□특집□

미 국방부의 정보관리 기술 아키텍쳐 프레임웍과 목표보안 아키텍쳐

김 정 덕† 심 영 철††

◈ 목 차 ◈

1. 서 론

1993년 1월 이후, 미 국방부는 정보관리 기술 아키텍쳐 프레임웍(TAFIM: Technical Architecture Framework for Information Management)을 통해 국방부 정보시스템의 통합을 도모할 수 있도록 하였다. 장기적 목표로, 국방성은 시스템 개발, 운영, 유지보수 모든 면에서 궁극적으로 공급자로부터 독립될 수 있도록 하는 개방 시스템 환경을 추구하고 있다. 이 결과, 시스템간의 상호운영성과 통합성, 소프트웨어의 이식성/재사용성 등을 기대할 수 있다. TAFIM V.2는 다음과 같은 7개 볼륨으로 구성되어 있다.

Vol. 1: 개관(Overview)

TAFIM은 모든 국방부 조직과 환경(전술적, 전략적 등)에 정보 시스템의 기술적 아키텍쳐를 의무적으로 적용시키기 위한 것이다. 즉 TAFIM은 모든 임무, 기능과 활동에서의 요구사항을 만족시켜주는 아키텍쳐 개발을 위한 지침이다. 특정 임무나 기능에서 요구하는 특정 기술 아키텍쳐는 TAFIM이 제공하는 지침과 개발 방법론을 통해 개발될 수 있다.

Vol. 2: 기술 참조모델과 표준 프로파일 요약 (Techinical Reference Model and Standard Profile Summary)

기술 참조모델의 목적은 국방부내에서 정보시스템의 다양한 구성요소의 구매, 개발, 지원 활동을 조화시키기 위해서 개념적 프레임웍을 제공하며, 공통 어휘와 기본 표준을 명시하기 위한 것이다. 이 표준들은 특정 임무의 요구사항을 만족시키기 위해 수정 적용될 수 있다.

Vol. 3: 아키텍쳐 개념과 설계 지침(Architecture Concepts & Design Guidance)

Vol. 2의 내용이 서비스와 개체간의 인터페이스를 서술하고 있으나, Vol. 3는 구성요소와 그 구성요소에 할당된 서비스에 대한 내용을 포함하고 있

† 정회원 : 중앙대 산업정보학과 부교수
†† 정회원 : 홍익대 컴퓨터공학과 조교수

다. 또한 아키텍쳐 개념에 대한 논의와 기술의 가용도와 성숙도에 기초한 설계 지침을 기술하고 있다.

Vol. 4: 표준기반 아키텍쳐 기획지침(DoD Stds-Based Architecture Planning Guide)

표준기반 아키텍쳐 방법론은 통합 아키텍쳐에 대한 다음과 같은 4가지 관점에 기초한다; 활동조직, 정보, 응용과 기술. Vol. 1,2,3는 주로 기술 아키텍쳐에 초점을 맞추었다. Vol. 4는 다른 3가지 관점(활동조직, 정보, 응용)을 기술 아키텍쳐에 적용(Mapping)할 수 있는 방법을 제공하여 준다. 즉 기업의 기능적/비지니스의 요구사항을 정보기술적 해결로 변환시켜주는 메커니즘을 제공하여 준다. 표준기반 아키텍쳐 기획지침은 전반적인 기획 및 구현 과정에 대한 방법과 주요 고려사항들을 서술하고 있다.

Vol. 5: 지원 계획(Support Plan)

현재 개발 중이며, 완성시 TAFIM에 포함될 예정임

Vol. 6: 국방부 목표 보안 아키텍쳐(DoD Goal Security Architecture: DGSA)

국방부 목표 보안 아키텍쳐는 TAFIM의 가장 핵심적인 부분이다. 주요 보안 원칙과 목표 보안 능력을 명시함으로써, 시스템 보안 설계자가 특정 보안 아키텍쳐를 설계할 경우 지침으로서 사용할 수 있도록 하기 위함이다. 국방부 목표 보안 아키텍쳐는 현재도 지속적으로 개발중이며 기술발전과 더불어 계속적으로 변화될 것이다. 또한, 국방부 목표 보안 아키텍쳐는 보안 제품과 메카니즘의 개발에 기초를 제공할 것이다. 이 부분의 자세한 내용은 다음 장에서 기술한다.

Vol. 7: 채택된 정보기술 표준(Adopted Information Technology Standards: AITS)

AITS의 목적은 국방부에서의 구매활동과 기존 시스템의 전환계획을 안내하기 위함이다. 즉, 국방부 관리자가 개방시스템 환경(Open System Environment)을 향해서 그들이 수행하는 프로그램과 프로젝트를 안내하기 위해 방향을 제시하고 필요한 정보를 제공하기 위함이다.

Vol. 8: 국방부 HCI 스타일 지침(DoD Human - Computer Interface Style Guide)

모든 국방부 응용시스템이 일관성있게 작동될 수 있도록 HCI 설계 및 구현을 위한 공통 프레임웍을 제공하기 위한 것이다. 이 프레임웍을 통해 HCI의 장기적인 가능상의 목적, 목표와 요구사항이 정의되고 문서화 될 것이다.

2. TAFIM의 목표 보안 아키텍쳐 (DGSA)

목표 보안 아키텍쳐(DGSA:DoD Goal Security Architecture)는 특정 정보시스템의 명세를 제공하는 것이 아니라 보안원칙과 목표 보안능력을 명시하므로써, 추후에 DGSA와 일관성이 있는 특정 보안 아키텍쳐를 개발하기 위한 지침을 제공하는데 있다. DGSA는 현재 계속적인 개발과정에 있으며 다음과 같은 반복적 과정을 거쳐 개발된다; 요구사항 분석, 아키텍쳐 구조 개발, 보안서비스 적용, 보안 구성요소와 메커니즘 선택.

2.1 보안 요구사항 및 아키텍쳐

DGSA보안정책은 아래와 같이 요약되는 국방부 정보시스템 보안정책(NSA, 1993)에서 언급하고 있는 보안 요구사항에 기초하고 있다.

① 국방부 정보시스템은 기밀정보는 아니나 민감한 정보 뿐만 아니라, 다양한 분야의 기밀정보 등을 포함하는 여러 형태나 복잡도

를 가진 보안정책하에서 정보처리를 지원해야 한다.

② 국방부 정보시스템은 개방시스템구조를 수용하는 다중 네트워크에서의, 다중 호스트간의 분산 정보처리가 가능하도록 충분히 보호되어야 한다.

③ 국방부 정보시스템은 상이한 수준의 보호가 요구되는 자원을 보유한 사용자간의 정보처리를 지원해야 한다.

④ 국방부 정보시스템은 공중망 통신을 허용할 수 있도록 충분히 보호되어야 한다.

이외에도 임무관련 운영목표와 보안 요구사항 간의 상호작용을 살펴보면 다음과 같다.

1) 조직의 사업과 보안

C4IFTW(Command, Control, Communication, Computer, and Intelligence For The Warrior)과 CIM(Corporate for Information Management)과 같이 국방부 전체에 해당되는 사업은 운영상의 목표를 가지고 있으며 이는 곧 정보보안에도 영향을 미친다. CIM은 정보의 집중화, 정보의 접근과 상호운영성을 강조하는데, 이는 보안을 제공하는 방법이 고립적이어서는 안되며 하나의 정보시스템에도 상이한 보안수준을 갖는 정보가 존재하며 적절한 분리, 인증, 레이블링, 접근제어가 제공되어야 함을 고려할 필요가 있다. C4IFTW는 전장에서 군인이 필요한 정보를 어떠한 매체나 위치에 상관없이 제공하기 위한 목적이다. 이러한 운영목표는 보안상 해결해야 할 문제를 제시하고 있다. 전쟁 장비를 위한 시스템 인터페이스는 일반적인 인터페이스와 상이해야 하며 따라서 새로운 인증문제를 제시한다. 또한 언제라도 필요한 정보에 접근하기 위해서는 상호운영성과 가용성이 요구되기도 한다.

2) 기존 소프트웨어나 장비의 사용

정보보안에 대한 의사결정시 항상 경제적인 관점에서 평가되어야 한다. 따라서 가능하면 이미 구현되어 사용할 수 있는 상용(COTS)이나 관용(GOTS: Gov't off-the-shelf) 장비에 보안기능이 표준적으로 구현되어 가격에 대한 최소한의 영향을 미치도록 해야한다. 이를 위해서는 국제, 상용, 국방부 표준을 준수해야 한다.

3) 인증과 인정

인증(Certification)은 모든 보안 메커니즘의 효과성을 결정하는 과정이고 인정(Accreditation)은 특정 조직이 정보시스템의 성능 및 보안에 대한 운영상의 책임을 수락하거나 거절하는 과정이다. 인증과 인정은 상호 보완적인 과정으로서 일관성과 적용가능성이 요구된다. 따라서 제품과 시스템의 인수에 필요한 시간을 단축시키고, 인정과정상의 불일치를 제거하기 위해서 표준적 절차가 요구된다. 이 절차는 또한 분산환경하에서 일관성있고 상호운용 가능한 보안을 보장하여 줄 것이다.

4) 분리의 필요

대부분의 임무를 수행하기 위해서는 여러 집단의 공동노력이 필요할 경우가 많다. 따라서 한 개인이 여러 집단에 소속되어 동시에 두 개 이상의 작업을 수행할 필요가 있을 경우가 있다. 이 경우로 인한 보안 요구사항은 여러 집단이 시스템과 정보를 공유할 수 있으면서 필요하면 정보와 사용자를 분리시킬 수 있는 메커니즘이 필요하다.

5) 투자수익율의 극대화

경쟁의 심화와 급격한 기술발전에 의한 새로운 기술로의 전이비용(transition cost)의 상승, 제한된 예산 등에 의해 전략적인 접근이 필요하다. 즉 장기적인 운영상의 목표를 지원하는 전략을 수립해야 하는데 예를 들면, 이식성 향상, 지속적인 기능향상, 확장성, 소프트웨어의 재사용, 인증과 인정 결과의 재사용 등이 있다. 각각의 전략은 보안

에 영향을 미치는 데, 특히 변경후 시스템과 제품에 대한 재 인정은 장기적으로 가장 큰 이득을 초래할 수 있는 전략이다.

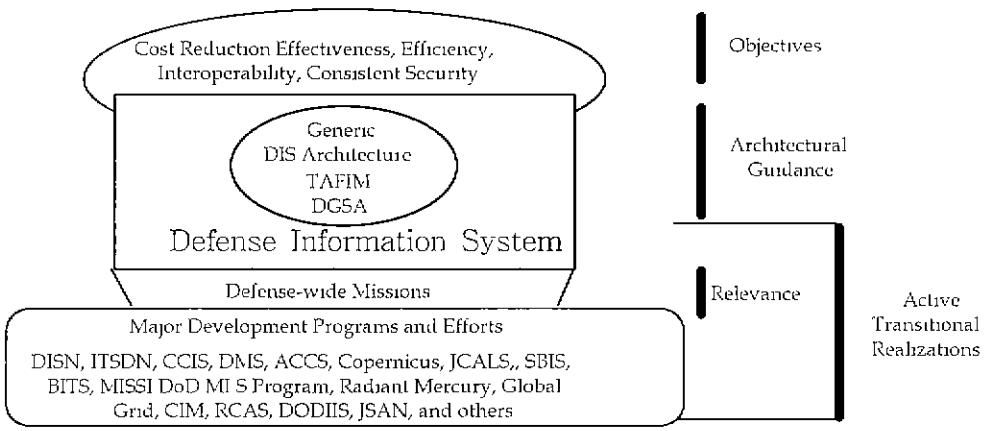
TAFIM, DGSA, 임무 지향 정보 시스템 및 DISN(Defense Information System Network)의 요구사항들은 DoD 계층의 각 구성요소들에 의해 설정된다. 이러한 구성요소들은 정보 관리를 위한 특정 응용소프트웨어를 개발하는 DoD 내의 모든 개발 프로그램과 공동 참여를 위한 기초를 형성한다. TAFIM 정보관리 통합 모델은 DoD 계층을 5 단계(기획, 임무, 기능, 응용 및 대인)로 나눌 수 있다. 이 통합 모델은 관리 책임을 분류하여 할당시킬 수 있는 기능들의 교차점을 명확히 함으로써, 정보관리의 통합 책임을 할당하기 위한 기초를 제공한다. 따라서, TAFIM 정보관리 통합 모델의 각 단계별 요구사항은 DIS 목표 아키텍쳐에서 고려되어 주요 응용소프트웨어 개발 프로그램과 공동 참여를 추진시키기 위하여 결합된다. TAFIM, DII 및 DGSA는 정보관리 지침과 범 DoD 임무를 지원하는 방향을 제공하기 위한 기획 단계의 요소들이다.

(그림 1)에서는 진화하는 DIS 목표 아키텍쳐를 구성하는 빌딩 블럭으로 목표, 아키텍쳐 지침, 적합성 및 구현과 통합 프로그램 사례가 있다.

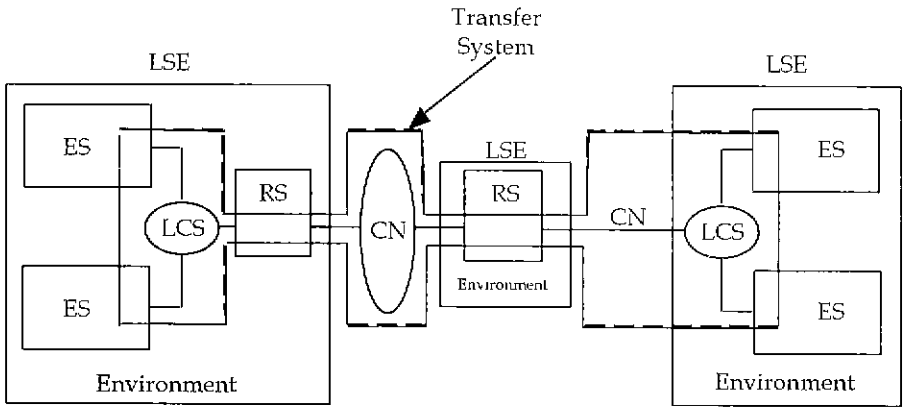
2.2 보안 서비스 및 개념

(1) 정보 시스템에서의 보안 측면

보안을 위하여 DIS 목표 아키텍쳐는 통신망(CN: Communications Network)으로 연결된 LSE (Local Subscriber Environment)로 정의되는 추상적 모델로 단순화될 수 있으며 이는 (그림 2)과 같다. LSE에는 사용자(또는 조직)의 통제하에 있는 모든 장비와 통신 시스템 등이 이에 포함되며 CN은 이러한 LSE로 하여금 정보를 공유토록 하는 통신 능력을 갖고 있다. LSE는 ISO 7498에 규정한 개방형 시스템 및 중계 시스템(RS: Relay System) 그리고 특정 운용환경하의 LCS(Local Communication System)로 구성될 수 있다. 또한 전송(transfer) 시스템에는 종단(End System) 및 중계 시스템에 통합된 통신 프로토콜과 LCS와 CN이 포함된다. LCS는 LSE의 통제를 받지만 CN은 그렇지 않다.



(그림 1) DIS의 빌딩 블럭



(그림 2) LSE의 보안 관점

하나의 LSE에는 워크스테이션과 같은 단일 종단 시스템, 라우터와 같은 단일 중계 시스템 또는 LCS를 경유하여 종단 시스템과 중계 시스템)들이 복잡하게 접속된 형태가 있을 수 있다. 정보 시스템 아키텍처의 모든 구성 성분들은 LSE의 일부이거나 아니면 CN이다. 이러한 보안 관점은 LSE들이 하나의 CN에 의해서만 연결됨을 의미하는 것이 아니라 여러 쌍의 CN들로 접속됨을 의미한다.

(2) 보안 서비스의 할당

DGSA 보안 서비스는 데이터 통신을 위한 ISO 7498-2(ISO, 1989)에 정의된 규정에 기초한다. 이러한 보안 서비스로는 인증, 접근제어, 데이터 무결성, 데이터 기밀성, 및 부인봉쇄가 있다. DGSA에서는 가용성을 기본 보안 서비스로 고려한다. DGSA는 모든 측면의 정보 시스템 보안에 적용되므로, 이러한 기본 서비스는 전송 시스템 뿐만 아니라 전반적인 LSE에도 적용되도록 고려된다.

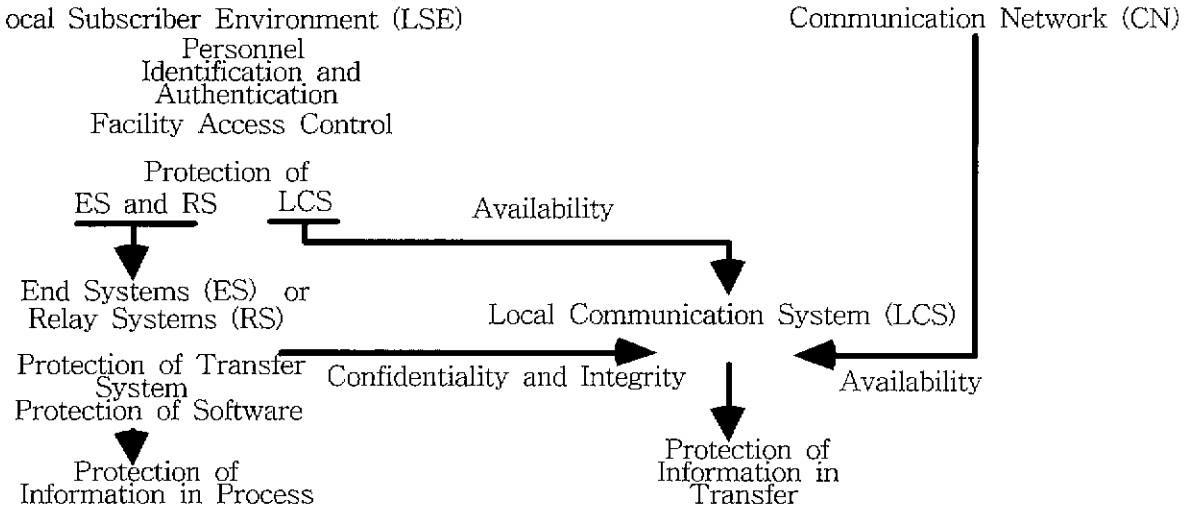
LSE에의 보안 서비스(일차적으로, 신분 확인 및 인증(I & A), 시설에 대한 접근제어) 할당은 원칙적인 기법(즉, 물리적, 관리적, 및 인적)들로 구현된다. 이와 같이 보안 서비스의 할당은 아키텍처 관점에서 이루어 지며, (그림 3)에서는 CN과 LSE 및 이의 구성 성분들에 대한 보안 서비스 할당이 요약되어 있다.

2.3 종단 시스템과 중계 시스템에서의 보안 구조

(1) 종단 시스템 보안 구조의 개괄

보안 서비스는 기본적으로 LSE에 할당되고 또 LSE내의 종단 시스템과 LCS에 할당된다. LSE에서의 보안 서비스는 LSE 내의 종단 시스템을 포함한 모든 자원을 보호하기 위한 것이다. 종단 시스템의 보안 구조에서는 종단 시스템의 하드웨어와 소프트웨어를 보호하기 위해 필요한 보안 서비스가 추가로 정의되어 있다.

LSE에 할당된 보안 서비스는 물리적, 관리적, 인사관리적인 메커니즘으로 구현되어 있다. LSE에 할당된 주요 보안 서비스는 설비에 대한 접근제어와 직원에 대한 인증이며 정보의 기밀성과 무결성을 제공하기 위한 보안 서비스, 시스템의 무결성과 가용성을 제공하기 위한 보안 서비스도 포함될 수 있다. 이러한 LSE 보안 서비스의 주 목적은 하드웨어를 보호하기 위한 것이다.



(그림 3) 보안 서비스의 할당 요약

하드웨어에서의 보안 서비스의 주 목적은 응용이나 운영체제와 같은 소프트웨어를 보호하기 위한 것으로 사용자와 신뢰할 수 있는 소프트웨어 사이에 보호된 통로를 제공한다. 하드웨어에서의 보안을 위해 다음과 같은 메커니즘들이 사용될 수 있다; 방송파 간섭이나 유출을 막기 위한 코팅이나 보호 용기, 시스템의 가용성을 높이기 위한 고장 허용 하드웨어 기능, 다양한 보안 서비스를 제공하기 위한 암호화 하드웨어.

소프트웨어에서의 보안 서비스의 주 목적은 정보를 보호하기 위한 것으로 다음과 같은 기능이 제공되어야 한다; 사용자 인증과 접근 제어, 처리되거나 저장되는 정보의 무결성.

(2) 중요 보안 기능

① 보안 정책 결정 기능(Security Policy Decision Function; SPDF): SPDF는 모든 보안정책 결정을 내리는 책임을 맡고 있으며 모든 종단 시스템 소프트웨어를 보안 정책으로부터 분리한다. 이러한 방법의 중요성은 다음과 같다.

- 다른 보안 정책을 가지는 다수의 정보 도메인을 지원할 수 있다. 이것은 보안 정책은 한 곳에 저장되며 한 가능에 의해서만 해석되기 때문이다.
- 보안 정책을 한 곳에 저장하므로 하나의 정보 도메인을 위한 보안 정책을 설치, 수정하거나 대치하는 것도 용이해진다.
- SPDF의 구현을 바꾸더라도 종단 시스템 소프트웨어의 다른 부분에는 전혀 영향이 없다.

② 인증 기능(Authentication Function): 인증 기능은 종단 시스템이 제공하는 메커니즘을 사용하여 사용자나 종단 시스템을 인증한다. 인증 기능에의 인터페이스는 정보 도메인 보안 정책이나 사용되는 인증 메커니즘과 독립적이다. 사용되는 메커니즘은 정보 도메인 정책에 의해 결정되며 만약 종단 시스템이 여러 개의 정보 도메인을 지원하면 여러 가지의 인증 메커니즘이 필요할 수 있다. 경우에 따라서 인증된 사용자의 신원이 정보시스템들 사이에 전달될 수도 있으며, 필요하다면 인증 메커니즘에 대한 정보도 전달될 수 있다.

③ 감리 기능(Audit Function): 감리 기능은 정보 도메인과 관리 정보 도메인 보안정책에 의하여, 종단 시스템의 여러 기능들로부터 감리 메시지를 받는다. 감리 레코드는 정보 관리 도메인의 일부분인 SMIB(Security Management Information Base)의 일부가 될 수 있다. 감리 기능은 감리 메시지가 분실되지 않고 메시지들 사이의 순서가 보존될 수 있도록 한다. 감리 레코드는 여러 저장 장소로 보내질 수 있으며, 지역적으로 다른 곳에 위치한 중앙 감리 센터에 보내질 수 있다.

④ 프로세스 스케쥴링 기능(Process Scheduling Function): 프로세스 스케쥴링 기능은 어느 프로세스가 언제 또 얼마나 오랫동안 CPU를 사용할 수 있는지를 결정한다.

⑤ 장비관리 기능과 장비 제어기(Device Management Function and Device Controller):
다음과 같은 자원을 관리하는 기능들이 보안 긴급 기능에 포함된다; 메모리 관리 기능, 파일 관리 기능, 디스플레이 관리 기능, 프로세스간의 통신 관리 기능, 암호화 서비스 관리 기능.

2.4 전송 시스템(Transfer System)

전송 시스템은 LCS와 CN과, 종단 및 중계 시스템에서의 통신 프로토콜로 구성되어 있다. 전송 시스템 보안 구조의 주 목적은 정보 공유 및 분산 처리가 가능하도록 전송중의 정보를 보호하는 것이다.

(1) 분산 보안 컨텍스트

포괄적인 전송 시스템 보안 구조에서는 서로 다른 종단 시스템이나 중계 시스템에 있는 보안 컨텍스트 속의 응용 프로그램들이 마치 이들이 같은 종단 시스템이나 중계 시스템에 있는 것 같은, 보안에 대한 확신을 갖고 서로 통신을 하도록 하는 구조를 찾고자 한다. 이러한 구조를 분산 보안 컨텍스트(distributed security contexts)이라 한다. 대화식(interactive)과 단계적 배달식(staged delivery)의 두 종류의 통신에 대해 고려한다. 단계적 배달식이란 근원지 종단 시스템 응용에서 중계 시스템 응용으로 또 다른 중계 시스템 응용으로 최종적으로 목적지 종단 시스템으로 전송이 되는 통신 방식으로, 전자 우편이 대표적인 예이다. 이외의 모든 통신 방식은 대화식 통신이라야 한다.

1) 대화식 통신을 위한 분산 보안 컨텍스트

대화식 분산 보안 컨텍스트는, 다른 종단 시스템에 있는 두 개의 보안 컨텍스트들이 보안 연계(security association)라 불리는 메커니즘들의 집합을 통하여 안전하게 연결될 때 형성된다. 보안 연계란 동일한 정보 도메인을 지원하는 다른 종단 시스템들의 두 보안 컨텍스트을 안전하게 바인드 하는데 필요한 통신과 보안 메커니즘 및 기능들을 말한다. 보안 연계란 OSI에서의 응용 연계의 확장된 개념이다.

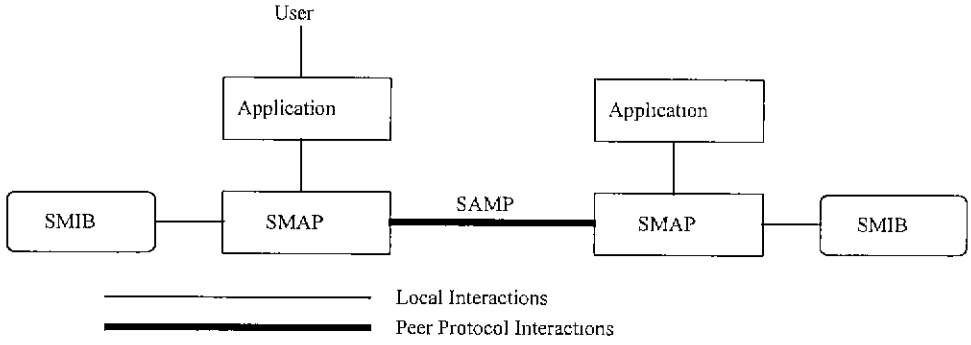
보안 연계에 대한 보안관리 정보는 ASSR(Agreed Set of Security Rules)이라 불리는 SMIB의 자료구조에 저장되어 있다. ASSR은 보안 컨텍스트를 형성하고 관리하기 위해 필요한 모든 보안 속성에 대한 정보를 가지고 있으며, 정보 도메인의 레이블과 암호화 알고리즘 식별자와 암호화 키와 같은 보안통신 속성이 있다. 보안 연계를 지원하는 각 종단 시스템은 국지적인 SAID(Security Association IDentifier)를 선택한다. SAID의 쌍에 의해 특정한 보안 연계가 유일하게 식별되며, 이 보안 연계에 ASSR을 연결시킨다.

보안 연계는 SAMP(Security Association Management Protocol)에 의해 형성된다. 근원지 종단 시스템에서 먼저 SMAP(Security Management Application Process)가 SAMP 구현을 호출하면, 이 SAMP는 목적지 종단 시스템의 SAMP 구현과 OSI 응

용연계를 형성한다. 이 두 SAMP 구현들은 SAMP 교환(exchange)의 집합을 통하여 상호 협동하여 보안 컨텍스트을 형성한다. SAMP 교환이 성공적으로 끝나면, 보안 연계가 형성된다. 목적지 종단 시스템은 적절한 정보 도메인에 대해 보안 컨텍스트을 형성하고, 근원지 종단 시스템에서의 응용 프로그램과 통신을 하기 위해 필요한 응용 프로그램을 수행한다. (그림 4)은 보안 연계를 생성하는 주요 구성 요소들 사이의 관계를 보여 주고 있다.

스에 의존하여야 하는 경우가 발생할 수 있다.

단계적 배달식 분산 보안 컨텍스트의 요구 사항을 만족하는 전자 우편 서비스를 위해서는 SDNS MSP(Message Security Protocol)와 같이 사양이 존재한다. 이 사양은 인증, 접근 제어, 기밀성, 무결성과 부인봉쇄 서비스를 제공한다. 또 하나의 메시지가 여러 수신자에 보내져야 할 때 근원지 종단 시스템에서 이 메시지의 여러 카피를 만들지 않고도, 모든 수신자들에게 전송되도록 하는 서비스를 제공한다.



(그림 4) 보안 연계를 생성하는 구성 요소들의 관계

2) 단계적 배달식 분산 보안 컨텍스트

단계적 배달식 분산 보안 컨텍스트는 근원지 종단 시스템으로부터 목적지 종단 시스템으로 전송된다. 근원지 종단 시스템은 전송될 정보를 암호화하고, 이것이 목적지 종단 시스템으로 전송된 후 목적지 종단 시스템이 원 정보를 복구한다. 가장 이상적인 상황은 근원지 종단 시스템에서의 암호화 과정이 전송되는 정보에 대한 모든 보안을 제공하고, 중계 시스템으로부터 보안 서비스를 전혀 받지 않는 것이다. 만약 공중 통신망 서비스를 사용하는 경우에는 이러한 환경이 제공되어야 한다. 그러나 암호화 과정이 완벽한 보안을 제공하지 못한다면 중계 시스템으로부터의 보안 서비

(2) 전송 시스템 지원

기본적인 전송 시스템의 활동을 지원하기 위해 다음과 같은 사항들이 필요하다.

1) SMAP(Security Management Application Process)

보안 연계와 분산 보안 컨텍스트를 생성 및 종료하고, 전송 시스템에서의 보안 서비스와 메커니즘을 제어하기 위해 SMAP은 다음과 같은 활동을 지원한다.

- GSS-API를 통한 종단 통신 응용 프로그램의 요청
- 추가적인 SMIB 정보 객체의 사용과 유지보수
- 디렉토리 접근 프로토콜을 사용하여 X.500

디렉토리로부터 보안 정보를 검색하고 유지 보수

- 단계적 배달식 보안 메시지를 위한 MSP의 처리
- 대화식 분산 보안 컨텍스트의 형성을 위한 SAMP 수행
- 보안 서비스와 보안 프로토콜 수행을 위한 암호화와 키의 관리
- 보안 정보의 안전한 교환을 위한 CMIP과 같은 일반적인 관리 프로토콜 수행

2) SMIB(Security Management Information Base)

전송 시스템의 수행을 지원하기 위해서 종단 시스템 SMIB과 정보 도메인 SMIB에 추가적인 정보가 필요하다. 정보 도메인 SMIB에는 다음과 같은 정보가 추가적으로 필요하다; SDNS 키 관리 증명서와 같은 적절한 보안 정보를 포함하기 위한 X.509 증명서, 분산 수행을 위한 사용자 접근 제어 정보, 트래픽과 메시지 키, 감리 데이터.

종단 시스템 SMIB에 추가적으로 필요한 정보는 다음과 같다; 키 관리 / 암호화 / 무결성 / 서명 알고리즘의 식별자와 보안 프로토콜 객체, 분산 연산을 위한 종단 시스템의 접근 제어 정보, 암호화 알고리즘의 초기화 정보, 보안 연계의 구성 정보, 손상 행위 정보, 우발 사고에 대한 계획 파라미터.

3) 보안 프로토콜

ISO에는 TLSP와 NLSP 같은 프로토콜이 있다 IEEE 802.10 SILS SDE 프로토콜은 LCS 보안 서비스에 적절하고, 전자 우편에는 DoD의 MSP가 적절하다. 현재는 DGSA의 요구 사항을 만족하는 SAMP가 없다. ISO에서 현재 이를 위한 프로젝트가 진행 중인데 초기 버전은 IEEE 802.10 SILS Part 3에 기초한다. 그리고 GULS SESEP가 SAMP 교환을 위해 사용될 것이다. 현재 많은 보안 프로토콜이 존재하는데 (그림 5)은 이들 프로토콜이 어떠한 보안 서비스를 제공하는지 보여준다.

4) 암호화

분산 보안 컨텍스트의 형성을 위해서는 암호화 메커니즘이 가장 중요하다. DGSA에서는 저렴한 가격의 암호화 장비가 매우 중요한 요소이다. 이 암호화 장비는 다양한 암호화 알고리즘과 키 관리 알고리즘을 지원할 수 있어야 하며 고성능의 워크스테이션과 함께 사용될 수 있으려면, 최소 10 Mbit/sec 정도의 처리 능력을 가져야 한다.

2.5 보안관리

DGSA 보안관리 개념은 ISO에서 표준으로 규정한 보안 프레임웍(7498-2)에서 제시하는 개념을 상당부분 그대로 수용하고 있다.

ISO 7498-2의 8.1.2절에서는 보안도메인에 대해서 기술하고 있다. 보안도메인은 하나의 보안정책을 준수하고 하나의 관리자에 의해 통제되는 개체로 정의되고 있다. 이는 DGSA에서의 정보도메인과 같은 의미로 대체할 수 있다. 단지 프레임웍에서와는 달리 DGSA에서는 정보도메인이 계층적인 관계를 갖지 못하도록 되어있다. 즉 서브셀이나 수퍼셀 개념이 필요없다.

ISO 7498-2의 8.1.2절에서는 보안관리 정보베이스(SMIB: Security Management Information Base)에 대해 기술하고 있다. SMIB는 모든 보안관련 정보의 개념적 저장소이다. SMIB는 분산 정보베이스로서 최종 시스템의 논리적/물리적 그룹에서 일관성있는 보안정책을 수행할 수 있도록 하여준다. 실제로 SMIB는 MIB(Management Information Base)와 통합될 수도 안될 수도 있다. DGSA에서는 SMIB를 정보도메인과 최종시스템 관리를 수행하기 위해 사용한다.

특정 정보도메인을 관리하기 위한 SMIB에는 다음과 같은 내용의 정보객체가 포함될 것이다; 정보도메인 보안정책 규칙, 사용자 등록정보, 사

Security Services	Protocol Layer 7	4	3	2	1
Peer Entity Authentication	Y	N	N	N	N	N
Data Origin Authentication	Y	Y	I	I	I	I
Access Control	Y	Y	Y	Y	N	N
Connection Confidentiality	P	N	Y	O_1	O	N
Connectionless Confidentiality	N	Y	N	O_2	N	N
Selective Field Confidentiality	N	N	N	N	N	N
Traffic Flow Confidentiality	N	N	N	N	N	Y
Connection Integrity with Recovery	N	N	O_1	O_1	N	N
Connection Integrity without Recovery	N	N	O_1	O_1	O	N
Selective Field Connection Integrity	N	N	N	N	N	N
Select Field Connectionless Integrity	N	N	N	N	N	N
Connectionless Integrity	N	N	N	Y	N	N
Non-Repudiation (Proof of Origin)	N	N	N	N	N	N
Non-Repudiation (Proof of Delivery)	N	N	N	N	N	N

Call Legend:

Y	Yes, the service is supported by the security protocol
N	No, the service is not supported by the security protocol
I	The service is implicitly provided, based on unique key
O	The service is optionally provided
O_1	Connection-oriented service option
O_2	Connetionless service option
P	The service is provided only for parts of the last protocol exchange

(그림 5) DGSA 보안 프로토콜과 보안 서비스

용자 인증 기준, 사용자 인증 정보, 사용자 속성(권한, 예: 접근권한, 도메인간 전송허용 권한 등), 가시적인 보안레이블 정보, 특정 응용시스템(도메인내와 도메인간의 정보전송을 포함한)을 위한 보안서비스와 메커니즘 요구사항.

최종 시스템 SMIB에는 다음과 같은 내용의 정보객체가 포함될 것이다: 최종 시스템 보안정책 규칙, 보안서비스 관리정보, 보안메커니즘 관리정보, 지원 서비스와 메커니즘 관리정보(예: 경보보고, 정보시스템 감리, 암호키 분배, 보안기능, 최종시스템에서 작동되는 보안관련 응용시스템).

ISO 7498-2의 8.1.5절에서는 보안관리정보의 통신에 대해 보안관리 프로토콜과 통신채널이 취약할 수 있으며 이를 위한 정보보안 조치가 필요하다고 서술하고 있다. 각 보안관리 정보는 각각의 관리정보도메인에서의 보안정책에 의거하여 보호되어야 한다.

ISO 7498-2의 8.1.6절에서는 다양한 시스템 관리자사이에 보안관련 정보가 교환되어 SMIB가 구축되거나 확장될 수 있어야 한다고 기술하고 있다. 어느 경우에는 보안 정보가 OSI가 아닌 통신회로를 통해 전송되거나 OSI에서 규정하지 않

은 비표준적인 방법으로 SMIB를 갱신할 수도 있다. SMIB 갱신을 위해서는 보안관리자의 사전 승인을 받을 필요가 있다. DGSA는 이 견해와 일치하며 DGSA의 분산 보안관리의 기초로 사용하고 있다. 각각의 관리 정보도메인은 관리 대상인 정보도메인의 SMIB를 사용하고 유지보수한다. 보안관리자는 SMIB를 유지보수하기 위해 OSI 또는 비OSI통신을 사용할 수 있다.

ISO 7498-2의 8.1.7절에서는 보안관련 정보의 교환을 위한 보안관리 응용 프로토콜을 요구하고 있다. ISO에서 정의하고 있는 일반 관리 응용 프로토콜은 CMIP(Common Management Information Protocol)이다. GULS(General Upper Layer Security) SESEP(Security Exchange Service Element Protocol)는 현재 국제표준초안(DIS, 1993)이다. GNMP(Gov't Network Management Profile, NIST, 1992)는 미정부 개방시스템 상호접속 프로파일(GOSIP)에 의해 반드시 준수되도록 규정되어 있다. GNMP는 특정 프로토콜을 명시하고 있지는 않지만, SNMP(Simple Network Management Protocol)와 CMIP를 공히 참조하고 있다. 현재는 SNMP v.2와 CMIP이 최선의 선택이지만 GULS SESEP은 미래에 중요한 도구가 될 수 있을 것이다.

ISO 7498-2의 8.2.1절에서는 아래와 같은 활동을 전형적인 보안관리 기능에 포함시키고 있다; 전반적인 보안정책관리(갱신, 유지보수 포함), 다른 OSI 관리기능과의 상호작용, 보안서비스 관리와 보안 메커니즘관리와의 상호작용, 사건 처리 관리, 보안 감리 관리, 보안 복구 관리. DGSA에서는 이러한 최종 시스템 보안관리의 개념을 전체 개방시스템 환경으로 확장시켜 여러 정보도메인을 지원할 수 있도록 하였다.

ISO 7498-2의 8.2.2절에서는 특정 보안 서비스의 관리에 관한 것으로 다음과 같은 전형적인 활동들을 포함하고 있다; 보안 서비스 정도의 결정과 할당, 요구된 보안 서비스를 제공하기 위한 보안 메커니즘의 선택 규칙의 작성 및 유지보수, 가용한 보안 메커니즘에 대한 타진, 보안 메커니즘의 개시, 보안 서비스 관리기능과 메커니즘 관리기능간의 상호작용 명시.

ISO 7498-2의 8.2.3절에서는 보안 메커니즘 관리를 특정 보안 메커니즘의 관리에 관한 것으로 다음과 같은 전형적인 활동들을 포함하고 있다; 키 관리, 암호화 관리, 디지털 서명 관리, 접근제어 관리, 데이터 무결성 관리, 인증 관리, 트래픽 패딩 관리, 경로제어관리, 공증 관리. DGSA는 이 목록을 채택하고 있으며 여기에 가용성 관리를 추가하고 있다.

3. 결 론

미 국방부가 발표한 정보관리를 위한 기술 아키텍처(TAFIM)중 목표보안 아키텍처(DGSA)는 핵심부분을 이루는 것으로서, 주요 보안개념, 기능 및 구조를 명시하고 있으며 이를 통해 특정 시스템의 보안 아키텍처를 설계할 때 지침으로 사용될 수 있도록 하기 위한 문서이다. 목표보안 아키텍처를 제시하므로써 미 국방부가 추구하는 개방시스템 환경으로의 전환을 가능하게 하며 이 결과, 시스템간의 상호운영성과 통합성, 소프트웨어의 이식성/재사용성 등의 효과를 볼 수 있다.

한국의 국방부에서는 현재 이와 같은 기술 아키텍처 및 보안 아키텍처의 개발이 없이 단편적인 시스템 개발을 해왔기 때문에 상호운영성이나 통합성에서 여러 문제를 내포하고 있다. 지금부터라도 효과적인 국방 정보시스템 구축을 위해서 기술 아키텍처 및 보안 아키텍처를 개발할 필요가 절실하다고 사료된다. 본 연구가 이러한 노력에 참고자료로서의 가치를 가질 것으로 예상된다.

참고문헌

[1] Kowalski, Stewart, "Cybernetic Anaysis of National Computer Security, " Jounal of Computers & Security, Vol.10, 1991, pp.217.

[2] U.S. Department of Defense, DoD 5200-28(D), Mar. 21, 1988.

[3] U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 73; Guidelines for Security of Computer Applications, Jun. 30, 1980.

[4] U.S. White House, Executive Order 12355, Apr. 1, 1982.

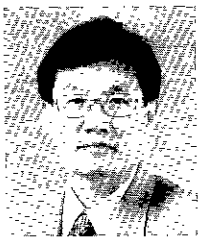
[5] beta.missilab.com:9000/

[6] csrc.ncsl.nist.gov/

[7] www.arpa.mil/

[8] www.disa.mil/

[9] www.ito.darpa.mil/



김 정 덕

1975년 연세대학교 정치외교학과 (학사)
1979년 연세대학교 경제학과 대학원 (석사)
1984년 Univ. of S. Carolina, 경영대학원 (MBA)
1986년 Texas A&M University, MIS (박사)
1991년-1993년 한국전산원 표준연구본부 선임연구원
1995-현재 중앙대학교 산업정보학과 부교수
관심분야 : 정보관리, 위험분석, 비즈니스 지속성 계획, 경영정보시스템 계획 및 평가

심 영 철

1975년 서울대학교 전자공학과 (학사)
1979년 한국과학기술원 전기 및 전자과 (석사)
1984년 Univ. of California, Berkeley 전산학 (박사)
1981년-1984년 삼성전자 컴퓨터 사업부
1991년-1993년 Univ. of California, Berkeley 연구원
1993년-현재 홍익대학교 컴퓨터공학과 조교수
관심분야 : 컴퓨터와 통신망 관리, 네트워크 컴퓨팅, 소프트웨어 공학