프라이버시 보호와 서비스 차별화를 위한 분류 가능한 익명성 제공*

박용남*, 박희재**, 김 종**
*포항공과대학교 정보통신학과
**포항공과대학교 컴퓨터공학과
e-mail : gudwns03@postech.ac.kr

Providing Discriminative Anonymity for Privacy Protection and Service Differentiation

Yong-Nam Park*, Hee-Jae Park**, Jong Kim**
*Dept. of Computer and Communications Engineering, Pohang University(POSTECH)
**Dept. of Computer Science and Engineering, Pohang University(POSTECH)

요 약

인터넷을 통한 서비스 제공은 법규 준수, 사용 권한 확인, 요금 부과, 차별화된 서비스 제공 등의 다양한 이유로 사용자 인증을 필요로 한다. 이러한 확인 과정은 인증만 되면 언제 어디서든 서비스를 이용할 수 있다는 측면에서 사용자에게도 편리성을 제공해 주지만 사용자의 서비스 이용 정보가 쉽게 기록되고 노출될 수 있는 문제점을 가지고 있다. 이를 해결하기 위한 방법으로 사용자 정보를 보호하면서도 불법적인 사용자에게 악용되지 않도록 하기 위해 추적 가능한 익명성을 보장하는 방안이 제안되고 있다. 하지만 이러한 방법으로는 법 준수를 위한 서비스 제한 규정이나 사용자 별 차별화를 필요로 하는 서비스 모델을 지원하지 못한다. 본 연구에서는 사용자에게는 익명성을 보장하고 적법한 절차를 통한 추후 구매자 추적이 가능하면서도 서비스 제공자에게는 서비스 그룹별로 차별화된 서비스 제공이 가능한 새로운 익명 생성 방안과 이를 적용하는 디지털 콘텐트 구매 프로토콜을 제안하고 있다.

1. 서론

네트워크 컴퓨팅의 발전과 인터넷의 보편화를 통한 정보화 시대의 도래는 모든 정보를 디지털화 하고 이러한 정보를 사고 파는 새로운 비즈니스 모델을 탄생시켰다. 인터넷을 통한 디지털 콘텐트의 구매는 시간과 공간 측면에서 많은 편리성을 제공해 주지만 사용자의 행위가 기록된다는 점에서 심각한 사생활 침해 문제를 야기시킬 수 있다. 예를 들어 디지털 콘텐트를 보호 하기 위한 수단인 DRM(Digital Rights Management)시스템은 콘텐트에 대한 권리를 효과적으로 보호하지만 이는 또한 사용자의 개인 정보 침해 문제를 야기시키는데 대부분의 상업용 DRM 시스템에서 서비스 제공자는 사용자 확인 및 인증, 판매 기록 보관, 판매된 콘텐트의 사용내역 추적을 통하여 쉽게 사용자의 개인 정보수집이 가능하기 때문이다[2]. 이러한 문제로부터 사용자의 개인 정보를 보호하기 위한 방안으로는 익명성을 보장하거나[1,3] 서비스 제공자로부터 서비스 구매 내역을 감추는 방식 등[4,5]이 있다. 그러나 익명을 통한 구매는 사용자가 구매한 콘텐트를 불법 유통한 경우에 대비하여 구매자 추적을 위한 별도의 방안을 필요로 한다. 이를 해결하기 위하여 추적 가능한 익명성을 보장하는 연구들이 진행되었는데[6-8] 구매 시에는 익명성을 보장하고 문제 발생시 신뢰성 있는 제 3 자를 통하여 구매자의 신분을 추적한다. 하지만 실제 환경에서는 콘텐트 제공 전에도 구매자의 신분확인을 필요로 하는 경우가 생길 수 있다. 성인 전용 콘텐트나 유료회원을 위한 프리미엄 서비스 제공이 이에 속하며, 기존의 추적 가능한 익명성 보장만으로는 이를 해결할 수 없다. 이에 본 연구에서는 사용자에게는 익명성을 보장하고 적법한 절차를 통한 추후 구매자 추적이 가능하면서도 서비스 제공자에게는 서비스 그룹별로 차별화된 서비스(Service Differentiation) 제공이 가능한 새로운 익명 생성 방안과 이를 적용하는 콘텐트 구매 프로토콜을 제안하기로 한다.

본 논문은 다음과 같이 구성된다. 2 장에서는 추적 가능한 익명성에 관련된 기존연구들을 다루고 있으며, 3 장에서는 본 연구의 목적, 4 장에서는 제안하는 프로토콜의 기반기술인 그룹 서명(Group Signature)을 소개하고 있다. 5 장에서는 본 연구가 제안하는 방식에 대해 단계별로 설명하고 있으며, 6 장에서는 제안하는 방

* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(홈네트워크연구센터) 지원사업의 연구결과로 수행되었음" (IITA-2007-(C1090-0701-0035))

식에 대한 보안 분석 결과를 제시하고, 7 장에서는 결론을 기술한다.

2. 관련연구

서비스 제공자로부터 콘텐트 구매 시 사용자 정보를 보호하기 위한 방안으로는 사용자의 익명성을 보장하는 방식과 서비스 구매 내역 자체를 숨기는 방법 등이 제안되고 있다. Jiang Zhang 는 사용자가 사전 비용 지불을 통해서 토큰(token)을 구매하고 이를 사용하여 콘텐트를 요청하는 방식을 제안하고 있으며[3], C. Conrado 는 스마트 카드의 공개키 정보처럼 사용자가 소유한 디바이스의 고유한 값을 자신의 익명 아이디로 사용하는 방식을 소개하고 있다[1]. 구매 과정의 익명성을 보장하는 방법에는 OT(Oblivious Transfer)방식을 적용하여 사용자의 콘텐트 선택 정보를 숨기는 방식과[5], Commutative Cipher 기법을 적용하여 사용자가 콘텐트 사용에 필요한 라이센스를 라이센스 서버 모르게 획득할 수 있는 방법 [4] 등이 있다. Kilian 등은 추적 가능한 익명성을 확보하기 위하여 신뢰할만한 제 3 자 개념을 도입하였다[6-8]. 여기에서 사용자는 자신의 신분을 제 3 자에게 공탁(escrow)하고 익명 아이디를 부여 받아 사용 함으로서 서비스 제공자에게 자신의 신분이 추적 가능함을 보이게 된다. 이러한 방식을 신원 공탁(Identity Escrow)이라 하는데, Yong-Ho Lee 는 이를 구현하는 다양한 방법을 소개하고 있다[7]. 이러한 방법 중 하나인 그룹 서명(Group Signature)은 그룹 멤버가 그룹의 이름으로 서명하는 것을 통해 익명성을 보장받는 방식으로[9], 신원 공탁을 구현하기 위해 널리 사용되고 있다[6-8]. 그룹 서명은 그 적용 방법은 다르지만 본 논문에서도 그룹 단위의 익명성을 보장하기 위한 기반 기술로 사용되고 있으므로 4 장에서 상세히 설명하고자 한다.

3. 연구의 필요성 및 목적

이전에 제안된 연구는 사용자의 정보 보호를 위해 익명성을, 불법 사용 방지를 위해 추적성(Traceability)을 제공하지만 이러한 방식으로는 법 준수를 위한 서비스 제한이나 고객 유형별 차별화된 서비스를 지원하고 있는 다양한 비즈니스 모델을 지원 할 수 없다. 본 논문에서 우리는 기존의 추적 가능한 익명성의 장점을 유지함과 동시에 차별화된 익명성 제공이 가능한 새로운 익명 아이디 생성 방안을 제안 한다. 제안하는 방법을 통해 사용자는 자신의 신분을 밝히지 않고 공탁기관(Escrow Authority)으로부터 익명의 아이디 획득이 가능하며 서비스 제공자(Service Provider)로부터 자신의 신분을 감추면서 동시에 가입한 서비스 그룹에 따른 차별화된 서비스를 받을 수 있다.

4. 기반 기술

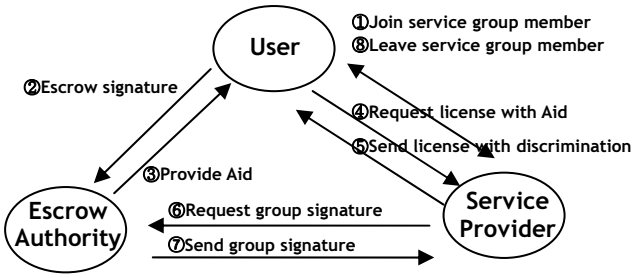
그룹서명은 그룹 멤버가 그룹의 이름으로 서명하는 것을 보장하는 디지털 서명(Digital Signature)의 한 형태로써 수신자로부터 서명자의 익명성을 보장해 주며 서명자의 신분 확인은 그룹을 관리하는 그룹 매니저(Group Manager)를 통해서만 가능하도록 설계되어 있다. 그룹 서명은 Chaum 등[9]에 의해 최초 소개 되었으며 이후 효율성과 실용성을 개선하기 위해 관련된 연구가 진행되고 있는 분야로 일반적인 그룹 서명 구조는 시스템 환경 설정 및 멤버 가입, 서명생성, 그룹 멤버 증명, 서명자의 신분확인, 그룹탈퇴 등의 기능수행을 담당하는 Setup, Sign, Verify, Open, Delete 의 프로세스로 나누어지며, 프라이버시 보호와 보안측면에서 다음과 같은 특성을 가진다[10,11].

- 익명성(Anonymity): 그룹의 이름으로 서명하기 때문에 수신자는 서명자의 신분을 알 수 없다.
- 비 연결성(Unlinkability): 수신자는 동일 그룹 멤버의 두 개의 서명 값을 구분할 수 없다
- 위조방지성(Unforgeability): 그룹내의 다른 멤버는 물론 그룹을 관리하는 그룹 매니저도 특정 그룹 멤버의 서명을 위조할 수 없다.

5. 제안하는 프로토콜

5.1 개요

제안하는 프로토콜은 서비스 그룹 가입 단계(①), 익명의 아이디 생성 및 라이센스 요청단계(②~⑤), 익명 추적 단계(⑥~⑦), 그룹 탈퇴 단계(⑧)로 구성되며 전체 처리 흐름은 (그림 1)과 같다.



(그림 1)Proposed scheme

5.2 가정

사용자 익명성을 보장하고 차별화된 서비스를 제공하기 위해 제안하는 방식은 다음과 같은 가정이 필요하다.

- 서비스 그룹의 크기는 사용자의 익명성을 훼손하지 않을 만큼 충분히 크다.
- 사용자가 가입한 서비스 그룹은 서비스 이용시점까지 변하지 않는다.
- 비용지불은 전자화폐 등 익명성을 보장하는 별도의 방식을 통해 이루어 진다.

5.3 표기

본 논문에서 사용되는 표기는 <표 1>과 같다.

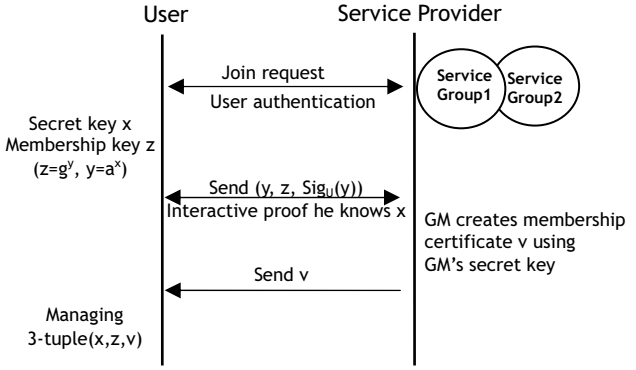
<표 1> 표기 설명

표기	설명
Y	그룹의 공개키
S_U	사용자의 서명 값(Signature)
GM	그룹 매니저(Group Manager)
H()	충돌방지(Collision resistant) hash 함수
N	서비스 제공자가 발행하는 넌스(Nonce)

r	랜덤 변수
Aid	익명 아이디(Anonymity ID)
sk	공탁기관의 비밀키
$E_{sk}()$, $D_{sk}()$	sk 를 이용하는 암호화/복호화 함수
$Sig_X()$	X's 디지털 서명 함수
Cid	콘텐트 아이디(Content ID)
LEApermit	법 집행 기관의 허가서
‖	연결(Concatenate) 함수

5.4 등록 단계

사용자는 서비스 제공자(Service Provider)가 제공하는 서비스 그룹들(유료회원그룹, 무료회원그룹 등)중 자신이 원하는 서비스 그룹을 선택하고, 해당 서비스 그룹 가입을 위해 요구되는 사전 작업을 수행하여야 한다. 여기에는 사용자가 그룹에 가입할 자격이 있는지를 증명하는 과정과 가입비 같은 관련된 비용을 지불하는 절차가 포함될 수 있다. 이후 사용자는 그룹 서명 방식의 Setup 프로세스에 따라 서비스 그룹에 가입한다. 등록 과정은 (그림 2) 와 같다.



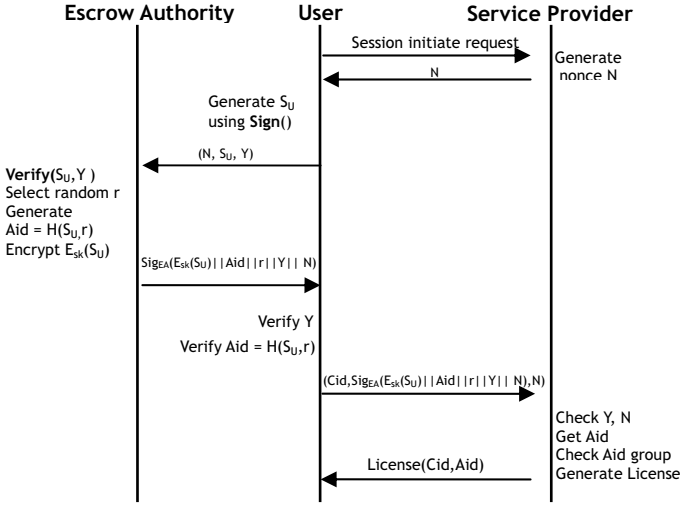
(그림 2)등록 처리 flow

본 연구에서는 Camenisch[10]가 제시한 그룹 서명 방식을 적용하였다. 사용자(User)는 개인키 x 를 생성하고 암호학적인 방식을 이용하여 이에 대응하는 공개키 y 와 z 를 만든다. 여기에 자신을 증명하기 위한 인증서를 첨부하여 그룹을 관리하는 GM 에게 전송한 후, 디지털 서명 방식을 이용하여 y 를 만드는데 필요한 x 를 알고 있음을 증명한다. GM 은 자신만이 알고 있는 비밀키를 이용하여 멤버 인증키(Membership Certificate Key) v 를 생성하고 사용자에게 전송해 줌으로써 사용자를 그룹 멤버로 추가한다. 위와 같은 방식은 사용자의 비밀키 x 를 GM 에게 제출하지 않기 때문에 그룹 내 다른 멤버나 GM 조차도 사용자를 대신하여 서명할 수는 없음을 보장한다.

5.5 익명의 아이디 생성 및 라이센스 요청 단계

서비스 제공자가 제공하는 특정 콘텐트를 사용하기 위해서 사용자(User)는 콘텐트에 대한 라이센스를 필요로 한다. 또한 사용자에 의한 익명 아이디(Anonymity ID, Aid)의 재사용 방지와 Aid 에 콘텐트 구매 정보가 연결되는 것을 방지하기 위해 Aid 생성단계와 콘텐트에 대한 라이센스 요청 단계는 하나의 처리 단위로 묶여진다. 상세 처리 과정은 (그림 3)과 같다. 사용자는 라이센스 요청에 필요한 nonce(N)를 서비스 제공자에게 요청하여 받은 후, 그룹 서명의 Sign 프로세스를 통하여 서명 값 S_U 를 생성 한다. 사용자는 (N,S_U,Y) 정보를 공탁기관(Escrow Authority, EA)에게 전송하고, EA 는 사용자의 서명 값 S_U 와 그룹 공개키 Y 를 이용하여 그룹 서명의 Verify 프로세스를 수행 함으로서 사용자가 해당 그룹의 멤버임을 확인한다. Verify 프로세스는 서명자가 자신의 비밀키 x 와, 그룹멤버 키 v 를 사용하여 서명 값을 생성하고, 그 서명에 사용된 x, v 를 알지 못하면 생성할 수 없는 "증명 값"을 함께 제출 함으로서 수신자에게 그룹 멤버가 서명했음을 확신시키는 방법을 사용하고 있다.

그룹 멤버 확인 과정을 거친 후 EA 는 사용자의 S_U 에 자신의 랜덤 값 r 을 추가하여 hash 함으로써 Aid 를 생성하고, 추후 Aid 에 대한 추적을 위해 사용자가 제출한 S_U 를 자신의 비밀키로 암호화 하는 작업을 수행한다. EA 는 S_U 의 암호 값, Aid, r, Y, N 전체에 대해 서명함으로써 사용자가 특정 그룹의 멤버임을 보증하며, 사용자 역시 $Aid = H(S_U,r)$ 확인을 통하여, Aid 가 자신이 보낸 정보로 만들어 졌음을 알 수 있다. 이후 사용자는 부여 받은 Aid 를 이용하여 자신이 원하는 콘텐트에 대한 라이센스를 요청하고 서비스 제공자는 EA 의 서명 확인을 통하여 Aid 관련된 그룹정보를 확인하고 해당 그룹별 차별화된 라이센스를 발급한다.

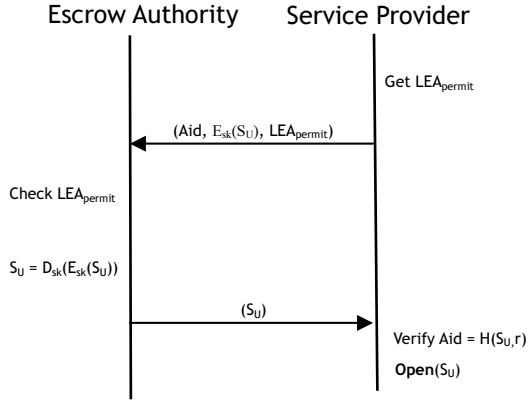


(그림 3)Anonymity ID 생성 및 라이센스 요청 flow

5.6 익명 추적 단계

개인 사생활 보호를 위한 익명성 보장 구조는 악의적인 사용자가 악용하지 않도록 하기 위해 적법한 절차에 의하여 공개적으로 익명성이 추적 가능함을 보여야 한다. 제안하는 방식은 서비스 제공자와 공탁기관의 협력을 통하여 구매자의 신분을 추적할 수 있다. (그림 4)는 익명성 추적 절차를 나타내고 있다. 불법 유통 등의 사유로 판매된 콘텐트의 구매자 신분 확인이 필요한 경우, 서비스 제공자는 구매자의 Aid 와 여기에 대응하는 $E_{sk}(S_U)$을 공탁기관에 보내고, 공탁기관은 이를 자신의 비밀키로 해독하여 되돌려 주는 방식을 통하여 서비스 제공자는 Aid 생성에 사용된 사용자의 서명 값 S_U 를 얻을 수 있다. 이때 불법적인 구매

자 추적을 방지하기 위해 서비스 제공자는 공탁기관에게 S_U 요청하기 전에 법 집행 기관(Law Enforcement Agent)의 허가를 얻어야만 한다. 서비스 제공자는 내부의 그룹 매니저에게 S_U 를 전달하고 그룹 매니저는 그룹 서명의 Open 프로세스를 수행함으로써 익명 구매자의 신분을 확인할 수 있다.



(그림 4)Anonymity ID 추적 flow

5.7 그룹 탈퇴 단계

서비스 그룹의 탈퇴 방식은 그룹 서명의 Delete 프로세스를 따른다. Delete 프로세스는 탈퇴한 그룹 멤버의 멤버십 키를 무효화 하기 위해 그룹의 공개키의 갱신과 기존 멤버십 키의 재 배포를 필요로 하므로 부하가 크다. 이런 부하를 최소화 하기 위해 탈퇴 멤버리스트를 관리하여 주기적으로 반영하는 방법을 적용한다[11].

6. 보안 분석(Security Analysis)

제안하는 구조는 다음과 같은 보안 특성을 가진다.

추적 가능한 익명성(Traceable Anonymity) 제공

익명 아이디(Anonymity ID, Aid)를 통해 라이센스를 요청하므로 구매자의 익명성이 보장 되며, 콘텐트 구매 시점마다 새로운 Aid 를 사용함으로 Aid 에 콘텐트 구매실적이 연결되지 않는다. 서비스 제공자와 공탁기관의 협력을 통해서 구매자의 신분확인이 가능하고, 신분확인 절차를 수행하기 위해선 법 집행 기관의 허가를 얻어야 함으로 불법적인 추적이 방지 된다.

무결성(Integrity) 제공

Aid 는 공탁기관이 생성하고 서명함으로써 누구도 Aid 를 변경할 수 없다. 또한 공탁기관은 Aid 생성에 사용한 랜덤 값 r 를 제공함으로 사용자와 서비스 제공자는 Aid 의 유효성 확인이 가능하며, hash 함수를 통해 Aid 를 생성하기 때문에 Aid 가 다른 사용자의 것으로 잘못 해석 되지 않는다.

재현 공격(Replay Attack) 방지

사용자는 라이센스 요청을 위해 서비스 제공자의 nonce 를 필요로 하고, 공탁기관은 이를 포함하여 서명 함으로 사용자는 동일한 Aid 를 두 번 사용할 수 없다.

가장 공격(Impersonate Attack) 방지

제안하는 방식은 그룹 서명(Group Signature)의 보안 특성을 훼손하지 않는다. 그룹 서명의 특성상 그룹 멤버가 아닌 사람은 그룹의 이름으로 서명할 수 없고, 그룹 멤버나 그룹 매니저도 다른 그룹 멤버를 위조할 수 없으므로 어느 누구도 특정 그룹 멤버를 가장(Impersonate) 할 수 없다.

7. 결론

제안된 방식을 통해 사용자는 콘텐트 구매 시 서비스 제공자와 공탁기관에게 자신의 익명성을 보장 받을 수 있으며, 서비스 제공자에게 익명으로 자신이 속한 서비스 그룹을 알림으로써 차별화된 서비스를 제공 받을 수 있다. 공탁기관은 사용자가 제출한 서명 값을 가지고 특정 그룹 멤버임을 확인하고, 서명 값을 암호화/복호화 하는 기능 만을 담당하므로 작은 부하만을 가지고 구현이 가능하다. 또한 익명성이 적법한 절차에 의해 추적 가능함을 명확히 함으로써 사용자의 불법적인 행동을 사전에 방지할 수 있다.

참고문헌

[1] C. Conrado, F. Kamperman, G.J. Schrijen, W. Jonker, “Privacy in an identity-based DRM system.”, Database and Expert Systems Applications, 2003.

[2] B. Park, J. Kim, and W. Lee, “PrecePt: A Privacy-Enhancing License Management Protocol for Digital Rights Management.”, Proceedings of AINA’04, 2004.

[3] Jiang Zhang, Bin Li, Li Zhao, Shi-Qiang Yang, “License Management Scheme with Anonymous Trust for DRM.”, ICME 2005.

[4] Daniel J. T. Chong, Robert H. Deng, “Privacy-Enhanced Superdistribution of Layered Content with Trusted Access Control.”, Proceedings of the ACM Workshop On Digital Rights Management, DRM'06.

[5] DaeHun Nyang. “Pseudonym and Anonymity with Traceability.”, In NETSEC-KR 2007.

[6] Kilian, J., Petrank, E. “Identity Escrow.”, Proceedings of the Conference on Advances in Cryptology (CRYPTO'98).

[7] Yong-Ho Lee, Im-Yeong Lee, and Hyung-Woo Lee, “New Identity Escrow Scheme for Anonymity Authentication.”, INDOCRYPT 2002.

[8] Stefan Kopsell, Rolf Wendolsky. “Revocable Anonymity.”, ETRICS 2006.

[9] D. Chaum and H. van Heyst, “Group Signatures”, In Advances in Cryptology – EUROCRYPT ’91.

[10] Jan Camenisch and Markus Stadler. “Efficient Group Signature Schemes for Large Groups.”, CRYPTO’97.

[11] He, Y. "New Dynamic Group Signature Scheme", Wuhan University Journal of Natural Sciences 11 (6), 2006.