공개키 기반하에서 응용화된 메시지 인증 프로토콜의 설계 및 구현

김영수*, 신승중**, 최흥식***
*국민대학교 정보관리학과
**한세대학교 컴퓨터공학과
***국민대학교 정보관리학과
e-mail:experkim@dreamwiz.com

Design and Implementation of Applied Message Based Authentication Protocol in the Public Key Cryptosystem

Young-Soo Kim*, Seung-Jung Sin**, Heung-Sik Choi***
*Dept of Management Information Systems, Kookmin University
**Dept of Computer Engineering, HanSei University
***Dept of Management Information Systems, Kookmin University

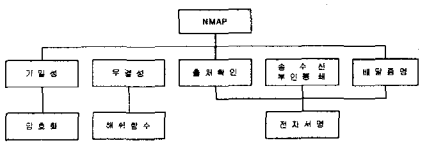
요 약

공개키 암호화와 X.400 프로토콜 그리고 PGP상에 존재하는 메시지 인증 문제를 해결하기 위하여 NMAP로 명명된 인증된 실체기반 암호화 시스템을 제안하고 이를 설계 구현하였다. 제안된 시스템은 전자상거래의 활성화와 비대화형 인증 서비스 제공에 사용될 수 있을 것이다.

1. 서론

전자상거래를 활성화 할 수 있는 가장 중요한 요소는 거래 메시지의 출처 확인과 거래메시지의 위·변조 그리고 거래 메시지의 부인을 방지하기 위한 효율적인 메시지 인증으로 이의 실현을 위해 Denning과 Sacco가 제시한 공개키 암호화 시스템[5]과 메시지 시스템의 표준안인 CCITT의 X.400[2] 그리고 메시지 보안 시스템인 PGP[6]를 분석하여 도출된 보안 취약점을 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[11]로 메시지에 부가되어 보안성을 제공해주는 인증 헤더의 설계를 중점적으로 연구하였고 (그림 1)과 같이 OSI의 보안 아키텍처와 X.411[10]에서 요구하고 있는 기밀성, 메시지 출처확인, 무결성, 송수신 부인봉쇄, 배달증명 서비스를 제공한다[13].



(그림 1) NMAP의 기본 구조

2. 메시지 시스템의 문제점 및 개선방안

X.400에서는 메시지 토큰 구성시에 암호화 후 서명 방식과 저장후 전송 방식 을 권고[8] 하고 있는데 이는 암호문과 서명값의 위조에 따른 위험에 노출되고 호환성을 위한 무결성의 훼손 가능성과 수신자의 암호화키를 시스템이 알고 있어야 하는 문제점이 있다[9]. 그리고 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[12].

따라서 본 논문에서는 이의 해결책으로 <표 1>과 같은 문제점을 파악하여 NMAP에 이를 반영하였다

<표 1> 메시지 보안시스템의 비교

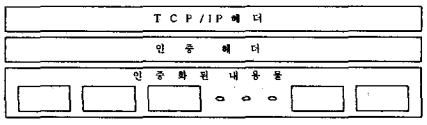
구 분	P G P	제안시스템(NMAP)
메시지 처리시간	다소 느림	다소 빠름
전송 대상	공개키 소유자	불특정 다수
사용자 식별	공개키	식별자
키 생성	개인키로 공개키 생성	공개키로 개인키 생성
암호화 방식	세션키 사용	비밀키 사용
토큰 구성	암호화후 서명방식	서명후 암호화방식
전송 방식	저장후 전송	직접 전송
배달증명 계산	평문대상	암호문대상
키 링	구축 필요	구축 불필요
인증서	필요	불필요
내용 기밀성	IDEA, RSA	DES, RSA
내용 무결성	MD5, RSA	MD5, RSA
발신처 인증	암호화후 서명방식	서명후 암호화방식
발신처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

3. NMAP 인증 구조

인증이란 실체인증과 메시지인증으로 구분되는데 통신의 당사자간의 연결이 확립되는 동안 이루어지는 실체인증에 대한 연구는 활발하게 이루어지고 있으나 비대화형 메시지 인증에 대한 연구는 미진한 실정이다. 연구 개발한 NMAP는 신뢰된 제3자를 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 (그림 2)와 같이 인증 관련 파라미터들을 메시지 헤더 부분에 위치 시키거나 디지털 서명된 데이터 구조를 정의하고 각종 보안 관련 파라미터들을 이 구조속에 위치시키으로써 인증을 실현하고 있다[4].



(그림 2) 인증 파라미터 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[7].

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[3].

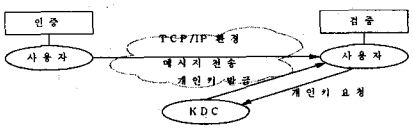
암호화와 서명 방식은 전자서명에 대한 기밀성을 제공하기 위한 추가 암호화에 대한 오버헤드가 요구하고 암호화후 서명 방식은 암호문에 의한 전자서명의 검증으로 위조된 암호문에 의해 생성된 전자서명의 유효성에 대한 논쟁의 가능성이 있고 서명후 암호화 방식은 복호화키 소유자만이 서명을 검증할수 있기 때문에 제삼자에 의해 전자서명이 공증될수 없다는 약점이 있다.

NMAP는 서명후 암호화방식을 적용하였고 향후 인증서를 기반으로 전자서명의 공증 서비스를 제공할 수 있도록 설계하였다.

4. NMAP의 프로토콜 설계 및 성능 분석

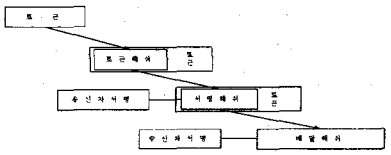
4.1 NMAP의 프로토콜 설계

NMAP는 송신자가 문자열 형태의 식별자를 사용하여 메시지를 암호화하여 전송하고 수신자는 키분배센타(KDC)로부터 그의 ID와 KDC의 비밀정보로 계산된 개인키를 발급받아 메시지를 복원하게 된다(그림 3).



(그림 3) NMAP 개념도

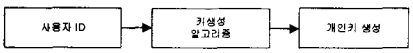
NMAP는 산출된 해쉬에 대해 일련의 연속적인 디지털 서명을 하는 방식으로 메시지 보안성을 유지한다(그림 4).



(그림 4) NMAP 해쉬 시컨스

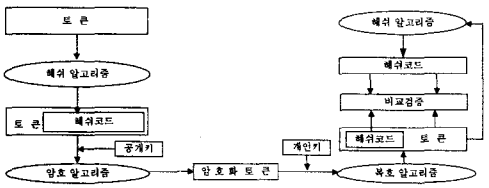
NMAP의 공개키 생성 방식은 인증서 기반 공개키 암호화 방식과는 달리 공개키로부터 개인키를 생

성한다(그림 5).



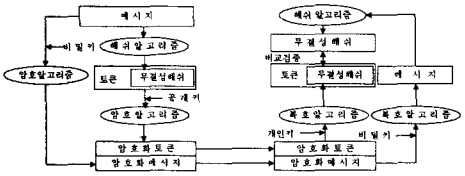
(그림 5) NMAP 키 생성방식

또한 메시지 토큰 속에 디지털 서명된 데이터 구조를 정의하여 각종 인증 관련 파라미터들을 모두 이 구조 속에 위치시켜 수신자에게 전달함으로 인증을 수행한다(그림 6).



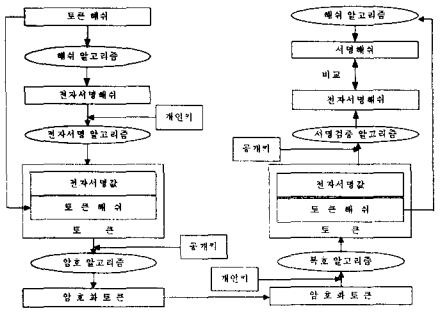
(그림 6) NMAP 토큰 처리 설계

NMAP의 무결성 처리 과정은 메시지의 내용이 전송 중에 변경되지 않았음을 검증하는 절차로 이를 위해서 메시지 다이제스트라고 하는 고정된 크기의 해쉬 코드를 계산하여 메시지에 부착하여 암호화 후 전송한다. 수신자는 그 역으로 수행하여 검증한다(그림 7).



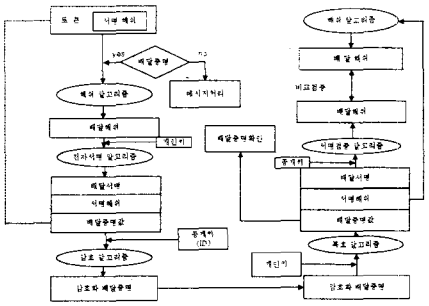
(그림 7) NMAP 무결성 처리 설계

무결성 검증 절차로 NMAP는 개인키와 공개키를 사용하여 해쉬코드에 대해 전자서명하여 암호화하고 메시지와 함께 다시 비밀키로 암호화하여 전송하면 수신자는 전자서명을 확인 후 해쉬코드을 비교하여 무결성을 검증한다(그림 8).



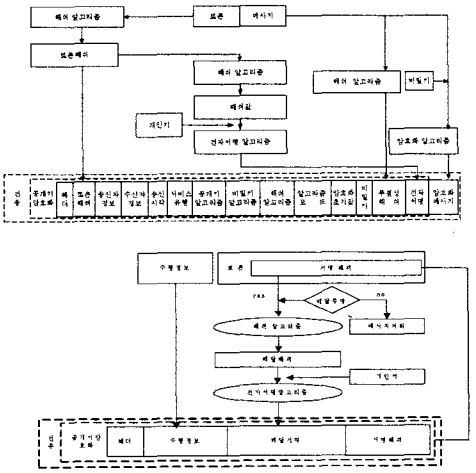
(그림 8) NMAP 전자서명 처리 설계

메시지가 실제로 수신자에 의해 수신되었음을 부정할 수 없게 하는 배달증명의 처리는 (그림 9)와 같이 송신자가 메시지를 전달할 때 배달증명 서비스를 요청하고 수신자는 수신된 메시지를 읽을 때 배달 증명 값을 계산한 후 수령증을 송부하여 송신자가 송부된 수령증을 확인하도록 설계하였다.



(그림 9) NMAP 배달증명 처리설계

NMAP는 암호방식에 기초를 둔 인증 프로토콜로 암호화 시스템을 통하여 전송할 메시지를 (그림 10)과 같이 구성한다



(그림 10) NMAP 프로토콜 설계

5. NMAP 성능 분석

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

<표 2>에서 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

6. 결론

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.

NMAP의 기대 효과를 살펴보면 사용의 용이성 제공으로 공개키 기반 응용 제품의 이용을 촉진하여 정보범죄를 방지하고 사용자의 프라이버시를 보호 할 수 있다.

또한 인터넷을 통하여 처리되는 메시지의 안전 및 신뢰성을 제공함으로써 인터넷 전자상거래의 활성화에 이바지하고 기업내 보고 및 결재 메시지의 교환에 사용하여 기업의 경쟁력을 향상시킬 수 있다.

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 연구 개발할 필요성이 있다.

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

참고문헌

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

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

[3] 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.

[4] Burrows, M, M Abadi, R Needham, "A logic of authentication,", ACM Trans. on Computer Systems, pp. 18-36, vol.8(1) 1990.

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

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

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

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

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

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

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

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