通信情報保護學會誌
第7卷 第2號, 1997. 6

국가 전산망을 위한 MISSI 분석

이 철 원*, 김 학 범*, 이 경 구*, 홍 기 웅*, 심 주 걸*

요 약

본 고에서는 행정, 교육, 과학기술, 금융, 국방, 공안, 외교 및 물류 등의 전산망을 위한 통합적인 보안 해결책 및 초고속정보통신망을 위한 보안 해결책을 제시하기 위한 일환으로 미국 NSA가 주도하여 수행하고 있는 MISSI에 대하여 소개를 한다. MISSI는 다중등급 보안을 근간으로 하고 있으며 무결성, 사용자 신분확인, 부인봉쇄, 비밀성 및 가용성 등의 보안 서비스를 제공하고 있다. 이들 보안 서비스를 위하여 Firewall, Fortezza, Guard 및 안전한 컴퓨터와 같은 상용의 보안 제품을 사용할 수 있도록 하고 있다. 본 고는 국가 전산망 및 초고속정보통신망의 효과적인 보안 해결책으로써의 지침을 제공해 주리라 생각된다.

1. 서 론

단일 컴퓨터 사용환경에서 컴퓨터와 통신을 이용한 정보처리 환경으로 변화해감에 따라 국내 외에서는 초고속정보통신기반 구축 등의 정보화 사회로의 촉진을 유도하고 있다. 우리나라에서도 정보화 촉진 및 정보보호를 위하여 지난 '95년 정보화촉진기본법을 제정하여 시행하고 있으며 이를 기반으로 하여 행정, 교육, 과학기술, 금융, 국방, 공안 및 물류 등의 정보화를 위한 정보화추진분과위원회를 설치하였다. 각 분과별로 해당 국가 전산망에 대한 관리, 설치 및 운용을 하고 있으며 개개의 망을 정보 고속도로화(Information Superhighway)하기 위한 노력을 계속해오고 있다. 조만간 모든 사람들이 시간과 공간의 제약 없이 다양한 정보통신 서비스를 받을 수 있으리라 예상이 되며 21세기 고도 정보화 사회로의 전환 및 국가 경쟁력과 국민 삶의 질적 향상 등이 이루어질 것이라 보여진다. 이러한 시점에서 개인과 조직이 가지고 있는 정보를 안전하게 저장, 검색 및 관리할 수 있는 보안 기술이 국가적 또는 사회적으로 요구되고 있다. 사실상 정보시스템 보안에는 컴퓨터에서 생성, 처리, 저장 및 통신되는 정보의 무결성, 인증, 가용성, 그리고 프라이버시의 보호 등이 포함된다 [1].

또한 오늘날과 같이 각 국가기관별로 전용의 전산망을 구축 운영하고 있는 상황에서 각 전산망의 효율적인 운영을 위하여 분리된 개개의 전산망을 통합된 하나의 전산망으로 구축 운영하려는 시도가 미국을 중심으로 하여 이루

* 한국정보보호센터

어지고 있다. 이 경우, 통합된 전산망에 서로 다른 등급의 정보가 저장, 처리 및 송 수신될 수 있으므로 이를 효과적으로 통제하고, 선택적으로 분배할 수 있는 기능은 필수적이라 하겠다. 이와 같이 서로 다른 다중의 보안등급을 가진 정보를 처리할 수 있도록 하는 것이 다중등급보안(MLS, Multi Level Security)이며 MISSI(Multilevel Information System Security Initiative)는 위와 같은 요구사항 및 현재 구축중인 미 국방부 초고속망(DII, Defense Information Infrastructure)을 위한 보안 해결책을 제공하고자 NSA(National Security Agency)가 주도가 되어 구축하고 있는 프로젝트의 명칭이다. 이것은 국방분야 뿐만 아니라 보안을 필요로 하는 기관의 주요 요구사항이며, 현재 미국은 MISSI의 사용자 요구사항을 병합하고 계속하여 그 기능을 향상시키고 있다 [2].

우리나라도 행정, 교육, 과학기술, 금융, 국방, 공안 및 물류 등의 전산망을 운영하고 있으며 초고속 정보통신망의 구축을 추진하고 있다. 이와 같은 시점에서 현재 미국에서 추진중인 통합 전산망 보안 해결책인 MISSI를 고찰하고 여기에 적용된 기술을 소개하여 우리나라의 초고속 정보통신망을 위한 보안 기술의 참고자료로 제공하고자 하는 것이 본 고의 목적이다.

본 고의 2장에서는 MISSI 및 제품군의 소개를 3장과 4장에서는 MISSI를 이용한 보안 해결책의 예제 및 MISSI의 보안 엔지니어링 방법론에 대하여 기술하며 5장에서 결론을 맺는다.

2. MISSI

개별적으로 구축 운영되고 있던 미 국방부 내의 정보 처리시스템을 통합하여 하나의 효과적인 전산망으로 구축하기 위한 전제조건인 다중등급 비밀정보를 동일한 전산망 내에서 처리하기 위한 해결책으로 MISSI가 제안되었다. 초기의 MISSI는 국방부 메시지 시스템(DMS : Defense Message System), 통합 전술 전략 디지털 전산망(ITSDN : Integrated Tactical and Strategic Digital Network) 그리고 1995년 시작된 최고사령부(CINC : Command IN Chief)의 다중등급 정보처리와 같은 요구사항을 처리하기 위한 사용자 요구조건을 만족시키는 것이 목적이었다. 그러나, 미 국방부 독자의 초고속망을 구축하면서 MISSI의 목적은 국방 초고속망을 기반으로 하는 다양한 업무들간의 상호운용상의 안전성을 제공하는 것으로 발전되었다. MISSI 보안 해결책은 사용자 특정 환경에 대한 위협으로부터 적절한 보안을 제공한다. 다양한 형태의 워크스테이션, 네트워크 보안 표준 및 공통의 보안관리 기반(Common security management infrastructure)을 통하여 MISSI는 사용자에게 다양한 정보처리 시스템의 보안을 제공한다. 제공되는 보안에는 송 수신되는 데이터의 검증, 강한 인증, 암호화, 디지털 서명 같은 보안 서비스가 포함된다. MISSI 표준은 대부분의 상용 컴퓨터 및 네트워킹 기술과 호환이 되도록 설계되었다. 예를 들어, 전자우편, 월드와이드웹(WWW, World Wide Web) 파일 전송, 원격 로그인 및 데이터베이스 관리 등과 같은 응용 프로그램에 적용될 수 있다 [2][3].

(그림 1)에서는 현재의 미 국방부 정보통신 시스템 환경을 (그림 2)에서는 향후의 미 국

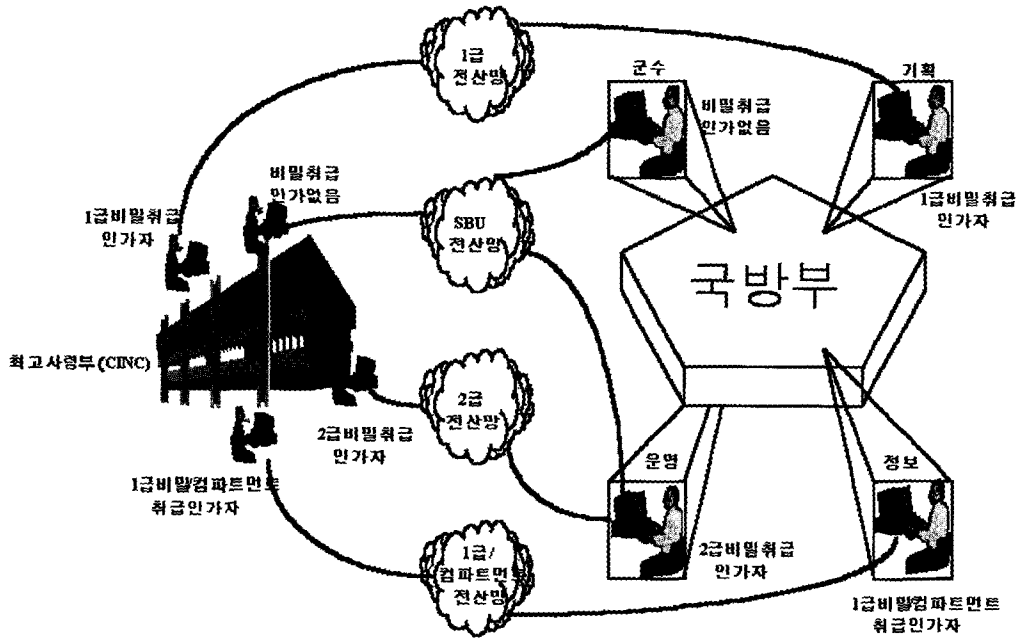

그림 1 현재의 미 국방부 네트워크

방부 정보통신 시스템 환경의 예를 보여주고 있다. (그림 2)의 DISN은 국방 정보시스템 네트워크(Defense Information System Network)를 의미한다.

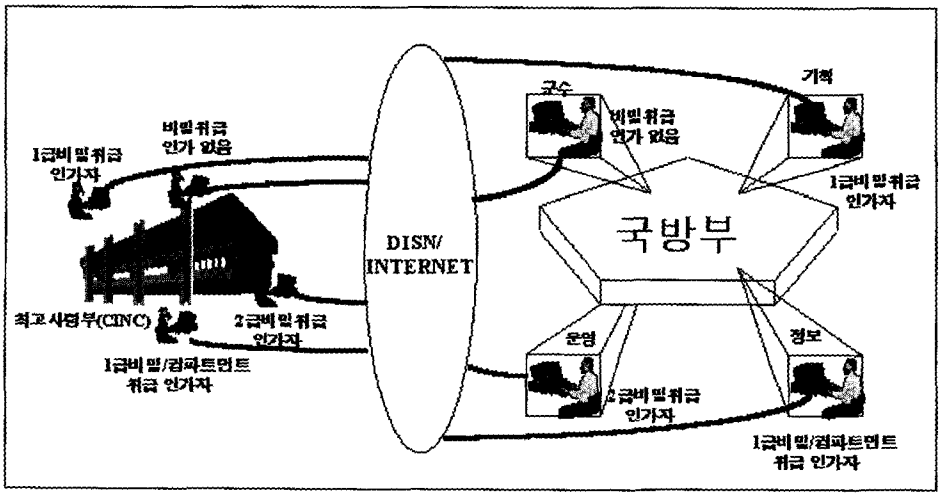

그림 2 향 후의 미 국방부 네트워크

현재의 미 국방부 네트워크 환경은 국방부와 최고사령부(CINC)내의 각 부서간의 보안 등급별 전용회선이 사용되고 있으며, (그림 1)에서 보는 바와 같이 2급의 신원허가를 가진 사용자는 2급 네트워크를 통하여 국방부내의 2급 취급 권한을 가진 사용자와만 통신을 할 수 있다. 그러나, 향후의 미 국방부 네트워크 환경에서는 전용회선망을 없애고, 인터넷 및 국방 초고속망과 같은 통합된 하나의 기반망을 이용하여 사용자간의 메시지 송 수신 등을 지원할 예정이다. 여기에서는 사용자 보안 정책에 기반을 두는 워크스테이션간의 상호 연결을 제공하며 개개의 워크스테이션에 다중등급 데이터 처리 기능을 부여하여 기존과 같은 데이터의 보안등급별 처리에 따르는 불편함을 해소할 예정이다.

MISSI의 또 다른 특성은 개별적으로 또는 서로 결합되어 여러 다른 사용자의 요구를 만족시킬 수 있는 유연성이다. MISSI의 가장 중요한 특성은 새로운 요구사항이 확인되고, 기술이 발전함에 따라 지속적으로 그 기능이 변경된다는 것이다.

가. 미 국방 초고속망과 MISSI

MISSI는 MISSI를 구성하고 있는 제품과 공통의 보안관리 기반으로 구성된 통합적이고 응집력 있는 구조를 통하여, DII 구성요소를 위한 혁신적이고, 상호 운용성이 있는 보안 해결책을 제공한다. 다음의 (그림 3)은 MISSI에서 제공하고 있는 보안 서비스 및 미 국방 초고속망과의 관계를 나타내고 있다.

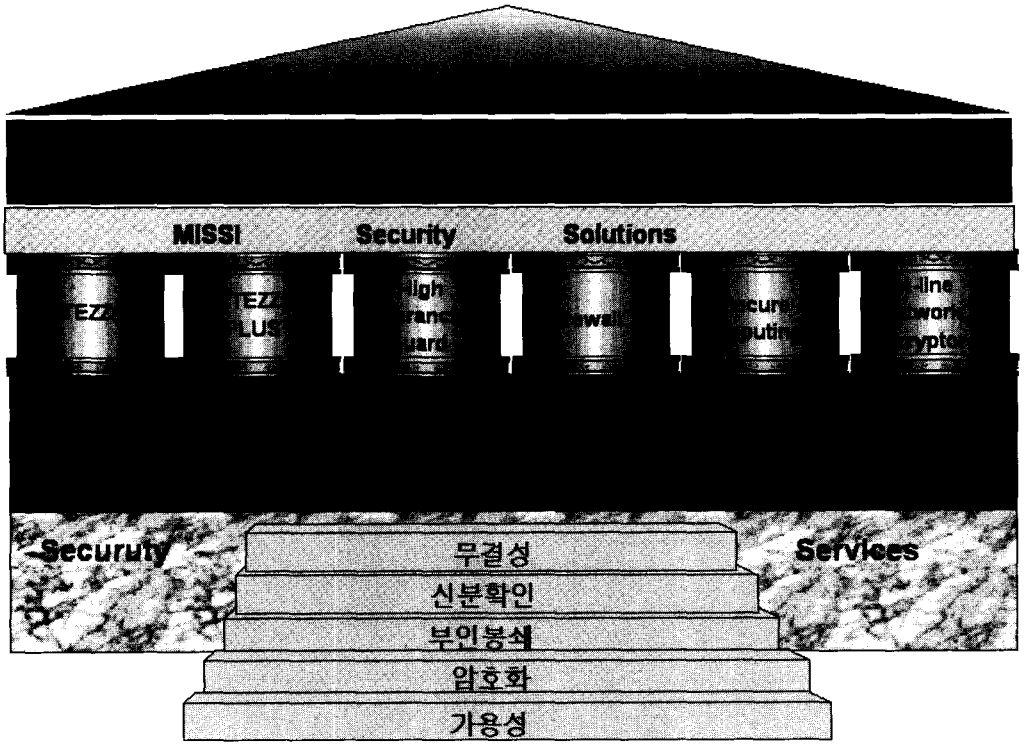

그림 3 MISSI의 보안 해결책

1) MISSI의 보안 서비스

- 무결성(Integrity)
  : 전송 또는 컴퓨터에서 데이터를 처리하는 도중에 변경이 발생하지 않음을 보증
- 신분확인(I&A : Identification & Authentication)
  : 수표의 서명이나 은행 카드의 PIN (Personal Identification Number)과 유사하게 트랜잭션의 발신처를 검증
- 부인봉쇄(Non-repudiation)
  : 은행의 전송과 같은 트랜잭션에서 트랜잭션에 참여한 송 수신자 양자의 부인 봉쇄
- 비밀성(Confidentiality)
  : 데이터의 전송 또는 컴퓨터에서 데이터를 처리중 전송되는 데이터를 스크램블링하는 것과 같은 방법으로 데이터를 암호화하여 프라이버시를 보장
- 가용성(Availability)
  : 데이터의 전송 또는 컴퓨터 처리시스템이 허가된 사용자의 사용을 보장

위 (그림 3)에서 DMS는 국방메세지 시스템(Defense Message System), GCCS는 광역명령통제 시스템(Global Command and Control System), GCSS는 전투지원 시스템(Global Combat Support System)을 DFAS는 국방부 재정 회계 서비스 시스템(Defense Finance and Accounting Service)을 의미한다.

나. MISSI를 구성하는 제품군

MISSI를 구성하는 제품군(그림 4)은 정부와 계약한 개발자들과 정부의 보안표준을 따르는 상업적인 벤더가 제공한다. 제품은 크게 다음과 같이 분류된다.

- 워크스테이션 보안 제품 : 이 제품은 워크스테이션의 보안 서비스를 제공하는 Fortezza 암호화 PC 카드 및 이를 이용한 응용 프로그램을 포함한다.
- Fortezza 응용 프로그램 : Fortezza 보안 서비스를 호출하는 상업적으로 이용가능한 사용자 소프트웨어이다
- 시스템/국지영역 보안 제품(System /Enclave Security Products) : 이 제품은 보통 국지 영역 내에 상주하며 국지영역과 외부망간의 액세스 제어와 암호화 서비스를 제공한다.
- 안전한 컴퓨터(Secure Computing) 제품 : 여기에는 정보의 비밀성 레이블을 지원하고 허가되지 않은 사용자에게 고의적 혹은 우연하게 정보가 유출되는 것을 막는 고도의 신뢰성을 가진 컴퓨터 운영체제와 응용 프로그램이 포함된다. 이러한 보안능력은 국지영역의 보안을 강화시킨다.
- 보안관리기반(SMI : Security Management Infrastructure) 제품 : 이 제품은 망의 보안관리를 지원하고 전자 키 생성과 분배, 사용자 인증표의 발행, 사용자 디렉토리의 관리, 그리고 사용자 권한 취소 등과 같은 서비스를 수행한다.

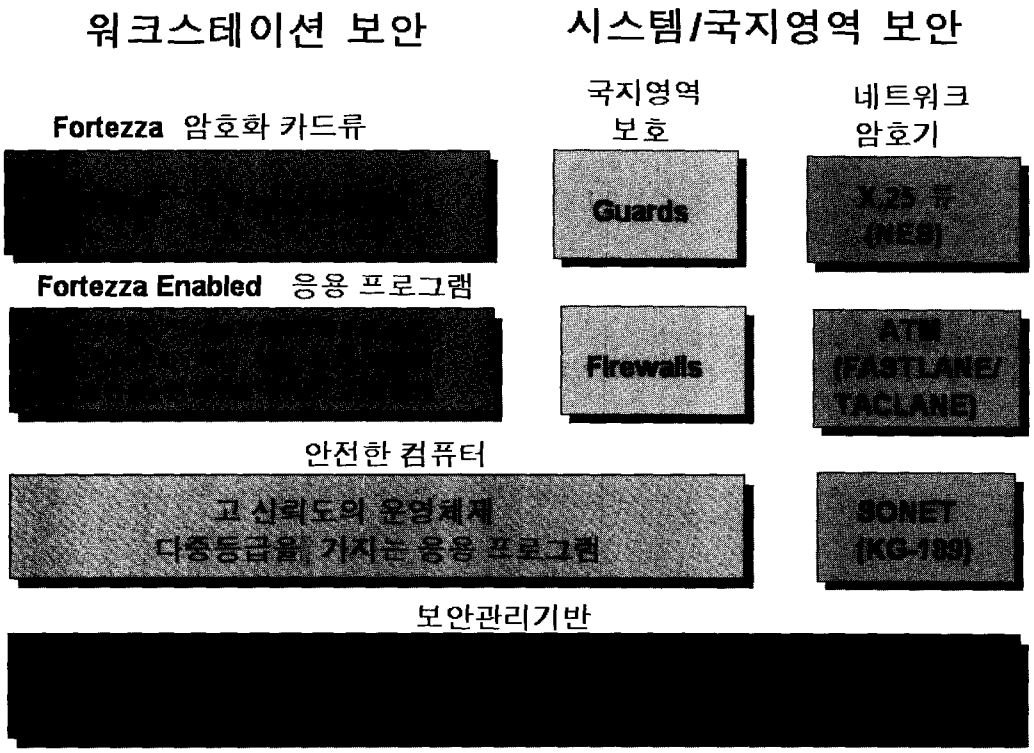

그림 4 MISSI의 제품분류

위 (그림 4)에서 NES(Network Encryption System)는 네트워크 암호 시스템으로 X.25 계층이나 IEEE 802.3 계층에서의 패킷을 암호화하는 장비이며 FASTLANE/TACLANE은 ATM 링크 암호화 시스템으로써, FASTLANE은 ATM에서 정보를 전송하는 형태인 셀을 암호화하는 장비로 멀티미디어 응용 프로그램을 위한 고속이며 투명한 보안 서비스를 제공하며 TACLANE은 ATM/IP를 기반으로 하는 전술 네트워크에서 다중등급 보안을 제공하는 장비이다. KG-189는 SONET(Synchonus Optical Network)과 호환 가능한 암호기이다.

다. MISSI 제품군의 개요

1) 워크스테이션 보안 제품

① Fortezza 카드

Fortezza 암호화 카드는 개인 사용자를 위한 개인용 보안 토큰이다. 카드 크기는 두꺼운 신용카드 크기이며 국제 PC 카드 표준(PCMCIA : Personal Computer Memory Card International Association)에 따라 구축된다. Fortezza 암호화 카드는 여러 업체에서 생산하고 있으나 기능적으로는 동일하다. MISSI SMI는 Fortezza 암호화 카드의 초기화를 지원한다. 초기화된 카드는 사용자 신분에 대한 효과적인 인증 및 액세스 권한을 제공한다 [4].

Fortezza 응용 프로그램과 결합된 Fortezza 카드는 비밀로 분류되지는 않았지만 비밀에 준하는(SBU : Sensitive But Unclassified) 데이터를 보호하기 위한 적절한 보안 서비스를 제공한다. 여기서, SBU란 비밀로 분류되지는

않았지만 이 정보의 누출이 국가안보에 영향을 미치는 즉, Type II로 분류된 정보를 의미한다. Fortezza 카드는 다음과 같은 특성을 가지고 있다.

- LAN 또는 WAN 환경하의 상업용 워크스테이션에서 사용되는 SBU 데이터의 보호
- 신분확인, 비밀성, 데이터 무결성, 부인봉쇄 서비스 제공
- 다양한 워크스테이션 운영체제(DOS/Windows와 UNIX)를 지원

Fortezza 보안 서비스에 대한 액세스는 PIN, Fortezza 암호화 카드, 그리고 카드의 서비스를 호출할 수 있는 하드웨어 혹은 소프트웨어 응용 프로그램을 필요로 한다. Fortezza 응용 프로그램에는 전자우편, 전자상거래/전자문서교환, 파일저장, 원격 DB 액세스, 월드 와이드 웹 브라우저 및 원격의 사용자 인증 등의 응용 프로그램이 포함된다.

② Fortezza Plus

Fortezza Plus는 강력한 암호화 방법을 이용하여 비밀로 분류된 사용자의 정보를 보호한다. Fortezza Plus는 Fortezza 카드를 보완한 것으로서 1급비밀(Top Secret)로 분류된 정보까지를 암호화하는데 사용할 수 있다. Fortezza Plus는 SNS(Secure Network Server)와 같은 보안 능력에 대한 신뢰성이 매우 높은 Guard와 같이 사용되는데 이때 Fortezza Plus는 정보를 암호화하는데 사용된다. 서로 다른 등급의 비밀로 분류된 정보를 처리하기 위한 Fortezza Plus의 사용은 시스템내의 다른 구성요소의 보안 제약점에 영향을 받는다 [4].

③ 하드웨어 플랫폼과 운영체제

Fortezza 암호화 카드와 카드 인터페이스 소프트웨어 드라이버는 대부분의 PC, UNIX 및 대형급 플랫폼과 운영체제에 쉽게 통합될 수 있다.

④ Fortezza 응용 프로그램

사용자를 위한 응용 프로그램을 수행하기 위하여 Fortezza 카드는 Fortezza 응용 프로그램과 상호 연동이 되어야 한다. 이러한 응용 프로그램(예, 전자우편)은 정부에서 개발하였거나 혹은 상업용으로 개발된 것중의 하나이며 이 응용 프로그램들은 Fortezza 보안 특성을 사용 및 인터페이스하기 위하여 수정되었다. Fortezza 카드와 함께 사용될 수 있는 전자우편과 같은 많은 응용 프로그램 즉, Fortezza 응용 프로그램이 개발되고 시험되어진 후 Fortezza 응용 프로그램에 추가된다. 주요 Fortezza 응용 프로그램에는 다음과 같은 것이 포함된다 [4].

- 전자 메세지(Electronic messaging) : Fortezza는 메세지 암호화, 인증 및 데이터 무결성을 제공하여 전자우편, 전자문서교환, 전자상거래 및 모사전송(FAX)을 안전하게 할 수 있다.
- 월드 와이드 웹 : Fortezza는 강한 인증 및 안전한 소켓계층과의 상호작용을 이용하여 WWW 트랜잭션을 안전하게 보호할 수 있다.
- 액세스 제어 및 강한 인증 : Fortezza는 PIN을 이용하여 강한 인증을 제공하며 강력한 액세스 제어를 제공하기 위하여 디지털 서명을 사용한다.
- 파일과 메디아 암호기 : 이것은 저장매체내의 사용자 파일을 안전하게 하기 위하여 Fortezza 를 사용할 수 있다.

- 원격의 DB 액세스(Remote DataBase Access) : 데이터베이스 응용 프로그램에 강한 인증을 적용함으로써, Fortezza는 강력한 액세스 제어 및 원격지와의 안전한 상호작용을 제공할 수 있다.

⑤ Fortezza 클라이언트-서버 해결방법

클라이언트-서버 환경의 사용자는 그들의 보안 요구를 위하여 Fortezza의 장점을 취할 수 있다. Fortezza 개발자는 특권이 있는 사용자 클라이언트가 안전한 방법으로 국방부 사무관리 시스템(예, 급여) 서비스에 로그인할 수 있도록 Fortezza 응용 프로그램을 작성할 수 있다. 다양한 서버/데이터베이스 시스템과의 상호 운용성의 최대화 및 향후의 성능개선 등을 위하여 응용 프로그램 개발 과정 중에 국가 및 국제 표준을 이용한다.

⑥ 전자상거래/전자문서교환(EC/EDI)

안전한 전자상거래 및 전자문서교환에 대한 요구가 증가함에 따라 Fortezza 개발자는 ANSI X.12 EC/EDI 표준과 Fortezza를 통합하고 있다. 이것은 정부와 정부를 상대로 하는 일반 민간 사업자 사이의 트랜잭션 인증, 무결성 및 비밀성을 제공한다.

⑦ 국방부 메세지 시스템(DMS : Defense Message System)

Fortezza는 DMS를 위한 워크스테이션상의 전자 메시지를 위한 보안을 제공한다. Fortezza는 DMS X.400 전자우편 응용 프로그램 및 DMS X.500 디렉토리 시스템과 상호 작용한다.

2) 보안관리 기반(SMI : Security Management Infrastructure)

MISSI 보안관리 기반은 모든 MISSI 제품군들을 위한 공통의 보안 지원 기반을 제공한다. SMI 능력은 다음의 것들을 통하여 제공된다(그림 5). SMI는 미 국방부 전자적 키관리 시스템과 호환성이 있으며 키관리 서비스를 지원받는다 [2].

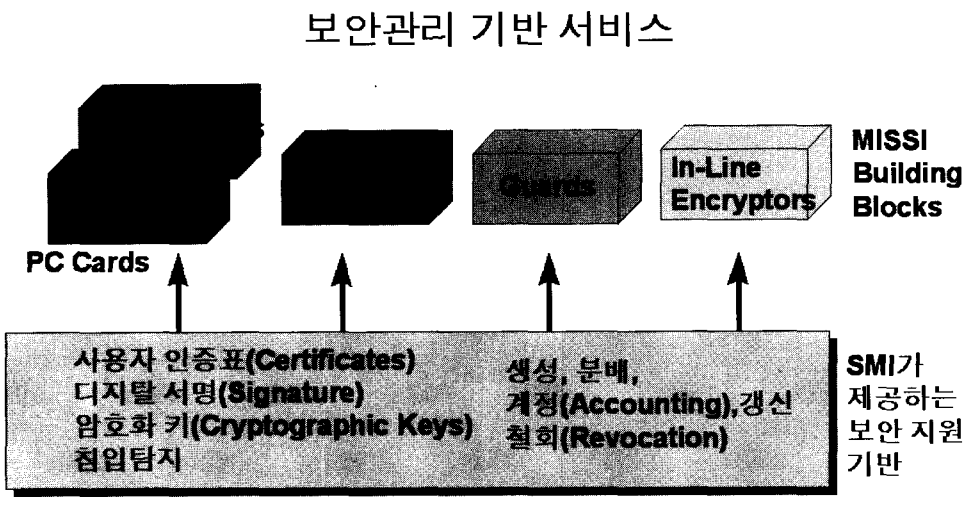

그림 5 MISSI 보안관리 기반

● CAW(Certification Authority Workstation)

: 신뢰성이 있는 운영체제를 가지고 있는 상용의 워크스테이션으로 특수한 목적의 응용 소프트웨어를 가지고 있다. CAW는 보편적으로 국지 시스템 내에 상주하며 보안 인증표(Security certificates), 신임장(credentials) 및 암호화 키를 포함한 사용자 보안 특성을 가진 Fortezza 암호화 카드를 관리한다.

● 디렉토리 시스템 에이전트(DSA : Directory System Agent)

: 전체적인 사용자 명(즉, Distinguished Name)을 제공하기 위하여 필수적인 것으로 DSA는 MISSI 제품들의 운영을 위해 필수적인 공개 보안정보 예를 들어 사용자의 X.500 인증표의 저장소를 제공한다.

● 메일 리스트 에이전트(MLA : Mail List Agent)

: 전자우편 메시지가 다수의 수신자(E-Mail list explosion)에게 전송될 때 사용되는 것으로 안전한 전자우편의 사용자 확장을 위하여 MLA에 보안이 첨가된다.

● 감사 관리자(Audit Manager)

: MISSI 제품과 관련한 보안관련 감사대상 사건의 수집 및 분석을 제공한다. 감사대상 사건의 예는 반복된 사용자 로그인 실패 등이 있다.

3) 안전한 컴퓨터(Trusted Computing)

안전한 컴퓨터는 컴퓨팅 환경의 전체 보안을 향상시키기 위해 보안 특성과 보증이 첨가된다. 보안 특성의 예로는 데이터 레이블링, 데이터

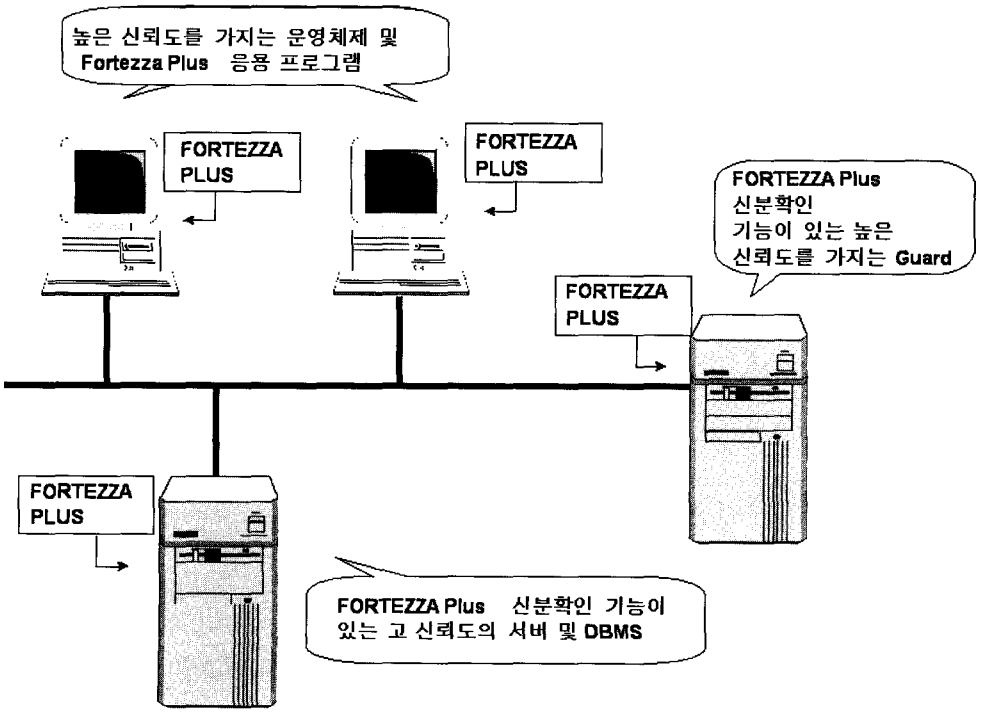

그림 6 안전한 컴퓨터와 Fortezza류의 조화

분리, 액세스 제어 리스트, 데이터 무결성, 보안 관련행위 감사 및 PC Card cryptographic invocation check 등이 있다. 보증은 특정한 설계 및 시스템 보안에 중요한 기능이 제대로 수행되는 지의 여부에 대한 신뢰도를 얻고 시스템 보안에 해로운 비밀통로(Covert channel)와 같은 숨겨진 기능이 제거 혹은 최소화되었는지를 알아보기 위해 취하는 설계 분석활동을 의미한다.

안전한 컴퓨터는 위에서 열거된 바와 같은 특성 및 보증을 가지는 다수의 신뢰성 있는 상용 UNIX의 운영체제를 포함한다. 또한 안전한 컴퓨터는 증가된 보안 능력을 가진 신뢰성 있는 데이터베이스 관리 시스템도 포함한다.

워크스테이션에 Fortezza/Fortezza Plus와 높은 보증을 가지고 있는 컴퓨팅 요소를 집적시켜 놓으면 데스크 톱 형태의 컴퓨터 사용자에 높은 보안을 제공할 수 있다. 이것은 외부에서 내부영역으로의 위협뿐 아니라 내부사용자에 의한 위협이 주는 취약성을 감소시킨다.

4) 보안정책 시행방법

① High Assurance Guard

High assurance guard는 비밀영역내의 비밀로 분류되지 않은 정보의 배포는 허용하면서 비밀로 분류된 정보의 불법적인 노출을 방지하기 위한 보안정책 Enabler이다. 이 다중등급 보안(MLS) 능력은 보호된 영역에 대한 외부의 액세스 요청을 허가해 주며 불법적인 공격을 막는다. Guard는 국지영역내에서 Fortezza로 보호된 워크스테이션에 대한 보안 서비스 요청을 보장하며 정보의 레이블링에 대한 자동 체크도 가능하다. MISSI Guard의 예로는 SNS(Secure Network Server)가 있다 [2].

② MISSI Firewall

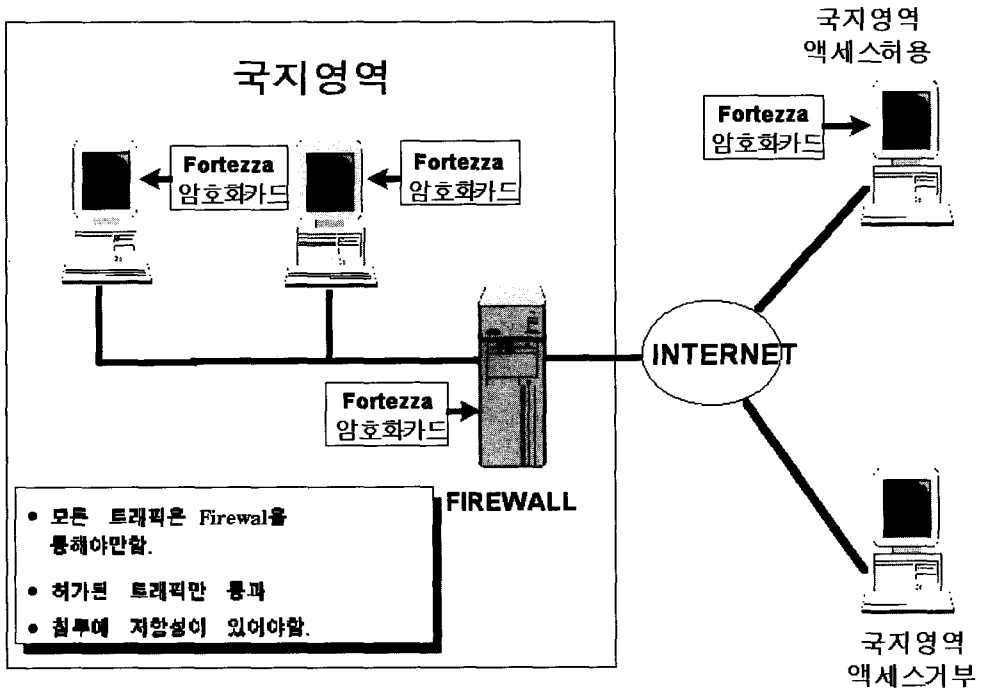

그림 7 MISSI Firewall의 사용

Firewall은 SBU 정보를 가지는 영역과 잠재적인 악성 망(malicious networks)간의 안전한 연결을 보장한다. Fortezza 신분확인을 가지는 Firewall은 영역외부의 사용자로부터 SBU 영역에 대한 제한된 액세스 및 강화된 보안을 허용한다. 보편적인 Firewall의 유형은 스크리닝 라우터(screening routers, packet-filtering systems), 응용계층 게이트웨이(application-level gateways, proxies and forwarders), 그리고 이 둘의 혼합형이 있다.

③ 현재 및 향후의 네트워크 암호기(INE : In-line Network Encryptor)

INE는 보통 국지영역과 외부망의 경계에 위치하며 암호화를 통하여 국지 및 광역 네트워크간의 데이터 비밀성과 무결성을 제공하며 암호적인 키관리를 통하여 액세스 제어 기능을 제공하며 특별한 경우에 트래픽 흐름 보안 서비스를 제공한다. 현재는 국지영역 수준의 데이터 보안을 제공한다.

INE에는 다음과 같은 것이 포함된다.

- X.25 패킷 교환 혹은 이더넷 네트워크를 지원하는 네트워크 암호화 시스템(NES : Network Encryption System)
- 비동기 전송모드(ATM, Asynchronous Transfer Mode)와 IP 전술 네트워크를 위한 KG-175(TACLANE)
- ATM에서 155Mbps까지 운용되는 KG-75(FASTLANE)
- Synchronous Optical Networks(SONET)에서 운용되는 KG-189

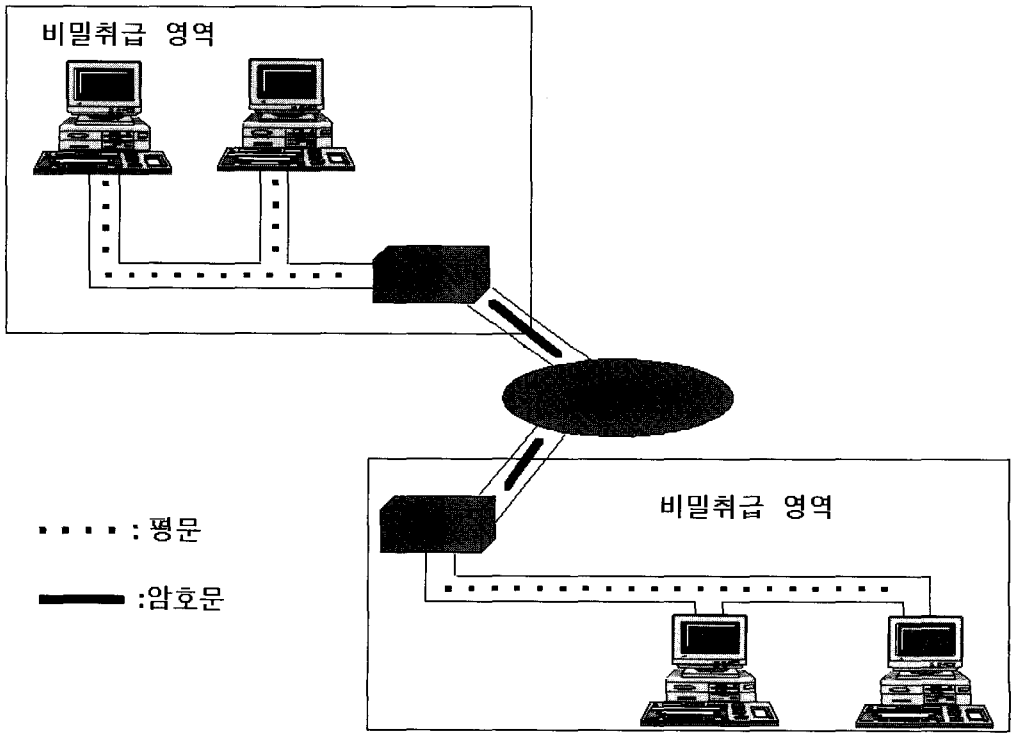

그림 8 네트워크 암호기 사용

3. MISSI를 이용한 보안 해결방안

사용자로 하여금 MISSI 제품에 대한 요구사항을 쉽게 이해하도록 여러 종류의 MISSI 보안 해결책이 구성, 통합, 시험 및 보안 프로파일되었다. 이 보안 해결책은 대부분 사용자의 공통적인 시스템 보안 요구조건을 포함하는 다양한 단일 등급 또는 다중 등급의 보안 구조를 나타내고 있다. 사용자들은 이러한 단순한 구조에서 자신들의 요구조건을 맞추어 보고 그들의 시스템에 MISSI 제품을 쉽게 구현할 수 있다. 즉 보안 해결책은 강제적이 아닌 유연한 가이드라인을 제공하고 있다. 궁극적으로 특정 환경에 대한 보안 대책은 지정된 승인자의 승인 하에 시스템 보안 엔지니어가 결정해야 한다 [2].

가. MISSI 트랜스포트 보안 해결책

MISSI 트랜스포트(Transport) 보안 해결책은 DISN 트랜스포트 네트워크 환경에서 보안서비스 중 가용성을 제공하는 것을 주목적으로 하는 다양한 네트워크 기반구조 서비스를 보여준다. 국방부 가입자는 MILNET에서 IP 기반 SBU Internet Protocol Router Network(NIPRNET), 그리고 궁극적으로 ATM 기반 네트워크로 이동하고 있다.

DISN 자원의 구성과 관리는 네트워크 관리 제어 센터(Network Management Control Center)에 의해 이루어진다. 네트워크 관리 명령을 인증하기 위하여 Fortezza 카드가 이용된다. Fortezza 신분확인 서비스가 설치된 Firewall과 통신 서버가 외부망으로부터 DISN을 보호하기 위해 사용된다.

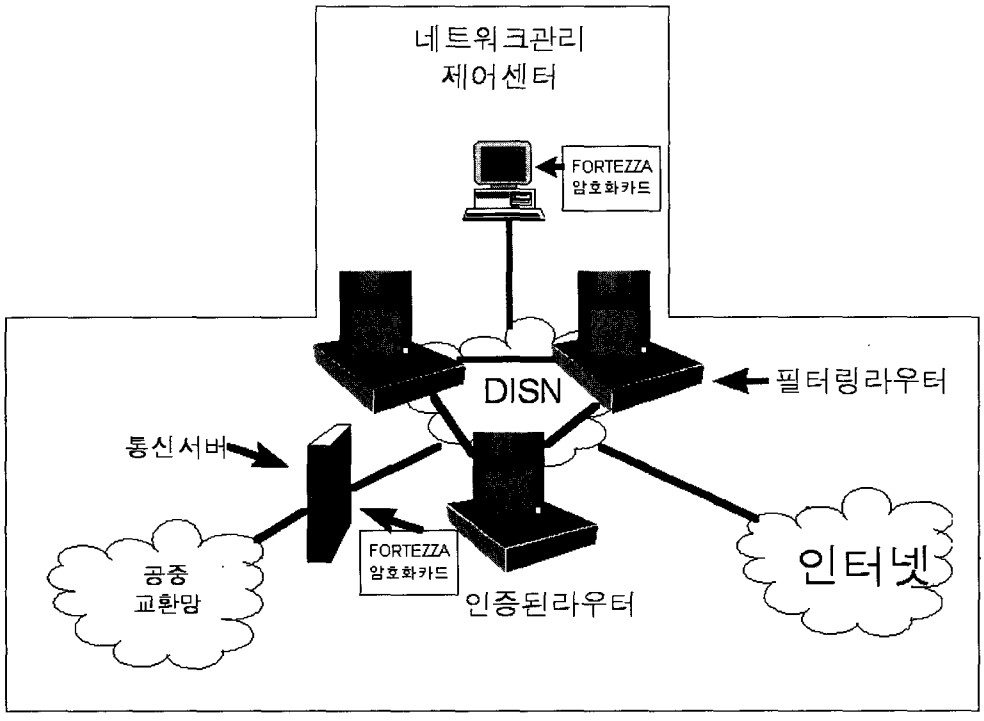

그림 9 MISSI 트랜스포트 보안 해결책

나. MISSI SBU-SBU 해결책 : 단일등급 보안

SBU와 SBU 간의 보안 해결책은 DISN을 통하여 SBU 정보를 전달하는 상용 워크스테이션간의 송 수신자 보안을 제공한다. 이들 워크스테이션에는 Fortezza와 Fortezza 응용 프로그램이 설치되어 있다. Fortezza는 데이터 비밀성, 사용자 PIN을 사용하여 Fortezza에 로그인할 것을 요구하는 강한 인증, 메시지 송수신 부인봉쇄 그리고 무결성을 제공한다. Firewall이 국지영역(LSE, Local Subscriber Enclaves)과 DISN간에 추가적인 보호를 위하여 사용된다. 네트워크 보안 관리 서비스는 모든 MISSI 구성요소에 요구되지만 지역 가입자 망 환경은 지역망 자체의 DSA, CAW 또는 MLA를 요구하지 않을 수도 있다.

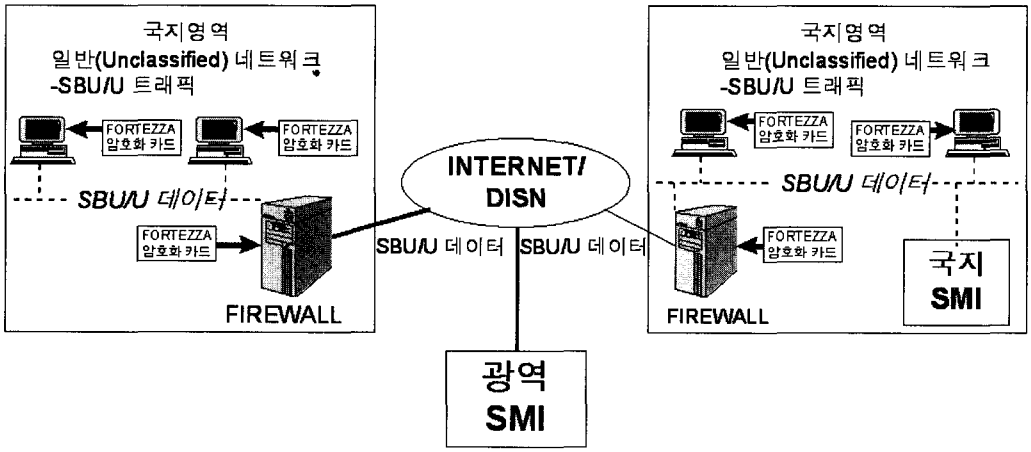

그림 10 MISSI SBU-SBU 보안 해결책 : 단일등급

다. MISSI SECRET-SBU 보안 해결책 : 다중등급 보안

이 보안 해결책은 2급(Secret) 네트워크에 있는 SBU 또는 비밀로 분류되지 않은 정보와 2급 네트워크 외부의 SBU 또는 일반 네트워크(Unclassified network) 사이의 정보 교환을 가능하게 한다. 이 보안 해결책의 구조는 SBU-SBU 구조에서 2급 네트워크 영역 내에 높은 보안 신뢰성을 가지고 있는 Guard를 설치함으로써 구성된다. SNS와 같은 Guard는 고 신뢰성의 하드웨어와 Guard 응용 프로그램을 갖는 상용의 플랫폼이다. 이 Guard 소프트웨어는 사용자가 설정할 수 있는 필터링 규칙(Customizable filtering)과 Fortezza 디지털 서명방식의 인증을 제공한다. 향후 고신뢰성 운영체제를 Fortezza 암호화 카드를 갖춘 영역내의 워크스테이션에 설치함으로서 이 보안 해결책의 보안 강도를 증가시키게 된다.

라. MISSI SECRET-SECRET-SBU 보안 해결책 : 다중등급 보안

이 보안 해결책은 위의 다 항에서 기술한 Secret-SBU 보안 해결책에 비밀로 분류된 영역사이의 비밀 데이터의 교환능력이 가미된 보안구조를 가진다. 비밀로 분류된 데이터를 보호하기 위한 Fortezza의 상위버전인 Fortezza

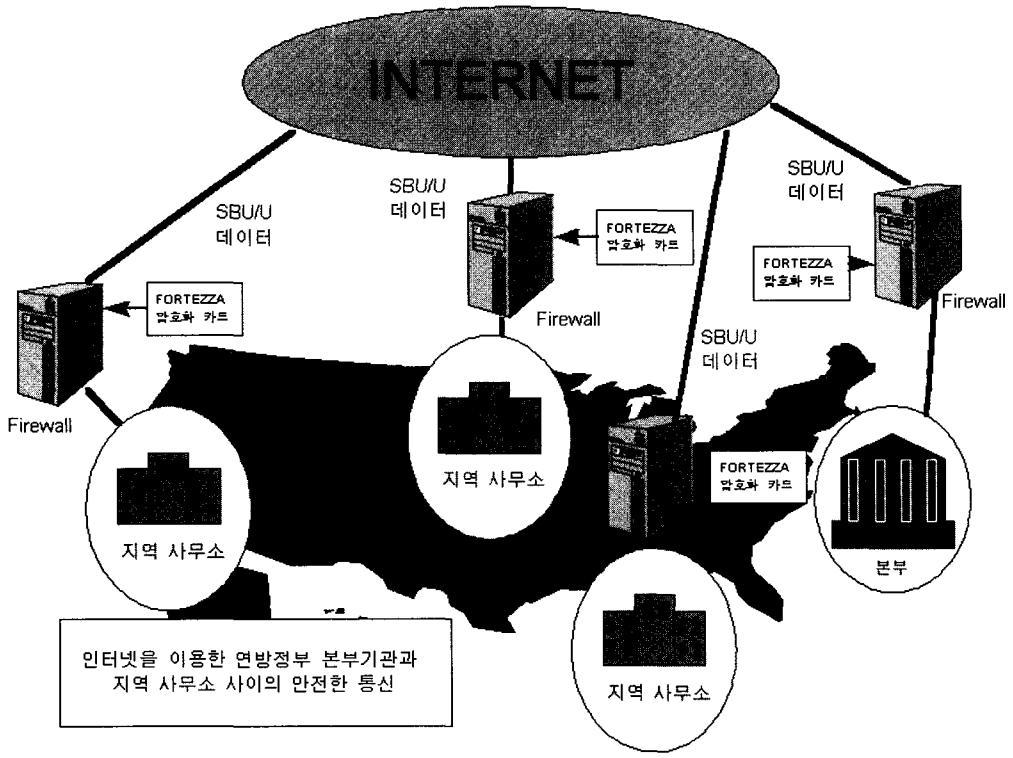

그림 11 MISSI SBU 환경의 보안 해결책 적용사례

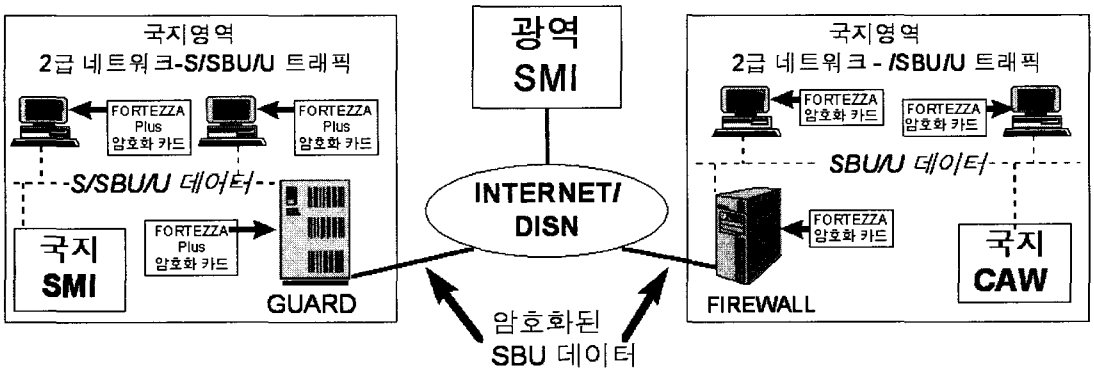

그림 12 MISSI Secret-SBU 보안 해결책 : 다중등급

Plus를 이용하여 2급 영역(Security enclave)은 Internet과 같은 신뢰할 수 없는 트랜스포트 네트워크를 통한 다른 2급 영역과 비밀로 분류된 정보의 교환을 할 수 있다. 높은 보안 신뢰도를 가지는 Guard를 이용하여 똑같은 비밀 등급을 가지는 영역은 다른 일반 영역과 SBU 혹은 비밀로 분류되지 않은 정보를 교환할 수 있다. Fortezza Plus는 비밀로 분류된 정보 혹은 SBU 정보의 안전한 전송을 보장하기 위하여 신분확인, 데이터 무결성, 비밀성 및 부인봉쇄를 제공한다.

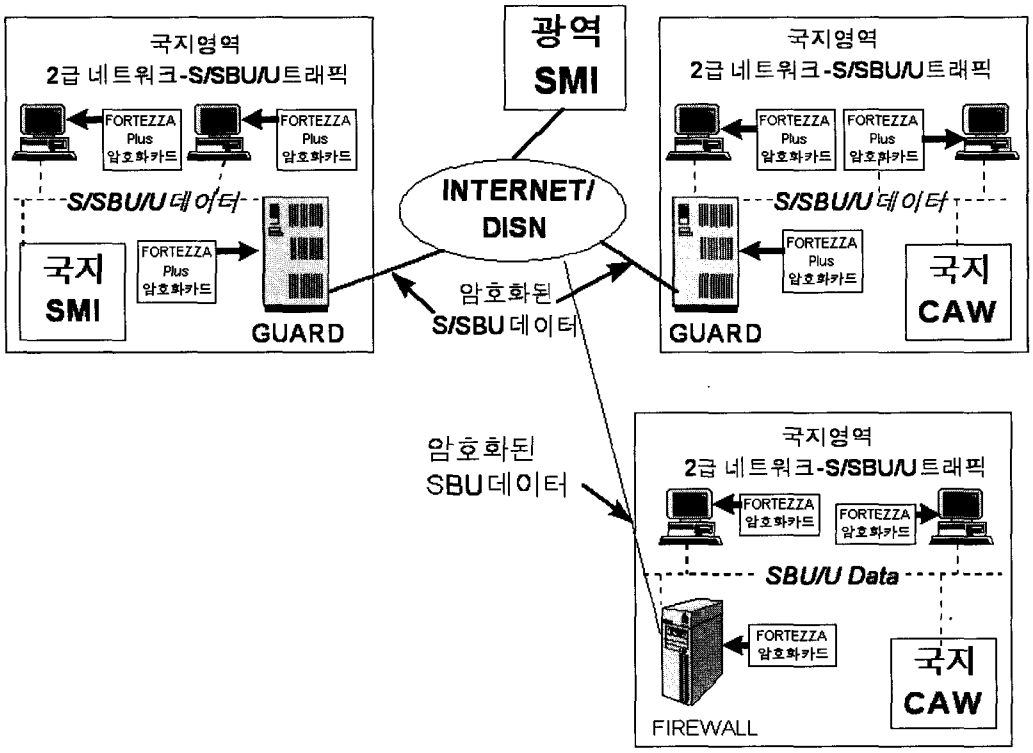

그림 13 MISSI Secret-Secret-SBU 보안 해결책 : 다중등급

마. MISSI TOP SECRET-SECRET 보안 해결책 : 다수의 단일등급 보안

이 보안 해결책은 트랜스포트 네트워크를 통한 "다수의 단일등급 보안(Multiple single level security)"을 제공한다. 1급(Top Secret)의 영역에 존재하는 정보는 네트워크로 전송될 때 1급의 키를 가지고 INE에 의해 암호화되며 동일한 1급의 키를 가진 다른 INE에 의해서만 복호화될 수 있다. 마찬가지로, 2급 영역 내에 존재하는 2급 비밀정보도 2급 키를 가지고 INE에 의해서 암호화되며 복호화된다. 이것은 똑같은 영역끼리 일반의 네트워크를 통한 정보의 공유를 보장한다. 일반적으로 1급 영역과 2급 영역간의 정보의 흐름은 허용되지 않으나

발신처에서 신뢰성 있는 데이터 레이블링 표준이 구현되었을 시에는 1급 영역에서 2급 영역으로의 정보흐름이 허용된다.

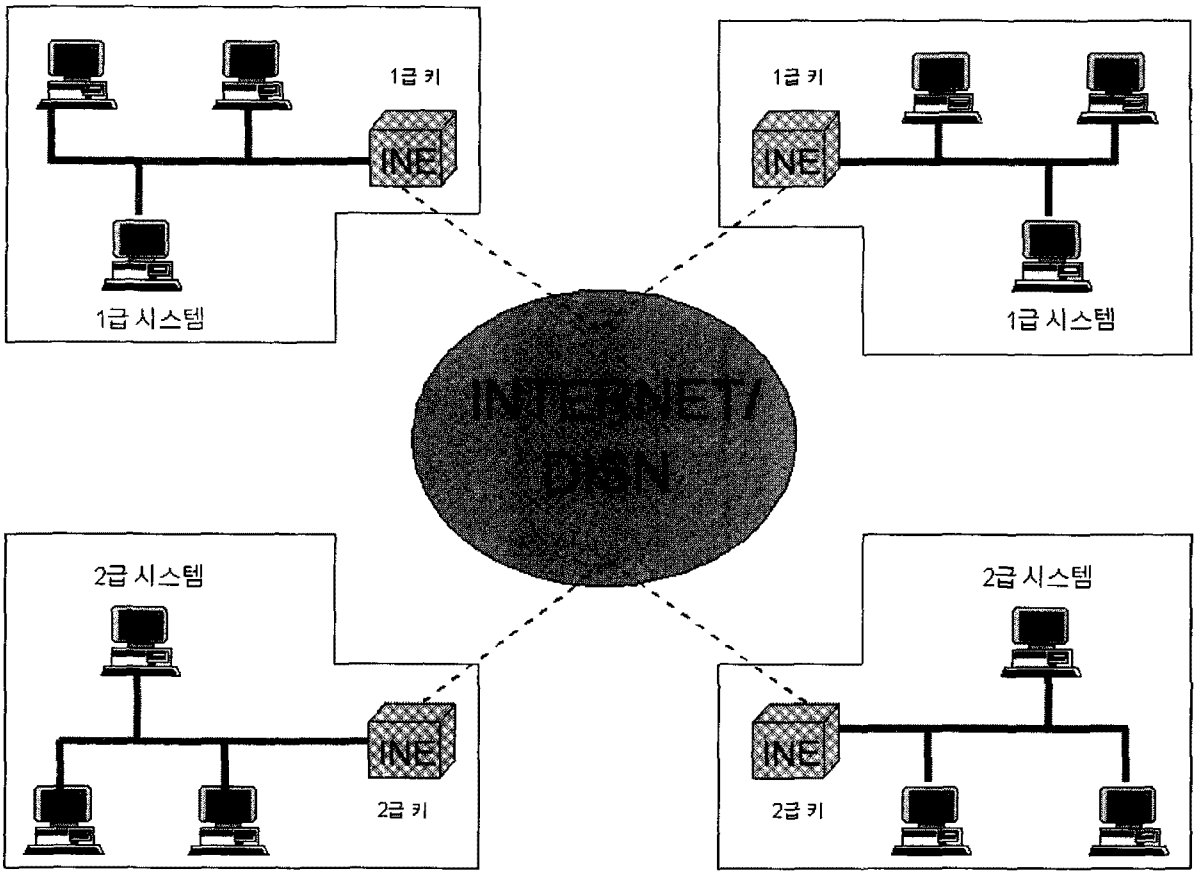

그림 14 MISSI Top Secret과 Secret 보안 해결책

4. 프로파일

시스템 보안 프로파일링(SSP : System Security Profiling)은 사용자의 운영환경(intended operational configuration environment)에서 시스템의 보안을 평가하기 위하여 시스템 엔지니어링 절차와 병행하여 수행되는 보안 엔지니어링 방법론이다. 프로그램 관리자와 시스템 인증자(Accreditor)를 지원하기 위하여 생성되어 시스템 보안 프로파일내에 문서화된 정보는 가격, 스케줄, 보안, 기능 및 다른 중요한 요소들 사이의 적절한 trade-off를 결정하는데 사용한다. 구조적 분석 방법과 침투시험을 이용하여 시스템 보안 프로파일링은 시스템 보안 요구사항을 위반하는 시스템의 취약성을 식별하고 문서화하는 위험관리 도구를 제공한다. 시스템 구성, 연결, 위협, 구성요소, 취약성 및 시스템 운영 같은 요소들 사이의 상호 의존성 및 상호작용에 대한 보안 분기(ramification)를 찾아내기 위해 소프트웨어가 사용된다. 결과적인 SSP는 고객 시스템 프로그램 관리자에 귀속되지만 다른 프로그램의 설계 지침으로써 재사용될 수 있다. 시스템 보안 프로파일링은 MISSI 구성요소의 적절한 배치와 특정 구조로의 통합을 지원한다. 이것은 또한 조직의 MISSI 해결책을 통합하는데 활용된다.

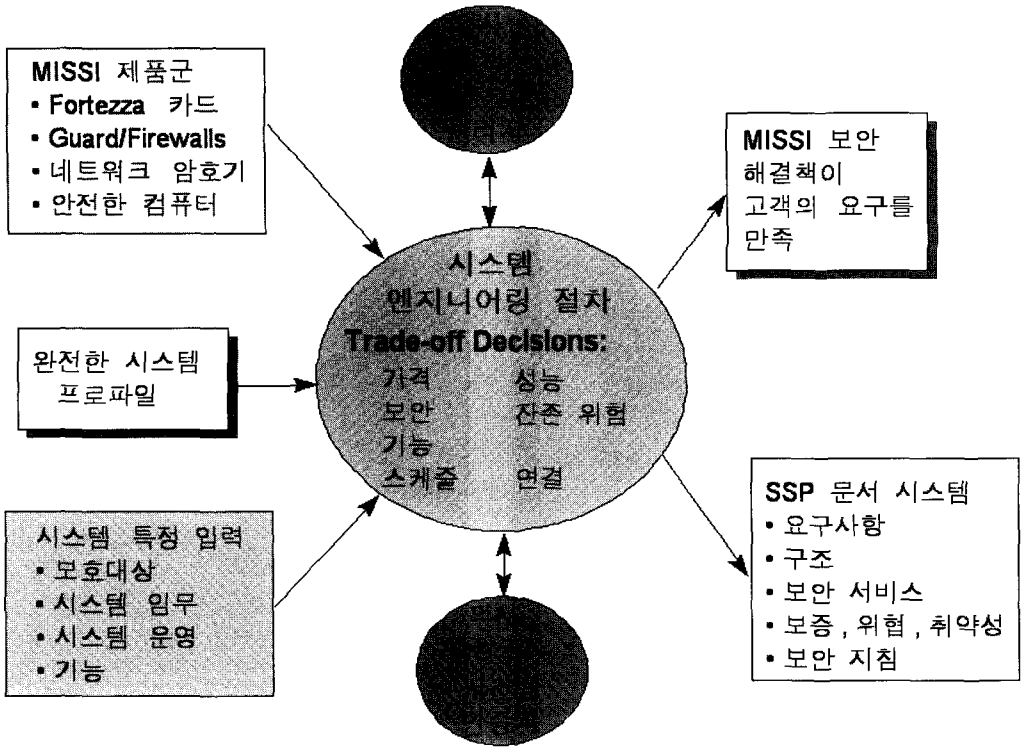

그림 15 시스템 보안 프로파일

5. 결 론

본 고에서는 미 국방부의 다중등급 데이터 보호를 위한 노력의 일환인 MISSI 프로젝트에 대하여 소개하였다. 또한 MISSI는 미 국방부 초고속망을 위한 종합적인 보안 해결책도 제공해 주고 있다. MISSI에서는 날로 변화되어 가는 보안 해결책의 응집력 있는 보안 구조를 정의하는 표준, 프로토콜 그리고 인터페이스를 개발하고 있다. 미국 NSA의 MISSI 확장 노력은 계속적으로 산업계 및 사용자와 함께 빠르게 발전하는 멀티미디어 환경을 위한 안전하고 상호연동성있는 상업용 소프트웨어를 개발하고 적용하는데 있다. 국방부와 국방부 산하 기관의 지원 속에서 MISSI는 현재와 미래의 다양한 정보시스템의 보안 요구사항을 만족시키는 혁신적이고 유용한 보안 해결책을 제공할 것이다.

본 고에서는 정보화촉진기본법에 따른 행정, 교육, 과학기술, 금융, 국방, 공안 및 물류 등의 전산망 운용 및 초고속 정보통신망의 설치에 즈음하여 이와 관련한 외국의 기술동향을 살펴보고 이를 분석하여 우리 나라의 환경에 맞는 종합적인 보안 해결책을 모색하고자 하였다. 이를 토대로 우리 나라의 실정과 기술을 고려하여 통합적인 보안 구조 및 보안 서비스에 대한 지속적인 연구 개발이 필요할 것이다.

참 고 문 헌

[1] 안전성 기술동향, 한국전자통신연구소, 1996. 7.

[2] http://beta.missilab.com, MISSI Introduction, 1996.

[3] http://www.armadillo.huntsville.al.us, Fortezza Home Page, 1996.

[4] http://www.rnbo.com/PROD/rmadillo/p/ptoc.html, FORTEZZA Application Implementor Guide for the PCMCIA based FORTEZZA Cryptologic Card, 1995.

[5] Defense Message System(DMS) Concept Operations(CONOPS), DISA, April 2, 199

□ 著者紹介

이 철 원

1987. 2. 충남대학교 수학과(학사)
1989. 8. 중앙대학교 대학원 전산학과(석사)
1989. 9. ~ 1996. 6. 한국전자통신연구소 선임연구원
1996. 6. ~ 현재 한국정보보호센터 선임연구원

※ 관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체제, 정보보호기술 표준화

김 학 범

1988. 2. 경기대학교 전자계산학과(학사)
1990. 8. 중앙대학교 대학원 전산학과(석사)
1996. 3. ~ 현재 아주대학교 대학원 컴퓨터공학과 박사과정 재학중
1991. 10. ~ 1996. 6. 한국전산원 주임연구원
1996. 7. ~ 현재 한국정보보호센터 주임연구원

※ 관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체제, 정보보호기술 표준화

이 경 구

1982. 2. 한양대학교 무기재료공학과(학사)
1986. 1. University of Central Arkansas Computer Science(학사)
1988. 5. University of Arkansas Computer Science(석사)
1996. 5. Kent State University Computer Science(박사)
1996. 7. ~ 현재 한국정보보호센터 선임연구원

※ 관심분야 : 컴퓨터 네트워크 보안, 정보보호시스템 평가체제, 라우팅 알고리즘, Interconnection Network

홍 기 웅

1985. 2. 전남대학교 전산학과(학사)
1990. 2. 중앙대학교 대학원 전산학과(석사)
1996. 2. 아주대학교 컴퓨터공학과(박사)
1985. 9. ~ 1995. 10. 한국전자통신연구소 선임연구원
1992. 9. ~ 1993. 6. 이탈리아 Alenia spazio S. P. A. 선임연구원
1994. 8. 정보처리기술사
1995. 10. ~ 1996. 4. 한국전산원 선임연구원
1996. 4. ~ 현재 한국정보보호센터 책임연구원, 평가체제팀장

※ 관심분야 : 컴퓨터 네트워크 보안, 정보보호시스템 평가체제, 정보보호기술 표준화

심 주 걸

1957년생
중앙대학교 전자공학과(학사)
건국대학교 대학원 전자공학과(석사)
성균관대학교 정보공학과 박사과정재학중
현재 한국정보보호센터 기준평가부장

※ 관심분야 : 정보보호시스템 기준 · 평가, 암호이론