부인봉쇄 서비스의 효율성 향상을 위한 TTP 개입의 최소화 방안

박상준° 홍충선 이대영
경희대학교 전자정보학부
sjpark@digital.kyunghee.ac.kr {cshong, dylee}@khu.ac.kr

The Minimum Intervention of Trusted Third Party for Improvement of Non-repudiation Service Protocol

Sang Jun Park° Choong Seon Hong Dae Young Lee
School of Electronics & Information. Kyung Hee University

요 약

네트워크를 통해 전송되는 메시지, 즉 전자문서들은 송신자와 수신자가 직접 만나서 전해주지 않는다. 이러한 경우 통신 상호간에 서로간의 메시지 송수신 여부를 쉽게 확인하기 어려운 특성이 있다. 따라서 메시지의 송신 부인 또는 수신 부인이 발생할 소지가 있다. 부인봉쇄 서비스는 이러한 논쟁 발생시 송수신 쌍방간의 행위에 대한 증거를 제공하여 주는 서비스이다. 본 논문에서는 이러한 부인봉쇄 서비스를 위해 개입되는 제 3의 신뢰기관인 TTP(Trusted Third Party)의 기능을 확장시켜 부인봉쇄 서비스에서의 효율성을 향상시키는 프로토콜을 제안한다.

1. 서론

현 사회의 정보화와 인터넷 등의 급속한 확산 및 상용화에 따라 지금까지는 정보보안기술을 이용하여 정보에 대한 무결성(integrity), 메시지에 대한 기밀성(confidentiality), 사용자에 대한 인증(authentication), 디지털 설명(digital signature) 등의 다양한 보안 서비스들이 제공되어지고 있으나, 송, 수신자의 상호 거래에 있어서 자신들의 거래행위를 부인하여 원래의 요청과는 위배되는 불법행위가 발생할 수도 있다. 이러한 문제들은 부인봉쇄 서비스(Non-repudiation service)[1]을 이용하여 해결할 수 있다.

본 논문에서는 이러한 부인봉쇄서비스에 개입되는 제 3의 신뢰기관(Trusted Third Party)[2]에 대한 의존성을 줄여 부인봉쇄 서비스의 효율성을 향상시키는 방법과 그 프로토콜을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 제공되어지고 있는 부인봉쇄 메커니즘에 대해 살펴보고, 3장에서는 이 논문에서 제안하고자 하는 TTP의 기능을 확장한 프로토콜 제시한다.

4장에서는 제시된 프로토콜의 시뮬레이션 결과를 분석하고, 5장에서는 현재의 부인봉쇄 서비스에서의 문제점들과 제안한 프로토콜에서 기대할 수 있는 효과를 논의하며 결론을 맺고 향후 연구 방향을 제시한다.

2. 부인봉쇄 메커니즘

부인 공격을 방지하기 위해서 다음과 같은 부인봉쇄 메커니즘이 제공되어져야한다.

· 송신부인봉쇄(NRO:Non-Repudiation of Origin):송신자가 보낸 메시지에 대한 송신자의 부인을 방지한다.

· 수신부인봉쇄(NRR:Non-Repudiation of Receipt):수신자가 메시지를 수신하고 이를 부인하는 것을 방지한다.

· 제출부인봉쇄(NRS:Non-Repudiation of Submission):송신자가 제출한 메시지가 배달되기 위하여 배달기관에 제출되었다는 증거를 제공한다.

· 전달부인봉쇄(NRD:Non-Repudiation of Delivery):메시지가 배달기관에 의해 수신자에게 전송되었다는 증거를 제공한다.

3. TTP 기능 확장을 위한 부인봉쇄 서비스

3.1 표준 부인방지 서비스와 기본 용어

현재 부인봉쇄 메커니즘과 관련하여 표준화가 이루어져 있는 부분으로는 OSI 환경에서의 송, 수신 부인봉쇄 서비스를 규정하는 Open System Interconnection - Security Framework in Part 4 : Non-Repudiation 과 ISO/IEC 13888의 Part1,2,3이 있다. 본 논문에서는 ISO/IEC 13888의 Part1,2,3의 부인봉쇄 메커니즘[3,4,5]을 기본으로 하여 TTP의 기능을 확장시키는 프로토콜을 제시한다.

본 논문에서 사용된 주요 기호의 의미는 다음과 같다.

- X||Y : 두 메시지 X와 Y의 연결
- $eK(X)$: 키 K를 이용하여 암호화한 메시지 X
- $dK(X)$: 키 K를 이용하여 복호화한 메시지 X
- $sK(X)$: 개인키 K를 이용한 메시지 X의 디지털 서명
- S_A, P_A : 주체 A의 개인키와 공개키
- M : A가 B로 보내거나, B가 A로 보내는 메시지
- M_A : TTP가 A, B에게 보내는 경고(Alert) 메시지
- C : 메시지 M의 암호문
  C = eK(M)
- f_{NRO} : NRO를 나타내는 플래그 정보
- f_{NRR} : NRR를 나타내는 플래그 정보
- f_{NRS} : NRS를 나타내는 플래그 정보
- f_{NRD} : NRD를 나타내는 플래그 정보
- T_C : 메시지가 보내진 시간(Time Check)
- T_S : 타임 스템프(Time Stamp)
- TTP : 제 3의 신뢰기관

3.2 TTP(Trusted Third Party)의 기능확장

현재 부인봉쇄 메커니즘과 관련하여 많은 연구가 진행중에 있다. 크게 나누어 국제 표준으로 제시된 메커니즘들이 충족시키고 있지 못한 부분을 보완하는 것과 효율성 개선이라는 두가지 측면에서 접근이 이루어지고 있다. 표준 메커니즘들이 만족하고 있지 못한 요소로는 수신자의 선택적 수신(selective receipt)문제와 공정성(Fairness)문제가 있다. 이러한 문제점들을 개선하기 위해 J. Zhou와 D. Gollmann등이 연구를 수행하고 있다.[1,6,7] 효율성 개선과 관련한 연구로는 기존의 부인봉쇄 메커니즘이 의존하는 제 3의 신뢰기관인 TTP의 의존도를 줄이는 방향으로 연구를 수행하고 있다. 또한 프로토콜 수행을 위한 통신량을 줄이는 방법에 대한 연구도 병행하여 이루어지고 있다.[8,9]

본 논문에서는 부인봉쇄 서비스의 효율성을 개선시키기 위한 방법으로 부인봉쇄 메커니즘이 의존하고 있는 제 3의 신뢰기관인 TTP(Trusted Third Party)의 기능을 확장하여 TTP의 의존도를 줄이는 프로토콜을 제시한다.

TTP를 사용자나 신뢰기관이 요구할 수 있는 로컬 보안정책에 따라 기존의 신뢰기관(Trusted Third Party)을 3 Level로 분류하여 TTP에 대해 차별화 된 기능을 부여한다. TTP의 기능이 확장되고 차별화됨에 따라 TTP를 이용하는 사용자나 신뢰기관은 보안 정책에 알맞은 TTP의 역할을 결정할 수 있다. 이로 인하여 TTP의 개입을 최소로 줄여줄 수 있어 현재 TTP에 대한 높은 의존률을 개선할 수 있다. TTP에 적용되는 Level은 High-Trust Level, Common-Trust Level, Low-Trust Level로 구분한다.

메시지 전달과정에서의 재전송 공격 방지(replay attack)[10]를 위해 타임 스탬프(Time Stamp, TS)[10]를 적용하였고, Common Level부터는 메시지의 전달시간을 확인하여 경고 메시지를 보내기 위해 Time Check(TC)을 도입하여 메시지의 전달시간을 확인할 수 있게 하였다. 또한, 메시지의 신뢰성 보장을 위하여 Low-Trust Level에서는 원문을 암호화하여 전송하였다.

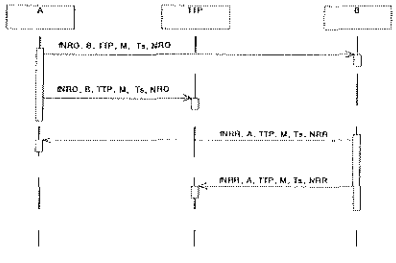
3.3 제안 프로토콜

첫째, High-Trust Level에서는 통신망이나 상대방에 대한 보안을 신뢰할 수 있어 송, 수신 쌍방 간에 어떠한 Non-repudiation 증거자료들의 확인 과정 없이 단순히 메시지들을 전달해주는 기능을 하며, 필요시에만 TTP에 보관되어지고 있는 Non-repudiation의 증거자료들을 송, 수신자에게 전달하는 기능을 부여한다.

이 과정에서 전달되어지는 메시지들은 다음과 같다.

1. A→ B, TTP : f_{NRO}, B, TTP, M, Ts, NRO
2. B→ A, TTP : f_{NRR}, A, TTP, M, Ts, NRR
   NRO : $sS_A(f_{NRO}||B||TTP||M||Ts)$
   NRR : $sS_B(f_{NRR}||A||TTP||M||Ts)$

<그림 1>에서 A는 자신의 요구사항을 위 1번 메시지와 같이 생성하여 B와 TTP에게 동시에 전달한다. 전달되는 메시지 중에서 NRO는 A의 개인키로 서명되어 있기 때문에 A에 대한 인증을 B와 TTP가 할 수 있게 해준다.



<그림 1> High-Trust Level TTP의 동작

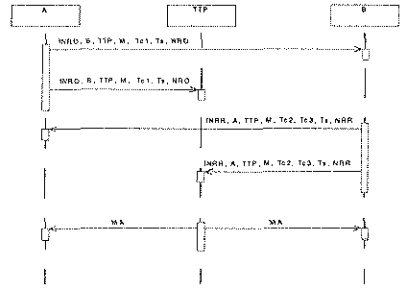
A의 메시지를 받은 B는 A에게 응답에 대한 회신을 2번 메시지와 같이 생성하여 A와 TTP에게 보낸다. 이때, 전송되는 메시지 중에서 NRR은 B의 개인키로 서명되어 있기 때문에, A와 TTP는 B에 대한 인증을 할 수 있다.

둘째, Common-Trust Level에서는 High-Trust 환경에서보다는 덜 안전한 통신망이나 상대방에 대한 신뢰에서 적용된다. 이 경우에도 High-Trust Level에서와 마찬가지로 송, 수신 쌍방 간에 어떠한 Non-repudiation 증거자료 없이 메시지를 전달하지만, network delay를 고려한 message 전달시간을 측정하여 기대치 이상의 지연시간이 발생할 경우에 각각의 이용자들에게 경고 메시지를 보내고 각 이용자들이 요구하는 Non-repudiation 증거자료를 보내주는 기능을 한다.

만약, 메시지가 기대 이상의 지연시간이 발생할 경우 전달되어지는 메시지들은 다음과 같다.

1. A→ B, TTP : f_{NRO}, B, TTP, M, T_{C1}, Ts, NRO
2. B→ A, TTP : f_{NRR}, A, TTP, M, T_{C2}, T_{C3}, Ts, NRR
3. TTP : Time Check
4. TTP→ A, B : MA
   NRO : $sS_A(f_{NRO}||B||TTP||M||T_{C1}||Ts)$
   NRR : $sS_B(f_{NRO}||A||TTP||M||T_{C2}||T_{C3}||Ts)$

<그림 2>에서 A는 High-Trust Level의 메시지에 자신이 메시지를 전송한 시간(T_{C1})을 첨가하여 생성된 1번 메시지를 B와 TTP에게 전송한다. B는 A의 메시지를 받고, A의 메시지를 전송받은 시간(T_{C2})과 자신이 메시지를 전송한 시간(T_{C3})을 첨가한 2번 메시지를 A와 TTP에게 전송한다.



<그림 2> Common-Trust Level TTP의 동작

TTP에서는 T_{C1}, T_{C2}와 T_{C3}의 정보를 비교하여 필요이상의 지연이 발견되거나, B의 메시지를 전달받지 못하였을 때 A와 B에게 경고메시지 M_A를 전달한다. 이 경고메시지를 받은 A와 B는 Non-repudiation 증거자료를 TTP에게 요구하여 이상여부를 확인할 수 있다.

셋째, Low-Trust Level에서는 통신망이나 상대방에 대해 신뢰할 수 없는 환경에서 적용된다. 여기서의 TTP는 철저히 부인봉쇄 기능을 수행하게 되며,각각의 이용자들에게 Non-repudiation 증거자료들을 전달하고 전달된 Non-repudiation 증거자료에 의해 행동하도록 유도한다.

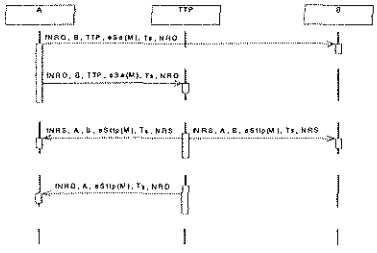
A가 보낸 메시지가 B에 전송되어 확인되어지기까지의 전달되는 메시지들은 다음과 같다.

1. A→ B, TTP : f_{NRO}, B, TTP, $eS_A(M)$, Ts, NRO
2. TTP→ A, B : f_{NRS}, A, B, $eS_{TTP}(M)$, Ts, NRS
3. TTP→ A : f_{NRD}, A, $eS_{TTP}(M)$, Ts, NRD
   NRO : $sS_A(f_{NRO}||B||TTP||eS_A(M)||Ts)$
   NRS : $sS_{TTP}(f_{NRS}||A||B||eS_{TTP}(M)||Ts)$
   NRD : $sS_{TTP}(f_{NRD}||A||B||eS_{TTP}(M)||Ts)$

<그림 3>에서 A는 High-Trust Level에서와 마찬가지로 B와 TTP에게 1번 메시지를 보낸다. 그러나 여기서는 메시지 M을 A의 개인키로 암호화하여 보냄으로서 정보에 대한 기밀성과 신뢰성을 높을 수 있다.

TTP는 A가 보낸 메시지를 받고 A와 B에게 2번 메시지를 보내준다. 이 메시지에 포함된 NRS를 전송함으로서 A가 제출한 메시지가 TTP에게 전달되었다는 증거를 제시할 수 있고, B는 전달받은 NRS를 TTP의 공개키로 복호하여 A가 보낸 메시지와 비교한 후 A가 보낸 메시지가 정당한지를 확인할 수 있다. TTP가

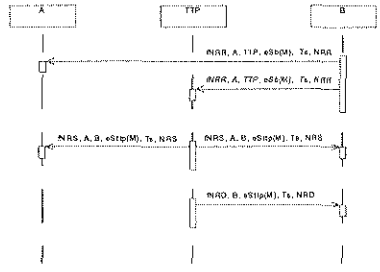
2번 메시지를 전달한 후 A에게 3번 메시지를 전송하여 A의 메시지가 B에게 전송되었다는 증거를 A에게 제시한다.



<그림 3> Low-Trust Level TTP에서 Origin 동작

B는 A가 보낸 메시지를 받고 이상이 없다고 확인되면, 다음과 같은 수신확인메시지를 보낸다.

4. B→ A, TTP : fNRR, A, TTP, eSB(M), Ts, NRR
5. TTP→ A, B : fNRS, A, B, eSTTP(M), Ts, NRS
6. TTP→ B : fNRD, B, eSTTP(M), Ts, NRD
   NRR : sSB(fNRR||A||TTP||eSB(M)||Ts)

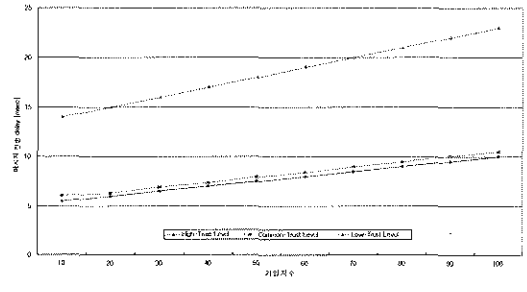


<그림 4>Low-Trust Level TTP에서 Receipt 동작

<그림 4>에서 B는 A가 보낸 메시지의 수신확인에 대한 4번 메시지를 A와 TTP에게 보낸다. TTP는 B의 메시지를 받고 인증과정을 거친 후, 자신이 서명한 5번 메시지를 다시 A와 B에게 보낸다. . 이 메시지에 포함된 NRS를 전송함으로서 B가 제출한 메시지가 TTP에게 전달되었다는 증거를 제시할 수 있고, A는 전달받은 NRS를 TTP의 공개키로 복호하여 B가 보낸 메시지와 비교한 후 B가 보낸 메시지가 정당한지를 확인할 수 있다. TTP가 5번 메시지를 전달한 후 A에게 6번 메시지를 전송하여 B의 메시지가 A에게 전송되었다는 증거를 B에게 제시한다.

4. Simulation 결과

<그림 5>는 TTP의 각 Level별 메시지의 전달시간을 비교한 시뮬레이션 결과이다. 서버와 통신을 하는 가입자가 증가할 때, 메시지의 전송지연시간을 측정한 것이다.



<그림 5> 각 Level별 메시지 전송 지연시간 비교

그림에서 알 수 있듯이 High-Trust Level 환경에서의 메시지 전송지연시간이 가장 낮게 나왔고, Low-Trust Level에서의 메시지 전송지연이 훨씬 높은 것으로 나왔다.

Common-Trust Level에서의 통신은 network delay를 고려한 message 전달시간을 측정하여 기대치 이상의 지연시간이 발생할 경우에 각각의 이용자들에게 경고 메시지를 보내고 각 이용자들이 요구하는 Non-repudiation 증거자료를 보내주기 때문에 High-Trust Level의 통신속도보다 많은 지연시간을 가지고 있다. Low-Trust Level에서는 부인봉쇄서비스가 전적으로 TTP에게 의존하기 때문에 다른 두 Level에서의 속도와 비교했을 경우 크게 차이가 남을 알 수 있다.

결과에서 알 수 있듯이 TTP의 개입이 클수록 부인봉쇄 서비스의 효율성은 감소함을 알 수 있다. 따라서 이러한 문제점들은 본 논문에서 제시한 바와 같이 자신의 환경에 알맞는 TTP의 Level을 선택하여 해결할 수 있다.

5. 결론 및 향후 연구과제

정보통신과 컴퓨터기술의 발전으로 인하여 전자상거래, 인터넷 통신, 전자우편 등과 같은 분야에서 보안 기술의 중요성이 날로 중요시되고 있다. 그러나 안전한 통신과 정보교환을 위해서는 사용자 인증, 메시지 암호화, 부인봉쇄 서비스 등과 같은 기반구조가 갖추어져야 한다. 그러나 기존의 부인봉쇄 메커니즘이 가지고 있는 보완해야할 문제점들로는 선택적 수신(selecrive receipt), 공정성(fairness)의 제공, 효율성의 개선, 사용자 시스템의 내장애성, 다른 기반구조와의 통합 운용성, 이종의 환경에서도 상호 호환 운영될 수 있게 해주는 문제들이 남아있다. 본 논문에서 제시한 TTP의 기능을 확장하는 프로토콜의 사용으로 제 3의 신뢰기관의 개입을 줄일 수 있어 부인봉쇄 서비스에서의 효율성을 개선할 수 있는 효과를 기대할 수 있다.

향후, 제시된 TTP 프로토콜 구현을 위한 TTP 서버의 구현과, TTP의 신뢰성을 높일 수 있는 TTP의 인증에 관한 연구를 고려해야 할 것이다.

[참고문헌]

[1] J. Zhou and D. Gollmann, "Observations on Non-repudiation", Proc. of ASIACRYPT '96, LNCS 1163, Springer-Verlag, pp. 133-144, Springer-Verlag, 1996

[2] J. Zhou and D. Gollmann. "A fair non-repudiation protocol", Proc. of 1996 IEEE Symposium on Security and Privacy, pp. 55-61, May 6-8, 1996

[3] ISO/IEC 13888-1:1997(E) Information technology-Security techniques-Non-repudiation Part 1:General

[4] ISO/IEC 13888-1:1997(E) Information technology-Security techniques-Non-repudiation Part 2:Mechanisms using symmetric techniques

[5] ISO/IEC 13888-1:1997(E) Information technology-Security techniques-Non-repudiation Part 3:Mechanisms using asymmetric techniques

[6] Kwangjo Kim, Sangjoon Park, Joonsang Baek, "Improving fairness and privacy of Zhou-Gollman's Non-repudiation Protocol", IEEE International Workshop on Security, Aizu, Sep.23-24, 1999

[7] J. Zhou, Non-repudiation, Ph.D Thesis, Royal Holloway, U. of London, 1997

[8] N.Asokan, *Fairness in Electronic Commerce*, Ph.D thesis, University of Waterloo, 1998

[9] J. Zhou, R. Deng, F. Bao, "Some Remarks on a Fair Exchange Protocol", to be appeared in PKC2000, Jan. 2000

[10] S. William, "Network security essentials: applications and standards", Prentice Hall, 1999