전자상거래에서의 디지털-티켓 유통 프로토콜

박복녕[0] 김태윤
고려대학교 컴퓨터학과
happy[0]@netlab.korea.ac.kr

Digital-Ticket Circulation Protocol of E-Commerce

Bok-Nyong Park[0] Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

현재의 전자상거래는 어떠한 물건이나 권리에 대해 거래할 경우 신용카드나 전자 화폐를 통한 유통과, 티켓 소유자의 특정한 권리를 보증하는 증명서 역할을 하는 디지털-티켓[1]에 의한 유통이 이루어지고 있다. 티켓 유통이 실행되면서 디지털-티켓은 악의의 사용자나 공급자로부터 티켓의 복제, 변경, 위조로부터의 보호와 사용자의 인증과 부인방지가 요구된다. 이에 본 논문에서는 디지털-티켓 시스템에 공개키 암호 기술과 토큰을 이용하여 프로토콜을 설계하여 티켓의 정당성과 유효성을 검증하고 신뢰된 티켓검증서버(*TVS : Ticket Verification Server*)를 통하여 티켓 소유자의 소유권을 검증하는 디지털-티켓 유통 프로토콜을 제안한다. *TVS*는 인터넷에 연결되어 사용자가 언제든지 자신만이 티켓의 유일한 소유자라는 것을 확인할 수 있고 소유한 티켓의 유효성을 검증할 수 있다.

1. 서론

현재 전자상거래는 인터넷 상에서 계속적으로 발전하고 있고 사람들의 생활에 일부가 되고 있다. 인터넷을 통한 전자상거래는 실생활의 상거래보다 편리함과 효율성을 가지고 있어서 사용자 수가 급증하고 있다. 현재의 전자상거래는 어떠한 물건이나 권리에 대해 거래할 경우, 신용카드나 전자 화폐를 통한 유통을 주로 하고 있고, 최근에는 극장표나 항공권 또는 그 밖의 상품에 대한 권리를 디지털화한 디지털-티켓이 제안되고 있다. 디지털-티켓 응용의 예로는 소프트웨어 라이센스, 콘서트 티켓, 비행기 표, 쿠폰 등이 있다.

디지털-티켓은 사용자가 발행자에게 티켓 발행을 요구하여 티켓을 발행 받고 이 티켓은 다른 사용자에게 전송될 수 있으며 최종의 티켓 소유자는 서비스 공급자에게 티켓을 제시하여 티켓에 대한 서비스나 상품을 제공받는다. 이러한 디지털-티켓이 유통됨에 따라 티켓 유통 참여자 상호간에 합법적인 참여자인지에 대한 인증이 요구되고, 유통되는 티켓은 유통 중에 악의적인 사용자나 공급자로부터 복제, 변경, 위조되지 않아 티켓이 안전하게 유통되어야 한다. 또한 티켓의 상환이나 전송시에 유통 상대자의 부인 방지가 요구된다.

본 논문에서는 [1]에서 제안된 디지털-티켓에 공개키 암호 기술을 이용하여 티켓의 정당성과 티켓 소유자의 소유권의 유효성 검증을 제공하는 디지털-티켓 유통 프로토콜을 제안한다. 본 논문에서 제안한 디지털-티켓 유통 프로토콜은 사용자의 요구에 티켓을 발행하는 티켓 발행 프로토콜, 소유한 티켓을 다른 사용자에게 전송하는 티켓 전송 프로토콜, 서비스 공급자에게 티켓에 명시된 서비스나 상품의 상환을 요구하는 티켓 상환 프로토콜로 구성된다[2]. 제안하는 티켓 유통 프로토콜은 공개키 암호 기술을 이용하여 티켓의 재발행, 악의적인 사용자에 의한 티켓의 위조 또는 변경 등으로부터 보호하여 티켓의 정당성을 검증할 수 있고 전송자의 서명으로 부인방지의 기능을 갖는다. 또한 티켓 소유자는 인터넷에 연결되어 있는 *TTP(Trusted Third Party)*에 의한 티켓검증서버 *TVS(Ticket Verification Server)*를 통해 언제든지 티켓 소유자의 소유권의 유일성과 티켓의 유효성을 확인할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 디지털-티켓의 유통 구조와 티켓 요구 사항에 대해 설명한다. 3장에서는 공개키 암호 기술과 디지털 서명, 토큰을 이용한 티켓 발생, 전송, 상환 프로토콜을 설명하고 4장에서는 제안된 프로토콜의 성능을 분석한다. 5장에서는 결론에 대해 설명한다.

2. 디지털-티켓 프레임워크

본 논문의 디지털-티켓 프로토콜은 디지털-티켓 프레임워크[1][2]에 기반하여 기술한다. 본 장에서는 논문에서 다루는 프레임워크의 유통 구조(Circulation System)와 요구 사항을 소개한다.

2.1 유통 구조

본 논문에서 제안하는 디지털-티켓 프레임워크의 유통 구조는 참여자와 트랜잭션으로 구분된다.

디지털-티켓의 참여자는 발행자, 사용자, 서비스 공급자로 구성된다. 발행자(Issuer)는 티켓의 발행과 티켓에 서명을 생성하고, 사용자(User)는 다른 사용자에게 발행된 티켓을 전송하고 서비스 공급자에게 티켓에 대한 상환 요구를 하며, 서비스 공급자(Service Provider)는 사용자에 의해 제시된 티켓의 권리에 대한 서비스나 명시되어 있는 임무를 이행한다.

디지털-티켓 유통 시스템에서 사용되는 트랜잭션은 발행(Issue), 전송(Transfer), 상환(Redemption)으로 구성되어 있다[2]. 발행 트랜잭션은 발생자가 사용자에게 티켓의 소유권을 주는 행위이고, 전송 트랜잭션은 티켓 소유자가 다른 사용자에게 티켓의 소유권을 주는 행위이며, 상환 트랜잭션은 티켓에 의해 제시된 티켓의 권리를 서비스 공급자에게 상환하는 행위로, 상환된 티켓이 존속되는 라이센스나 여권같은 상환(presentation)과 이벤트 티켓이나 전화카드같이 시간에 따라 유효성이 감소하는 티켓의 상환(consumption)이 있다.

디지털-티켓은 발행, 전송, 상환 트랜잭션을 이용하여 참여자

들 사이에 *I->U0-> U1->...-> Un->SP*로 유통된다[2]. *I*는 티켓 발행자, *U*는 티켓의 소유자, *SP*는 서비스 공급자를 말한다.

발행자는 티켓 발행시 검증서버로부터 발행되는 티켓 고유의 일련번호를 부여받아 티켓과 같이 전송한다(티켓에 일련번호 저장). 즉, 디지털-티켓 T = *{TypeID, TicketID, Ticketvalidity, IssureID, Promise, OwnerID, Signature, sn}* 으로 정의되고 유통시에는 간단하게 $T = SignedI(I,P,U)$로 정의된다[2]. *P*는 티켓 소유자와 약속된 티켓 권리를 말한다[1]. 일련번호는 티켓의 재발행을 금지한다. 전송 트랜잭션에서는 전송 증명서 $T_{list} = Signed_{U_0}(U_0, transfer(T), U_1)$를 같이 전송하고 상환 트랜잭션에서는 상환 증명서 $Tr = Signed_U(U, redeem(T), SP)$가 같이 전송된다[2].

사용자는 티켓 발행자에게 비행기 표나 콘서트 표 등 자신이 원하는 티켓의 발행을 요구하여 티켓을 발행 받는다. 티켓 소유자는 다른 사용자에게 티켓을 소유권을 전달 할 수 있다. 마지막 티켓 소유자는 서비스 공급자에게 티켓을 제시하여 티켓 소유권의 정당성을 확인 후에 티켓에 명시되어있는 서비스나 상품을 제공받는다. 각각의 과정에서는 논문에서 제안하는 프로토콜과 *TVS*(*TVS*는 *TTP*이다)을 통하여 티켓 소유자의 정당성과 티켓의 유효성을 검증할 수 있다. 그림 1은 티켓 유통 구조를 나타낸다[6].

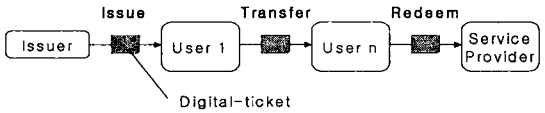

그림 1 티켓 유통 구조

2.2 요구 사항

디지털-티켓을 이용한 서비스 유통 기법에서 고려해야 할 요구 사항으로는 아래와 같은 것들이 있다[1].

- 복제(DUPLICATION) : 티켓은 원본만이 존재해야 하며 복사되어서는 안된다.
- 변경(ALTERATION) : 티켓의 권리를 불법적으로 변경해서 허가받은 서비스는 제공받아서는 안된다.
- 위조(FORGERY) : 위조를 통해 인정된 티켓이 유통되어서는 안된다.
- 재발행(REPRODUCTION) : 이미 발행된 디지털-티켓이 재발행되어서는 안된다.
- 부인방지(NON-REPUDIATION) : 디지털 권리 유통은 디지털-티켓 유통상에서 발행, 전송, 상환등에서 유통의 상대자가 나중에 거절이나 부정하지 못하게 해야한다.
- 비밀보증(ENSURING PRIVACY) : 디지털-티켓의 유통시에 참여자들의 비밀키나 공개키가 쉽게 노출되어서는 안된다.

3. 제안한 디지털-티켓 유통 프로토콜

디지털-티켓은 악의적인 사용자나 서비스 공급자로부터 보호되어야 하고, 복제 및 위조, 변경, 재상환 또는 재발행 등으로부터 안전해야 한다. 이 장에서는 각각의 트랜잭션에 적합한 프로토콜을 제안한다.

3.1 티켓 발행 프로토콜

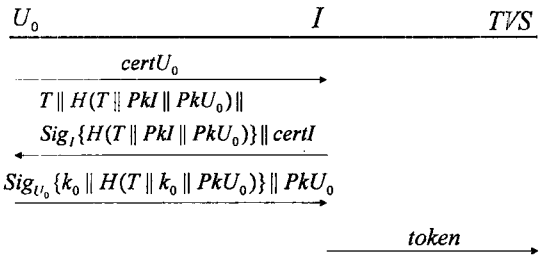

그림 2 티켓 발행 프로토콜

그림 2의 티켓 발행 프로토콜이 시작되면 사용자 U_0가 발행자 *I*에게 티켓 발행을 요청 후 발행자 *I*와 사용자 U_0는 자신들의 공개키 *PkI*, *PkU*를 교환해서 가지고 있다. U_0는 자신의 인증서 $certU_0$를 *I*에 전송한다. *I*는 티켓 *T*와 해쉬함수로 처리한 $H(T||PkI||PkU_0)$와 이 데이터를 서명한 $Sig_I\{H(T||PkI||PkU_0)\}$와 자신의 증명서 *certI*를 U_0에 전송한다. 사용자 U_0는 가지고 있던 공개키와 전송받은 증명서로 정당한 사용자인지 검증하고 발행자에게 서명된 $Sig_I\{H(T||PkI||PkU_0)\}$와 $H(T||PkI||PkU_0)$를 비교하여 이 정보가 확실히 발행자로부터 생성되어 전송되었다는 것을 검증하고 인정한다. U_0는 난수를 이용하여 티켓의 키 k_0을 만들어 공개키 PkU_0와 해쉬 함수로 처리한 티켓 *T*와 티켓 키 k_0, 공개키 PkU_0를 *I*에 전송한다. 발행자 *I*는 전송받은 티켓 *T*와 $H(PkU_0)$와 PkU_0의 해쉬값을 비교하여 사용자를 검증한 후 토큰 $token=(H(T), H(PkI), H(K_0))$을 만들어 *TVS*에 전송한다. 이것은 티켓 티켓과 티켓 키 값의 비교로 소유자가 정당한 티켓을 소유하고 있음을 확인할 수 있다.

3.2 티켓 전송 프로토콜

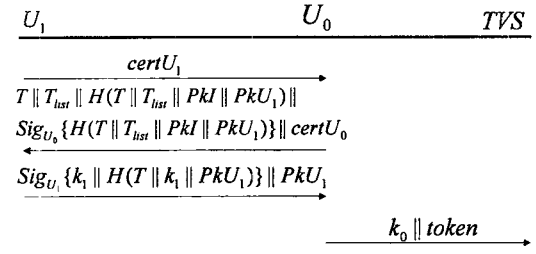

그림 3 티켓 전송 프로토콜

그림 3의 티켓 전송 프로토콜)이 시작되면 사용자 U_0는 사용자 U_1에게 티켓을 전달하기 위해서 각자의 공개키를 교환하고 사용자 U_0는 티켓확인을 위해 발행자의 공개키 *PkI*를 보내고, 사용자 U_1의 인증서 $certU_1$을 전달받아 가지고 있다. 사용자 U_0는 U_1에게 티켓 *T*와 티켓 전달 증명서 T_{list}와 해쉬 함수로 처리한 티켓 *T*, 티켓 전달 증명서 T_{list}, 공개키 *PkI*와, PkU_1을 서명된 $Sig_{U_0}\{H(T||T_{list}||PkI||PkU_1)\}$과 인증서 $certU_0$를 사용자 U_1에 전송한다. 사용자 U_1은 가지고 있던 PkU_1과 인증서로 정당한 사용자인지 검증하고, $Sig_{U_0}\{H(T||T_{list}||PkI||PkU_1)\}$와 $H(T||T_{list}||PkI||PkU_1)$을 비교하여 티켓이 발행자 *I*로부터 발행된 정당한 티켓임을 검증하고 티켓의 유효성을 인정한다. 사용자 U_1은 새로운 티켓 키 k_1을 생성하여 $H(T||k_1||PkU_1)$와 함

께 서명하여 공개키 PkU_1과 함께 U_0에 전송한다. 사용자 U_0는 티켓과 사용자 U_1의 공개키를 비교하여 검증한 후 새로운 토큰 $token=(H(T), H(PkI), H(k_1))$을 만들어 가지고 있던 k_0과 TVS로 전송한다. TVS는 가지고 있던 $H(k_0)$와 전송받은 k_0의 해쉬값을 비교하여 일치하면 토큰을 새로받은 토큰으로 교체한다.

3.3 티켓 상환 프로토콜

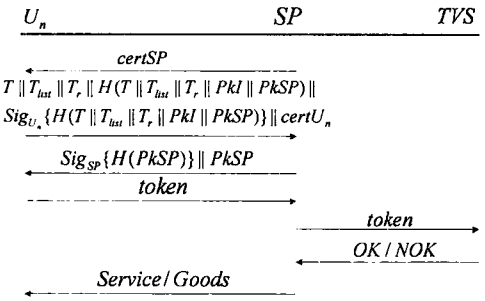

그림 4 티켓 상환 프로토콜

그림 4의 티켓 상환 프로토콜이 시작되면 최종의 티켓 소유자인 사용자 U_n은 서비스 공급자에게 티켓 상환을 요구한다. 사용자 U_n과 서비스 공급자 SP는 서로의 공개키와 각자의 인증서를 교환하여 가지고 있다. 사용자는 상환 증명서 Tr과 그 밖의 정보를 서비스 공급자에게 전송한다. 전송 프로토콜과 같은 방법으로 서로의 공개키와 인증서, 서명등을 이용하여 정당한 사용자와 서비스 공급자임을 검증한다. 사용자 U_n은 가지고 있던 토큰을 서비스 공급자 SP에게 전송한다. 서비스 공급자는 이 토큰을 TVS에 전송하여 정당한 티켓의 토큰인지 확인한다. TVS는 전송받은 토큰과 가지고 있던 토큰을 비교하여 일치하면 이 토큰의 정보를 삭제한 후 서비스 공급자 SP에 OK 메시지를 전송한다. 서비스 공급자는 OK 메시지를 받으면 티켓에 나타나있는 서비스나 상품을 사용자에게 제공한다.

4. 성능 분석

본 논문에서 제안한 프로토콜은 공개키 암호 기술과 디지털 서명 등으로 유통 참여자의 신원을 검증할 수 있고, 전달 증명서와 상환 증명서로 티켓의 소유권 이동을 확인할 수 있다. 또한 티켓의 유효성과 정당성을 검증할 수 있고, 티켓 키 k를 이용하여 악의 적인 사용자의 티켓 복제로부터 티켓 소유권의 유일성을 확인할 수 있으며, 언제든지 티켓 소유자는 TVS를 통하여 티켓의 소유권을 확인 할 수 있다. 티켓에는 일련번호를 부여하여 티켓의 재발행을 금지한다.

- 복제 : 정당하지 못한 사용자는 티켓을 복제하여 사용할 수 있다. 그러나 티켓 사용 프로토콜에서의 서명을 생성해 낼 수 없으므로 티켓의 복제 사용은 방지될 수 있다.
- 변경 : 티켓의 변경은 논문에서 제시한 토큰의 확인으로 막을 수 있다. 티켓을 변경하였을 경우 티켓을 해쉬 함수로 처리할 경우 해쉬값이 바뀌기 때문에 토큰의 $H(T)$와 티켓 T의 해쉬값의 비교로 티켓이 변경되어 정당하지 않음을 알 수 있다.
- 위조 : 티켓의 위조는 TVS에 저장된 토큰 $H(PkI||k||T)$과 입력받은 토큰 값의 비교로 막을 수 있다. 또한 발행 프로토콜에서의 $H(T||PkI||PkU_0)$와 $Sig_k\{H(T||PkI||PkU_0)\}$, $H(PkI)$와 전송받은 PkI의 해쉬값의 비교로 위조되었는지 검증할 수 있다.
- 재발행 : 티켓에 삽입한 일련번호 sn의 확인으로 가능하다. 즉, 이미 부여된 일련 번호를 다시 부여하지 않으므로 티켓의 재발행을 막을 수 있다.
- 부인방지 : 유통의 상대자가 나중에 그 사실을 부정하지 못하게 해야한다. 이것은 티켓과 각각의 프로토콜에서 사용한 발송자의 서명 $Sigx$로 부인방지를 할 수 있다.
- 비밀 보증 : 프로토콜에서 사용한 공개키 암호 기술과 디지털-서명과 해쉬 함수의 이용으로 비밀 보증이 가능하다.
- 상호 인증 : 참여자 상호간에 공개키와 PkX와 증명서 $certX$로 서로 상대방을 인증하므로 상호 인증이 가능하다.
- 소유권 확인 : 사용자는 TVS를 통해 소유하고 있는 토큰의 비교로 언제든이 자신의 티켓의 유효하다는 것과 티켓 소유권의 유일성을 확인할 수 있다.
- TVS는 신뢰된 서버로 티켓의 토큰을 저장하여 사용자가 티켓의 유효성 검증을 원할 때 언제든 검증을 해주고, 티켓 소유자가 티켓의 유일한 소유자인 것을 확인해준다. 또한 상환 프로토콜에서 서비스 공급자의 요구로 사용자 티켓의 유효성을 확인하여준다.

5. 결론

전자상거래의 발달과 디지털-티켓의 유통으로 인해, 디지털-티켓은 악의의 사용자나 공급자로부터 티켓의 복제, 변경, 위조로부터의 보호와 사용자의 인증과 부인방지가 요구된다.

본 논문에서는 디지털-티켓 유통에 있어 공개키 암호 기술과 디지털 서명 등을 이용하여 상호간의 인증과 티켓의 정당성과 유효성을 검증하고 인터넷에 연결된 티켓검증서버 TVS를 통하여 티켓의 소유자가 언제나 티켓 소유권의 유효성을 확인 할 수 있는 디지털-티켓 유통 프로토콜을 제안하였다. 제안한 프로토콜은 공개키 암호 기술과 디지털 서명을 이용하여 상호 인증과 기밀성을 제공하고 티켓의 일련 번호를 통해 중복 발행을 막으며 악의의 사용자로부터 티켓의 복제 및 위조를 막을 수 있어 디지털-티켓 유통 참여자는 보다 안전성 측면에서 개선된 티켓 유통을 할 수 있다.

참고문헌

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

[2] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and Sekine, "Digital-Ticket-Controlled Digital Ticket Circulation", 8th USENIX Security Symposium, August 1999.

[3] W. Diffie and M.E. Hellman, "New Directions in Cryptography". IEEE Transaction on Information Theo, Vol. IT-22, No.6, pp.644-654, Nov. 1976.

[4] Schneier, Bruce, "Applied Cryptography, Second Edition", Essential reference for cryptographic engineers by the foremost pundit in the field, Wiley, 1996.

[5] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Right Trading Infrastructure", 4th Smart Card Research and Advanced Application Conference (CARDIS 2000), September 2000.

[6] Matsuyama, K. and Fujimura, K. "Distributed digital-ticket management for right trading system", In Proceedings of the 1st ACM Conference on Electronic Commerce, 1999.