정보처리를 응용한 메시지 보안 시스템의 설계 및 검증

신승중*,김석우*,류대현*,권창희*,김영수**
*한세대학교 IT학부
**국민대학교 정보관리학과

e-mail:expersin@hansei.ac.kr*
swkim@hansei.ac.kr*
dhryu@hansei.ac.kr*
kwonch@hansei.ac.kr*
experkim@dreamwiz.com**

Design and Verification of Applied Information Processing Protocol in the Message Security System

Seung-Jung Shin*,Suk-Woo Kim*,Dae-Hyun Ryu*
Chang-Heui Kwon*,Young-Soo Kin**
*Division of Information Technology, Han-Sei University
**Dept of Information Management, Kook-Min University

요 약

인터넷환경에서 전자상거래는 여러 가지 상황관계를 상호간에 메시지를 통해서 이루어진다. 그러므로 이에대한 가장 중요한 요소는 메시지 인증이며, 이는 거래당사자들이 수신된 메시지의 신뢰성을 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 연구에서는 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 퍼지 적분을 사용하였다. 제안된 시스템은 전자상거래의 활성화와 비대화형 인증 서비스 제공에 사용될 수 있을 것이다.

1. 서론

정보시스템에 대한 사용자수가 급속히 증가하면서 인터넷을 이용한 전자상거래가 확대되고 있으며, 상대방과 직접 대면할 수 없는 가상공간이라는 특성으로 상거래 상대자의 신원을 확인에 보증이 어렵게 된다.

그러므로, 메시지 수신자는 그 메시지가 송신자를 사칭하는 사람이 아닌 실제 송신자한테서 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.

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.

2. 메시지 시스템 개선 방안

암호화 방식의 경우 인증서를 위한 처리시간과 기억장소가 많이 소요되고 인증기관으로부터 공개키 인증서를 발급받지 못한 사용자에게는 메시지를 전송 할 수 없다는 한계가 있다. 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	암호화 후 서명 방식	암호화와 서명 방식
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 부결성	MD5, RSA	MD5, RSA
발신처 인증	서명후 암호화방식	암호화와 서명방식
발신처 부인봉쇄	서명후 암호화방식	암호화와 서명방식
배달 부인봉쇄	서명후 암호화방식	암호화와 서명방식

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.

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].

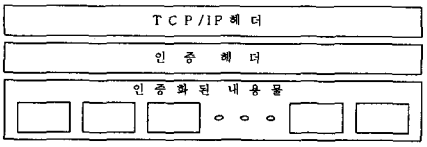

그림 1. 인증 파라미터 캡슐 구조

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[12].

NMAP는 보안성의 강화를 위해 암호화 처리를 위한 약간의 오버헤드를 가지는 암호화와 서명방식을 적용하였고 향후 인증서 기반으로 운영되도록 설계하였다.

3.3 NMAP 설계

프로토콜의 기본 구조는 그림 2과 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.

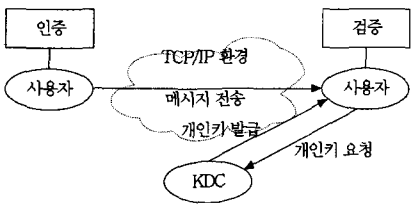

그림 2. NMAP 개념도

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.

복호화과정은 메시지 판독 시점에서 개인 키를 생성하여 메시지를 복호화하도록 설계하였다. PGP는 암호화를 위해 압축과정을 수행한다.

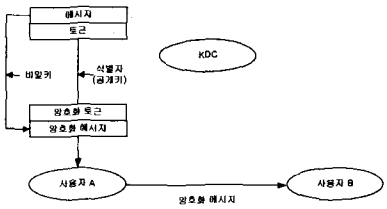

그림 3. NMAP 암호화 처리 설계

토근 처리 절차의 수행은 서비스 유형에 관계없이 디폴트로 제공하도록 하였고 토근에 대해 암호화와 서명을 독립적으로 수행하여 전송하도록 구현 하였다. 반면 PGP는 토근에 대해 먼저 암호화한 후 서명하는 방식을 취하고 있는데 전자서명

의 검증에 사용하는 암호문의 위조를 가능하게 한다.

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

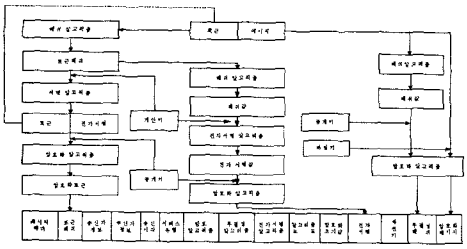

그림 4. NMAP 프로토콜 설계

4. NMAP의 프로토콜 검증

4.1 프로토콜 평가 모델

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.

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 알고리즘소개

평가 대상 문제가 여러개의 항목으로 구성된 계층구조로 주어져 있을 경우에 계층 퍼지적분 알고리즘은 그림 5과 같다.

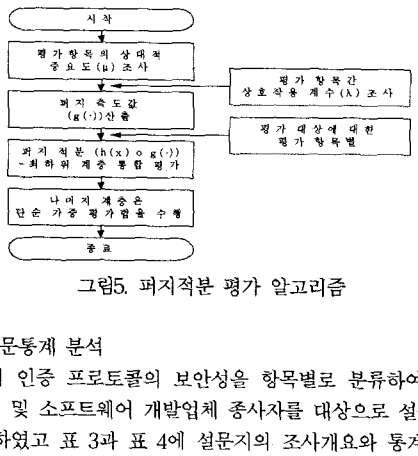

그림5. 퍼지적분 평가 알고리즘

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 분석 결과를 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%

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 중요도를 설정한다.

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.

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

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 퍼지측도치 g(·)에 대한 자료를 이용한 수게노 퍼지적분 평가 알고리즘의 계산과정을 표로 제시해야한다.

5. 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.

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 데이터베이스시스템 의 품질 평가에 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.