정보보호의 연속성관리를 위한 보안프로토콜 검증

신승중* 송영규**
*중부대학교 컴퓨터안전관리학과
**충남대학교 전자공학과

The Verification in Security Protocol for Security Continuity Management

Seung-Jung Shin* , Young-gyu Song**
Dept of Computer Security Management, Joong-Bu University
Dept of Electronics, Chung-nam University

요 약

본 논문은 TCP/IP 상에서 보안 개념을 지속적으로 유지하기 위해 전자서명과 공개키 분배 및 인증 등의 기능이 포함된 메시지전송 프로토콜로 구현된 프로그램의 검증문제를 Choquet 퍼지적분을 이용하여 해결하고 이를 퍼지적분과 비교분석하였다. 기능별로 보안기술, 보안정책, 전자문서처리, 전자문서전송, 암·복호화키로 나누어 분류하여 구현된 내용을 기능별점수와 전문가의 요구사항을 구현된 프로토콜에서 산출 값과 비교하여 메시지 보안프로토콜을 기능별로 점수화하여 검증하였다.

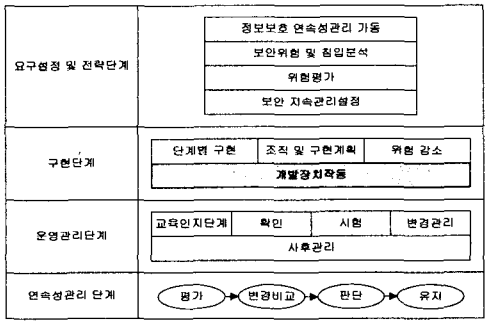
Abstract

The objective of this paper was to cope with the verification of the message transfer protocol that integrates the electronic signature and the distribution and authentication of public key in TCP/IP using security continuity management Choquet fuzzy integral compared with fuzzy integral. They were classified into the security technology, the security policy, the electronic document processing, the electronic document transportation and the encryption and decryption keys in its function. The measures of items of the message security protocol were produced for the verification of the implemented document in every function.

1. 서론

글로벌시대의 생각과 속도의 변화가 중요한 문제로 부각되면서 핵심기술인 암·복호화 문제를 구사하는 분야부터 대형 시스템의 물리적인 관리까지 총체적인 개념에서 문서의 전달은 매우 중요한 문제라 할 수 있다.[1] 그러므로 사용상의 문제점으로 위·변조, 처리속도, 송수신확인, 메시지보안 등을 말한다.[2]

TCP/IP 상에서 빈번히 일어날 수 있는 전자 서명과 공개키 분배 등 인증상의 문제를 도출해 내어 이를 해결하기 위한 방안으로 메시지를 안전하게 보내는 방법과 기존 연구를 통해 이에 대한 처리과정을 비교하여 정책에 대한 성능 및 기능 검증을 통한 보다 효율적인 방법이 필요하다. MSP(Message Security Protocol)에 대한 기술을 기본으로 하여, 우리 실정에 입각하여 실용적이고 법적인 문제와 전자문서를 암호화하고 전자서명과 수신자 확인서의 발급으로 완벽한 전자문서 관리 시스템을 구현한 프로토콜을 지속적으로 관리하는 것이 본 연구의 목적 있다.[10][11]



[그림 1] SCM 모델

[그림 1]은 단계별 정보보호의 연속성을 유지하기 위해서 지속 관리 모델이다. 특히, 기능별로 MSP와 SCMP(Security continuity Management Protocol)를 비교하였다. 초기단계에서 탐지유·무를 진단하고 전략개념으로 안전성을 구현하고, 운영관리 단계를 거쳐서 정보보호를 위한 연속성 관리 단계가 전개되는

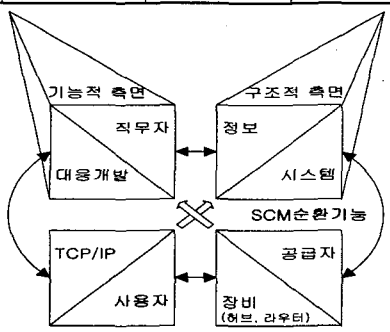
것이 SCM(Security continuity Management) 모델이다. 메시지 접근 보안등급, 다중등급보안에 대하여 MSP 에서의 차이점과 SCMP에서 처리되는 사항을 비교하였다.

2. SCM의 기능과 프로토콜의 구조

2.1 보안프로토콜의 구조

MSP는 메시지의 인증과 무결성, 기밀성, 부인봉쇄, 배달증명 등을 포함한 보안기술을 포함시켜 NSA의 주도하에서 개발되었다. 이러한 MSP의 기본 구조는 암호화된 메시지를 헤딩(Security Heading)하는 것으로 특히, 상호연결 개방시스템은 이기종 시스템이나 서로 다른 운영체제 하에서도 안전하게 메시지를 전달하는 기능을 구현하기 위한 구조이다. [그림 2]의 MSP의 구조 내용을 국제 표준 기구의 표준안과 비교하면 [표 1]과 같다[2][3][4].

구분	내 용		
구조	MSP		
	메시지전송		검색
	헤딩(Heading)	MSP내용	각 메시지별 캡슐화
기능	정보처리시스템	상호연결 개방시스템	안전한 자료네트워크시스템
	메시지전송	키관리	인 증
	메시지핸드링	보안프로토콜	디렉토리, 메일 프로토콜



[그림 2] MSP의 구조 기능과 SCM 기능

메시지 전송시스템은 통신 프로토콜 위에 정보의 누출을 방지하는 프로토콜을 이용하여 구현되는 시스템으로 [표 1]의 여러 기능이 구현되도록 설계되어 보안성 및 안전성이 보장되어야 하기 때문에 미국방성에서는 보안 제품의 기준을 정리하고 있다. 또한, [표 1]의 보안제품 기준안에는 MSP가 포함되어 있으며, MSP에 사용되는 DES나 RSA는 미국 상무성 표준국(NBS : 현재의 NIST)이 1977년에 제정 발표한 표준암호 방식[4]으로, 1993년에 제정된 인터넷의 PEM(Privacy Enhanced Mail))의 표준으로 사용되고 있다.

이러한 MSP 프로토콜은 기존의 X.400 MTS에 투명성을 제공하고 MSP 보호 서비스를 위한 MSP UA와 기능 개체(Functional entity)들로 구성되어 있으며 [그림 3]와 같은 기본 골격으로 구성되어 있다.

MSP는 대형 시스템에서 주로 운영되며 등급 보안을 다중화 하기 위하여 비밀등급카드를 이용하여 접근자를 통제하고 있고 수신자의 인증표(Certificate), 사용자주요자료(UKM), 보조벡터(Auxiliary vector, AV)를 얻기 위해 X.501과 X.509의 디렉토리 시스템을 이용하는 특징을 가지고 있다.

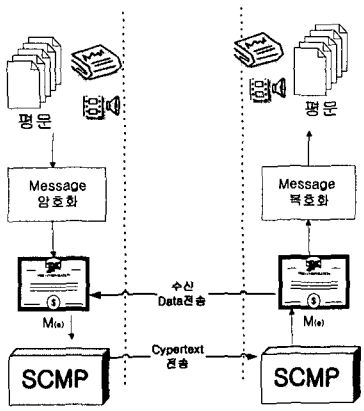
[표 1] 메시지 관련 기준안 비교표

형태	내용	기준안 구분
정보처리시스템	개방시스템상호연결- 보안구조	ISO 7498/2
상호연결 개방시스템	CCITT 응용을 위한 기본참고모델, 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	Models. 인증의 기본틀	CCITT X.501 CCITT X.509
메일전송프로토콜	J. B. Postel, August 1982	RFC821
ARPA 사용메시지의 기본틀을 위한 표준안	D. Crocker, 13 August 1982	RFC822
안전한자료망 구성 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
미 국방부의 보안제품 기준안	서비스 기본 배경과 지원부분 프로토콜의 내용 및 정의와 분류사항 메시지전송을 위한 요구조건 전송시스템의 접근요구 사항 전송시스템의 접근요구 사항	MIL-STD-2045-18500

2.2 SCMP의 구조

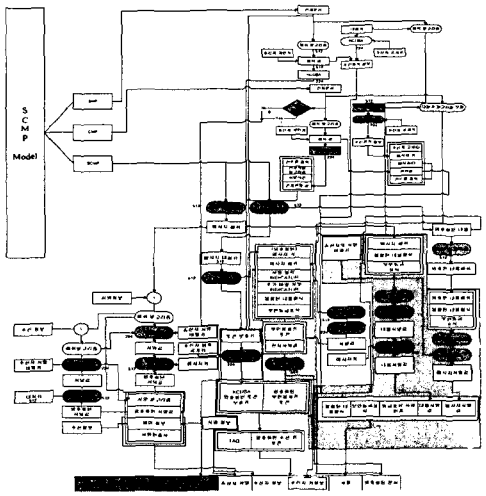
본 연구에서 설계된 SCMP는 일괄처리로 인한 시간소모를 해결하고 이기종 간에 메시지 전달을 원활히 하며 접근카드 미사용/클라이언트의 PC사용 가능성/메시지의 전달 여부를 서버에서 알 수 있도록 하였다. 특히 위기관리에 대처 할 수 있도록 구현하였다. 구체적으로 메시지를 헤더프로토콜에 탑재하여 메시지를 전송하는 단계를 중점적으로 연구하였으며 미 국방부 보안제품 기준안과 CCITT의 표준안에 따른 메시지 전송 요구사항, 송수신 프로토콜의 상세화, 인증의 개념을 추가하였다. SCMP는 일괄처리로 인한 시간소모를 제거하기 위해 문서를 중요도 등급별로 구분하여 처리하도록 설계되어 전자문서 교환의 효율성을 증대시킬 수 있으나 다양한 접근자들에 대한 복잡한 관리가 요구된다. 이러한 다중 관리를 위한 부수적 시스템 관리를 최소화하기 위해 문서등급을 미리 분류하여 처리하는 합리적 기능을 설계에 반영하였다.

또한 메시지 접근의 통제 수단으로 사용되는 카드를 제거하기 위해 MLMLP(Multi Layer Multi Link Protocol, 이하 MLMLP)기능을 이용함으로써 클라이언트 시스템을 PC급 시스템으로 대체할 수 있게 되었다.



[그림 3] SCM를 배경으로한 SCMP의 기본개념도

MLMLP는 SCMP 헤더에 Switching System을 부착하여 메시지가 기능별, 문서 내용별, 주요 사양별로 처리될 수 있도록 세 가지 형태로 개발되었다.



[그림 4] SCMP 프로토콜

이러한 SMP(Security Message Protocol)은 해쉬 알고리즘을 이용한 전자서명의 검증과 CMP (Cryptography Message Protocol) 헤더 생성을 위한 복잡한 과정으로 인해 처리 시간이 지연되는 단점이 있으나 취급되는 문서의 보안 처리 문제가 더 중요한 경우에는 유용하다. [그림 4]는 제안된 프로토콜의 처리 과정과 구조를 도시한 것으로 SCMP을 결합하여 재 설계한 것이다. 각각의 헤더를 따로 분리하여 메시지를 전송하기 위하여 기다리는 불편이나, 등급별에 의한 분류를 할 수 있으며, 취약점이 발견될 시 즉시 수정보완을 지향하는 프로토콜이다.

2.3 MSP와 SCMP의 분석

MSP는 대형시스템 내에서 구현되었고 SCMP는 중·소형 서버에서 운영될 수 있도록 설계하였다. 간단한 구조에서 복잡한 암호화를 거쳐 만들어진 문서를 전송하는 헤더이다. [표 2]는 SCMP와 MSP의 헤더 기능을 비교한 것으로 헤더 보유, 수신자 암호데이타, 암호화된 전자문서, 문서 각 기능을 캡슐화하여 확장부분에 탑재하는 기능이 공통적이다.

[표 2] 항목별 헤더기능 비교표

헤더기능	SCMP	MSP	비고
헤더보유	o	o	
서명블럭		o	
수신자암호데이타	o	o	
요구확인서	o		
메세지 보안등급 및 분류처리	o		
서명알고리즘		o	
메세지 목록		o	
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 관리시스템이 필요하다. 반면 SCMP의 요구확인서, MLML, 키정보는 현재 보유하고 있는 시스템에서 다중 처리 기능을 지원하도록 설계되었다.

한편 MSP와 SCMP의 기능을 종합적으로 비교한 결과는 [표 3]과 같다. 먼저 헤더 사용 시 여러 기능을 탑재하여 속도, 시스템 사용시간, 데이터로드 및 처리 시간을 각각 비교한 결과 전송처리시간에 있어서는 SCMP가 처리의 단순화로 다소 빠른 것으로 예상되었다.

한편 MSP는 접근자 처리에 있어 접근자 관리 시스템에서 키 관리에 따른 접근자의 개별정보를 요구하고 있으나 SCMP는 비밀키를 업무 처리자에게 별도 부여함으로써 간단히 처리할 수 있다. 또한 MSP의 보안 전송 기능은 OSI 참조 모델의 응용계층에서 처리되도록 설계되었다.

또한 SCMP는 SSL(Secure Socket Layer)을 이용함으로써 보다 안전한 전송이 이루어질 수 있도록 설계되었으며 메시지가 SCMP에 등록되면 문서 등급에 따라 선택되어질 프로토콜로 로드되어 메시지 앞에 헤더값이 붙도록 하였다.

3. 프로토콜의 검증 및 고찰

본 논문에서 제안된 프로토콜과 메세지 보안 프로토콜과의 비교우위를 검증하기 위하여 Choquet 퍼지적분을 이용하였다. 적용된 퍼지적분은 어떤 대상이 여러 항목에 대해서 평가되고 각 평가 항목의 중요도에 차이가 있을 때 이들에 대한 평가치를 종합하는데 유효하다. 따라서 보안 프로토콜에 대한 비교분석에서 고려해야할 보안기술, 정책등의 여러 항목에 대한 비교우위를 검증하는 데에 적용하였다. 먼저 분석할 보안 프로토콜이 갖추어야 할 조건을 결정한 다음 각 조건의 상대적인 중요도를 결정할 수 있다. 퍼지적분을 적용하기 위하여 보안을 위한 메시지 프로토콜의 기능적인 부분을 항목별로 분류하여 빈도분석을 한 내용을 SCM를 배경으로 나타내었다.

[표 3] 프로토콜별 데이터

번호	대항목	소항목	점 수	MSP(h(x)			CMP(h(x)		
				1	2	3	SCMI	CMP	SMP
1	보안기술	기밀성	0.05380	0.99	0.99	0.99	0.99	0.91	0.85
2		무결성	0.04782	1.00	1.00	1.00	1.00	0.98	0.97
3		송신부인봉쇄	0.04136	0.90	0.90	0.90	0.91	0.90	0.88
4		수신부인봉쇄	0.04878	0.92	0.92	0.92	0.92	0.91	0.90
5	보안정책	메세지 등급 제한	0.04830	0.00	0.00	0.00	0.90	0.90	0.90
6		메세지 분류 처리	0.04734	0.00	0.00	0.00	0.95	0.98	0.95
7		메세지 접근 등급	0.05236	0.00	0.00	0.00	0.98	0.50	0.00
8		다중등급보안	0.04854	0.99	0.99	0.99	0.00	0.00	0.00
9	전자문서관리	수신자확인서	0.03778	0.98	0.98	0.98	0.95	0.91	0.00
10		전자서명	0.05786	0.95	0.95	0.95	0.94	0.94	0.00
11		수신자키정보	0.04423	0.88	0.88	0.88	0.90	0.89	0.00
12		암호화된 전자문서	0.04902	0.99	0.99	0.99	0.97	0.55	0.23
13	전자문서전송	송수신자확인	0.04902	1.00	1.00	1.00	1.00	1.00	0.00
14		내용 위·변조확인	0.05595	0.97	0.97	0.97	0.96	0.95	0.00
15		송·수신시간확인	0.04089	1.00	1.00	1.00	1.00	1.00	1.00
16		인증및 인증서확인	0.05691	0.00	0.00	0.00	0.00	0.00	0.00
17	암·복호화키	RSA	0.07030	1.00	1.00	1.00	0.00	0.00	0.00
18		KCDSA	0.04160	0.00	0.00	0.00	1.00	1.00	1.00
19		DES	0.06647	1.00	1.00	1.00	0.00	0.00	0.00
20		SEED	0.04160	0.00	0.00	0.00	1.00	1.00	1.00

[표 4] MSP와 SCMP의 결과비교

구분 / 종류	MSP	SCMP	CMP	SMP
FUZZY INTEGRAL 에 의한 방법	0.667660	0.702470	0.612170	0.290344
CHOQUET FUZZY INTEGRAL에 의한 방법	0.165381	0.220113	0.203884	0.142592

수게노(Sugeno)의 일반적인 퍼지적분의 정의는 다음과 같다.

$$\int_X h(x) \circ g(\cdot) = \sup_{E \subseteq X} \mathrm{Min}[\min_{x \in E} h(x), g(E)]$$

그리고 적용된 Choquet 퍼지적분은 다음과 같이 정의된다.

$$\int_X h(x) \circ g(\cdot) = \sum_{i=1}^{n} h(x_i)[g(A_i) - g(A_{i+1})]$$

여기서 h(x)는 데이터에 대한 MSP와 CMP의 처리결과이고 g(x)는 각 항목에 대한 척도이다. 먼저 퍼지적분에 의한 방법에서는 CMP1에 의한 방법이 가장 우수한 것으로 나타나 있다. 반면에 Choquet에 의한 방법에서는 기존의 CMP과 CMP2에 의한 방법이 우수한 것으로 나타나 있다.

CMP에 SCM를 포함시킨 SCMP는MSP에 비하여 알고리즘의 제한 규모가 작고 MSP는 항목에 의한 알고리즘이 골고루 배치되어 있으므로 상기와 같은 결과를 볼 수 있다.

4. 결론

본 논문에서는 미국의 MSP의 메시지 처리환경을 보완하고, 다중 등급 보안을 토대로 지속적인 정보보호를 기반으로 하여 우리나라의 시스템환경에 적합하도록 SCMP를 개발하였다. 이를 사용하여 각각의 문서에 차등을 적용하여 합리적인 방법으로 메시지를 처리하도록 하였다. 또한, MSP와 CMP의 프로토콜의 검증을 위하여 퍼지적분을 이용하여 수행하였다.

이로서 보안알고리즘으로 구성된 프로그램은 수시로 보완될 수 있도록 SCM의 절차를 준수하고 이를 통하여 관리하는 프로토콜은 외부에서 침입하고자 하는 의도에 따라 제한된 사항을 준수하고 갈수록 지능화되어 가는 시스템보호 측면에서 지속적인 연구가 요구되며, 이를 검증하기 위해서 Choquet 퍼지적분을 사용하여 MSP와 SCMP의 등급별, 항목별의 결과 값에 다소 차이가 있는 것을 확인할 수 있다. 또한 각 문서에 따른 평가데이터의 구성에 있어서 보다 효율적인 면에서 구성이 보완되어야 할 것으로 보고, 아직까지는 SCMP의 보안 평가치가 다소 낮은 것을 볼 수 있으나, 앞으로 이를 바탕으로 새로운 보안 서비스 설계 및 구현에 많은 참조가 되기를 바라며 향후 지속적인 형상관리와 개발 및 분석을 통하여 좀 더 안전하고 합리적인 보안 서비스 설계가 이루어져야 할 것으로 사료된다.

참고문헌

[1] 신승중, 정보시스템 안전론, 홍진출판사, pp.9, 2000

[2] 정보보호센타, 정보보호뉴스 22호, 한국정보보호센타, pp2, 1999.

[3] 정보보호 심포지움 '99, "인증관리 센터 구축 및 운영계획" 1999.

[4] H. Feistel, "Cryptography and Computer Privacy, "Scientific American, pp.15-23, 1973.

[5] National Bureau of Standards, Data Encryption Standard, U.S. FIPS PUB49, pp. 17-18, 1977.

[6] A. Simmizu and S.Miyaguchi, "Fast Data Encipherment Algorithm FEAL, "Eurocrypt'87, pp. 267-278, 1987.

[7] 한국 정보 보호 센터, "인증 업무 준칙, "한국 정보 보호 센터 내부 자료, 1999.

[8] 정보통신부,"정보보호산업발전대책(1998-2002)", pp70-77, 1997.

[9] 한국전자통신 연구원, "인터넷 상거래의 물결", 한국전자통신 연구원, pp128-129, 1998.

[10] http://www.kisa.or.kr/pds/att/missi.hwp

[11] http://www.imc.org/workshop/sdn701.txt 1994.

[12] Caption J. Detombe CD, A Comparison of Two Protocols - PEM vs MSP, 7th ACCSS, May, 1995.

[13] http://www.imc.org/workshop/sdn701.txt 1997.

[14] http://www.armadillo.huntsville.al.us/index.html

[15] 신승중, 박인규 "퍼지적분을 이용한 메시지 프로토콜 검증" vol.3, no7, 한국정보처리학회, 2000

[16] 신승중, 김현수 "보안문서 전용 메시지 프로토콜 구현" vol.2, no 2, 한국DB학회, 2000