안전한 선택을 위한 "Magic Sticker" 기법

박희운, 이임영
순천향대학교 정보기술공학부

"Magic Sticker" Scheme for Secure Selection

Hee-Un Park, Im-Yeong Lee
Division of Information Technology Eng, Soonchunhyang University

요 약

우리는 일상 생활을 통해 갖가지 경우에 있어 수없이 많은 선택을 수행하고 있다. 이들 중 몇몇은 누구나 알 수 있도록 알리기도 하고 또 몇몇은 선택되어진 특정 인원들이 알 수 있게 할 수 있다. 이러한 선택의 형태는 암호 프로토콜 상에서, 이 프로세서와 관련된 모델링 기법들을 통해 많은 진척이 보여지고 있다. 그러나 보안 서비스 상에서 익명성을 가지는 구체적인 선택 프로토콜에 대해서는 아직 많은 논의가 필요한 상태이다. 본 논문에서는 네트워크 상에서 익명성을 제공하는 안전한 선택 기법인 "Magic Sticker" 기법을 제안한다. 이와 관련된 응용 분야는 전자 투표, 전자 화폐, 입찰 계약 등과 같이 다양한 분야에서 적용 가능하며, 특히 내용의 공개에 따른 자신의 선택 부분을 안전하게 보호할 수 있다는 특징을 가지고 있다.

1. 서론

컴퓨터의 보급 확산과 네트워킹 기술의 발달로 현대 사회는 다양한 형태의 디지털 정보를 이용하고 있다. 관공서 및 회사를 비롯하여 일반 가정에서도 E-mail 및 워드 프로세서(Word Processor) 작업을 수행하고 있으며, 일반적인 쇼핑(Shopping) 역시 전자 상거래(Electronic Commerce)라는 전자화된 도구를 통해 수행할 수 있으니 그만큼 실용적이고 편리한 시대가 도래하고 있음을 의미하고 있다. 이러한 디지털 정보의 혁명은 문서들을 통해 저장되어 오던 많은 정보들을 인터넷이라는 디지털 공간으로 이동시켰으며, 전 세계를 하나의 가상 공간으로 끌어들이면서 "정보 사회"를 잉태한 것이다.

우리가 이렇듯 쉽게 사용하는 디지털 정보는 그 특성상 복사 및 변조의 위험 속에 노출되어 있다. 또한 메시지 송신상에서 변조가 되지 않았다 하더라도 유효성을 확인할 방법이 없다면 그 정보는 아무런 의미를 가지지 못할 것이다. 심지어 메시지를 송신 및 수신한 사람들이 이를 부인할 경우가 발생한다면, 이를 해결해야 할 방법 역시 필요할 것이다. 이러한 정보 사회의 역기능을 해결하기 위해 각광을 받고 있는 기법 중에 하나가 "암호 기법"이다. 즉 메시지의 안전한 송신 및 기밀성 보장을 위해 대칭키 암호 및 비대칭 암호화 기법을 사용하고 있으며, 메시지 송·수신의 부인을 방지하기 위해 디지털 서명 기법을 사용하고 있다. 또한 그 외의 여러 문제점들을 해결하기 위해 다양한 기법들이 제시되고 있다.

이러한 여러 종류의 암호 기법들은 표면상 나타나는 상당수의 문제점들에도 불구하고 공통적인 특성을 가지고 있다. 그 이유는 암호학적 기법(Protocol)들을 수용하는데 있어서 기밀성(Confidentiality), 무결성(Integrity), 인증성(Authentication) 등이 기본적 서비스로 제공되는데 기인하는 것으로 보인다. 또한 한층 복잡화된 복합적인 서비스들은 서로 다른 각 프로토콜을 이용 및 결합할 수 있는데 예를 들면 다음과 같다.

- 디지털 서명 프로토콜은 무결성과 인증 서비스를 제공한다.
- 은닉 서명(Blind Signature)은 익명 및 서명 서비스를 제공한다.

그 외에도 다양한 서비스들을 위해 진보된 보안성과 효율성을 갖는 해결책들이 제시되고 있다. 더욱이

동일 목적을 갖는 비슷한 프로토콜의 부류들을 분석해 본다면 이들 프로토콜에 대하여 향상되고 개선된 해결책들을 제시할 수 있을 것이다.

본 논문에서는 이러한 복합적인 문제들 중 서로 다른 사용자 집합간의 모순된 요구 사항에 대해 안전한 선택(Secure Selection) 서비스를 제공하는데 그 초점을 맞춘다. 즉 일반적으로 공개되어 있는 여러 가지 선택 사항 중에서 메시지 생성자(Originator)가 선택한 값으로 인해 상대방의 행보가 결정되는 경우 그 선택 정보는 신뢰성을 보장하여야 하지만 결코 생성자를 식별하게 해서는 안될 것이다. 일 예로 투표를 가정해 보자. 투표의 경우 투표자의 투표값은 안전하게 신뢰성을 보장하여야 하지만, 결과 발표시 투표자의 비밀성를 유지하기 위해 결코 누가 누구를 투표했는지 알려져서는 안된다. 그 밖에도 위탁 암호, 공정한 전자 화폐, 그룹 서명 및 익명 회의 등 여러 분야에서 이와 동일한 서비스를 요구하고 있다[1][3][4][5].

현재 네트워크 상에서의 익명성을 제공하는 선택 서비스를 해결하기 위한 기법들의 연구는 부분적인 면에서 진행되고 있으며, 아직 통합적인 메커니즘으로서 연구되고 있지는 못한 상황이다[2]. 따라서 본 논문에서는 이러한 안전한 선택 문제의 해결책으로서 "Magic Sticker" 기법을 제안한다. 또한 이 기법이 현재 선택 서비스와 관련된 여러 분야에 어떻게 적용 가능한지 기술하게 될 것이다.

2. 안전한 선택(Secure Selection)

안전한 선택과 관련하여 다음과 같은 사항을 고려해 보자.

엘리스는 MSWI(Multimedia S/W Inc.)의 자회사에 속한 노동 조합원이다. 그녀는 모든 자회사를 대상으로 노동 조합장 투표를 네트워크를 통해 중앙에서 관리하려 하고 있다. 안전 장치의 마련을 위해 네트워크를 통한 전자 투표를 수행할 경우 기밀성과 인증성을 보장하기 위해 암호 기법과 디지털 서명을 사용하기로 했다. 또한 전국의 조합원들이 확인할 수 있도록 투표 결과를 보여 주기로 하였다. 그러나 그녀는 투표 실행 전날 밤 중요한 딜레마에 빠지게 되었다. 조합장 후보들이 매수를 통해 투표자들을 설득했고 이를 모니터를 통해 투표 결과를 확인하려 한다는 소문이 있었기 때문이다. 또한 특정 후보는 회사 임원들의 지원하에 공공연히 투표 결과를 통해 인사 고가를 반영하려 하는 움직임이 발생하였다. 과연 그녀는 어떻게 이러한 불법적인 행위를 저지할 수 있을까? 또한 어떻게 투표자들이 안전하게 투표 값을 선택하면서도, 다른 사람들이 개별적인 투표 결과를 확인하지 못하도록 할까?

상기 예에서 도출된 문제점들은 선택 행위에 있어서 안전성에 기반한 자율성이 얼마나 중요한지를 보여주는 단적인 예가 된다. 동시에 선택 결과의 신뢰적 등록과 익명성의 보장은 전반적인 프로세스에 있어 안전성과 밀접한 관계를 가진다. 이처럼 전자화된 네트워크 상에서 사용자가 자신의 자유의지로 선택을 수행하고 이에 대한 안전한 신원 보장을 이룰 수 있는 서비스를 '안전한 선택(Secure Selection)'이라 한다.

다음에 제시된 항목들은 안전한 선택과 관련하여 다양한 서비스를 요구하는 몇몇 예들을 기술한 것이다.

- 전자 투표 : 투표자가 선택한 투표 결과는 제 3자에게 숨겨져야 한다.
- 전자 화폐 : 화폐에 대한 정당한 사용자는 완전한 익명성을 제공하지만 불법적인 사용자에 대해서는 소유자 추적 또는 동전추적을 할 수 있어야 한다.
- 전자 입찰 : 입찰자 및 응찰가는 프로세스 과정에서는 안전하게 보장되어야 하며, 공개 단계에서 오직 참여자들만이 입찰가를 알아야 한다.
- 익명 회의 : 회의에 참석한 사람들과 회의 결과와의 연결은 불가능해야 한다.

3. 물리적 Magic Sticker개념

매직 스티커는 2개 이상의 영상을 편광 각도가 다른 홀로그래피(Holography) 필름에 2차원으로 합성시켜 광원의 각도에 따라 서로 다른 형체를 표현할 수 있도록 한 필름형 스티커를 의미한다. 그림 1.은 이에 대한 간단한 구조를 그림으로 표현한 것이다. A)는 2개의 영상과 필름을 합성한 형태를 보이고 있으며, B)는 빛의 각도에 따라 각기 다른 영상이 보여지는 것을 표현한 것이다. 이때 각 영상의 어느 위치에나 눈에 보이지 않는 정보를 저장할 수 있으며, 매직 스티커를 생성할 때 적용된 특수 정보를 아는 사람만이 확인 가능하다.

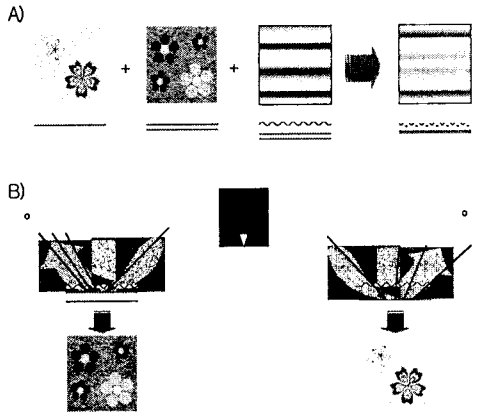

그림 1. 물리적 매직 스티커의 일반적인 형태

이러한 정보는 만약 특수 정보를 모르는 사람이 인위적으로 필름을 벗겨낼 경우에는 저장된 정보 및 영상 모두가 파괴된다. 또한 저장 정보 확인을 위해서는 특수 정보가 필요하게 되므로 인위적인 편법을 통해 이를 확인하는 것은 불가능하게 된다. 이때 저장 정보의 내용이 생성자가 2개의 영상 중 하나를 선택한 값이라면, 물리적으로 안전한 선택이 가능해 진다. 이러한 특성을 암호학적으로 접근할 경우 안전한 선택 서비스를 네트워크 상에서도 수행할 수 있게된다.

4. 암호학적 Magic Sticker 기법 제안

본 장에서는 안전한 선택을 실용화하여 다양한 분야에 적용될 수 있는 통합적 해결책인 암호학적 "Magic Sticker"를 제안한다. 이를 위해 본 방식은 다음과 같은 특성을 포함한다.

- 본 방식은 대칭 및 비대칭 암호화 기법들 중 어떠한 것을 사용하여도 무관하다. 단, 본 기법은 상기 두 방식을 혼용한 기법으로 설명한다.
- 공개키/비밀키 인증 및 분배를 위하여 CA(Certi-fication Authority)를 가정한다.
- 송신자가 선택 메시지를 생성하며, 원하는 대상자를 지정하여 이를 확인할 수 있도록 한다. 단 본 논문에서는 수신자가 이를 확인하는 것으로 가정한다.

4.1 시스템 계수

. CA, A, B : 인증기관, 송신자 A, 수신자 B
. H : 128비트 안전한 일방향 해쉬 함수
. ID* : *의 식별자
. Mkey : 통신 및 인증을 위한 마스터 키
. [*]/2 : *의 비트 중 길이를 반으로 나눈 값
. Ckey : 통신키, Ckey = H(IDA||Mkey)
. Ekey : 암호화 키, Ekey = [H(IDA||Mkey)]/2
. Akey : 인증키, Ekey를 만들고 난 나머지 값
. PkA, SkA : A의 공개키 및 개인키
. PkB, SkB : B의 공개키 및 개인키
. r : A가 선택한 값, r ∈ {0, ..., n} n은 선택할 항목의 개수
. CMi : 선택 항목, i∈ {0, ..., n}
. CMj : 부가 항목, j ∈ {0, ..., n}, j≠i
. || : 연접 연산자

4.2 프로토콜

1) 송신자 A 및 수신자 B

. 자신들의 공개키를 CA에 등록한 다음, CA로부터 상대방 공개키에 대한 인증서 Cert를 제공받는다.
  Cert(PkA), Cert(PkB)
. 선택 항목 송신 및 수신을 위해 필요한 키들을 CA에게 요청한다.

2) CA

. CA는 수신자에게 Mkey를 생성하여 B의 공개키로 암호화하여 B에게 전송한다.
  PkB(Mkey)
. CA는 송신시 기밀성을 제공하기 위하여 A의 ID와 Mkey를 이용해 통신키 Ckey를 생성한다. 그런 다음 이를 A의 공개키로 암호화하여 송신한다.
  Ckey = H(IDA||Mkey)
  PkA(Ckey)

3) 송신자 A

. 수신된 Ckey를 확인한다.
  SkA(PkA(Ckey)) = Ckey
. A는 선택 항목 중에서 자신이 원하는 값을 선택한다.
  CMi (i ∈ {0, ..., n})
. 물리적 Magic Sticker에서처럼 선택 항목에 대응되는 부가 항목을 선택한다.
  CMj (j ∈ {0, ..., n}, j≠i)
. 선택 값의 식별자 r (= i)를 계산한 다음, 자신의 개인키로 서명을 수행한다.
  SkA(r)
. 자신이 선택한 값 CMi와 SkA(r)을 연접해 인증

키 Akey로 암호화한다.

Akey(CMi||SkA(r))

. 암호화된 정보에 부가 정보 CMj를 연접해, Ekey로 암호화한다.

Ekey(Akey(CMi||SkA(r))||CMj)

. 상기 정보에 IDA를 연접해 B의 공개키로 암호화하여 전송한다.

PkB(Ekey(Akey(CMi||SkA(r))||CMj)||IDA)

4) 수신자 B

. 수신된 Mkey를 확인한다.

SkB(PkB(Mkey)) = Mkey

. A로부터 수신된 정보를 자신의 개인키로 확인한 다음 IDA를 이용하여 Ckey를 생성한다.

Ckey = = H(IDA||Mkey)

. Ekey를 생성하여 부가 정보 CMj를 확인한 다음, CMj만을 다시 암호화한다.

Ekey(CMj)

. Akey를 이용하여 CMi를 확인하고, A의 공개키를 이용하여 서명된 r 값을 확인한다. 만약 r = i이면 선택이 정확히 이뤄진 것으로 판단하고 Akey로 CMi를 암호화한다.

PkA(SkA(r)) = r

Akey(CMi)

. 수신된 IDA, Ekey(CMj), Akey(CMi)를 공개한다.

5) 송신자 A

. 공개된 암호 값으로부터 선택 및 부가 항목이 등재되었는지 확인한다. 이를 통해 수신자가 정당한 Mkey를 가지고 있으며, 공개키의 주인인지 확인하게 된다.

Ekey(Ekey(CMj)) = CMj

Akey(Akey(CMi)) = CMi

. CMi가 Akey로 암호화되었는지, r = i 인지 확인함으로서 자신의 선택 항목이 확인되었는지 검증하게 된다.

4.3 제안 방식 고찰

본 방식은 다음과 같은 특성들을 만족하고 있다.

. 전송 기밀성 : 송·수신되는 모든 정보는 공개키를 이용하여 전송하므로 기밀성을 보장한다.

. 공개 안전성 : 각 메시지는 대칭키(Ekey, Akey)로 암호화되어 공개되므로 이 키들을 모르는 한 안전하게 운용된다.

. 안전한 선택성 : 송신 후, 제 3자가 Ekey, Akey 및 r 값을 추측한다 할지라도 수신자가 소유한 SkA(r)를 확인하지 않는한 결코 송신자의 선택 항목을 검증할 수 없다.

. 부인 방지 : r에 대해 송신자의 서명을 사용함으로서 송·수신 양자간의 부인 방지가 가능하다.

5. 결론

정보 사회의 발전은 다양한 부분에서 편리성과 유용성을 제공하지만, 아직 몇몇 부분에 있어서는 해결해야할 문제들이 산재해 있다. 그 예로, 우리는 일상생활 속에서 무수히 많은 선택을 수행하게 되며, 이러한 선택 중에는 제 3자에게 익명성을 유지해야만 하는 경우가 생길 수 있다.

본 논문에서는 전자 투표, 공정한 전자 화폐, 위탁 암호, 그룹 서명, 전자 입찰 및 익명 회의 등 디지털화된 네트워크 상에서 안전한 선택을 수행하는데 유용한 Magic Sticker 기법을 제안하였다. 제안 방식을 통해 전송상의 기밀성, 공개 안전성, 부인 방지 및 안전한 선택성을 확보할 수 있었으며, 향후 안전한 선택성이 필요한 여러 분야에 적용시켜 봄으로서 그 안전성과 실효성을 검증해볼 계획이다.

[참고문헌]

[1] D. Chaum, "Group Signature," Advances in Cryptology-EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp.257-265.

[2] R. Cramer, I. Damgard and B. Schoenmakers, "Proofs of partial knowledge and simplified design of withness hiding protocols," CRYPTO'94, pp. 174-187, 1994

[3] A. Fiat and A. Shamir, "How to prove yourself : practical solutions to identification and signature problems," Advances in Cryptology -CRYPTO'86 Lecture Notes in Computer Science, pages 186-194, Springer-Verlag, 1986.

[4] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," In Security Protocol Workshop, 1997.

[5] H. Petersen and G. Poupard, "Efficient scalable fair cash with off-line extortion prevention," Information and Communication Security, ICICS'97, pages 463-473, November 1997.