니즘을 갖고 있다. 프로토콜 데이타유니트(PDU)에서 사용되는 체크섬(Check sum)도 한 가지 예이다. 에러의 경우와는 달리 의도적인 변조를 감지해 내기 위해서 사용되며 PDU의 체크섬이 암호화되어 전송된다면 이러한 의도적인 변조 행위를 쉽게 감지할 수 있을 것이다.

2.2.7 경로제어(Routing Control)

네트워크계층에서 메시지의 안전한 전송을 위해 미리 정의된 혹은 동적으로 정하는 안전한 경로 선택을 할 수 있는 것을 경로제어 메카니즘이라고 말한다.

2.2.8 공증(Notarization)

제3의 공증자(third-party notary)를 두어 통신에서의 무결성(integiry), 발신처, 시간, 수신처 등을 법적으로 확증해 주는 메카니즘이다.

2.2.9 신뢰할 수 있는 기능 (Trusted Functionality)

주어진 메시지 자체의 수동적 혹은 능동적 위협으로부터의 방어 이외에도 시큐리티를 보장하기 위해 시큐리티 수준을 정해 관리하는 방법도 이용된다. 시큐리티를 유지해야 하는 수준을 정해 거기에 맞는 관리를 행해야 한다. 참조 모니터(reference monitor)를 두는 방법이 이용될 수 있다.

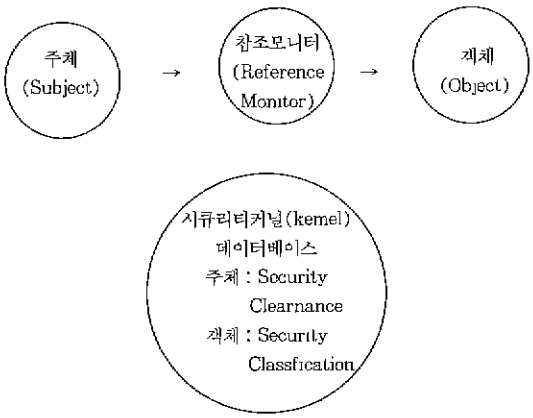


그림 6 참조 모델의 개념

2.2.10 시큐리티 레이블(Label)

PDU 등의 자원에 시큐리티 분류 등급을 지시하는 레이블을 둠으로서 관리를 용이하게 하는 기법이다.

2.2.11 사건탐지(Event Detection)

시큐리티와 연관된 사건이 발생했을 경우 이를 탐지하는 메카니즘으로 OSI 관리기능의 일부이다. 예를 들어 시큐리티 위반, 미리 등록한 특정사건, 미리 정의한 횟수(부정한 로그인 등)의 초과 등을 탐지 기록하는 기능을 말한다.

2.2.12 시큐리티 감사일지 (Security-Audit Trail)

시큐리티 감사일지는 시큐리티와 관련된 정보를 기록함으로서 시큐리티 위반 사실 등을 사후에 추적하는 목적으로 이용된다.

2.2.13 시큐리티 회복(Security Recovery)

다른 시큐리티 위반이 발견되었을 때 취하는 조치로서 즉시처리, 한시적(Temporary)처리, 장기(Long-term)처리 등으로 구분된다.

즉시 처리는 위반 사실의 발견 즉시 사용 중지를 시키는 것이며 한시적 처리는 일정기간 동안 그리고 장기처리는 장기적으로 블랙리스트 등을 통해 관리한다거나 키의 변경 등의 조치를 취하는 것이다.

2.3 시큐리티 서비스

시큐리티 서비스는 OSI계층에 의해 제공되며 시스템이나 데이타 전송에 적당한 시큐리티를 보장하기 위한 서비스이며 앞에 소개된 시큐리티 메카니즘을 통하여 이루어진다. 인증(Authentication), 접근제어(Access Control), 데이타 비밀성(Data Confidentiality), 데이타 무결성(Data Integrity), 부인봉쇄(Nonrepudiation) 등 크게 다섯가지 서비스로 나누어진다.

2.3.1 인증(Authentication)

인증서비스는 두 가지로 구분되는데 첫째는 대등 실체인증(Peer-entity Authentication)으로 연결설정단계 등에서 상대방이 정당한 상대방인지를 확인하는 서비스이다. 즉, 가장(masquerade) 혹은 재연(replay) 등의 시도를 막을 수 있다. 둘째는 데이타 발신자 인증(Data-origin Authentication)으로 전자 메일 등에서 이용된다. 이 서비스가 데이타유니트의 중복이나 변조 등에 대해 보증하여 주지는 않는다.

2.3.2 접근제어(Access Control)

호스트시스템에 접근하는 것을 제한하거나 제어하는 서비스이다.

2.3.3 데이타 비밀성(Data Confidentiality)

비밀성 서비스는 전송되는 메시지가 수동적인 공격으로부터 보호받도록 해 주는 서비스이다. 가상채널이 유지되는 동안 계속적으로 서비스하는 경우와 단위 메시지에 대해 혹은 특정 부분(field)에 대해서만 비밀성 서비스를 제공할 수도 있다. 암호화 메카니즘이 사용된다.

2.3.4 데이타 무결성(Data Integrity)

데이타 무결성 서비스는 전송메시지가 중복, 삽입, 변조되지 않았으며 재연(replay)된 것도 아니라는 것을 보증하는 서비스이다. 데이타파괴의 경우에도 이 서비스가 적용대상이 된다.

2.3.5 부인봉쇄(Nonrepudiation)

데이타의 발신자가 발신 사실을 수신자가 수

표 2 시큐리티 서비스와 메카니즘과의 관계

	Enciper-ment	Digital Signature	Access Control	Data Integrity Authentication	Authentica-tion Exchange	Traffic Padding	Routing Control	Notari-zation
Peer entity Authentication	Y	Y	·	·	Y	·	·	·
Data origin Authentication	Y	Y	·	·	·	·	·	·
Access Control	·	·	Y	·	·	·	·	·
				Data Confidentiality				
Connection Confidentiality	Y	·	·	·	·	·	Y	·
Connectionless Confidentiality	Y	·	·	·	·	·	·	·
Selected field Confidentiality	Y	·	·	·	·	·	·	·
Traffic flow Confidentiality	Y	·	·	·	·	·	·	·
				Data Integrity				
Connection integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selected field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selected field connectionless integrity	Y	Y	·	Y	·	·	·	·
				Nonrepudiation				
Nonrepudiation origin	·	Y	·	Y	·	·	·	Y
Nonrepudiation delivery	·	Y	·	Y	·	·	·	Y

Y=Yes : the mechanism is considered to be appropriate, either on its own or in combination with other mechanisms
=THe mechanism is considered not to be appropriate

신 사실을 부인하는 것을 봉쇄하는 서비스이다.

2.4 메카니즘과 서비스의 관계

시큐리티 서비스는 시큐리티 메카니즘에 의해 구현된다. 따라서 서비스를 구현하는 메카니즘은 여러 가지 일 수도 있다. 표 2에서는 이들간의 관계를 보여주고 있다.

3. 초고속 정보화를 위한 보안 기술 분야

초고속 정보통신 환경에서 주요 전산자원 및 국가, 기업, 개인의 정보를 보호하고 국가보안기관에서 인증 받을 수 있는 시스템 보안, 전

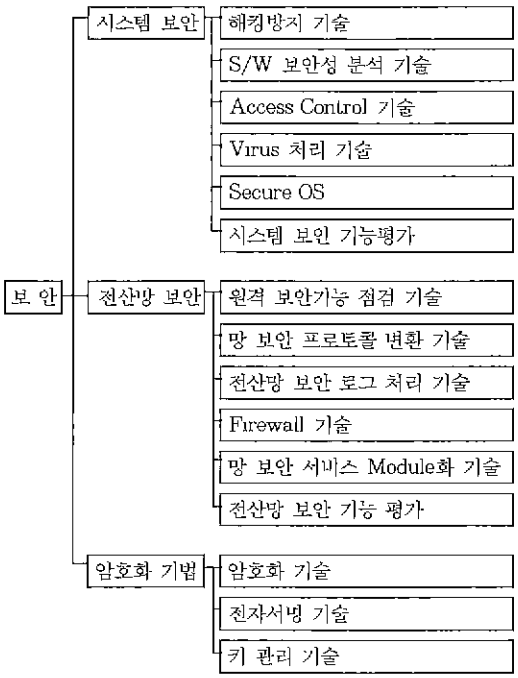


그림 7 초고속 전산망 보안 기술의 체계

산망 보안, 암호화 기법의 특징을 살펴보고 고속 전산망 환경에서의 보안기술 분야를 살펴보겠다.

초고속 전산망 보안 기술은 크게 시스템 보안, 전산망 보안, 암호화의 세 분류로 분류한다.

3.1 시스템 보안 기술

● 해킹 방지

해킹 가능성을 사전에 예방하기 위하여 하드웨어, 소프트웨어의 보안 취약성 진단, 사용자들의 시스템 사용 관리, 모니터링을 통하여 사전에 시스템 침입을 예방하고, 다양한 경로를 통한 해킹을 감지하고 해킹형태를 분석한다. 또한 해커의 위치를 실시간 추적하고 보안 사고를 분석한다.

● 소프트웨어 보안성 분석

전산망에서 제공되는 모든 서비스는 시스템 또는 응용 소프트웨어를 통해 제공되고 있으며 일반적으로 해킹은 대부분 이러한 소프트웨어의 보안 취약성을 통하여 행해지고 있다. 전산망 운영에 사용되는 소프트웨어의 보안 취약성을 찾아낸다.

● 접근제어(Access control)

접근제어는 어떤 개체가 어떤 자원의 활용이 가능한지의 여부를 결정하는 기법을 말하며 시스템에 접근하고자 하는 개체가 시스템에 자신의 신원을 제시한 후 시스템에 자신의 신원을 인증하며 인증된 개체가 자원에 접근 할 수 있는 권리를 확인함으로서 다양한 전산자원(하드웨어,소프트웨어,데이타베이스)을 보호하며 접근 기록을 남겨 이를 감시함으로서 시스템의 보안을 강화한다. 즉, 전산자원의 사용을 인증받은 사람에 한해서 사용하게 하여 불특정 다수의 사용자로부터 주요 전산자원을 보호한다.

● 바이러스 처리

주요 데이터 및 소프트웨어를 파괴하는 바이러스를 비롯한 worm, 박테리아 등 다양한 형태의 악성 프로그램을 제거시킨다. 이러한 악성 프로그램의 패턴을 인식하여 궁극적으로 인체의 항체 자동생성과 같은 시스템을 개발한다.

● 안전한 OS개발

사용자 관리, 비밀번호 관리, 파일시스템의 변조 방지 및 검증, 망 서비스 접근제어, 관리자 권한분산 등의 기능을 OS에 통합한다.

● 시스템 보안 기능 평가

시스템 보안 평가의 기준을 설정하고 시스템 보안기능의 평가를 자동화한다.

3.2 전산망 보안 기술

● 원격 보안 기능 점검

해킹예방, 탐지, 추적, 복원, 소프트웨어 보안성 분석, 접근제어, 바이러스 처리기술 등 한 시스템 내부에서의 이루어지는 기술을 보안센터와 같은 원격지에서 전산망을 통하여 동시에 많은 시스템의 보안 관리를 가능하게 한다.

● 전산망 보안 프로토콜의 변환

상이한 프로토콜을 사용하는 전산망이 게이트웨이를 통하여 상호연동시 암호화,키 관리, 사용자 정보 등 보안정보의 상이성에 대한 투명성을 제공한다.

● 방화벽(Firewall) 기술

특정한 전산망을 외부 전산망으로부터 격리하여 특정 전산망의 내부 정보를 보호하고 외

부에서 들어오는 정보와 사용자를 선별하여 전산망의 보안성을 향상시킨다. 또한, 전산망의 일부를 보안환경에 따라 전산망의 범위를 재조정한다.

● 전산망 보안 서비스 모듈화

전산망 응용 서비스에 필요한 암호화, 인증, 키관리 등 공통 보안 기능을 분리하여 응용서비스가 공통적으로 사용하고 응용서비스의 개발시 보안 관련 기능은 공통 보안 서비스의 모듈화를 사용하게 한다.

● 전산망 보안 평가

전산망 보안 평가 기준을 설정하고 전산망 보안 기능의 평가를 자동화한다.

3.3 암호화 기법

● 암호화

암호화 알고리즘은 초기 평문의 각 문자를 다른 문자나 심볼로 일대 일 대응시킴으로서 평문의 문자나 어떠한 암호문자로 변환되는지를 알수 없도록 혼동에 목적을 둔 환자 암호방식과 평문의 문자를 다시 재배열하는 방식으로 평문과 키를 가지고 정보를 암호문 전체에 분산시키는 전치 암호 방식, 환자와 전치암호 방식을 혼합한 DES(Data Encryption Standard)방식, 1976년 Diffie와 Hellman이 제시한 공개키 암호방식인 RSA(Rivers, Shamir, Adleman) 방식, 공개키 암호 방식의 또 다른 흐름으로 NP-complete Knapsack 문제에 기반한 Trapdoor Knapsack 암호방식 등이 기존의 전산망에서 이용되고 있다. 이와같은 암호화 방식을 기반으로 초고속 전산망에서는 응용서비스를 통하여 전달되는 대용량 데이타의 암호화를 위한 새로운 암호화 기법을 개발하고 이 기법이 실시간 처리되어야 한다.

● 전자서명

대표적인 암호화 프로토콜로서 디지탈 서명은 종래의 종이서류에 의한 문서수발 업무 등이 컴퓨터 통신망을 통해 빠르고 경제적으로 이루어지므로, 메시지 전송시 상대방의 신분을 확인하거나 사용자의 정당성을 인증하고 송·수신간에 일어날 수 있는 제반 분쟁을 해결할 수 있도록 통상적인 (인감)도장과 같은 역할을 해줄 수 있는 제도나 절차가 요구된다. 이와같이 컴퓨터 통신망을 통해 메시지 전송시 필요한 메시지 서명 방식을 말한다.

이러한 프로토콜에는 첫째, 다른 매개수단을 통하지 않고 송.수신자간에 직접 메시지와 서명을 송.수신하는 직접서명과 둘째, 송·수신자간에 제3자의 중재자를 통하여 메시지를 송.수신함으로서 중재자에 의해서 송신자의 서명이 인증되는 간접서명 방법, 셋째, 직접 서명방법과 간접 서명 방법을 혼용한 혼합서명 방법이 있다. 디지탈 서명은 개인의 고유성과 정당성을 제공하고 메시지 인증과 송.수신자 사이에 발생하는 제반 문제를 해결해 주어야 하기 때문에 수신자는 메시지 서명을 보고 송신자를 확인할 수 있어야하며 수신자를 포함한 어느 누구도 메시지 내용을 변조하거나 송신자의 서명을 위조할 수 없어야 한다. 또한 만약 송신자가 메시지의 내용이나 서명을 부인할 경우 제3자가 송신자와 수신자의 분쟁을 해결해 줄 수 있어야한다. 이러한 기법을 기반으로 초고속 전산망에서 응용서비스를 통하여 전달되는 대용량 데이타의 변조방지를 위한 무결성 검증 방식으로 새로운 전자서명 기법을 개발하고 이것이 실시간 처리되어야 한다.

● 키관리

네트워크가 대규모화되고 또 장애나 신규 가입자 의한 빈번한 변동이 수반되고 있는 정보화 사회에 있어서 키의 분배 및 관리는 중요문제로 나타나고 있다. 초고속 전산망 환경에서 응용서비스별로 보안 기능에 필요한 데이타의 암호화와 전자서명에 필요한 키의 분배 및 관리를 효율화하기 위한 메카니즘이 개발되어야 한다.

4. 결 론

통신망을 사용하는 사용자의 요구와 통신망에서 제공하는 서비스는 끊임없이 변화해 가고 있는데 이러한 변화 추세를 살펴보면 다음 몇가지로 요약할 수 있다.

첫째, 서비스를 제공하기 위한 대역폭의 확대이다. 즉, 앞으로 보편화될 서비스들은 현재 음성 서비스에서 제공하는 대역폭의 수천배를 요구할 것이다.

둘째, 음성, 데이타 등 각각의 서비스가 분리된 트래픽을 전달하는 것에서 음성과 화상이 복합되거나 음성과 데이타 및 화상이 복합된 형태의 서비스가 급속히 확장될 것이다.

셋째, 공중망을 중심으로 서비스가 제공되던 형태에서 다양한 형태의 사설망이 구성되는 것이다. 이는 각종 데이타베이스를 제공하는 사설 VAN(Value Added Network)의 확대를 의미하기도 한다.

이처럼 기존의 통신망에서 제공하는 서비스와 사용자들의 요구사항을 종합해서 보면 고품질, 높은 전송속도, 새로운 형태의 서비스에 유연하게 대처할 수 있는 새로운 통신망에 대한 요구가 증가하면서 1995년 이후부터 본격적으로 광대역종합정보통신망(B-ISDN)에 관한 연구를 수행하여 오고 있다. 즉, B-ISDN은 사용자측 뿐만아니라 망측에서도 음성, 데이타, 오디오, 비디오 등의 서비스 통합과 통신 서비스의 광대역화를 실현하고자 하는 통신망이다. B-ISDN이 수용하여야 할 통신 서비스는 ISDN에서 제공하는 서비스 외에 무엇보다도 큰 대역폭을 요구하는 비디오 관련 서비스와 B-ISDN을 경유한 고속데이타통신서비스이다.

이러한 광대역종합정보서비스가 본격적으로 진행되면 서비스를 이용하고자 하는 사용자들은 엄청나게 늘어나게 될 것이고 개인의 은밀한 정보나 기업의 민감한 정보 즉 이익에 관계되는 정보가 통신과정에서 도청될 가능성은 지금의 통신망에서는 느낄 수 없을 정도로 높아질 것이다. 이때문에 서비스들을 이용하는 사용자들은 그들의 전자정보가 송신될 때 제3자에 의해 수정되거나 폭로되지 않고 원하는 수신자에게 전달될 것이라는 확실한 믿음이 있어야만 서비스들을 사용할 것이다. 따라서 도청, 고의, 감염등의 악의로 부터 기밀을 지키기 위한 암호 통신 시스팀이 개발되고 사용되어지고 있다. 그러나 이러한 알고리즘들은 계산량이 많고 처리 시간이 다소 오래 걸려 실시간 처리를 요하는 광대역 통신 시스팀에서 구현하는데 어려움이 있다. 따라서 기존 암호 방식의 단점인 많은 계산량과 늦은 처리 속도를 개선하여 초고속 정보통신 환경에 효율적으로 적용시키기 위해서는 새로운 고속화 알고리즘의 개발이 필요하다. 이러한 시큐리티 문제는 이제까지 존재해온 문제이지만 앞으로 초고속 정보통신망으로 진행되면서 더욱 그 심각성이 증대되고 있기 때문에 21세기 초고속 정보통신 구축 사업에서 보안 문제는 결코 소홀히 할 수 없는 분야인 것이다.

참고문헌

[1] 정진욱, "암호화프로토콜의 연구동향", 데이타 보호기술 워크샵,1991.

[2] CCITT Recommendation X.400 - X.430, "Data Communication Networks Message Handling Systems", 1989.

[3] CCITT Recommendation X.435, "Message Handling Systems : EDI Messaging Systems", 1990. 9.

[4] CCITT Recommendation F.435, "Message Handling Systems : EDI Message Systems", 1990. 9.

[5] CCITT, "Recommendation X.509, The Directory-Authentication Framework",1989

[6] Rivest,R., "The MD4 Message-Digest algorithm(RFC 1186)", 1990.

[7] Rivest,R., "The MD5 Message-Digest algorithm", July, 1991.

[8] Kent,S., Linn,J., "Privacy Enhancement for Internet Electronic Mail", Internet Activities Board Privacy Task Force, 1989. 8.

[9] Richard Hill, "EDI and X.400 using Pedi : The guide for implementation and users", Technology Apprasals LTD, 1990. 12.

[10] 0. Suzki,K., Nakao,K. "Proposals on a Secure Communication Service Element (SCSE) in the OSI Application Layer", IEEE Journal on Selected Areas in Communication, Vol.7, No.4, 1989.

[11] Christopher Mitchell, Michael Walker, David rush, "CCITT/ISO Standards for Secure Message Handling", IEEE Journal on Selected Areas in Communication, Vol. 7, No.4, 1989.

[12] Thomas Beth, Dieter Gollman, "Algorithm Engineering for Public Key Algorithms", IEEE Journal on Selected Areas in Communication, Vol.7, No.4, 1989.
[13] Man Young Rhee, "Cryptography and Secure Communications", 1993.
[14] Ashok K.Agrawala. Bijendra N.Jain, "Open Systems Interconnection : Its Architecture and Protocols", 1990.
[15] Albert J.Marcella, Jr.and Sally Chan, "EDI Security, control, and audit", 1993.
[16] Cemil Betanov, "Introduction to X.400", 1993.
[17] D.W.Davies, W.L.Price, "Security for Computer Networks", 1989.
[18] 한국전산원, "개방형 EDI의 표준화에 관한 연구", 1992.
[19] 한국전산원, "국가기간전산망 EDI 메시지 통신 기능표준(안)", 1992.
[20] 임채호,변옥환, "ISO 응용계층의 시큐리티 서비스 설계 및 구현 연구",동계 컴퓨터 통신 워크 샵, 1990.
[21] Daniel C. Lynch, Marshall T. Rose, "Internet SystemHandbook", Addison-Wesley, 1993.
[22] Warwick Ford, "Computer Communication Security", Prentic Hall, 1994.
[23] 이필중, 정진욱, 박명순, 이재용, "전산망의 안전대책 개요", 정보통신보호학회지, 1권2호, 3호.
[24] 임채호, 한상철, 변옥환, "연구전산망 보안 가이드", 동계컴퓨터통신워크샵논문집.
[25] William Stallings, "ISDN and Broadband ISDN", Macmillan, 1992.
[26] 임채호, "인터네트보안", KRNET'93, 7. 1993, KTRC.
[27] 현대암호학, 한국전자통신연구소편저, 1991. 8.
[28] 원동호, "암호방식과 키 분배", 한국통신정보보호학회지, 1권, 1호, 1991.
[29] 시스템공학연구소, "Workstation Security Guide Summary", 1993.
[30] 한국전산원, 전산망 안전 신뢰성 표준개요, 1993.4
[31] TIS, Internet Firewalls Toolkit-An Overview, User's Overview, 1993.
[32] RFC1244, Site Security Handbook.
[33] RFC1282, Guidelines for Secure Operation of the Internet.
[34] Rihard D.Pethia Kenneth R.Van WYK. Computer Emergancy Response-An International Problem,CERT/CC SEI CMU, 1990.
[35] Eugene H.Spafford, "The Internet Worm Program : An Analysis",Purdue Technical Report CSD-TR-823, Nov. 1988.
[36] KUS, "WG-SECURITY : 0002,IETF Security Ares 활동 현황", 1992. 7.

정 진 욱

1974.2 성균관대 전기공학 졸업 (공학사)
1979.2 성균관대 전자공학 졸업 (공학석사)
1991.2 서울대 계산통계학 졸업 (이학박사)
1973.9～1981.12 한국과학기술연구소 연구원
1982.1～1985.2 한국과학기술연구소 실장
1981.9～1982.8 미국 Recal-Milgo Co. 객원연구원
1978.9～1985.2 서강대,동국대,단국대 강사
1992.1～1993.1 미국 Maryland 대학교 객원연구원
1985.3～현재 성균관대학교 정보공학과 정교수
관심분야 : 초고속통신망, 통신프로토콜, 네트워크관리, 네트워크 보안, ATM 트래픽관리