通信情報保護學會誌
第5卷 第3號, 1995. 9

OSI 통신망에서 응용 계층 보안

이 창 진* 노 봉 남**

1. 서 론

컴퓨터 네트워크의 발달로 인한 개방 분산 환경은 다양한 계산 자원들의 공유를 통하여 서로 다른 지역에 위치한 많은 정보들을 이용할 수 있게 되었다. 그러나 필연적으로 정보의 공유로 인하여 많은 문제점들이 야기되었는데, 그 중에서도 보안 침해 문제가 심각하게 대두되고 있다.

보안 침해는 그 의도에 따라 여러가지 형태로 나타날 수 있는데 크게 정보의 정상적인 흐름의 방해(interruption), 정보를 중간에서 가로채기(interception), 정보의 불법적인 변경(modification), 그리고 정당한 사용자를 가장(masquerade)하는 것과 같은 네 가지 범주로 나누어 생각해 볼 수 있다.

OSI에서는 이러한 보안 침해 사고에 대비해 시스템의 정상적인 동작 및 중요한 정보의 보호를 위하여 여러가지 보안 서비스 및 보안 메카니즘들을 정의하고 있다. 보안 서비스들은 그 기능에 따라 적당한 계층에 정의되며, 보안 서비스를 지원하기 위하여 여러가지 보안 메카니즘들이 응용 영역에 따라 선택적, 또는 복합적으로 이용된다.

본 기사에서는 OSI/RM에서 제공하는 여러가지 보안 서비스와 보안 메카니즘들을 살펴보고, 이들이 응용 계층의 서비스들, 특히 X.400 MHS 서비스, X.500 디렉토리 서비스, FTAM 서비스의 보안을 유지하기 위하여 어떻게 사용되는가를 알아본다. 그리고 보안 서비스 및 보안 메카니즘들이 망 관리에서 보안을 유지하기 위하여 어떻게 이용되는가에 대하여도 살펴본다.

2. OSI 보안 서비스 및 보안 메카니즘

OSI/RM에서 보안 유지를 위한 다양한 보안 서비스와 메카니즘들이 존재한다. 이들은 각각의 기능에 따라 여러 계층에 위치하며, 보안 정책이나 사용자의 요구 사항을 만족시켜 주기 위하여 비 OSI 서비스 및 메카니즘과 결합되어 사용된다. 또한 보안 서비스를 구현하기 위하여 여러가지 보안 메카니즘들이 결합되어 이용된다. 보안 서비스 및 보안 메카니즘들은 다음과 같은 것들이 있다.

* 전남대학교 대학원 전산통계학과 석사과정
** 전남대학교 전산학과 교수

2.1 보안 서비스

보안 서비스는 각각의 기능에 따라 아래와 같이 크게 다섯 개의 범주로 나눌 수 있다.

- 인증(authentication)
- 접근 제어(access control)
- 데이타 비밀성(data confidentiality)
- 데이타 무결성(data integrity)
- 비부인(non-repudiation)

먼저, 인증은 대등 개체 인증과 데이타 근원 인증으로 나눌 수 있다. 대등 개체 인증 서비스는 (N)-계층 개체들이 서로 상대방이 자신이 요청한 개체인지를 확인하는 서비스이다. 이 서비스는 상호 연결된 여러 개체들을 확인하기 위하여 데이타 전송을 위한 연결 설정 단계나 실제 데이타 전송 도중에 제공되어질 수 있다. 또한 이 서비스는 가장(masquerade)이나 이전 단계의 이용했던 연결을 불법적으로 반복(replay)하는 것을 방지하여 줄 수 있다. 인증은 일방에 의해서 행해질 수도 있고 쌍방에 의해서 행해질 수도 있다. 한편, 데이타 근원 인증은 (N)-계층 개체들 사이에 데이타의 근원지를 확인하는 서비스이다. 그러나 이 서비스는 데이타의 중복이나 수정으로부터 데이타를 보호해 주지는 못한다.

둘째, 접근 제어 서비스는 망의 자원들을 불법적인 사용으로부터 보호한다. 망에 존재하는 자원들은 정당한 권한을 가진 사용자에 의해서만 사용되어야 한다. 이 보안 서비스는 다양한 형태의 접근(정보에 대한 읽기, 쓰기, 수정, 삭제 등)에 대하여 적용될 수 있다. 보안 정책에 따라 서로 다른 접근 제어 서비스가 선택적으로 이용될 수 있다.

셋째, 데이타 비밀성은 데이타가 불법적으로는 노출되는 것을 방지하는 서비스를 말한다. 이는 다시 연결 비밀성, 비연결 비밀성, 선택된 필드의 비밀성, 트래픽 흐름 비밀성으로 나누어진다.

넷째, 데이타 무결성은 고의적인 보안 위협으로부터 데이타를 보호하는 것을 말하며, 데이타가 불법적으로 변경되는 것을 방지하는 것을 말한다.

마지막으로 비부인(non-repudiation) 서비스는 크게 두 가지 형태로 나누어진다. 첫번째가 데이타의 근원지에 대한 증명이 수신자에게 제공되는 경우이다. 이것은 송신자가 수신자에게 데이타를 보내지 않았다고 거짓으로 부인하는 경우를 방지한다. 두번째는 데이타의 송신자에게 데이타가 전송되었다는 증명을 제공하는 경우이다. 이것은 수신자가 데이타를 받지 않았다고 거짓으로 부인하는 경우를 방지한다.

2.2 보안 메카니즘

여러가지 보안 메카니즘들이 앞절에서 설명된 보안 서비스를 지원하기 위하여 적당한 계층에 포함된다. 이들을 다음과 같이 요약할 수 있다.

- 암호화(encipherment)
- 디지탈 서명(digital signature)
- 접근 제어 메카니즘
  (access control mechanisms)
- 데이타 무결성 메카니즘
  (data integrity mechanisms)
- 인증 교환 메카니즘
  (authentication exchange mechanism)
- 트래픽 첨가 메카니즘
  (traffic padding mechanism)
- 라우팅 제어 메카니즘
  (routhing control mechanism)
- 공증 메카니즘(notarization mechanism)

먼저 암호화는 데이타나 트래픽 흐름 정보 등에 대한 비밀성을 제공하며, 다른 보안 메카

니즘의 일부로 이용되거나 다른 메카니즘을 보완하기 위하여 사용된다. 암호화 알고리즘은 크게 다음과 같이 두가지로 나누어진다.

- 대칭 알고리즘 : 암호화 키와 복호화 키가 같은 경우
- 비대칭 알고리즘 : 암호화 키와 복호화 키가 다른 경우

둘째, 디지탈 서명 메카니즘은 데이타에 서명하는 과정과 서명된 데이타를 검증하는 두 단계로 구성된다. 첫번째 과정은 서명을 한 사람만이 알고 있는 정보를 이용하여 행해지며, 두번째 과정은 서명을 한 사람뿐만 아니라 다른 사람들에게도 알려진 정보를 이용한다.

셋째, 접근 제어 메카니즘은 객체의 접근 권한을 검사하기 위하여 개체의 인증된 신원, 능력과 같은 정보를 이용한다. 만약 자원들에 대하여 불법적인 접근 시도가 행해진다면, 이 접근은 접근제어 기능에 의하여 거절되고 보안 일람을 발생하며, 보안 회계 감사를 위하여 기록된다. 접근제어 메카니즘은 통신하는 양쪽 종단간이나 중간에 모두 놓일 수 있다.

표 1. 보안 서비스와 보안 메카니즘 사이의 관계

Mechanism / Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control Service			Y					
Connection Confidentiality	Y						Y	
Connectionless Confidentiality	Y						Y	
Selective Field Confidentiality	Y							
Traffic Flow Confidentiality	Y					Y	Y	
Connection Integrity without Recovery	Y			Y				
Connection Integrity without Recovery	Y			Y				
Selective Field Connection Integrity	Y			Y				
Connectionless Integrity	Y	Y		Y				
Selective Field Connectionless Integrity	Y	Y		Y				
Non-repudiation Origin		Y		Y				Y
Non-repudiation Delivery		Y		Y				Y

넷째, 데이타 무결성 메카니즘은 단일 데이타나 필드에 대한 무결성과 일련의 데이타나 필드에 대한 무결성을 지원하는 메카니즘이 서로 다르다. 데이타를 전송할 때 무결성을 유지하는 방법으로는 데이타 자체의 함수로부터 계산한 값을 암호화하여 데이타의 마지막에 첨가하는 것이 있다. 그러면 수신자는 똑같은 함수를 적용하여 구해진 값을 상호 비교하므로써 데이타가 변경되었는지를 확인할 수 있게 된다.

다섯째, 인증 교환 메카니즘은 송신자와 수신자 사이에 상대방을 인증할 수 있는 정보를 교환하는 방법으로, 패스워드와 같은 인증 정보의 사용, 암호화 기법의 이용, 그리고 송신자나 수신자의 특징이나 소유물을 이용하는 방법 등이 있다.

여섯째, 트래픽 첨가 메카니즘은 트래픽을 분석하므로써 보안을 침해하는 여러 위협으로부터 데이타를 보호하기 위하여 사용된다. 그러나 이 메카니즘은 첨가된 부분이 비밀성 서비스에 의하여 보호되어야만 효과적으로 동작할 수 있다.

일곱째, 라우팅 제어 메카니즘은 비밀 정보를 교환하기 위하여 특정 서브네트워크나 링크 또는 중계기 등을 피해서 라우팅을 하는 것을 말한다. 즉, 이 메카니즘은 보안을 침해할 수 있는 경로를 피해서 라우팅을 할 수 있는 수단을 제공한다.

마지막으로 공증 메카니즘은 제삼자(third party)를 통하여 데이타의 무결성, 근원지나 목적지, 또는 시간 등을 확인하는 방법이다. 공증인은 송신자와 수신자 모두에 의하여 신원이 확실하다고 인정되어야 하며, 여러 정보를 보증하기 위하여 필요한 정보를 보유하고 있어야 한다.

지금까지 설명한 보안 서비스와 보안 메카니즘 사이의 관계를 표 1과 같이 요약할 수 있다.

3. OSI 표준 응용 프로토콜에서의 보안

OSI 응용 계층에서는 다양한 응용 서비스들이 존재한다. 이번 장에서는 그 중에서 X.400 MHS 서비스, X.500 디렉토리 서비스, 그리고 FTAM 서비스에서의 보안 서비스 및 보안 메카니즘들에 관하여 살펴보자.

3.1 X.400 MHS 서비스에서의 보안

X.400 MHS 시스템의 주요 기능은 전자 메일 시스템을 상호 접속하는 것이다. X.400 권고안의 첫번째 버젼에서는 보안과 관련된 기능은 고려되지 않았다. 따라서 이러한 시스템들은 아무런 보안 기능이 없이 단순히 전자메일의 교환에만 사용되었다. 그러나 새로운 권고안(1988)은 많은 보안 정책들을 지원할 수 있는 여러가지 보안 서비스들을 정의하였다. 이 보안 서비스들은 표준 MHS에 부가적으로 확장되었고 많은 보안 공격이나 위협으로부터의 위험을 최소화하기 위하여 사용되어질 수 있다. 그럼에도 불구하고 기존의 MHS에 대한 확장은 진정으로 "안전한 MHS"를 지원하지는 못한다. 또한 X.400 MHS에서의 보안 서비스는 다양한 보안 메카니즘들에 의하여 제공되어질 수 있다.

X.400 시스템에서 이용가능한 OSI 표준 보안 서비스들은 아래와 같다.

- 개체 인증
- 접근 제어
- 데이타 비밀성 / 내용 비밀성
- 데이타 무결성 / 내용 무결성 / 메시지 순서 무결성
- 비 부인

위에 설명된 대부분의 서비스들은 암호화에 기반을 두고 있는 여러가지 보안 메카니즘에

의하여 지원된다. MHS 시스템에서는 암호화를 위하여 몇몇 경우 비대칭 알고리즘이 사용되는 것을 제외하고는 대칭 알고리즘 및 비대칭 알고리즘을 선택적으로 사용할 수 있다.

X.400 시스템에서 보안 기능을 구현하기 위한 보안 서비스 요소들은 X.500 디렉토리 인증환경의 지원을 받아야만 한다. 디렉토리 시스템은 MHS에서 인증을 제공하는 사용자들 사이의 신분 확인증을 교환하기 위하여 사용되는 공개키의 확인된 복사본을 저장하고 있다. 그렇게 하므로써 비밀성과 무결성을 보장해 줄 수 있는 메카니즘이 제공된다.

이러한 보안 서비스들에도 불구하고 MHS와 사용자, 또는 사용자들 사이의 통신에서 어떤 보안에 대한 공격이 있을 수 있다. 따라서 이러한 위협들을 제거하기 위하여 가까운 미래에 현재의 보안 서비스 및 보안 모델들을 확장할 필요가 있다.

X.400에 대한 보안 서비스들이 안전한 메시지 교환을 위한 수단을 제공하지만 그것들을 사용할 때, 다음과 같이 많은 한계점이 있다.

- 메시지를 완전히 보호하기 위하여 여러 개가 결합된 보안 서비스가 이용될 때는 무결성, 인증, 비밀성의 순서로 적용되어야 한다.
- 비 전달의 증명은 X.400 권고안에 언급되지 않았지만, delivery에 대한 증명은 전달에 대한 목표지점이 메시지 저장소인 경우를 제외하고는 가능하다. 메시지 저장소의 경우는 메시지를 복호화하거나 메시지가 제대로 배달되었는지 검사할 수 없다.
- 메시지 전송에 대한 증명은 메시지를 보내는 MTA가 사적인 영역에 있고 메시지가 공공 영역에 있는 MTA로 보내질 경우에는 특정 프로토콜의 제한 때문에 MHS에 의하여 제공되지 못한다.
- X.400은 트래픽 흐름 분석에 의한 공격에 대하여는 보안 기능을 제공하지 못한다.

3.2 X.500 디렉토리 서비스에서의 보안

3.2.1 X.509 인증 서비스

OSI 디렉토리에 저장된 정보를 접근하기 위하여 인증과 접근 제어의 두가지 보안 서비스가 제안되었다. X.500 권고안은 사용자들에 대한 디렉토리의 개체 인증 서비스를 제공하기 위한 구조를 정의하고 있다. 이 사용자들은 다른 응용이나 서비스뿐만 아니라 디렉토리 자체도 포함된다.

X.500 권고안은 디렉토리가 가지고 있는 인증 정보의 형태를 기술하고 있으며, 어떻게 인증정보들을 디렉토리로부터 얻을 수 있는가도 포함하고 있다. 또한, 이러한 인증 정보들이 어떻게 만들어지고 디렉토리에 저장되는가에 대하여도 언급하고 있으며, 다른 응용들이 인증을 수행하기 위하여 이 인증 정보들을 이용할 수 있는 세가지 방법을 정의하고 있다. 그리고 다른 보안 서비스들이 어떻게 인증에 의하여 지원될 수 있는가에 대하여도 기술하고 있다.

X.509는 다음과 같이 두가지 수준의 인증을 정의하고 있다.

- 단순 인증 : 신원확인을 위하여 패스워드를 이용
- 강한 인증 : 암호화 기법을 이용하여 만들어진 신원확인서를 이용

단순인증이 불법적인 접근에 대하여 단순히 몇 가지 제한된 형태의 보호만을 제공하는 반면, 강한 인증은 보안 서비스를 제공하기 위한 기반으로 사용될 수 있다. 인증과 다른 보안 서비스들은 정의된 보안 정책의 범위 내에서만 제공되어질 수 있으며, 보안 정책을 정의하는 것은 응용 서비스의 사용자들에게 달려있다.

3.2.2 X.509 접근 제어 서비스

디렉토리 사용자들은 접근 제어 정책에 따라 그들에게 부여된 접근 권한에 의해서 디렉토리 정보베이스(DIB : Directory Information Base)에 저장된 정보들에 대하여 접근할 수 있다. X.500에서는 접근 제어 보안 서비스를 각각의 보안 영역 자체의 문제로 남겨 놓았다. 그러나 이러한 보안 서비스의 구현이 접근을 제어할 수 있는 몇 가지 수단을 필요로 하고, X.500의 미래 버젼에서는 접근 제어 정보를 생성하고, 유지하고, 적용할 수 있는 표준화된 수단을 정의할 것이다.

X.500 서비스에서 접근 제어를 관리하기 위한 프로시져를 만드는데 있어서 두가지 기본 원칙은 다음과 같다.

1. 디렉토리 정보 트리(DIT)를 불법적인 변경으로부터 보호하여야 하며, 디렉토리를 불법적인 조사, 변경 등으로부터 보호할 수 있는 수단이 제공되어야 한다.
2. 특정 연산을 수행하기 위한 사용자의 권한을 결정하는데 필요한 정보는 그 연산을 수행하는데 포함된 디렉토리 서비스 대행자(DSA)들만이 이용할 수 있어야 한다.

현재 아래와 같이 다섯가지 보안이 X.500권고안에 정의되어 있다.

- 디렉토리 정보 트리의 전체 서브트리의 보호
- 하나의 엔트리의 보호
- 하나의 엔트리내의 전체 속성들의 보호
- 일부 선택된 속성 값들의 보호

3.3 FTAM 서비스에서의 보안

FTAM(File Transfer, Access, and Management) 표준의 목적은 개방 시스템의 사용자들에 의한 화일의 관리 및 전송을 촉진시키는데 있다. FTAM 권고안은 다음과 같이 세부분으로 구성되어 있다.

- 가상화일 정의
  일반적인 가상 화일 포맷은 표현 계층에 의하여 제공된다. 각 사용자들은 이 가상 화일 포맷과 화일 원래 포맷 사이의 변환을 하여야 한다.
- 화일 서비스 정의
  사용자들이 안전하게 화일을 접근할 수 있는 작업 환경을 제공해 주는 일련의 프리미티브와 파라미터들이 정의되어 있다.
- FTAM 서비스가 제공하는 화일 프로토콜의 사양서
  이것은 가상화일에서 국부화일로 화일을 변환하는데 필요한 표현 서비스의 사용을 위해서 필요하며, 세션 링크의 설정이나 원격 화일에 대한 접근을 위하여 필요한 체크포인트를 설정하기 위하여 사용된다.

3.3.1 FTAM에 대한 접근 제어 서비스

보안 정책에 관계없이 접근 제어 서비스를 다음과 같이 크게 두가지 형태로 나누어 볼 수 있다.

- 강제적 접근 제어
  (Mandatory Access Control)
  사용자와 저장된 정보에 보안 등급이 부여되고, 이 보안 등급을 기반으로 접근을 제한하게 된다.
- 자율적 접근 제어
  (Discretionary Access Control)
  권한부여가 사용자의 신원 및 요청된 정보의 형태에 의존한다.

FTAM에서는 접근 제어 서비스의 단위가 계층적으로 구성되어 있는 가상 화일의 구조에 따른다. 각각의 FADU(개별적으로 접근되는 화일 요소의 단위)는 접근 제어 서비스가 이용하는 보안 속성들과 관련이 있다.

3.3.2 FTAM에서의 신원 인증 서비스

분산화된 환경에서 몇몇 사용자들은 자신들의 보안 등급이나 신원을 속이고 자신에게 접근 권한이 없는 정보에 접근하려 할 수 있다. 이러한 것을 방지하기 위하여 FTAM에서는 수행되고 있는 연산의 보안을 보장해 줄 수 있는 보안 서비스가 필요하다. 단순히 살펴보면 이러한 서비스들은 크게 다음과 같은 두가지에 의존한다.

- 운영체제
  운영체제 수준에서 사용자가 자신의 보안등급이나 신원과 같은 접근 제어 속성들을 변경하지 못하도록 하여야 한다.
- 통신 서비스
  OSI 하위 계층들은 침입자에 의한 잘못된 접근 제어 정보가 전달되지 않도록 안전한 서비스를 제공해야 한다.

이렇게 일단 접근 제어 서비스가 사용자의 신원에 의하여 설정되면 표현계층은 이 서비스를 FTAM에게 전달한다.

4. OSI 망 관리 보안

OSI 표준안에서는 시스템 관리를 결함 관리, 구성 관리, 회계 관리, 성능 관리, 그리고 보안 관리 다섯개 기능 영역으로 나누고 있다. 이 관리 기능 영역은 그림 1과 같이 여러가지 시스템 관리 기능들의 지원을 받고, 다시 시스템 관리 기능은 OSI 표준 망 관리 서비스인 CMISE 서비스의 지원을 받아 수행된다.

이 장에서는 13개의 시스템 관리 기능 중에서 보안 관리와 밀접한 관련이 있는 보안 알람 보고 기능(security alarm reporting function), 보안 회계 검사 기능(security audit trail function), 접근 제어 기능(access control function)에 대하여 살펴보자.

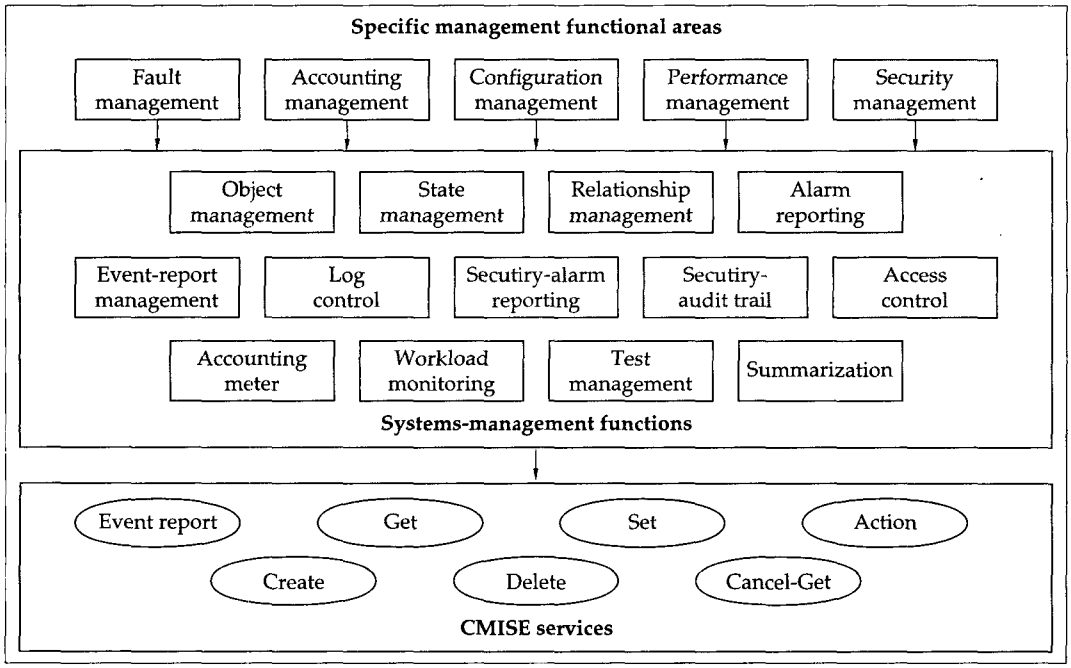


그림 1 OSI 시스템 관리

4.1 보안 알람 보고 기능

보안 알람 보고 기능은 X.736/ISO 10164-7 표준안에 정의되어 있으며 보안 서비스 및 보안 메카니즘에서 발생한 보안관련 사건이나 잘못된 동작을 보고하는 기능을 수행한다. 이 기능은 일반적인 보안 알람 통지들과 파라미터들을 기술하고 있으며, 보안 알람들을 제어하고 관리자가 지정한 곳으로 통보하기 위하여 EFD(event forwarding discriminator)를 생성, 삭제 및 수정하는 서비스를 제공한다. 즉, 이 기능은 망에 보안 위협이 있을 때 이를 관리자에게 알려주는데 목적을 두고 있다.

보안 알람은 아래와 같이 다섯 가지 형태가 지원된다.

- 무결성 파괴
  정보가 불법적으로 변경, 삽입, 삭제되는 것과 같이 정상적인 정보의 흐름을 방해하는 사건 발생을 보고
- 정상적인 동작 파괴
  서비스의 잘못된 호출이나 오동작, 사용불가 등의 이유로 인하여 요청된 서비스를 제공할 수 없음을 보고
- 물리적인 파괴
  물리적인 자원의 파괴를 보고
- 보안 서비스나 보안 메카니즘의 파괴
  보안 서비스나 보안 메카니즘에 의하여 불법적인 보안 공격을 보고
- 시간 영역 파괴 : 사건의 허용된 기간 외의 발생을 보고

4.2 보안 회계 감사 기능

X.740/ISO 10164-8에서는 보안 회계 감사 기능을 정의하고 있는데, 이 기능은 보안 메카니즘의 수행뿐만 아니라 개방 시스템의 보안을 평가하기 위하여 로그에 기록되어야 할 사건 보고들을 정의하고 있다. 보안 회계 감사 기능은 발생 당시에 찾아내지 못한 보안 공격들을 찾아내기 위하여 사용된다. 이 기능은 로그 제어 기능을 확장한 것이다.

보안 회계를 위하여 사용될 수 있는 보안 관련 사건들은 다음과 같은 것들이 있다.

- 연결 설정
- 연결 해제
- 보안 메카니즘의 이용
- 관리 연산
- 이용 감사

4.3 접근 제어 관리 기능

접근 제어 관리 기능은 X.741/ISO 10164-9 표준안에 정의되어 있으며, 관리 정보 및 연산에 대한 접근을 제어하기 위한 모델에 대하여 기술하고 있다. 여기서는 접근 제어 정책에 따라서 접근을 허용하거나 접근을 제한하는데 사용되는 관리 객체 및 속성들을 정의하고 있다.

접근제어는 관리자에 의한 관리 연산의 수행을 통제하고, 사건 발생으로 인한 통지가 권한이 없는 관리자에게 통보되는 것을 방지하며, 관리 정보가 불법적으로 노출되는 것을 방지하기 위하여 필요하다. 접근 제어를 다음과 같이 크게 세가지 형태로 나누어 행해진다.

- 관리 연결 설정에 대한 접근 제어
- 관리 연산에 대한 접근 제어
- 관리 통지에 대한 접근 제어

관리 연결 설정에 대한 접근 제어는 관리 연산을 위한 연결 설정을 할 때에 접근 제어가 이루어지는 것을 말하며, 관리 연산에 대한 접근 제어는 관리자에 의하여 정상적인 망 관리 연산이 수행될 때 이루어지는 접근 제어를 의미한다. 한편, 관리 객체로부터 발생하는 통지에 대하여도 적절한 접근 제어가 수행되어

통지가 올바른 관리자에게 보고될 수 있도록 하여야 한다.

접근 제어를 위한 메카니즘은 여러가지가 있을 수 있다. 대표적인 것으로는 접근 행렬, 접근 제어 리스트, 능력 리스트, 그리고 보안 등급에 의한 것이 있다. 어떠한 메카니즘을 사용할 것인가의 선택은 응용 영역 및 환경에 따라 달라진다.

5. 결 론

컴퓨터 네트워크의 출현은 많은 자원 및 정보의 공유를 가져왔지만, 그와 반면에 심각한 보안 문제를 야기시켰다. 기업체나 연구소 및 학교의 중요한 정보들이 불법적인 사용자들에 의해 유출되거나 변경되어 엄청난 재산상의 손해를 가져온 사건들이 자주 발생하고 있다.

보안 침해로 인한 영향은 막대하기 때문에 OSI도 보안의 필요성을 인식하고 이를 방지하기 위하여 여러가지 보안 서비스와 메카니즘들을 정의하고 있다. 보안 서비스와 메카니즘들은 OSI 각 계층에 위치하여 정보의 안전한 전송 및 네트워크의 정상적인 동작을 지원한다.

본 기사에서는 OSI/RM에서 제공하는 여러가지 보안 서비스와 보안 메카니즘들에 관하여 살펴보았다. 그리고 특히, 이들이 X.400 MHS 서비스, X,500 디렉토리 서비스, FTAM 서비스와 같은 응용 계층 서비스들의 보안을 유지하기 위하여 어떻게 이용되는가를 알아보았다. 또한 망 관리에서 보안을 유지하기 위하여 어떠한 기능들이 제공되고 있는지에 대하여도 간단히 살펴보았다. 그러나 아직도 보안에 관한 관심은 다른 분야에 비하여 미진한 실정이며, 추후로도 많은 연구가 절실히 요구되는 분야이다.

참 고 문 헌

[1] ISO/IEC 8571, "Information Processing Systems - Open System Interconnection - File Transfer, Access and Management".

[2] ISO/IEC 9594-1/CCITT X.500, "Information Technology - Open System Interconnection - The Directory - Part 1 : Overview".

[3] ISO/IEC 9594-8/CCITT X.509, "Information Technology - Open System Interconnection - The Directory - Part 8 : Authentication Framework".

[4] ISO/IEC 10021/CCITT X.400, "Information Processing - Text Communication - Message Oriented Text Interchange System".

[5] ISO/IEC 10040/CCITT X.701, "Information Technology - Open System Interconnection - System Management Overview".

[6] ISO/IEC 10164-7/CCITT X.736, "Information Technology - Open System Interconnection - Security Alarm Reporting Function".

[7] ISO/IEC 10164-8/CCITT X.740, "Information Technology - Open System Interconnection - Security Audit Trail Function".

[8] ISO/IEC 10164-9/CCITT X.741, "Information Technology - Open System Interco-nnection - Objects and Attributes for Access Control".

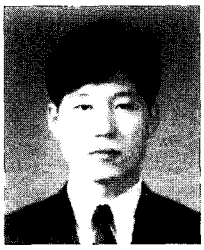
[9] CCITT X.800, "Security Architecture for Open System Interconnection for CCITT Applications".

[10] Allan Leinwand, Karen Fang, Network Management A Practical Perspective, 1993.

[11] S. Muftic, A. Patel, P. Sanders, R. Colon, J. heijnsdijk, U. Pulkkinen, Security Architecture for Open Distributed Systems, John Wiley & Sons, 1993.

[12] William Stallings, SNMP, SNMPv2 and CMIP, Addison - Wesley, 1994.

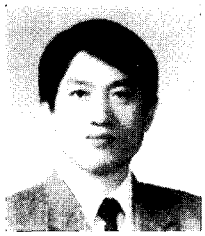
□ 著者紹介



이 창 진

1994년 전남대학교 전자계산학과 이학사
1994년 ~ 현재 전남대학교 대학원 전산통계학과 석사과정

※ 주관심분야 : 통신망 관리, 정보 보안 등



노 봉 남

1978년 전남대학교 수학교육과 이학사
1982년 한국과학기술원 전산학과 공학석사
1994년 전북대학교 대학원 전산통계학과 이학박사
1982년 ~ 현재 전남대학교 전산학과 교수

※ 주관심분야 : 객체지향 시스템, 통신망 관리, 정보 보안, 컴퓨터와 정보사회 등