通信情報保護學會論文誌
第 7 卷 第 4 號. 1997. 12

보안 서비스를 제공하기 위한 지능망개념모델의 확장

김 영 화*, 조 세 형*, 류 재 철**

An Expansion of the Intelligent Network Conceptual Model for Providing Security Services

Young-Hwa Kim, Se-Hyeong Cho, Jae-Cheol Ryou

요 약

충분한 보안 메카니즘과 보안 통신 능력이 없는 지능망에서는 우연이든 고의적이든 민감한 정보에 대한 적법하지 못한 노출이나 변경이 가능성이 더 높게 존재한다. 암호화 및 복호화 알고리즘과 같은 보안 메카니즘이 존재한다는 가정하에서, 이 논문은 현재의 지능망에 보안 통신 능력을 추가하기 위한 포괄적인 프레임웍을 제안한다. 이를 위해, 서비스평면(SvP: Service Plane), 총괄기능평면(GFP: Global Functional Plane), 분산기능평면(DFP: Distributed Functional Plane) 및 물리평면(PhP: Physical Plane)으로 구성되는 현재의 지능망개념모델(INCM: Intelligent Network Conceptual Model)을 기본으로, INCM의 각 평면에서 추가되어야 할 보안 통신 능력을 제시한다.

Abstract

There are higher possibilities of outlawed exposure and modification against sensitive information accidentally or intentionally if Intelligent Networks do not include sufficient security mechanisms and security communication capabilities. This paper proposes generic frameworks for adding security communication capabilities to the current Intelligent Networks under the assumption that there are security mechanisms such as encryption and decryption algorithms. On the basis of the current Intelligent Network Conceptual Model (INCM: Intelligent Network Conceptual Model) consisting of four Planes of the Service Plane(SvP), the Global Functional Plane(GFP), the Distributed Functional Plane(DFP), and the Physical Plane(PhP), this paper presents security communication capabilities to be added in each plane of INCM.

* 지능망서비스연구실장(ETRI)
* * 충남대 컴퓨터과학과 교수

1. 서 론

엄밀한 의미로 지능망에서 보안 능력이 전혀 존재하지 않는다고 단정할 수 없다. 신용통화 서비스에서 서비스가입자번호와 비밀번호간의 관계를 검사하거나 또는 가상사설망 서비스에서 허가번호를 이용하여 접근제어를 수행하는 것이 그 예이다. 그러나, 현재의 지능망이 보안 능력이 너무 취약하다는 것은 표준화의 상황이나 다수의 문헌들을 통해 주지되고 있는 사실이다.

지능망과 보안은 각각의 자신들만의 영역에서 진화 단계를 거치고 있으나, 이들은 이제 초기 단계를 지나 자신들의 방법론이나 기술들을 다른 분야에 까지 응용하고자 다양한 노력을 기울이고 있는 상황이 전개되고 있다. 예를 들면, 보안의 경우 현재 거의 모든 통신 시스템의 설계 및 제작에 있어서 중요한 요구사항으로 자리잡고 있다. 그리고 지능망의 경우, 공통선 신호방식 기반의 분산환경에서 서비스 로직을 수행하는 과정은 대부분의 통신망 환경을 구축하는데 중요한 방법론을 제공한다.

일반적으로 지능망에서는 서비스가입자번호와 비밀번호간의 일치성을 검사하여 호·연결의 접속 여부를 결정하는 가장 단순한 인증 방식을 적용한다. 이는 추측을 통해 시도·실패의 반복으로 비밀번호가 노출될 수 있으며, 부당한 이용자가 서비스가입자번호만을 확인한 후 틀린 비밀번호를 입력함으로써 정당한 이용자의 서비스 요청을 차단시킬 수 있다.

또한, 지능망은 분산 환경을 기반으로 운용되기 때문에 서비스가입자의 프로파일이나 개인 신상(위치 등)에 관련된 중요한 정보가 다수의 통신 채널 및 시스템을 통해 전달된다. 따라서, 보안 메카니즘 능력이나 보안 통신 능력이 충분히 고려되지 않은 상황에서는 정보 전달 과정 중 우연이든 고의든 정보의 노출이나 변경의 가능성은 더 높아진다.

이러한 배경하에, 서비스평면(SvP: Service Plane), 총괄기능평면(GFP: Global Functional Plane), 분산기능평면(DFP: Distributed Functional Plane) 및 물리평면(PhP: Physical Plane) 등 네개의 평면으로 구성되는 지능망개념모델(INCM: Intelligent Network Conceptual Model)을 기본으로 인증, 접근제어, 비밀성, 무결성 및 부인봉쇄 등과 같은 정통 보안 분야의 기술과 OSI(Open System Interconnection) 상위계층 분야의 보안 프레임웍을 적용하여 각 평면에서 요구되는 보안 통신 능력들을 분석·정의한다.

본 논문의 제2장에서는 지능망을 위한 보안 요구사항을 기술하며, 제3장에서는 지능망에서 보안 서비스를 제공하기 위해 INCM을 구성하는 각 평면에 대한 확장 요소들을 정의한다. 제4장에서는 지능망 응용 프로토콜에서 현재의 지능망 응용계층과는 다른 응용계층 구조와 보안통신 응용서비스요소(SC-ASE: Secuity Communication-Application Service Element)를 제안하며, 제5장에서는 확장된 INCM에 따라 보안 서비스를 응용할 수 있는 가상 서비스 시나리오를 선정하고 진행 과정을 분석한다. 최종적으로 제6장에서는 본 논문에 대한 결론 및 향후 연구사항을 기술한다.

2. 지능망 보안 요구사항

1993년 초, ITU-T(International Telecommunication Union-Telecommunication) SG(Study Group) 11의 WP(Working Party) 4에서 지능망 서비스를 이용하거나 제공할 때 요구되는 접근 및 정보 보안의 방법 및 절차를 권고하기 위해 Q.29/11연구항목이 "정보 보안"이라는 이름하에 다음과 같은 이유로 출현하였다[13].

- 많은 통신 서비스들은 종단 이용자가 통신망에 접근할 때 종단 이용자나 서비스제공자의 신원을 검사하기 위해 다양한 방법이나 절차들을 필요로 한다. 이를 위해 다양한 서비스들에게 폭넓게 지원될 수 있는 공통성, 그리고 서로 다른 접근 형태(예: 유선 및 무선)간 사용할 때의 편의성 및 전이성이 중요한 요소이다.
- 접근 방식에 있어서 보편성을 제공하는 종합개인통신(UPT: Universal Personal Telecommunications)과 같은 서비스들은 지구촌에서 지역 경계가 없이 이루어지는 서비스를 목표로 하기 때문에 부정한 사용을 야기할 수 있고 실시간 이용에 대한 감시 또한 어려워진다.
- 서비스 관리 측면에서 통신망에서 유지하고 있는 민감성 정보에 대한 접근 권한, 무결성 등과 같은 보안을 요구한다.
- 지능망이 보편화됨에 따라 인터페이스 상에서 망운용자, 서비스제공자 및 종단 이용자들간 비밀성 정보(예: 비밀번호, 개인 위치 정보)의 교환이 불가피하며, 이는 결국 통신망의 보안 및 데이터의 무결성에 심각한 위험 요인으로 작용할 수 있다.

이러한 상황하에서 Q.29/11에서는 어떤 분야의 보안 관련 권고안을 완성할 것인가에 초점이 모아졌으며, 첫단계의 작업 계획으로써 불법 이용자에 대한 접근 보안(이하 Issue 1로 칭함)과, 시스템 인터페이스 또는 저장된 데이터에 대한 망보안(이하 Issue 2로 칭함)으로 분리하여 표준화를 진행하기로 하였다.

Issue 1의 경우, UPT(Universal Personal Telecommunications) 및 이동 서비스 등과 같은 특정 서비스에 대해서는 이미 광범위하게 연구를 진행하고 있으며, 스마트 카드의 이용이나 통신망에서 인증센터의 도입 등으로 이들 서비스에 대해 실제 해결 방안이 적용되고 있다. 그러나, Issue 2에 대해서는 현재 두드러진 진전이 없는 상태이다. 이는 지금까지 보고된 불법 사용이 주로 액세스 인터페이스를 공격 대상으로 삼았기 때문이다. 그러나, 분산형 및 개방형 통신망 구조로 진행되는 현재의 통신망 진화 경향은 Issue 2에 대한 불비를 추궁하는 위험 요소에 미리 준비해야 하는 상황이다.

추가적으로, '97년 2월 스위스 제네바에서 개최된 가장 최근의 SG 11 회의에서 이전의 Q.29/11의 "정보 보안"이라는 연구항목이 Q.3/11의 "보안을 위한 신호방식 요구사항"으로 변경되었으며, 지능망, 광대역 통신망 또는 UPT 등 다양한 도메인의 상위계층에서 공통적으로 이용할 수 있는 보안 관련 프로토콜을 권고하기 위해 기고서를 요청하고 있다.

지능망을 기반으로 한 보안 서비스를 제공하기 위해 지능망 및 보안에 관한 전반적인 기술과 ITU-T의 보안 관련 표준화 동향 등의 내용을 근거로 다음과 같은 요구사항들을 적용하여 본 논문을 전개해 나간다.

- 모든 인터페이스 상에서 적용되는 보안 메카니즘은 필수형이 아닌 선택형을 우선으로 적용한다.
- 지능망에서 보안 서비스를 제공하기 위해 이미 표준화 된 메카니즘을 적용해야 하며, 새로운 메카니즘을 고안하지 않는다. 지능망의 영역은 메카니즘의 창출이 아니라 메카니즘의 응용에 있기 때문이다.
- 암호방식의 선정에 있어서 융통성이 있어야 한다. 암호방식은 시간이 지남에 따라 해독될 수 있으며, 응용이나 용도에 따라 서로 다른 암호방식을 이용할 수 있기 때문이다.
- 보안 서비스를 제공하기 위해 No.7 프로토콜을 보완해야 하는 경우, 신호연결제어부

(Signalling Connection Control Part) 이하의 계층에는 보안 서비스를 제공하지 않도록 하며, TCAP를 포함한 응용계층에서만 프로토콜을 보완하거나 확장하도록 한다.

- 디렉토리 시스템을 이용하여 인증 절차를 수행해야 하는 경우, X.509(디렉토리 인증체계) 권고안의 규정을 기본적으로 지원해야 하며, 지능망으로 정합하기 위해 상황에 따라 관련 기능을 선택적으로 수용할 수 있도록 한다.
- 보안 서비스를 제공하거나 보안 관련 정보를 전달하기 위한 프로토콜은 지능망응용 프로토콜(INAP: Intelligent Network Application Protocol)을 기반으로 한다.
- 기존의 지능망 인터페이스와 접속될 수 있는 역호환성을 지켜야 한다.
- 암호화와 같은 보안 메카니즘은 응용 프로세스 및 응용 프로토콜 중 응용 프로세스 수준에서 수행 · 관리한다. 암호 알고리즘, 동작 모드, 키, 그리고 초기화 벡터 등과 같은 보호 문맥을 저장하고 운용하는 보안 메카니즘에 대한 수행 · 관리 모듈은 프로토콜 구조의 특성상 계층 관리 기능에 속한다. 현재로서는 지능망의 응용계층 수준에서 계층 관리 기능은 존재하지 않는다.

3. INCM 확장

지능망에서는 INCM이라는 도구를 이용하여 단계적으로 서비스 및 서비스특징, 기능 능력 그리고 프로토콜을 정의하고 있다. 보안 서비스를 위한 INCM을 확장하기 위해 SvP에서는 보안에 관한 서비스 정의 혹은 서비스특징 정의를, GFP에서는 보안에 관한 망능력인 SIB(Service Independent building Block)를, DFP에서는 보안에 관한 정보흐름을, 그리고 PhP에서는 물리적 구성요소를 확인하고 보안 관련 프로토콜을 포함해야 한다. INCM의 확장 과정은 상하향 방식, 하상향 방식 그리고 혼용 방식 등 세가지 방식을 적용할 수 있다. 본 논문에서는 모든 평면을 단계별로 상세히 정의하지 않고 이 평면에서 저 평면으로 그리고 그 역과정으로 자유로이 옮기면서 최종적으로 모든 평면을 정의하는 혼용 방식을 적용한다.

3.1 SvP

IN CS-1(Intelligent Network Capabilities Set-1)에서 서비스를 "하나 또는 그 이상의 필수적인 서비스특징과 선택적인 서비스특징으로 구성되며, 그 자체로서 상용으로 제공 가능한 무형의 정보 통신 기능"으로 정의한다. 그리고 서비스특징은 "다른 서비스 또는 서비스 특징과 연계하여 사용될 수 있는 서비스의 한 특성으로, 상용으로 제공 가능한 무형의 정보 통신 기능의 한 부분"으로 정의한다[16].

IN CS-2(Intelligent Network Capabilities Set-2)에서는 IN CS-1의 서비스를 통신 서비스(telecommunication services)로 규정하고, 망운용자 및 서비스제공자가 수행하는 활동, 예를 들면, 가입 및 해제, 감시(monitoring), 유지보수(maintenance) 및 요금청구(billing) 등을 지원하기 위한 관리 기능을 서비스 관리 서비스로 규정하고 있다. 그리고 종단 이용자에게 다가가는 서비스를 기술하거나 검증하는 등의 망운용자 및 서비스제공자가 수행하는 활동을 지원하기 위한 생성 기능을 서비스 생성 서비스로 규정하고 있다. 결국, 서비스의 정의가 진화 단계를 거치면서 포괄적인 형태로 바뀌고 있음을 알 수 있다[21].

IN CS-1R(Intelligent Network Capabilities Set-1 Refinement)의 "인증(authentication)"

또는 "권한부여(authorization)"와 같은 서비스 특징과 현재로서는 전혀 고려되지 않은 보안 서비스들인 무결성, 비밀성 및 부인봉쇄를 포함하여 지능망 관점에서의 서비스로 추상화하여 접근할 수 있다. SvP에서 또다른 형태로 보안 서비스를 정의할 수 있는 방법으로써, 본 본문에서 적용한 방식이다. 즉, 지능망의 서비스 수준이 아닌 서비스특징 수준에서 다음과 같이 보안 서비스를 정의하는 것이다.

"보안 서비스특징은 암호화 및 전자서명 등과 같은 메카니즘들을 이용하여 정보보호를 목적으로 통신 서비스, 서비스 관리 서비스 및 서비스 생성 서비스를 보조하여 해당 실체에게 정보보호의 수단을 제공한다."

3.2 GFP

SvP에서 확정된 서비스특징(들)을 지원하기 위해 요구되는 망능력은 GFP에서 정의된다. 보안 서비스특징을 지원하기 위한 SIB를 정의하기 위해 기존의 SIB를 확장하거나 새로운 SIB를 정의할 때 이용할 수 있는 절차로 ITU-T에서 권고한 절차를 그대로 적용한다[17].

SIB에 대한 그래픽 표현은 IN CS-1 표기법과 IN CS-2 표기법이 서로 다르다. IN CS-1 표기법에서는 특정 서비스로직을 SIB 집합으로 구성하나, IN CS-2 경우는 서비스로직의 병렬 수행까지를 고려하였으며, 하나의 SIB에 대한 표현과 그 SIB내의 오퍼레이션에 대한 표현을 분리하고 특정 서비스로직을 오퍼레이션의 집합으로 구성하여 더욱 상세히 그 서비스로직을 정의한다. 본 논문에서는 지능망 환경에서 보안 서비스를 비교적 용이하게 접근하기 위해서 IN CS-1표기법을 이용한다.

본 논문에서는 통상의 보안 서비스를 지능망의 서비스특징 수준으로 SIB를 결정하기 위해 인증 관련 SIB는 "AUTHENTICATE", 무결성 관련 SIB는 "INTEGRATE", 비밀성 관련 SIB는 "SECRETE", 접근제어 관련 SIB는 "CONTROL ACCESS", 그리고 부인봉쇄 관련 SIB는 "NON-REPUDIATION"와 같은 다섯개의 SIB를 정의한다. 이들 SIB들 중 "AUTHENTICATE" SIB는 기존의 SIB를 확장한 것이며, 나머지 네개의 SIB들은 새로이 정의한 SIB들이다.

3.2.1 "AUTHENTICATE" SIB

IN CS-1R에서 정의한 "AUTHENTICATE" SIB를 확장하기 위해 이 SIB의 정의 상태와 보안 관점에서 지능망의 인증에 관한 요구사항을 확인해 볼 필요가 있다. 현재 이 SIB는 인증을 위한 메카니즘으로 서비스가입자번호와 비밀번호간의 일치성 여부를 검사하는 단순 인증 방식으로, Authenticate Name 및 Authenticate Password라는 서비스지원데이터(SSD: Service Support Data) 및 호인스턴스데이터(CID: Call Instance Data)를 이용하여 구체적으로 정의하고 있으나, 토큰카드나 스마트카드를 이용하는 강력 인증 방식에 대한 인증은 "외부적으로 정의된 인증 기능을 수행한다"는 정도의 표현만 있을 뿐 상세한 인증 능력은 포함하고 있지 않다.

결국, IN CS-1R에서 정의한 "AUTHENTICATE" SIB는 인증 과정에 있어서 다양한 액세스 방식이나 인증 방식 그리고 선택사항을 지원하기 위해 수정 또는 확장되어야 한다. 그리고 인증에 관한 SIB를 수정하거나 확장할 때 논문 9에서와 같이 두개로 분리하는 방식은 지능망에서 인증 망능력을 지원하기 위해 최종적으로 IN CS-1R의 "AUTHENTICATE" SIB, 그리고 논문 9의 "Authentication by IN" SIB 및 "Authentication via IN" SIB와 같은 세개의 SIB가 정의되어야 하는데, 동일한 망능력을 다수의 SIB로 정의하는 것은 표현의 중복성 문제나 하위 평면과의 호환성 문제 등

을 야기할 수 있다[9][17]. 따라서, 그림 1과 같이 단순 인증 및 강력 인증 방식을 동시에 포함하고 다양한 선택사항들을 함께 제공하는 확장된 SIB로써 특정 실체의 정체(identity)에 대한 보장 기능을 제공하는 "AUTHENTICATE" SIB를 제안한다. 해당 오퍼레이션은 다음과 같다.

Acquire: 청구자(claimant)나 입증자(verifier)가 하나의 인증 인스턴스에 대해 특정 교환인증정보(exchange authentication information)를 생성하기 위해 필요한 정보를 획득한다.

Generate: 청구자(claimant)가 교환인증정보를 생성한다.

Verify: 입증자가 청구자로부터 수신한 교환인증정보를 검증한다.

Generate and Verify: 상호 인증이 필요한 상황에서 Generate 동작과 Verify 동작을 연계하여 수행한다.

3.2.2 "INTEGRATE" SIB

인가받지 않은 변경, 생성 및 삭제 동작을 감지하고 데이터를 보호하는 SIB로써, 해당 오퍼레이션은 다음과 같다.

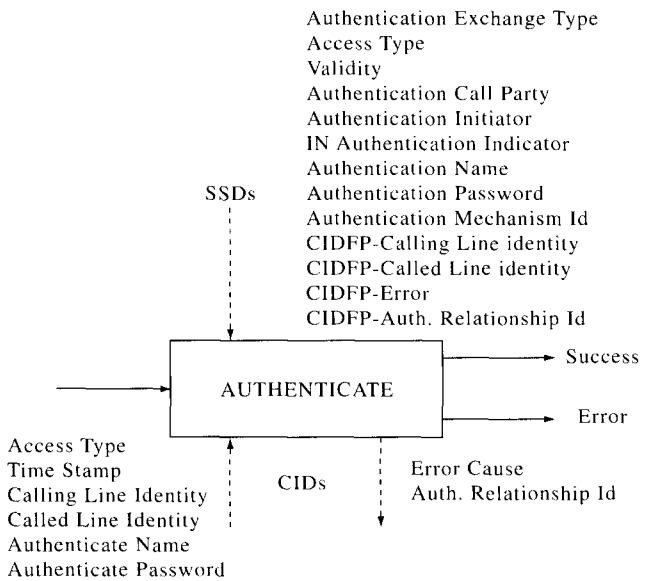
shield: 무결성 보호의 순방향 메카니즘을 이용하여 데이터로부터 무결성보호 데이터(integrity protected data)를 생성한다.

validate: 무결성 실패를 감지하기 위해 데이터, 암호검사값 및 키등을 이용하여 무결성보호데이터를 검사한다.

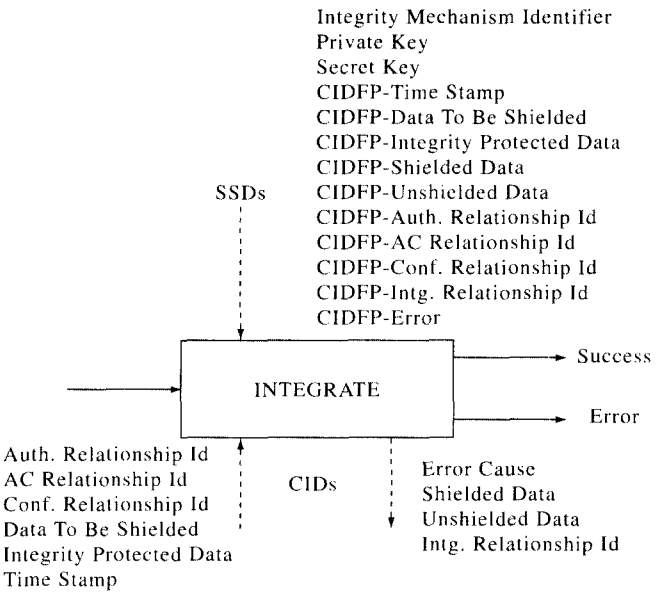
unshield: 무결성 보호의 역방향 메카니즘을 이용하여 무결성보호데이터로부터 데이터를 재생성한다.

3.2.3 "SECRETE" SIB

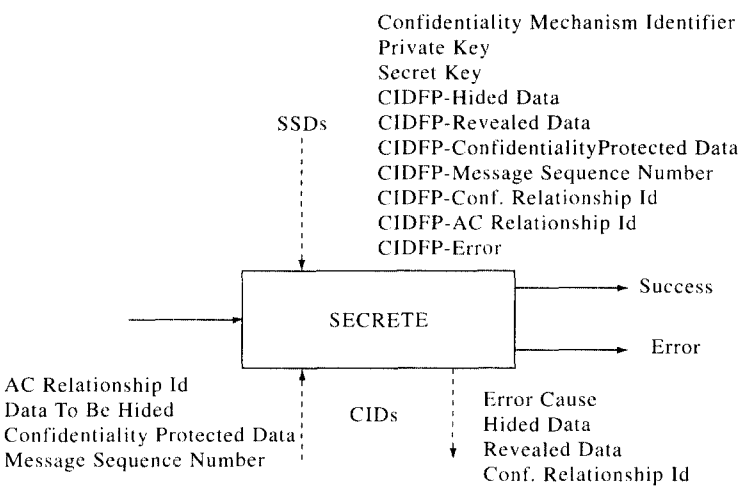
인가받은 실체에게만 정보를 이용할 수 있



〈그림 1〉 확장된 "AUTHENTICATE" SIB



〈그림 2〉 "INTEGRATE" SIB



〈그림 3〉 "SECRETE" SIB

도록 하는 SIB로써, 해당 오퍼레이션은 다음과 같다.

Hide: 비밀성 보호의 순방향 메카니즘을 이용하여 데이터로부터 비밀성보호데이터(confidentiality protected data)를 생성하거나, 이미 수행된 비밀성보호데이터로부터 또다른 비밀성보호데이터를 생성한다.

Reveal: 비밀성 보호의 역방향 메카니즘을 이용하여 비밀성보호데이터에 대한 최종 비밀성 보호를 제거한다.

또한, 개방된 통신 자원에 대한 접근을 제한하는 "CONTROL ACCESS" SIB, 그리고 논쟁이나 시비를 해결하기 위해 증거에 대한 생성, 기록 및 (재)검증을 지원하는 "NON-REPUDIATION" SIB에 대한 그래픽 표현은 생략하며, 각각의 SIB에 대한 오퍼레이션은 다음과 같다.

- "CONTROL ACCESS" SIB 오퍼레이션

  Acquire initiator-bound ACI: 개시자(initiator)에 한정된 접근제어정보(ACI: Access Control Information)를 획득한다.

  Acquire target-bound ACI: 목표자(target)에 한정된 접근제어정보를 획득한다.

  Generate access request-bound ACI: 접근제어결정을 수행하기 위해 필요한 정보들, 즉 개시자에 한정된 접근제어정보(ACI) 및 접근요청에 대한 접근제어정보들을 이용하여 접근요청에 한정된 접근제어정보를 생성한다

  Verify bound ACI and derive ADI: 한정된 접근제어정보의 유효성을 검사하고 접근제어정보로부터 접근제어결정정보(ADI :Access control Decision Information)를 유도한다.

  Get contextual information: 접근제어결정을 수행하기 위해 필요한 전후관계 정보를 획득한다.

  Decide access: 접근이 허용되는지를 결정한다.

- "NON-REPUDIATION" SIB 오퍼레이션

  Generate evidence: 증거물을 생성한다.

  Generate time stamp: 타임스탬프를 생성한다.

  Generate notarized evidence: 증거물을 삼자신뢰실체(TTP: Trusted Third Party)에게 공탁한다.

  Validate evidence: 증거물의 정당성 여부를 검사한다.

3.3 DFP

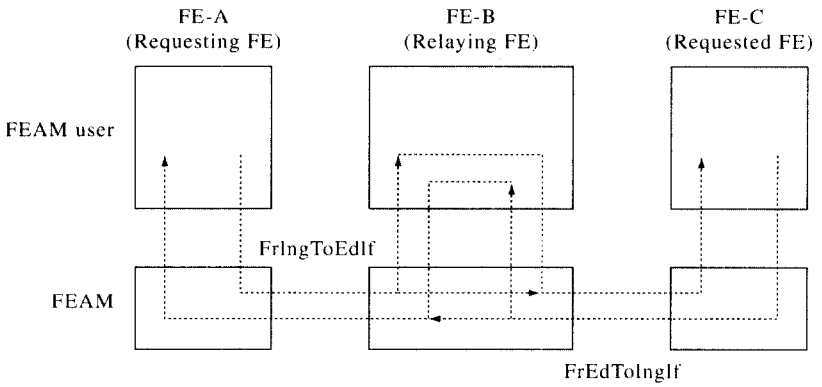
현재의 지능망 기능실체를 이용하여 인증, 접근제어, 비밀성, 무결성 및 부인봉쇄와 같은 보안 능력을 종합적으로 제공할 수 없다. SvP 및 GFP에서 서비스특징을 정의하고 망능력을 확장한 것처럼 DFP에서도 필요한 기능실체를 추가하고, 관련 기능실체들간 연관성을 정의해야 한다[18].

3.3.1 SIB 단계 2 정보흐름

전장의 GFP에서 정의된 SIB들은 SIB단계 1에 대한 정의로써, 이 SIB들을 DFP의 관련 기능실체들간 정보흐름 관점에서 정의하는 것이 SIB 단계 2 정보흐름이다. 이들 정보흐름은 각각의 SIB에 따라 다르게 나타날 수 있으며, 하나의 SIB에서도 조건에 따라 다르게 나타날 수 있다. 예를 들면, "AUTHENTICATE" SIB의 경우, One-way, Two-way, 및 Three-way 전송 절차에 따라 그리고 단일 인증 및 상호 인증과 같은 인증 형식에 따라 정보흐름이 다르게 나타난다.

우선 이러한 정보흐름의 복잡성을 줄이기 위해 보안 관련 SIB에 대한 정보흐름을 추상적으로 정의한다. 이를 위해 보안 서비스를 요청하는 기능실체, 실제로 보안 서비스를 수행하는 기능실체, 그리고 종단 기능실체들간 정보흐름을 중계하는 기능실체로 구분하여 그림 4와 같은 정보흐름 모델을 사용한다[25].

따라서, 요청 및 수행 기능실체들은 동일한 보안 서비스에서 서로의 역할이 분리되며, 해당 보안 메카니즘을 운영한 결과로 생성된 파라미터를 FrIngToEdIf(요청 기능실체에서 수행 기능실체로 전달되는 정보흐름) 및



〈그림 4〉 정보흐름 모델

FrEdToIngIf(수행 기능실체에서 요청 기능실체로 전달되는 정보흐름)의 정보흐름을 제어하는 FEAM(Functional Entity Access Manager) 기능을 이용하여 상호 통신한다.

각각의 SIB에 대한 정보흐름은 다음과 같이 구문 표현을 이용하여 정의한다.

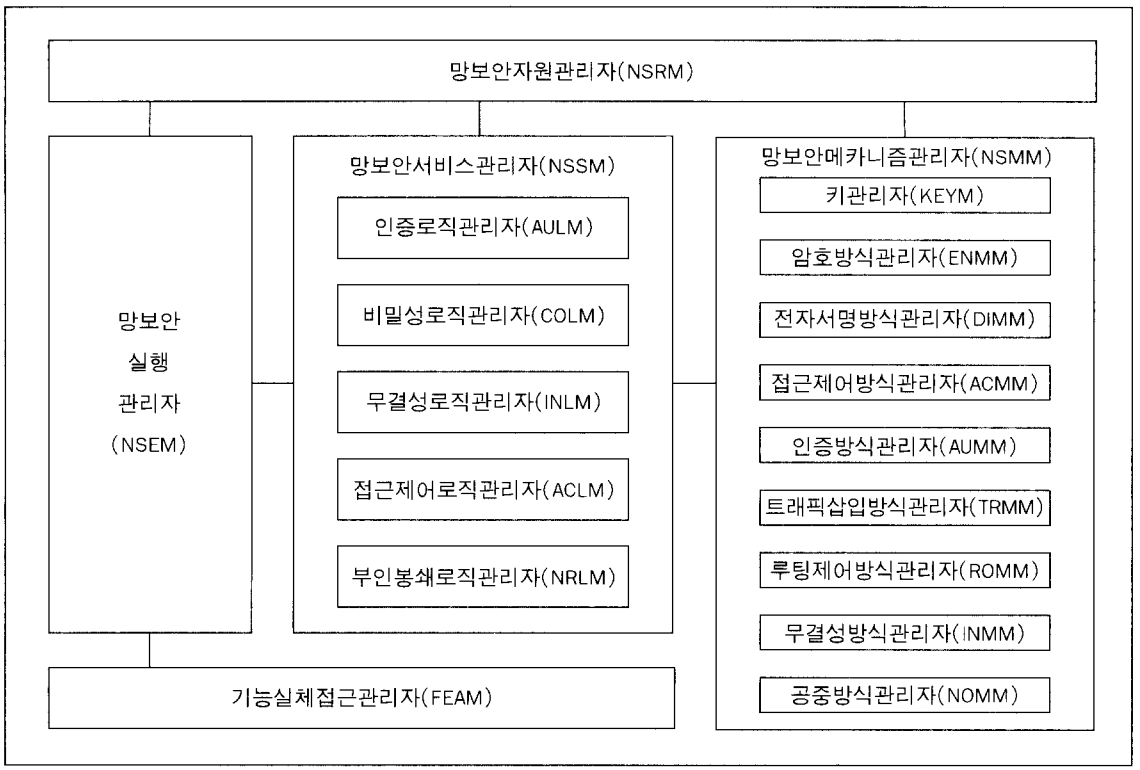
요청 정보흐름 ::=SIB,
"_", "FrIngToEdIf", '_', 일련번호
수행 정보흐름 ::=SIB,
"_", "FrEdToIngIf", '_', 일련번호
SIB ::=CHOICE
{"AUT"--"AUTHENTICATE" SIB
|"INT"--"INTEGRATE" SIB
|"SEC"--"SECRETE" SIB
|"CON"--"CONTROL ACCESS" SIB
|"NON"--"NON-REPUDIATION" SIB}

예로써, "AUTHENTICATE" SIB에서 요청 기능실체가 전송하는 정보흐름은 "AUT_FrIngToEdIf_1"로 표현할 수 있으며, 이에 대한 응답으로 수행 기능실체가 전송하는 정보흐름은 "AUT_FrEdToIngIf_2"로 표현할 수 있다.

3.3.2 망보안기능 모델

논문 9 및 12에서는 강력 인증이나 접근제한 등과 같은 보안 서비스를 제공하기 위해 DFP에서 각각 키분배기능(KDF: Key Distribution Function) 및 서비스제어접근기능(SCAF: Service Control Access Function)라는 기능실체를 추가하고 있다[9][12]. KDF는 비밀키 암호방식를 사용하는 경우 종단 사용자에게 비밀키를 제공하고, 공개키 암호방식을 사용하는 경우 인증자를 분배하는 기능실체이다. SCAF는 관련된 서비스로직프로그램의 초기에 모든 암호화 동작을 수행하여 인증 및 접근제어에 대한 처리 결과를 출력하는 기능실체이다.

이들 논문에서는 보안을 위한 새로운 기능실체의 필요성은 주장하였지만, 기능실체의 구체적인 모델 등을 제시하지 않았다. 이러한 이유로, 본 논문에서는 기존의 지능망 기능실체에 그림 5와 같은 망보안 기능실체(NSF: Network Security Function)를 추가하고, 이를 "지능망에서 서비스이용자나 망운용자에게 인증, 접근제어, 비밀성, 무결성 및 부인봉쇄와 같은 보안 능력을 제공하는 기능실체"로 정의한다.



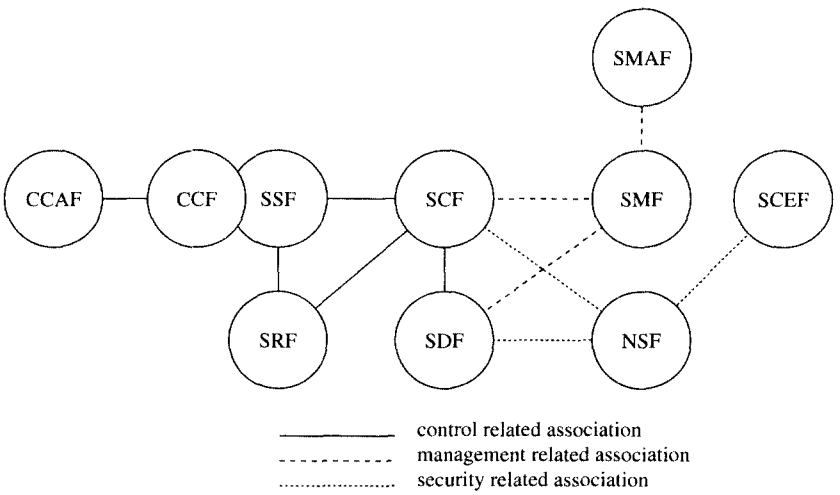
〈그림 5〉 NSF 모델

상기 모델중 기능실체 접근관리자(FEAM: Functional Entity Access Manager)는 망보안 실행관리자가 SCF(Service Control Function) 기능실체와 정보를 교환하도록 하는 메시지 처리 기능성을 제공한다. 이 메시지 처리 기능성은 OSI 구조 및 원칙에 따른 신뢰성 있게 메시지를 전송할 수 있어야 한다. 망보안 실행관리자(NSEM: Network Security Execution Manager)는 전체의 망보안 로직을 수행하며, 각각의 망보안 서비스관리자가 공통으로 요구하는 기능성을 제공한다. 이 모듈은 역호환성을 위해 SDF(Service Data Function) 기능실체의 "보안 관리자" 모듈이 제공하는 기능을 포함한다. 망보안 서비스관리자(NSSM: Network Security Service Manager)는 인증, 접근제어, 무결성, 비밀성 및 부인봉쇄와 같은 특정 보안 서비스에 대한 로직을 수행한다. 망보안 메카니즘관리자(NSMM: Network Security Mechanism Manager)는 인증, 접근제어, 무결성, 비밀성 및 부인봉쇄와 같은 특정 보안 서비스에서 필요로 하는 보안 메카니즘들, 예를 들면 암호화, 전자서명, 접근제어, 무결성, 인증, 트래픽삽입, 경로제어 및 공증에 대한 방식 자체의 기능성을 제공한다. 망보안 자원관리자(NSRM: Network Security Resource Manager)는 NSEM, NSSM 및 NSMM 모듈들에서 필요로 하는 보안과 관련된 국지 자원들을 등록·해제 또는 할당·복구하며, 보안 관련된 망 차원의 자원에 대한 접근을 제어한다. 이 모듈은 역호환성을 위해 SDF 기능실체의 인증 데이터 및 운용 데이터에 대한 관리를 포함한다.

상기의 기술처럼 보안 서비스를 제공하기 위해 NSF와 같은 새로운 기능실체를 정의하여 지능망의 하나의 독립된 기능실체로 분리할 수 있으나, SDF와 같은 기존의 기능실체에 보안 관련 기능을 추가하여 확장한 모델을 적용하는 것도 고려할 수 있다.

3.3.3 분산기능모델

그림 6의 분산기능모델은 NSF 기능실체를 포함한 다수의 기능실체들간의 연관성을 나타낸다.



〈그림 6〉 확장 분산기능모델

3.4 PhP

보안 서비스를 제공하기 위한 PhP에서의 확장은 DFP에서 확인된 분산기능모델을 이용하여 물리실체의 구성요소에 대한 다양한 시나리오를 확인하고 해당 인터페이스를 정의하므로써 이루어진다[19]. PhP의 확장 중 인터페이스의 정의는 다음장에서 다룬다.

각각의 기능실체를 실제로 어떠한 물리실체에 할당할 것인가는 해당 지능망 운용자의 정책에 따라 달라진다. 예를 들면, 안내방송이나 디지트 수집을 담당하는 SRF(Specialized Resource Function) 기능실체는 일반적으로 IP(Intelligent Peripheral)에 할당되나, 상황에 따라서는 SSP(Service Switching Point)에 할당될 수있다. 표 1은 그림 6의 확장 분산기능모델 중 서비스 제어 및 보안 관련 기능실체들을 중심으로 하는 기능할당 시나리오를 나타낸다.

SSP에서 NSF는 SSP가 SCF 또는 SCF/SDF를 포함할 때 적용할 수 있는 조건적인 할당 시나리오이다. 망장치들 중 서비스 제어 및 보안 관련 물리실체들은 서로 No.7 공통선 신호방식을 통해 접속하며, NSP(Network Security Point)는 "지능망에서 서비스이용자나 망운용자에게 인증, 접근제어, 비밀성, 무결성 및 부인봉쇄와 같은 보안 능력을 제공하기 위해 암호화, 전자서명, 접근제어, 무결성, 인증, 트래픽삽입, 경로제어, 그리고 공증과 같은 보안 메카니즘들을 수행하는 물리실체"로 정의한다.

〈표 1〉 기능할당 시나리오

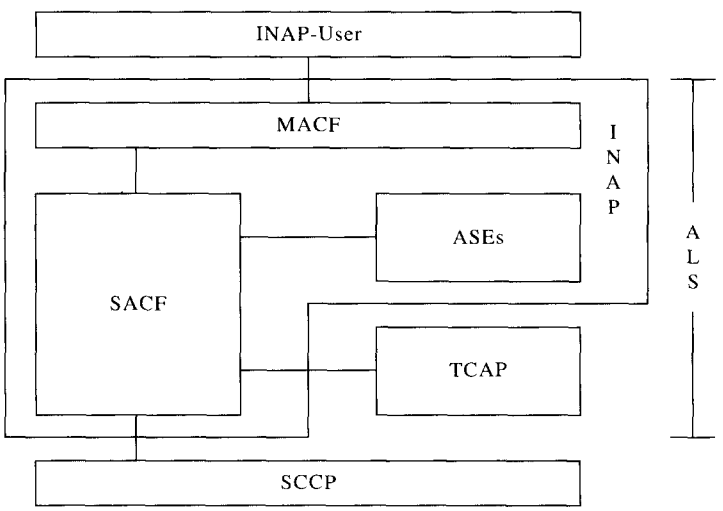
PEs	NSF	SCF	SDF	SSF	CCF	SRF
NSP	C	-	-	-	-	-
SCP	O	C	O	-	-	-
SDP	O	-	C	-	-	-
SSP	O	O	O	C	C	O
AD	O	C	C	-	-	-

4 지능망 응용계층 프로토콜

4.1 개요

IN CS-1, IN CS-1R 그리고 IN CS-2에서 응용계층의 구조를 ISO 표준안 9545의 ALS(Application Layer Structure)를 기초로 기능모델들을 정의하고 있다. 그림 7은 ITU-T에서 표준화되어 있는 응용계층의 표준화 모델에 대한 간략형이다.

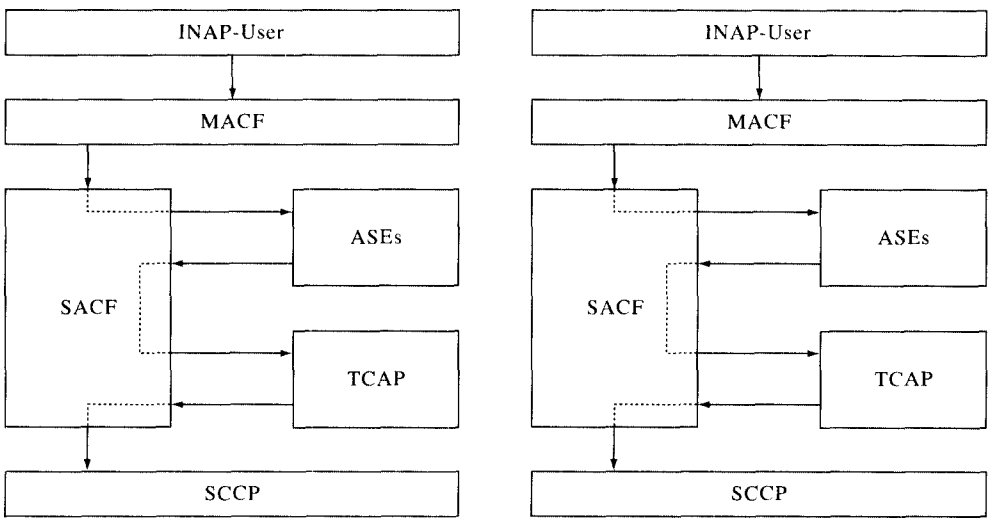
표준화 모델에서의 문제점 하나는 SCCP에서 SAO(Single Association Object)에 대한 주소지정 규칙이 없기 때문에 SCCP가 특정 SAO를 확인할 수 없다는 점이다. SCCP에서 주소지정은 신호점부호(SPC: Signaling Point Code) 및 서브시스템번호(SSN: SubSystem Number)의 조합을 이용하여 결정한다. SSN은 해당 신호점에서 지원하고 있는 응용 또는 서비스로직을 가리키며, 특정 SAO를 지칭하지 않는다. SAO는 응용 독립적인 특성을 지니고 있다. 간접적으로 특정 SAO를 확인할 수 있는 정보는 기능실체간 최초 관계 메세지에 있는 응용문맥이 될 수 있다. 동작부호도 현재로서는 가능하지만 디렉토리 관련 동작부호와 순



〈그림 7〉 응용계층 표준화 모델

수한 INAP 관련 동작부호가 중복된다. 동작부호를 가지고 특정 SAO를 확인하는 방식은 부호의 중복성으로 인해 적절하지 않다. 이들 정보에 대한 접근은 SCCP의 역할도 아니며, TCAP 메세지가 다양하고 메시지 길이가 가변적일 수 있기 때문에 SCCP는 정보들의 위치를 제대로 확인할 수 없다.

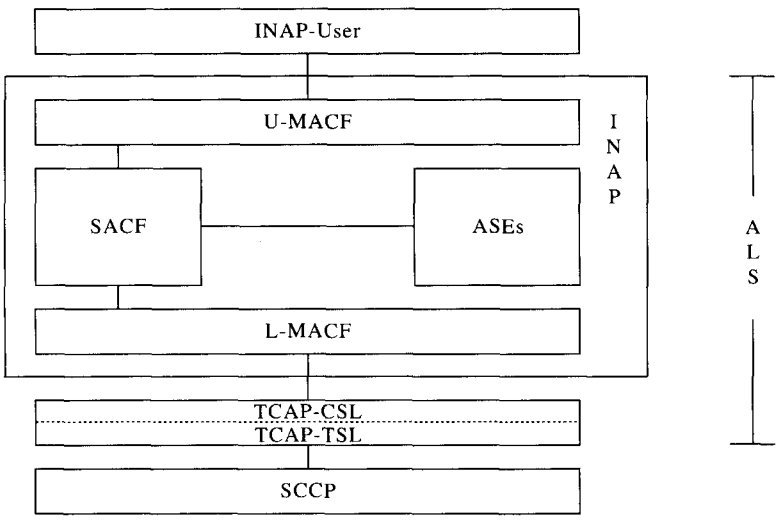
표준화 모델에서의 다른 문제점 하나는 SCCP가 특정 SAO를 확인할 수 있다고 가정하더라도, 기존의 TCAP 및 SCCP 권고안에서 정의된 프리미티브 관점에서 볼 때, SACF(Service Control Access Function)/TCAP 및 SACF/SCCP 사이 인터페이스는 복잡한 제어 흐름을 야기한다는 것이다. TCAP 및 SCCP 권고안 Q.774 및 Q.714에서 정의된 절차를 기초로, TCAP 및 SCCP 사이의 국지적인 통신은 TCAP 및 SCCP 권고안 Q.771 및 Q.711에서 정의된 프리미티브를 이용한다. 이들 절차와 호환성을 유지하기 위해서는 SACF가 TCAP 및 SCCP 사이에서 있는 그대로 받고 보내고 하는 투명 동작을 수행해야 하며, 결국 그림 8과 같은 복잡한 제어 흐름이 존재해야 한다. 적어도 이런 상황에서는 SACF 존재가 무의미하다.



〈그림 8〉 표준화 모델의 제어흐름

4.2 프로토콜 구조 변경

표준화 모델에서 문제점들을 해결하는 기본적인 사항은 SCCP가 특정 SAO를 확인할 수 없다는 SCCP 주소지정 방식의 제한에서 출발한다. 해결 방법은 두 가지가 있을 수 있다. 첫째는, 비록 TCAP이 특정 SAO를 확인할 수 있는 정보에 접근할 수 있다 하더라도 현재의 TCAP과 호환성을 유지하기 위해 INAP 자체에서 특정 SAO를 확인하는 능력을 갖도록 하는 것이다. 그림 9는 이에 대한 기능모델로써, 하위다중결합제어기능(L-MACF: Lower Multiple Association Control Function)의 기본 기능은 TCAP으로부터 프리미티브를 수신한 이후 특정 SAO를 확인하는 것이다.



〈그림 9〉 응용계층의 기능모델 변경

둘째로, TCAP-CSL(Transaction Capabilities Application Part - Component SubLayer)이 수신한 응용문맥을 이용하여 특정 SAO를 확인하는 기능을 갖도록 하는 것이다.

제안된 기능모델들 중 하나를 선정할 때 표준화 모델에서의 문제점들을 해결할 수 있다. 첫번째의 문제점은 L-MACF(또는 TCAP-CSL)가 TCAP-CSL(또는 TCAP-TSL: Transaction Capabilities Application Part - Transaction SubLayer)로부터 프리미티브를 수신한 후 응용문맥을 이용하여 특정 SAO를 확인할 수 있기 때문에 해결된다. 두번째 문제점은 TCAP 및 SCCP가 SACF를 경유하지 않고 바로 통신할 수 있기 때문에 해결된다.

제안하는 두개의 기능모델 중에서 적절한 기능모델은 그림 9의 기능모델이다. 후자의 기능모델은 국지적 절차이든 원격적 절차이든 TCAP에게 영향을 준다. 다른 응용을 지원하기 위해 특정 ASE(예를 들면, 보안 관련 ASE)를 추가하거나 변경해야 한다면 INAP 자체 뿐만 아니라 TCAP 또한 수정해야 한다. 따라서, L-MACF 및 U-MACF(Upper Multiple Association Control Function) 구성요소들이 ALS 설계자나 구현자들에게 어느 정도 혼동을 야기할 수 있으나 명확한 처리 과정을 지원하기 위해서는 그림 9의 기능모델이 적절하다.

4.3 SC-ASE

전장의 그림 4에서 나타난 정보흐름 모델을 참고하면 지능망에서 보안 능력은 다음과 같은 두가지 방식으로 제공할 수 있다.

(1) 응용 프로세스 지원 방식
(2) 응용 프로토콜 지원 방식

첫번째의 응용 프로세스 지원 방식은 응용 프로토콜의 사용자인 응용 프로세스가 보안 메카니즘을 수행하고 관리하는 능력을 제공하고, 응용 프로토콜에서는 보안 관련 정보들을 교환할 수 있는 보안 통신 능력을 제공하는 방식이다. 두번째의 응용 프로토콜 지원 방식은 응용 프로토콜에서 보안 메카니즘을 수행하고 관리하는 능력과 보안 관련 정보들을 교

환할 수 있는 보안 통신 능력을 동시에 제공하는 방식이다.

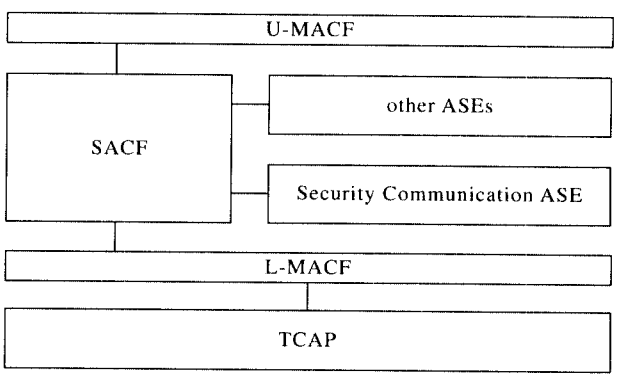
OSI 상위계층에서 보안 능력을 규정하는 X.831 및 X.832 권고안들은 보안교환서비스요소(SESE: Secure Exchange Service Element)라는 이름의 ASE를 이용한 응용 프로세스 지원 방식을 따르고 있으며, 논문 14는 인증, 무결성, 그리고 비밀성과 같은 보안 서비스를 중심으로 보안통신 서비스요소(SCSE: Secure Communications Service Element)라는 이름의 공통 응용서비스요소, 보안 관련 제반 설비 그리고 SMIB(Security Management Information Base)를 이용한 응용 프로토콜 지원 방식을 따르고 있다[14][33][34].

X.831 및 X.832 권고안들의 경우, 비확인형의 SE-TRANSFER 및SE-U-ABORT와 제공자 개시형의 SE-P-ABORT 등 세개의 프리미티브를 이용하여 보안 서비스를 제공한다. 그러나, 대상으로 하는 보안 서비스가 무엇이며, 어떻게 SESE 프로토콜을 이용할 수 있는지 명확하지 않다[33][34]. 논문 14의 경우, OSI의 ACSE (Association Control Service Element) 프로토콜을 사용하는 연결지향형에 알맞은 구조를 제안하고 있으며, 응용 프로토콜 지원 방식을 통한 보안 능력을 제공한다[14]. 따라서, 이들 보안 ASE들이 지능망의 응용계층에서 적용할 수 있는 통신 능력을 제공하지 못한다고 볼 수 있다.

본 논문에서는 지능망에서 보안 능력을 제공하기 위해 첫번째의 응용 프로세스 지원 방식을 적용한다. 그리고 그림 9에서 제시한 지능망 응용계층 프로토콜 구조 상에서, 그림 10과 같이 공통선 신호방식 기반의 INAP에 적합한 보안 서비스용 응용서비스요소, 즉 SC-ASE를 포함하는 보안 통신용 프로토콜 구조를 제안한다.

전장에서 SIB 단계2에 대한 정보흐름은 추상적으로 정의되어 있어 SC-ASE를 정의하는데 직접 이용할 수 없다. 따라서, 좀더 구체적인 형태의 오퍼레이션을 정의해야 하며, 표 2는 이러한 오퍼레이션들을 나타낸다. 여기서 SIB 단계 2 정보흐름 컬럼중 'N'은 최종 일련번호를, "XXX"는 다섯개의 SIB중 하나를, 그리고 'M'은 '1'과 'N' 사이의 번호를 의미한다.

요구형 오퍼레이션을 송수신한 후에 결과형 오퍼레이션을 송수신할 수 있으며, 이들 오퍼레이션 사이에 전송형 오퍼레이션을 상호 송수신할 수 있다. 각각의 결과형 오퍼레이션은 관련 요구형 오퍼레이션의 연쇄 오퍼레이션으로 동작한다. 모든 오퍼레이션들은 등급 2로 동작하고 오퍼레이션 수행시 에러가 발생한 경우 해당 상황을 보고한다. 또한, 트랜잭션을



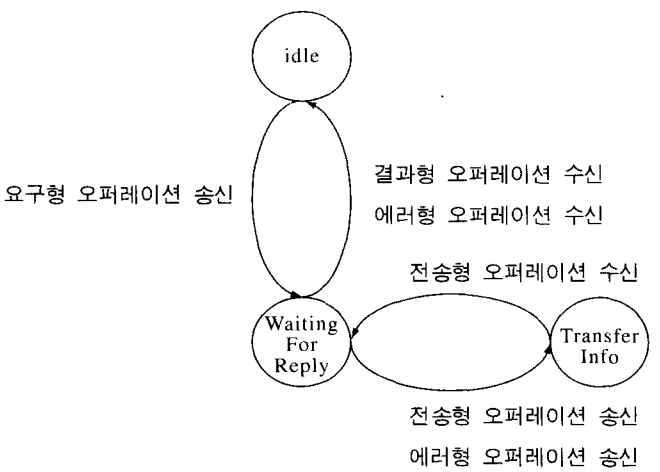
〈그림 10〉 보안 서비스를 위한 지능망 응용계층 프로토콜 구조

〈표 2〉 SC-ASE 오퍼레이션 정의

SIB 단계 2 정보흐름	오퍼레이션	비고
AUT_FrIngToEdIf_1	RequestAuthentication	요구형
AUT_FrEdToIngIf_N	ResultOfAuthentication	결과형
CON_FrIngToEdIf_1	RequestAccessControl	요구형
CON_FrEdToIngIf_ N	ResultOfAccessControl	결과형
SEC_FrIngToEdIf_1	RequestConfidentility	요구형
SEC_FrEdToIngIf_ N	ResultOfConfidentility	결과형
INT_FrIngToEdIf_1	RequestIntegity	요구형
INT_FrEdToIngIf_ N	ResultOfIntegity	결과형
NON_FrIngToEdIf_1	RequestNonRepudiation	요구형
NON_FrEdToIngIf_ N	ResultOfRepudiation	결과형
XXX_FrIngToEdIf_M	TransferInfomation	전송형
XXX_FrEdToIngIf_M	TransferInfomation	전송형

개시된 후 오퍼레이션들을 송수신할 수 있다. 전송형 오퍼레이션을 전송하고 이에 대한 에러형 오퍼레이션을 수신하는 경우, 이전에 수신한 요구형 오퍼레이션에 대한 응답으로써 전송형 오퍼레이션의 에러 수신을 표시한 에러형 오퍼레이션을 송신한다. 전송형 오퍼레이션은 정보를 요청하고, 해당 정보를 전송하는 흐름과 일방적으로 정보를 전송할 수 있는 흐름이 존재한다.

이러한 요구형, 결과형 및 에러형 오퍼레이션들을 상호 교환하여 보안 통신 능력을 제공하는 SC-ASE 프로토콜의 유한상태머신은 그림 11과 같다.



〈그림 11〉 SC-ASE 유한상태머신

5. 보안 서비스 가상 시나리오

지능망에서 보안 서비스를 제공하기 위해 제안된 확장 INCM을 적용하여 특정 지능망 서비스를 대상으로 각 평면에서의 보안 통신 능력을 확인해 볼 필요가 있다. 본 내용에서는 복잡함을 피하기 위해 PhP에 대한 시나리오는 포함하지 않는다.

보안 서비스를 적용할 지능망 서비스는 온라인 환경에서의 UPT 서비스로 하며(이후, "UPT 보안 서비스"라 칭함), 본 내용에서는 다음과 같은 사항들을 가정한다[18].

- 스마트카드를 이용하는 접근 방식으로 한다.
- 비밀키 암호방식을 적용한다.
- 인증은 Challenge · Response 형식으로 진행한다.

5.1 SvP 시나리오

이용자 인증은 인증받지 않은 서비스 도용을 방지하기 위해 UPT 서비스제공자가 UPT 이용자의 신원을 확인하는 서비스특징이다. 적용할 수 있는 보안 서비스는 인증 등이 있다.

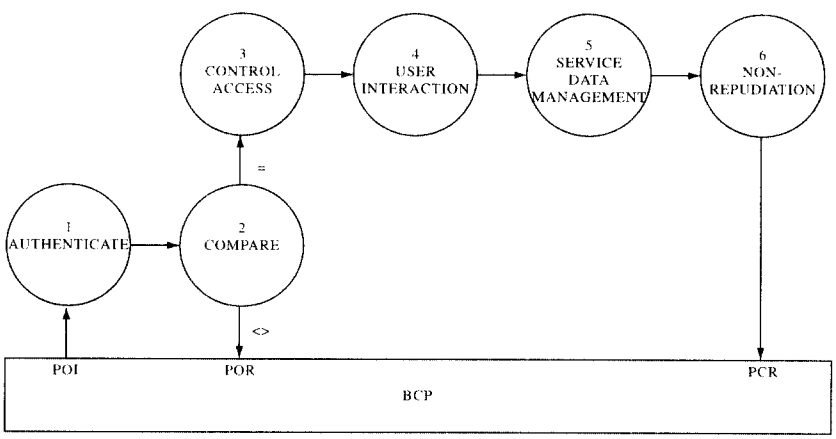
서비스 프로파일 수정은 UPT 이용자가 자신의 서비스 프로파일을 수정할 수 있도록 하는 서비스특징이다. 적용할 수 있는 보안 서비스는 접근제어 및 부인봉쇄 등이 있다.

5.2 GFP 시나리오

모든 SIB에 대한 CID 및 SSD의 입출력과 INCS-1R의 SIB는 본 내용에서 다루지 않으며, 보안 관련 SIB들에 한하여 본 논문에서 제안한 SIB들을 적용한다.

그림 12는 이용자 인증, 서비스 프로파일 수정에 대한 총괄서비스로직(GSL: Global Service Logic)을 나타내며, 이들 전체 로직에 대한 산문식 기술은 다음과 같다.

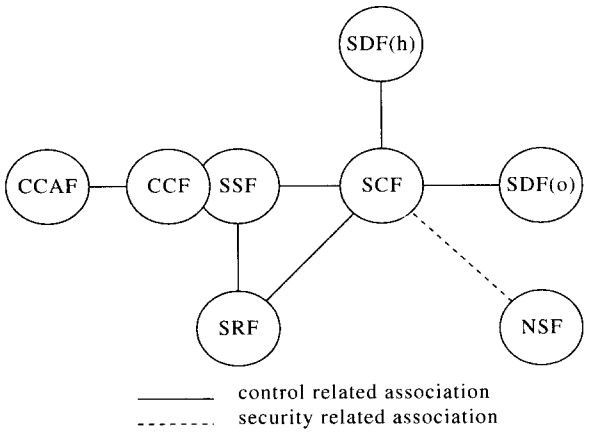
- 서비스이용자는 인증 절차를 성공적으로 수행한다.
- 서비스이용자는 프로파일을 수정하기 위한 접근제어 요청에 대한 허가를 획득한다.
- SDF(h)는 수정하고자 하는 정보를 요청하고, 서비스이용자는 해당 정보를 SDF(h)로 전송한다.
- SDF(h)는 해당 정보를 수정한다.
- 정보 수정에 대한 사후 문제를 방지하기 위해 부인봉쇄를 수행한다.



〈그림 12〉 이용자 인증 및 서비스 프로파일 수정의 GSL

5.3 DFP 시나리오

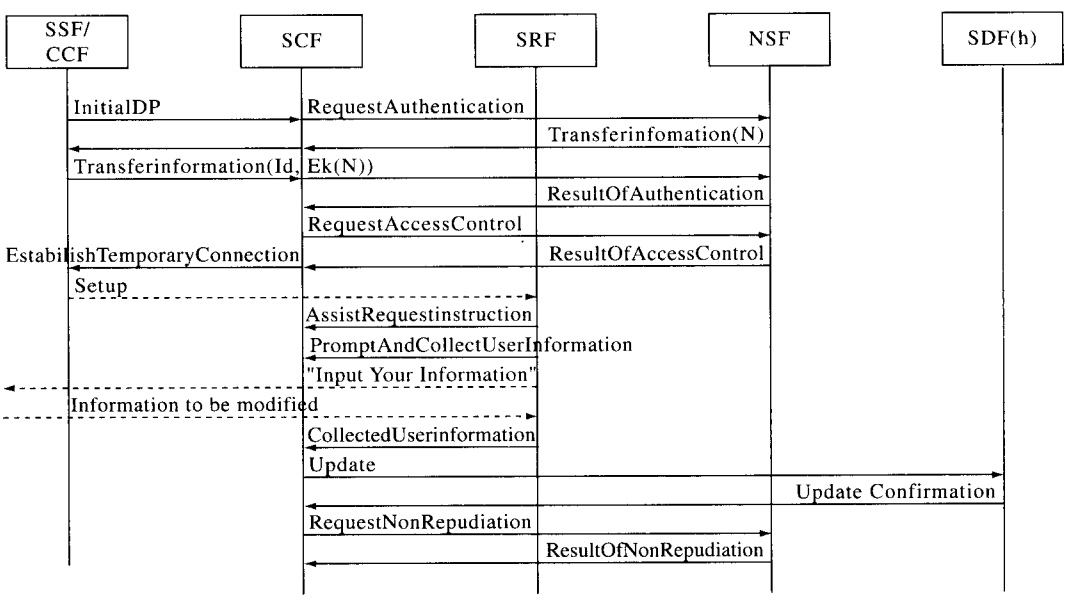
그림 13은 이용자 인증 및 서비스 프로파일 수정에 대한 UPT 보안 서비스를 제공하기 위한 단순한 기능모델이다.



〈그림 13〉 UPT 보안 서비스를 제공하기 위한 단순 기능모델

5.3.1 분산서비스로직

그림 14는 이용자 인증 및 서비스 프로파일 수정에 대한 UPT 보안 서비스를 제공하기 위한 단순 기능모델상에서 진행되는 분산서비스로직(DSL: Distributed Service Logic)이다.



〈그림 14〉 이용자 인증 및 서비스 프로파일 수정의 DSL

6. 결론 및 향후 연구사항

본 논문은 현재의 지능망에 다양한 보안 메카니즘 능력이 존재한다는 가정하에 보안 통신 능력을 추가함으로써 보다 안전한 정보 통신 이용 환경을 구축하는 과정을 기술하였다. 이를 위해, 지능망과 보안을 접목시키기 위해 필요한 보안 통신 능력들을 INCM 기반으로 분석 · 정의하였으며, 주로 다음과 같은 내용들을 포함하였다.

- 지능망에서 보안 통신 능력을 위한 요구사항
- 보안 서비스를 제공하기 위한 INCM의 확장
- 지능망 응용계층의 프로토콜 구조 및 SC-ASE
- UPT를 이용한 가상 보안 서비스 시나리오

좀더 구체적으로 살펴 보면, 보안 서비스를 적용할 수 있는 INCM을 확장하기 위해 SvP에서는 통상의 보안 서비스를 서비스특징 수준으로 정의하였으며, GFP에서는 "AUTHENTICATE", "INTEGRATE", "SECRETE", "CONTROL ACCESS", 그리고 "NON-REPUDIATION"로 이루어진 다섯개의 SIB들을 정의하였다. DFP에서는 SIB 단계에 대한 정보흐름과 NSF라는 보안 전용의 망보안 기능실체를 제안하고, PhP에서는 지능망 응용계층의 프로토콜 구조와 SC-ASE를 제시하였다.

향후 SDL 도구 등을 이용한 검증 과정을 거친다면 DFP의 정보흐름과 망보안 기능실체, 그리고 PhP의 프로토콜적 절차 등이 좀더 보완될 수 있다. 그리고 오퍼레이션의 정보요소들에 대한 상세한 정의와 각각의 파라미터에 대한 부호화 규칙 등이 규정된다면 더욱 완벽한 INCM으로 진화할 수 있다. 본 논제에서 향후 진행해야 할 연구사항은 다음과 같다.

- 확장 INCM의 시뮬레이션 도구를 이용한 검증 및 보완
- SIB 단계 2에 대한 정보흐름
- 망보안 기능실체에 대한 동작 과정
- 오퍼레이션에 대한 상세 파라미터 및 부호화 규칙
- 키관리를 위한 보안 통신 능력 추가

현재, 지능망에 보안 능력을 적용하기 위해 ITU-T나 ETSI(European Telecommunications Standards Institute)와 같은 표준화 단체에서 지능망 보안 능력에 대한 요구사항이나 관련 규정을 준비하고 있고, 지역에 따라서는 상당한 수준의 내용을 발표 · 제안하고 있는 상황에서, 국내에서도 이에 대한 준비나 연구가 절실히 요구되는 시점이다. 조속히 국내 지능망 보안의 요구사항을 마련하고 보안 분야와 지능망 분야가 서로 협력할 수 있는 연구 · 개발 분위기를 조성되어야 할 것이다.

참 고 문 헌

[1] 임채호, 정진욱, "OSI 시큐리티 연구 현황", pp. 89~102, VOL 4 No.1, Jun. 1990

[2] 김동규, "OSI 통신망 구조에서의 보안 메카니즘", pp. 103~109, VOL 4 No.1, Jun. 1990

[3] 원동호, "암호학", pp. 110~122, VOL 4 No.1, Jun. 1990

[4] 윤경옥, 강태규, "디렉토리 기술이 도입된 세대별지능망 표준화동향분석", 전자통신동향분석, pp. 59~71, 제10권 제2호, 1995년 7월

[5] 배현주, 도현숙, 유재건, 김태준, "차세대 지능망 표준화 동향 분석: IN CS-2를 중심으로", pp. 85~98, 제10권 제4호, 1996년 1월

[6] 김신효, 조진만, 조현숙, "스마트카드를

이용한 선지불 DBS 유료 방송 서비스", Proc. 7th Joint Conference On Communications and Informations (JCCI), pp. 236~239, 1997년 4월

[7] 한국전자통신연구소, "차세대 지능망 개념서", 1991년 12월

[8] 한국전자통신연구소, "UPT 요구사항서", 1994년 9월

[9] Refik Molva, Pierre-Alain Etique, Jean-Pierre Hubaux, "Strong Authentication in Intelligent Networks", Proc. 3rd International Conference On Univeral Personal Communications (ICOUPC), pp. 629~634, Sep. 1994

[10] Ciaran Clissmann, Ahmed Patel, "Security for Mobile Users of Telecommunication Services", Proc. 3rd International Conference On Univeral Personal Communications (ICOUPC),pp. 350~353, Sep. 1994

[11] Stephen A. Sherman, Richard Skibo, Richard S. Murray, "Secure Network Access Using Multiple Applications of AT&T's Smart Card", AT&T TECHNICAL JOURNAL, pp. 61 ~ 72, Oct. 1994

[12] Alexander Herrigel, Xuejia Lai, "Authentication and Authorization in the IN based on Symmetric and Asymmetric Techniques", Porc. 3rd International Conference on Intelligence in Networks (ICIN), pp. 157~162, Oct. 1994

[13] A. Skomedal, C. Galard, "User Security in IN, Identification Service and Protection of User Data", Proc. 2nd International Conference on Intelligence in Networks (ICIN),pp. 32 ~ 37, Mar. 1992

[14] Kouji Nakao, Kenji Suzuki, "Proposal on a Secure Communications Service Element (SCSE) in the OSI Application Layer", IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989

[15] COM XI-R 198-E, "Functional Description of Transaction Capabilities", Revised Recommendation Q.771, Apr. 1992

[16] ITU-T SG 11 WP 4, "Introduction to Intelligent Network IN CS-1", Recommendation Q.1211, Mar. 1993

[17] ITU-T SG 11 WP 4, "Global Functional Plane for Intelligent Network IN CS-1", Draft Recommendation Q.1213, Apr. 1995

[18] ITU-T SG 11 WP 4, "Distributed Functional Plane for Intelligent Network IN CS-1", Draft Recommendation Q.1214, Apr. 1995

[19] ITU-T SG 11 WP 4, "Physical Plane for Intelligent Network IN CS-1", Recommendation Q.1215, Sep. 1994

[20] ITU-T SG 11 WP 4, "Application Protocol for Intelligent Network IN CS-1", Draft Recommendation Q.1218, Apr. 1995

[21] ITU-T SG 11 WP 4, "Introduction to Intelligent Network IN CS-2", Draft Recommendation Q.1221, Nov. 1995

[22] ITU-T SG 11 WP 4, "Global Functional Plane for Intelligent Network IN CS-2", Draft Recommendation Q.1223, Nov. 1995

[23] ITU-T, "The Directory: Authentication Framework", Recommendation X.509, Nov. 1993

[24] ITU-T, "Security Architecture for Open Systems Interconnection for CCITT Applications", Recommendation X.800, 1991

[25] ITU-T, "Upper Layers Security Model", Recommendation X.803, Jun. 1994

[26] ITU-T, "Security Frameworks for Open

Systems: Overview", Recommendation X.810, Nov. 1995

[27] ITU-T, "Security Frameworks for Open Systems: Authentication Framework", Recommendation X.811, Apr. 1995

[28] ITU-T, "Security Frameworks for Open Systems: Access Control Framework", Recommendation X.812, Nov. 1995

[29] ITU-T, "Security Frameworks for Open Systems: Non-repudiation Framework", Recommendation X.813, Oct. 1996

[30] ITU-T, "Security Frameworks for Open Systems: Confidentiality Framework", Recommendation X.814, Nov. 1995

[31] ITU-T, "Security Frameworks for Open Systems: Integrity Framework", Recom--mendation X.815, Nov. 1995

[32] ITU-T, "Generic Upper Layers Security: Overview, Model and Notation", Recommendation X.830, Jul. 1994

[33] ITU-T, "Generic Upper Layers Security: Security Exchange Service Elements(SESE) Service Definition", Recommendation X.831, Jul. 1994

[34] ITU-T, "Generic Upper Layers Security: Security Exchange Service Elements(SESE) Protocol Specification", Recommendation X.832, Apr. 1995

□ 著者紹介

김 영 화

1987년 2월 전남대학교 계산통계학과 졸업(이학사)
1997년 2월 충남대학교 컴퓨터공학과 졸업(이학석사)
1988년 2월 ~ 현재 한국전자통신연구원
광대역전송연구부 접속기술연구실 선임연구원

※ 주관심 분야 : IN, Security, Access Network 등

조 세 형

1981년 서울대학교 공과대학 공학사
1983년 서울대학교 대학원 계산통계학 석사
1992년 펜실베니아 주립대학 전산학 박사(인공지능)
1984년 ~ 1998년 한국전자통신연구원 근무, 현 지능망서비스 연구실장

※ 주관심 분야 : 지능망, 멀티미디어 접속 기술, 인공지능 응용

류 채 철

1985년 2월 한양대학교 산업공학 학사
1988년 5월 Iowa State Univ. 전산학 석사
1990년 12월 Northwestern Univ. 전산학 박사
1991년 2월 ~ 현재 충남대학교 컴퓨터과학과 조교수

※ 주관심 분야 : 컴퓨터 및 통신 보안체제, 네트워크 관리, 분산처리