2004년도

한국 정보보호학회 하계학술대회 최종논문 제출본

디지털 컨텐츠 거래에서의 사용자 익명성 보장 기법

강석규, 김광조

한국정보통신대학교, 국제정보보호기술연구소

Preserving User-Privacy for Digital Contents

Seok-kyu Kang and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

요 약

웹을 기반으로 하는 전자 상거래에 있어 사용자의 프라이버시 보호는 중요한 문제 중 하나이다. 사용자의 구매패턴이나 정보등이 침해되거나 악용될 수 있으며, 따라서 대다수의 사용자들은 이러한 문제에 매우 민감해 하고 있다. 특히 웹을 통한 디지털 컨텐츠 거래에 있어서 고객의 정보를 익명화 할 수 있는 기법들이 소개되었지만, 지불과정 특성상 고객의 정보를 제공해야 하기 때문에 제한적인 익명성을 제공한다. 본 논문에서는 디지털 컨텐츠 거래에 있어서 익명 채널과 공개 채널을 혼용하여 기존의 지불절차 환경에서도 고객에게 효과적인 익명성을 제공함과 동시에 판매자에게 필요한 정보를 제공할 수 있는 방식을 제안한다.

I. 서론

인터넷을 활용한 전자 상거래가 활발하게 이루어지고, 그 중요성 또한 증가하고 있는 지금의 환경 하에선 소비자의 프라이버시 문제는 더 이상 간과할 수 있는 문제가 아니다. 웹을 기반으로 하는 많은 기업들은 자신들의 사업적 이익을 위해 고객의 프라이버시를 침해하거나 그에 따라 많은 전자상거래 이용자들이 개인정보 유출 문제를 아주 심각하게 받아들이고 있다.

지금까지 전자상거래시 고객의 프라이버시를 보호할 수 있는 시스템들이 몇 가지 제안되었다. 이들 시스템에서는 고객의 프라이버시 보호를 위해 제품 검색정보를 익명으로 처리하고, 실제 제품을 구매할 경우 지불 프로세스에서 고객의 정보를 제공하거나[1], 혹은 판매자의 제품정보, 암호키 그리고 암호화된 컨텐츠로 구성된 secure package를 사용자가 다운로드 받아 PIR(Private Information Retrieval)을 응용하여 해당 컨텐츠를 복호화 할 수 있는 키를 얻음으로써 고객의 익명성을 보장한다.[2] 이 시스템에서는 고객의 익명성을 충분히 보장하지만, 판매자의 입장에서 사업적으로 필요한 정보까지 숨기게 되므로 그리 현실적이지 못하다고 볼 수 있다. 따라서 고객의 제품 browsing정보나 구매정보에 대한 익명성을 보장함과 동시에 판매자에게 제품판매에 대한 정보를 동시에 제공하는 시스템이 현실적으로 필요하고 설계할 필요가 있다고 볼 수 있다.

이에 따라 본 고는 고객의 컨텐츠구매 패턴 정보를 익명화 하여 프라이버시 보호를 보장하고, 동시에 판매자에게 고객의 구매정보를 제외한 컨텐츠판매정보들을 제공하여 실제 적용 가능한 시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 제안된 시스템 구조와 관련된 관련 연구들에 대해 간략하게 서술하고 제 3장에서는 고객의 익명성과 판매자에게 필요한 정보를 보장하는 시스템 구조를 제안한다. 제 4장에서는 지금까지 제안된 관련 시스템과 본 논문에서 제안된 시스템을 비교해 보고, 마지막 제 5장에서 결론을 끝으로 본 논문을 마무리 짓고자 한다.

II. 관련연구

1. PKI와 익명채널을 이용한 모델[1]

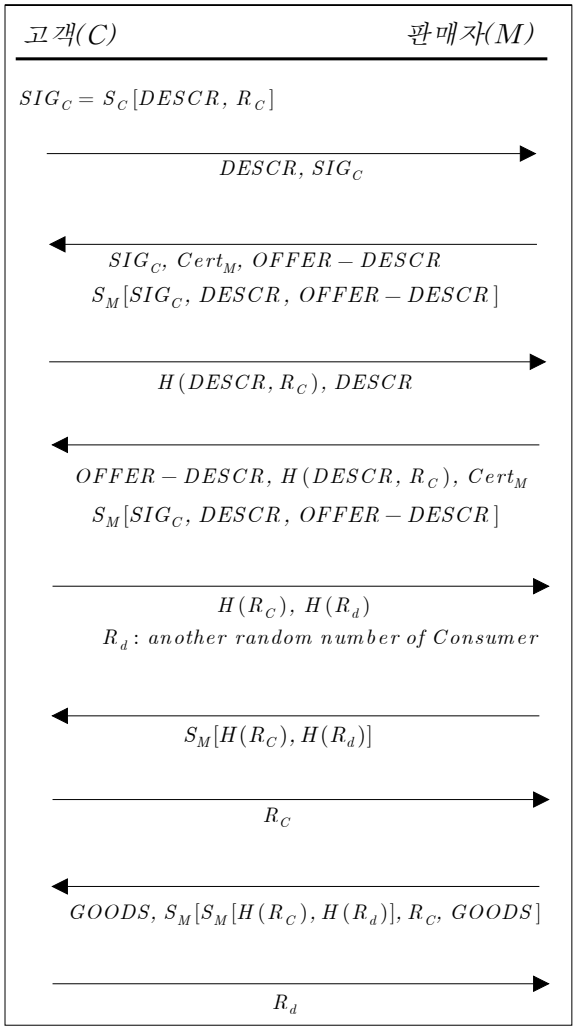
본 모델은 1996년 Hauser와 Tsudik이 제안한 PKI 환경과 익명채널을 이용하여 익명 전자 상거래 활동

방법을 제공한다. 여기서는 고객의 전자상거래 활동을 크게 Pre-Purchase Browsing(PPB)단계와 Electronic Merchandise Deliverry(EMD)단계로 나누며 이 두 단계에서만 익명성을 제공하고, 지불단계에서의 익명성 보장은 고려하고 있지 않다.

1) 기호

$H()$: 일방향 해쉬함수 (SHA-1 또는 MD5)
PK_x : 개체 X의 공개키
SK_x : 개체 X의 비밀키
$S_x[text]$: 비밀키 SK를 이용한 서명.
즉, $S_x[text] = SK_x[H(text)]$
R_x : 개체 X의 랜덤 수(nonce)
$Cert_x$: 개체 X의 공개키 인증서, PK_x를 가짐.
DESCR : 구매하고자 하는 아이템정보
OFFER-DESCR : 판매하고자 하는 아이템정보

2) 프로토콜



<그림 1> PPB와 EMD 프로토콜

3) 문제점

PKI와 익명채널을 이용한 본 모델은 앞서 언급한 바와 같이 크게 PPB 단계와 EMD단계로 나뉘어 고객에게 익명성을 제공하고 있다. 익명채널을 기반으로 하여 해쉬함수와 공개키 암호 서명기법을 통해 고객은 PPB와 EMD단계에서 익명성을 제공받는다. 하지만 만약 고객이 제품을 구매하고자 할 때, 고객은 지불을 위해 자신의 정보를 제공해야하며, 여기서 고객에 대한 완전한 익명성 보장은 깨지게 된다. 또 다른 문제점은 만약 시스템이 판매자에 의한 익명 지불 프로세스를 지원하고자 할 경우 독립된 제 3의 신뢰기관(Third Trust Party)을 두어 고객의 R_c와 $Cert_M$을 전달하면, 판매자에게 고객의 구매정보를 숨길 수 있으나, 이 경우 TTP가 고객의 모든 정보를 알게 되므로 완전한 고객정보 익명성 보장은 힘들다고 볼 수 있다.

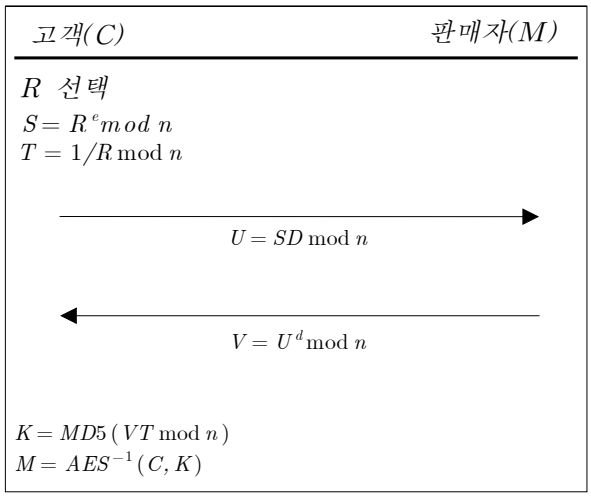
2. PIR(Private Information Retrieval)응용 모델

이 모델은 2001년 Bao와 Deng이 PIR개념[3][5]을 이용한 디지털 컨텐츠 거래에서 고객의 구매정보 익명성을 제공하기 위해 제안했다[2]. 고객은 지불에 필요한 개인정보를 제공하여야 하지만, 고객이 어떠한 제품을 구매했는가는 판매자 입장에서 알 수 없다. 이러한 기능을 제공하기 위하여 판매자는 미리 간략한 제품정보, 암호화된 암호키 그리고 암호화된 디지털 컨텐츠를 생성하여, 구매자는 무료로 이를 다운로드 받을 수 있다. 만약 구매자가 해당 컨텐츠를 구매하고자 하면, 구매자는 독립된 Transaction Server(TS)로부터 해당 컨텐츠에 대한 키를 부여받는다. 물론 지불에 관한 모든 프로세스는 이 TS와 이루어진다. 다음 절에서는 TS와 고객 사이에서의 대략적인 키 획득 프로토콜을 설명하고자 한다.

1) 기호

R : 1023비트의 랜덤 수
e : TS의 공개키
d : TS의 비밀키
n : $p \times q$, $p=2p'+1$, $q=2q'+1$, p와q는 소수
C : AES(Advanced Encryption Standard)[4]로 암호화된 디지털 컨텐츠
D : 컨텐츠 복호화를 위한 암호화된 키
M : 평문의 디지털 컨텐츠

2) 프로토콜



<그림 2> 키 획득 프로토콜

3) 문제점

Bao와 Deng이 제안한 이 모델은 고객입장에서의 구매정보 익명성을 충실히 제공하는 반면, 판매자를 위한 정보, 예를 들어 제품의 판매량, 판매일자, 재고파악 등 여러 가지 유효한 정보를 획득하기 힘들다. 왜냐하면, 키 획득과정에서 고객이 제공하는 $U = SD_j \bmod n$의 D_j값을 TS가 알 수 없기 때문이며, 단순히 TS는 고객으로부터 받은 U를 통해 $V = U^d \bmod n$ 을 계산하고, 다시 이를 전송하여 고객이 V를 통해 해당 컨텐츠의 암호키를 획득하기 때문이다. 따라서 TS나 판매자는 고객이 구매한 컨텐츠의 어떠한 정보도 획득할 수 없다.

또 다른 문제점은 만약 고객이 동시에 복수 개의 컨텐츠를 구매할 경우 고객은 한 컨텐츠에 대한 암호키를 획득할 수밖에 없기 때문에 구매한 컨텐츠의 개수만큼 키 획득 프로토콜을 수행해야 한다.

III. 제안기법

1. 특징

이 논문에서 제안하는 시스템은 판매자와 고객은 익명채널을 이용하며, 정당한 지불을 위해 고객은 독립된 TS와 공개된 채널을 이용한다. 하지만 위에서 언급한 두 시스템과는 달리, 제안된 방식에서는 TS와 판매자 모두 완전한 고객의 정보를 획득할 수 없다. 다시 말해 TS는 고객이 지불한 컨텐츠의 비용을 알 수 있지만, 고객이 무엇을 구매했는지는 알 수 없으며, 반대로 판매자는 어떤 고객이 해당 컨텐츠를 구매했는지 알 수 없다. 단지 어떤 컨텐츠가 판매되었는지 그리고 언제 판매되었는지 등을 알 수 있을 뿐이다. 따라서 TS와 판매자가 서로 담합하지 않는 이상 고객의 구매패턴, 구매정보 그리고 고객의 신원정보를 알 수 없게 된다.

2. 요구사항 정의

본 시스템에 대한 요구사항 정의는 다음과 같다.

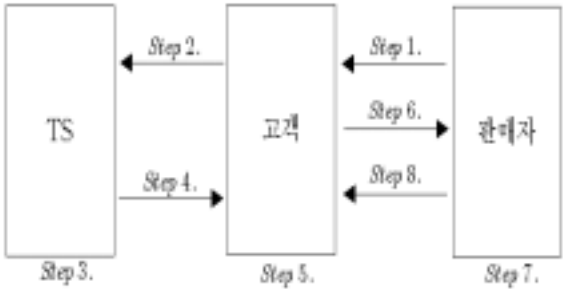
- *고객은 지불을 위해 자신의 정보를 제공해야 한다.*
- *판매자는 판매된 컨텐츠에 대한 정보만 가질 뿐 고객이 어떠한 컨텐츠를 구매했는가는 알 수 없다.*
- *판매자는 컨텐츠의 판매량, 판매일자 등을 알 수 있어야 한다.*
- *판매자와 TS는 고객의 구매패턴/정보를 얻을 수 없어야 한다.*
- *TS는 고객이 지불하는 금액에 대해 어떤 컨텐츠에 대한 금액인지 알 수 없어야 한다.*

3. 프로토콜

1) 기호

C : 샘플컨텐츠 정보
M : 디지털 컨텐츠
P : 가격 정보
K, K^{-1} : 공개키 및 비밀키
N : 랜덤 수
t : 타임 스탬프
$H()$: 일방향 해쉬 함수 (SHA-1 혹은 MD5)
$PAID$: $\{P, t, N\}_K$
$Receipt_X$: 개체 X의 *receipt*
K : 컨텐츠 암호키
E : 대칭키 암호화 알고리즘

2) 프로토콜



Step 1: 고객은 판매자가 미리 생성해 둔 $[C_i, \{P_i\}_{K_{sp}^{-1}}]$를 다운로드 받아 C_i를 확인하여 컨텐츠 구입여부를 결정한다.

Step 2: 고객이 구입을 결정하면, $\{P_i\}_{K_{sp}^{-1}}$를 TS에 전송한다.

Step 3: 고객과 TS사이에 지불절차가 끝나고 나면, TS는 $S = H(P_i \| N_{TS} \| t_i)$를 계산하여 고객의 $PAID_C = \{S, P_i, N_{TS}\}_{K_C}$와 판매자의 $PAID_M = \{S_i, P_i, N_{TS}\}_{K_M}$을 생성하여 각각을 위한 *Receipt*를 계산한다.

고객 Receipt :
$Receipt_C = \{PAID_C, t_i, H(PAID_M \| S)\}_{K_C}$

판매자 Receipt:
$Receipt_M = \{PAID_M, t_i\}_{K_M}$

만약 고객이 n개의 컨텐츠를 구매하고자 한다면, TS는 $S = H(P_1 ... P_n \| N_{TS} \| t_i)$를 계산하고, 또한 $PAID_C = \{S, P_1 ... P_n, N_{TS}\}_{K_C}$와 $PAID_M = \{S_i, P_1 ... P_n, N_{TS}\}_{K_M}$을 생성하여 *Receipt*를 계산하면 된다.

Step 4: 고객에게 $Receipt_C$와 $Receipt_M$을 전송한다.

Step 5: 고객은 TS가 올바른 P_i에 대해 바르게 처리했는지 확인하기 위해 $S = S' = H(P_i \| N_{TS} \| t_i)$를 확인한다. 그리고 TS로부터 전송받은 $Receipt_C$와 $Receipt_M$이 동일한 P_i에 대한 *Receipt*인지 확인하기 위하여, $H'(PAID_M \| S) = H(PAID_M \| S)$를 확인한다.

Step 6: 익명채널을 통하여 고객은 판매자에게 C_i와 $Receipt_M$를 전송한다.

Step 7: 판매자는 컨텐츠 암호화를 위한 키 $K_i = H(N_{TS} \| t_i)$를 이용하여 $D_i = AES(M_i, K_i)$생성한다.

Step 8: 고객 역시 자신이 소유한 N_{TS}와 t_i를 이용하여 암호키 K_i를 생성, D_i를 복호화한다.

IV. 비교분석

앞서 2장에서 논의한 바와 같이 기존에 제안된 모델에서는 고객에 대한 조건적인 익명성을 제공하고 있다. Hauser와 Tsudik이 제안한 모델은 PPB단계와 EMD단계에서는 익명채널을 이용하여 고객의 익명성을 제공하지만, 지불단계에 있어서는 고객은 판매자에게 자신의 정보를 제공하여야 한다. 만약, 이 단계에서도 익명성을 보장받고자 한다면, 고객의 정보는 TTP를 거쳐 판매자에게 전달되기 때문에 결국 TTP는 고객의 모든 정보를 알게 된다. 따라서 이 모델에서 제안하는 익명성 제공은 한계를 가진다고 볼 수 있다.

Bao와 Deng이 제안한 모델은 PIR(Private Information Retrieval)개념을 응용하여 판매자가 생성한 Secure Package를 고객이 무료로 다운로드 받고, 이를 구매하고자 할 때, 고객은 TS로부터 Blinding RSA Decryption를 기반으로 하여 키를 얻어낸다. 하지만 이 모델에서는 TS와 판매자 모두 판매된 컨텐츠에 대한 정보를 얻을 수 없기 때문에 향후 컨텐츠 로열티 지불 문제를 가지고 있다. 그리고 복수개의 컨텐츠에 대한 키 획득을 위해선 고객이 구매하고자 하는 컨텐츠의 개수만큼 키 획득 프로토콜을 반복 수행하여야 한다.

본 논문에서 제안된 프로토콜은 이 두 모델들과 비교하여 볼 때, 고객의 익명성을 충실히 보장하고 있다. 제안된 모델에서의 TS는 기존에 제안된 방식과는 달리 고객이 구매하고자 하는 컨텐츠를 알 수 없고 단지 지불 프로세스만 담당하며, 판매자는 TS가 생성한 Receipt정보를 통해 고객이 구매한 컨텐츠를 전달할 수 있다. 따라서 판매자는 판매된 컨텐츠에 대한 정보를 얻을 수 있음과 동시에 고객은 TS와 판매자 양쪽 모두에 자신의 구매와 관련된 모든 정보를 숨길 수 있게 된다. 또한, 고객이 복수개의 컨텐츠를 구매하더라도 그 개수와는 상관없이 한번의 프로토콜을 수행하게 된다.

[표 1] 기존 기법과 비교

	PKI/익명채널 이용모델[1]	PIR응용모델 [3][5]	제안 모델
판매정보 제공	○	×	○
고객 구매정보 익명성	×	○	○
익명채널이용	○	△	○

○: 만족 ×:불만족 △: 선택적

V. 결론

인터넷을 이용한 전자상거래에 있어서 고객의 익명성 보장은 매우 중요한 사안 중에 하나이다. 판매자 측에서 획득한 고객의 구매정보나 패턴 등은 유익한 방향으로 활용될 수 있으나 악용될 소지 또한 크다고 볼 수 있다. 따라서 이러한 익명성 보장을 위해 지금까지 많은 기법들이 소개되어 왔으나 거의 제한적인 익명성을 보장할 뿐이었고, 특히 지불과정을 위해선 고객의 개인 정보제공은 반드시 필요한 요구사항 중 하나였다. 본 논문에서 제안한 모델은 정상적인 지불 방식 하에서 고객의 정보를 효과적으로 익명화하고 동시에 판매자에게 필요한 정보를 제공해 줄 수 있다.

본 논문에서는 효과적으로 고객의 정보를 익명화하여 고객으로 하여금 익명 전자 상거래를 이용할 수 있음을 보였으며, 현실적인 시스템 구현의 한 방법으로써 고려해 볼 수 있을 것이다.

VI. 참고문헌

[1] R. Hauser and G. Tsudik. *On shopping incognito*. In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, pp.251-7, Oakland, California, November 1996.

[2] F. Bao and R. Deng, *Privacy Protection for Transaction of Digital Goods*, ICICS2001, Xian,China, 2001.

[3] B. Chor, O. Goldreich, E. Kushilevita, and M. Sudan, *Private Information retrieval*, In Proceedings of 36th FOCS, pp.41-50, 1995.

[4] Advanced Encryption Standard, http://csrc.nist gov/encryption/aes

[5] B. Chor and N. Gilboa, *Computational private information retrieval*, In Proceedings of 29th STOC, pp.304-313, 1997