通信情報保護學會誌
第9券第2號 1999. 06

효율적 국방망 구축을 위한 MISSI 분석

강 상구*, 송 유진**, 신 재호*

요 약

본 고에서는 국방부의 현대적 전쟁환경에 맞는 새로운 정보 시스템을 구축하여 폭넓은 정보교환과 효율적인 정보관리 능력을 증강하기 위하여 행정, 교육, 금융, 공안, 외교 및 물류 등의 독립적인 전용 전산망을 통합된 하나의 전산망으로 구축할 경우 다중등급보안을 처리하기 위해 미국 NSA가 주도하여 수행하고 있는 MISSI와 이에 이용되는 Fortezza, 그리고 현재 미국에서 구축 중에 있는 DII의 구성에 대해 분석하였다. 본 고는 향후 정보전을 대비한 효율적인 국방망 구축을 위한 기초 자료이다.

Ⅰ. 서 론

현대적 전쟁환경에 맞는 새로운 정보 시스템의 필요성에 따라 단일 정보 관리 프로그램을 통합, 즉 각 기관별로 독립적인 전용 전산망을 통합된 하나의 전산망으로 구축하여 폭넓은 정보교환과, 국방부의 임무를 효과적으로 수행하기 위한 컴퓨팅, 통신, 그리고 정보관리 능력을 증강하고, 또한 최소한의 통신과 컴퓨팅 기술 지식으로도 정보에 접근하고 분배, 교환할 수 있도록 하기 위해 효율적인 국방망을 구축이 필요하다. 이러한 필요성을 인식하고 DMRD(Defense Management Report Decision) 918C에 의해 단일 정보 관리 프로그램을 통합함으로써 개발된 미국의 DII(Defense Information Infrastructure)는 산업, 정부, 대학, 그리고 연합군의 정보 인터페이스도 DII의 영역으로 포함함으로써 보다 폭 넓은 정보교환을 제공하고 있다. 각 기관별로 전용의 전산망을 구축 운영하고 있는 상황에서 각 전산망을 통합할 경우, 이 통합된 전산망에 서로 다른 등급의 정보가 저장, 처리 및 송 수신될 수 있으므로 이를 효과적으로 통제하고, 선택적으로 분배할 수 있는 기능, 즉 서로 다른 다중의 보안등급을 가진 정보를 처리할 수 있도록 하는 다중등급보안(MLS, Multi-Level Security)이 필요하며, 이를 위해 NSA(National Security Agency)가 주도가 되어 구축중인 MISSI(Multilevel Information System Security Initiative)는 이와 같은 요구사항을 만족하는 보안 해결책이라 할 수 있다. MISSI를 구성하는 제품들 중 Fortezza 암호화 PC 카드를 통해서 기밀성, 무결성, 인증, 부인봉쇄의 보안 서비스를 제공하며, 이를 이용한 응용 프로그램은 대외비 정보에 대한 보안 서비스를 제공함으로써 전자적 정보를 다루는데 있어 안전성을 제공하고 있다.

Ⅱ. MISSI의 개요

1. MISSI의 개념

전산망이 각 국가 기관 개별적으로 구축되어 운영되고 있던 미 국방부 내의 정보 처리시스템을 통합하여 하나의 전산망으로 구축할 경우, 통합된 전산망에 서로 다른 등급의 정보를 처리할 필요가 있으며 이를 위해 MISSI라는 프로젝트 명칭하에 NSA가 주도가 되어 구축중이다. 초기의 MISSI는 국방부 메시지 시스템(DMS, Defense Message System), 통합 전술 전략 디지털 전산망(ITSDN, Integrated Tactical and Strategic Digital Network), 그리고 최고사령부(CINC, Command IN Chief)의 다중등급 정보 처리를 위한 것 이였으나, 미 국방부의 초고속망을 구축하면서 MISSI의 목적은 국방 초고속망을 기반으로 하는 다양한 업무들간의 상호 운용상의 안전성을 제공하기 위한 것으로 발전되고 있다[1][2].

* 동국대학교 전자공학과 정보보호 및 신호처리 연구실 (sgkang@cakra.dongguk.ac.kr)
** 동국대학교 정보산업학과 (song@mail.dongguk.ac.kr)

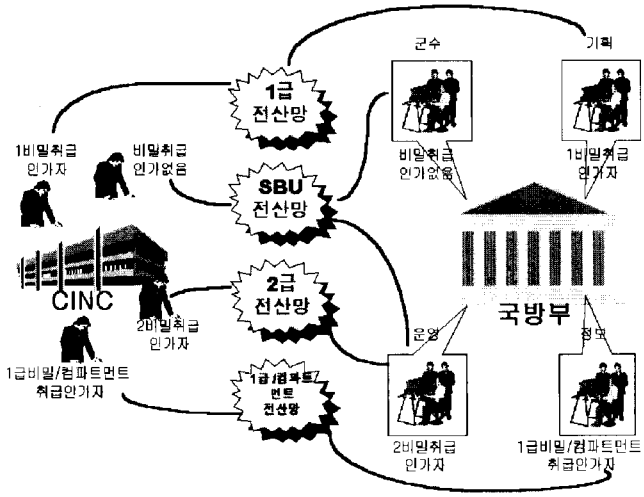

그림 1. 현재의 미 국방부 네트워크

그림 1과 같이 현 미 국방망은 국방부와 최고사령부(CINC) 내의 각 부서간의 보안 등급별 전용회선을 이용 2급 신원허가를 가진 사용자는 2급 네트워크를 통하여 국방부내의 2급 취급 권한을 가진 사용자와만 통신을 할 수 있었으나, 그림 2에서 보는 것처럼 향후 미 국방망 환경에서는 전용회선 망을 없애고 인터넷이나 국방 초고속망(DISN, Defense Information System Network)과 같은 통합된 하나의 기반망을 이용, 다중등급 데이터 처리 기능을 부여함으로써 기존의 데이터의 보안등급별 처리에 따르는 불편함을 해소할 예정이다[1][2].

2. MISSI 시스템

미 국방 정보기반 구조(DII)에 대한 상호 보안서비스, 즉 다중등급보안(MLS)을 제공하기 위한 MISSI는 그림 3과 같이 공통의 보안관리 기반을 토대로 MISSI를 구성하고 있는 제품과의 통합적이고 상호 운용성을 바탕으로 보안 해결책을 제시하고 있으며 MISSI를 구성하고 있는 제품군은 정부의 보안 표준을 따르는 상업적인 벤더가 제공한다[1][2].

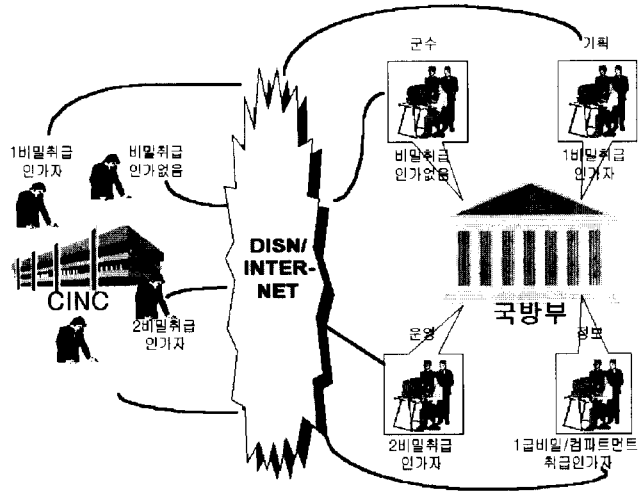

그림 2. 향후의 미 국방부 네트워크

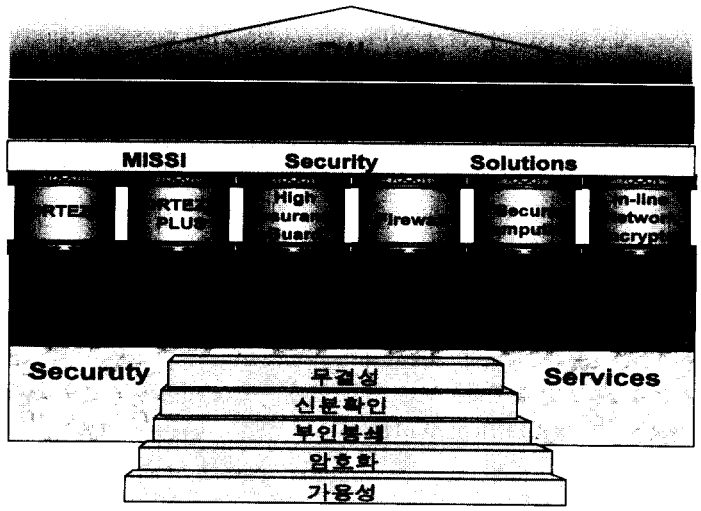

그림 3. MISSI의 보안 해결책

MISSI를 구성하고 있는 보안 시스템(제품)은 그림 4와 같으며 크게 워크스테이션 보안과 시스템/국지영역 보안 시스템으로 나눌 수 있다. 워크스테이션 보안 시스템은 워크스테이션 상에 보안 서비스를 제공하기 위한 것으로 Fortezza 암호화 PC 카드 및 이를 이용하여 전자우편, 전자상거래/전자문서 교환, 웹 브라우저, 파일저장, 원격 로그인, 파일전송, 원격 DB 엑세스, 신분확인과 같은 서비스를 제공하기 위한 응용프로그램으로 구성되며, 시스템/국지영역 보안 시스템은 국지영역 내에 상주하면서 국지영역과 외부망간의 엑세스 제어와 암호화 서비스를 제공한다. 안전한 컴퓨터는 국지 영역의 보안을 강화시키기 위해 정보에 대한 비밀성 레이블을 지원하여 허가되지 않은 사용자에게 정보가 유출되는 것을 막기 위한 고도의 신뢰성을 가진 컴퓨터와 응용프로그램을 말한다. 네트워크 암호 시스템으로는 X.25 계층이나 IEEE 802.3 계층에서 패킷을 암호화하기 위한 NES(Network Encryption System), ATM에서 셀을 암호화하기 위한 장비인 FASTLANE과 ATM/IP를 기반으로 하는 전술 네트워크에서 다중등급 보안을 제공하기 위한 TACLANE, SONET (Synchronous Optical Network)과 호환 가능한 암호기인 KG-189가 있다.

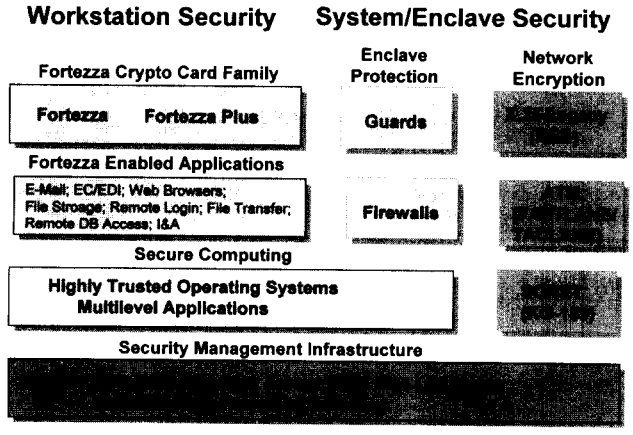

그림 4. MISSI의 제품군

3. MISSI 접근제어 개념 및 메커니즘

MISSI에서 사용되는 접근제어는 사용자가 어떠한 리소스, 즉 데이터에 접근하려 할 때 그 사용자가 해당 리소스에 대한 접근 권한을 가지고 있는지를 확인하여 인가된 사용자에게만 접근을 허가하는 메커니즘을 말한다[4].

1) 보안 레이블(Security Label)

그림 5와 같이 객체(object)와 묶여있는 보안 특성정보(security attribute information)들의 집합을 말하여, 여기서 객체는 전송되거나 저장되어 있는 데이터나 물리적인 리소스를 말한다. 보안 레이블은 X.411 MTS Abstract Service syntax로부터 야기된다.

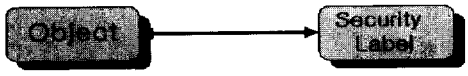

그림 5. 객체와 보안 레이블과의 관계

```
SecurityLabel ::= SET {
  security-policy-identifier OBJECT IDENTIFIER OPTIONAL,
  security-classification    INTEGER OPTIONAL,
    -- values of security-classification field are defined by
       security-policy-identifier
  privacy-mark               PrivacyMark OPTIONAL,
  security-categories        SecurityCategories OPTIONAL }
  PrivacyMark ::= PrintableString (1..ub-privacy-mark-length)
  SecurityCategories ::= SET (SIZE (1..ub-categories)) OF
                         SecurityCategory}
```

MISSI에서, 보안 레이블은 객체의 등급(security-classification)을 포함하고 있으며, 객체에 적용할 security category와 privacy mark와 관련된 보안 등급을 시행하기 위해 security policy 식별을 위한 security-policy-identifier가 사용된다. 따라서, MISSI와 호환되기 위해서는 security-policy-identifier를 포함해야하며 security-policy-identifier가 없는 보안 레이블은 MISSI 호환 소프트웨어에 의해 거부된다.

2) X.509 인증서(Certificate)와 보안객체식별자(Security Policy Object Identifier)

X.509 인증서는 시스템에 의해서 사용되는 정보를 식별하기 위한 version, serial number, signature, issuer, validity, subject, subjectPublicKeyInfo, extension fields와 같은 다양한 field가 있는데, MISSI에서는 extension field에 있는 subjectDirectoryAttributes의 사용을 요구한다. 이 subjectDirectoryAttributes는 prbacInfo, prbacCAConstraints, sigOrKMPrivileges, 그리고 commPrivileges 4개의 부 속성을 수행한다. 이중 prbacInfo Attribute는 securityPolicyID, prbacClassifications, SSLPrivileges로 구성되며 각각의 기능은 아래와 같다.

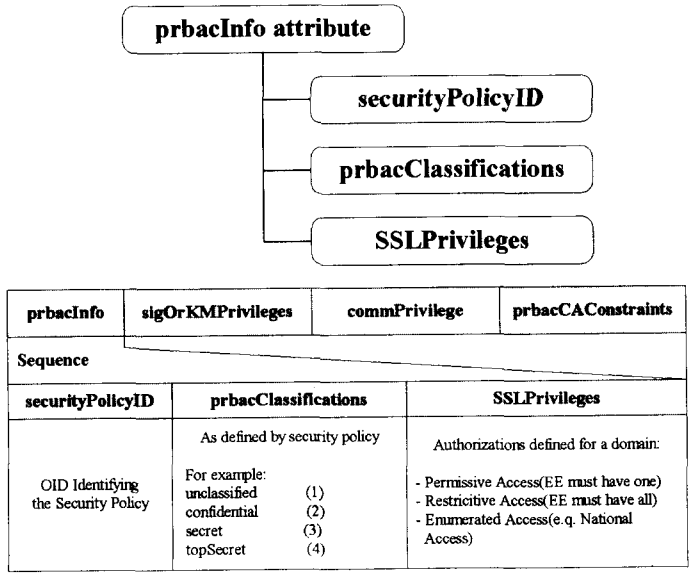

그림 6. prbacInfo attribute 구조

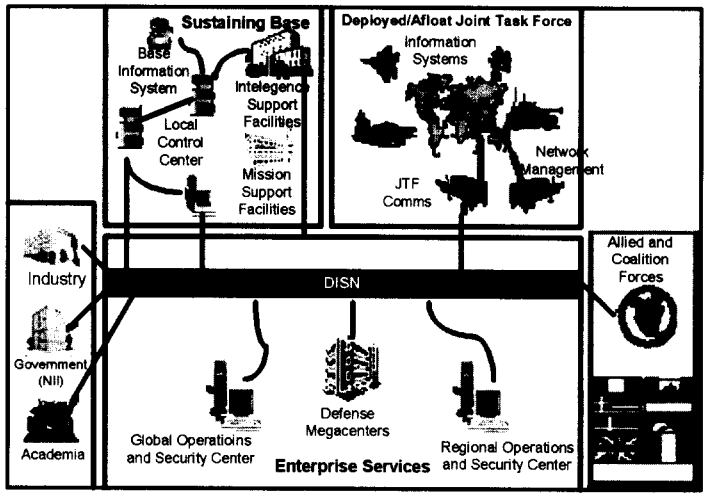

그림 7. DII Architecture Concept(DII의 영역)

- securityPolicyID
  어떠한 옵션 구성 요소가 인증서의 prbacInfo attribute에 제공되어야 하는지를 식별하기 위한 객체 식별자
- prbacClassifications
  사용자의 승인과 계층적 허가를 정의
  (e.g. secret, top secret, confidential)
- SSLPrivileges
  restricitve, permissive bit mapped security categories를 식별(optional security categories)

Ⅲ. DII 분석

1. DII의 개념

1992년 미 국방부는 현대적 전쟁환경에 맞는 새로운 정보 시스템의 필요성을 인식하게 되었고, 이에 DMRD 918C에 의해 단일 정보 관리 프로그램을 통합함으로써 DII가 개발되었다. 즉 각 기관별로 독립적인 전용 전산망을 통합된 하나의 전산망으로 구축하여 불필요한 정보 체계를 줄여 새로운 컴퓨터 환경하에서 최신 응용 소프트웨어를 이용, 정보 처리와 데이터 전송 서비스를 구현함으로써 폭넓은 정보교환과 국방부의 임무를 효과적으로 수행하기 위한 컴퓨팅, 통신 그리고 정보관리 능력을 증강하기 위함이다. 또한 DII는 OSD(the Office of the Secretary of Defense), Military Departments, CJCS(the Chairman of the Joint Chiefs of Staff), the Defense Agencies, Combatant Commands의 정보기반을 포함한 산업, 정부, 대학, 그리고 연합군의 정보 인터페이스를 DII의 영역으로 포함함으로써 보다 폭 넓은 정보교환을 통해 안전한 정보 생성과 서비스를 제공하는데 목적이 있다[6].

2. DII 구성

DII의 가장 큰 목적은 전투 명령기관, 군사 서비스와 방위청에 정보 서비스를 제공하기 위함으로 그림 8과 같이 많은 집단들로 구성되어 있으며 각 집단들은 마치 퍼즐 조각처럼 연결되어 모든 집단이 없이는 완전할 수 없다[6].

1) Foundation : Program and Related Technical Activities

DII 모든 집단에게 life-cycle를 제공하고, 모의실험 능력, 새로운 기술에 대한 지속적인 평가, 정보 전송과 처리에 대한 기준마련, 실험 및 평가, 권한이 없는 접근에 대해 보호하고 공격에 대해 대응하기 위한 기능을 제공하며 상위 계층의 통신 및 컴퓨터 기반 구조(Communication and Computer Infrastructure), 일반 어플리케이션(Common Application), 기능적 지역 어플리케이션(Functional Area Applications)은 Foundation에서 제정한 요구사항, 정책 및 표준에 따른다.

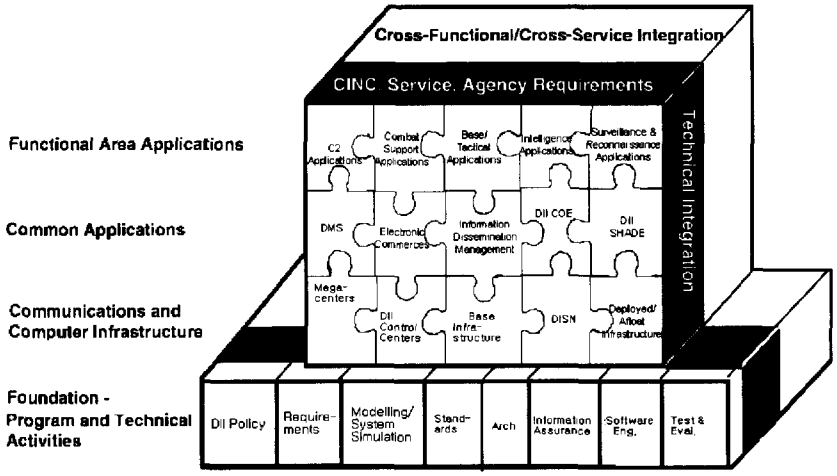

그림 8. DII의 구성

2) 통신 및 컴퓨터 기반구조

기능적 지역 어플리케이션과 일반 어플리케이션에 의해 사용된 정보를 처리 및 전송 서비스를 제공한다. 정보 전송을 위한 DISN, 정보 시스템 처리를 위한 방위 메가센터(Defense Megacenters), DII 네트워크와 시스템을 관리하는 DII 통제센터(Control Centers), 통신과 컴퓨터 자산을 위한 Base 및 Deployed/Afloat로 구성된다.

(1) 국방초고속망(Defense Information System Network)

군사 조직을 축소하고 신뢰성을 증대시키기 위해 국방부는 위기 상황시 신속한 대처, 기동성 증대, 그리고 명령의 효과적인 전달의 필요성을 인식하고 DISN을 개발하게 되었다. 국방부의 정보 전송 기반인 DISN은 DII와 DII 경계에서 정보 전송 서비스를 제공하는 DII의 부 집단으로써, 모든 다른 DII의 집단은 정보 전송을 위한 광역 네트워크로의 연결을 위해 DISN에 의존하게 된다. 이는 사용자의 정보자원 관리를 용이하게 하고 국가 안보에 민감하다.

(2) DII 통제센터(Control Centers)

DISA, 서비스 그리고 다른 정부기관들의 현행 시스템과 네트워크 관리는 다양한 이종의 시스템을 사용하여 성취되었는데, 이러한 개별적인 DII 통제센터는 DII의 기술적 구조에 end-to-end 관리를 제공하고, DII의 통합된 관리에 대한 책임은 DISA, 서비스, 그리고 다른 정부기관들에게 분담된다.

- 광역운영보안센터(GOSC, Global Operations and Security Center)
  DII에 대한 관리와 운영상의 감독 수행.
- 지역운용보안센터(ROSCs, Regional Operations and Security Centers)
  명확한 책임지역(AOR, Area OF Responsibility)에 대한 시스템과 네트워크의 관리 및 운영 제어를 수행한다. 정보전쟁 (IW, Information Warfare) 전역, 국방 메시지 시스템(DMS), 광역명령통제 시스템(GCCS, Global Command and Control System)을 제공하는 DISN 백본이 DII의 지역 구성요소를 지원.
- 지역제어센터(LCCs, Local Control Center)
  국부 서브집단에 대한 네트워크와 시스템 관리 및 운용 제어 수행.
- 그밖에 DMCs, COOP(Defense Continuity of Operations), DCTF(Test Facility)를 지원하는 시스템 관리센터(SMCs, System Management Centers)와 광역명령통제시스템관리센터(GMC, Global Command and Control System Management Center), 그리고 남서부아시아지역운용보안센터(SWA ROSC, South West Asia)와 같은 전역제어센터가 있다.

(3) Base and Deployed/Afloat Communications and Computer Infrastructure

DISA가 국방부의 DII 통신과 컴퓨팅 구조 부분에 대한 책임이 있는 반면, C/S/As는 기지로의 기능확장과 사용자들을 배치 또는 유포하는 책임이 있다.

(4) 정보기관(Intelligence community) 통신 및 컴퓨터 기반구조

정보기관은 국가 정부기관과 전술 소비자 즉, Joint Task Force and Combined Task Force Commanders Command와 C4I (Command, Control, Communications, Computers and Intelligence)에게 적절한 정보를 제공함으로써 군과 정부작전본부를 지원하기 위한 것이다.

3) 일반 어플리케이션

일반 어플리케이션은 기관에 의해 사용되는 메시징, 전자 거래와 같은 기능을 제공하는 응용 프로그램으로 정보의 처리와 전송을 제공하기 위해 DII 통신 및 컴퓨터 기반구조에 의존한다. 사람과 기관에 대한 문서교환 기능을 제공하는 DMS, 전자 거래를 위한 EC/EDI, 공통으로 제공되는 서비스를 통합하고 소프트웨어 개발환경 일치시키기 위한 DII COE(Common Operating Environment), 국방부 임무를 관리하는데 필요한 군사 서비스와 functional areas 사이의 데이터 계층에서 기능적 지역 어플리케이션 상호 운용을 위한 SHADE (Shared Data Environment), NCA에 의한 정보 공급에 대응하는 정보보급관리(Information Dissemination Management)로 구성된다.

(1) 국방메시지시스템(DMS)

DMS는 DISN에서 동작하도록 구성된 전자 서신 교환의 새로운 방법으로 국방부의 기존 AUTODIN(Automatic Digital Network)와 e-mail 시스템을 대체하고 있다. 즉, 집약적인 자원과 오래된 AUTODIN을 제거함으로써 비용과 인력을 줄이기 위해, 또한 개선된 메시징, 디렉토리 서비스를 구현하고 국제 표준을 도입함으로서 병력에 대한 지원을 향상하기 위함이다.

(2) 전자거래(Electronic Commerce)

ECI(Electronic Commerce Infrastructure)를 사용하여 모든 업무를 처리하기 위한 EC 기술을 개발하여 이용함으로써 전쟁능력을 유지 및 병력을 지원하는 동원을 통해 평시 국가 군사 전략을 수행할 수 있다.

(3) DII COE(Common Operation Environment)

응용 소프트웨어 개발을 지원하는 구조원칙, 지침 및 방법을 제공한다.

(4) SHADE(Shared Data Environment)

군사 서비스와 functional area 사이의 데이터 계층에서 기능적 지역 어플리케이션의 상호 운용성을 제공한다.

(5) 정보보급관리(Information Dissemination Management)

군사 어플리케이션에 의해 DBS(Direct Broadcast Service)와 VSATs(Very Small Aperture Terminals)와 같은 고 대역 전송로가 개발됐고 각각의 통신량이 DISN으로 점차 집중됨에 따라 정보관리처리(information management process)를 통합할 필요성이 생기게 되었다. 이에 ASD/C3I는 이러한 필요성을 인식하게 되었고 DISA에 의해 정보보급관리가 개발되었다.

4) 기능적 지역 어플리케이션

전술상의 어플리케이션을 포함하는 C2(e.g. GCCS)와 전투지원 어플리케이션(e.g. GCSS)과 같은 모든 국방부 기관을 포함하며, C2I(Command and Control, Intelligence)와 아래와 같은 집단에 의해 개발되었다.

(1) DSS(Distribution Standard System)
: Logistics community;
(2) MOCAS(Mechanization of Contract Administrative Services)
: Procurement community;
(3) DCPDS(Defense Civilian Personnel Data System)
: Civilian personnel community;
(4) DBSS(Defense Blood Standard System)
: Health community;

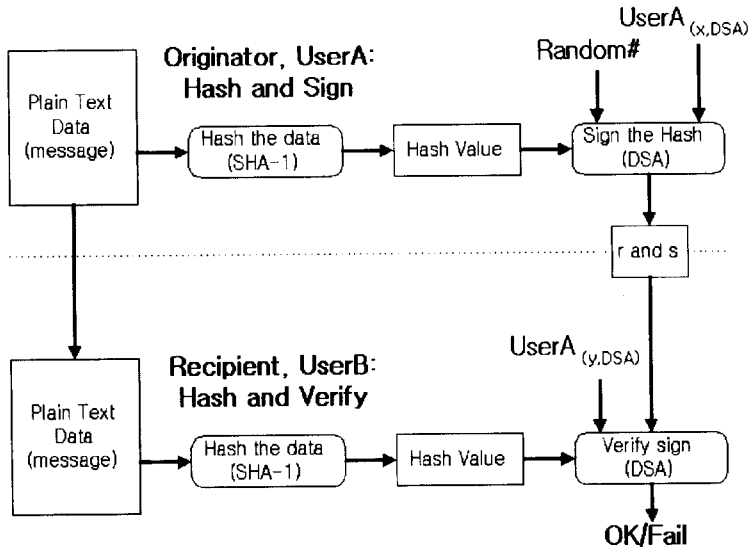

그림 9. 해쉬와 전자서명

기능적 지역 어플리케이션은 적당한 기능상의 조정이 없이 발전되어 왔기 때문에 다른 기관에서 동일한 기능을 수행하는 다수의 어플리케이션들이 있다. 이러한 중복된 어플리케이션들과 기반구조(사람, 장비, 건물)로 인해 국방부의 상당한 자원을 낭비하고 있고, 이러한 것을 개선하기 위해서 국방부에서 통합이 시도되고 있다.

Ⅳ. MISSI를 위한 Fortezza 분석

1. Fortezza 서비스

전자적 정보를 다루는데 있어 정밀성과 안전성이 요구됨에 따라 NSA의 Fortezza 프로그램은 대외비 정보에 대한 보안 서비스를 제공함으로써 이러한 요구 조건을 만족시킬 수 있다. Fortezza의 개별적인 디바이스와 'Fortezza Crypto Card'라 불리우는 PC 카드를 통해서 무결성, 인증, 부인봉쇄, 기밀성의 보안서비스를 제공하게 되며, PC 카드에는 사용자에 대한 정보와 암호화 키, 암호화 알고리즘이 저장된다.

1) Fortezza 카드가 수행할 수 있는 암호화 기능[3]

(1) 해쉬(Hash)

데이터에 해쉬 알고리즘을 적용하여 160bit (20byte)의 해쉬 값을 생성, 데이터에 대한 무결성을 제공하며, SHA-1(FIPS 180-1) 해쉬 알고리즘을 사용한다.

(2) 전자서명(Digital Signature)

수신자에게 송신자의 신원(인증 및 부인봉쇄)을 확인시키기 위해 제공되며, DSS(Digital Signature Standard, FIPS-186)의 DSA(Digital Signature Algorithm)을 사용한다.

(3) 기밀성(Confidentiality)

암호화와 복호화는 송신자와 수신자에게 분배된 단일키에 의해 구현되며, 이때 키는 카드에 의해 랜덤하게 생성된다. SKIPJACK algorithm (FIPS -185)이 사용된다.

(4) 키 교환(Key Exchange)

암호화 알고리즘에 필요한 키를 wrap하여 안전하게 수신자에게 전송되는데, 이때 KEA(Key Exchange Algorithm)가 사용된다.

모든 메시지는 해쉬된 후, 출력된 해쉬값에 전자서명을 적용함으로써 데이터의 무결성과 해쉬값에 대한 서명자의 인증과 무결성이 제공된다.

그림 9와 같이 UserA가 메시지에 대한 무결성과 사용자 인증 보안서비스를 요구할 경우, UserA는

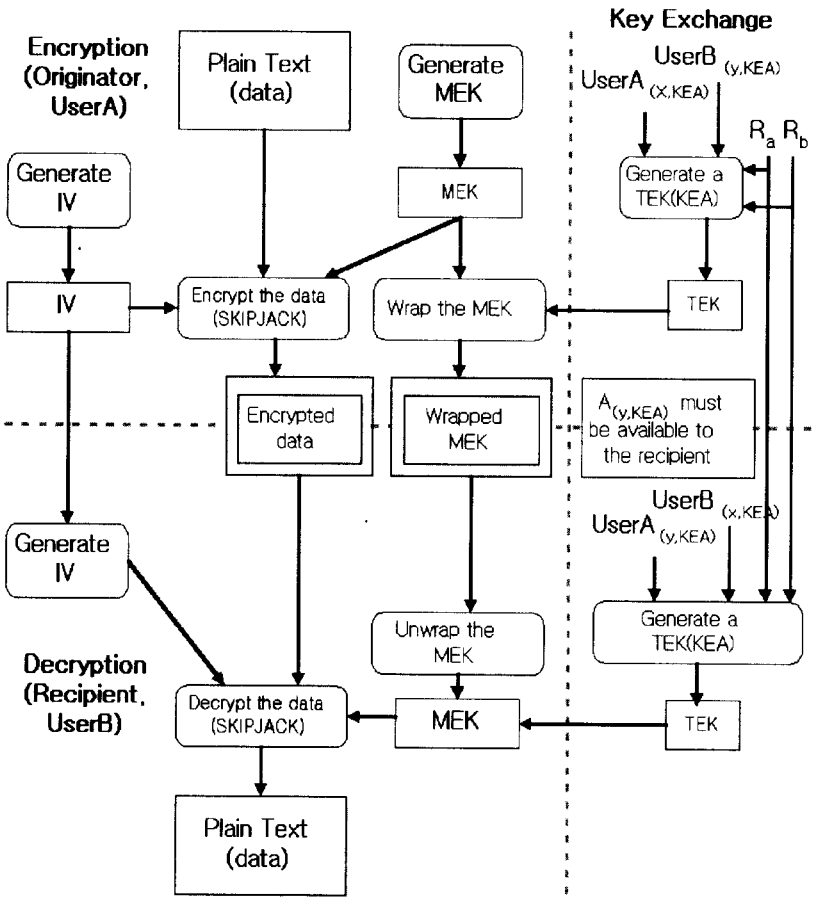

그림 10. 암호화, 복호화 및 키 교환

메시지에 해쉬 기능을 수행하여 출력된 해쉬값에 전자서명 알고리즘을 수행하게 되는데, 전자서명시 해쉬값과 UserA의 카드에 저장되어 있는 비밀키 및 카드에 의해 생성된 난수가 필요하게 된다. 서명의 결과로 2개의 20바이트 파라미터 "r"과 "s"가 출력되며 메시지와 함께 수신자, 즉 UserB에게 전송된다. UserB에게 수신된메시지에 독립적으로 수행하여 얻은 해쉬값과 UserA의 공개키 및 "r", "s"를 사용하여 메시지에 대한 무결성과 인증을 확인하게 된다[3].

그림 10은 TEK(Token Encryption Key)를 생성함으로써 수신측에서 복호화하기 위해 필요한 MEK(Message Encryption Key)를 어떠한 방법으로 안전하게 수신자에게 송신하는가를 보여준다. 먼저 TEK는 송신자의 개인키 $x_{(KEA)}$와 수신자의 공개키 $y_{(KEA)}$, 두 개의 난수를 입력으로 KEA에 의해서 생성된다. 생성된 TEK는 MEK를 wrap하여 수신자에게 송신하게 되고, wrap된 MEK를 수신한 수신자는 자신의 비밀키 $x_{(KEA)}$와 송신자의 공개키 $y_{(KEA)}$를 사용, unwrap하여 MEK를 확인 후 메시지를 복호화하게 된다.

2. CMP(Common Message Protocol)과 Fortezza

Fortezza 카드는 주어진 데이터에 대한 간단한 암호학적 처리만 수행할 뿐 단독으로는 메시지 처리를 할 수 없기 때문에 대부분의 컴퓨터와 네트워크 환경에서 사용되는 CMP과 함께 사용되어야한다[3].

1) SMTP(Simple Mail Transport Protocol)

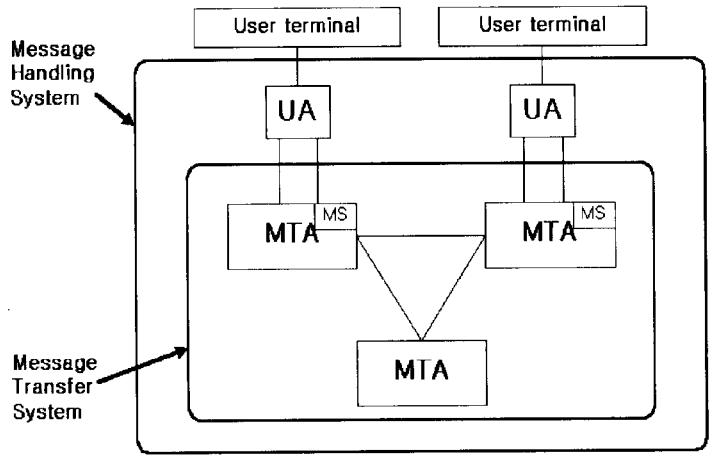

그림 11. Message Handling System

RFC(Request For Comment) 821에 명시되어 있는 e-mail 프로토콜로 ASCII 문자만 사용할 수 있고 또한 1000 문자 이하로 body의 길이에 제한이 있기 때문에 멀티미디어(picture, sound etc.) 데이터의 송·수신이 필요할 경우 'base 64 bit encoding' 또는 'uuencoding'의 일반적인 방법을 사용하여 표준 ASCII 형태로 변환시키는 작업이 필요하다.

2) MIME(Multipurpose Internet Mail Extension)

SMTP RFC 821 프로토콜을 사용하여 비-ASCII(multimedia data)를 전송할 수 있는 메커니즘을 제공하며 RFC 1521에 명시되어 있다.

3) X.400

상이한 컴퓨터 시스템 상호간의 통신에 있어서 다양한 형태의 데이터에 대한 규약으로 X.400의 전체 환경은 그림 11과 같이 MHS(Message Handling System)에 포함되어있다. MHS는 메시지를 처리하는 UA (User Agent)와 UA 메시지를 검색, 저장 및 삭제할 수 있는 MS(Message Store), 메시지를 전송하는 MTA(Message Transfer Agent), MTA의 백본인 MTS (Message Transfer System)으로 구성된다.

4) ACP 123(Allied Communications Protocol 123)

군 MHS와 민간의 X.400 사이의 상호 운용을 안전하게 하기 위해 필요한 서비스와 프로토콜을 규약하는 것으로서 DMS e-mail은 ACP 123을 따른다.

5) X.500

X.500 디렉토리는 전화번호부 책과 비교할 수 있으며, 여기에는 엔터티(사람 또는 시스템)의 e-mail 주소, Fortezza 및 사용자와 관련된 정보가 포함된다.

6) SDNS(Secure Data Network System)

민간 사업자와 NSA에 의해 공동으로 개발된 프로토콜들의 집합으로 컴퓨터와 통신 네트워크 및 메시지 시스템의 보안 기술을 향상하고 상호 공용이 가능할 뿐만 아니라 효과적인 비용에 중점을 두고 있으며 이와 관련된 문서는 SDN.701, SDN.702, 그리고 SDN.704가 있다.

- SDN.701:MSP(Message Security Protocol)
- SDN.702:SDNS의 디렉토리 표준
- SDN.704:SMTP/MIME 메시지를 위한 MSP 메시지 포맷

3. Fortezza 시스템

1) 키 관리 구성

암호화 키를 생성하고 분배, 확인, 만기 및 폐지 등과 같이 키를 관리하기 위해서 인증서와 CRL (Certificate Revocation List), CKL(Compromised Key List)이 필요하다. Fortezza 인

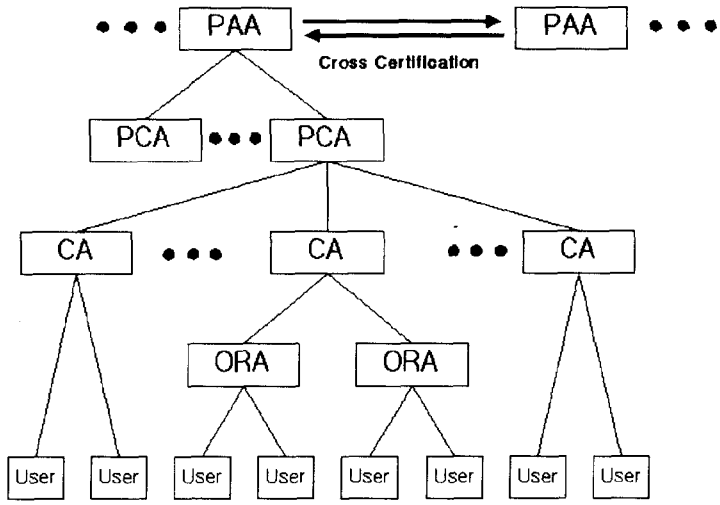

그림 12. 인증서 인증 체계

증서의 경우 ITU-T X.509 권고에 명시된 인증서에 기반하며 사용자의 신원과 공개키 정보가 저장되어 있다. 또한 인증서가 만기되거나 데이터에 변화가 있을 시, 즉 사용자가 이사를 하여 주소에 변화가 있던가 카드가 파손되었을 경우, 그리고 더 이상 인증서가 필요 없어 폐지된 인증서의 정보를 저장하고 있는 CRL이 있다. CKL은 카드와 PIN을 분실하거나 시스템의 보안을 상실하였을 경우 절충하기 위한 것으로 CRL에 함께 저장된다.

2) 인증서 인증 체계

Fortezza 키 관리는 그림 12와 같이 X.509에서 권고한 다중 레벨 체계(multilevel hierarchy)에 기반한다.

(1) CA(Certificate Authority)

하부 사용자의 키와 인증서를 생성 및 인증, 폐지할 수 있는 권한이 있다.

(2) PCA(Policy Creation authority)

계층의 최상위에 위치하며 CA를 생성 및 인증, 폐지 하는 책임이 있다.

(3) PAA(Policy Approval Authority)

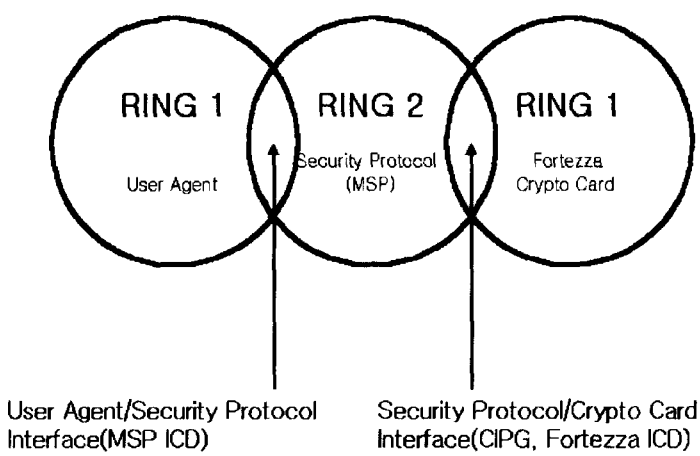

그림 13. Fortezza 시스템 모듈

계층에서 PCA의 상위에 있지만 PCA의 생성에는 제한이 있으며, 또한 CRL이나 CKL에 대한 권한이 없고 어떠한 인증서도 폐지할 수 없다.

(4) User

최하위 계층, 즉 사용자로 CA에 의해 카드와 함께 제공된다.

(5) ORA(Organizational Registration Authority)

CA와 User의 중간 매체로 키와 카드의 요청과 분배에 있어서 CA를 돕는다.

3) 시스템 모듈

Fortezza 프로그램은 그림 13과 같이 3개의 링으로 개념화될 수 있고 각각의 링은 Fortezza의 다양한 모듈을 상징한다.

(1) User Agent(RING 1)

첫 번째 링인 UA(User Agent)는 e-mail과 같은 메시지 시스템으로 일반적으로 프로토콜에 의해 정의되며 어떠한 보안 서비스가 사용자에게 어떻게 제공될 것인지를 결정한다. 또한 CRL로부터 인증서의 유효성을 확인하는 능력을 가지고 있다.

(2) User Agent/Security Protocol Interface(MSP ICD)

UA와 Security Protocol 사이의 인터페이스로 UA로부터 Security Protocol을 추출하는 역할이 있다.

(3) Security Protocol(RING 2)

두 번째 링인 Security Protocol은 보안 서비스의 구현에 있어서 논리적 또는 물리적 식별을 제공한다. 즉, UA 메시지와 헤더 정보를 처리하여 요청된 보안 서비스를 제공하는 역할이 있다.

(4) Security Protocol/Crypto Card Interface(CI Library)

Fortezza 암호화 카드와 인터페이스를 위해 필

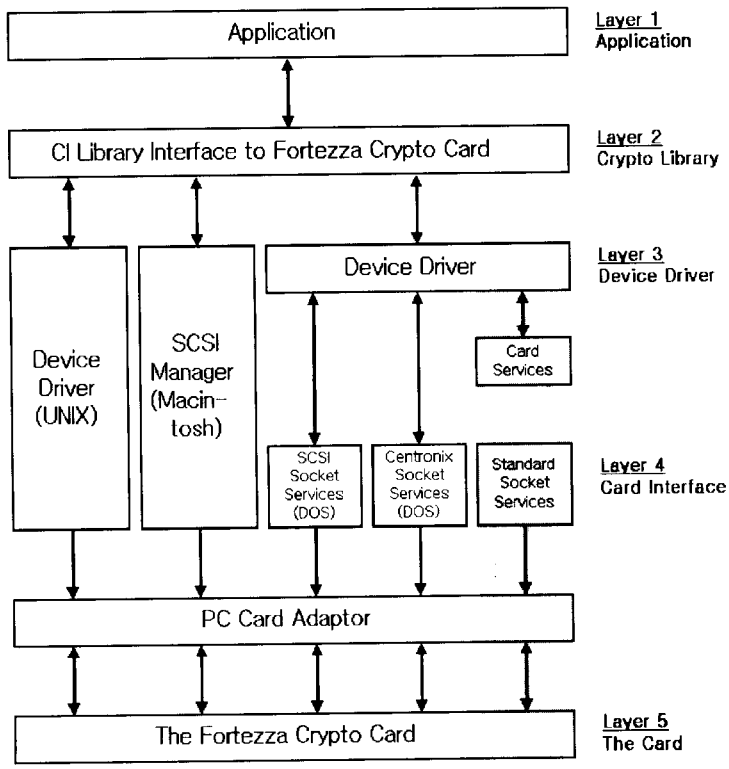

그림 14. Fortezza 카드 인터페이스

요한 CI(Cryptographic Interface) Library로 CIPG(Cryptologic Interface Programmers Guide For The Fortezza Crypto Card)에 자세히 상술되어 있다[7].

(5) Crypto Card(RING 3)

세 번째 링인 Crypto Card는 물리적 암호화 장치인 Fortezza 카드를 나타낸다. 카드에는 비밀키, 공개키, 발행자의 인증서가 저장되어 있고 디지털 서명, 해쉬 알고리즘, 키 교환, 암호화 및 복호화 기능을 수행한다. 한편 외부 디바이스로의 인터페이스는 그림 14와 같이 하드웨어 프랫폼과 운영체제(OS)에 따라 환경을 설정함으로써 올바른 동작을 할 수 있다[5].

V. 결 론

본 고에서는 국방부의 현대적 전쟁환경에 맞는 새로운 정보 시스템을 구축하여 폭넓은 정보교환과 효율적인 정보관리 능력을 증강하기 위하여 행정, 교육, 금융, 공안, 외교 및 물류 등의 독립적인 전용 전산망을 통합된 하나의 전산망으로 구축할 경우 다중등급보안을 처리하기 위해 미국 NSA가 주도하여 수행하고 있는 MISSI와 이에 이용되는 Fortezza, 그리고 현재 미국에서 구축중에 있는 DII의 구성에 대해 분석하였다. 또한, 향후 정보전에 대비한 각종 국방망의 통합 관리 및 운영을 위해 관련 미국의 DII 동향을 살펴보았고 국내 국방환경에 맞는 종합적인 대책의 기초 자료로서 역할을 하고자 한다. 이러한 자료를 통해 국내의 실정과 보안기술을 반영하여 효율적인 국방망 구축을 위한 지속적인 연구 및 투자가 이루어져야 할 것이다.

참 고 문 헌

[1] http://beta.missilab.com/MISSI/info/cover.html, "MISSI Introduction", 1996.

[2] 이철원외 3인, "국가 전산망을 위한 MISSI 분석", *한국통신정보보호학회지*, pp35-54, Vol. 7, No.2, 1997. 6.

[3] http://www.armadillo.huntsville.al.us/Fortezza_docs/ovrvw40a.pdf, "Fortezza Program Overview", February, 1996.

[4] http://www.armadillo.huntsville.al.us/Fortezza_docs/sdn801r30.pdf, "MISSI Access Control concept and Mechanisms", May, 1997.

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

[6] http://www.disa.mil/diimp/diimpo.pdf, "DII Master Plan Overview Version 7.0", March 2, 1998

[7] http://www.armadillo.huntsville.al.us/Fortezza_docs/cipg152.pdf, "Fortezza Cryptologic Interface Programmers Guide", January 30, 1996.

강 상 구(Sanggoo Kang)

1998년 2월 : 순천향대학교 전자공학과 졸업
1999년 2월~현재:동국대학교 전자공학과 석사과정

〈관심분야〉 네트워크 보안, 멀티미디어, 신호처리

송 유 진(Youjin Song)

1982년 2월:한국항공대학교 졸업
1987년 2월:경북대학교 석사
1995년 2월:일본 동경공업대학교 박사
1986년~1988년:LG 정보통신
1988년~1996년:한국전자통신연구원
1996년~현재:동국대학교 정보산업학과, 국제정보대학원 정보보호학과 교수

〈관심분야〉 암호이론, 인증 및 부호화이론, 전자상거래 응용, 전자화폐 등

신 재 호(Jaeho Shin)

1979년 2월:서울대학교
전자공학과 졸업
1982년 2월:서울대학교
전자공학과 석사
1987년 2월:서울대학교
전자공학과 박사
1978년 9월~1980년 4월:(주)대영전자 연구원
1983년 3월~1988년 2월:명지대학교
전자공학과 조교수
1992년 6월~1993년 6월:일본 新潟대학교
객원 연구원
1988년 3월~현재:동국대학교 전자공학과 교수

〈관심분야〉 신호처리, 멀티미디어, 정보보호