□특집□

미 국방부의 다수준 정보체계보안사업(MISSI)

김 종 기†

◈ 목 차 ◈

1. MISSI의 배경
2. MISSI 구성 요소
3. MISSI에 의한 보안 해결방안
4. 결 언

1. MISSI의 배경

미 국방부는 전시, 위기시, 평화시를 망라한 모든 군사작전의 상황에서 필요한 정보처리 및 통신 요구사항을 만족할 수 있는 국방정보화 기반구조(Defense Information Infrastructure; DII)를 구축하고자 국방 전체의 차원에서 노력을 기울이고 있다. DII는 통신 네트워크, 컴퓨터 하드웨어, 소프트웨어, 데이터베이스, 응용체계, 그리고 데이터를 제공하며, 음성, 자료, 이미지 등을 수집, 배포, 저장, 처리 및 표현하는 장비, 소프트웨어의 구축과 유지보수를 위한 응용체계와 데이터 공학방법론, 그리고 DII의 설계, 구축, 관리 및 운영을 위한 인력 및 자원을 포함한다.

DII의 개념은 C4IFTW(Command, Control, Communications, Computers and Intelligence For The Warrior)에 그 근거를 두고 있다. C4IFTW는 걸프전에서도 나타난 바와 같이 전쟁 양상이 대규모 물량전에서 상대방의 핵심 요소에 대한 신속하고 정밀한 타격을 가하기 위한 고속 기동전으로의 변천을 가능케 하기 위하여 적 정보를 아군이 실시간으로 공유하자는 것이다. 즉, 최종사용자인 전투원이 필요한 어떠한 정보라도 언제나 그리고 어디에서든지 이용할 수 있도록 하자는 것이다. 이러한 기본적인 요구사항을 충족하기 위해서는 현재 통합되어 있지 못하는 수많은 개별 정보처리시스템을 단일한 기반구조 위에서 원활한 정보유통이 가능하도록 만들어야 한다.

다수준 정보체계보안사업(Multi-level Information System Security Initiative; MISSI)의 목적은 DII를 구성하는 여러 요소들 간의 안전한 상호운용성(secure inter-operability)을 제공하는 다양한 대책을 제시하는데 있다. 이러한 목적을 달성하기 위하여 현재 또는 미래의 사용자의 요구를 충족시킬 수 있도록 사용자의 특정한 환경에 기인하는 보안상의 위협에 적절히 대처할 수 있는 시스템 차원의 보안대책을 제공한다. MISSI는 미 국가보안국(NSA)에 의해서 범국가적으로 추진되고 있는 정보체계 보안 프로그램인 MLS (Multi-Level Security) 프로그램과 밀접하게 관련되어 있다. MLS는 데이터의 다양한 비밀 수준과 종류에 따라 시스템

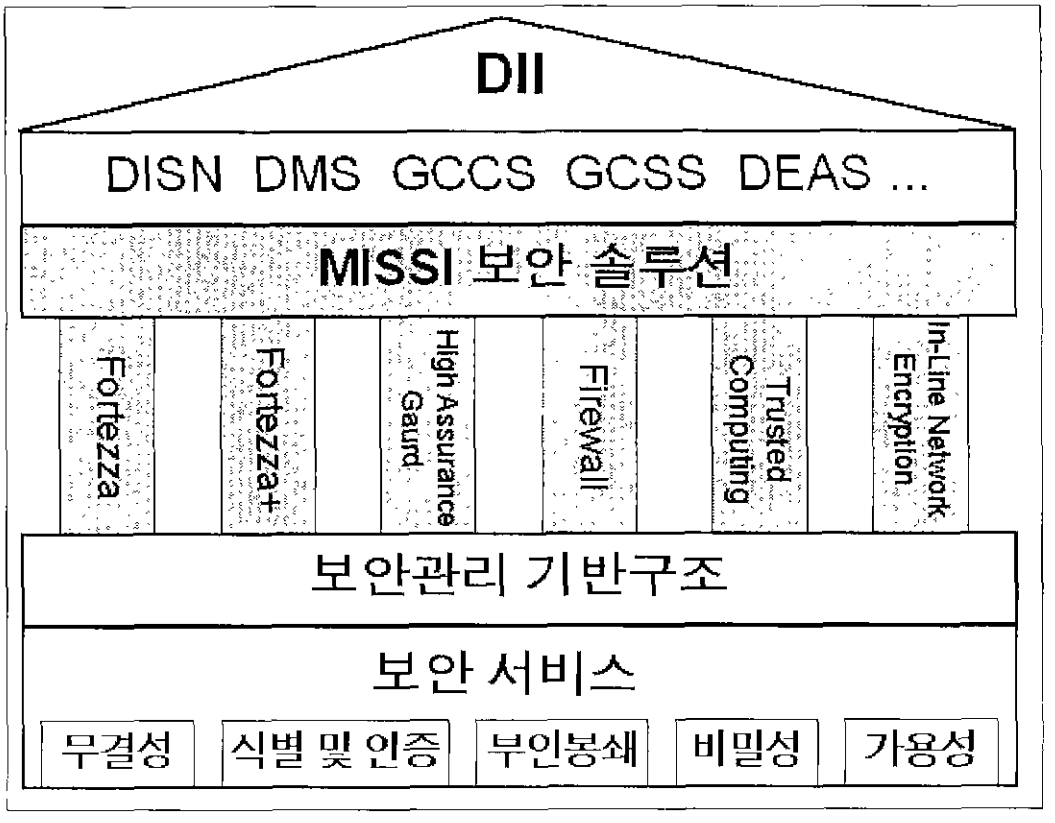
† 정회원 : 국방정보체계연구소 정보보호기술실 실장

에서 저장되거나 처리될 때 사용자의 비밀취급 권한과 업무상 인지필요성(need-to-know)에 따라 선택적으로 데이터에 대한 접근을 허용하는 보안 방법이다. 국방 환경에서 MLS의 결여는 상호운용성과 데이터의 통합을 제한함으로 운영상의 심각한 취약성을 초래할 우려가 있다.

MISSI는 다양한 워크스테이션과 네트워크 보안 표준, 그리고 공통적으로 적용되는 보안관리 기반구조(common security management infrastructure)를 통하여 사용자에게 광범위한 정보보안 기능을 제공한다. 전송되는 데이터가 제삼자에 의해서 우발적으로 또는 고의적으로 훼손되지 않도록 보장하는 서비스를 포함하여 강력한 식별 및 인증 기능이 워크스테이션과 네트워크 게이트웨이에 포함되어 비인가자의 접근을 막아준다. 통신되는 데이터는 암호화되며, 고도의 보안성이 요구되는 경우에는 데이터의 비밀성을 한층 더 강력하게 보장하는 고비도의 암호화를 이용한다. 그리고, 발신자의 신분을 확인할 수 있도록 디지털 서명이 이용된다. MISSI 표준은 대부분의 상용화된 전산 및 네트워크 표준에 부합하도록 되어 있으며, 전자우편, 월드 와이드 웹(World Wide Web)상에서의 파일 전송, 원격 로그인, 데이터베이스관리 등과 같은 응용체계를 그 대상으로 한다.

2. MISSI 구성 요소

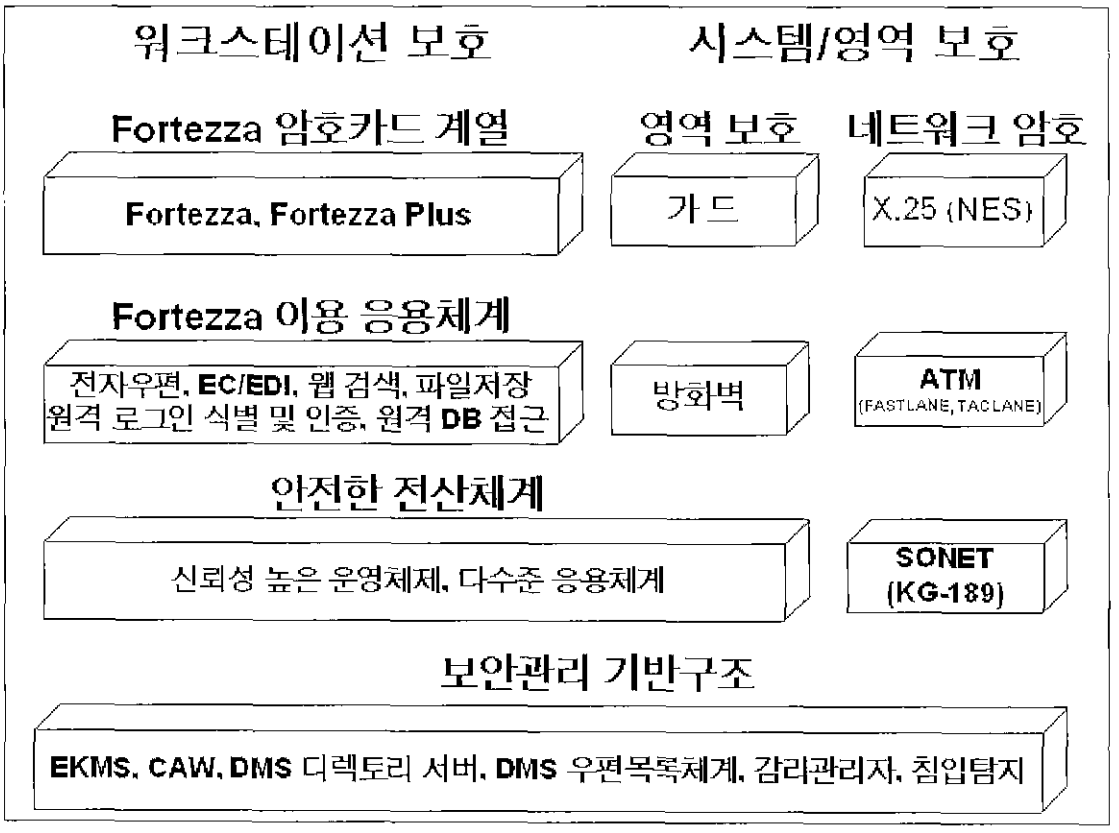
MISSI는 상호 호환성을 가진 제품과 공통된 보



(그림 1) MISSI의 전반적 구조

안관리 기반구조로 이루어진 통합된 보안구조를 통하여 DII를 구성하는 여러 시스템에 상호운용이 가능한 보안제품을 제공한다. DII의 주요 구성요소는 미 국방부의 다양한 정보체계의 단대단(end-to-end) 정보교환을 가능케 하는 통신 기반구조인 국방정보체계 네트워크 (Defense Information Systems Network; DISN), 미 국방부의 표준화된 전문전달 기능을 제공하는 국방전문처리체계 (Defense Message System; DMS), 군사작전에 필요한 제반 정보의 수집, 처리 및 분배와 작전 명령의 전달을 위한 전역 지휘통제체계 (Global Command and Control System; GCCS), 군수, 경리, 의무, 수송, 인사 등의 업무를 통합한 전역 전투지원체계 (Global Combat Support System; GCSS) 등이 있다.

DII의 여러 응용체계에 대하여 MISSI에서 제공되는 보안 서비스는 무결성, 식별 및 인증, 부인봉쇄, 비밀성, 그리고 가용성이 있다. 무결성은 처리되는 데이터가 무단으로 변경되지 않고 원래의 형태 그대로 유지되는 성질을 말하며, 식별 및 인증은 정보시스템을 이용하고자 하는 사용자의 신분을 확인하여 사용자의 정당성을 입증하는 절차이며, 부인봉쇄는 데이터의 송신자 또는 수신자가 송·수신 사실을 부정하지 못하도록 하는 것이다. 또한, 비밀성은 데이터의 내용을 열람할 권한이 없는 자에게 노출되지 않도록 하는 것이며, 가용



(그림 2) MISSI의 구성 제품

성이란 정당한 사용자에게 데이터가 항상 이용 가능하도록 하는 것이다. 이러한 보안 서비스를 제공하기 위하여 아래 그림 2에 나타난 바와 같은 다양한 제품들이 정부에서 발주되어 개발되거나 정부의 보안표준에 적합한 상용제품이 이용된다. MISSI에서 제공하는 제품은 응용체계 수준에서 암호화 기능을 제공하는 Fortezza/Fortezza+ 카드, Fortezza를 이용하는 응용체계, 신뢰성 높은 운영체제와 데이터베이스관리체계를 제공하는 안전한 전산체계, LAN 또는 일정한 영역 내에 있는 복수의 전산체계를 외부의 위협으로부터 보호하기 위한 시스템/내부영역 보안제품, 통신되는 데이터의 보안을 위한 네트워크 암호체계, 그리고 다양한 보안 제품들간의 원활한 상호운용성을 보장하기 위하여 키관리체계, 디렉토리 서비스, 인증 권한 워크스테이션과 같은 보안관리 기반구조로 구분된다.

2.1 Workstation 보안제품

워크스테이션에 대한 보안 서비스는 Fortezza 암호 카드와 Fortezza를 이용할 수 있는 응용체계에 의해서 제공되는데, Fortezza 카드는 LAN이나 WAN 환경에서 상용 워크스테이션에서 처리되는 대외비 수준의 데이터를 보호하는 서비스를 제공한다.

Fortezza 카드는 보안 서비스를 제공하는데 필요한 프로세서, 알고리즘 및 암호자재를 내장한 PCMCIA (Personal Computer Memory Card International Association) 규격의 장치로서, 처리되는 전문의 비밀 수준에 적합한 Capstone 칩 기술과 사용자의 증명(certificates), 그리고 사용자가 입력하는 개인식별번호(PIN)를 처리할 수 있다. 이 장치는 DMS에 대해서도 암호화와 인증 서비스를 제공하는데, PCMCIA 카드 판독기를 통하여 처리되며, 카드에 대한 인터페이스를 제공하는 서버, 워크스테이션, 또는 PC의 소프트웨어로 지원된다. Fortezza 카드에는 전자서명표준 (Digital Signature Standard) 알고리즘, 안전한 해쉬 알고리즘, Skipjack 암호화 알고리즘, 그리고 키 쌍 교환을 위한 키 암호화 알고리즘이 구현되며, 계산 수행을 위해 Capstone 칩이 사용된다. 모든 암호 알고리즘은 Capstone 칩에 내장되며, 사용자의 비밀키, 공개키, 승인, 비밀취급수준, 권한, 자료저장 키, 그리고 기타 암호와 관련된 요소들도 카드에 저장된다.

비밀정보를 취급하는 사용자를 위하여 강력한 암호화 기법을 이용한 Fortezza+는 Fortezza를 개량한 것으로 I급 비밀까지 암호화하는데 사용할 수 있다. Fortezza+를 이용하여 상이한 수준의 비밀정보를 처리하는 경우에는 시스템의 다른 요소의 보안상의 취약점에 의해서 영향을 받을 수 있다. 따라서, Fortezza+는 반드시 안전한 네트워크 서버(Secure Network Server)같은 고수준 보증 가드(high assurance guard)와 함께 사용되어야 한다.

사용자가 응용체계가 제공하는 기능을 수행하기 위해서 Fortezza 카드는 반드시 Fortezza를 이용 가능한 응용체계와 호환되어야 한다. 이러한 응용체계는 정부에 의해서 개발되거나 Fortezza의 보안기능과 접속되도록 수정된 상용 제품이다. 이러한 응용체계는 현재 다양하게 개발되어 있고 앞으로도 많이 추가될 것이다. Fortezza를 이용 가능한 응용체계의 주요 유형은 다음과 같다.

○ 전자 문서 처리 - Fortezza는 E-mail, EDI/EC, 펙시밀리 등에 암호화, 식별, 그리고 데이터 무결성의 보안 서비스를 제공한다.

○ WWW - 강력한 식별 및 인증 기능과 안전한 소켓 계층(secure sockets layer) 접속을 이용하여 WWW의 안전한 이용을 보장한다.

○ 파일과 저장매체의 암호 - 저장매체에 수록된 데이터를 암호화할 수 있는 응용체계를 Fortezza를 이용하여 개발한다.

○ 접근통제/강력한 인증 - 사용자의 개인식별번호(PIN)와 전자서명을 이용하여 강력한 식별 및 인증 기능을 제공하는 응용체계를 Fortezza와 연계할 수 있다.
○ 원격 데이터베이스 접근 - Fortezza의 식별 및 인증 기능을 이용하여 원격지로부터 데이터베이스 응용체계에 대한 접근통제 기능을 제공한다.
○ Fortezza 클라이언트-서버 제품 - 클라이언트-서버 환경에서도 사용자의 보안 요구를 충족시키기 위하여 Fortezza 카드를 이용할 수 있다. Fortezza 카드를 이용 가능한 응용체계는 인가된 사용자가 클라이언트에서 안전하게 서버로 로그인할 수 있게 한다. 응용체계 개발에 미국 또는 국제 표준을 준수한다면 다양한 서버/데이타베이스 시스템의 상호운용성을 극대화하면서 향후에 무리 없이 추가적인 개선이 가능하다.
○ EC/EDI - 전자 상거래와 자료 교환의 안전성을 확보하기 위하여 ANSI X.12 EC/EDI 표준과 Fortezza를 결합하여 정부와 민간 회사간의 거래의 인증, 무결성, 그리고 비밀성을 제공한다.
○ 국방전문처리체계 (DMS) - DMS X.400 E-mail 응용체계와 X.500 디렉토리 체계와 연계하여 DMS의 보안 기능을 제공한다.

2.2 보안관리 기반구조 (Security Management Infrastructure)

보안관리 기반구조는 모든 MISSI 구성요소에 대한 공통적인 보안 지원을 위한 기반을 다음의 도구를 이용하여 제공한다.
○ 증명 권한 워크스테이션 (Certification Authority Workstation) - 신뢰성 높은 운영체제와 특수 목적의 응용 소프트웨어를 탑재한 상용 워크스테이션이다. 보통 로컬 시스템 내에 위치하며, 암호 키와 같은 사용자의 보안 특성을 내장한 Fortezza 카드를 관리한다.
○ 디렉토리 시스템 체계 (Directory System Agent) - 사용자의 보편적인 이름을 제공하여 MISSI 제품의 운영에 필수적인 공개된 보안 정보를 저장한다. 사용자에 대한 X.500 증명이 대표적인 예이다.
○ 우편 목록 체계 (Mail List Agent) - 다수의 수신자에게 E-mail이 발송될 때 안전성을 제공한다
○ 감리 관리자 (Audit Manager) - MISSI 제품에 대한 보안과 관련이 있는 감리 사건을 수집하고 분석하는 기능을 제공한다.

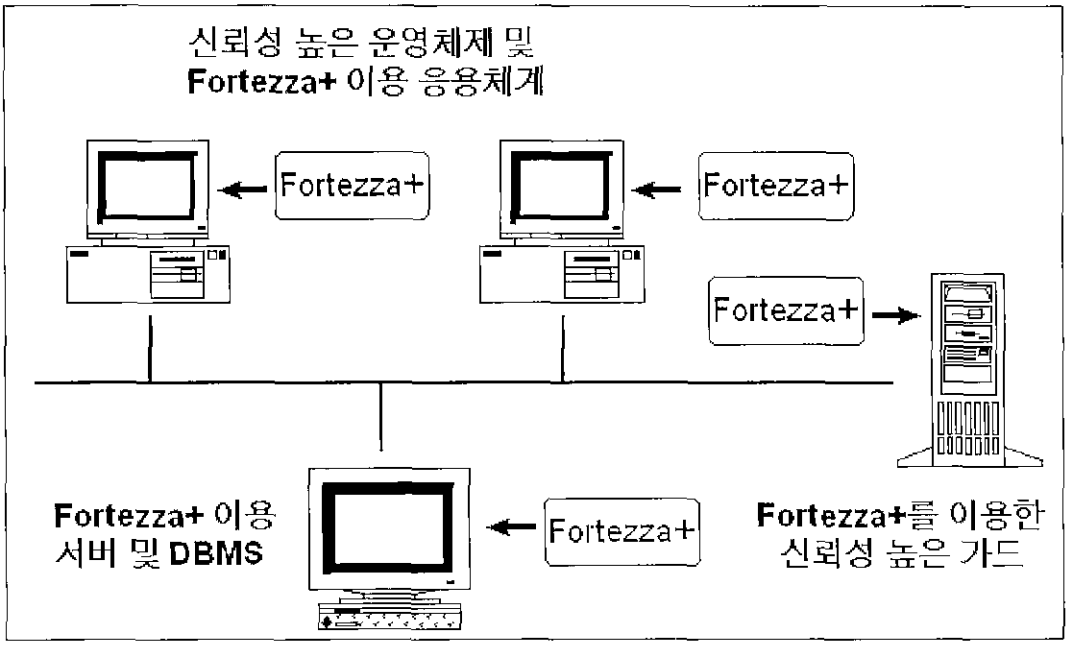
2.3 안전한 전산체계 (Secure Computing)

안전한 전산체계에는 전산환경의 전반적인 보안성을 향상시키기 위한 기능과 그 기능의 적절함에 대한 보증이 추가된다. 데이터 레이블, 데이터 분리, 접근통제목록, 데이터 무결성, 보안 관련 활동의 감리, PC 카드를 이용한 암호화 등의 기능이 그 예이다. 보증은 보안에 중요한 기능이 적절하게 수행되고 있다는 확신을 얻기 위한 구체적인 설계와 설계 분석 활동이다. 위장된 접근경로(covert channel)같은 보안성을 저해하는 숨겨진 기능이 제거되거나 최소화되어야 한다.

워크스테이션 보안을 향상시키기 위하여 위에서 설명한 기능과 보증을 가진 상용화된 UNIX 계열의 신뢰할 수 있는 운영체제와 함께 다수의 데이터베이스관리체계(DBMS)가 있다. 그림 4에 나타난 바와 같이 워크스테이션에 Fortezza/Fortezza+를 고보증 전산 요소와 통합함으로써 송신자와 수신자간의 통신의 보안성을 향상시킨다. 이렇게 함으로써 궁극적으로 정보처리 영역 외부와 내부의 위협에 대한 취약점을 감소시킬 수 있다.

2.4 체계/내부 영역 보안제품

고수준 보증 가드(high assurance guard)는 비밀이 아닌 정보의 공개는 허용하면서 비밀정보의



(그림 3) 신뢰성 높은 전산체계의 구성 예

비인가된 공개는 허용하지 않는다는 보안정책을 수행한다. 이러한 다수준 보안 (MLS) 기능은 보안영역 외부로부터의 접근 요청을 승인하여 보안영역에 대한 외부의 공격을 막는다. 이 가드는 또한 자동적으로 정보 레이블을 검사하여 Fortezza로 보호되는 워크스테이션에서 보안 서비스가 작동되도록 보장한다. 안전한 네트워크 서버(Secure Network Server; SNS)는 MISSI 가드의 한 예이다.

MISSI 방화벽(firewall)은 대외비 (SBU) 정보 영역과 잠재적인 위험을 가진 네트워크 사이의 연결을 보호한다. Fortezza를 이용한 식별 및 인증 기능을 가진 방화벽은 대외비 영역 외부의 사용자에 의한 접근을 통제하는 기능을 수행한다. 방화벽의 일반적인 형태는 스크리닝 라우터 (패킷 필터 시스템), 응용수준 게이트웨이 (프락시), 그리고 라우터와 응용수준 게이트웨이의 복합형이 있다.

네트워크 선로 암호장치(In-Line Network Encryptor)는 보통 내부 영역과 외부 네트워크의 경계에 위치한다. INE는 암호화를 이용하여 LAN과 WAN에서 비밀성과 무결성을 제공하며, 암호키 관리로 접근통제를 수행하며, 특별한 경우에는 전송량의 흐름에 대한 정보의 노출을 막아준다. INE에는 다음과 같은 제품이 있으며, MISSI를 지원하는 상용 제품은 표 1과 같이 다양하게 개발되어 있다.

○ Motorola NES - X.25 패킷 스위치 또는 이더넷 네트워크에서 운영되는 네트워크 암호체계

○ GTE KG-175 TACLANE - ATM 또는 IP 전술 네트워크에서 운영

○ GTE KG-75 FASTLANE - 622Mbps까지의 ATM에서 운영

○ Motorola KG-189 암호장치 - 동기 광섬유 네트워크(SONET)에서 운영

<표 1> MISSI 상용 제품

종류	상용 제품
보안관리 기반구조	- BBN CA Workstation - Motorola Audit Agent - Motorola Audit Manager - Motorola CAW
PC 암호 카드	- Spyrus Fortezza Card - IRE A400S Fortezza Modem - Mykotronx Fortezza+ Card
SMTP 전자우편	- LJL Armor-Mail Add-on for cc:Mail, Eudora Pro, MacOS, MS Exchange, MS Mail - SecureWare SecureMail/MSP
그룹웨어	- Lotus Notes DMS - MS Exchange - Novell Groupwise 5 for DMS
X.400 전자우편	- ESL EXM DMS - Lotus Notes Express - MS Exchange
파일 암호장치	- AT&T Secret Agent - Lockheed-Martin Minotaur II - Spyrus Locksmith
네트워크 가드 및 방화벽	- BDM CyberShield - Checkpoint Firewall-1 - Raptor Systems Eagle - Wang DMS Guard - Wang DMS Firewall Plus - TIS DMS Firewall Plus - SCC Sidewinder - SCC SNS 2a & 2b - V-ONE SmartWall - V-ONE DMS Firewall Plus
식별/인증	- SCC LOCKout Fortezza

3. MISSI에 의한 보안 해결방안

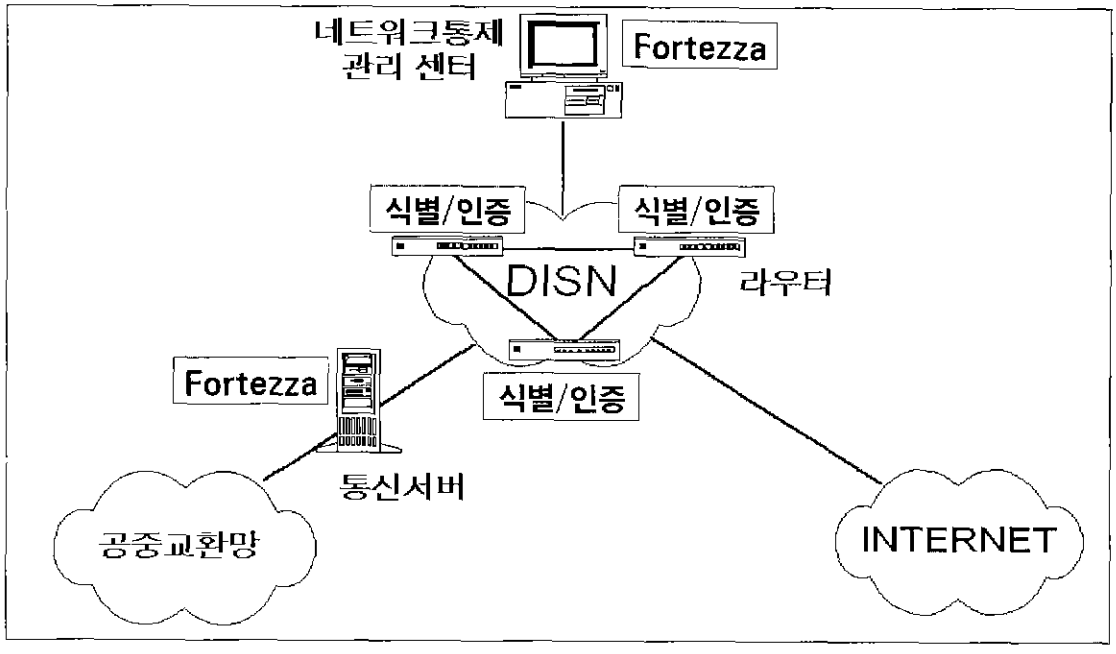
MISSI 제품들이 실제로 어떻게 적용되는지에 대한 몇 가지 방안이 제시되어 있다. 이러한 해결방안은 대부분의 일반적인 사용자의 보안 요구사항을 반영하는 단일 수준 또는 다수준 보안 구조를 나타낸다. 제시되어 있는 간단한 구조적 모형을 사용자의 요구사항과 비교해봄으로써 MISSI 제품을 사용자의 체계에 쉽게 구현할 수 있도록 한다.

그림 4는 MISSI의 통신보안에 대한 해결방안을 보여준다. 이 방안은 DISN 통신 네트워크 환경에 대한 보안서비스 중에서 가용성에 중점을 두고 있다. 미 국방부의 통신망 가입자들은 MILNET에서 IP 기반의 NIPRNET으로 전환해 가고 있으며, 향후에는 ATM 기반의 네트워크로 옮겨갈 것이다. DISN 자원에 대한 관리는 네트워크관리 통제센터에서 이루어지며, 네트워크 관리 명령을 인증하기 위하여 Fortezza가 채택된다. 외부 네트워크로부터 DISN을 보호하기 위하여 Fortezza의 식별 및 인증 기능을 가진 라우터와 통신 서버가 이용된다.

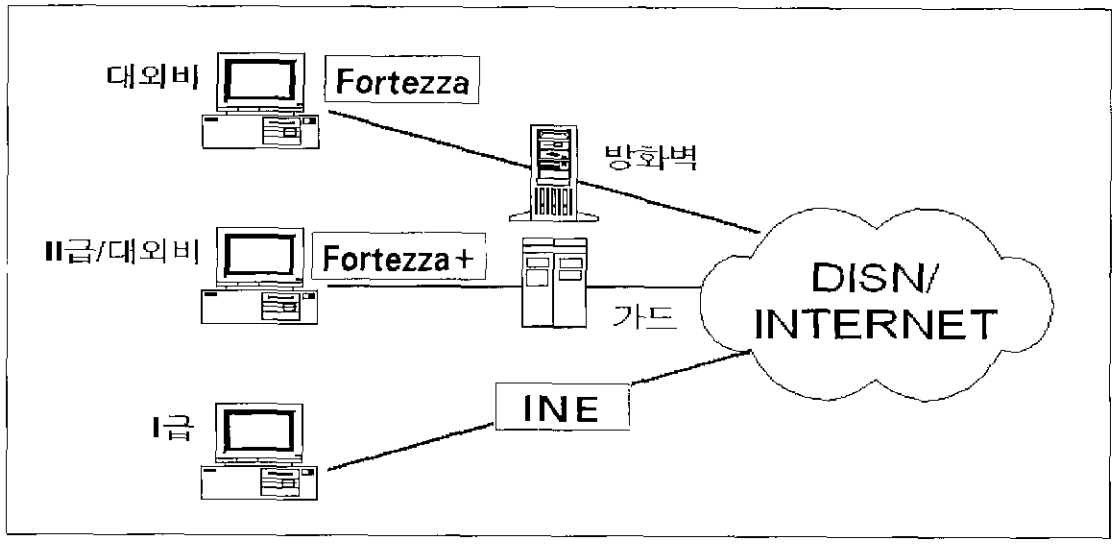
DISN과 INTERNET을 통하여 대외비 이하 정보를 통신하는 경우에는 Fortezza와 Fortezza를 이용하는 응용체계가 탑재된 워크스테이션을 이용하는 단일 수준 보안 구조가 해결방안으로 제시되었다. 내부 영역과 DISN 간의 분리는 방화벽이 이용된다. II급 비밀을 통신할 수 있는 네트워크에서 대외비 이하의 정보를 외부와 교환하고자 할 때에는 고보증 가드를 DISN 또는 INTERNET과의 접속점에 배치한다. 한편, I급 비밀을 통신하기 위해서는 내부영역과 DISN 또는 INTERNET 사이에 네트워크 선로 암호장치(INE)를 설치한다. 비밀등급 별로 각각의 보안장비를 이용함으로써 그림 5와 같이 동일한 통신망에서 상이한 비밀등급을 가진 정보의 교환이 가능해진다.

4. 결 언

MISSI는 일관된 보안구조의 정립을 위한 표준, 프로토콜 및 인터페이스의 개발에 의하여 미 국



(그림 4) 통신보안 해결방안



(그림 5) 다수준보안 해결방안

방부의 DII의 보안에 대한 해결방안을 제시한다.

미 국방부는 앞으로 멀티미디어 환경에 신속하게 적응하기 위하여 보안성이 높은 상용 제품의 개발을 위하여 업계와 긴밀하게 협조해 나갈 예정

이다. MISSI는 현재와 미래의 다양한 정보체계의 보안 요구사항을 만족할 수 있는 적절한 해결방안을 제시해 줄 것이다.

MISSI의 핵심은 보안상의 취약점을 가지고 있는 네트워크에서 사용자가 안전하게 통신할 수 있는 수단을 제공해 주고자 하는 것이다. 우리 나라의 공공기관이나 정부, 특히 민감한 정보의 통신을 많이 필요로 하는 조직에서는 전용 정보통신망을 구축하여 이용하고 있다. 그러나, 통신망의 확장에 따른 경제적인 면에서나 외부망과의 연결 필요성 때문에 전용망 만을 고집하기에는 한계가 있다. 또한 전세계적인 통신망을 구축할 필요가 있는 대기업은 INTERNET을 이용하여 가상 사설망을 구축하기도 한다. 이러한 경우, 보안 문제의 해결은 필수적인 전제조건이 되며, MISSI와 같은 다수준 보안 개념이 적절한 해결방안이 될 것이다.

참고문헌

[1] Department of the Army, "Information Systems Security," Army Regulation 380-19, August 1990.

[2] Morrie gasser, "Building a Secure Computer System," Van Nostrand Reinhold Co., N.Y., 1988.

[3] Charles P. Pfleeger, "Security in Computing," Prentice Hall, N.J., 1989.

[4] Department of Defense, "Security Requirements for Automated Information Systems DoD 5200.28," March 1988.

[5] Department of Defense, "Information Security Program Regulation DoD 5200.1-R." January 1997.

[6] G.F. Hice and S.H. Wold, "DMS: Prologue to the Govement E-Mail Revolution," J.G. Van Dyke & Associates, Inc., MD, 1995.

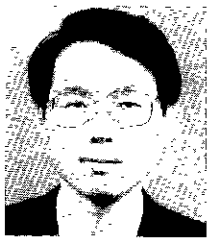
[7] R. Cooncy and G. Bilinski, "The Multilevel Information Systems Security Initiative," Department of the Navy, December 1995.

[8] DISA, MMSSI Program, URL: http://beta.missilab.com/MISSI/info

[9] DISA, DMS Program Overview, URL: http://www.disa.mil/D2/DMS/docs/progovw

[10] W. DeLora, A. sharpe, S. May, and C. Bonnatti, "Defense Message System Messaging, Directory Services, and Security Services." URL: http://www.disa.mil/D2/DMS/docs/milcom/smay.html

[11] 김기복, 김종기, "미 국방부의 정보체계 보호 제도 고찰," 정보보호와 암호학 워크숍 (WISC) 논문집, 한국전자통신연구소, pp. 367-381, 1996.



김 종 기

1987년 부산대 경영학과 졸업 (경영학사)
1988년 미국 아칸소주립대 대학원 졸업 (경영학석사)
1992년 미국 미시시피주립대 (경영정보학박사)
1993년 국방정보체계연구소 선임연구원
1995년 - 현재 국방정보체계연구소 정보보호기술실 실장
관심분야 : 정보보호 정책, 위험분석