제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

안전한 메시지 전송을 위한 CMP 프로토콜에 관한 연구

최호진*, 양환석*, 정재영**
*조선대학교 전산통계학과
*서강정보대학 멀티미디어학부
e-mail:hjchoi@naju.ac.kr

A Study on CMP Protocol for Secure Message Transfer

Ho-Jin Choi*, Yang-Hwan Seok*, Jea-Young Jeong**
*Dept of Computer Science and Statistics, Graduate School, Chosun University
**Dept of Multimedia Information, Seokang College

요 약

메시지 전송 분야에 있어 보안 및 인증문제를 해결하기 위한 메시지 전송 프로토콜과 관련하여 국내의 정보통신시스템 및 정보처리 환경에 적합한 보안기술을 채택하여 CMP를 설계했으며 또한 제안한 CMP 프로토콜의 검증을 위해 메시지 보안 프로토콜인 MSP와 성능실험 및 보안성 분석을 통해 그 기능을 비교 평가하였다. CMP 프로토콜과 기존 MSP 프로토콜간의 성능비교를 위해 자료 유형별, 전송횟수별, 파일종류별로 실제 전송결과 얻어지는 수치를 중심으로 평균값을 비교한 결과 전반적인 성능분석에서 CMP의 평균속도가 MSP보다 전송속도가 빠르게 나타남을 알 수 있었다.

1. 서론

현대 사회는 정보화 시대로 컴퓨터기술과 통신기술의 발달로 컴퓨터를 이용한 정보통신 분야가 급속히 발전하고 있다. 인터넷 및 E-mail 사용이 급증하며 이들을 사용한 정보의 양도 폭발적으로 증가하고 있다. 이와 함께 정보시스템에 대한 보안 사고도 점차 증가하고 있어 사회적으로 많은 문제가 야기되어 공공기간, 기업 등 정보시스템을 운영하는 조직들은 보안점검도구, 방화벽 등 각종 보안 솔루션을 도입하여 정보시스템 보안을 강화하는데 노력을 기울이고 있다[1][2].

향후 세계의 모든 인류는 시간과 공간의 제약 없이 다양한 정보통신 서비스를 받을 수 있게 될 것이며, 고도의 정보화 사회로의 전환에 따라 삶의 질이 향상되는 혜택을 받게 될 것이다. 그러나 이러한 정보화 사회의 실현을 위해서는 정보의 효율적 공유를 위한 통신기반의 확충이 전제되어야 하며, 이와 함께 인터넷 활용의 역기능 즉 사생활 보호, 정보 해킹 등은 효과적으로 사전에 예방되어야 한다[3][4].

현재 인터넷 등 네트워크 상에서 발생되는 여러 가지 보안 문제들을 해결하기 위해 국내외적으로 많은 연구가 진행 중에 있다. 그러나 이 중에서도 메시지 전송에 있어, 보안 및 인증문제를 해결하기 위한 메시지 전송 프로토콜에 관한 연구는 매우 미진한 실정이며, 특히 국가적인 기밀사항으로 관리하고 있어 대부분 비공개를 원칙으로 하고 있다.

따라서 메시지 전송 프로토콜을 도입하려면 외국의 기본 설계를 근간으로 하여 국내 정보시스템 특성에 맞게 상당기간 수정 및 보안작업을 실시해야 한다. 이와 같은 메시지 전송 시스템 도입의 제도적, 현실적인 난관을 극복하기 위해서는 국내의 정보통신시스템 및 정보처리 환경에 적합한 보안기술을 채택하여 자체적인 메시지 전송 프로토콜을 개발할 필요가 있다. 본 논문은 이와 같은 개발의 필요성 인식 하에서 국내 실정에 맞는 메시지 전송 프로토콜 중에서 메시지 보안 프로토콜의 개발 및 구현을 목

표로 하고 있다.

2. 메시지 보안 프로토콜(MSP)

메시지 전송 개념은 전자화된 문서를 보안 서비스를 포함하여 전달하는 것이며, 메시지 전송시스템은 분산 컴퓨팅 환경에서 보안 서비스를 부가하여 전자우편과 안전한 메시지 처리를 위한 정보통신 시스템 응용기술이다.

메시지 전송 프로토콜은 CCITT의 X.400을 기반으로 기밀성, 무결성, 송·수신자 정보 전달, 송신자 부인봉쇄 등의 다양한 기능을 구사함으로써 자료의 위·변조를 막고 인증된 상태에서의 메시지를 전송할 수 있어 군사적 목적에 사용할 수 있게 되었다[5][6].

메시지 보안 프로토콜(MSP)은 미보안국(NSA : National Security Agency)이 주도하여 여러 종류의 MISSI 보안 해결책으로 구성, 통합, 시험 및 보안 프로파일 형태로 되어있다. 이러한 보안 해결책은 대부분의 사용자들의 공통적인 시스템 보안 요구조건을 나타내는 다양한 단일 등급 또는 다중 등급의 보안구조를 가지고 있다.

1986년에 MSP 1.0이 발표되고 1992년에 안전하게 전송 메시지를 전달할 수 있도록 응용한 것이 MSP 2.0이다. 그러나 다중사용자나 개방형 시스템 및 분산시스템 환경에서 메시지를 전달하고 위·변조, 인증문제의 기능을 첨가하여 발전시킨 것이 MSP 3.0이다. 그리고 E-mail에 적용하고 위·변조기술, 인증, 다중사용자 관리기능을 부가하여 MSP 4.0 및 4.0.1을 개발하였으며 1998년 공중서비스로 전환하기 위하여 CSP(Common Security Protocol)로 명칭을 변경하여 1999년 3월에 소개하였다.

이러한 메시지 보안 프로토콜의 기본구조는 그림 1과 같으며 상호연결 개방시스템은 이기종 시스템이나 서로 다른 운영체제 하에서도 안전하게 메시지를 전달하는 기능을 구현하기 위한 구조이다[7][8].

MSP는 기존의 x.400 메시지 전송시스템에 투명성을 제공하고 MSP 보호 서비스를 위한 MSP 사용관리자(UA)와 기능 개체들로 구성되어 있다. MSP는 자체망을 이용한 시스템에서 주로 운용되며 등급 보안을 다중화하기 위하여 비밀등급카드를 이용하여 접근자를 통제하고 있고 수신자의 인증서, 사용자 주요 자료, 보조벡터를 얻기 위해 x.501과 x.509 디렉토리 시스템을 이용한다

MSP의 문제점은 기능적 측면, 문서 처리 측면, 군수품 규제 측면으로 나누어 분석할 수 있다. 먼저 기능적인 측면에서는 통합된 전산망 사용으로 유지보수 비용이 발생되며 초대형 시스템의 다중접근 방식으로 이한 주변 시스템의 필요성이 증대된다. 또한 일괄처리로 인한 지연 및 중요도에 관계없는 처리과정의 문제가 발생하고 있다.

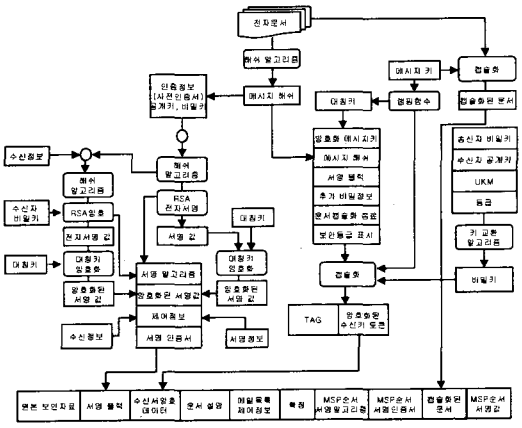

그림1. MSP 프로토콜

문서 처리 측면에서는 단일화된 통신채널 이용으로 병목현상이 우려된다. 군수품 규제 측면에서는 현 컴퓨터 환경에서 보안성이 낮은 비트만을 사용하도록 규제하고 있는 문제가 있다.

3. CMP 프로토콜의 설계 및 성능분석

3.1 CMP 프로토콜 설계

본 연구에서는 메시지 보안 프로토콜(MSP)의 문제점을 해결하고 국내 상황에 적합한 프로토콜인 새로운 CMP(Cryptography Message Protocol)를 설계 및 구현하였다.

CMP는 일괄처리로 인한 시간소모를 해결하고 이기종 간에 메시지 전달에 있어서 효율성을 높였으며, 접근카드 미사용, 클라이언트 PC 사용의 가능성, 메시지의 전달 여부를 서버에서 확인할 수 있도록 하였다. 구체적으로 메시지를 헤더 프로토콜에 탑재하여 메시지를 전송하는 단계를 연구하였으며 미 국방부의 보안관련 표준안(MIL-STD-2045-18500)과 국제전신전화자문위원회(CCITT)의 표준안에서 요구되는 메시지 전송 요구사항, 송수신 프로토콜의 상

세화 및 인증 개념을 추가하여 설계하였다. 또한, 새로운 프로토콜에 메시지 전송에 따른 비밀키를 사용하기 위해 SSL(Secure Socket Layer) 기능을 추가로 이용한다.

CMP는 문서등급별로 별도로 설계되었으며 각각 CMP1, CMP2, CMP3으로 분류한다. CMP1은 1급 비밀에 해당하는 중요한 전자문서를 전송할 때 사용할 목적으로 설계하며, CMP2는 대외비에 준하는 전자문서 취급시 사용할 목적으로 설계하고, CMP3은 일반적인 메일과 공고용 문서인 경우를 전송하기 위해서 설계한다.

CMP는 일괄처리로 인한 시간낭비를 줄이기 위해 문서를 중요도에 따른 등급별로 구분하여 처리하도록 설계하였으며, 다중 관리를 위한 부수적 시스템 관리를 최소화하도록 설계에 반영하였다.

MSP의 경우에는 다중접근 처리를 중심으로 처리하기 때문에 중앙에 접근 카드 데이터베이스를 운영하여 접근자의 업무처리 등급 및 직급에 따라 문서의 접수여부를 판별하도록 설계되어 있다. 그러므로 국내실정에서 이러한 시스템 환경에 알맞게 구축하려면 여러 가지 통합기술과 장비의 개발이 필요하다. <표1>은 메시지 보안 프로토콜과 CMP의 기능을 종합적으로 비교 분석한 결과이다.

<표1> MSP와 CMP 비교

구분	MSP	CMP1	CMP2	CMP3
전자서명	RSA	KCDSA	KCDSA	KCDSA
비밀키	DES	SEED	SEED	-
해쉬	MD5	MD5	MD5	MD5
헤더	전체정보	전체정보	송수신정보	키정보
문서전송	전체전송	전체전송	일부전송	내용전송
키관리	카드사용	비밀키	비밀키	비밀키
전송기반	응용계층	SSL이용	SSL이용	SSL이용

3.2 CMP 구현

CMP 프로토콜을 구현하기 위해서 메인 구조와 헤더구조 그리고 메인을 지원하는 라이브러리 형태로 구분하여 구현하였다. 메인 구조와 헤더는 Visual C++로 구현하였으며 라이브러리 형태는 키관리와 전자서명 알고리즘인 KCDSA와 대칭키 시스템인 SEED를 사용하였다. 메인 구조는 전송 송신처리기(CMP Sender)와 전송된 메시지를 처리할 수신서버 처리기(CMP Server)로 나누어 개발하였다.

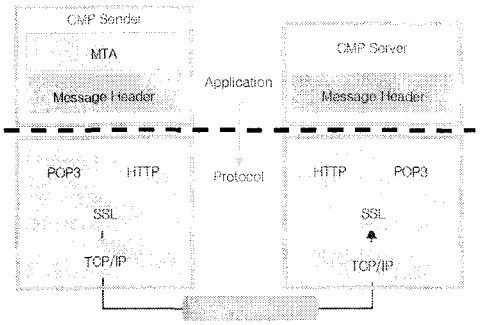

그림 2. CMP 구현 흐름도

CMP 메시지 전송 완료 화면은 그림 3과 같이 전송 시스템에서 암·복호화를 하고 헤더로 작성된 메시지가 네트워크상에서 전송되는 시간까지 표시할 수 있도록 하였으며 이 부분은 문서관리에 중요한 요소로서 시간관리에 해당하는 부분이다. 특히 알림창에서는 0.01ms의 문서처리와 0.11ms의 전송 속도를 나타내고 있다.

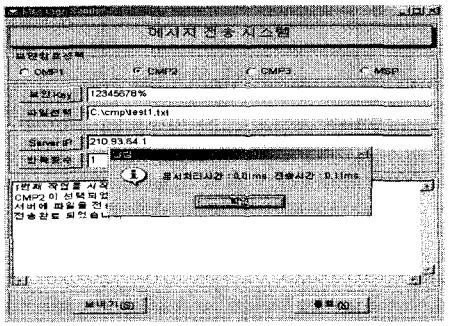

그림 3. CMP 메시지 전송완료

3.3 CMP 성능분석

본 논문에서 구현한 CMP의 성능에 대하여 MSP에 대한 상대적 우위성을 검증하기 위해 모의실험에 의한 분석을 시행하였다. 프로토콜간의 성능비교를 위해 자료 유형별 전송횟수별 전송결과 얻어지는 수치를 중심으로 평균값을 비교하는 방식을 채택했다.

성능비교를 위한 실험 순서는 메시지 보안 프로토콜(MSP)과 CMP1, CMP2, CMP3 순으로 하고 실험한 후 얻어지는 자료에 대한 최적 분석 방법을 실시

하였다.

<표2> 100회 실시CMP 누적값(60KB±)

(단위:ms)

구 분	CMP1	CMP2	CMP3	CMP평균	MSP
음 악	313.00	306.00	285.00	301.33	305.00
동영상	824.00	780.00	679.00	761.00	761.00
그 림	298.00	268.00	214.00	260.00	264.00
압 축	320.00	310.00	210.00	280.00	280.00
숫 자	290.00	230.00	105.00	208.33	219.00
영 문	295.00	274.00	213.00	260.67	272.00
한 글	498.00	456.00	390.00	448.00	452.00

3.4 CMP 보안성 분석

본 논문에서 구현한 CMP의 보안성 분석을 위하여 국제공통평가기준(CC : Common Criteria)과 내용 면에서는 공통성이 있는 미연방 정보처리기준(FIPS : Federal Information Processing Standard)과 비교하여 유사성을 가장 많이 분석할 수 있는 항목을 선정하여 분석한다[9]

보안성 분석의 암호모듈 명세서 요구사항과 운영시스템 보안 사항 그리고 자가 시험에서는 MSP와 CMP 모두 공인된 알고리즘을 사용하며 인증기반 운영자 신원확인으로 인한 최상위 평가를 할 수 있으며 암호모듈 인터페이스와 암호키 관리 요구사항에서는 CMP의 전송포트 등급별 분리를 통한 관리와 MSP의 포테자 카드사용으로 인한 분실의 위험으로 정보유출의 문제 때문에 MSP보다 CMP가 보안성 분석에서는 좋은 결과를 얻었다.

보안기능성 평가 및 보증성 평가에서는 MSP와 CMP 모두 유사한 성능 분석결과가 나타남을 알 수 있었다.

4. 결론

본 논문은 메시지 전송 시스템과 관련하여 국내의 정보통신시스템 및 정보처리 환경에 적합한 보안기술을 채택하여 CMP를 설계했으며 또한 제안된 안전한 메시지 전송 프로토콜인 CMP의 검증을 위해 메시지 보안 프로토콜인 MSP와 성능실험을 통해 그 기능을 비교 평가하였다.

제안한 CMP 프로토콜과 기존 MSP 프로토콜간의 성능비교를 위해 자료 유형별 전송횟수별로 실제 전송결과 얻어지는 수치를 중심으로 평균값을 비교한 결과, 100회 전송횟수별 분석결과에서는 전반적인 성능분석에서 CMP의 평균속도가 MSP보다 전송속도가 음악파일에서는 3.67ms, 그림 파일에서는 4.00ms, 숫자파일에서는 10.67ms, 영문파일에서는 11.33ms, 한글파일에서는 4.00ms 각각 빠르게 나타남을 알 수 있었다.

CMP의 보안성 분석결과에서는 CMP는 암호모듈 인터페이스, 암호키 관리에서 MSP보다 우수한 성능을 보였으며, 암호모듈 명세서, 역할 서비스와 인증, 운영시스템 보안, 자가시험, 보안기능성, 보증성에서는 유사한 성능을 보였다.

참고문헌

[1] E-Commerce Security "Security Blanket Has a Few Tatters", Network Computing, vol.11, no1, 2000, pp.64-68.

[2] Hughes, "Free-space Quantum Key Distribution in Daylight", Journal of Modern Optics, vol. 47, no.2-3, 2000, pp.549-562.

[3] IEEE Mag, "Internet Security", IEEE Communications Magazine, vol. 38, no.1, 2000, pp. 18-23.

[4] Barbara Guttman, Robert Bagwill, "DRAFT : Internet Security Policy: A Technical Guide", 1997, pp.108-148.

[5] E. Kabay Michel, "The NCSA Guide to Enterprise Security Protecting Information Assets", 1996, pp.225-230.

[6] Bruce Schneier, "Applied Cryptography", Willy, 1996, pp.3-12.

[7] Yi-Shiung, "Construct Message Authentication Code with One-Way Hash Functions and Block Ciphers", IEICE Trans, Fundamentals, vol E82-A, no.2, 1999, pp. 390-392.

[8] Common Criteria Editorial Board, "Common Criteria for Information Technology Security Evaluation", Part 1 : Introduction and General Model, Ver 2.0, 1997, pp.15-40.

[9] CMEB, Common Evaluation Methodology for Information Technology Security, Part 2 : Evaluation Methodology, Ver 0.6, 1999, pp.20-45.