퍼지적분을 이용한 메시지 프로토콜 검증

신 승 중† · 박 인 규††

요 약

본 논문은 TCP/IP 상에서 전자서명과 공개키 분배 및 인증 등의 기능이 포함된 메시지전송 프로토콜로 구현된 프로그램의 검증문제를 퍼지적분을 이용하여 해결하였다. 기능별로 보안기술, 보안정책, 전자문서처리, 전자문서전송, 암·복호화키로 나누어 분류하여 구현된 내용을 기능별점수와 전문가의 요구사항을 구현된 프로토콜에서 산출 값과 비교하여 메시지 보안프로토콜을 기능별로 집수화하여 검증하였다.

A New Approach to the Verification of a Message Protocol : Fuzzy Integral

Seung-Jung Shin† · In-Kue Park††

ABSTRACT

The objective of this paper was to cope with the verification of the mesage transfer protocol that integrates the electronic signature and the distribution and authentication of public key in TCP/IP using 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. 서 론

최근 기업간의 경쟁이 치열해 지면서 조직의 생산성 증대와 효율화를 위한 정보시스템의 역할이 더욱 중요해지고 있다[1]. 전자문서전송 프로토콜 기능에도 크게 광의적인 개념과 협의적인 개념으로 나누어 볼 수 있다. 광의적인 개념으로는 시스템 전반에 걸쳐 전사적이며 통합된 상태이다. 특히 핵심기술인 암·복호화 문제를 구사하는 분야부터 대형 시스템의 물리적인 관리까지 총체적인 개념이다 반면에 협의적인 개념으로는 사용상의 문제점으로 위·변조, 처리속도, 송수신확인, 메시지보안 등을 말한다. 따라서 협의적인 전자서명이나 암호방식에 의한 당사자간의 확인이며 이러한 방법으로 네트웍 상에 자신과 당사자를 서로 확인하는 과정을 말하며 이러한 것을 '증명한다'라고 말할 수 있다[2].

TCP/IP 상에서 빈번히 일어날 수 있는 전자 서명과 공개키 분배 등 인증상의 문제를 도출해내어 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 현재 미국에서 개발한 메시지보안 프로토콜에 대한 기술을 기본으로 하여 전자문서처리 및 전자서명에 관한 기본 사항과 이에 따른 제반 사항을 작성하고, 우리 실정에 입각하여 실용적이고 법적인 문제와 전자문서물 암호화하고 전자서명과 수신자 확인서의 발급으로 완벽한 전자문서 관리 시스템을 구

† 정 회 원 : 중부대학교 정보공학부 컴퓨터안전관리학과 교수
†† 정 회 원 : 중부대학교 정보공학부 전자계산학과 교수
논문접수 : 2000년 1월 13일, 심사완료 2000년 6월 8일

현하는데 본 연구의 목적이 있다[10, 11].

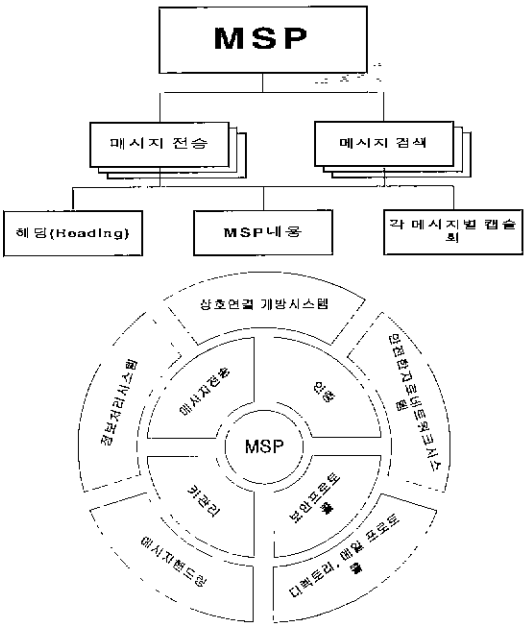
현재 인터넷상에서의 문서이동이 급증하고 있고 지속적으로 전자정부에 대한 연구가 여러 분야에서 활발히 이루어지고 있는 실정이다. 이는 문서를 Web상에서 안전하게 전달하는 것이 최고의 과제라 하겠다. 이러한 추세에 부합하기 위한 일환으로 보안 프로토콜의 개발을 위한 방법으로 기존의 메시지보안프로토콜보다 효율적인 새로운 메시지프로토콜을 설계하였다. 또한 제안된 프로토콜의 성능을 검증하기 위하여 보안 프로토콜의 대표적인 기능들을 선별하여 그 기능들을 퍼지 적분을 이용하여 검증하였다. 기능별로 메시지 보안 프로토콜과 새로운 메시지 프로토콜를 비교하여, 각 기능별의 차이점을 도출 및 비교를 통한 차이점을 구체적으로 살펴보면서 보안기술에서 소항목에 해당하는 기밀성과 무결성, 송신부인봉쇄, 수신부인봉쇄를 설문지에서 추출한 값으로 그 차이를 분석하여 각 기능을 비교하였다. 정책에 의한 구체적인 내용에서도 메시지 보안등급 제한, 메시지 접근 보안등급, 다중등급보안에 대하여 메시지보안 프로토콜에서의 차이점과 새로운 메시지 프로토콜에서 처리되는 사항을 비교하였다

2. 메시지보안프로토콜과 새로운 메시지프로토콜의 구조

2.1 메시지보안프로토콜의 구조

메시지보안 프로토콜은 메시지의 인증과 무결성, 기밀성, 부인봉쇄, 배달증명 등을 포함한 보안기술을 포함시켜 NSA의 주도하에서 개발되었다. 이러한 메시지 보안 프로토콜의 기본 구조는 (그림 1)과 같이 암호화된 메시지를 해딩(Security Heading)하는 것으로 특히, 상호연결 개방시스템은 이기종 시스템이나 서로 다른 운영체제 하에서도 안전하게 메시지를 전달하는 기능을 구현하기 위한 구조이다. (그림 1)의 메시지보안 프로토콜의 구조 및 기능의 내용을 국제 표준 기구의 표준안과 비교하면 <표 1>과 같다[2-4]

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 미 국방성에서는 보안 제품의 기준을 다음 <표 2>와 같이 정리하고 있다. <표 2>의 보안제품 기준안에는 메시지보안 프로토콜이 포함되어 있으며, 메시지보안 프로토콜에 사용되는 DES나 RSA는 미국 상무성 표준국(NBS : 현재의 NIST)이 1977년에 제정 발표한 표준암호 방식[4]으로, 1993년에 재정된 인터넷의 PEM(Privacy Enhanced Mail)의 표준으로 사용되고 있다.



(그림 1) 메시지보안 프로토콜의 구조와 기능

〈표 1〉 메시지보안 프로토콜 관련 기준안 비교표

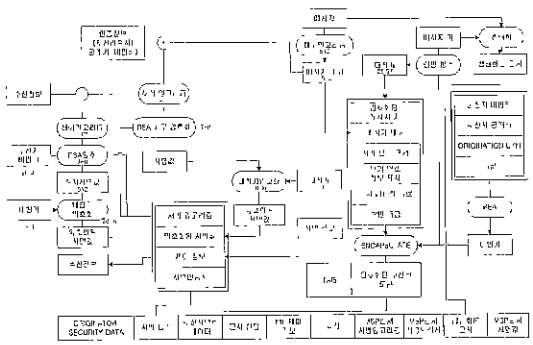
항 목	내 용	기준안 구분
정보처리시스템	개방시스템상호연결 - 보안구조	ISO 7498/2
상호연결 개방시스템	CCITT 응용을 위한 기본참고모델, 변환문 요약의 상세화, 변화문 요약을 위한 기본암호규칙의 상세화	CCITT X.200 CCITT X.208 CCITT X.209
메시지운용	서비스의 시스템의 요약, 메시지전송시스템 요약정보서비스의 정의 및 절차, 프로토콜의 상세화, 메시지 시스템	CCITT X.400 CCITT X.411 CCITT X.419 CCITT X.420
훈령집	Models 인증의 기본틀	CCITT X.501 CCITT X.509
메일전송프로토콜	J. B Postel, August 1982	RFC821
ARPA 사용메시지의 기본틀을 위한 표준안	D Crocker, 13 August 1982	RFC822
안전한 자료망구성 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

〈표 2〉 미 국방부의 보안제품 기준내역

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

이러한 메시지보안프로토콜은 기존의 X.400 MTS에 투명성을 제공하고 메시지보안 프로토콜 보호 서비스를 위한 메시지보안 프로토콜 UA와 기능 개체(Functional entity)들로 구성되어 있으며 (그림 2)와 같은 기본 골격으로 구성되어 있다.

메시지보안 프로토콜은 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.

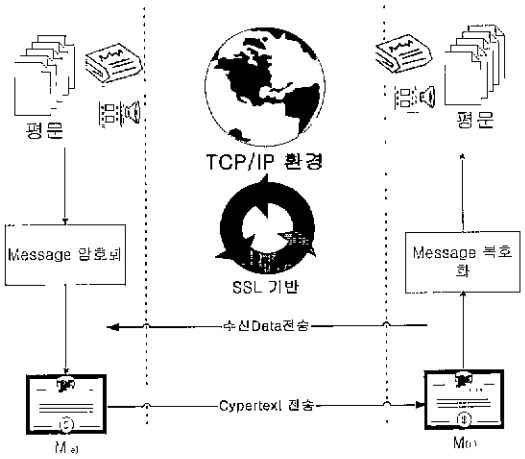


(그림 2) 메시지보안 프로토콜 프로토콜

그리고 본 연구에서는 새로운 메시지프로토콜를 CMP (암호문 메시지프로토콜 : Cryptography Message Protocal, 이하 CMP)라고 하겠다.

2.2 CMP의 구조

본 연구에서 설계된 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) CMP 1, 2, 3은 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.



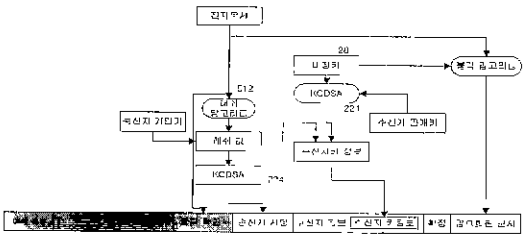
(그림 3) CMP의 기본개념도

또한 메시지 접근의 통제 수단으로 사용되는 카드를 제거하기 위해 MLML(Multi Layer Multi Link, 이하 MLML)기능을 이용함으로써 클라이언트 시스템을 PC급 시스템으로 대체할 수 있게 되었다. MLML는 CMP 헤더에 Switching System을 부착하여 메시지가 기능별, 문서 내용별, 주요 사양별로 처리될 수 있도록 세 가지 형태로 개발되었다.

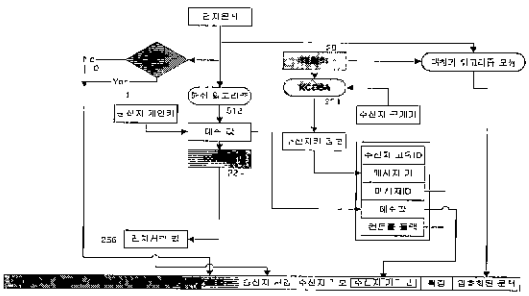
(그림 4)의 MLML3는 문서의 복잡도와 시스템 트래픽에 따라 문서를 구분하고 보안 등급에 따라 처리하도록 하였다. 이러한 전자문서관리시스템을 암호화 방법이 간단하고 보다 신속한 업무처리 지원할 수 있는 장점이 있어 단순한 메시지, 서신, 공지사항 등에 사용할 수 있다. MLML3은 CMP3과 같은 명칭으로 전자문서를 1회 암호화하고 이를 수신자 키 정보에 수록하여 전송함으로써 간단하지만 안전성을 고려한 프로토콜이다

(그림 5)의 MLML2는 메시지보안 프로토콜의 메시

지 헤더 부분에 전체 정보가 아니라 송수신자 암호 데이터의 해쉬값만을 전송하도록 단순화시킨 전자문서관리시스템이다



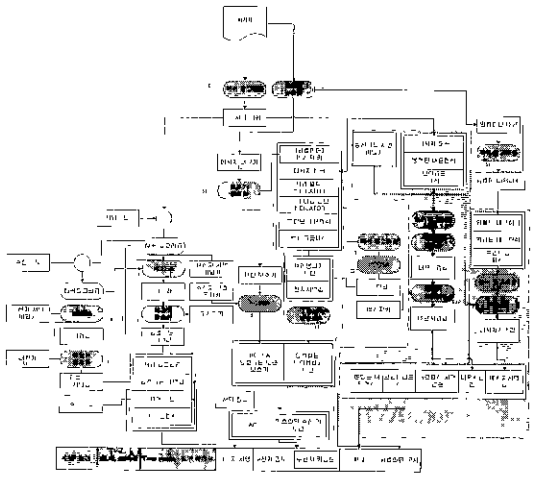
(그림 4) MLML3 프로토콜을 이용한 CMP3



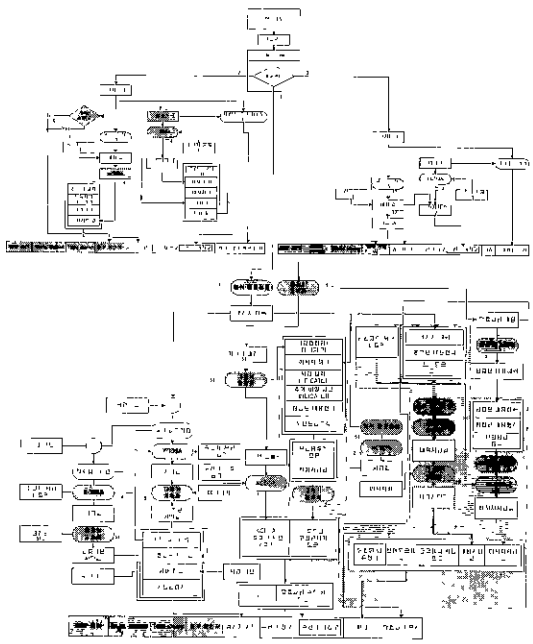
(그림 5) MLML2 프로토콜을 이용한 CMP2

MLML2는 암호화 및 복호화가 용이하고 대체로 안전하게 문서 처리를 할 수 있는 프로토콜로 비교적 단순하면서 보안성을 요구할 때 사용된다. MLML2는 CMP2와 같은 명칭으로 대외비 또는 어느 정도의 비밀성을 유지해야 하는 문서처리를 위해 설계된 프로토콜이다 (그림 6)의 MLML1은 CMP1과 같은 명칭으로, 메시지보안 프로토콜의 메시지 헤더 부분에 있는 송수신자 데이터를 암호화, 캡슐화하여 기록하는 확장부분을 일부 수정한 프로토콜이다. MLML1은 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 MLML1은 해쉬 알고리즘을 이용한 전자서명의 검증과 CMP 헤더 생성을 위한 복잡한 과정으로 인해 처리 시간이 지연되는 단점이 있으나 취급되는 문서의 보안 처리 문제가 더 중요한 경우에는 유용하다. (그림 7)은 제안된 프로토콜의 처리 과정과 구조를 도시한 것으로 CMP1, 2, 3을 결합하여 재 설계한 것이다. 각각의 헤더를 따로 분리하여 메시지를 전송하기 위하여 기다리는 불편이나, 등급별에 의한 분류를 할 수 있는 프로토콜이다.



(그림 6) MLML1 프로토콜을 이용한 CMP1



(그림 7) CMP 프로토콜

2.3 메시지보안프로토콜과 CMP의 분석

메시지보안 프로토콜은 대형시스템 내에서 구현되었

고 CMP는 중·소형 서버에서 운영될 수 있도록 설계하였다. 간단한 구조에서 복잡한 암호화를 거쳐 만들어진 문서를 전송하는 헤더이다 <표 3>은 CMP와 메시지보안 프로토콜의 헤더 기능을 비교한 것으로 헤더보유, 수신자 암호데이타, 암호화된 전자문서, 문서 각 기능을 캡슐화하여 확장부분에 탑재하는 기능이 공통적이다.

〈표 3〉 항목별 헤더기능 비교표

헤더기능	CMP	메시지 보안프로토콜	비고
헤더보유	o	o	
서명블럭		o	
수신자암호데이타	o	o	
요구확인서	o		
메세지 보안등급 및 분류처리	o		
서명알고리즘		o	
메세지 목록		o	
암호화된 긴자문서	o	o	
확정	o	o	
키정보	o		

메시지보안 프로토콜 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 CMP의 요구확인서, MLML, 키정보는 현재 보유하고 있는 시스템에서 다중 처리 기능을 지원하도록 설계되었다

한편 메시지보안 프로토콜과 CMP의 기능을 종합적으로 비교한 결과는 <표 4>와 같다. 먼저 헤더 사용시 여러 기능을 탑재하여 속도, 시스템 사용시간, 데이터로드 및 처리 시간을 각각 비교한 결과 전송처리시간에 있어서는 CMP가 처리의 단순화로 다소 빠른 것으로 예상되었다.

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

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

〈표 4〉 메시지보안 프로토콜과 CMP 비교표

구 분	메시지보안 프로토콜	CMP1	CMP2	CMP3	비 고
전송처리시간	메시지보안 프로토콜	-	,-	-	
공개키암호화 알고리즘	RSA	KCDSA	KCDSA	KCDSA	군수품 수출규제로 국내 표준 사용
비밀키암호화 알고리즘	DES	SEED	SEED	-	규제
해쉬값	MD5	MD5	MD5	MD5	
메시지 헤더	전체정보	전체정보	공수신정보	키정보	class 이용
문서전송	전체전송	전체전송	일부정보전송	내용위주전송	
위변조확인	확인	recv_stemp ,	recv_stemp ,	recv_stemp ,	
송·수신 확인		분류	-	-	통합관리 가능
인증서비스	접근자의 정보에 따라 인증제공	송·수신자 정보로 인증 관리	송·수신자 정보로 인증 관리	송신자 서명이 의해 인증	
키관리	접근시 키드사용	비밀키	비밀키	비밀키	
보안기능 전송기반	OSI에넘의 응용층 이용	SSL이용	SSL이용	SSL이용	

3. 프로토콜의 검증 및 고찰

본 논문에서 제안된 프로토콜과 메세지 보안 프로토콜과의 비교우위를 검증하기 위하여 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 고려해야 할 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 <표 5>에 나타내었다. 특히 보안기술, 보안정책, 전자문서관리, 전자문서전송, 암·복호화키의 다섯가지 항목으로 분류하고, 각 항목에 대해 세부항목을 작성하였다.

위에서 제시된 프로토콜의 기능별 통계표 의하여 다음에 나타나 있는 항목에 따른 퍼지척도의 결과를 <표 6>에 나타내었다 분류에 의한 갑을 병의 등급은 퍼지적분의 부분집합을 구성 및 정규화과정을 위해 편의상 갑, 을, 병, 정으로 분류하였다.

〈표 5〉 프로토콜의 기능별통계표

Statistics

	N		Mean	Median	Mode	Std. Deviation	Minimum	Maximum	Percentiles		
	Valid	Missing							25	50	75
키 생성	47	0	3.7021	4.0000	4.00	1.2287	1.00	5.00	3.0000	4.0000	5.0000
은자경성	47	0	43.7021	33.0000	.00a	37.4547	1.00	120.00	13.0000	33.0000	59.0000
무결성	47	0	3.4894	3.0000	3.00	2.2803	1.00	8.00	2.0000	3.0000	5.0000
키 생성	47	0	4.7872	5.0000	5.00	2.9183	1.00	9.00	2.0000	5.0000	6.0000
키 노출	47	0	4.7234	5.0000	5.00	2.1803	1.00	9.00	4.0000	5.0000	6.0000
노출 시점	47	0	4.2979	5.0000	5.00	2.2929	1.00	9.00	2.0000	5.0000	6.0000
키 삭	47	0	4.2553	5.0000	5.00	2.4511	1.00	10.00	2.0000	5.0000	6.0000
생성	47	0	4.7872	5.0000	5.00	2.4899	1.00	10.00	4.0000	5.0000	6.0000
노출 시점	47	0	4.2128	5.0000	5.00	2.1145	1.00	10.00	2.0000	5.0000	6.0000
생성	47	0	1.2340	1.0000	1.00	.4260	1.00	3.00	1.0000	1.0000	1.0000
노출 시점	47	0	3.6809	5.0000	5.00	1.7659	1.00	5.00	2.0000	5.0000	5.0000
노출 시점	47	0	4.3617	5.0000	5.00	2.5737	1.00	10.00	2.0000	5.0000	5.0000
키 삭제	47	0	4.4894	5.0000	5.00	2.7601	1.00	10.00	2.0000	5.0000	5.0000
생성	47	0	3.9787	4.0000	5.00	1.5395	1.00	8.00	2.0000	4.0000	5.0000
노출 시점	47	0	3.9362	5.0000	5.00	2.2289	1.00	10.00	2.0000	5.0000	5.0000
삭제	47	0	3.8511	3.0000	2.00	2.2165	1.00	8.00	2.0000	3.0000	5.0000
노출 시점	47	0	4.3617	5.0000	5.00	2.1888	1.00	10.00	4.0000	5.0000	6.0000
생성	47	0	2.7234	2.0000	2.00	1.5147	1.00	5.00	1.0000	2.0000	3.0000
키 개인	47	0	5.7234	5.0000	5.00	2.7170	1.00	10.00	4.0000	5.0000	7.0000
삭제하도	47	0	5.1489	5.0000	5.00	2.3187	1.00	10.00	3.0000	5.0000	7.0000
관리등급	47	0	4.6170	5.0000	5.00	2.0353	1.00	10.00	3.0000	5.0000	5.0000
RSA	47	0	5.5106	5.0000	5.00	2.2021	1.00	10.00	3.0000	5.0000	10.0000
KCDSA	47	0	3.4043	3.0000	5.00	1.9551	1.00	10.00	2.0000	4.0000	5.0000
DES	47	0	5.5532	5.0000	10.00	3.4753	1.00	12.00	2.0000	5.0000	10.0000
SEED	47	0	3.7021	5.0000	5.00	1.9391	1.00	10.00	2.0000	5.0000	5.0000

a. Multiple modes exist. The smallest value is shown

〈표 6〉 항목에 따른 퍼지척도

번호	대항목	소항목	집수	분류
1	보안기술	기밀성	0.05380	을
2		무결성	0.04782	병
3		송신부인봉쇄	0.04136	병
4		수신부인봉쇄	0.04878	빙
5	보안정책	메세지 보안등급 개한	0.04830	병
6		메세지 분류 커리	0.04734	병
7		메세지 접근 보안등급	0.05236	을
8		다중등급보안	0.04854	빙
9	전자문서관리	수신지확인서	0.03778	정
10		전자서명	0.05786	을
11		수신자키정보	0.04423	빙
12		암호화된 전자문서	0.04902	병
13	전자문서전송	송수신자확인	0.04902	병
14		내용 위·변조확인	0.05595	을
15		송·수신시간확인	0.04089	병
16		인증기관 및 인증서확인	0.05691	을
17	암·복호화키	RSA	0.07030	갑
18		KCDSA	0.04160	병
19		DES	0.06647	갑
20		SEED	0.04160	빙

<표 6>에 나타난 항목에 대한 부분집합을 30개의 부분집합으로 구성한 예를 <표 7>에 나타내었다. 이러한 부분집합이 가지는 의미는 일단 대상에 대한 평가의 각도를 전체적인 면에서가 아닌 부분들에 대한 평가치들로 고려한 다음에 이러한 모든 부분집합들에 대한 평가치들을 전체적으로 고려(적분)하여 최종적인 평가를 할 수가 있다

항목의 집합 X = {보안기술, 보안정책, 전자문서관리, 전자문서전송}라고 할 경우, 평가항목의 중요도를 다음과 같은 퍼지척도 g(·)로 나타낸다고 하면 각 등급에 따른 문서에 대한 메시지보안 프로토콜, CMP의 각 프로토콜에 대한 항목에 대한 입력값이 <표 8>에 나타나 있다. g({보안기술}) = 0.1, g({보안정책}) = 0.4, g({전

〈표 7〉 항목에 따른 부분집합

부분집합(E)의 수	항 목 번 호
1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
2	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
3	5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
4	1 2 3 4 9 10 11 12 13 14 15 16 17 18 19 20
5	1 2 3 4 5 6 7 8 13 14 15 16 17 18 19 20
6	1 2 3 4 5 6 7 8 9 10 11 12 17 18 19 20
7	1 2 3 4 5 6 7 8 9 10 11 12
8	1 2 3 4 5 6 7 8 13 14 15 16
9	1 2 3 4 5 6 7 8 17 18 19 20
10	1 2 3 4 9 10 11 12 13 14 15 16
11	1 2 3 4 13 14 15 16 17 18 19 20
12	5 6 7 8 9 10 11 12 13 14 15 16
13	5 6 7 8 9 10 11 12 17 18 19 20
14	5 6 7 8 13 14 15 16 17 18 19 20
15	9 10 11 12 13 14 15 16 17 18 19 20
16	1 2 3 4 5 6 7 8
17	1 2 3 4 9 10 11 12
18	1 2 3 4 13 14 15 16
19	1 2 3 4 17 18 19 20
20	5 6 7 8 9 10 11 12
21	5 6 7 8 13 14 15 16
22	5 6 7 8 17 18 19 20
23	9 10 11 12 13 14 15 16
24	9 10 11 12 17 18 19 20
25	13 14 15 16 17 18 19 20
26	1 2 3 4
27	5 6 7 8
28	9 10 11 12
29	13 14 15 16
30	17 18 19 20

〈표 8〉 등급별 문서에 따른 데이터

번호	대항목	소항목	메시지보안 프로토콜(h(x))			CMP(h(x))		
			1	2	3	1	2	3
1	보안기술	기밀성	1	1	1	1	1	1
2		무결성	1	1	1	1	1	1
3		송신부인봉쇄	1	1	1	1	1	1
4		수신부인봉쇄	1	1	1	1	1	1
5	보안정책	메세지 등급 세한	0	0	0	1	1	1
6		메세지 분류 커리	0	0	0	1	1	1
7		메세지 접근 등급	0	0	0	1	0.5	0
8		다중등급보안	1	1	1	0	0	0
9	전자문서관리	수신지확인서	1	1	1	1	1	0
10		전자서명	1	1	1	1	1	0
11		수신자키정보	1	1	1	1	1	0
12		암호화된 전자문서	1	1	1	1	0.5	0.1
13	전자문서전송	송수신자확인	1	1	1	1	1	0
14		내용 위·변조확인	1	1	1	1	0.5	0
15		송·수신시간확인	1	1	1	1	1	1
16		인증및 인증서확인	0	0	0	0	0	0
17	암·복호화키	RSA	1	1	1	0	0	0
18		KCDSA	0	0	0	1	1	1
19		DES	1	1	1	0	0	0
20		SEED	0	0	0	1	1	1

자문서관리}) = 0.35, g({전자문서전송}) = 0.15이다. 이때 예를 들어 g({보안기술, 보안정책})를 구하려고 하면, 여기에서의 퍼지척도 g(·)가 기법성을 만족하므로 g({보안기술}) + g({보안정책})에 의해 값이 0.5라는 것을 쉽게 알 수 있다. g({보안기술, 보안정책, 전자문서관리, 전자문서전송}) = 1, g({보안기술, 전자문서관리, 전자문서전송}) = 0.6, g({전자문서관리, 전자문서전송}) = 0.5. g({전자문서관리}) = 0.35와 같이 부분집합을 구성할 수 있다. 다음으로 입력 문서 A에 대한 프로토콜의 평가치는 h_A({보안정책}) = 0.7, h_A({보안기술}) = 0.8, h_A({전자문서전송}) = 0.85, h_A({전자문서관리}) = 0.95이다 라고 하면, 이상의 평가항목의 중요도 g와 문서에 대한 평가치 h_A를 이용하여 평가항목이 유한집합이므로 여러 항목에 대한 평가치인 퍼지적분에 의해 구할 수 있다

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

위 식에 의해 퍼지적분에 대한 결과를 다음과 같이 구할 수 있다. (Max = ∨, Min = ∧) (h_A({보안정책}) ∧ g({보안기술, 보안정책, 전자문서관리, 전자문서전송}) ∨ (h_A({보안기술}) ∧ g({보안기술, 전자문서관리, 전자문서전송}) ∨ (h_A({전자문서전송}) ∧ g({전자문서관리, 전자문서전송}) ∨ (h_A({전자문서관리}) ∧ g({전자문서관리}) = (0.7 ∧ 1) ∨ (0.8 ∧ 0.6) ∨ (0.85 ∧ 0.6) ∨ (0.95 ∧ 0.35) = 0.7 따라서 메시지보안 프로토콜의 평가치는 0.7이 된다. 반면에 CMP의 각 평가항목에 대한 평가치가 다음과 같다고 하자 h_B({보안기술}) = 0.6, h_B({보안정책}) = 0.85, h_B({전자문서전송}) = 0.8, h_B({전자문서관리}) = 0.9이다라고 하면 위에서와 같은 방법으로 결과를 구할 수 있다. (h_B({보안기술}) ∧ g({보안기술, 보안정책, 전자문서관리, 전자문서전송}) ∨ (h_B({전자문서전송}) ∧ g({보안정책, 전자문서관리, 전자문서전송}) ∨ (h_B({보안정책}) ∧ g({보안정책, 전자문서관리}) ∨ (h_B({전자문서관리}) ∧ g({전자문서관리}) = (0.6 ∧ 1) ∨ (0.8 ∧ 0.9) ∨ (0.85 ∨ 0.75) ∨ (0.9 ∧ 0.35) = 0.8로써 CMP의 평가치는 0.8이다 이 두 Sugeno의 퍼지적분의 결과로부터 CMP값이 메시지보안 프로토콜보다 속도면에서 다소 빠른 차이가 있다고 할 수 있다.

<표 9>에서 5가지 영역은 점수 환산에 의한 부분집합으로 분류하여 메시지보안 프로토콜과 CMP를 비교하기 위한 보안 급수로 나뉘어 적분한 값을 말한다. 위 내용에 의거하여 메시지보안 프로토콜과 CMP를 등급별로 비교하여 보았다.

<표 9> 메시지보안 프로토콜과 CMP의 결과비교

영역	보안급수	메시지보안 프로토콜	CMP	비고
I	1급	0.200130	0.386390	
	2급	0.200130	0.386390	
	3급	0.200130	0.186260	
II	1급	0.200130	0.386390	
	2급	0.200130	0.386390	
	3급	0.186260	0.200130	
III	1급	0.200130	0.200130	
	2급	0.200130	0.200130	
	3급	0.186260	0.200130	
IV	1급	0.200130	0.200130	
	2급	0.200130	0.200130	
	3급	0.186260	0.200130	
V	1급	0.200130	0.386390	
	2급	0.200130	0.386390	
	3급	0.000000	0.200130	

4. 결 론

본 논문에서는 미국의 메시지보안 프로토콜의 메시지 처리환경을 보완하고, 다중 등급 보안을 토대로 이를 우리나라의 시스템환경에 적합하도록 CMP를 개발하였다 이를 사용하여 각각의 문서에 차등을 적용하여 합리적인 방법으로 메시지를 처리하도록 하였다 또한, 메시지보안프로토콜과 CMP의 프로토콜의 검증을 위하여 퍼지적분을 이용하여 수행하였다.

퍼지적분을 사용하여 메시지보안프로토콜과 CMP의 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 CMP의 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.

부 록

일반적으로 어느 원소가 여러 개의 집합중에 임의의 집합에 속할 가능성을 퍼지척도를 사용하여 계량화하고 있다. 이러한 퍼지척도는 다음과 같은 성질에 따라

서 각각의 부분집합들이 [0, 1] 사이의 값을 가진다

1) $g(\varnothing)=0$이고, $g(X)=1$이다. 여기서 $\varnothing$는 공집합이고, X는 전체집합이다.
2) $E \subset F$라면 $g(E) \subset g(F)$이다
3) $E_1 \subset E_2 \subset \cdots$이거나 $E_1 \supset E_2 \supset \cdots$라면 $\lim n \to \infty\ g(E_n) = g(\lim\ n \to \infty\ E_n)$이다.

퍼지척도에 대해 1)은 경계조건이고, 2)는 단조성과 3)은 연속성을 나타낸다. 이러한 퍼지척도를 바탕으로 집합 X를 어떤 대상에 대한 평가 항목이라 하자. X의 멱집합(power set)의 원소 $E \in P(X)$에 대해 정의되는 퍼지척도 g(E)는 대상의 전체적인 평가에 대해 항목 E의 평가치가 기여하는 정도, 즉 평가항목의 부분집합 E의 중요도(degree of importance)라고 하고 그리고 X를 정의구역으로 하여 정의되는 함수 $h_{(X)}$, $x \in X$는 평가항목 x에 대한 평가치라고 할 경우에, 임의의 보통집합 X에 대하여 퍼지척도 $g : P(X) \to [0, 1]$가 정의되어 있고, X를 정의구역으로 하고 구간 [0, 1]을 치역으로 하는 함수 $h : X \to [0, 1]$가 정의되어 있다고 하자.

$$\int_X h(x) \circ g(\cdot) = \underset{E \subset X}{Sup}\ Min[\ \underset{x \in E}{Min}\ h(x),\ g(E)]$$

이때 $A(A \subseteq X)$에서의 함수 h의 퍼지척도 g에 대한 수게노의 퍼지적분은 위와 같이 정의된다.

참 고 문 헌

[1] 김현수, 정보시스템 진단과 감리, 법영사, p.3, 1999
[2] 정보보호센터, 정보보호뉴스 22호, 한국정보보호센타, p.2, 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)", pp.70-77, 1997.
[9] 한국전자통신 연구원, "인터넷 상거래의 물결", 한국전자통신 연구원, pp.128-129, 1998.
[10] http : //www.kisa.or kr/pds/att/missi hwp
[11] http : //www.imc.org/workshop/sdn701 txt 1994.
[12] Capuon 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

신 승 중

e-mail expersin@joongbu.ac.kr
1984년 한성대학교 경영학과졸업(학사)
1982년 세종대학교 경영학과(경영학석사)
1985년 건국대학교 산업대학원 전자계산학과(공학석사)
2000년 국민대학교 대학원 정보관리학과 보안관리응용(경영학박사)
1995년~현재 중부대학교 정보공학부 컴퓨터안전관리학과 조교수
관심분야 네트워크 장애관리, 보안감리, 정보보호 및 메시지 전송

박 인 규

e-mail : ikpark@joongbu.ac.kr
1985년 원광대학교 전기공학과 졸업(공학사)
1987년 연세대학교 대학원 전기공학과 전자계산기응용(공학석사)
1996년 원광대학교 대학원 전자공학과 마이크로프로세서응용(공학박사)
1997년~현재 중부대학교 정보공학부 전자계산학과 조교수
관심분야 퍼지논리, 신경회로망, 최적화이론