문서의 등급을 고려한 메시지전송 프로토콜 구현에 관한 연구

신 승 중* · 김 현 수**

A Study on the Implementation of a Message Transfer Protocol with Document Classification

Seung-Jung Shin* · Hyun-Soo Kim**

Abstract

In this paper we have developed a message transfer protocol, CMP, which improves MSP's message processing capability. The proposed method has taken into account document classification to improve the efficiency of message processing. The difference between the conventional MSP and CMP has been addressed. The CMP's performance has been shown by various experiments including number, alphabet, Korean letter, Chinese letter, music sound and compression file transmission. And security capability of both protocols has been compared based on the specification of FIPS 140-2. The CMP's overall performance is shown to be superior to that of MSP on the processing speed in the performance perspective and on the function of cryptographic module interface and cryptographic key management in the security perspective respectively.

* 중부대학교 정보공학부 교수
** 국민대학교 정보관리학부 교수

1. 서 론

최근 인터넷 확산과 이를 기반으로 한 전자상거래가 전세계적으로 활성화되면서 그에 따른 여러 가지 문제점들이 발생하고 있다. 이중에서 해커들에 의한 해킹은 최근 사회적인 문제로 비화될 정도로그 영향력이 커져가고 있는 상황에 있다. 네트웍 상에서 발생되는 여러 가지 보안 문제들을 해결하기 위해 외국은 물론 국내에서도 많은 연구가 진행 중이다. 그러나, 이중 가장 기본이 되는 메시지 전송에 관한 보안 및 인증 문제를 해결하기 위한 메시지 전송프로토콜은 현재 미국내 군수품에 관한 수출 규제로 인해 국내에 도입되고 있지 못한 실정에 놓여있고, 실제 도입이 된다 하더라도 국내 정보시스템 특성에 맞게 수정 및 보완을 하기 위해 상당한 시일이 소요될 것으로 예상된다.

본 연구는 이러한 상황하에서 국내 정보시스템 및 보안 환경의 특성을 고려한 암호문 메시지 프로토콜(CMP : Cryptography Message Protocol)구현 및 분석연구를 수행하였다.

이를 위하여 먼저, 분산 컴퓨팅환경에서 보안서비스를 제공하기 위해 미 국방부(DoD)에서 사용하고 있는 MSP(Message Security Protocol)를 기반으로하여 MSP의 문제점을 도출하고, 이를 해결할 수 있는 방안에 대해 연구하였다. 국내 정보시스템 환경에 적합한 메시지 보안체계를 조사하기 위하여 전문가 그룹을 대상으로 면담과 설문을 실시 하였다. 수집된 요구사항을 프로토콜 설계에 반영하였다.

본 논문의 구성은 다음과 같다. 제2장에서는 미 국방부에서 표준으로 채택하고 있는 MSP에 관해 살펴보고, MSP의 문제점과 국내 정보시스템 환경하에서의 보안요구사항에 대해 조사한 결과를 제시하였다. 제3장에서는 MSP의 문제점을 해결하고 국내 정보시스템 환경에 적합한 메시지 전송 프로토콜인 CMP의 설계 상세내용을 제시하고, CMP와 MSP을 구현하였다. 제4장에서는 실제 구현한 CMP와 MSP를 보안성측면과 성능측면에서 각각 비교하고 토의 및 분석을 하였다. 마지막 제5장에서는 결론을 제시하였다.

2. MSP 및 관련연구

2.1 메시지전송시스템의 정의 및 발전

본 연구에서의 메시지전송시스템은 분산 컴퓨터 환경에서 보안서비스를 부가하여 안전하게 메시지를 처리하는 시스템이다.

메시지 전송프로토콜은 X.400을 기반으로 기밀성, 무결성, 송·수신자 정보 전달, 송신자 부인봉쇄 등의 다양한 기능을 구사함으로써 자료의 위·변조를 막고 인증된 상태에서의 메시지를 전송 할 수 있어 군사적 목적에 사용할 수 있게 되었다.

〈표 1〉 MSP 발전추이

구 분	내 용	년도
MSP Ver1.0	X.400(메시지전송환경) 기초로 한 메시지 전송	1986
MSP Ver2.0	SDNS(Secure Data Network System) 적용 및 응용화	1992
MSP Ver3.0	SDN(Secure Data Network).701	1994
MSP Ver4.0	e-mail의 응용적용, 다목적 활용 응용화	1996
MSP Ver4.0.1	SDN.701 기술변화	1997
CSP	Common Security Protocol(명칭 변경)	1998
	SDN.702 : X.509, CRL(Certification Revocation List) 기능 추가	1999

1986년에 MSP 버전 1.0이 발표되었으며, 1992년에 전송 메세지를 보다 안전하게 전송할 수 있도록 개선한 것이 MSP 버전 2.0이다. 다중사용

자나 개방형 시스템 및 분산시스템환경에서 메시지를 전달하고 위·변조, 인증문제해결 기능을 첨가하여 발전시킨 것이 MSP3.0이다. 그리고 e-mail에 적용하고, 위·변조기술, 인증, 다중사용자관리기능(접근카드사용)을 부가하여 MSP 4.0 및 4.0.1를 개발하였고, 1998년 공공서비스로 전환하기 위해서 CSP(Common Security Protocol)로 명칭을 변경하고, 인증서 제공기술과 인증서취소목록관리(CRL : Certification Revocation List)에 필요한 기술을 첨가하여 1999년 3월에 보완된 버전을 발표하였다. 본 논문에서는 CSP까지를 포함하여 MSP로 통칭하기로 한다.

최근의 메시지 전송 관련 제품들은 <표 2>와 같으며 이는 FIPS(Federal Information Processing Standard) 140-1에 의해서 1995년부터 2000년 1월까지 제품, 공급회사, 사용된 암호키들을 비교한 것이다. 메시지 전송 시스템들은 S/W 또는 H/W 형태로 개발되었으며, 사용된 암호화 관련 알고리즘은 공개키 및 전자서명알고리즘(RSA : Rivest, Shamir, Adleman), 대칭키(DES : Data Encryption Standard), 해쉬함수(MD5 : Message Digest 5, SHA : Secure Hash Algorithm) 등으로 문서의 인증을 고려한 제품들이다[Abram & Podell 1987, FIPS 49 1977, Simmizu & Miyaguchi 1987].

최초의 상용화 제품은 1995년 10월 출시한 Entrust Technologies Limited 사의 S/W 형태의 Entrust Cryptographic Kernel v1.9이며, H/W 제품으로는 Motorola사의 ASTRO제품이 대표적이다.

여기서 RSA는 키교환 데이터 암호화 및 전자서명에 사용되며, 각종 보안 알고리즘과 공유하여 사용되고 있다. 해쉬함수를 동반하여 전자서명을 하면 필요한 데이터의 변환이 생기고, 이러한 변환으로 메시지를 위·변조 확인작업 및 인증을 한다. 또한 대칭키로 사용되는 DES는 비밀키라고도 하며, 대칭키(Symmetric Key)방식의 암호화이다. DES는 1976년에 미국의 표준으로 채택되어 매 5년마다 표준여부를 결정한다. 그러나 1997년에 암호화키가 깨어져 이를 보강하는 알고리즘개발이 한창이며, 후속 대칭키로는 Triple DES, RC2(Rivest's Cipher를 의미하며, DES보다 2-3배 빠름, RSA사가 개발한 블록알고리즘임), RC5, AES(Advanced Encryption Standard)등이 있다.

<표 2> 메시지전송 관련 제품 비교표

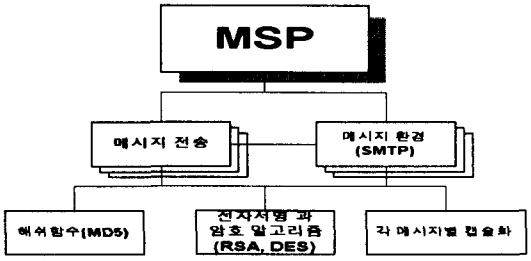
구분	제품명	공급회사	암호알고리즘의 사양	공급일
S/W	Entrust Cryptographic Kernel, v5.0	Entrust Technologies Limited	DES, DES MAC, DSA/SHA-1, RSA, Triple DES RC2, RC4, IDEA, MD5, MD2, RIPEMD-160, HMAC-SHA-1, and D-H key agreement	2000.1.7
	P/M 650000-2	Mykotronx 사	DES/SHA-1, Skipjack, KEA	99.8.11
	Postage Plus Client Communication Module	Neopost 사	DES, SHA-1, Triple DES	98.10.28
	Entrust Cryptographic Kernel, v4.0	Entrust Technologies Limited	DES, DSA/SHA-1, Triple DES(미정부허가), DES/SHA-1, RC2-5, MD2, MD5, RSA, D-H	98. 7.30
H/W	ASTRO-TAC Digital Interface Unit (DIU) Encryption Module Controller (EMC)	Motorola 사 Secure Design Center	DES DES-XL, DVP-XL, DVI-XL, DVI-SPFL	2000.1.5
	FORTEZZA Crypto Card	Mykotronx 사	DES/SHA-1, Skipjack, KEA	99.9.13
	Luna2	Chrysalis-ITS	Triple DES(미정부허가), DES/SHA-1, RC2-5, MD2, MD5, RSA, D-H	98.12.8
	ASTRO	Motorola	DES, DES-XL, DVP	98.1.30
	Netscape Security Module 1 (ID : fipscm_v1)	Netscape Communications 사	DES, DSA, SHA-1 RSA, RC4, RC5, MD2, MD5.	97.8.29

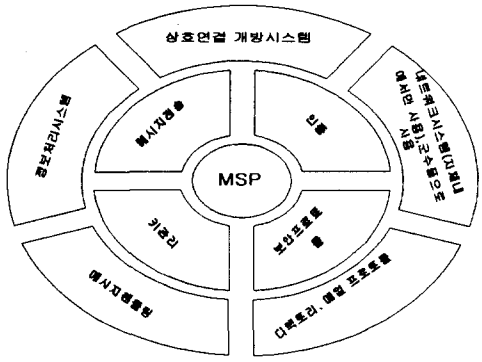
해쉬함수인 MD는 1989년에 MD2, 1990년에 MD4, 1991년 MD5가 Rivest에 의해서 개발되었으며, SHA는 NIST에서 개발하여, FIPS로

발표하였고, SHA-1은 SHA의 개정판으로 1994년에 발표되었다.

2.2 MSP의 구조 및 특징

MSP는 본래 미국 NSA(National Security Agency)에서 국가의 행정, 국방, 교육, 의료, 물류 등 각 분야의 종합 보안 해결책의 하나로 개발되었으며, 컴퓨터보안, 통신보안, 물리적 보안, 개인정보보호, 행정업무보안을 목적으로 하는 메시지 전송시스템이다.





(그림 1) MSP의 구조와 기능

이러한 MSP의 기본 구조는 (그림 1)과 같이 SMTP(Simple Mail Transfer Protocol)환경하에서 암호화된 메시지를 헤딩(Security Heading)하여 전송하는 것으로 특히, 상호연결 개방시스템은 이기종 시스템이나 서로 다른 운영체제 하에서도 안전하게 메시지를 전달하는 기능을 구현하기 위한 구조이다. 또한 메시지를 접근자(포테자카드 소지자)의 취급등급에 따라 처리되도록 설계하였으며, 문서의 중요성을 감안하여 메시지별로 캡슐화하는 기능도 포함되어 있다.

(그림 1)에서 나타난 MSP의 구조 및 기능의 내용을 국제 표준 기구의 표준안과 비교하여 상세히 표현하면 <표 3>과 같다[FIPS 49 1977, FIPS 140-2 1999, SDN701 1994]. <표 3>에서 보는 바와 같이 정보처리시스템, 상호연결 개방시스템, 메시지운용, 훈령집 등은 ISO(국제표준화 기구) 및 CCITT(국제전신전화자문위원회)의 표준을, 메일 전송 프로토콜 및 Internet 표준안은 RFC(Request For Comments - IAB : Internet Architecture Board의 권고안)를, 망구성 시스템은 SDN(보안자료전송네트워크)의 표준을 참조하고 있다.

메시지 전송시스템은 통신 프로토콜 위에 정보의 누출을 방지하는 프로토콜을 이용하여 구

〈표 3〉 MSP 관련기준안 비교표

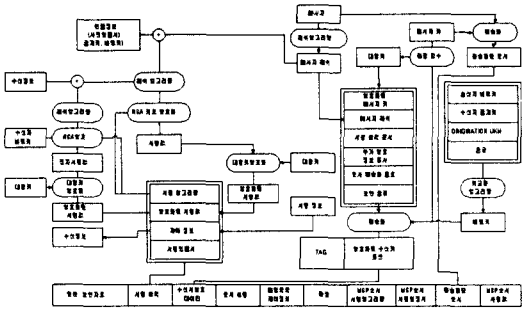
형 태	내 용	기준안 구분
정보처리시스템	개방시스템상호연결-보안구조	ISO 7498/2
상호연결 개방시스템	CCITT 응용을 위한 기본 참고모델, 변환문 요약의 상세화, 변화문 요약을 위한 기본암호규칙의 상세화	CCITT X.200 CCITT X.208 CCITT X.209
메시지운용	서비스와 시스템의 요약, 메시지전송시스템 요약정보서비스의 정의 및 절차, 프로토콜의 상세화, 메시지 시스템	CCITT X.400 CCITT X.411 CCITT X.419 CCITT X.420
훈령집	메일디렉토리 Models. 인증의 기본틀	CCITT X.501 CCITT X.509
메일 표준안	메일전송프로토콜	RFC821
Internet 표준안	ARPA 사용메시지의 기본틀을 위한 표준안	RFC822
안전한자료망구성 시스템	메시지보안프로토콜, SDNS MSP 이용을 위한 훈령의 상세화, X.400 Rekey Agent Protocol. 접근기능개념의 문서, 접근기능의 상세화, 키관리프로토콜의 상세화	SDN.701 SDN.702 SDN.703 SDN.801 SDN.802 SDN.903

현되는 시스템으로 <표 3>의 여러 기능이 구현되도록 설계되어 보안성 및 안전성이 보장되어야 하기 때문에 미 국방부에서는 보안 제품의 기준을 다음 <표 4>와 같이 제시하고 있다.

<표 4>의 보안제품 기준안에는 MSP가 포함되어 있으며, MSP에 사용되는 DES나 RSA는 미국 상무부 표준국(NBS : 현재의 NIST)이 1977년에 제정 발표한 표준암호 방식으로, 1993년에 제정된 인터넷의 PEM(Privacy Enhanced Mail)의 표준으로 사용되고 있다[SDN701 1994].

〈표 4〉 미 국방부의 보안제품 기준안

구 분	내 용	비고
MIL-STD-2045-18500-1	서비스 기본 배경과 지원부분	
MIL-STD-2045-18500-2	프로토콜의 내용 및 정의와 분류사항	
MIL-STD-2045-18500-3	메시지전송을 위한 요구조건	
MIL-STD-2045-18500-4	전송시스템의 접근 요구 사항	MSP 사용
MIL-STD-2045-18500-5	전송시스템의 접근 요구 사항	MSP 사용



(그림 2) MSP 프로토콜

이러한 MSP 프로토콜은 기존의 X.400 MTS (Message Transfer System)에 투명성을 제공하고 MSP 보호 서비스를 위한 MSP UA(User Agent)와 기능 개체(Functional entity)들로 구성되어 있으며 (그림 2)와 같은 기본 골격으로 구성되어 있다. MSP는 대형 시스템에서 주로 운영되며 등급 보안을 다중화 하기 위하여 비밀등급카드를 이용하여 접근자를 통제하고 있고 수신자의 인증서(Certificate), 사용자 Keying Material(UKM), 보조벡터(Auxiliary Vector, AV)를 얻기 위해 X.501과 X.509의 디렉토리 시스템을 이용하는 특징을 가지고 있다.

2.3 문제점 및 개선방안

MSP의 문제점은 기능적 측면, 문서처리측면, 군수품 규제 측면으로 나누어 분석 할 수 있다. 우선 기능적인 측면에서는 통합된 전산망사용으로 유지보수비용이 발생되며, 초대형 시스템의 다중 접근 방식 사용에 따른 주변 시스템의 필요성이 증대된다. 또한 일괄처리로 인한 지연 및 중요도에 관계없는 처리과정의 문제가 발생하고 있다. 문서처리측면에서는 단일화된 통신채널 이용으로 병목현상이 우려된다. 군수품 규제 측면에서는 현 컴퓨터환경에서 보안성이 낮은 비트만을 사용하도록 규제하고 있는 문제가 있다. 이러한 문제점을 요약하면 다음 <표 5>와 같다.

〈표 5〉 MSP의 문제점

구 분	MSP의 문제점	비 고
기능적인 측면	통합된 전산망을 사용하기 위해 파일전송을 위한 다양한 모듈과 H/W적인 장치요구 및 유지보수에 대한 비용 발생	운영체제에 대한 처리문제
문서처리 측면	단일화 된 IP를 사용하므로서 병목현상으로 업무처리 시 지연발생	메시지별 보안 차별화 처리
군수품 규제	암호화에 대한 미국의 강력한 보호와 미래에 대한 자국의 권익으로 메시지전송기술 사용에 대한 제한 사항 발생 예상	자체적인 개발의 필요성

이러한 MSP의 문제점을 개선하고 안전한 메시지 처리 시스템을 구현하기 위해 메시지전송 프로토콜이 갖추어야 할 기능의 우선 순위에 대하여 전문가를 대상으로 설문조사를 실시하였다. 설문조사는 국내 연구소와 관련기관 종사자 53명을 대상으로 실시되었으며 총 응답자 47명 중 5명은 응답내용의 오류로 인하여 분석대상에서 제외하고, 42명의 응답을 분석하여 <표 6>과 같은 결과를 얻었다. <표 6>의 속성값들은 전체의 합이 1이 되도록 하여 각 대항목별로 0.2씩의 가중치를 배분한 후 나온 결과에 따라 주요기능별로 제시된 것이다.

〈표 6〉 전자문서 속성별 결과표

번호	대항목	소항목	속성값
1	보안기술	기밀성	0.05380
2		수신부인봉쇄	0.04878
3		무결성	0.04782
4		송신부인봉쇄	0.04136
5	보안정책	메세지 접근 보안등급	0.05236
6		메세지 분류 처리	0.04734
7		다중등급보안	0.04854
8		메세지 보안등급 제한	0.04830
9	전자문서 관리	전자서명	0.05786
10		암호화된 전자문서	0.04902
11		수신자키정보	0.04423
12		수신자확인서	0.03778
13	전자문서 전송	인증기관 및 인증서확인	0.05691
14		내용 위 · 변조확인	0.05595
15		송수신자확인	0.04902
16		송 · 수신시간확인	0.04089
17	암호화 알고리즘	RSA	0.07030
18		DES	0.06647
19		KCDSA	0.04160
20		SEED	0.04160

대항목의 보안기술 부분에서는 기밀성이 0.0538, 보안정책에서는 메시지접근보안등급이 0.0524, 전자문서관리에서는 전자서명에서 0.0579, 전자문서 전송에서는 인증기관 및 인증확인서가 0.0570의 값을 나타내어 각 대항목에서 가장 중시되는 요소들인 것으로 나타났다.

따라서 새로운 프로토콜에서는 기밀성과 송수신 인증 기능을 보완하고, 메시지 보안 등급을 구분하여 설계할 필요가 있다. 이와 같은 새로운 프로토콜 설계 요구사항을 설명하면 다음과 같다. **첫째**, 일괄처리로 인한 시간소모를 줄일 수 있도록 3개의 분리된 프로토콜로 구현한다. 즉, 기존 프로토콜은 문서의 보안등급에 관계없이 중앙시스템을 통하여 통합관리로 운영되는 메모리관리하에서 분산되는 형태로 구성되어 있기 때문에 국내 실정에 맞도록 시간과 시스템의 병목현상억제, 경제성을 고려할 필요가 있다. MSP에서는 다중접근자보안과 서명알고리즘, 메시지목록을 이용하여 접근자를 통제해야하기 때문에 송 · 수신에 관련하여 반드시 접근자 등록자료를 비교 처리해야하는 한다. 따라서 시간이 지연되고, 별도의 데이터베이스를 운영해야하는 문제점이 있다. 그러므로 문서등급을 선분류 한다면, 위와 같은 문제점을 제거할 수 있을 것이다. **둘째**, 중앙집중식 접근통제를 분산시킴으로써 보안등급 카드사용(Fortezza card)을 막고, 시스템 부하를 줄이기 위한 시스템을 구현할 필요가 있다. MSP에서는 접근자들을 합리적으로 관리하기 위해서 접근자의 정보를 별도로 관리 해야하며, 수시로 문서사용자가 권한등급에 맞도록 문서내용과 문서처리관련자에 대한 새로운 데이터를 문서발생처리건수 만큼 만들어야한다. 이때 잘못 처리되거나, 퇴직자 또는 문서취급등급변경자(징계자)등에 대한 정보를 공유해야하므로 대용량 및 초고속 시스템을 반드시 필요로 하는 문제점을 가지고 있다. 따라서 새로운 프로토콜에서는 사용자의 키정보만으로도 합리적인 문서전송을 할 수 있

도록 설계 할 필요가 있다. 셋째, 소용량의 서버로도 관리가 가능하도록 할 필요가 있다. 즉 현재 사용하고 있는 PC에서도 사용가능하며, 분산된 환경에서도 사용할 수 있도록 설계할 필요가 있다.

3. CMP 설계

3.1 기본 개념 및 구조

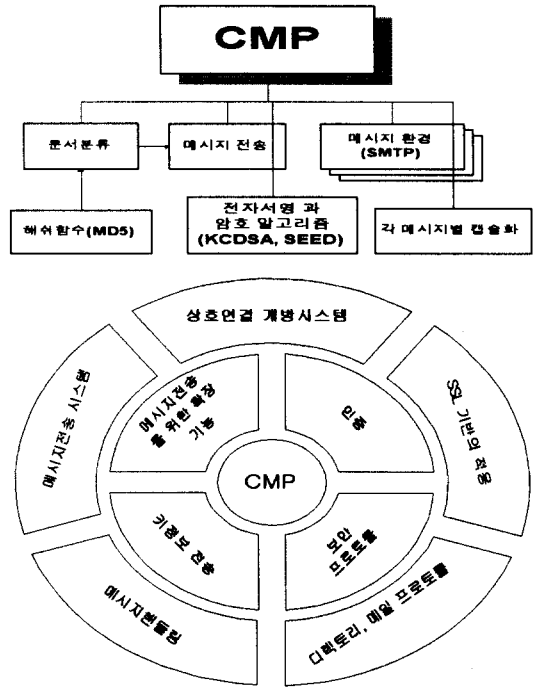
본 연구에서는 MSP의 문제점을 해결하고, 국내 전문가들의 요구사항을 반영한 프로토콜을 설계하였으며, 이를 CMP(Cryptography Message Protocol)로 명명하였다. CMP는 일괄처리로 인한 시간소모를 해결하고 이기종 간에 메시지 전달을 원활히 하며 접근카드 미사용, 클라이언트의 PC사용 가능성, 메시지의 전달 여부를 서버에서 알 수 있도록 하였다. 구체적으로 메시지를 헤더프로토콜에 탑재하여 메시지를 전송하는 단계를 중점적으로 연구하였으며 미 국방부 보안제품 기준안과 CCITT의 표준안에 따른 메시지 전송 요구사항, 송수신 프로토콜의 상세화, 인증의 개념을 추가하였다((그림 3) 참조).

그리고 SSL(Secure Socket Layer)의 기능을 추가 이용하였다. SSL은 전송계층과 응용계층 사이에 세션계층에서 데이터를 암호화하는 기능이다.

CMP는 문서등급별로 별도로 설계되었으며, 각각 CMP1, CMP2, CMP3로 명명되었다.

CMP는 일괄처리로 인한 시간낭비를 제거하기 위해 문서를 중요도 등급별로 구분하여 처리하도록 설계되어 있으며, 다중 관리를 위한 부수적 시스템 관리를 최소화하여 처리하는 합리적 기능을 설계에 반영하였다.

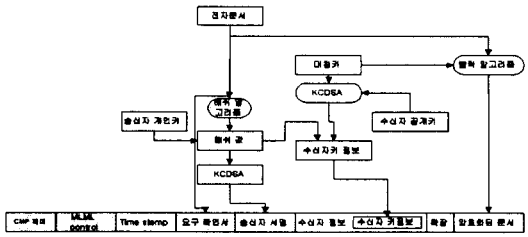
또한 메시지 접근의 통제 수단으로 사용되는 카드를 제거하기 위해 MLMLH(Multi Layer Multi Link Header)기능을 이용함으로써 클라이언트 시스템을 PC급 시스템으로 대체할 수 있게 되었다. MLMLH는 통합된 CMP프로토콜에 스위칭시스템(Switching System)을 부착하여 메시지가 기능별, 문서 내용별, 주요 사양별로 처리될 수 있도록 CMP1, 2, 3 각각에 대해 별도의 형태로 개발되었다.



(그림 3) CMP의 기본개념도

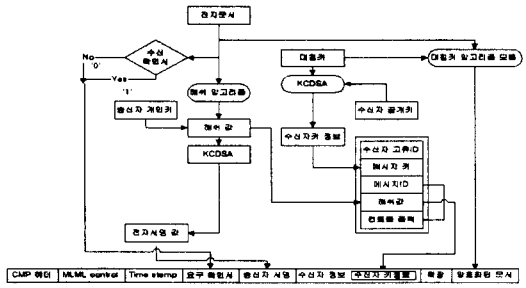
(그림 4)의 MLMLH3은 CMP3을 위해 설계되었으며, 문서의 복잡도와 시스템 트래픽에 따라 문서를 구분하고 보안 등급에 따라 처리하도록 하였다. MLMLH3은 CMP3헤더의 명칭으로 전자문서를 암호화하고 이를 수신자 키 정보에 수록하여 전송함으로써 안전성을 고려하는 프로토콜이다. 이러한 시스템은 암호화 방법이 간단하고 보다 신속한 업무처리 지원할 수 있는 장점이 있어 단순한 메시지, 서신, 공지사항 등

에 사용 할 수 있다. 여기서 KCDSA(Korean Certificate-based Digital Signature Algorithm)는 전자서명기능 만을 사용하여 문서가 위·변조되었는지 여부만 체크하기 때문에 신속한 처리를 할 수 있다.



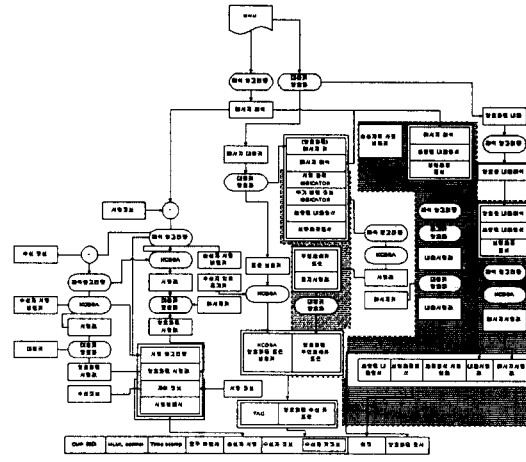
(그림 4) CMP3의 구조

(그림 5)의 CMP2는 MSP의 메시지 헤더 부분에 전체 정보가 아니라 송수신자 암호 데이터의 해쉬값만을 전송하도록 단순화시킨 전자문서관리헤더부분이다. CMP2는 암호화 및 복호화가 용이하고 대체로 안전하게 문서 처리를 할 수 있는 프로토콜로 비교적 단순하면서 보안성을 요구할 때 사용된다. CMP2는 대외비 또는 어느 정도의 비밀성을 유지해야하는 문서처리를 위해 설계된 프로토콜이다.



(그림 5) CMP2의 구조

(그림 6)의 CMP1은 MSP의 메시지 헤더 부분에 있는 송수신자 데이터를 암호화, 캡슐화하여 기록하는 확장부분을 일부 수정한 프로토콜이다. CMP1은 완벽한 1급 비밀 또는 국가기밀 정보를 취급, 전송할 때 사용할 수 있도록 설계된 프로토콜로 안전성 유지를 위한 복잡한 암호화 처리, 캡슐화를 위한 송수신자 정보의 탑재, 암호문서에 요구확인서 부분 추가 등을 고려하여 설계되었다. 이러한 MLMLH1은 암호관련 알고리즘을 이용한 전자서명의 검증과 CMP 헤더 생성을 위한 과정으로 인해 처리 시간이 지연되기는 하지만, 취급되는 문서가 중요한 경우에는 유용하게 사용될 수 있는 프로토콜이다.



(그림 6) CMP1 구조

3.2 MSP와 CMP의 구조상의 차이점

MSP는 대형시스템 내에서 구현된데 비해, CMP는 중·소형 시스템에서 운영될 수 있도록 설계되었다. <표 7>은 CMP와 MSP의 헤더 기능을 비교한 것으로 헤더 보유, 서명블럭, 수신자 암호데이타, 요구확인서, 메시지 보안등급 및 분류처리, 서명알고리즘, 메시지목록, 암호화된 전자문서, 확장기능, 키정보로 분류하여 비교하였다. 특히 CMP는 요구확인서기능과 메시지보안등급 및 분류처리기능, 키정보 기능이 특징적이며, MSP는 다중관리를 위한 서명에 관한 기능들이 특징적이다. 그리고 문서를 각 기

능에 맞도록 캡슐화하여 확장부분에 탑재하는 기능은 공통적이다.

〈표 7〉 항목별 헤더기능 비교표

헤더기능	CMP	MSP	비 고
헤더보유	o	o	
서명블럭		o	다중접근자 관리
수신자암호데이타	o	o	
요구확인서	o		
메시지 보안등급 및 분류처리	o		
서명알고리즘		o	다중접근자의 위·변조방지
메시지 목록		o	다중관리시 공유파일로 사용
암호화된 전자문서	o	o	
확장	o	o	
키정보	o		

MSP 헤더의 서명블럭, 서명알고리즘, 메시지 목록은 문서 내용과 문서 이용자의 정보를 비교하여 접근의 범위를 미리 조절하는 기능으로 이를 처리하기 위해 초대형 시스템과 접근자 관리 시스템이 필요하다. 반면 CMP의 요구확인서, MLMLH, 키정보는 현재 보유하고 있는 시스템에서 다중 처리 기능을 지원할 수 있도록 설계되었다.

MSP와 CMP의 기능을 종합적으로 비교한 결과는 아래 <표 8>과 같다. 먼저 헤더 사용시 여러 기능을 탑재하여 속도, 알고리즘관계, 해쉬값의 비교, 메시지헤더, 문서전송, 위변조확인, 송·수신자파일, 인증서비스, 키관리, 보안기능 전송기반으로 구분하여 비교하였다. 보안기능전송기반은 MSP는 응용계층에서 데이터가 전송되어지며, 전송에 관련된 암호화 및 보안문제처리를 대형서버에서 관리하도록 설계되어 있으며, CMP는 소형서버에서도 사용이 가능하도록 SSL을 이용한다. 시스템 사용시간, 데이터로드 및 처리 시간을 개념적으로 비교한 결과 전송처리시간에 있어서는 CMP1, 2, 3 각각이 MSP에 비하여 빠르거나(CMP3), 늦을 것(CMP1)으로 예상된다.

〈표 8〉 MSP와 CMP 비교표

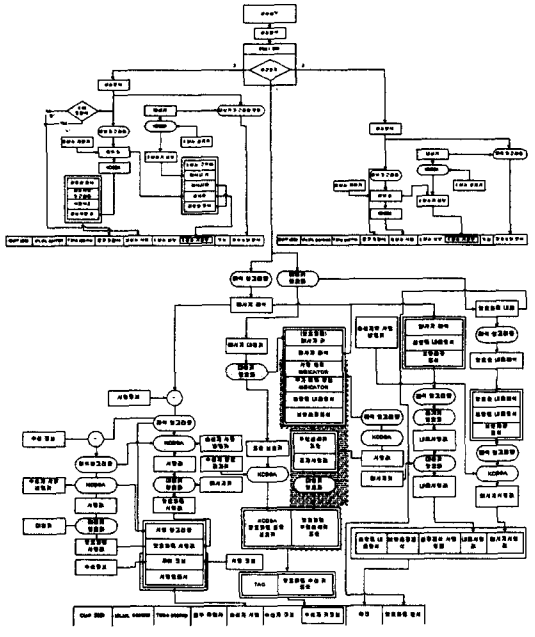
구 분	MSP	CMP1	CMP2	CMP3	비 고
전송처리시간	MSP	--	-.-	-	
공개키암호화 알고리즘	RSA	KCDSA	KCDSA	KCDSA	군수품 수출규제로 국내 표준 사용
비밀키암호화 알고리즘	DES	SEED	SEED	없음	규제
해쉬값	MD5	MD5	MD5	MD5	
메시지 헤더	전체정보	전체정보	송수신정보	키정보	class 이용
문서전송	전체전송	전체전송	전체전송	내용위주전송	
위변조확인	확인	송신자 확인서	송신자 확인서	송신자 확인서	
송·수신 파일		분류	-	-	통합관리가능
인증서비스	접근자의 정보에 따라 인증제공	송·수신자 정보로 인증 관리	송·수신자 정보로 인증 관리	송신자 서명에 의해 인증	
키관리	접근시 카드사용	비밀키	비밀키	비밀키	
보안기능 전송기반	OSI에서의 응용층 이용	SSL이용	SSL이용	SSL이용	

MSP는 접근자 관리 시스템에서 키 관리에 따른 접근자의 개별정보를 요구하고 있으나 CMP는 비밀키를 업무 처리자에게 별도 부여함으로써 간단히 처리할 수 있다. 또한 MSP의 보안 전송 기능은 OSI 참조 모델의 응용계층에서 처리되도록 설계되었다. CMP는 SSL을 이용함으로써 보다 안전한 전송이 이루어질 수 있도록 설계되었으며 메시지가 CMP에 등록되면 문서 등급에 따라 선택되어질 프로토콜 메시지 앞에 헤더값이 붙도록 하였다.

(그림 7)은 CMP 프로토콜의 처리 과정과 구조를 도시한 것으로 CMP1, 2, 3를 결합하여 종

합한 구조이다. CMP는 각각의 헤더를 따로 분리하여 처리함으로써 메시지를 전송하기 위하여 기다리는 불편이나, 등급별에 의한 분류를 분명히 할 수 있는 프로토콜이다.

그러므로 본 프로토콜은 각각의 다른 내용의 헤더를 전달하므로서 전송시간과 메시지헤더 제작시 시간관리에 측면에서 우수할 것으로 예측된다.



(그림 7) CMP 프로토콜

4. 구현 및 성능분석

4.1 실험방법 및 과정

본 연구에서는 성능 및 보안성기준으로 CMP와 MSP를 비교분석하였다. 실험순서는 MSP와 CMP1, CMP2, CMP3를 순으로 하고, 자료별, 용량별, 그리고 횟수별로 실험 후 얻어지는 자료에 대한 비교분석을 실시하였다.

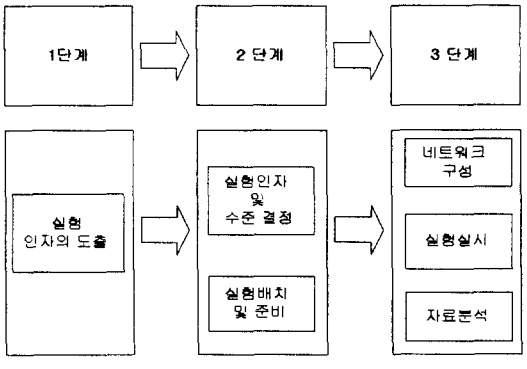
CMP와 MSP구현시 Visual C++를 이용하였고, Win98과 NT에서 운영될 수 있도록 개발되었다.

숫자나 영문자, 한글, 그림파일, 동영상, 음악파일, 압축파일로 구성된 문서들을 선택하여 문서의 크기(3바이트-900킬로바이트)와 횟수(100회, 1,000회)를 다양하게 변경시키며 실험하였다.

실험시 문서 크기별로 실험횟수를 교차하여 속도를 측정하였으며, 실험에 사용된 시스템 환경은 펜티엄 PC와 NT 및 네트워크환경이다. 1,000번 이상의 실험을 실시하면 메모리 부족 현상과 버퍼오류등의 현상이 발생하기 때문에, 오류 및 오차를 고려하여 전체 횟수를 결정하였다.

실험순서는 IP가 다른 시스템을 서울과 대전에 총 3대를 설치하고 시스템의 IP를 이용하여 서로다른 시스템간의 문서전달이 이루어지도록 하였다.

후속작업으로 실험결과를 분석하고, 분석 결과의 해석, 확인실험을 하였다. 전체적인 실험 실시 흐름은 아래 (그림 8)과 같다.



(그림 8) 실험 실시 흐름도

실험 결과의 타당성을 높이기 위해 다중 보안등급의 송신자와 수신자의 정보를 모두 보유하도록 하여 전송 자료와 속도 차이를 줄인 후 각 기능을 검증하였다. **실험인자 및 수준의 결정**은 자료의 이동이 얼마나 적은 루틴(단계)으로

전개되는가에 따라 결정되어진다. 실험에 필요한 하드웨어적인 시뮬레이션 자료를 준비하였으며, **실험을 실시**(100, 1000 횟수실시)하고 **자료**(헤더제작과정과 네트워크 형성 전달시간)를 분석하였다.

4.2 성능분석결과

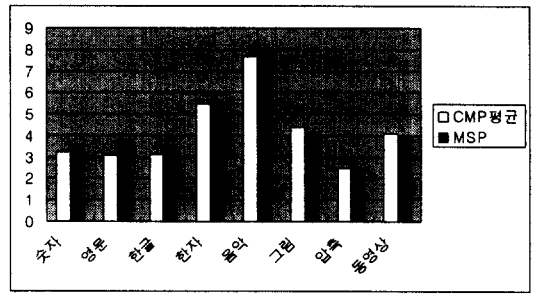
전반적인 성능분석에서는 CMP가 MSP보다 실험횟수가 많아질수록 좋은 성능을 보이는 것으로 나타났으며, 데이터의 크기에 따른 처리속도의 차이는 유의하게 나타나지 않았다. CMP가 MSP보다 처리속도가 빨라지는 것으로 나타났으며, 속도 측면에서는 CMP1, CMP2가 MSP와 유사한 속도를 보이며, CMP3는 MSP보다 약 1.5-2배 정도 처리속도가 빠른 것으로 나타나고 있다. 100회 실험 결과는 <표 9>와 같다. CMP가 MSP에 비하여 총평균이 0.16ms 빠른 결과를 보이고 있으나, 동영상과 음악에서는 CMP가 MSP보다 암호화처리에 많은 시간을 소모하는 것으로 나타났다. 이는 CMP1에서 송신자의 서명과 수신자의 정보를 만들기 위해서 전자서명과 암호키가 다양하게 사용됨으로써 시간지연이 발생하기 때문이다. 한편 CMP3에서는 키정보만을 사용하기 때문에 속도가 1.02ms로 MSP의 4.36ms보다 3.34ms 더 빠르게 전송할 수 있는 것으로 나타났다.

다음 <표 10>에서 보듯이, 실험횟수가 1,000회 늘어나면서 MSP의 처리 속도보다 CMP의 처리속도가 빠르게 나타나고 있음을 알 수 있다.

CMP평균과 MSP의 차이는 숫자 31.405ms, 영문자 4.485ms, 한글 1.585ms, 한자 1.248ms, 음악 -2.000ms, 그림 0.780ms, 압축 0.170ms 동영상 -2.750ms로 CMP가 빠르게 나타났다. 즉, CMP가 MSP에 비하여 우수한 성능을 보이고 있으나, 동영상과 음악에서는 CMP가 MSP보다

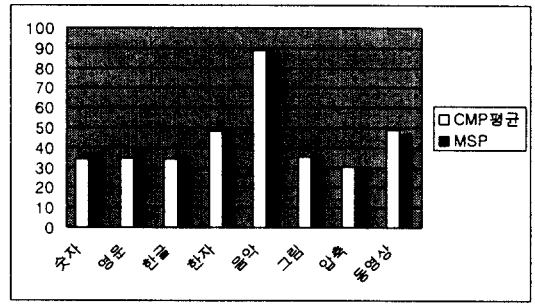
〈표 9〉 실험횟수 100회 실시평균차(단위 : ms)

구 분	CMP평균	MSP	차이
숫 자	3.229	3.45	0.221
영 문	3.075	3.773	0.698
한 글	3.129	3.474	0.345
한 자	5.445	5.6	0.155
음 악	7.670	8.000	0.330
그 림	4.420	4.09	-0.330
압 축	2.500	2.500	0.000
동영상	4.090	4.000	-0.090
합 계	33.558	34.887	1.329
평 균	4.19	4.36	0.16



〈표 10〉 실험횟수 1000회 실시평균차(단위 : ms)

구 분	CMP평균	MSP	차이
숫 자	34.106	36.850	31.405
영 문	34.807	38.591	4.485
한 글	34.065	35.650	1.585
한 자	48.085	49.333	1.248
음 악	89.000	87.000	-2.000
그 림	35.220	36.000	0.780
압 축	30.090	30.250	0.170
동영상	48.750	46.000	-2.750
합 계	354.123	359.674	34.923
평 균	44.26	44.95	4.36



암호화처리에서 많은 시간을 소모하는 것으로 나타났다. 이는 CMP1에서 송신자의 서명과 수신자의 정보를 만들기 위해서 전자서명과 암호키가 다양하게 사용되므로서 시간지연이 발생하며, CMP2에서도 정보의 전달을 명확하게 하기 위하여 송신자확인 기능을 추가하여 사용하기 때문이다. CMP3에서는 키정보만을 사용하기 때문에 1000회 평균값이 11.74ms로 MSP의 44.95ms보다 33.21ms 빠르게 나타나고 있다.

처리과정 분석 결과를 살펴보면 다음과 같다. 먼저 CPU 처리 속도는 MSP가 0.2433ms, CMP가 0.2346ms로 CMP가 MSP에 비하여 0.0087ms 빠른 것으로 나타났다.

보안처리 작업 시간도 CMP가 MSP에 비하여 5.34ms 빠르며, 네트워크도 0.96ms 빠르게 나타나 성능 면에서 CMP가 MSP보다 우수한 결과를 보이고 있다. 실험과정에서 서울과 대전의 거리에 의한 성능 차이는 없었으나, 네트워크환경이 사용자가 많을 때는 네트워크 속도가 현저하게 낮아지며, 문서의 전송횟수 및 문서의 량이 많은 경우 사용 횟수에 따른 차이는 있는 것으로 나타났다.

〈표 11〉 결과 비교표

구 분	MSP	CMP	차이	비 고
CPU처리속도	0.2433ms	0.2346ms	-0.0087ms	
보안화작업시간	45.22ms	39.88ms	-5.34ms	각 보안키 사용
네트워크	73.66ms	74.62ms	-0.96ms	

4.3 보안성분석

이 절에서는 CMP의 보안성을 MSP와 비교하기 위해 보안성 분석기준으로 FIPS PUB 140-2(Federal Information Processing Standard PUBlication) [SDN701 1994, Simmizu & Miyaguchi 1987, www.imc.org 1994]에 있는 기준을 사용하였다. 결과 분석을 위해 사용된 보안성 항목별 등급 기준표는 아래 <표 12>와 같다.

〈표 12〉 보안성 항목별 등급 기준표

구 분	Security Level 1	Security Level 2	Security Level 3	Security Level 4
암호모듈 명세서	모든 하드웨어, 소프트웨어, 펌웨어 컴비네이션이 포함된 암호모듈. 모듈보안정책			
암호모듈 인터페이스	모든 인터페이스와 입출력물 경로 명세서		보안척도에 대한 데이터포트를 다른 데이터포트와 분리	
역할, 서비스와 인증	논리적 분류	역할 기반	신원기반의 운영자 인증	
제한된 상태의 기계모델	한정된 상태의 기계모델 명세서, 운영 상태, 상태변화 다이어그램			
물리적 보안	기본 보안장치	무허가 접근에 대한 증거	접근에 대한 응답	봉쇄응답.
암호키 관리	입증된 키 생성/키 분배기술		작업 진행 시 각각의 키를 사용(유지관리)	
전자기 간섭 및 적합성(EMI/EMC)	미연방통신위원회(FCC) Part 15. Subpart B, ClassA(Business use). 적절한 FCC 요구사항 (for voice)		미연방통신위원회(FCC) Part 15. Subpart B, Class B (Home use)	
운영시스템 보안	단일운영자	CAPP가 EAL2를 평가	신뢰성 경로 평가	보안정책 모델과 감춰진 채널분석
자기시험(Self-Tests)	암호알고리즘 테스트		통계적 테스트- 요구	
설계 보증	구성관리, 보안설비	보안분산, 기능적 명세서.	고급언어 구현	공식 모델
다른 공격의 완화	위 사항에서 들어가 있지 않은 공격 완화에 대한 명세서			

위 표에서 보는 바와 같이 보안성 기준은 암호모듈명세서, 암호모듈인터페이스, 역할·서비스와 인증, 제한된 상태의 기계모델, 물리적 보안, 암호키관리, 전자기 간섭 및 적합성(EMI/EMC : Electromagnetic Interference / Electromagnetic Compatibility), 운영시스템보안, 자기시험(Self-

Tests), 설계보증, 다른 공격으로부터의 완화 등 11개이다. 각 기준에 대한 CMP와 MSP의 보안성 비교 분석결과는 <표 13>과 같다.

〈표 13〉 보안성 분석비교표

보안성요구사항	MSP	CMP	비교
암호모듈 명세서	◎	◎	공인된 알고리즘의 사용
암호모듈 인터페이스	○	◎	CMP의 전송포트 등급별분리
역할, 서비스와 인증	◎	◎	인증기반 및 운영자의 신원확인
제한된 상태의 기계모델	—	○	보안요구 및 암호화 요구조건을 만족하는 시스템
물리적 보안	◎	○	MSP의 통합관리로 인한 결과임.
암호키 관리	△	○	MSP는 문서접근시 카드를 이용하여 문서열람이 가능함. 분실시 치명적인 정보의 유출이 예상됨.
운영시스템 보안	◎	◎	신뢰성을 기본으로 한 시스템 구축
전자기 간섭 및 적합성	—	—	사용시스템의 조건에 따라 달라질 수 있음
설계 보증	○	○	공식모델 및 공개정도
다른 공격의 완화	◎	◎	예상 밖의 공격 대비
자기시험 (Self-Tests)	◎	◎	MSP는 시험 및 성능에 의한 결과 산출

◎ : 아주좋음 ○ : 좋음 △ : 보통 — : 비교불가능

암호모듈 명세서의 경우, MSP와 CMP가 모두 공인된 암호모듈을 사용하고 있어 기준에 부합하고 있다. **암호모듈 인터페이스의 경우,** MSP는 다중접근자에 의한 다중처리로 서버에서 접근자의 인적사항과 비교한 후에 문서전송을 하고 있는 반면에 CMP는 수신자가 직접 접속 하도록 설계되어 있어 CMP 접속이 유리하다고 볼 수 있다. **역할·서비스와 인증의 경우** CMP 및 MSP 프로토콜은 모두 메시지전송이라는 역할이 구분되어 있고, 보안성 서비스를 위해서 여러 개의 알고리즘을 사용하였으며, 인증을 위한 해쉬함수을 사용하였다. **제한된 상태의 기계모델의 경우,** MSP을 사용하기 위한 시스템의 요구사항이나 주변 클라이언트 시스템 사양에 대해서는 미국측의 보안사항으로서 파악하기가 불가능하였으나 CMP는 기존의 PC와 NT서버 수준에서 모두 운영가능하며, 호환성을 고려하여 개발하였다. **물리적인 보안의 경우,** MSP는 접근자에 대한 접속횟수 및 종합데이터를 산출하여, 전체종합관리에 영향을 미칠 수 있도록 자료화하기 때문에 메시지를 생성하여 암호화를 거친후 메시지를 캡슐화하여 전송하는 MSP는 접근자를 통합하여 관리한다. 그러나, CMP는 접근자들의 업무에 관련하여 키를 부여하고 문서만을 관리하기 때문에 물리적 기능에서는 MSP가 유리하다. **암호키 관리의 경우,** 요구사항은 암호키의 적절한 보호관리를 전제로 하기 때문에 키생성, 키분배, 유지관리 세단계로 구분하여 볼 수 있다. MSP는 접근자 송·수신카드를 이용하는 반면에 CMP는 공개키를 사용하므로서 키생성 및 키분배에 있어 유리하다고 할 수 있다. **운영시스템보안의 경우,** MSP는 전산망의 기술환경과 새로운 데이터전송방식, 전송매체, 망 서비스의 변화에 대해 적합성을 보이고 있고, CMP도 MSP의 기본운영기술을 공유하였기 때문에 두 프로토콜 모두 적합하다고 할 수 있다. **전자기 간섭 및 적합성의 경우,** 두 프로토콜 모두 범용성을 지니고 있으나 본 연구의 범위를 벗어나기 때문에 분석을 하지 않았다. **자기시험의 경우** MSP와 CMP는 비인가자 및 불법접근의 제어 가능한 무결성 보장과 인가된 자에 의해서만 자료를 변경할 수 있는 기밀성 유지, 장소 및 시간에 관계없이 사용 가능한 상태의 가용성이 확보되어 있어 모두 적합하다고 할 수 있다. **설계보증의 경우,** MSP나 CMP 모두 암호문전송에 해당하는 기본기능을 사용하여 동일한 조건에 있다고 할 수 있다. **다른 공격 완화의 경우,** 메시지전

송시스템의 기본취지로서, 항상 예상할 수 없는 외부의 침입으로부터 메시지를 보호해야 하기 때문에 이 부분은 각 프로토콜 모두 요구 사항에 맞도록 구현되었다.

종합하면 CMP는 암호모듈인터페이스, 역할·서비스와 인증, 운영시스템보안, Self-Tests, 다른 공격의 완화 등의 측면에서 MSP보다 유리하거나 동등하다고 할 수 있다.

4.4 토의 및 분석

본 연구는 메시지전송시스템에 중에서 새로운 전송프로토콜을 구현하여 성능실험과 보안성검토를 하였다. 먼저 구조적인 측면과 기능적 측면들이 전송프로토콜에 미치는 영향을 살펴보면 다음과 같다.

구조적 측면에서 볼 때 MSP의 시스템구조는 통합화 단일 시스템으로 미 국방부 차원에서 각 주 주둔부대와 연계되어 상용 컴퓨팅 및 네트워킹 기술과 호환 되도록 운영할 수 있는 초대형 시스템이다. 그리고 구현되어 사용중인 소프트웨어구조는 시스템구조에 맞도록 통합화하여 데이터의 검증, 인증, 암호화, 디지털서명 같은 보안서비스가 제공되도록 설계하였다. 이에 대해 CMP는 주로 규모에 관계없이 서버와 클라이언트환경에서 메시지를 전송할 수 있도록 설계하였으며, 상용컴퓨터와 각종 네트워킹에서도 호환성을 지닐 수 있도록 설계되었다. 또한 송·수신자의 정보와 암호키를 이용하여 메시지를 전달 할 수 있도록 하였다.

이로 인한 효과를 살펴보면 보안유지를 위한 MSP시스템의 효과는 우수하지만 이로 인한 경비와 투입되는 장비는 상당한 예산비용을 초래할 것으로 분석된다. 또한 포테자(Fortezza : 암호화카드, 다중접근카드)를 이용하여 신분확인, 데이터의 무결성, 비밀성 및 부인봉쇄를 제공하고 있지만 이를 분실할 경우 매우 위험한 전송처리문제가 발생할 수 있다. 이에 대해 CMP는 슈퍼컴퓨터, 대형컴퓨터나 주변기기가 별로 필요치 않으므로 경제성과 호환성을 지니고 있으며, 접근관리 및 문서접수시 사용할 암호알고리즘은 비밀키를 사용하기 때문에 분실로 인한 문제를 해결할 수 있다. 요약하면 MSP는 대형화 및 보안장비요구, 전반적인 통합관리와 다수의 단일등급보안을 제공하는 구조이며, CMP는 소형이면서 대형으로 호환이 가능하고 거의 보안장비가 필요치 않은 시스템이며, 경제성이 있는 차이점을 가지고 있다.

메시지전송시스템에서 기능적인 측면은 전자서명과 암호알고리즘, 해쉬함수를 사용하였다. MSP는 RSA, DES, MD5를 사용하고 있으며, CMP는 KCDSA, SEED, MD5를 사용한다. 이중에서 RSA는 소인수분해를 전자서명에 이용하고 있기 때문에 승산횟수가 많은 것과 전처리가 불가능한 것이 단점이다. KCDSA(Korean Certificate-based Digital Signature Algorithm)은 국내에서 표준안으로 제정되어 사용되고 있으며, 장점으로는 서명의 크기가 작고 전처리가 가능하며, 단점으로는 난수의 기밀성이 필요하다. 요약하면 RSA는 안전성이 높지만 계산이 복잡하여 속도가 느리고, 전처리가 불가능한데 비해, KCDSA는 계산이 RSA에 비교하여 빠르고 전처리가 가능하다. 그러나 국내에서만 사용되고 국가차원에서의 표준으로 제정되어 있기 때문에 앞으로 보다 많은 사용을 통하여 안전성을 확보하는 것이 필요하다. 문서 송·수신시 처리되는 과정에서 사용되는 암호알고리즘의 경우 MSP에서는 비밀키 또는 대칭키라고 하는 DES를 이용하였다.

전송기반의 기능에 있어서 MSP는 자체내에 있는 보안 장비 및 방화벽을 이용하여 메시지를 전송하고 있다. 그러므로 MSP에 대한 보안취

약점을 분석하기는 쉽지 않다. CMP에서는 SSL기반을 이용하였으나, SSL역시 미국내 암호화 소프트웨어 수출 금지법에 규제되어 있다. 그러나 호주에서 SSL(미국의 SSL과 다소 차이가 있으나 기본 기능은 동일함) 소스를 공개하므로서 SSL의 사용이 빈번해 지고 있다. SSL은 다양한 암호 알고리즘을 지원하며, 대칭키 및 비 대칭키에도 지원이 가능하 기 때문에 CMP는 보안 목적으로 안전하게 사용 할 수 있으며, 외부로부터 의도된 침해에도 안전성을 지닌 메시지 전송 시스템이라 할 수 있다.

5. 요약 및 결론

본 연구에서는 MSP의 설계도에 따라 주요 모듈들을 개발하고, MSP의 문제점을 보완한 CMP프로토콜을 구현한 후 성능 및 보안성 측면에서 비교 분석하였다. 성능 분석은 숫자, 영문자, 한글, 음악, 그림, 압축, 동영상 데이터파일을 준비하고, 실험 횟수를 증가시켜 가면서 처리시간을 비교하였다. 보안성분석은 FIPS PUB 140-2에 있는 보안성 구분기준에 의해서 수행되었다.

처리시간 분석결과 CMP는 숫자, 영문자, 한글, 한자, 음악, 압축파일 등의 데이터에서 MSP보다 좋은 결과를 나타내었다. 그림이나 동영상 파일에서 속도가 늦는 것으로 나타나고 있으나, 메시지의 내용이 문자 위주임을 감안할 때 대체로 CMP가 MSP보다 우수한 성능을 가지고 있다고 볼 수 있다.

보안성 분석의 경우, 정보의 신뢰성과 안정성을 기반으로 하는 전산망의 사용과 보안 사고의 신속한 대응책여부 등에 대하여 종합적으로 분석한 결과, CMP와 MSP간의 뚜렷한 차이는 없었다. CMP는 보안척도를 구분하여 처리할 수 있도록 암호모듈 인터페이스 기준에서의 합리성과 적합성을 가지고 있으며, 역할·서비스와 인증, 운영시스템보안, Self-Tests, 다른 공격의 완화 등의 측면에서 MSP와 동등하다. 특히 암호키 관리 부분에서는 CMP가 공개키를 사용하므로서 사용상의 편리성과 보안성을 가지고 있다고 할 수 있다. CMP1의 경우 복잡한 암호화 및 토큰설정을 사용하고, 해쉬함수로 전자서명을 유도하고, 이를 다시 종합하여 암호화된 메시지 및 헤더와 결합함으로서 다른 프로토콜에 비해서 시간이 필요하다. CMP2에서는 토큰을 제외시켰으며, CMP3에서는 수신자 블럭정보를 제외하였기 때문에 처리속도가 증가하게 된다.

본 연구에서는 암호관련 기술에 대한 규제로 다양한 암호알고리즘을 적용하지 못하고, 공개된 암호알고리즘을 사용하여 제한적인 분석을 수행할 수 밖에 없었다.

향후에 보다 완벽한 MSP를 구현하고, 다양한 암호알고리즘을 비교분석하며, CMP를 개선하는 연구가 필요할 것이다.

참 고 문 헌

[1] 한국정보보호센터, 암호기술입문(전자서명-KCDSA), 한국정보보호센터, 1999, pp.105-136.

[2] Bennett, G. 저, 이영화 편역, *인터네트워크 @TCP/IP (원제 : Designing TCP/IP Internetworks)*, 범한서적(주), 1999.4, p.691

[3] Abram, M., and Podell, H. *Computer and Network Security.* Los Alamitos, CA : IEEE Computer Society Press, 1987.

[4] National Bureau of Standards(FIPS 49), "Data Encryption Standard," U.S. FIPS PUB 49, 1977, pp.1-18.

[5] National Institute of Standards and Tech-

nology(FIPS PUB 140-2), "Security Requirements for Cryptographic Modules," U.S. FIPS PUB 140-2, 1999, pp.1-19.
[6] National Institute of Standards and Technology(SDN701), "SDNS Message Security Protocol," SDN701, Rev 3.0, 1994, pp. 5-11.
[7] Simmizu, A. and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL," *Eurocrypt'87*, 1987, pp.267-278.
[8] http://csrc.nist.gov/cryptval/140-1/1401val1997.htm
[9] http//csrc.nist.gov/cryptval/140-1/1401val1998.htm
[10] http://csrc.nist.gov/cryptval/140-1/1401val1999.htm
[11] http://csrc.nist.gov/cryptval/140-1/1401val2000.htm
[12] http://www.armadillo.huntsville.al.us/index.html
[13] http://www.imc.org/workshop/sdn701.txt 94.3.21.
[14] http://www.imc.org/workshop/sdn801.txt 97.2.6
[15] http://www.kisa.or.kr/pds/att/missi.hwp
[16] http://www.kisa.or.kr/sysevaluation

■ 저자소개

신 승 중

한성대학교 경영학과를 졸업하고, 세종대 경영학석사, 건국대 전자계산학과 공학석사, 그리고 국민대 정보관리학과에서 박사과정을 수료하였으며, 기업관리 소프트웨어 개발회사를 운영하였다. 현재 중부대학교 정보공학부 컴퓨터안전관리학 전공 교수 재직하고 있으며 주요관심분야는 메시지전송, 정보보호관리, 보안감리분야이다.

김 현 수

서울대학교 원자핵공학과를 졸업하고, 한국과학기술원에서 경영과학석사, 그리고, University of Florida에서 경영정보학 박사학위를 취득하였으며, (주)데이콤, 한국정보문화센터 등에서 정보시스템과 전략업무를 담당하였다. 현재 국민대학교 경상대학 정보관리학부 부교수로 재직하고 있으며, 주요관심분야는 정보시스템 진단과 감리, 데이터마이닝, 프로젝트관리 등이다.