신뢰성 분산에 기반한 강건한 Certified E-mail 프로토콜

서 철° 양종필 이경현
부경대학교 전자계산학과°
부경대학교 전자컴퓨터정보통신공학부
{kahlil°, bogus}@mail1.pknu.ac.kr, khrhee@pknu.ac.kr

A Robust Certified E-mail Protocol based on Distributed Confidence

Chul Sur° Jong-Phil Yang Kyung-Hyune Rhee
Department of Computer Science, Pukyong Nat'l Univ.
Division of Electronic, Computer and Telecommunication Engineering, Pukyong Nat'l Univ.

요 약

Certified E-mail 프로토콜은 공정한 교환(fair exchange)을 보장하기 위하여 신뢰된 제 3자 (Trusted Third Party, TTP)를 사용한다. 그러므로, Certified E-mail을 사용하는 유저들은 원격지의 TTP를 완전히 신뢰(fully-trust)해야 한다. 만약 TTP가 훼손되거나 유저와 공모하여 악위적인 행동을 한다면 Certified E-mail 프로토콜의 공정성(fairness)은 붕괴된다. 본 논문에서는 Threshold secret sharing을 사용하여 TTP의 신뢰성을 분산시킨 강건한 Certified E-mail 프로토콜을 제안한다. 분산된 TTP(Distributed TTP, DTTP)를 사용하므로써 유저와 공모하는 악위적인(malicious) TTP에 대한 공격을 막을 수 있으며 어느 한 DTTP가 훼손되더라도 전체 프로토콜에 영향을 주지 못한다.

1. 서 론

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. Certified E-mail 프로토콜은 공정성(fairness)을 보장하기 위하여 TTP를 사용한다. 그러나, TTP에 완전한 신뢰성(fully-trust)을 두므로써 TTP가 훼손되거나 어느 한 유저와 공모한 악위적인(malicious) 행동을 할 경우 프로토콜의 공정성(fairness)은 붕괴된다.

본 논문에서는 TTP 전체의 신뢰성 훼손없이 신뢰성을 여러 서버에 분산시킴으로써 악위적인 TTP와 어느 한 TTP의 훼손에 영향을 받지않는 강건한(robust) Certified E-mail 프로토콜을 제시한다.

본 논문은 다음과 같이 구성된다. 2장에서는 Certified E-mail 프로토콜에 대하여 살펴본 후 Certified E-mail의 요구사항에 대하여 소개하겠다. 3장에서는 threshold secret sharing에 기반한 강건한 Certified E-mail 프로토콜을 제시하며, 4장에서는 제안 프로토콜을 분석한 후 5장에서 결론을 맺는다.

2. Certified E-mail 프로토콜

Certified E-mail 프로토콜은 TTP의 사용방법에 따라 on-line 프로토콜과 optimistic 프로토콜으로 분류된다.

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 보낸후 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 그에따라 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 보낸후 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.

2.1. Certified E-mail 프로토콜 요구사항

Certified E-mail 프로토콜은 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.
- 송신의 부인방지(non-repudiation of origin) : 프로토콜 종료후 송신자는 자신이 보낸 정보에 대하여 부인할 수 없어야 한다.
- 수신의 부인방지(non-repudiation of receipt) : 프로토콜 종료후 수신자는 자신이 받은 정보에 대하여 부인할 수 없어야 한다.

특히, 공정성(fairness)은 Certified E-mail 프로토콜에서 가장 중요한 요구사항이다. 그러므로, 프로토콜은 공정성(fairness)을 유지하기 위하여 TTP의 훼손과 어느 한 유저와 공모하는 악위적인(malicious) TTP에 대하여 강건(robust)해야 한다.

3. 제안 프로토콜

본 장에서는 $(n, t+1)$ threshold secret sharing을 사용하여 TTP의 신뢰성을 $3t+1 \le n$을 만족하는 n개의 DTTP로 분산시킴으로써[9] 유저와 공모하는 악위적인 DTTP나 t개까지의 DTTP의 훼손에도 영향을 받지 않는 강건한(robust) on-line 프로토콜과 optimistic 프로토콜을 제안한다.

3.1. 전제사항

제안 프로토콜은 송신자, 수신자, $3t+1 \le n$을 만족하는 n개의 DTTP들로 구성된다[9]. 프로토콜은 공정성(fairness)과 기밀성(confidentiality)을 보장하기 위하여 대칭키 암호화기법, 공개키 암호화기법, 해쉬 함수, 전자서명기법등과 같은 알려진 암호기법(cryptographic technology)을 사용한다. 송신자와 수신자, DTTP들은 각각 공개키(public key), 비밀키(private key) 쌍을 가진다. 제안 프로토콜에서 전체 서비스를 위한 TTP의 비밀키 sharing에 대한 초기 가정사항은 다음과 같다. DTTP들중 임의의 DTTP가 TTP의 역할을 대신하여 프로토콜에 사용될 TTP의 공개키, 비밀키 쌍을 생성하고 TTP의 비밀키를 $(n, t+1)$ threshold secret sharing[6][7][8][10]을 사용하여(특히, RSA function sharing) 비밀키의 share값들을 다른 $n-1$개의 DTTP들에게 확인가능한 방법으로(예, verifiable secret sharing) sharing한 후 비밀키를 제거함으로써 TTP의 비밀키가 n개의 DTTP들에게 신뢰성있게 sharing되어 있다는 것을 가정한다. 위의 초기 가정사항은 프로토콜의 결과에서 프로토콜 진행동안 TTP가 참여한다는 것이 명백하지만 실제 TTP는 존재하지 않으므로 TTP 숨김성(invisibility)을 만족시킨다[4]. 그리고, 각 구성자간의 통신로는 안전하고(secure) 인증(authenticated) 되었다고 가정한다.

제안 프로토콜에서 사용하는 표기법은 다음과 같다.

S : 송신자의 식별자(identifier)

R : 수신자의 식별자(identifier)

K : 메시지 암호화를 위해 송신자에 의해 랜덤하게 만들어지는 세션키(session key)

$FR(T, DTTP_i)$: $DTTP_i$의 share 값을 이용하여 암호문 T를 부분 복호화한 partial result 값

$E_K(\cdot)$: 세션키 K를 사용한 대칭키 암호화

$E_R(\cdot)$: 수신자의 공개키를 사용한 공개키 암호화

$E_{TTP}(\cdot)$: TTP의 공개키를 사용한 공개키 암호화

$SIG_S(\cdot)$: 송신자의 비밀키를 사용한 전자서명

$SIG_R(\cdot)$: 수신자의 비밀키를 사용한 전자서명

$SIG_{DTTP_i}(\cdot)$: $DTTP_i$의 비밀키를 사용한 전자서명

$C := E_K(M)$: 세션키 K로 메시지 M을 암호화한 값

$T := E_{TTP}(S, R, E_R(K))$

3.2. On-line 프로토콜

제안 on-line 프로토콜에서 송/수신자는 프로토콜의 매개자로 DTTP를 사용하여 송신자가 메시지를 수신자에게 보낸후 수신자는 분산되어 있는 DTTP들 중 어느 한 DTTP를 대리인(delegate)으로 선택하여 프로토콜을 수행한다.

On-line 프로토콜의 절차는 아래와 같다.

1. 송신자는 랜덤하게 생성한 세션키로 메시지를 암호화한 후 $S, C, T, SIG_S(R, C, T)$를 수신자에게 전송한다.
2. 수신자는 송신자의 전자서명 확인후 만약, 전자서명이 올바르다면 수신의 증거인 $SIG_R(SIG_S(R, C, T))$를 생성후 분산된 DTTP들 중 어느 한 DTTP에게 $T, S, SIG_R(SIG_S(R, C, T))$를 전송한다.
3. $DTTP_{대리인}$은 단계 2.에서 받은 메시지를 전체 DTTP들에게 브로드캐스팅한다.
4. 단계 3.에서 메시지를 받은 DTTP들은 전송받은 메시지의 전자서명 확인후, 전자서명이 올바르다면 암호문 T를 partial decryption한 후 결과값 $FR(T, DTTP_i)$을 자신의 비밀키로 전자서명한 후 $DTTP_{대리인}$에게 전송하고 $SIG_{DTTP_i}('ok', T)$를 송신자에게 전송한다.
5. $DTTP_{대리인}$은 DTTP들로부터 수신받은 응답중 각 DTTP의 $SIG_{DTTP_i}(PR(T, DTTP_i))$값들에 대해 전자서명 확인후, 전자서명이 올바른 $t+1$개의 DTTP들이 전송한 $FR(T, DTTP_i)$값으로 T를 복호화한다. T를 복호화한 이후의 DTTP들로부터 전송된 응답은 폐기한다. 그리고, $E_K(K)$를 자신의 비밀키로 전자서명한 후 수신자에게 전송하고 수신의 증거인 $SIG_R(SIG_S(R, C, T))$를 송신자에게 전송한다.
6. 수신자는 $SIG_{DTTP_{대리인}}(E_R(K))$의 전자서명 확인후, 전자서명이 올바르다면 $E_R(K)$를 자신의 비밀키로 복호화한 후 세션키 K로 C를 복호화하여 메시지 M을 얻는다.

제안 on-line 프로토콜에서 $SIG_S(R, C, T)$는 메시지 송신의 증거(proof of origin)가 되고 $SIG_R(SIG_S(R, C, T))$는 메시지 수신의 증거(proof of receipt)가 된다. 메시지 송/수신의 증거는 송신자와 수신자의 전자서명으로 이루어지므로 DTTP를 포함한 제 3자에 의한 영수증의 가장(impersonate)이나 위조(forgery)를 막을 수 있다. 그리고 수신자의 공개키를 사용하여

세션키를 암호화하므로 DTTP를 포함한 제 3자는 메시지를 읽을 수 없다. 또한, 제안 on-line 프로토콜은 보내고 잊기 (send-and-forget) 방식을 실현한다.

3.3. Optimistic 프로토콜

위의 on-line 프로토콜은 optimistic 프로토콜로 쉽게 전환될 수 있다. 제안된 프로토콜은 먼저 송신자가 수신자에게 메시지를 보내고 이때 보내지는 메시지의 형태가 on-line과 optimistic 프로토콜에서 같으므로 on-line 프로토콜과 optimistic 프로토콜은 서로 쉽게 전환되어진다.[5]

Optimistic 프로토콜의 절차는 아래와 같다.

1. 송신자는 랜덤하게 생성한 세션키로 메시지를 암호화한 후 $S, C, T, SIG_S(R, C, T)$를 수신자에게 전송한다.
2. 수신자는 송신자의 전자서명 확인후 만약, 전자서명이 올바르다면 $SIG_R(SIG_S(R, C, T))$를 생성후 송신자에게 전송한다.
3. 송신자는 수신자의 영수증의 전자서명을 확인후, $E_K(K)$를 수신자에게 전송한다.
4. 수신자는 $E_K(K)$를 자신의 비밀키로 복호화한 후 세션키 K로 C를 복호화하여 메시지 M을 얻는다.

위의 optimistic 프로토콜은 DTTP가 단지 예외상황일 때만 사용되므로 DTTP에 대한 효율성이 증가된다. 만약, 예외상황이 발생하였을 경우(수신자가 송신자에게 영수증을 전송하였지만 송신자가 암호화된 키값을 수신자에게 전송하지 않는 경우) 수신자는 이러한 문제의 해결책으로 on-line 프로토콜로 전환할 수 있다. 또한, 송신의 증거(proof of origin)와 수신의 증거(proof of receipt)의 형태가 on-line 프로토콜과 같기 때문에 on-line 프로토콜과 같은 보안 특성을 가진다. 그러나, on-line 프로토콜이 가지는 보내고 잊기 (send-and-forget) 방식은 실현되지 못한다.

4. 제안 프로토콜 분석

본 장에서는 제안 프로토콜에 대하여 Certified E-mail의 요구사항과 악위적인 TTP에 의한 공격에 대하여 분석한다.

- 공정성(fairness) : 송신자가 메시지를 수신자에게 보낸후 수신자가 메시지를 읽기 위해서는 수신의 증거(proof of receipt)를 DTTP(on-line 프로토콜) 또는 송신자(optimistic 프로토콜)에게 보내야 한다. 그러므로, 송/수신자 모두 자신이 원하는 결과를 얻는다.
- 인증(authentication) : 송/수신자는 메시지 전송시 자신의 비밀키로 전자서명하므로 송/수신자에 대한 신원을 인증할 수 있다.
- 기밀성(confidentiality) : 메시지를 암호화하는 세션키는 수신자의 공개키로 암호화되기 때문에 제 3자에 대한 기밀성은 유지된다.
- 무결성(integrity) : 송신자는 암호화된 메시지와 수신자의 식별자를 전자서명한다. 만약, 제 3자가 전송내용을 위조한다면 이는 쉽게 발견된다.
- 부인방지(non-repudiation) : 송신의 증거와 수신의 증거에 송/수신자의 전자서명을 사용하므로 프로토콜 종료후 송/수신자는 자신이 보낸 메시지에 대하여 부인할 수 없다.
- 악위적인 DTTP 단독에 의한 공격 : 세션키는 수신자의 공개키로 암호화 되어 있으므로 DTTP는 메시지를 읽을 수 없다. 또한, 수신의 증거는 송/수신자의 전자서명으로 이루어져 있으므로 DTTP는 수신의 증거를 가장하거나 위조할 수 없다.
- 악위적인 DTTP와 송신자간의 공모에 의한 공격 : 이 공격이 성공하기 위해서는 송신자는 최소한 $t+1$개의 DTTP와 공모해야 한다. 수신자는 DTTP의 응답이 없을 경우 자유롭게 다른 DTTP를 대리인으로 사용할 수 있다.
- 악위적인 DTTP와 수신자간의 공모에 의한 공격 : 이 공격이 성공하기 위해서는 수신자는 최소한 $t+1$개의 DTTP와 공모해야 한다. 만약, $DTTP_{대리인}$과 수신자가 공모하여 수신의 증거를 송신자에게 전송하지 않는 경우에도 송신자는 프로토콜에 참여한 DTTP들에게 받는 $SIG_{DTTP_i}('ok', T)$을 제출함으로써 수신의 증거를 획득할 수 있다.

5. 결론

본 논문에서는 TTP의 신뢰성(confidence)을 분산시킴으로써 TTP의 훼손과 악위적인(malicious) TTP에 의한 공격에 대해 강건한(robust) on-line 및 optimistic Certified E-mail 프로토콜을 제시하였다. 또한, 이동 공격자들(mobile adveraries)의 공격에 의한 DTTP들에 대한 훼손이 발생할 경우 제안 프로토콜은 proactive secret sharing[10][11]을 이용한 프로토콜으로 확장되어질 수 있다.

6. 참고문헌

[1] J. Zhou and D. Gollmann. "Certified electronic mail". In Computer Security- ESORICS'96 Proceedings, pages 55-61. Springer Verlag. 1996.

[2] B. Schneier and J. Riordan. "A certified e-mail protocol". 13th Annual Computer Security Applications Conference, pages 100-106, Dec. 1998.

[3] M.Franklin and M.Reiter. "Fair exchange with a semi-trusted third party". In Proc. ACM Conference on Computer and Communications Security. 1997.

[4] 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.

[5] Kenji Imamoto, Kouichi Sakurai. "A Certified E-mail System with Receiver's Selective Usage of Delivery Authority". INDOCRYPT 2002, LNCS 2551, pp. 326-338, 2002.

[6] P.Gemmel. "An introduction to threshold cryptography". in CryptoBytes, a technical newsletter of RSA Lab. Vol. 2, No. 7. 1997.

[7] 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.

[8] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. "Robust and efficient sharing of RSA functions". In Advances in Cryptology-Crypto'96, LNCS 1109, pp. 157-172, 1996

[9] 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.

[10] S. Jarecki. "Proactive Secret Sharing and Public Key Cryptosystems". Master thesis. MIT. 1996.

[11] Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. "Proactive RSA". In Advances in Cryptology-Crypto'97, LNCS 1294, pp.440-454, 1997