익명의 디지털 티켓

김형식[0]
삼성 전자 기술총괄
{hyungsik.kim[0]}@samsung.com

Anonymous Digital Ticket

Hyoungshick Kim[0]
Corporate Technology Operations, Samsung Electronics

요 약

디지털 티켓이란 티켓의 소유자에게 전자 서비스에 대한 특정한 권한을 보장하는 증명서이다. 디지털 티켓이 사용되는 응용 분야는 다양하며, 분야에 따라서 사용되는 티켓의 종류가 달라진다. 익명의 디지털 티켓이란 일반적인 디지털 티켓의 조건을 만족시키는 동시에 티켓 소유자에 대한 익명성을 보장하는 디지털 티켓을 말한다.
익명의 디지털 티켓은 전자 화폐와 유사한 특성을 갖지만, 액수에 대한 정보를 노출시키지 않아야 한다는 점에서 차이를 가진다. 본 논문에서는 은닉 서명과 일 방향 함수를 이용하여 n 번 사용 가능한 익명의 디지털 티켓 문제에 대한 프로토콜을 설계하고 이에 대한 안전성을 보인다.

1. 서 론

오늘날 인터넷은 여러 가지 측면에서 인간의 삶을 보다 윤택하게 만들고 있다. 유용한 정보를 효율적으로 수집하고 처리할 수 있게 만들 뿐만 아니라, 물리적인 접촉 없이 온라인을 통해서 다양한 유형의 상품과 서비스를 획득할 수 있도록 만들고 있다.
많은 실제적인 경우에 있어서, 주요한 정보와 서비스는 멤버쉽 인증(authenticating membership)과 전자 지불(electronic payment) 등과 같은 기법을 통하여 사용자의 접근을 제한하고 있다[1]. 예를 들어 '*The Wall Street Journal Interactive Edition*'을 구독하기 위해서 사용자는 먼저 구독 서비스에 대한 사용료를 지불해야 한다[8].
암호화된 크레디트 카드(encrypted credit cards)와 전자 화폐(digital cash), 소액 지불 시스템(micropayment)과 같은 많은 수의 전자 지불 방법 등이 전자 상거래를 위하여 설계되고 구현되었다[4][5][6][7][9][13].
디지털 티켓(digital ticket)이란 티켓의 소유자(ticket owner)가 티켓에 명시된 서비스를 요구할 수 있도록 권한을 보장하는 디지털 증명서(digital certificate)이다. 디지털 티켓은 전자적으로 기록되고 전달될 수 있다[2][10]. 디지털 티켓은 인터넷 상에서 일어나는 많은 작업을 효율적으로 처리하고 응용 문제를 단순화시키는 장점을 가진다. '*E-Stamp*'나 '*e-gold*'와 같은 디지털 티켓들이 실용적인 예이다[11][12]. 하지만, 이러한 장점과 함께 서비스 공급자가 사용자의 온라인 행위를 감시(monitor)하고 기록하는 일이 매우 쉬워진다는 단점을 가진다. 결과적으로 사용자의 민감한 정보가 공급자에게 노출될 수 있는 것이다. 이러한 정보는 이후에 사용자에게 손실을 끼칠 수 있다. 사용자는 회사의 경영 전략이나 연구 방향, 구매 경향, 성인 콘텐츠(contents) 등의 이용과 같은 행위에 관련된 민감한 정보가 외부에 노출되는 것을 바라지 않을 것이다[3].
본 논문에서는 기존에 연구되었던 디지털 티켓에 익명성이라는 부가적인 속성이 추가된 익명의 디지털 티켓(anonymous digital ticket)을 제안한다. 익명의 디지털 티켓은 전자 화폐와 많은 유사성을 갖지만, 액수에 대한 정보가 필요하지 않는다는 차이점을 가진다. 익명의 디지털 티켓은 티켓의 사용 횟수에 대해서 n 번으로 일반화 될 수 있다. 디지털 티켓의 정의와 조건에 대해서는 Fujimura가 연구한 바 있다[10].

2. 익명의 디지털 티켓

익명의 디지털 티켓 문제(anonymous digital ticket problem)는 다음과 같이 정의한다.

2.1 참가자

참가자는 티켓 발행자 I, 티켓 사용자 U, 티켓 검사자 C로 구성된다. 많은 실제적인 응용 분야에서 I와 C가 같으므로 본 논문에서도 I와 C를 동일한 객체로 다룬다.

2.2 프로토콜의 구성

디지털 티켓에 관련된 프로토콜은 티켓의 발급(ticket issuance)과 티켓의 소비(ticket consumption)인 2단계로 구성된다.
먼저 티켓의 발급 단계에서 I와 U는 n번 사용 가능한 티켓 발급에 동의하고 I는 U에게 티켓을 발급한다. U는 발급된 티켓이 이상이 없는지를 확인하고, 이상이 없을 경우 티켓을 안전한 곳에 보관한다. 티켓의 소비 단계에서 U는 I에게 티켓을 전송하고 I는 티켓의 적법성을 판단한다. 만약 I가 티

켓이 정상이라고 판단한다면 티켓의 권한에 해당하는 서비스를 U에게 제공한 뒤, 티켓을 소비한다.

2.3 필수적인 속성

n번 사용 가능한 익명의 디지털 티켓이 가져야 되는 속성은 다음과 같다.

속성 1. 티켓의 위조(forgery)가 불가능해야 한다.

속성 2. 티켓의 중복된 사용(double spending)이 금지되거나 검출되어야 한다.

속성 3. 티켓 사용자의 익명성이 보장되어야 한다.

속성 4. 티켓 소비 단계에서 사용된 티켓의 나머지 사용 횟수가 노출되지 말아야 한다.

임의의 프로토콜이 속성 4를 만족하지 못할 경우, 다음과 같은 문제가 발생할 수 있다. 예를 들어 I가 사용자 A에게 100회 이용 가능한 티켓을 발급하고 사용자 B에게 5회 이용 가능한 티켓을 발급하였다고 가정하여 보자. 이후에 두 명의 사용자 중 누군가가 티켓을 소비했을 때, I는 사용된 티켓의 나머지 사용 횟수로부터 방금 전에 티켓을 사용한 객체가 A인지 B인지를 정확하게 구분할 수 있다.

3. 프로토콜

먼저 몇 가지 표기법에 대하여 정의하고자 한다. X가 객체이고 M이 메시지라면, $SIG_X\{M\}$은 M에 대해서 X가 디지털 서명한 것을 의미한다. b(M)은 메시지 M이 임의의 방법에 의하여 은닉되었음을 의미한다. 간략화를 위해서 모든 메시지는 서명 되기 전에 일 방향 함수(one-way function)에 의하여 해쉬(hash)되고, 서명 안에 포함된다. I의 디지털 서명은 은닉 기능을 제공하고, U와 I가 서로 주고 받는 메시지는 암호화(encryption)와 디지털 서명(digital signature)을 통하여 안전하게 주고 받을 수 있다고 가정한다.

3.1 1회 이용 가능한 익명의 디지털 티켓

1회 이용 가능한 익명의 디지털 티켓은 은닉 서명을 이용하면 간단하게 설계할 수 있다. 먼저 I와 U가 한번만 사용 가능한 티켓 발급에 동의하였다고 가정한다.

3.1.1. 1회용 티켓의 발급

U는 임의의 수 r을 선택한다. 선택한 r을 이용하여 메시지 M = (" *P's ticket* ", r)을 만들고, M을 은닉(blind)한다. U는 b(M)을 I에게 보낸다. I는 b(M)을 서명하고 U에게 전달한다. 즉, U는 $SIG_I\{b(M)\}$을 받는다. U는 받은 $SIG_I\{b(M)\}$에 대하여 I의 서명을 검증하고, $SIG_I\{M\}$을 계산하여 보관한다.

3.1.2. 1회용 티켓의 소비

U는 $SIG_I\{M\}$을 I에게 보낸다. I는 서명을 검증함으로써 자신이 발급한 티켓인지를 확인하고, 서명이 맞을 경우, I는 티켓의 중복 사용 여부를 검사한다. 만약 I가 받은 티켓에 대해서 새로운 티켓이라고 판단한다면 티켓의 권한에 해당하는 서비스를 U에게 제공한 뒤, 티켓을 소비한다. 중복 사용 여부에 대한 검사 방법은 M에 포함된 r이 이전에 소비된 티켓들의 r' 들 중에 동일한 값이 존재했는지를 검사함으로써 이루어진다. 만약 없었다면 r을 기록하여 차후에 r이 포함된 티켓이 중복해서 사용되지 않도록 한다.

3.1.3 1회용 티켓의 안전성

1회 이용 가능한 익명의 디지털 티켓의 안전성은 쉽게 증명될 수 있다. 속성 1과 속성 3은 은닉 서명의 안전성에 기반한다는 것을 직관적으로 알 수 있다. 속성 2의 경우는 모든 소비되는 티켓의 r 값들이 기록되기 때문에 동일한 티켓이 중복하여 사용되는 것을 방지할 수 있다. 물론 적법한 사용자가 피해를 입지 않도록 r의 선택 범위가 충분히 크도록 설계되어야 한다. 1회 이용 가능한 익명의 디지털 티켓의 경우, 사용 횟수 유무에 상관 없이 사용자의 익명성이 항상 보장되므로 속성 4는 특별한 의미를 갖지 않는다.

3.2 *n*회 이용 가능한 익명의 디지털 티켓

n회 이용 가능한 익명의 티켓은 1회 이용 가능한 디지털 티켓과 매우 유사한 방법으로 설계될 수 있을 것처럼 기대되어 보인다. 즉, U가 메시지 M을 만들 때, M을 (" *P's ticket*", n, r)의 형태로 작성하는 것이다. U는 이전과 유사한 방법으로 M에 대한 I의 서명을 획득할 수 있다. 그러나 U가 사용 횟수를 I에게 속일 수 있으므로 분할 선택 방법(cut and choose procedure)을 이용하여 U가 I를 속일 수 없도록 한다. 즉, I는 U에게 n의 액수를 갖는 전자 화폐를 발급하는 것과 유사하다. 티켓의 소비 단계에서 U와 I는 $SIG_I\{M\}$을 소비하고, 사용 횟수가 1이 줄어든 새로운 디지털 티켓을 발급 단계를 시작한다. 그러나 이러한 전략은 몇 가지 문제점을 가진다. 가장 큰 문제점은 속성 4를 만족하지 못한다는 사실이다. 티켓을 소비할 때, n이 노출됨으로써 I는 티켓의 나머지 사용 횟수에 대한 정보를 정확하게 알 수 있다. 두 번째 문제점은 티켓의 소비 단계에서 매번 분할 선택 방법과 은닉 서명이 사용되어야 하기 때문에 프로토콜의 계산 비용이 너무 크다고 할 수 있다. 따라서 1회 이용 가능한 익명의 디지털 티켓을 이와 같은 방법으로 단순하게 확장시키는 접근 방법은 적절하지 못하다.

대안적인 방법으로 티켓의 발급 단계에서 1회 이용 가능한 익명의 디지털 티켓을 n개 발급 하는 방법을 고려할 수 있다. 이 경우에 U가 발급 받은 n개의 티켓에 대한 데이터에 대한 연관성(data linkability)이 없으므로 속성 4를 만족하는 것을 쉽게 알 수 있다. 하지만, 티켓의 관련된 정보를 저장하기 위하여 사용 횟수에 따라서 선형적인 공간 비용이 필요하게 된다. 또한, U가 임의로 티켓의 일부를 다른 사용자들에게 분배 가능하다는 점에서 자연스러운 n회 이용 가능한 익명의 티켓이라고 보기 힘들다. 무엇보다 가장 큰 문제점은 n회 이용 가능한 익명의 티켓을 위해서 n개의 고유한 난수가 필요하다는 점이다. 이러한 단점은 r을 고르는 정의역(domain)이 커져야 한다는 점에서 치명적이라고 할 수 있다.

본 논문에서는 이러한 문제점들을 모두 해결한 n회 이용 가

능한 새로운 익명의 디지털 티켓을 제안한다.

3. 2. 1. *n* 회용 티켓의 발급

U 는 분할 선택 방법을 이용하기 위하여 임의의 수를 *k* 개 선택한다. 이때 선택된 각 수를 r_i라고 놓는다. *U* 는 각 r_i와 자신의 신분을 나타내는 *Username* 을 이용하여 메시지 M = (*Username* , r_i)을 만들고, 일 방향 함수 H로부터 H(M)을 계산한다. 이때 계산된 H(M)을 $x_{i,0}$라고 놓는다. *U* 는 계속해서 차례로 함수 H를 적용하여 다음의 연속된 값들을 구한다.

$$x_{i,0},\ x_{i,1},\ x_{i,2},\cdots,\ x_{i,n},\ x_{i,n+1}$$

이때, *j* 가 1부터 *n* + 1 사이의 수인 경우에 $x_{i,j}$는 $x_{i,j} = H(x_{i,j-1})$의 식을 만족한다. *U* 는 1부터 *k* 사이의 모든 *i* 에 대해서 $x_{i,n+1}$를 은닉하고, 은닉한 모든 $b(x_{i,n+1})$를 *I* 에게 보낸다. *I* 는 은닉된 메시지 중 하나인 $b(x_{i,n+1})$를 임의로 선택하여 서명하고, *U* 가 자신을 속이지 않았는지를 검사하기 위해서 나머지 *k* - 1개의 은닉된 메시지에 대해서 *U* 가 공개하기를 요구한다. *U* 는 요구 받은 모든 *i* 에 대하여 r_i와 $b(x_{i,n+1})$에서 $x_{i,n+1}$를 계산할 수 있는 언바인드 키(unbind key)를 보낸다. *I* 는 공개된 모든 $x_{i,n+1}$가 적절한지를 확인하고 *U* 에게 $SIG_I\{b(x_{i,n+1})\}$를 보낸다. *U* 는 받은 $SIG_I\{b(x_{i,n+1})\}$에 대하여 *I* 의 서명을 검증하고, $SIG_I\{x_{i,n+1}\}$을 계산하여 보관한다.

3. 2. 2. *n* 회용 티켓의 소비

U 는 $SIG_I\{x_{i,n+1}\}$와 $x_{i,n}$을 *I* 에게 보낸다. *I* 는 $SIG_I\{x_{i,n+1}\}$에대한 서명을 검증하고, $x_{i,n+1} = H(x_{i,n})$인지를 확인한다. 만약 이 두 가지 검사에서 아무 이상이 없으면, *I* 는 티켓의 중복 사용 여부를 검사한다. 즉, $x_{i,n+1}$이 이전에 사용된 적이 없는 새로운 값인지를 확인한다. *I* 는 새로운 티켓이라고 판단될 경우에 티켓의 권한에 해당하는 서비스를 *U* 에게 제공한 뒤, $x_{i,n}$에 서명한다. 서명한 $SIG_I\{x_{i,n}\}$을 *U* 에게 보낸다. 티켓의 중복 사용을 막기 위해서 $x_{i,n+1}$을 기록한다.

3. 2. 3 *n* 회용 티켓의 안전성

티켓의 위조 가능성은 *I* 의 디지털 서명의 안전성에 기반한다. 그러나 만약 최초의 메시지 M = (*Username* , r_i)가 없다면, *U* 는 발급 받은 디지털 티켓의 사용 횟수를 조작할 수 있다. M에 포함된 *Username* 은 분할 선택 방법을 적용할 때, *U* 가 사용 횟수를 속이지 않았다는 것을 증명하는데 사용된다. 티켓의 중복 사용 문제는 *I* 가 소비된 티켓의 $x_{i,s}$를 항상 기록하기 때문에 쉽게 방지할 수 있다. 속성 3인 익명성은 일 방향 함수의 안전성에 기반한다.
속성 4 역시 일 방향 함수의 안전성에 기반한다. 일 방향 함수 H가 순열(permutation)인 경우에, *I* 는 사용된 티켓의 나머지 사용 횟수가 *q* 인 경우와 *w* 인 각각의 경우를 구분할 수 없다.

4. 결론 및 향후 과제

본 논문에서는 익명성이라는 부가적인 특성을 추가한 익명성을 보장하는 디지털 티켓에 대한 프로토콜을 제안하였다. 익명의 디지털 티켓은 전자 화폐와 유사하지만, 전자 화폐는 지불 시에 액수에 대한 정보를 공개하는 반면에 익명의 디지털 티켓 은 사용 횟수에 대한 정보를 노출시키지 않는다. 제안된 프로토콜은 익명의 디지털 티켓의 모든 속성들을 만족시킬 뿐만 아니라, 계산이 간단하고 효율적이므로 실제적인 구현에 용이할 것으로 기대된다.
그러나 현재 제안된 프로토콜은 사용자의 익명성을 보장하는 반면에 동일한 사용자의 복수의 접근에 대한 비연관성(unlinkability)은 보장하지 못 한다. 향후에는 사용자의 복수의 접근에 대한 비연관성까지 보장하는 프로토콜에 대해서 연구하고자 한다.

참고문헌

[1] N. Asokan, P. A. Janson, Michael Steiner, and M. Waidner, " The State of the Art in Electronic Payment Systems," *IEEE Computer*, Sep., pp. 28-35, 1997.

[2] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, " Copy Prevention Scheme for Right Trading Infrastructure, " *4th Smart Card Research and Advanced Application Conference*, Sep., 2000.

[3] Stuart G. Stubblebine and Paul F. Syverson, " Authentic Attributes with Fine-Grained Anonymity Protection," *Financial Cryptography*, 2000.

[4] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro, " The Millicent Protocol for Inexpensive Electronic Commerce," *In proceedings of WWW4, http://www.w3.org/Conferences/WWW-W4/Papers/246/.*

[5] Peter Wayner, " Digital Cash, " *Academic Press Ltd.*, 1997.

[6] The NetBill Electronic Commerce Project, http://www.ini.cmu.edu/netbill.

[7] Secure Electronic Transaction (SET) specifications, http://www.mastercard.com/set/

[8] The Wall Street Journal Online, http://www.wsj.com.

[9] T. Okamoto and K. Ohta, " Universal Electronic Cash," *In Advances in Cryptology, Proceedings of CRYPTO ' 91, J. Feigenbaum (Ed.), LNCS 576*, pp. 324-337, 1991.

[10] K. Fujimura and Y. Nakajima, " General-purpose Digital Ticket Framework," *3rd USENIX Workshop on Electronic Commerce*, pp. 177-186, 1998.

[11] E-Stamp Corporation, " E-Stamp," http://www.e-stamp.com/

[12] Gold & Silver Reserve, Inc., " e-gold," http://www.e-gold.com/

[13] Silvio Micali and Ronald L. Rivest, " Micropayments Revisited," *Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, pp. 149 - 163, 2002.