通信情報保護學會誌
第2卷 第2號, 1992.3

통신정보 보호체제의 프레임워크와 모델

김 동 규*

1. 序 論

현대사회의 특징중의 하나는 다양한 환경에서 통신 사용자간에 데이타를 효율적으로 전송하는 정보통신 기술이 괄목할 수준까지 진척된 정보화사회라는 점이다. 이처럼 컴퓨터가 널리 보급되고 정보통신 기술이 발전함에 따라 지리적으로 먼거리에 있는 사람에게 정보를 주고 받을 수 있게 되었는데, 이러한 편리함과 더불어 통신 정보 내용의 불법적인 유출이나 비자격의 네트워크 액세스, 그리고 불법적인 사용자에 의한 내용과 순서의 변경등과 같은 여러가지 안전성 문제들이 대두되게 되었다.

현재 우리나라에서도 정보화사회 진입을 위해 컴퓨터 시스템이 사회의 넓은 분야에 보급되고 있으며 정보화 사회 확립을 위해 5대 기간 전산망을 국책과제로 구축하고 있다.

이러한 전산망 구축과 컴퓨터 시스템의 보급확대와 더불어 정보의 유통 활성화에 따른 편리성, 효율성 제고라는 긍정적 측면을 극대화 시키기 위해서도 필연적으로 뒤따르는 컴퓨터 범죄, 프라이버시 침해, 컴퓨터 바이러스 등의 부정적 효과를 최소화 시킬 수 있도록 컴퓨터/네트워크 시스템의 안전성 및 신뢰성을 확보하여야 한다.

따라서 본 考에서는 이러한 안전성 문제들을 해결하기 위한 기반 연구의 일환으로써 통신 정보 보호체제의 안전성 프레임워크에 대하여 기술하고, 또한 이러한 안전성 프레임워크 개념을 상위 계층에 적용한 안전성 모델의 하나인 SCSE에 대해 알아보고자 한다.

2. 개방 시스템 안전성 프레임워크(Open Systems Security Framework)

안전성 프레임워크는 시스템과 시스템의 객체(Object)를 보호하는 방법의 정의와 시스템간의 상호작용(Interaction)에 관련되며, 시스템과 메카니즘을 구축하기 위한 방법론은 관심범위에서 제외시킨다. 즉, 특정한 안전성 서비스를 제공하기 위한 데이타 요소(Data Element)와 동작의 순서(Sequence of Operation)를 다룬다. 안전성 서비스는 시스템간에 교환되는 데이타, 시스템에 의해 관리되는 데이타, 그리고 시스템내의 통신하는 실체(Entity)에 적용될 수 있다.

신분확인(Authentication), 액세스 제어(Access Control), 무결성(Integrity)등 안전성 문제와 관련된 특정한 기능적 영역들은 포괄적이고 일관된 기술이 필요하다. 안전성 프레임워크(Security Framework)는 이러한 필요성을 만족시키기 위하여 연

* 亞洲大學校 電算學科 敎授.

구되는 분야이다. 따라서 안전성 프레임워크는 특정한 개방 시스템 구조(Open System Architecture)의 컨텍스트(Contexts)에 각 영역의 기능들이 어떻게 적용될 수 있는가를 다루며 개방시스템의 안전성에 대하여 통일된 관점 제공을 목적으로 개발되고 있다. 여기에서 개방 시스템은 데이타 베이스(Database), 분산응용(Distributed Application), ODP(Open Distibuted Process), 그리고 OSI(Open Systems Interconnection)등을 포함한다.

가. 신분확인 프레임워크

1) 기본 개념

신분확인 프레임워크에서는 두 레벨(level)의 신분확인을 기술한다. Simple 신분확인은 패스워드(password)에 기반을 두어 인증되지 않은 액세스에 대하여 제한된 보호(Protection)를 제공하는 반면 Strong 신분확인은 암호기술(Cryptographic Check Techniques)에 그 기반을 두어 안전성 서비스를 제공하는 기본으로 사용되어지고 공개키 암호화 시스템을 이용한다. 본 프레임워크에서는 일반적으로 특별한 암호화 알고리즘의 사용에 의존하지 않고 있으며, 실제로는 많은 다른 알고리즘들이 사용될 수 있을 것이다. 그러나, 신분확인을 원하는 두 사용자는 같은 알고리즘을 사용해야 한다[2].

2) 메카니즘

Simple 신분확인은 평문(Plain-text)인 이름(Name)과 패스워드를 이용한 신분확인 방법으로 제한된 보호를 제공한다. Strong 신분확인은 one-way 신분확인, mutual(two-way) 신분확인, 그리고 three-way handshake에 의한 mutual신분확인이 있다. One-way 신분확인은 한 실체의 신분만을 확인하며, mutual 신분확인은 두 실체 모두의 신분을 확인한다. Two-way 신분확인과 three-way 신분확인의 차이는 three-way 신분확인은 물리적 혹은 논리적으로 동기된 클럭(clock)을 필요로 하지 않는다는 점이다.

나. 액세스 제어 프레임워크

액세스 제어의 주된 목적은 컴퓨터 혹은 통신 시스템의 요소(Element)를 포함하는 인증되지 않은 Operation을 막기 위함이다. 아래 그림 1은 이러한 액세스 제어 서비스를 제공하기 위한 추상적인 방법을 나타낸다. 액세스 제어에 관련되는 기본적인 Function은 액세스 요청을 수행하는 AEF(Access Control Enforcement Function)와 액세스에 대한 타당성을 검사하는 ADF(Access Control Decision Function)이다. AEF는 ADF가 요청한 액세스의 타당성을 검사할 수 있도록 액세스 제어 정보(Access Control Information)를 제공한다. 또한 액세스 제어 정보를 정확하게 해석하기 위한 구문정보(Contextual Information)가 필요하다[3].

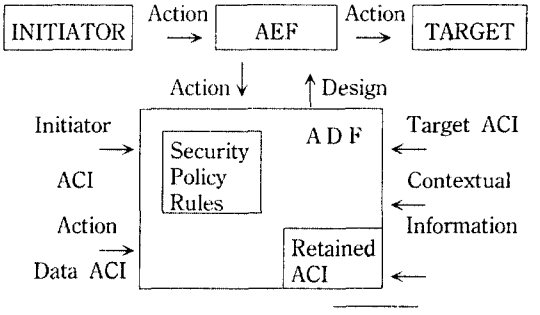


그림 1. 액세스 제어 프레임워크

다. 부인봉쇄 프레임워크

1) 기본개념

부인봉쇄 서비스는 데이타의 송신 혹은 수신 사실을 증명할 수 있는 정보를 수집하고 관리한다. 송신자의 송신 사실 부인으로부터 수신자를 보호하는 송신 부인봉쇄 서비스(Non-repudiation with proof of origin)와 수신자의 수신 사실 부인으로부터 송신자를 보호하는 수신 부인봉쇄 서비스(Non-repudiation with proof of delivery)가 있다. 부인봉쇄 서비스는 실체(Entity)간에 전송되는 데이타의 어떤 성질(예: 무결성, 송신자, 시간, 수신자)에 대한 증거를 제시함으로서 얻어지며, 디지탈 서명, 암호

화, 데이타 무결성, 공증 메카니즘 그리고 다른 시스템 서비스의 사용을 통하여 제공될 수 있다. 이러한 메카니즘과 시스템 서비스들의 사용여부는 응용(Application)의 요구사항(Requirements)에 의존한다[4].

2) 메카니즘

메카니즘은 크게 공증과 Cryptographic checkvalue를 이용하는 것으로 구분하여 살펴볼 수 있다. 공증 메카니즘은 실체간에 통신되는 데이타의 성질(무결성, 송신자, 시간, 수신자)에 대한 보증을 제공하는 메카니즘이다. 공증인(Notary)은 디지탈 서명, 암호화, 데이타 무결성 메카니즘을 필요에 따라 제공할 수 있는 능력을 지니고 있다. Cryptographic checkvalue는 데이타에 추가되는 데이타에 대한 어떤 함수의 결과를 의미한다. 이것은 무결성 서비스 제공에 적합하며 디지탈 서명은 Cryptographic checkvalue의 한 예이다.

라. 비밀성 프레임워크

1) 기본 개념

많은 응용들은 정보의 비밀에 의존하는 안전 요구사항(Security Requirement)이 있다. 신분확인, 액세스 제어, 혹은 무결성 등과 같은 안전성 서비스 제공시, 만일 공격자에게 알려지는 경우 안전성 서비스의 효율을 감소시키거나 무효화시킬 수 있는 정보는 보호될 필요가 있다. 이러한 정보의 비밀을 유지하는 것을 비밀성이라 한다. 비밀성 서비스는 데이타를 비밀성이 보호된 데이타(Confidentiality Protected Data)로 바꾸는 Hide과정과 이 과정의 반대인 Reveal과정으로 이루어진다. 공격(Attack)은 시스템의 상태를 변화시키는 능동적 공격(Active Attack)과 상태를 변화시키지 않는 수동적 공격(Passive Attack)이 있다. 비밀성 보호 시스템(Confidentiality Protected System)의 형태는 공격자가 다큐멘트된 메카니즘을 악용하지 않는 공격으로부터 보호하는 시스템, 외부에서의 공격으로부터 보호하는 시스템 그리고 외부공격과 내부공격으로부터 보호하는 시스템으로 구별될 수 있다[6].

2) 메카니즘

비밀성 메카니즘은 액세스 제어와 Mapping기술을 사용할 수 있으며 Mapping기술은 암호화, 데이타 패딩(Padding), Spread Spectrum, 경로 제어(Routing Control)를 포함한다. 비밀성에 대한 위반을 행하는 공격자가 액세스 제어를 받아야 하는 경우 액세스 제어 메카니즘을 이용할 수 있으며 암호화 메카니즘은 한 데이타 단위(Data Unit) 혹은 데이타의 흐름을 보호하기 위하여 사용된다. Spread Spectrum은 데이타가 많은 가능한 채널중에서 한 채널에만 존재하며 공격자가 한정된 시간내에 데이타가 있는 채널을 발견할 수 없는 경우에 사용될 수 있다. 경로 제어는 안전성 요구사항을 만족하는 네트워크로 경로를 선택함으로서 비밀성 서비스를 제공할 수 있으며 데이타 패딩은 필요없는 허위의 데이타를 전송하여 공격자가 원래의 데이타와 구별할 수 없도록 하는 서비스를 제공한다. 비밀성 서비스는 요구사항에 따라 이러한 메카니즘을 적절히 조합하여 이루어질 수 있다.

마. 무결성 프레임워크

1) 기본 개념

많은 응용들은 정보의 무결성에 의존하는 안전 요구사항(Security Requirement)이 있다. 신분확인, 액세스 제어, 비밀성, 부인봉쇄 등과 같은 안전성 서비스 제공시, 만일 공격자가 정보를 수정한다면 안전성 서비스의 효율을 감소시키거나 무효화시킬 수 있는 정보는 보호될 필요가 있다. 무결성 서비스는 데이타로부터 무결성 보호 데이타(Integrity Protected Data)를 생성하는 Shield과정과 무결성 보호 데이타로부터 무결성을 체크(Check)하는 Unshield 과정으로 이루어진다[5].

무결성 서비스는 만일 데이타에 Unshield과정을 수행할 때 공격사실이 발견된다면 원래의 데이타를 복원할 수 없고 단지 (Error)를 알리는 Integrity without recovery와 데이타에 Unshield과정을 수행할 때 공격사실이 발견되면 원래의 데이타를 복원하여 공격사실을 알리는 Integrity with recovery의 두가지형태로 나눌 수 있다.

2) 메카니즘

무결성 메카니즘의 형태는 액세스 제어와 Time Stamp, Checksum 또는 Cryptographic checkvalue를 데이타에 붙이는 두가지 형태로 구분될 수 있다. 액세스 제어를 이용한 무결성 서비스는 인증되지 않은 사용자로부터 고의적인 데이타 수정을 방지하며, 이 경우 무결성에 대한 위반(Violation)은 액세스 제어하에 있어야 한다. Checksum은 사고에 대한 데이타의 수정을 방지하며 Time Stamp는 재전송(Replay) 공격을 막기 위한 방법이다. 사고에 의한 데이타의 수정과 고의적인 데이타의 수정을 막기 위하여 암호화 즉, Cryptographic checkvalue를 사용할 수 있다. 무결성 서비스는 필요에 따라 이러한 메카니즘을 적절히 조합하여 제공될 수 있다.

3. 개방시스템 안전성 모델 (Open Systems Security Model)

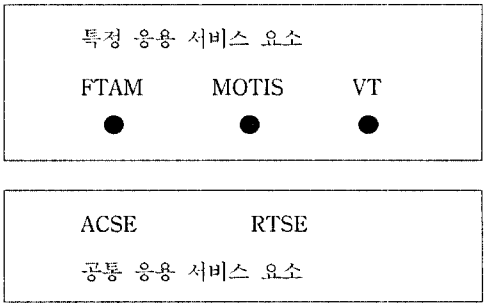
OSI모델의 목적은 OSI안전성 구조와 안전성 프레임워크의 개념을 OSIBRM(OSI Basic Reference Model)의 상위 계층과 하위 계층에 적용하는 것이다.

본 考에서는 응용계층에서 서비스를 제공하는 SCSE(Secure Communication Service Element)를 설명하고자 한다.

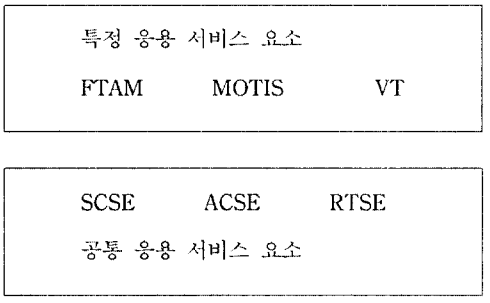
가. SCSE의 개념

SCSE 모델의 구조는 SASE(Specific ASE), 예를 들면 FTAM(File Transfer Access and Management), VT(Virtual Terminal), MOTIS(Message Oriented Text Interchange System)등에서 요구하는 안전성 서비스들이 현재 OSI Security Architecture에서 제안된 2~3개의 일반적인 안전성서비스로 제한되어 있으며, 이들이 각각의 SASE마다 구현되어 있음으로 인해서 생기는 중복성을 제거하자는 것이다[8].

SCSE모델에서는 응용계층의 SASE에서 공통적으로 요구되는 안전성 서비스를 하나의 SCSE로 묶어서 수행하는데, 이것을 도식적으로 표시하면 그림 2와 같다.



(a) 각 특정 응용 서비스 요소에서 안전성 기능을 제공



(b) 공통 응용 서비스 요소에서 안전성 기능을 제공

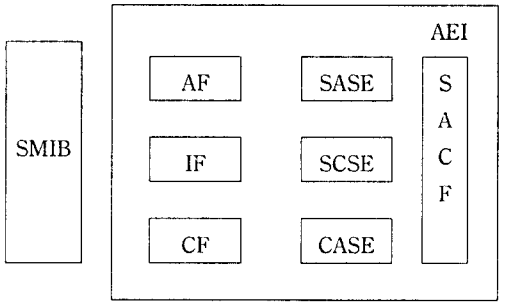
⊙ ● : Security Function
⊙ FTAM : File Transfer Access and Management
⊙ MOTIS : Message Oriented Text Interchange System
⊙ VT : Virtual Terminal
⊙ ACSE : Association Control Service Element
⊙ RTSE : Reliable Transfer Service Element

그림 2. 응용 계층에서 안전성 기능의 할당

나. SCSE의 구성

SCSE의 내부구조는 그림 3과 같이 안전성 기능을 제공하는 Facility와 비밀 정보를 저장하는 데이타베이스인 SMIB(Secure Management Information

Base)등으로 구성된다. 그림 3은 AEI(Application Entity Invocation)와 SMIB(Secure Management Information Base)로 구성된 SCSE모델을 보여주고 있으며, 이와 같은 SCSE의 응용 계층에서의 구조적인 위치는 CASE와 SASE의 중간계층에 위치하게 된다.



► SMIB: Secure Management Information Base
► AF : Authentication Facility
► IF : Integrity Facility
► CF : Confidentiality Facility
► SASE : Specific Application Service Element
► SCSE : Secure Communication Service Element
► CASE : Common Application Service Element
► SACF : Single Association Control Function
► AEI : Application Entity Invocation

그림 3. SCSE 모델

SCSE 모델에서는 공통적으로 요구되는 안전성 서비스를 제공하기 위하여 신분확인 서비스를 위한 AF(Authentication Facility), 데이타 무결성 서비스를 위한 IF(Integrity Facility)』 그리고 데이타 비밀성 서비스를 위한 CF(Confidentiality Facility)와 같이 3가지로 나누었다.

► AF(Authentication Facility) : 연결지향 통신에서 통신 관련자의 신분을 확인하고 해당 통신에 참여할 자격 유무를 검사하는 Facility이다. 대등실체(Peer Entity)의 신뢰성 있는 연결의 확립 또는 데이타 전송의 과정에서 수행되는 대등실체 신분확인 서비스(Peer Entity Authentication Service)를 제공해주는 Facility로서 Identification Check 또는 암호화 Function 등을 수행한다.

► IF(Integrity Facility) : 전송되는 데이타의 무결성을 점검하는 무결성 서비스를 제공하는 Facility로서 MAC(Message Authentication Code)를 이용하여 무결성을 Check하고 데이타의 순서를 Check한다. 무결성(Integrity)은 내용의 무결성을 점검하는 내용 무결성(Content Integrity)과 전송되는 전문의 순서를 점검하는 순서 무결성(Sequence Integrity)으로 나누어 진다.

► CF(Confidentiality Facility) : 통신되는 데이타가 불법적으로 내용이 노출되는 것을 방지하는 데이타 비밀성 서비스를 제공하는 Facility로서 암호화 메카니즘을 사용하여 전송되는 데이타의 내용을 감출 수 있다.

SCSE 모델에서도 ECMA와 ISO/IEC JTC1/SC21/WG6에서 제안한 안전성을 논리적으로 완전하게 분해한 기능적인 요소, 즉 안전성 서비스의 최소단위인 Facility의 개념을 사용하고 있으며, 이 Facility들이 서로 결합하여 하나의 응용 서비스 요소를 구성하게 된다.

다. SMIB(Secure Management Information Base)의 구성

그림 3에서 보는 바와 같이 SCSE의 3가지 Facility들은 각각 해당되는 서비스를 위한 암호화 알고리즘, 암호화 동작 모드, 암호화 키, 초기 벡터(Initialization Vector)등의 정보를 유지하기 위하여 국지(Local)의 SMIB를 사용하게 된다. SMIB에 저장된 정보들은 Context 단위로 처리되는데 이를 PRC(Protection Context)라 하며 각각의 PRC ID에 의하여 구분된다. 이러한 정보들은 각 호스트에 있는 국지의 SMIB에 동일하게 저장되어야 하므로 OSI 보안 관리(Security Management) 프로토콜 등에

의하여 관리되어야 한다.

4. 結 論

현재까지의 안전성에 관한 관련 연구는 ISO(International Organization of Standardization), CCITT(International Telephone and Telegraph Consultative Committee), ECMA(European Computer Manufacturers Association)등의 국제 표준화 기관을 중심으로 활발한 연구가 진행되고 있다. 이러한 노력의 결과로 ISO/IEC JTC1/SC21에서는 OSI(Open System Interconnection)환경에서 안전성을 위한 표준 참조모형인 OSI Security Architecture를 발표하였다. OSI Security Architecture는 비록 추상적인 개념이지만 통신 정보 보호 체제의 표준으로서 받아들여지고 있다. OSI Security Architecture에서는 대부분의 안전성 서비스를 OSI 응용계층, 프리젠테이션 계층, 트랜스포트 계층에 위치시키고 있다. 또한 하위계층의 안전성 모델로서 NIST의 SP3와 SP4, 그리고 LAN의 안전성을 위한 IEEE의 SILS등이 발표되었다.

본론에서는 개방시스템 안전성 프레임워크로서 제안된 신분확인 프레임워크, 액세스 제어 프레임워크, 부인봉쇄 프레임워크, 비밀성 프레임워크, 무결성 프레임워크의 기본개념과 각각의 메카니즘에 대하여 간단히 기술했고 그러한 프레임워크를 기반으로 하여 하나의 응용 서비스로서 OSI 응용계층에 위치한 개방시스템 안전성 모델인 SCSE의 기본개념과 구성 그리고 SMIB의 구성에 대하여 살펴보았다.

안전성에 관련된 국제 표준화 기관이나 기구에서의 활발한 표준화 작업에 따라 한국에서도 이에 관련된 기술과 표준화 양면에서의 연구와 실용화 작업이 조직적으로 진척되어야 할 필요에 직면해 있다. 특히 위에서 언급한 개발시스템 안전성 프레임워크와 안전성 모델에 대한 깊은 이해, 그리고 통신환경에서의 구현방안등이 주요 연구과제임을 직시하고 이에 필요한 기술과 능력을 배양할 필요가 있다.

참 고 문 헌

1. "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture", ISO 7498-2, 1988.

2. "Information Processing Systems - Open Systems Interconnection - Security Framework for Open Systems - Part 2 : Authentication"

3. "Information Processing Systems - Open Systems Interconnection - Security Framework for Open Systems - Part 3 : Access Control"

4. "Information Processing Systems - Open Systems Interconnection - Security Framework for Open Systems - Part 4 : Non-repudiation"

5. "Information Processing Systems - Open Systems Interconnection - Security Framework for Open Systems - Part 5 : Integrity"

6. "Information Processing Systems - Open Systems Interconnection - Security Framework for Open Systems - Part 6 : Confidentiality"

7. "Information Technology Security Evaluation Criteria, version 1", May 1990.

8. Nakao, K. and Suzuki, 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, May 1989.

9. "Security Framework for the Application Layer of Open System", ECMA/TC32/87/282, Dec. 1987.

10. "OSI 통신망 구조에서의 네트워크 안전체제 연구", 과학기술처 최종보고서(3차년도), 아주대, 1991.

11. 김용근, "OSI 응용계층에서 안전한 통신을 위한 서비스 요소의 설계와 구현", 석사학위 논문, 아주대, 1990.

12. 김영호, "OSI 환경하에서 액세스 제어 서비스의 설계와 구현", 석사학위 논문, 아주대, 1991.2.

□ 著者紹介

김 동 규

1947年生
서울 大學校 工科大學 卒業(學士)
서울 大學校 自然科學大學院 卒業(碩士)
美國 KANSAS 州立大 大學院 卒業(Ph.D. 電算學, 情報通信 專攻)
美國 KANSAS 州立大 電算學科 教授
現在 亞洲大學校 電算學科 教授
저서: 데이타 통신 시스템, 회중당, 1986년
컴퓨터 통신 네트워크, 상조사, 1988년
研究 關心 分野: 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링, 정보통신 Security, 분산처리시스템