

Light-Weight 사용자를 위한 새로운 Certified E-mail 시스템 설계

정지원*, 서철**, 이경현***
* 부경대학교 정보보호학과.
** 부경대학교 전자계산학과
*** 부경대학교 전자컴퓨터정보통신공학부

The Design of New Certified E-mail System for Light-Weight Users

Ji-Won Jung*, Chul Sur**, Kyung-Hyune Rhee***
* Dept. of Information Security, PuKyong Nat'l University
** Dept. of Computer Science, PuKyong Nat'l University

*** Devison of Electronic, Computer & Telecommunication Engineering, PuKyong Nat'l University

요 약

본 논문에서는 비밀분산기법과 임계 암호시스템을 사용하여 사용자의 공개키 암호 알고리즘 연산과 공개키 유효성 검증에 대한 연산의 오버헤드를 최소화시킨 새로운 Certified E-mail 시스템을 제안한다. 따라서, 제안 방안은 셀룰러 폰이나 무선 PDA와 같은 컴퓨팅 파워가 취약한 메일 사용자에게 적합하다. 또한, 제안 시스템은 신뢰성을 완전히 분산시킨 TTP(Trusted Third Party)를 사용함으로써, TTP의 훼손이나 악의적인 사용자의 공모 공격에 강건하도록 설계되었다.

1. 서론

최근 개방형 네트워크 환경인 인터넷의 급속한 발전으로 중요한 정보의 교환이 off-line이 아닌 on-line상에서 빈번하게 이루어지고 있다. 그 중 하나로 전자메일(e-mail)이 있으며, 전자메일은 현대인이 상호간의 중요 정보를 교환 할 때 가장 보편적으로 사용하는 통신수단이 되었다. 그러나, 인터넷은 상호간 교환하는 정보에 대하여 신뢰성, 안전성 등을 제공하지 못하며 전자적 처리에서의 동시성의 결핍으로 인하여 통신 당사들 간의 공정한 교환(fair exchange) 문제를 발생시킨다. 공정한 교환이란 교환을 하는 쌍방이 원하는 정보를 모두 가지게 되거나, 혹은 둘 다 가지지 못함을 보장하는 것이다[1].

공정한 교환 문제에 대한 고전적인 해결 방법은 점진적(gradually) 교환 방법으로 정보의 작은 부분을 점진적으로 교환하는 것이다. 이 방법은 많은 계산량과 높은 전송 능력을 요구하므로 비현실적이다[3]. 공정한 교환의 또 다른 해결방법으로 Certified E-mail 시스템이 제안되었다[2][9][10]. Certified E-mail 시스템은 공정성을 보장하기 위해 TTP를 사용하며, TTP의 완전한 신뢰성(fully-trust)을 기반으로 한다. 그러므로 TTP의 훼손이나 TTP가 사용자와 공모하여 악의적인 행동을 할 경우 공정성은 붕괴된다[10]. 그러나, 기 제안되었던 Certified E-mail 시스템은 TTP의 훼손이나 악의적인 TTP에 의한 공모공격에 대한 신뢰성 및 안전성을 제공해주지 못하고 있으며 또한, 메일 사용자에게 대한 오버헤드를 고려해주고 있지 못하다.

본 논문에서는 기존의 방안에서 나타난 문제점을 보완한 새로운 Certified E-mail 시스템을 제안하고자 한다. 제안 시스템은 비밀분산기법(Secret sharing scheme)과 임계 암호시스템(Threshold cryptosystem)[6][8]을 사용하여 사용자의 공개키 암호 알고리즘 연산과 인증서의 유효성 검증에 필요한 연산을 줄인다. 또한 메일 사용자의 오버헤드를 최소화하며 TTP의 신뢰성을 여러 서버에 분산시킴으로써 TTP 단독의 악의적인 행동이나 사용자와의 공모 공격을 사전에 차단할 수 있는 강건한 Certified E-mail 시스템이다.

본 논문의 구성은 다음과 같다. 2장 관련연구 기술을 살펴본 후, 3장에서 새로운 Certified E-mail 시스템 제안한다. 그리고 4장에서는 제안시스템을 분석하고, 5장에서 결론을 맺는다.

2. 관련연구

Certified E-mail 시스템은 공정한 교환을 위해 신뢰된 TTP를 사용하며, TTP의 사용 방법에 따라 on-line 프로토콜과 optimistic 프로토콜로 나뉜다[9][10].

- On-line 프로토콜 : 공정한 교환을 위해 항상 TTP가 개입한다. TTP는 전송 정보의 공정성과 유효성을 보장한다. 그러나, 프로토콜의 매개체로서 TTP가 항상 관여하게 됨으로써 사용자가 프로토콜을 사용하는 횟수에 비례하여 TTP의 계산량과 통신상의 비용도 증가한다.
- Optimistic 프로토콜 : 이 프로토콜은 TTP가 예외 상황,

즉, 분쟁이 발생했을 때만 관여해서 분쟁을 해결한다. 그러나, 송/수신자는 정보를 진송하고 상대방의 응답을 계속 기다려야 함으로 사용자에 상당한 오버헤드를 발생시킨다.

2.1 Certified E-mail 요구사항

일반적으로 Certified E-mail 시스템이 충족해야할 기본 요구사항은 아래와 같다.

- (1) 공정성(Fairness) : 송/수신자간에 서로가 원하는 정보를 모두다 가지거나, 둘 다 가지 못함을 보장해야 한다.
- (2) 인증(Authentication) : 송/수신자는 정보 전달에 있어서 자신이 원하는 상대방지를 인증할 수 있어야 한다.
- (3) 기밀성(Confidentiality) : 송/수신자가 주고받는 정보는 인증되거나 허가되지 않은 제 3자로부터 보호 되어야 한다.
- (4) 무결성(Integrity) : 송/수신자가 주고받은 정보는 공격자에 의해 변조되어서는 안된다.
- (5) 부인방지(Non-Repudiation)

- ① 송신 부인 방지(Non-Repudiation of Origin)
: 프로토콜 종결 후, 송신자는 보낸 메일에 대하여 부인 할 수 없어야 한다.
- ② 수신 부인 방지(Non-Repudiation of Receipt)
: 프로토콜 종결 후, 수신자는 받은 메일에 대하여 부인할 수 없어야 한다.

특히, 공정성은 Certified E-mail의 가장 중요한 요구사항이다. 그러므로, 공정성 보장을 위해 TTP는 공격자의 악의적인 공격이나 공모 공격에 대하여 강건해야 한다.

2.2 임계 암호시스템(Threshold Cryptosystem)

(n, t) 임계 암호 시스템, $n \geq 2t + 1$ 은 n 개로 구성된 서버 시스템의 비밀값, 주로 공개키 암호 알고리즘을 위한 비밀키(secret key)를 n 개의 서버로 각각 분배(sharing)시킨다. 즉, n 개의 각 서버들은 자신의 비밀 분배값(share) s_i 를 소유하게 된다. 암호학적 연산을 수행하기 위해서는 최소 $t+1$ 개의 부분 서명값이 모여야 된다. 따라서 최소한 $t+1$ 개의 서버를 공격해야 만이 공격자는 서버를 가장하여 암호학적 연산을 수행할 수 있다[6][8].

2.3 mRSA(mediated RSA)

간단한 임계 암호시스템인 mRSA는 소인수 분해의 어려움에 기반 한 RSA의 변형으로, 이것은 RSA의 개인키를 두 부분으로 분리하여 두 사용자에 각각 분배하며, 각 사용자는 자신이 소유한 부분 개인키로 다른 사용자의 부분 개인키를 유도할 수 없다. 그러므로, mRSA 사용자들은 서로의 합의 없이는 메시지를 복호화 또는 서명할 수 없다[4]. 공개키는 RSA와 동일하며 개인키는 아래와 같이 계산되어진다.

$$d = d_{u1} + d_{u2} \text{ mod } \Phi(n)$$

일반적인 RSA와는 다르게 mRSA에서는 CA(Certificate Authority)가 모든 키쌍을 생성하며, d_{u1} 과 $d_{u2} = d - d_{u1}$ 를 나누어서 각각 사용자와 TTP에게 안전하게 전송한다.

3. 새로운 Certified E-mail 시스템 제안

본 장에서는 비밀 분산기법과 임계 암호시스템을 사용하여 메일 사용자의 오버헤드를 최소화하며 TTP의 신뢰성을 분산시킴으로써, TTP 단독의 악의적인 행동뿐만 아니라 사용자와 공모 공격에 강건한 새로운 Certified E-mail 시스템을 제안한다.

3.1 가정사항 및 용어 정리

제안 시스템은 다음과 같은 환경을 가정한다.

- 사용자 키 생성 및 분배 : 메일 사용자의 공개키/개인키쌍은 CA에서 생성한 후 개인키를 $d = d_{u1} + d_{u2}$ 로 분할하여 d_{u1} 은 메일 사용자에게 안전하게 진송하고 d_{u2} 는 비밀 분산기법을 사용하여 n 개의 비밀 분배값(share), s_i ($1 \leq i \leq n$)로 분배한 후 DTTP_{*i*} ($1 \leq i \leq n$)(Distributed TTP)에게 s_i 를 안전하게 전송한다고 가정한다..
- 통신 모델 : 제안 시스템의 각 서버들간의 통신은 안전하고 상호 인증된 채널을 사용한다고 가정한다.
- 암호학적 기법 : 대칭키/공개키 암호, 해쉬 함수, 비밀분산 및 임계 암호 등 제안 시스템에서 사용되는 여러 암호학적 기법은 안전하다고 가정한다.

제안 시스템에서 사용되는 용어는 아래와 같다.

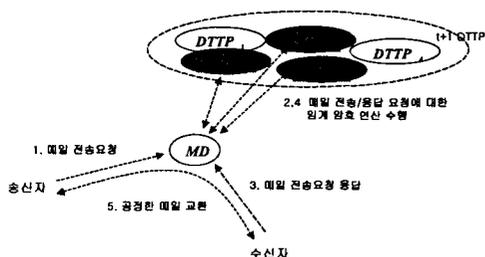
- S, R : 송/수신자의 식별자(identifier)
- MD : 메일전달 서버, 예) 기존 메일 시스템.
- K : 메일 메시지 m 을 암호화하기 위해 송신자가 랜덤하게 생성한 세션키
- $E_K(X)$: X 를 세션키 K 로 대칭 암호화 수행
- $E_R(X)$: X 를 수신자의 mRSA 공개키로 공개키 암호화 수행
- $PS_S(X), PS_R(X), PS_{PD_{DTTP_i}}(X)$: X 를 송/수신자와 분산된 DTTP_{*i*}가 각각 mRSA 부분 개인키로 부분 서명한 결과 값
- $PD_R(X), PD_{DTTP_i}(X)$: X 를 수신자와 분산된 DTTP_{*i*}가 각각 mRSA 부분 개인키로 부분 복호화 한 결과 값
- $SIG_S(X)$: X 를 송신자의 개인키로 서명한 결과 값.
- $SIG_R(X)$: X 를 수신자의 개인키로 서명한 결과 값.

t : 타임 스탬프 값

$\alpha := S, R, E_K(M), E_R(K), t$: 송신자 메일 요청 메시지

3.2. 시스템 구성요소

제안 시스템은 DTTP(Distributed TTP), MD(Mail Delivery), 사용자로 구성되어지며, (그림 1)은 본 논문에서 제안하는 시스템의 전체적인 구조를 보여주고 있다.



(그림 1) 제안 시스템 구조

- **DTTP** : DTTP는 네트워크상의 분리된 프로세서에서 각각 실행되는 $2t+1 \leq n$ 을 만족하는 n 개 서버들의 집합이다. 각각의 $DTTP_i$ ($1 \leq i \leq n$)는 메일 사용자의 mRSA 부분 개인키에 대한 비밀 분배값(share), s_i ($1 \leq i \leq n$)을 저장하고 있으며 메일 전송 서비스 요청 시, 자신이 소유한 비밀 분배값으로 임계 암호 연산을 수행한다.
- **MD(Mail Delivery)** : MD는 사용자의 메일 전달을 담당하는 서버이다. MD는 사용자가 요청한 서비스 수행을 위한 암호학적 연산을 수행하기 위하여 $t+1$ 개의 DTTP들과 협력 작업을 시도한다.
- **사용자** : 메일을 보내고자 하는 송신자와 메일 수신자.

3.3 메일 전달 프로토콜

제안 시스템의 메일 전달 프로토콜은 아래와 같다.

[Step-1] 송신자는 세션키를 랜덤하게 생성해서 메일을 암호화한 후, 송신 메시지만 α 를 자신이 소유한 mRSA 부분 개인키로 부분 서명한 값 $PS_S(\alpha) = (\alpha)^{d_{s1}}$ 를 MD에게 전송한다.

[Step-2] MD는 송신자의 메일 전송요청 정보를 $t+1$ 개의 DTTP들에게 전송한다. 메일 전송요청 정보를 수신한 DTTP들은 송신자의 공개키에 대한 폐지 여부를 검증한다. 검증이 성공하면, 자신이 소유하고 있는 송신자의 비밀 분배값을 사용하여 메일 전송요청에 대한 부분 서명값 $PS_{DTTP_i}(\alpha)$ 을 생성한 후 MD에게 전송한다.

[Step-3] MD는 $t+1$ 개의 DTTP들로부터 전송 받은 부분 서명값으로 $PS_{DTTP}(\alpha) = (\alpha)^{d_{s2}}$ 를 계산한다. 계산된 값은 송신자의 부분 서명값 PS_S 와 mRSA 연산을 아래와 같이 수행하여 송신자의 서명문을 생성한 후 수신자에게 전송한다.

$$SIG_S(\alpha) = PS_S(\alpha) \cdot PS_{DTTP}(\alpha) = (\alpha)^{d_{s1}} \cdot (\alpha)^{d_{s2}} = (\alpha)^{d_s}$$

이것은 송신의 부인 방지 토큰이 된다.

[Step-4] 수신자는 자신이 소유한 mRSA 부분 개인키로 수신 메시지에 대한 부분 서명값 $PS_R(SIG_S(\alpha))$ 을 생성한 후, $PS_R(SIG_S(\alpha)), E_R(K)$ 를 MD에게 전송함으로써 메일 응답 요청을 수행한다.

[Step-5] MD는 수신자의 메일 응답요청 정보를 $t+1$ 개의

DTTP들에게 전송한다. 메일 응답요청 정보를 수신한 DTTP들은 수신자의 공개키에 대한 폐지 여부를 검증한다. 검증이 성공하면, 자신이 소유하고 있는 수신자의 비밀 분배값을 사용하여 메일 응답요청에 대한 부분 서명값 $PS_{DTTP_i}(SIG_S(\alpha))$ 와 부분 복호화값 $PD_{DTTP_i}(E_R(K))$ 을 생성한 후 MD에게 전송한다.

[Step-6] MD는 $t+1$ 개의 DTTP들로부터 전송 받은 부분 서명값으로 $PS_{DTTP}(SIG_S(\alpha)) = (SIG_S(\alpha))^{d_{s2}}$ 를 계산한다. 계산된 값은 수신자의 부분 서명값 PS_R 와 mRSA 연산을 아래와 같이 수행하여 수신자의 서명문을 생성한다.

$$SIG_R(SIG_S(\alpha)) = PS_R \cdot PS_{DTTP} = (SIG_S(\alpha))^{d_{s1}} \cdot (SIG_S(\alpha))^{d_{s2}} = (SIG_S(\alpha))^{d_R}$$

수신자의 서명문 $SIG_R(SIG_S(\alpha))$ 는 수신자의 부인방지 토큰이 되며, 이것은 송신자에게 전송된다.

그리고, $t+1$ 개의 DTTP들로부터 전송 받은 부분 복호화값으로 $PD_{DTTP}(E_R(K)) = (E_R(K))^{d_{k2}}$ 를 계산한 후, 수신자에게 전송한다.

[Step-7] 수신자는 자신의 mRSA 부분 개인키로 세션키 K 에 대해 부분 복호화 한 $PD_R(E_R(K)) = (E_R(K))^{d_{k1}}$ 값과 MD에게서 받은 $PD_{DTTP}(E_R(K)) = (E_R(K))^{d_{k2}}$ 로 세션키 K 를 아래와 같이 복호화 한다.

$$K = E_R(K)^{d_{k1}} \cdot E_{DTTP}(K)^{d_{k2}}$$

그리고, 세션키 K 를 사용하여 암호화된 메일 메시지 $E_R(M)$ 을 복호화하여 메시지 M 을 얻는다.

4. 제안 시스템의 분석

본 장에서는 제안 시스템에 대하여 분석한다. 제안 시스템은 아래와 같이 2.1절에서 정의한 Certified E-mail의 기본요구사항과 함께 추가적인 보안 서비스를 제공한다.

- **공정성** : 수신자는 메일을 읽기 위해 메일 수신자의 증거를 MD에게 보내야만 한다. 그러므로 송/수신자 모두 자신이 원하는 결과를 가진다.
- **인증** : 송/수신자는 메시지 전송 시 자신의 비밀키로 전자서명 함으로 송/수신자에 대한 신원을 인증할 수 있다.
- **기밀성** : 메일 메시지를 암호화하는 세션키는 수신자의 공개키로 암호화되어 있으므로 제 3자는 메일 메시지를 읽을 수 없다.
- **무결성** : 송신자는 암호화된 메시지와 송/수신자의 식별자를 서명한다. 만약, 제 3자가 전송내용을 위조한다면 이는 쉽게 발견된다.
- **부인방지** : 송신의 증거와 수신자의 증거에 송/수신자의 전자서명을 사용하므로 프로토콜 종료 후, 송/수신자는 자신이 보낸 메시지에 대하여 부인할 수 없다.
- **MD와 송신자(또는 수신자)간의 공모에 의한 공격** : 이 공격이 성공하기 위해서는 송신자(또는 수신자)는 최소 $t+1$ 개의 DTTP와 공모해야 가능하다. 또한 MD는 송신자(또는 수신자)의 mRSA 부분 개인키에 대한 분배값을 소유

하고 있지 않으므로, 메시지 서명문 혹은 복호문에 대한 값을 생성할 수 없다. 따라서 서명값이나 복호화값을 위조할 수 없다.

- 사용자 연산상의 효율성 : 제안 시스템은 간단한 임계 암호시스템인 mRSA를 사용하여 설계되었다. 그러므로, 사용자에 대한 공개키 유효성 검증은 DTTP에서 수행하여 사용자측에서의 공개키 유효성 검증을 제거하였으며 사용자가 전자서명 및 복호화 연산을 수행시, 기존의 RSA보다 적은 지수승 연산을 수행한다.

- 사용자 통신상의 효율성 : 제안 시스템에서 사용자의 통신횟수는 송신자가 1번의 송신과 1번의 수신 횟수를 가지며 수신자는 1번의 송신과 2번의 수신 횟수를 가지므로써 사용자의 통신횟수를 최적화시켰다.

5. 결론

본 논문에서는 메일 사용자의 오버헤드를 최소화하고 TTP의 신뢰성을 분산시킨 새로운 Certified E-mail 시스템을 제안하였다.

제안 시스템은 전달 메시지의 공정성 및 안전성을 보장하기 위해 전통적인 암호기법과 함께 비밀분산기법 및 임계 암호시스템을 사용함으로써 사용자의 오버헤드를 최소화하여 셀룰러 폰이나 PDA와 같은 장치를 통한 메일 전송에 적합하다. 또한, 제안 시스템은 TTP의 훼손이나 사용자와의 공모 공격에 강건하도록 설계되었다.

6. 참고문헌

- [1] N. Asokan, V. Shoup, M. Waidner "Asynchronous Protocols for Optimistic Fair Exchange". Proceedings of the IEEE Symposium on Research in Security and Privacy. 1998.
- [2] G. Ateniese, B. D. Medeiros and M. T. Goodrich. "TRICERT: A Distributed Certified E-Mail Scheme". In ISOC 2001 Network and Distributed System Security Symposium(NDSS'01), San Diego, CA, USA, Feb. 2001.
- [3] M. Ben-Or, O. Goldreich, S. Micali, and R. L. Rivest. "A fair protocol for signing contracts" IEEE Transactions on Information Theory, 36(1):40-46, January 1990.
- [4] D. Boneh, X. Ding, G. Tsudik, C. Ming Wong. "A Method for Fast Revocatin of Public Key Certificates and Security Capabilities". In proceedings of the 10th USENIX Security Symposium, pp. 297-308.
- [5] M. Castro and B. Liskov. "Practical Byzantine fault tolerance". In Proceedings of the 3th USENIX Symposium on Operating System Design and Implementation(OSDI'99), pp 173-186, USA, 1999.
- [6] A. De Santis, Y. Desmedt, Y. Frankel and M. Yung. "How to share a function securely". In Proceedings of the 26th ACM Symposium on the Theory of Computing, pages 522-533, Santa Fe, 1994.
- [7] M. Franklin and M. Reiter. "Fair exchange with a

semi-trusted third party". In Proc. ACM Conference on Computer and Communications Security. 1997.

- [8] P. Gemmel. "An introduction to threshold cryptography" in CryptoBytes, a technical newsletter of RSA Lab. Vol.2, No. 7. 1997.
- [9] B. Schneier and J. Riordan. "A certified e-mail protocol". 13th Annual Computer Security Applications Conference, pages 100-106, Dec. 1998.
- [10] J. Zhou and D. Gollmann. "Certified electronic mail". In Computer Security- ESORICS'96 Proceedings, pages 55-61. Springer Verlag. 1996.