이동 네트워크 환경을 위한 Certified E-mail 시스템

박남현*, 이경현**
*부경대학교 전산정보학과
**부경대학교 전자컴퓨터정보통신공학부

A Certified E-mail System for Mobile Network Environment

Nam-Hyun Park*, Kyung-Hyune Lee**
*Dept. of Computer and Information Science, PuKyong Nat'l University
E-mail : egcpnh@hanmail.net
**Division of Electronic, Computer & Telecommunication Engineering University
, Pukyong National University
E-mail : khrhee@pknu.ac.kr

요 약

전자 메일(e-mail)은 현대인의 삶에서 매우 보편적으로 사용되고 있으며, 또한 비즈니스 측면에서도 필수적인 통신도구가 되고 있다. 현대 사회의 인프라가 온라인 환경으로 이동함에 따라서 전통적인 면대면(face-to-face)방식에서 예기치 못한 문제가 발생하고 있다. 하지만, 인터넷은 전자적 정보에 대한 안전하고, 공정한 교환(fair-exchange)과 같은 비즈니스 통신 모델에서 요구되는 서비스를 제공하지 못한다. 본 논문에서는 기존의 보안 메일 기술인 S/MIME, PGP와는 차별화된 기술로서, 전달 메시지의 암호화는 물론 송·수신자 사이의 공정한 교환을 보장하는 Certified E-mail 시스템을 제안하고자 한다. 본 논문에서 제안하는 방안은 셀룰러 폰이나 PDA 사용자 단말기의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하도록 설계 되었다.

1. 서론

인터넷을 통한 전자정보의 발달은 효율성의 증진과 개발속도의 향상이라는 이점을 가져 왔으며 상업적인 인프라(infra)를 off-line에서 on-line으로 이동시켰다. 상업적 인프라가 on-line으로 이동함에 따라 off-line의 면대면(face-to-face)방식에서 예기치 못했던 문제가 발생하였다. 실생활에서는 물건을 구입할 때 물건을 구입하는 동시에(simultaneously) 영수증(receipt)을 발급받는다. 그러나, on-line에서의 전자정보 교환은 면대면 방식과 같은 동시성(simultaneity)을 성취시키지 못한다. 이러한 동시성의 결핍은 공정한 교환(fair exchange) 문제를 낳는다. 공정한 교환(fair exchange)이란 네트워크상의 두 참여자가 서로의 물건을 교환할 때, 서로가 손해보지 않는다는 것을 보장하는 교환방식이다.

공정한 교환(fair exchange)문제에 대한 고전적인 해결방법은 교환하는 전자정보의 작은 부분을 점진적으로(gradually) 교환하는 방법에 기본을 두고 있다. 그러나, 이러한 점진적(gradually) 교환방법은 이론적이며, 높은 컴퓨터 계산능력과 네트워크 전송능력을 요구하므로 현실성이 떨어진다. 공정한 교환(fair exchange)문제의 다른 해결방법으로 Certified E-mail 프로토콜을 이용한 배달(delivery)방법이 있다. Certified E-mail 배달방법은 메일 송신자(sender)가 메일 수신자(recipient)로부터 수신의 증거(proof-of-receipt)를 받았을 때만 메일 수신자는 메일의 내용을 획득할 수 있다.

본 논문에서는 simple threshold cryptosystem인 mRSA를 사용하여 메일 사용자의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하는 구조를 가

짐으로써 셀룰러 폰이나 wireless PDA와 같은 mobile device를 이용하는 메일 사용자에 적합한 Certified E-mail 프로토콜을 제시한다.

본 논문은 다음과 같이 구성된다. 2장에서는 제안프로토콜에서 사용되는 mRSA와 Certified E-mail 프로토콜에 대하여 살펴본 후 Certified E-mail의 요구사항에 대하여 소개하겠다. 3장에서는 simple threshold cryptosystem인 mRSA를 적용한 Certified E-mail 프로토콜을 제시하며, 4장에서는 결론을 맺는다.

2. 관련연구

2.1. mRSA(mediated RSA)

공개키 암호 방식으로 소인수 분해의 어려움을 이용한 RSA의 변형에 기반을 둔 mRSA[1]의 주요 idea는 각 RSA 개인키를 두 부분으로 분리하여 한 부분은 사용자에게 다른 부분은 MD(Mail Delivery)에게 주어진다. 따라서, 부분 개인키(half private key)로는 전체 개인키를 유도하는데 사용될 수 없다. 그러므로, 사용자나 MD 어느 누구도 쌍방의 합의 없이는 메시지를 해독하거나 서명을 생성 할 수 없다.

공개키 : RSA와 같이, 각 사용자(U)는 두 개의 큰 소수 p와 q의 곱인 $n = p \cdot q$이 주어졌을 때, $\phi(n)$과 서로소인 e를 선택하여 공개키로 (n, e)값을 갖는다.

비밀키 : RSA와 같이, $e \cdot d = 1 \bmod \phi(n)$을 만족하는 d를 계산하여, 대응되는 비밀키 (n, d)이 계산된다. 하지만, 사용자나 MD 어느 누구도 d값을 소유하지는 않는다. 대신에, d는 아래와 같이 두 부분으로 나누어진다.

$$d = d_{MD} + d_U \bmod \phi(n)$$

일반적인 RSA와는 달리, mRSA에서는 CA(Certificate Authority)가 모든 키 설정을 다룬다. CA는 RSA와 동일한 방식으로 p, q, e, d 값을 생성하고, $[1, \phi(n)]$ 범위에서 랜덤하게 d_{MD}를 선택하고, $d_U = d - d_{MD}$를 계산한다. 위와 같이 계산된 d_{MD}를 MD에게 안전하게 전송하고, d_U를 사용자에게 안전하게 전송한다.

mRSA 전자서명

1. 사용자는 메시지 m을 MD에게 전송을 한다.
   - MD는 사용자의 공개키가 취소되지 않을 경우, 부분 서명(partial signature)를 계산하여, 사용자에게 전송한다.

$$PS_{MD} = m^{d_{MD}} \bmod n$$

   - 동시에, 사용자도 $PS_U = m^{d_U} \bmod n$을 계산한다.
2. 사용자는 수신된 PS_{MD}를 사용하여,

$m' = (PS_{MD} \cdot PS_U)^e \bmod n$을 계산하고, 만약 $m' = m$이면, 전자 서명문을 아래와 같이 계산한다.

$$(PS_{MD} \cdot PS_U) = m^d \bmod n$$

서명문의 검증 절차는 일반적인 RSA와 동일하게 수행된다.

mRSA 복호화

암호화 절차는 일반적인 RSA와 동일하게 수행된다. 반면, 복호 절차는 서명문 생성 절차와 유사하다.

1. 사용자는 암호문(c)를 MD에게 전송한다.
   - MD는 사용자의 공개키가 취소되지 않은 경우, 부분 평문을 아래와 같이 계산하여 사용자에게 전송한다.

$$PD_{MD} = c^{d_{MD}} \bmod n$$

   - 동시에, 사용자도 $PD_U = c^{d_U} \bmod n$을 계산한다.
2. 사용자는 수신한 PD_{MD}를 사용하여

$c' = (PD_{MD} \cdot PD_U)^e \bmod n$을 계산한다. 만약 $c' = c$이면, 아래와 같이 평문을 복호화 한다.

$$(PD_{MD} \cdot PD_U) = c^d \bmod n$$

mRSA는 간단한 (2,2)-threshold RSA 암호 시스템으로 다음과 같은 특징을 가진다.

•

CA-based Key Generation

RSA에서, 개인/공개 키 쌍은 보통 사용자 자신에 의해 생성되지만, mRSA에서는 키 쌍이 보통 CA에 의해 생성된다. 이는 CA는 모든 사용자에게 속하는 개인키를 안다는 것을 의미하며, 이는 사용자의 key escrow 기능을 제공한다.

- Immediate Revocation

각 사용자의 공개키 인증서를 폐기하기 위하여 각 사용자에 대한 MD에게 사용자의 공개키 인증서의 폐기를 알림으로써 MD가 사용자에게 토큰을 발행하는 것을 중단하라고 지시한다. 그 즉시 사용자의 서명 또는 해독 능력은 취소된다. 이러한 사용자 키의 즉각적인 취소기법으로 사용자는 인증서 검증을 할 필요가 없다.

- Transparency

mRSA는 data를 암호화하거나 서명을 검증하는 사용자들에게 완전히 투명하다. 이들에게 mRSA는 표준 RSA와 구별할 수 없도록 나타나며, mRSA인증서는 표준 RSA인증서와 동일하다.

- No Authentication

mRSA는 MD와 사용자 사이에서 어떤 명시적인 인증을 요구하지 않는다. 서명을 생성하거나 암호를 해독할 때 MD가 생성하는 토큰은 해당 사용자에게만 유용한 정보이므로, MD와의 통신시 토큰이 보호되거나 인증될 필요가 없다.

2.2. Certified E-mail

Certified E-mail은 수신자가 메일을 받았을 때만 송신자가 영수증을 받는 시스템으로, 이는 mail과 영수증(receipt)의 공정한 교환을 보장해 준다.

대부분의 실용적인 Certified E-mail 프로토콜은 제3의 신뢰기관인 TTP(Trusted Third Party)를 사용하여 메일 전송의 공정성을 보장하고 있으며, 이러한 프로토콜은 TTP가 항상 참여하는 on-line 프로토콜[2,3,4]과 TTP를 예외적인 경우에만 참여시키는 optimistic 프로토콜[5,6]로 나눌 수 있다.

On-line 프로토콜은 배달채널(delivery channel)으로 TTP를 사용한다. 송신자와 수신자는 자신의 전송정보를 TTP에게 보내고 TTP는 전송정보에 대하여 무결성(integrity)을 확인하고 전송정보의 교환에 대한 공정성(fairness)을 보증한다. 또한 on-line 프로토콜은 전통적인 메일 시스템이 가지는 큰 이점인 보내고 잊기(send-and-forget) 방법을 실현한다. 보내고 잊기(send-and-forget) 방법이란 메일 송신자는 메일을 보낸 후 수신자의 응답(reply)을 기다릴 필요가 없고, 수신자도 송신자의 도움없이 메일을 읽을 수 있음을 뜻한다. 그러나, on-line 프로토콜은 TTP가 프로토콜 중간에 계속 관여하게 되므로 유저가 프로토콜을 사용하는 횟수에 비례하여 TTP의 계산량이 증가하게 되고 그에 따라 TTP에 대한 통신상의 병목현상도 발생할 수 있다.

Optimitic 프로토콜은 TTP가 단지 예외상황이 발생했을 경우에만 사용이 된다. 그러므로, TTP에 대한 부하가 적고 통신상의 병목현상도 제거될 수 있어 TTP에 대한 효율성(efficiency)이 증진된다. 그러나, optimistic 프로토콜에서는 송신자가 전송정보를 보낸 후 송신자와 수신자간에 몇 번의 정보를 교환하는 동안 송신자와 수신자간의 통신이 유지되어야 한다. 그래서, 송신자와 수신자 양측 모두 상대방의 응답을 기다려야 한다. 그러므로, optimistic 프로토콜에서는 전통적인 메일 시스템이 가지는 큰 이점인 보내고 잊기(send-and-forget) 방법을 실현할 수 없다.

2.3. Certified E-mail의 요구사항

Certified E-mail은 기본적으로 다음과 같은 요구사항들을 만족해야 한다.

- 공정성(fairness) : 송/수신자 양쪽 모두 프로토콜 종결후 자신이 원하는 결과를 얻거나 양쪽 모두 자신이 원하는 결과를 얻지 못해야 한다. 또한, 송/수신자 어느쪽도 자신에게 유리한 결과가 나오도록 프로토콜을 방해하거나 조작할 수 없어야 한다.
- 인증(authentication) : 송/수신자는 정보를 전달하고 있는 상대방이 확실히 의도된 상대방인지를 인증할 수 있어야 한다.
- 기밀성(confidentiality) : 전송되는 정보는 송/수신자 이외의 제 3자가 읽을 수 없어야 한다.
- 무결성(integrity) : 프로토콜 수행도중 전송정보는 공격자에 의하여 변조되어져서는 안된다.
- 부인방지(non-repudiation) : 프로토콜 종료후 메일 사용자는 자신이 받은 정보에 대하여 부인할 수 없어야 한다.

특히, 공정성(fairness)은 Certified E-mail 프로토콜에서 가장 중요한 요구사항이다.

3. 제안 프로토콜

본 장에서는 simple threshold cryptosystem인 mRSA를 사용하여 메일 사용자의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하는 구조를 가지는 Certified E-mail 프로토콜을 제안한다.

제안 프로토콜은 송신자, 수신자, 다수의 MD들, CA로 구성되며 시스템 초기 시작시 송/수신자와 MD는 CA로부터 mRSA 키쌍을 발급 받았다고 가정한다.

제안 프로토콜에서 사용하는 표기법은 아래와 같다.

- S : 송신자의 식별자
- R : 수신자의 식별자
- MD : 메일 전달자의 식별자
- $H(m)$: 메일 메시지 m의 해쉬값
- $E_X(m)$: 통신개체 X의 공개키를 사용한 공개키 암호화
- $S_X(m)$: 통신개체 X의 개인키를 사용한 전자서명

- SK : 세션 암호화를 위한 세션키. 대칭키 암호 알고리즘 기반
- $[m]_X$: 메일 메시지 m을 대칭키 X로 대칭키 암호화
- PS_X : 통신개체 X의 부분 서명문
- PD_X : 통신개체 X의 부분 복호문

[그림 1]은 제안 방안의 전체적인 동작을 보여주고 있다. 본 논문에서는 프로토콜의 간략화를 위해서 RSA에서의 $mod\ n$ 표기를 생략한다.

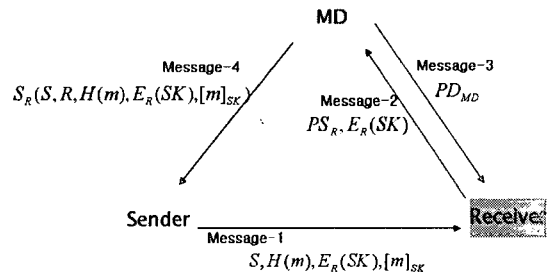

그림 1 제안 프로토콜

프로토콜 설명

(1) 송신자는 세션키(SK)를 랜덤하게 생성하여, 메일 메시지 m의 해쉬값, 세션키로 대칭키 암호화한 값, 수신자의 공개키로 암호화한 세션키, 송신자 식별자로 구성된 message-1을 수신자에게 전송한다.

(2) 수신자는 수신된 정보를 사용하여

$\alpha = S, R, H(m), E_R(SK), E_{SK}(m)$로 두었을 때, 아래와 같이 부분 서명값(PS_R)을 계산한다.

$$PS_R = \{S, R, H(m), E_R(SK), E_{SK}(m)\}^{d_R}$$

수신자는 계산된 PS_R값과 $E_{SK}(m)$로 구성된 message-2를 MD에게 전송한다.

(3) MD는 수신자의 부분 서명값(PS_R)을 사용하여 수신자의 전체 서명값을 아래와 같이 계산한다.

$$S_R(\alpha) = \alpha^{d_R} \cdot \alpha^{d_{MD}}$$

그리고, $E_R(SK)$를 복호화하기 위하여, MD는 부분 복호값을 아래와 같이 계산하여 message-3으로서 수신자에게 전송한다.

$$PD_{MD} = E_R(SK)^{d_{MD}}$$

(4) 수신자는 수신된 message-3과 자신의 소유하는 부분 개인키를 사용하여, 자신의 공개키로 암호화되었던 세션키를 복호화한다.

$$SK = E_R(SK)^{d_{MD}} \cdot E_R(SK)^{d_R}$$

위에서 복호된 세션키를 사용하여, 암호화되었던 메일 메시지를 복호화한다.

(5) MD는 메일 수신자의 수신에 대한 영수증으로서 $S_R(\alpha)$를 메일 송신자에게 전송한다.

제안한 프로토콜에서는 메일 전송의 공정성 보장뿐만 아니라 certified e-mail의 다른 기본 요구사항을 만족시키며, 전통적인 메일 시스템이 가지는 이점인 보내고 잊기(send-and-forget) 방식을 실현한다.

3. 결론

본 논문에서는 simple threshold cryptosystem인 mRSA를 사용하여 메일 사용자의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하는 구조를 가지는 Certified E-mail 프로토콜을 제시하였다. 제안 프로토콜은 셀룰러 폰이나 wireless PDA와 같은 mobile device를 이용하는 메일 사용자에 적합하다.

[참고문헌]

[1] D. Boneh, X. Ding and G. Tsudik, "Instantaneo us Revocation of Security Capabilities"

[2] R. H. Deng, L. Gong, A. A. Lazar and W. Wang, "Practical Protocols For Certified Electronic Mail", Journal of Network and Systems Management, (4(3)):279-297, 1996.

[3] A. Bathreman, "Certified electronic mail", in Proceedings of Symposium on Network and Distributed Systems Security, pp. 3~19, 1994.

[4] M. Abadi, N. Glew, B. Horne and B. Pinkas, "Certified Email with a Light On-line Trusted Third Party: Design and Implementation", WWW2002, May 7-11, 2002, Honolulu, Hawaii, USA.

[5] G. Ateniese, B. Medeiros, and M. T. Goodrich, "TRICERT: A Distributed Certified E-Mail Scheme", in NDSS'01, pp. 47~58, 2001.

[6] B. Schneier and J. Riordan, "A Certified E-mail Protocol", 13th Annual Computer Security Applications Conference, pages 100-106, Dec. 1998.