공개정보를 응용한 메시지 보안 시스템의 인증 프로토콜 설계 및 검증

(Design and Verification of Applied Public Information Based Authentication Protocol in the Message Security System)

김영수*, 신승중**, 최흥식***
(Young Soo Kim, Seung Jung Shin, Heung Sik Choi)

요 약 전자상거래는 개인과 개인, 기업과 기업, 개인과 기업 상호간에 메시지의 교환을 통해서 이루어진다. 전자상거래를 활성화 할 수 있는 가장 중요한 요소는 메시지 인증으로서, 이는 거래당사자들이 수신된 메시지의 진정성을 확인하는 과정이다. 메시지의 진정성은 위조불가, 부인불가, 변경불가, 출처인증으로 구성되어 있고, 공개키 암호화를 통해 수행 할 수 있다. X.400 메시지처리 시스템과 공개키 암호화에 기반을 두고 있는 PGP가 메시지 교환에 널리 사용되고 있다. 본 논문에서는 공개키 암호화와 X.400 프로토콜 그리고 PGP상에 존재하는 메시지 인증 문제를 해결하기 위하여 NMAP로 명명된 공개정보 기반 암호화 시스템을 제안하고 이를 설계 구현하였다. 구현된 메시지 인증 프로토콜의 검증을 위해 퍼지적분을 사용하였다. 제안된 시스템은 전자상거래의 활성화와 비대화형 인증 서비스 제공에 사용될 수 있을 것이다.

Abstract E-Commerce, characterized by the exchange of message, occurs between individuals, organizations, or both. A critical promotion factor of e-Commerce is message authentication, the procedure that allows communicating parties to verify the received messages are authentic. It consists of message unforgery, message non-repudiation, message unalteration, and origin authentication. It is possible to perform message authentication by the use of public key encryption. PGP(Pretty Good Privacy) based on X.400 MHS(Message Handling System) and PKC(Public Key Cryptosystem) makes extensive use of message exchange. In this paper we propose, design and implement NMAP(New Message Authentication Protocol), an applied public information based encryption system to solve the message authentication problem inherent in public key encryption such as X.400 protocol and PGP protocol and were to cope with the verification of NMAP using fuzzy integral. This system is expected to be use in the promotion of the e-Commerce and can perform a non-interactive authentication service.

1. 서 론

인터넷에 대한 사용자수가 급속히 증가하면서 인터넷을 이용한 전자상거래가 확대되고 있다. 인터넷을 이용한 전자상거래는 상대방과 직접 대면할 수 없는 가상 공간이라는 특성으로 상거래 상대자의 신원을 확인하거나 거래내용에 대한 진정성을 보장하기 어렵게 된다.

따라서, 전자상거래에서의 메시지 수신자는 그 메시지가 송신자를 사칭하는 사람이 아닌 실제 송신자한

* 국민대학교 대학원 정보관리학과 박사수료
** 한세대학교 컴퓨터공학과 부교수
*** 국민대학교 정보관리학부 부교수

테서 그 메시지가 송신되었다는 것과 수신한 메시지는 전송도중 변경되지 않았다는 것을 확인 할 수 있어야 하고 사후에 메시지 송신자가 메시지의 송신 자체를 부인하는 것을 방지 할 수 있어야 한다.

전자상거래를 활성화 할 수 있는 가장 중요한 요소는 거래 메시지의 출처 확인과 거래메시지의 위·변조 그리고 거래 메시지의 부인을 방지하기 위한 효율적인 메시지 인증 메카니즘에 달려있다.

메시지 인증 방법으로는 암호방식에 기초를 둔 인증 프로토콜이 많이 사용되는데[1] 공개키와 개인키라는 두 개의 키를 사용하는 공개키 암호화 방식에 의한 전자서명 값의 생성을 통한 메시지 인증 방식이 널리 사용된다.

그러나 공개키 암호화 제품의 가장 큰 문제점은 사용의 복잡성과 메시지 전송의 제한 그리고 키 관리의 어려움으로 사용자가 사용을 꺼리고 외면한다는 점이다.

이와 같은 문제점을 해결하고 메시지에 보안성을 제공할 수 있는 새로운 메시지 인증 프로토콜의 개발 및 구현을 목표로 메시지 처리 시스템의 표준안인 X.400과 공개키 암호화 기반 전자우편 시스템인 PGP 그리고 공개키 암호화 방식에 의한 메시지 인증 프로토콜을 분석하여 문제점을 개선 할 수 있는 방안를 제안하고 이를 설계·구현하였다.

또한 성능분석을 위해 다양한 크기의 메시지와 키를 사용해 인증 메시지를 구성하는데 소요되는 시간을 측정하는 모의실험을 행하였고 수게노의 퍼지적분을 적용하여 프로토콜 검증을 수행하였다.

본 논문의 구성은 다음과 같다. 제 2절에서는 메시지 보안 시스템의 문제점과 개선방안을 제시하고 제 3절에서는 NMAP로 명명된 새로운 메시지 인증 프로토콜의 설계와 성능 분석을 살펴보고 제 4절에서는 NMAP의 프로토콜 검증을 보이며 제 5절에서는 결론 및 요약과 함께 주요한 시사점을 논의한다.

2. 메시지 보안 시스템의 분석 및 개선 방안

X.400에서는 저장후 전송 방식과 메시지 토큰 구성시 암호화 후 서명 방식을 권고[2] 하고 있는데 메시지 중계노드에서의 호환성을 위한 무결성의 훼손 가능성과 특정 보안 서비스 제공을 위한 개인키의 공유로 인한 비밀키의 노출 가능성 그리고 토근 암호문의 위조를 통한 서명의 진위에 대한 논쟁의 가능성이 존재한다[3].

또한 인증서 기반 공개키 암호화 방식의 경우 인증서를 위한 처리시간과 기억장소가 많이 소요되고 인증기관으로부터 공개키 인증서를 발급받지 못한 사용자에게는 메시지를 전송 할 수 없다는 한계가 있다.

그리고 PGP는 공개키와 개인키의 효율적인 관리를 위해 공개키와 개인키 링을 구축하여 키를 관리 하는데 동일한 사용자가 단일 공개키와 관련된 다수 ID가 존재 할 수 있고, 다수 공개키가 배포 될 수 있으므로 공개키 관리가 매우 복잡하다[4].

표 1. 메시지보안시스템의 비교

구 분	P G P	제안시스템(NMAP)
메시지 처리시간	다소 느림	다소 빠름
전송 대상	공개키 소유자	불특정 다수
사용자 식별	공개키	식별자
키 생성	개인키로 공개키 생성	공개키로 개인키 생성
암호화 방식	세션키 사용	비밀키 사용
토큰 구성	암호화후 서명방식	암호화후 서명방식
전송 방식	저장후 전송	직접 전송
배달증명 계산	평문대상	암호문대상
키 링	구축 필요	구축 불필요
인증서	필요	불필요
내용 기밀성	IDEA, RSA	DES, RSA
내용 무결성	MD5, RSA	MD5, RSA
발신처 인증	서명후 암호화방식	암호화후 서명방식
발신처 부인봉쇄	서명후 암호화방식	암호화후 서명방식
배달 부인봉쇄	서명후 암호화방식	암호화후 서명방식

따라서 새로운 인증 프로토콜에는 아래과 같은 사항을 고려하여 표 1과 같은 분석 결과를 제안 시스템에 반영하였다. 첫째 메시지가 저장후 전송되는 방식을 탈피하여 직접 전송될수 있도록 해야 한다. 둘째 인증 메시지 구성 및 처리로 인한 오버헤드를 감소시켜야 한다. 셋째 사용자의 공개된 정보만을 이용하여 암호화 메시지를 구성할 수 있도록 해야 한다.

3. NMAP의 설계 및 성능 분석

3.1 NMAP의 개요

메시지의 출처 확인과 메시지의 위·변조 그리고 메시지의 부인을 방지하기 위한 효율적인 메시지 인증의 구현을 위해 Denning과 Sacco가 제시한 공개키 암호화 시스템[5]과 메시지 시스템의 표준안인

CCITT의 X.400[6] 그리고 메시지 보안 시스템인 PGP[7]를 분석하여 도출된 문제점을 개선하고 개인 사업자나 중소기업에 적합한 메시지 인증 프로토콜을 설계하여 이를 NMAP(New Message Authentication Protocol)로 명명하였다.

NMAP는 공개되어 있는 정보만을 이용하여 암호화 메시지를 구성하여 불특정 다수에게 메시지를 안전하게 전송할수 있는 실체 기반 암호화 프로토콜[8][9]로 메시지에 부가되어 보안성을 제공해주는 인증 헤더의 설계를 중점적으로 연구하였고 그림 1과 같이 OSI의 보안 아키텍쳐와 X.411[10]에서 요구하고 있는 기밀성, 메시지 출처확인, 무결성, 송수신 부인봉쇄, 배달증명 서비스를 제공한다[11].

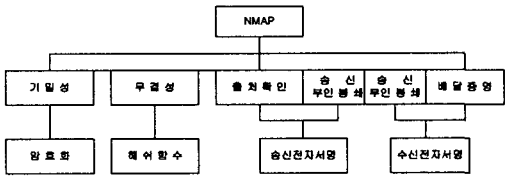


그림 1. NMAP의 기본 구조

3.2 NMAP 인증 구조

인증이란 실체인증과 메시지인증으로 구분되는데 통신의 당사자간의 연결이 확립되는 동안 이루어지는 실체 인증에 대한 연구는 활발하게 이루어지고 있으나 비대화형 메시지 인증에 대한 연구는 미진한 실정이다. 연구 개발한 NMAP는 신뢰된 제삼자를 포함하지 않는 메시지 인증 구조를 다루고 있다.

메시지 인증이란 메시지를 교환하는 당사자들이 수신된 메시지의 진정성을 확인하는 과정이다. 메시지의 진정성은 위조불가, 부인불가, 변경불가, 출처인증으로 구성되어 있고 공개키 암호화 방식을 통해 수행 할 수 있다[1].

메시지 인증을 위해 NMAP는 그림 2와 같이 인증 관련 파라미터들을 메시지 헤더 부분에 위치시키고 디지털 서명된 데이터 구조를 정의하여 각종 보안 관련 파라미터들을 이 구조 속에 위치시킴으로써 인증을 실현하고 있다.

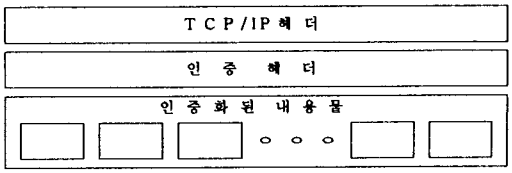


그림 2. NMAP 인증 캡슐 구조

프로토콜 구현 방법으로는 인증헤더와 메시지를 결합해서 전송하는 방식과 인증헤더를 먼저 보내고 승인을 기다린후 메시지를 보내는 방법 그리고 헤더를 구성하는 파라미터를 한번에 하나씩 보내 긍정의 응답을 받아 처리하는 방식이 있다[12]. NMAP에서는 개인사업자나 중소기업의 메시지 전송 환경을 고려하여 핸드쉐이킹에 의한 오버헤드를 최소화하도록 인증헤더와 메시지를 결합해서 일괄 전송하는 방식을 채택하였다.

공개키 암호화와 전자서명을 결합해서 수행하는 디지털 서명 방식으로는 암호화와 서명(Encrypt-and-Sign) 방식과 암호화후 서명(Encrypt-then-Sign) 방식 그리고 서명후 암호화(Sign-then-Encrypt)방식이 있다[13].

암호화와 서명 방식은 전자서명에 대한 기밀성을 제공하기 위한 추가 암호화에 대한 오버헤드가 요구되고 암호화후 서명 방식은 암호문에 의한 전자서명의 검증으로 위조된 암호문에 의해 생성된 전자서명의 유효성에 대한 논쟁의 가능성이 있고 서명후 암호화 방식은 복호화키 소유자만이 서명을 검증할수 있기 때문에 제삼자에 의해 전자서명이 공증될수 없다는 약점이 있다.

NMAP는 서명후 암호화방식을 적용하였고 향후 인증서를 기반으로 전자서명의 공증 서비스를 제공할 수 있도록 설계하였다. 반면 PGP는 X.400의 권고사항인 암호화후 서명방식을 적용하고 있다.

3.3 NMAP 설계

프로토콜의 기본 구조는 그림 3과 같이 송신자가 문자열 형태의 식별자를 사용하여 메시지를 암호화하여 수신자에게 직접 전송하고 수신자는 키분배센타로부터 KDC(Key Distribution Center)의 비밀정보와 식별자로 계산된 개인키를 발급받아 메시지를 복원하게 된다.

PGP는 저장후 전송 방식에 의해 메시지를 전달하고 공개키를 소유하고 있는 수신자에 한해서 암호화된 메시지를 전달할 수 있다.

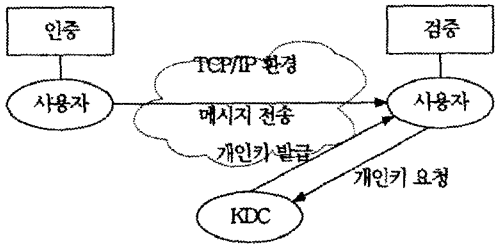


그림 3. NMAP 개념도

NMAP의 서비스 유형을 기밀성, 무결성, 전자서명, 부인봉쇄로 분류 설계하여 사용자가 서비스 유형을 선택적으로 사용하도록 하였다. 그림 4는 서비스에 따라 수행되는 보안성 구조를 표시하고 있는데 마름모 형태는 서비스의 유형를 표시하고 원은 서비스의 범위를 나타내고 있다. 서비스 기능 구현시 원의 내부에서 외부 순으로 수행되고 처리하는 대상을 표현하고 있다.

송신자가 기밀성 서비스를 요청하면 메시지를 비밀키로 암호화하고 무결성 서비스를 요청하면 메시지와 토근의 해쉬코드를 계산하여 토큰 형성 후 공개키로 암호화하여 전송한다.

또한 전자서명 서비스를 선택하면 토근의 해쉬값에 대해 전자서명값을 계산하고 배달증명을 요청하면 배달증명을 위해 수신자는 배달증명값을 산출하여 무결성처리와 서명처리를 수행한 후 상대방에게 전송할 때는 공개키로 암호화하여 전송한다.

인증 서비스를 제공하기 위한 해쉬 계산 과정은 그림 5와 같고 해쉬에 대해 일련의 연속적인 계산을 수행하여 인증 서비스를 제공한다.

PGP의 경우에는 인증헤더를 구성하는 파라미터에 대해 해쉬를 분리하여 별도로 산출하는 반면 NMAP에서는 수반되는 인증 서비스를 반복 처리하도록 해쉬를 시퀀스하여 단순화하고 있다.

토큰이라는 서명된 데이터 구조를 그림 6과 같이 정의하고 각종 보안 관련 파라미터들을 위치시켜 전달함으로서 보안 서비스를 실현한다. PGP는 배달증명을 위한 별도의 파라미터를 포함하고 있으나 NMAP에서는 서비스 유형으로 이를 대체하고 수신자 측에서 이를 구성하도록 하여 구조를 단순화하였다.

토근 처리 절차의 수행은 그림 7과 같고 서비스의 유형에 따라 처리되는 토근의 내용이 다르다 . 비밀키는 난수 생성기에 의해 생성되고 공개키에 대응되는 개인키 파라미터는 솟수 생성기에 의해 생성되어 토근에 부착하도록 설계하였다.

또한 토근에 대한 해쉬코드를 생성하여 부착 후 수신자의 공개키로 암호화하여 전송하면 수신자는 개인키로 복호화한 후 토근의 서비스 유형에 따라 처리하도록 설계하였다.

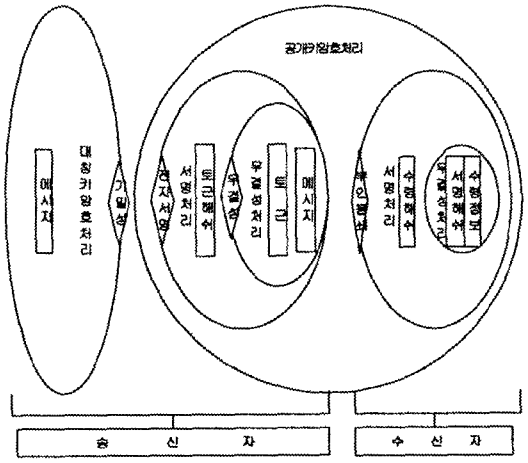


그림 4. NMAP 서비스 구조

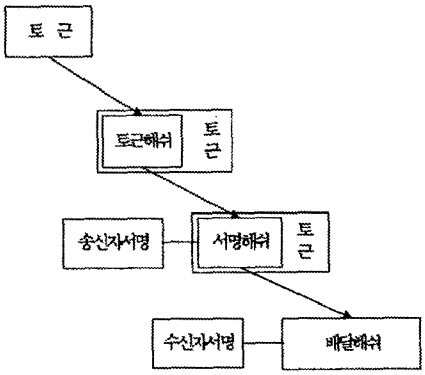


그림 5. NMAP 해쉬 시컨스

토 근												
식별정보			서비스	공개정보				키정보	세션정보	해쉬시퀀스		
송신자식별자	수신자식별자	송신시각	서비스유형	공개키암호알고리즘확인자	비밀키알고리즘확인자	해쉬알고리즘확인자	알고리즘모드	암호화초기값	비밀키	토큰해쉬값	무결성해쉬값	전자서명값

그림 6. NMAP 토근 구조 설계

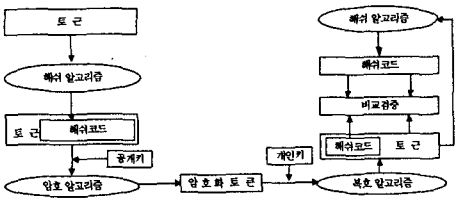


그림 7. NMAP 토큰 처리 설계

키 생성 방식은 PGP와는 달리 그림 8과 같이 복호화시점에서 공개키로부터 개인키를 생성한다. PGP는 키 생성 알고리즘을 통해 개인키를 생성하고 이를 기반으로 공개키를 생성한다. 따라서 암호화 메시지를 작성하기 이전에 공개키와 개인키가 생성됨으로 개인키의 분실과 노출의 방지를 위해 많은 노력을 기울여야 한다.

기밀성을 제공하기 위한 암복호화 과정은 그림 9와 같다. 송신자는 길이가 긴 메시지를 난수로 만들어진 비밀키를 사용하여 암호화하고 토근의 인증 파라미터에 대해서는 해쉬 시퀀스를 공개키로 암호화하여 기밀성을 제공한다. 복호화과정은 메시지 판독 시점에서 개인 키를 생성하여 메시지를 복호화하도록 설계하였다. PGP는 암호화를 위해 압축과정을 수행한다.

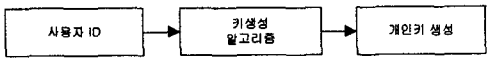


그림 8. NMAP 키 생성 설계

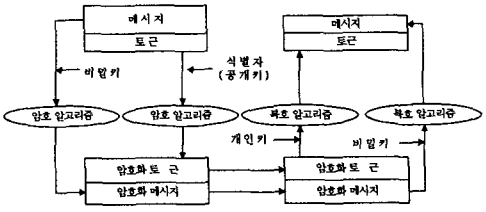


그림 9. NMAP 암·복호화 처리 설계

무결성 처리 과정은 메시지의 내용이 전송 중에 변경되지 않았음을 검증하는 절차로 그림 10과 같이 수행되고 메시지 다이제스트라고 하는 고정된 크기의 해쉬 코드를 계산하여 메시지에 부착하여 암호화 후 전송한다.

수신자는 그 역으로 수행하여 검증한다. PGP는 각각의 인증 서비스를 위해 독립적인 해쉬값을 계산하나 NMAP는 해쉬 시퀀스를 통해 이를 실현하고 있다.

전자서명 서비스의 수행 과정은 그림 11과 같이 토근해쉬를 개인키로 전자서명하고 수신자의 공개키를 사용하여 암호화하여 기밀성을 제공하도록 하였다. PGP는 토근을 구성하는 서명정보에 대한 해쉬값을 개인키로 전자서명화하여 전송하여 개별적으로 처리하고 있어 프로토콜이 복잡하다.

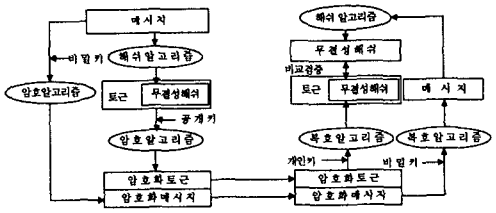


그림 10. NMAP 무결성 처리 설계

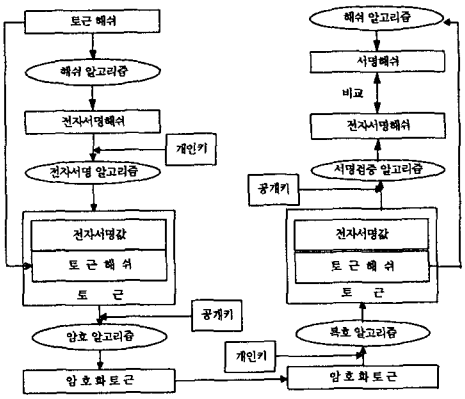


그림 11. NMAP 전자서명 처리 설계

메시지가 실제로 수신자에 의해 수신되었음을 부정할수 없게 하는 배달증명 프로토콜의 구현 과정은 그림 12와 같고 송신자가 메시지를 전달할 때 배달증명 서비스를 요청하고 수신자는 수신된 메시지를 읽을 때 배달 증명 값을 계산한 후 수령증을 송부하여 송신자가 송부된 수령증을 확인하도록 설계하였다.

PGP는 배달증명을 계산하기 위하여 평문으로 복호화하기 때문에 개인키를 시스템이 알고 있어야 하고 이는 시스템 관리자에게 개인키가 노출될 수 있는 가능성을 제공한다.

반면 NMAP는 개인키로 전자서명을 검증한 후 서명해쉬에 대해 배달증명을 계산해 전달하도록 함으로써 개인키의 노출을 최소화 하도록 하였다.

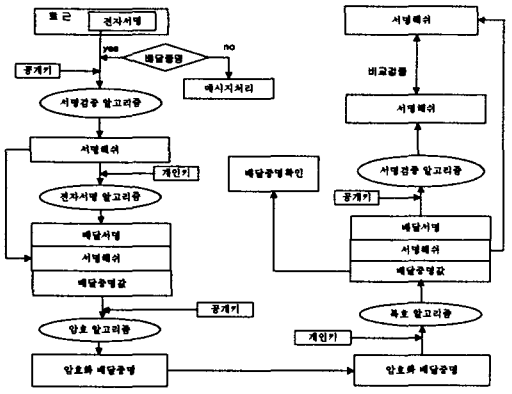


그림 12. NMAP 배달증명 처리설계

NMAP는 암호방식에 기초를 둔 인증 프로토콜로 그림 13과 같이 암호화 시스템을 통하여 전송할 메시지를 구성한다.

기밀성을 제공하기 위하여 메시지를 암호화하면 무결성이 부산물로 제공되는데 이는 암호화된 메시지가 도중에 수정이 되면 해독이 불가능하기 때문이다.

그러나 NMAP에서는 해쉬 알고리즘을 적용하여 무결성을 분리 수행하고 메시지 무결성에 대한 제어를 유연하게 할수 있도록 하였다.

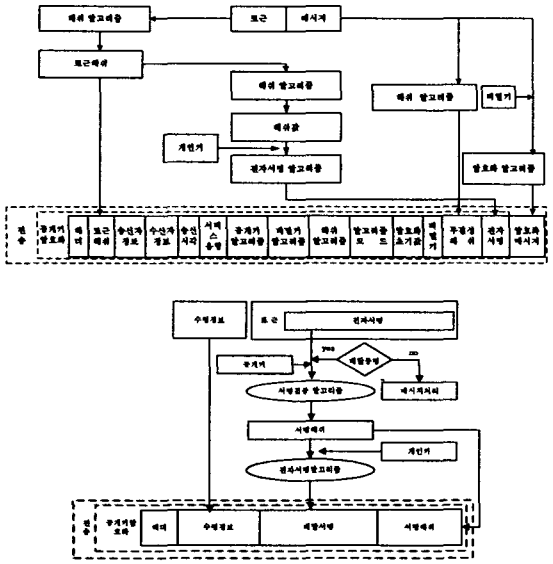


그림 13. NMAP 프로토콜 설계

3.4 NMAP 성능 분석

모의실험 환경으로 셀러론 850MHz와 윈도우즈 2000운영체제 하에서 메시지의 크기와 키의 길이를 상이하게 하여 인증 메시지를 구성하는데 소요되는 시간을 측정하여 실험하였다.

표 2에서 보는 것과 같이 공개키 암호화 방식을 사용한 PGP 보다는 문자열형태의 공개키와 비밀키를 이용하여 인증 메시지를 구성하는 NMAP의 암호화 속도가 다소 빠르다는 것을 알 수 있다.

표 2. 인증메시지 제출 시간 테이블 (단위 : 초)

구분	PGP			NMAP			PGP-NMAP
	512	1024	2048	512	1024	2048	
100K	0.4358	1.0338	2.8418	0.42	1.018	2.826	0.0158
200K	0.8718	2.0678	5.6858	0.838	2.034	5.652	0.0338
300K	1.3078	3.1018	8.5298	1.258	3.052	8.48	0.0498
400K	1.7436	4.1356	11.3736	1.676	4.068	11.306	0.0676
500K	2.1796	5.1696	14.2176	2.096	5.086	14.134	0.0836

4. NMAP의 프로토콜 검증

4.1 프로토콜 평가 모델

NMAP 프로토콜과 PGP 프로토콜의 비교우위를 검증하기 위하여 계층 퍼지적분을 사용하였다. 적용된 계층 퍼지적분은 어떤 대상이 여러 항목에 대해서 평가되고 각 평가항목의 중요도에 차이가 있을 때 이들에 대한 평가치를 종합하는데 유효[14]하다.

퍼지적분을 사용한 프로토콜 검증에 대한 기존 연구로는 퍼지계층 평가, 알고리즘의 개발과 그 적용에 관한 연구[15]와 퍼지적분을 이용한 메시지 프로토콜 검증[16] 그리고 퍼지집합을 이용한 데이터베이스 시스템의 품질평가에 관한 연구[17]등이 있다.

NMAP 프로토콜의 비교우위에 대한 검증을 위해 OSI 보안 아키텍처와 X.400 메시지 보안 서비스에서 정의하고 있는 보안항목을 평가항목으로 구성하였다. 이를 시스템적 관점에서 도식화하면 그림 14와 같이 표현된다.

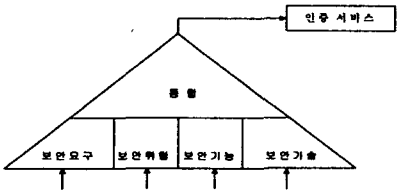


그림 14. 프로토콜 검증 개념도

메시지 인증의 목적은 메시지에 보안성을 제공하는 것이다. 메시지 보안성은 보안요구, 보안위협, 보안기능, 보안기술의 네가지 면을 고려해야 한다 [11]. 그림 15는 평가항목별 세부 평가항목을 보여주고 있다.

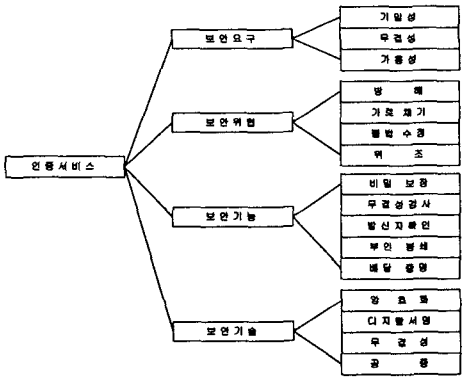


그림 15. 평가항목 계층구조

계층 퍼지적분은 복잡한 문제의 계층화로부터 평가항목에 의한 평가대상의 평가치를 구하여 이와 함께 퍼지 적분을 각 계층에서 기본적으로 한다. 그리고 이들을 각 계층간에 통합하게 되며 이 통합은 전계층을 통하여 하게 된다.

인간이 행하는 주관적 평가에는 애매모호함이 수반되기 때문에 그 애매모호함에 대처한 분석법이 필요하다. 퍼지측도는 모호한 대상을 평가할 때 사용되는 주관적 측도라고 해석된다. 쯔까모또의 퍼지측도[18]와 수게노의 퍼지적분[14]을 사용하여 비교우위를 검증하였다.

4.2 퍼지적분 평가 알고리즘

평가 대상 문제가 여러개의 항목으로 구성된 계층구조로 주어져 있을 경우에 계층 퍼지적분 알고리즘은 그림 16과 같다.

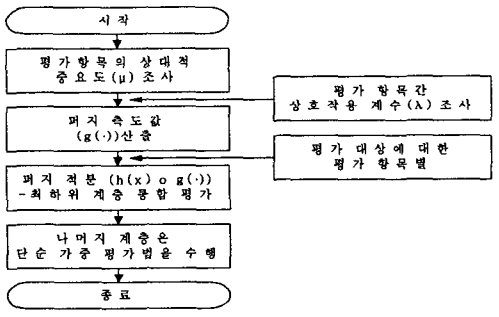


그림 16. 퍼지적분 평가 알고리즘

4.3 설문통계 분석

메시지 인증 프로토콜의 보안성을 항목별로 분류하여 보안관련업체 및 소프트웨어 개발업체 종사자를 대상으로 설문조사를 수행하였고 표 3과 표 4에 설문지의 조사개요와 통계 분석결과를 정리하였다.

표 3. 조사 개요

조사대상	보안관련업체 및 소프트웨어 개발업체 종사자
조사방법	전화통화후 이메일을 통한 방법
조사기간	2003. 1. 4 ~ 2003. 1. 20.
설문회수율	80%

표 4. 설문 통계

번호	대항목	소항목	평균값
1	보안요구	기밀성	2.5
2		무결성	4.5
3		가용성	3.0
4	보안위협	방해	1.5
5		가로채기	1.7
6		불법수정	4.5
7		위조	3.0
8	보안기능	비밀보장	3.0
9		무결성 검사	4.8
10		발신자확인	4.3
11		부인봉쇄	4.5
12		배달증명	3.7
13	보안기술	암호화	3.1
14		디지탈서명	4.8
15		무결성	4.4
16		공증	3.7

4.4 평가항목 중요도 결정

평가항목의 중요도(μ)는 점수산정 모형을 사용하여 통계표상의 점수합계에 대한 상대적인 비율로 결정하였다. 그리고 상호작용계수(λ)는 항목간에 독립성을 가정하여 λ=0을 사용하였다.

이는 메시지 인증 프로토콜의 보안성을 여러 측면에서 평가·검증하기 위해서이다. 산출된 평가항목의 중요도는 표 5와 같다.

표 5. 평가항목의 중요도

번호	대항목	소항목	중요도
1	보안요구	기밀성	0.044
2		무결성	0.079
3		가용성	0.053
4	보안위협	방해	0.026
5		가로채기	0.030
6		불법수정	0.079
7		위조	0.053
8	보안기능	비밀보장	0.053
9		무결성 검사	0.084
10		발신자확인	0.075
11		부인봉쇄	0.079
12		배달증명	0.065
13	보안기술	암호화	0.054
14		디지탈서명	0.084
15		무결성	0.077
16		공증	0.065

4.5 평가항목의 퍼지측도값

수게노가 제안한 퍼지측도(g(·))는 계산과정이 복잡하기 때문에 최근 연구에서 계산방법을 간단하게 해주는 쯔카모토가 제안한 퍼지측도를 사용하였다.

$$g(\cdot)=\begin{cases}(1+\lambda)^{u}-1)/\lambda & \text{if} \quad \lambda\neq 0\\ u & \text{if} \quad \lambda=0\end{cases}$$

특히 표 6과 같이 평가항목에 대한 부분집합을 13개의 부분집합으로 구성하여 평균에 의해 평가치 g(·)를 산출하였다.

이러한 부분집합이 가지는 의미는 일단 대상에 대한 평가의 각도를 전체적인 면에서가 아닌 부분들에 대한 평가치들로 고려한 다음에 이러한 모든 부분집합들에 대한 평가치들을 적분하여 최종적인 평가를 위해서이다.

표 6. 평가항목 부분집합

부분집합수	항 목 번 호	g(·)
1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	0.0625
2	1 2 3 4 5 6 7 8 9 10 11 12	0.0599
3	1 2 3 4 5 6 7 13 14 15 16	0.0585
4	4 5 6 7 8 9 10 11 12 13 14 15 16	0.0635
5	1 2 3 4 5 6 7	0.0519
6	1 2 3 8 9 10 11 12	0.0665
7	1 2 3 13 14 15 16	0.0574
8	4 5 6 7 8 9 10 11 12	0.0604
9	4 5 6 7 13 14 15 16	0.0585
10	1 2 3	0.0583
11	4 5 6 7	0.047
12	8 9 10 11 12	0.0712
13	13 14 15 16	0.0703

4.6 부분집합 평가치

평가항목별 평가치는 PGP와 NMAP의 구현 비교표를 대상으로 보안 전문가 그룹에 의해 수행되었다. 평가기준은 먼저 구현항목에 따라 평가항목을 선정하고 구현내용에 따라 앞서 구한 측도치를 고려하여 상대적 점수를 부여하여 평균 평가치를 산출하였다.

PGP와 NMAP의 구현 항목의 비교는 표 7과 같고 항목 평가치는 표 8에 표시하였다. 각 항목 평가치를 입력치로 하여 평균에 의한 부분집합의 평가치 h(·)를 표 9와 같이 구하였다.

표 7. PGP와 NMAP 구현 비교

구분	PGP	NMAP
메시지처리시간	상대적 느림	상대적 빠름
전송대상	공개키 소유자	불특정 다수
사용자 식별	공개키	사용자 ID
키 생성	개인키로 공개키 생성	공개키로 개인키 생성
암호화 방식	세션키 사용	비밀키 사용
토큰 구성	서명후 암호화방식	암호화후 서명방식
전송 방식	저장후 전송	직접 전송
배달증명 계산	평문대상	암호문대상
키 링	구축 필요	구축 불필요
인증서	필요	불필요
내용 기밀성	IDEA, RSA	DES, RSA
내용 무결성	MD5, RSA	MD5, RSA
발신처 인증	서명후 암호화방식	암호화후 서명방식
발신처부인봉쇄	서명후 암호화방식	암호화후 서명방식
배달부인봉쇄	서명후 암호화방식	암호화후 서명방식

표 8. PGP와 NMAP 평가치

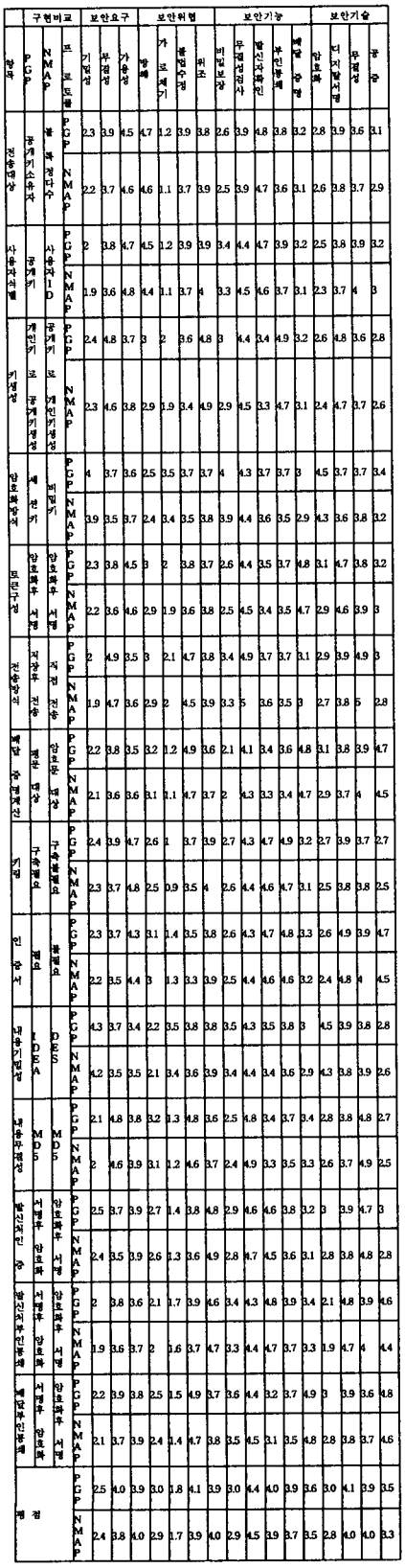


표 9. 부분집합 평가치

부분 집합수	항 목 번 호	h(·)	
		PGP	NMAP
1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	0.063	0.063
2	1 2 3 4 5 6 7 8 9 10 11 12	0.062	0.062
3	1 2 3 4 5 6 7 13 14 15 16	0.061	0.060
4	4 5 6 7 8 9 10 11 12 13 14 15 16	0.063	0.063
5	1 2 3 4 5 6 7	0.059	0.059
6	1 2 3 8 9 10 11 12	0.065	0.065
7	1 2 3 13 14 15 16	0.063	0.063
8	4 5 6 7 8 9 10 11 12	0.0622	0.0623
9	4 5 6 7 13 14 15 16	0.0603	0.0601
10	1 2 3	0.0612	0.0615
11	4 5 6 7	0.0565	0.0565
12	8 9 10 11 12	0.0668	0.0669
13	13 14 15 16	0.064	0.0637

구현 비교표에 의한 프로토콜의 평가항목별 평점을 비교하면 거의 대동소이하게 나타나고 있다. NMAP가 가용성과 위조방지, 무결성 검사, 무결성 메커니즘에서 약간 우세하게 점수가 할당되어 있음을 확인할수 있다.

4.7 퍼지 적분치

수게노가 제안한 퍼지적분을 사용하여 평가항목에 대한 퍼지적분을 구하여 인증 프로토콜의 비교우위 검증을 수행하였다. 수게노의 퍼지적분은 수학에서의 적분과는 성격이 다른 것으로 어떤 대상을 여러 항목(관점)에 대해서 평가할 때 이들 각 항목에 대한 평가치를 퍼지척도를 사용하여 종합하는 방법으로 사용된다. 특히 이 퍼지적분은 주관적인 판단이 개입되는 평가 문제에서 유용하게 사용될수 있다. 수게노의 퍼지적분은 다음과 같이 정의되고 3단계로 나누어 해석해 볼 수 있다.

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

1 단계 : $\underset{x\in E}{Min}\ h(x), g(E)$는 평가항목의 부분집합 E에 대해서 가장 부정적인(보수적인) 평가치를 선택한다.

2 단계 : $Min[\ \underset{x\in E}{Min}\ h(x), g(E)]$는 평가항목 중 가장 부정적인 평가치와 평가항목 E의 중요도 중에서 작은 것을 선택하는 것이다. 이렇게 선택하는 바탕에는 평가치들 중에서 가장 작은 것을 선택함으로써 가장 안전한(보수적인) 평가치를 가짐과 동시에 이 평가치가 평가항목의 중요도보다 클 수 없다는 것을 뜻한다.

3단계: $\underset{E\subseteq X}{Sup}\ Min[\ \underset{x\in E}{Min}\ h(x), g(E)]$로 적분결과를 수행함으로써 여러 가지 가능한 E중에서 가장 큰 값을 취하여 전체 평가치를 종합하고 있다. 즉 이 부분에서는 긍정적인(유리한) 항목을 부각시켜 낙관적인 평가를 하는 측면이 있다.

계층 퍼지적분은 복잡한 문제의 계층화로부터 평가항목에 의한 평가대상의 평가치를 구하여 이와 함께 퍼지 적분을 각 계층에서 기본적으로 한다. 그리고 이들을 각 계층간에 통합하게 되며 이 통합은 전계층을 통하여 하게 된다. 평가항목별 평가치 h(·)와 각 평가항목으로 이루어진 모든 부분집합들에 대한 퍼지 측도치 g(·)에 대한 자료를 이용한 수게노 퍼지적분 평가 알고리즘의 계산과정과 결과는 표 10과 같다.

표 10. 퍼지적분 결과

부분 집합수	측도치 g(·)	PGP h(·)	NMAP h(·)	PGP 평가치	NMAP 평가치
1	0.0625	0.063	0.063		
2	0.0599	0.062	0.062		
3	0.0585	0.061	0.060		
4	0.0635	0.063	0.063		
5	0.0519	0.059	0.059		
6	0.0665	0.065	0.065		
7	0.0574	0.063	0.063	0.0668	0.0669
8	0.0604	0.0622	0.0623		
9	0.0585	0.0603	0.0601		
10	0.0583	0.0612	0.0615		
11	0.047	0.0565	0.0565		
12	0.0712	0.0668	0.0669		
13	0.0703	0.064	0.0637		

PGP와 NMAP에 대한 함수 h의 퍼지척도 g에 대한 수게노의 퍼지적분값을 분석해 보면 점수 환산에 의한 부분집합으로 분류된 각각의 영역에서 PGP와 NMAP의 보안성 평가치가 거의 차이가 나지 않는다. 그러나 NMAP는 가용성이 높이 평가되어 있음을 확인할수 있고 사용의 편의성과 저렴한 구축 비용으로 메시지에 보안성을 요구하는 중소기업이나 개인 사업자의 메시지 보안시스템으로 적합하다는 것을 알 수 있다.

5. 결 론

NMAP 프로토콜은 공개되어 있는 정보만을 이용하여 암호화 메시지를 구성하여 불특정 다수에게 메시지를 안전하게 전송하고 복호화 시점에서 개인키를 생성 함으로써 키관리의 복잡성을 감소시켜 주는 암호화 시스템으로 기본적으로 문자열 형태의 사용자 식별자를 암호화키로 사용하고 디지털 서명을 비롯한 각종 공개키 암호시스템이 가지는 장점을 갖고 각종 보안 서비스를 사용자의 편의성을 고려하여 구현하고 있다.

개발 구현된 NMAP는 메시지 처리 시스템의 표준안인 X.411의 보안성 분석 결과 MTA(Message Transfer Agent)와 MS(Message Store)가 기능 수행시 수신자의 비밀키를 알고 있어야 하는 문제점이 파악되어 송신자가 발송한 메시지가 수신자에게 직접 전달되는 방식을 사용하였고 PGP의 분석 결과 공개키 관리와 프로토콜이 복잡하다는 문제점이 발견되어 복호화 시점에서 개인키를 생성하는 방식을 적용하였다.

또한 인증서 기반 공개키 암호화 방식의 경우 인증서의 처리 시간과 기억장소가 많이 소요되고 메시지 전송을 위해 복잡한 사전 작업이 필요하다. 무엇보다도 공개키 인증서를 갖지 못한 사용자에게는 메시지를 전송 할 수 없다는 문제점을 해결하기 위해 문자열 형태의 사용자 ID를 공개키로 사용하고 공개키와 개인키 그리고 비밀키를 사용하여 인증 메시지를 구성하도록 하였다.

NMAP의 기대 효과를 살펴보면 사용의 용이성 제공으로 공개키 기반 응용제품의 사용을 촉진하여 정보범죄를 방지하고 사용자의 프라이버시를 보호 할 수 있다.

또한 인터넷을 통하여 처리되는 메시지의 안전 및

신뢰성을 확보함으로써 인터넷 전자상거래의 활성화에 이바지하고 기업내 보고 및 결재 메시지의 교환에 사용하여 기업의 경쟁력을 향상시킬 수 있다는 점이다.

향후 연구방향으로는 디지털 기밀 정보가 기밀의 가치가 없어지는 특정 시점에 불특정 다수에게 접근 권한을 부여해 배포하는 방식을 취하고 있어 네트웍 트래픽의 폭주를 야기하고 있다. 따라서 본 연구를 기반으로 시간개념을 도입한 메시지 기밀성을 유지할 수 있는 메커니즘를 연구개발할 필요성이 있다.

기존 암호화방식에서는 메시지의 기밀성을 유지하기 위해 접근제어 메카니즘을 사용하고 있으나 비대화형 메시지의 기밀성을 관리하는데는 적합하지 않다. 비대화형 메시지의 기밀성을 유지하기 위해서 암호화시 메시지에 기밀의 가치가 없어지는 특정 시점이 포함되도록 하여 정해진 특정시점에 가서야 메시지의 복호화가 가능한 방식이어야 한다.

참 고 문 헌

[1] 인증 메카니즘 구현 및 접근제어 기법 연구, 한국전자통신연구소, 1996. 11.

[2] King, J., "X.400 Security", Computers & Security, pp. 707-710, 11(1992).

[3] Manros, C., The X.400 Blue Book Companion. Twickenham, England: Technology Appraisals, 1981.

[4] Schneider, B. E-Mail Security : How to Keep Your Electronic Messages Private, John Wiley & Sons, Inc., 1995.

[5] Denning, D., "Timestamps in Key Distribution Protocols." Communications of the ACM, August 1981.

[6] CCITT Recommendation X.400, X.411. X.412 X.433, 1988.

[7] Kaufman, C., Radia Perlman and Mike Speciner, Network Security : Private Communication in a Public World, Prentice Hall, Englewood Cliffs, New Jersey 07632, 1995.

[8] Boneh, D., and M. Franklin, "Identity based encryption from the Weil paring", Advances in Cryptology: Crypto, 2001(LNCS 2139), pp. 213-229, 2001.

[9] Shamir, A., "Identity-based cryptosystems and signature schemes", Advances in Cryptology : Crypto, 1984(LNCS 196), pp 47-53, 1985.

[10] Mitchell, C., M. Walker, and D.Rush, "CCITT/ ISO Standards for Security Message Handling," IEEE. J.Sel.Areas in Comm., V.7, N.4, May, pp.51-524, 1989.

[11] Stallings, W., Network and Internetwork Security: Principles and Practice, Prentice Hall, 1995.

[12] Kille, S., "Implementing X.400 and x.500 : The PP and QUIPU Systems", Artech House Inc. 1991.

[13] Bellare, M., and C.,Namprempre, "Authenticated encryption", In T. Okamoto, editor, Asiacrypt 2000, volume 1976 of LNCS, pages 531-545. Springer-Verlag, Berlin Germany, Dec. 2000.

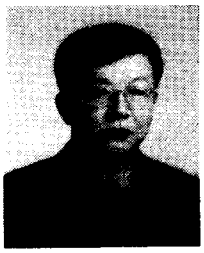
[14] Sugeno, M., "Theory of Fuzzy Integral and Its Applications.", Doctorial Thesis, Tokyo Institute of Technology, pp.18-55. 1974.

[15] 노홍승, "퍼지 계층 평가, 알고리즘의 개발과 그 적용에 관한 연구", 박사학위논문, 한국해양대학교 대학원, 1993.

[16] 신승중, 박인규, "퍼지적분을 이용한 메시지 프로토콜 검증", 정보처리학회지 제7권, 제6호, 2000.

[17] 이병성, "퍼지집합을 이용한 데이터베이스시스템의 품질평가에 관한 연구", 석사학위논문", 대구효성카톨릭대학교 대학원, 1998.

[18] 稼本弥八郎, 田代勸, "Fuzzy 逆問題の解法", 計測自動 制御 學會 論文集, 15. PP. 21-25, 1979.



김 영 수 (Young Soo, Kim)

전북대학교에서 회계학 전공으로 경영학 학사학위를 받았고 경희대학교 대학원에서 경영학석사학위를 받았으며 국민대학교 대학원에서 시스템공학 전공으로 박사학위를 수료하였다. 주요관심분야로는 전자상거래, 인터넷 응용, 정보보안, 자바기술이다.

신 승 중 (Seoung Jung, Shin)

국민대학교에서 시스템공학 전공으로 경영학 박사학위를 받았다. 현재 한세대학교 컴퓨터공학과 부교수로 재직중이며 (주)MLML 대표이사로 활동 중이다 주요 관심분야로는 네트워크보안, 정보보호시뮬레이션, 인공지능응용, 네트워크게임 등이다.

최 흥 식 (Heung Sik, Choi)

로체스터 대학에서 컴퓨터 정보시스템으로 경영학 박사학위를 받았으며 현재 국민대학교 정보관리학부와 비즈니스 IT 전문대학원에서 부교수로 재직중이다. 주요 연구분야는 비즈니스 정보통신 영역으로서 정보통신경영과 전략, 정보통신산업과 정책, 전자상거래, 기업통신망 설계 및 무선통신등을 꼽을 수 있다.