

프라이버시 속성 인증을 위한 PC Agent 모델

류춘열, 박지환
부경대학교 전자계산학과

The PC Agent Model for Certification of Privacy Attributes

Chun-Yeol Ryu, Ji-Hwan Park
Dept. of Computer Science, PuKyong National University

요약

현재 인터넷의 사용 증가로 인한 개인 정보의 유출이 급증하고 있다. 특히, 인증과 권한의 허가가 동일한 시스템 내에서 이루어지므로 처리에 불필요한 개인 정보가 과다하게 공개되고 있다. 이러한 문제를 해결하기 위해 인증과 권한, 처리를 개별적으로 분리한 프라이버시 속성 인증 제어 시스템 모델이 제시되어 있다. 그러나 프라이버시 보호를 위한 처리 모델은 서버로 하여금 서비스 이용자의 각종 지원 서비스와 서버 운영 통제 처리 분석을 불가능하게 한다. 본 논문에서는 공개 가능한 개인 속성 정보만을 선별적으로 참조 가능하게 하는 프라이버시 속성 인증 네트워크 프레임으로 확장하기 위한 모델을 제안한다.

1. 서론

현재 인터넷이 사회의 한 기반을 형성하고 있으며, 인터넷을 이용하면서 여러 가지 서비스를 공유할 때 개인의 인권 침해 문제 등이 다수 발생하고 있다. 특히, 인터넷상의 웹 서버를 이용할 때 불특정 다수에게 서버 이용자들의 ID 정보, 연령, 혈액형 등의 개인 정보가 필요 이상으로 공개되고 있다[1].

UNIX와 같은 대부분의 시스템에서 특정한 자원 접근을 허용하기 위해 접근제어를 수행한다. 이러한 시스템 자원 이용을 허가하는 과정은 인증과 권한 정보가 같은 영역에서 관리되므로 불필요한 정보가 시스템 관리자에게 노출된다. 이와 같은 문제점을 해결하기 위해 제안된 SPKI(Simple Public Key Infrastructure)[3][4] 접근제어 방식은 인증을 위해 제3의 인증개체를 이용하여 인증과 권한처리를 독립하였다[4][5]. 그러나 서비스 이용자의 속성을 참조해야 하는 컨텐츠 서비스에 적용이 불가능하여, 이를 보완한 프라이버시 보호를 고려한 속성 인증 프로토콜[7]이 제안되었다.

이와 같이 개인의 프라이버시 보호를 위한 보안 강화로 개인 정보 유출은 막을 수 있지만, 서버의 개인화된 서비스 제공을 위한 최소한의 개인 속성 정보 참조가 제한되어, 실제 제공되는 고객의 다양한 온라인 서비스나 CRM(Customer Relationship Marketing)과 같은 운영 정책을 적용하기 어렵다.

본 논문에서는 개인의 인권이 보호되는 프라이버시 속성 인증 모델 기반 위에서 제한된 프라이버시 속성 정보를 서버에 제공하도록 확장하여 서비스 이용자와

제공자가 만족하는 상호 접근 제어 모델을 제안하고자 한다. 본 논문은 2장에서 기존 논문이 제안하고 있는 프라이버시 보안 모델을 살펴보고, 3장에서는 PC Agent를 이용하여 서버의 프라이버시 속성 정보가 참조되는 확장 모델을 제안한다. 그리고 4장에서는 기존에 제시된 모델과 비교를 통한 결론 및 향후 연구 과제에 대해 기술한다.

2. 관련 연구

본 장에서는 개인의 프라이버시 보호를 위해 제안된 모델을 알아보고, 제안된 각 모델이 처리하는 기능에 대해서 간단히 살펴본다.

2.1 프라이버시 중시 접근 제어 시스템

프라이버시 중시 접근 제어(Privacy-Enhanced Access Control)[1]은 SPKI 공개키 기반의 접근 제어를 권한 증명서를 이용하여 수행한다.

Server, Client, Issuing Agent로 구성된 시스템의 접근 제어는 서버에 의해 발행되어진 권한증명서를 클라이언트가 취득해서 그것을 원래의 서버에 제출하여 권한을 관리한다. 여기서 Server와 Client는 접근 제어 서비스를 주고받는 주체이다. Issuing Agent는 지역적 개체이며, PKIX(Public Key Infrastructure with X.509)[8]의 공인된 CA와 서로 다르다.

SPKI의 권한 증명서 양식은 참고문헌[5]에서 제시된 양식에 따라 기술한다. SPKI 권한 증명서는 식(1)과 같이 5-tuple로 구성된다.

$$\langle I, S, D, A, V \rangle_{\text{SPKI}} \quad (1)$$

단, 각 항목은 아래와 같이 나타낸다.

- Issuer I : 증명서를 발행한 주체의 공개키
- Subject S : 증명서가 양도되어진 주체의 공개키
- Delegation D : 증명서의 지정 권한정보(Boolean)
- Authorization A : 행사할 수 있는 권한
- Validity V : 권한 증명서 유효 기간

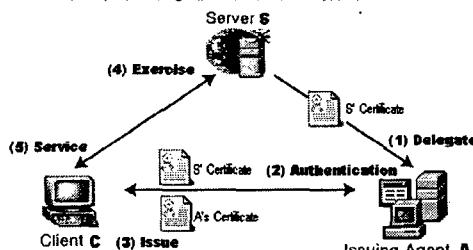
서버의 권한 증명서는 권한 위임이 가능하다. 권한 위임시 새로운 증명서가 생성됨으로써, 한 단위의 접근 제어에 있어서 식(2)와 같이 복수의 증명서를 이용한다. 이러한 이용 권한은 식(3)과 같이 간략화 될 수 있다.

$$\langle I_1, S_1, D_1, A_1, V_1 \rangle, \langle I_2, S_2, D_2, A_2, V_2 \rangle \quad (2)$$

$$\langle I_1, S_2, D_2, A_1 \text{Intersect}(A_1, A_2), V_1 \text{Intersect}(V_1, V_2) \rangle \quad (3)$$

$A\text{Intersect}(A_1, A_2)$ 는 권한 A_1 과 권한 A_2 의 공통된 권한 값을 가진다. $V\text{Intersect}(V_1, V_2)$ 는 V_1 과 V_2 를 비교해서 가장 근간의 기한을 권한 종료일로 한다.

프라이버시를 중시한 접근 제어 시스템은 사용자 접근 제어를 위해 3가지 구성 요소들을 이용하여 처리한다. Server 구성 요소는 2장의 권한 증명서 Cert_1' , Cert_2' 를 Client로부터 접수 받아서 이에 대응하는 서비스를 수행한다. Issuing Agent는 Server로부터 권한 증명서 Cert_1' 을 받아서 Client로 서비스를 위한 권한 증명서 Cert_2' 를 Cert_1' 과 같이 발행하며, ACL(Access Control List) 정책을 유지한다. Client는 Issuing Agent로부터 받은 Cert_1' , Cert_2' 를 Server로 제출해서 서비스 제공을 받는다. [그림 1]은 이러한 SPKI의 제어 과정을 나타내고 있다.



[그림 1] SPKI의 제어 과정

시스템 구성요소 간의 관계로 Server와 Issuing Agent, Issuing Agent와 Client는 상호 신뢰하는 관계이다. 그러나 Server와 Client는 상호 신뢰하지 못한다[1].

각 주체는 증명서를 위임, 발생, 행사를 수행한다. Server는 Issuing Agent를 인증하며, 인증 후 권한 증명서 Cert_2' 를 발행하는 권한을 권한 증명서 Cert_1' 을 이용하여 Issuing Agent에 양도한다. Issuing Agent는 Server로부터 양도 받은 권한을 이용하여 Client에게 Server 접근을 허가하기 위한 권한 증명서를 발행한다. 이때 발행된 권한 증명서는 위임된 접근 권한 이내에서 처리되어야 한다. Server는 클라이언트로부터 요청받은 접근 서비스를 제공하기 위해 권한 증명서 Cert_1' , Cert_2' 를 검증한다. 접근 서비스를 위해 허가 여부를 판단하여 정당한 Client에 대해 대응되는

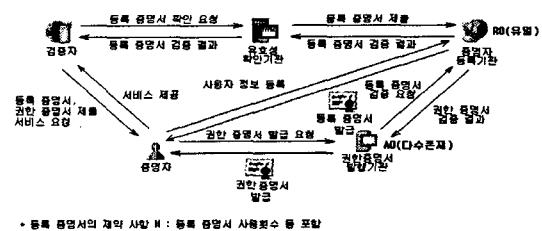
서비스를 처리하기 위한 권한 행사를 수행한다. 접근 서비스는 증명서에 대응되는 P(C)로 암호화하여 처리된다.

2.2 프라이버시 속성 인증 방식의 모델

프라이버시를 중시한 속성 인증 방식[7]의 모델은 2.1에서 언급한 프라이버시 중시 접근 제어 모델에 속성 인증 처리를 추가한 보안 모델이다. 온라인상에서 서비스 이용자가 자신의 신원이나 권한을 증명하기 위해서는 디지털 증명서 이용시 제공되는 일부 개인정보를 통해 서비스 이용자가 어떠한 서비스를 어디서 제공 받았는지가 추적되지 않도록 보완하고 있다.

속성 인증 방식의 모델은 증명서 등록기관, 권한 증명서 발급기관, 증명자, 검증자, 유효성 확인기관으로 구성된다. 여기서 증명자는 서비스 이용자이며, 검증자는 서비스 제공자에 해당한다.

프라이버시 속성 인증 방식의 모델은 개인을 증명하는 등록 증명서를 증명자 등록 기관으로부터 발급 받은 다음에 권한증명서 발급기관에 제출하여 주어진 제한 범위 이내의 권한증명서를 발급 받는다. 발급된 권한증명서는 서비스 제공을 위해 서버에 제출되며, 이때 자신을 증명하기 위한 등록증명서도 같이 보내어 진다. 서버는 제출된 서비스 이용자의 신원을 확인하기 위해 등록증명서를 유효성 검증 기관에 제출하며, 유효성 검증 기관은 서버로부터 제출받은 등록증명서를 다시 증명자 등록기관으로 제출하여 인증을 받아 그 결과를 서버에 알려준다. 서버는 제출된 등록증명서의 인증이 성공적으로 수행된 이후, 권한증명서에 명시된 권한 이내에서 서비스를 제공한다. [그림 2]은 이러한 전체 처리 과정을 나타내고 있다.



[그림 2] 프라이버시 속성 인증 모델

프라이버시 속성 인증 모델의 각 구성 요소는 속성 인증에 따른 증명서 위치 불가능, 증명서 유용 불가능, 증명자 프라이버시 보호 안전성 요건[7]을 충족시킨다.

3. 속성 인증을 위한 PC Agent 모델

본 장에서는 서버에서 이용자의 공개 가능한 속성을 참조하여 운영에 필요한 개인 속성 정보 수집 및 처리를 위해 PC(Privacy Certification) Agent 모델을 기술한다.

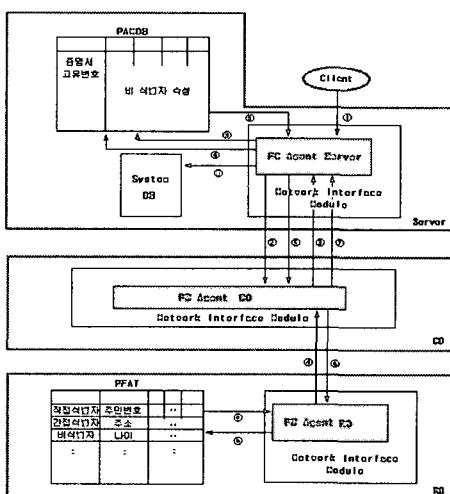
WWW상의 웹 사이트 운영시 서버 관리자가 서비스 이용에 대한 각종 통계 및 분석을 수행하기 위해서는 반드시 서비스 이용자의 부분 정보를 필요로 한다. 그러므로 서버는 CA로부터 서비스 이용자의 신원

확인이 불가능한 부분적 속성 정보를 필요시 참조할 수 있어야 한다. 이러한 처리를 위해 프라이버시 속성 인증 모델은 우선 서버가 유효성 검증 기관인 CO(Certify Organization)를 통해 간접적으로 증명서 발급 기관인 RO(Register Organization)에 접근하여 요구 속성을 획득할 수 있어야 한다. 그리고 네트워크의 부하를 최소화하기 위해 조건에 따른 일괄 처리 작업을 RO와 연동할 수 있도록 한다.

이러한 속성 참조는 개인의 신원을 확인할 수 없는 비 식별자에 한하여 수행되어야 한다. 그러므로 서비스 이용자의 프라이버시 부분정보에 직접 접근이 가능하며, RO는 서비스 이용자 정보 레코드의 각 구성 항목을 직접 식별자, 간접 식별자, 비 식별자 영역에 포함되도록 정의하여 관리한다. 여기서 직접 식별자(Direct Identifier)란 개인을 직접 식별할 수 있는 속성(예: 주민번호, e-mail, 휴대폰 번호 등)으로 정의된다. 그리고 간접 식별자(In-Direct Identifier)는 개인을 간접적으로 식별할 수 있는 속성(예: 주소, 이름, 소속 집단명 등)으로 정의되고, 비 식별자(Non-Direct Identifier)는 개인을 식별할 수 없는 속성(예: 나이, 키, 몸무게, 취미 등)으로 정의된다.

3.1 전체 처리 과정

서버가 프라이버시의 속성을 참조하기 위해서는 CO와 RO가 연동되어야 한다. [그림 3]은 확장된 프라이버시 속성 참조 모델의 전체 구성을 보여주고 있다.



[그림 3] 확장된 프라이버시 속성 참조 모델의 전체 구성

확장된 프라이버시 속성 참조 모델은 기준이 되는 구성 요소에 따라 크게 두 가지 처리 형태로 구분할 수 있다. 다음은 [그림 3]에서 나타내고 있는 Server의 프라이버시 속성 처리 과정을 요약하고 있다.

- ① 서비스 요청자의 RO cert'(동록 증명서), AO cert'(권한 증명서) 제출

- ② RO cert' 확인 요청
 - ③ RO cert' 확인 결과
 - ④ RO cert'의 고유번호 존재 유무 검색
 - ⑤ RO cert'의 고유번호 검색 결과 반환
 - ⑥ 프라이버시 속성 정보 요청
 - ⑦ 허가된 프라이버시 속성 정보 리스트
 - ⑧ 요청된 속성 항목 확인
- ⑨ PAMDB(Personal Attribute Management Data Base)에 속성 정보 저장
- 그리고 RO의 처리 과정은 다음과 같다.
- ⓐ 프라이버시 속성 수집 요청
 - ⓑ 처리 모드에 따른 프라이버시 속성 추출 요청
 - ⓒ 추출된 프라이버시 속성 추출 값(리스트) 반환 및 일괄 처리
 - ⓓ 요청 속성 반환
- * 단, 여기서 등록 증명서 확인 절차 생략.

PAMDB는 RO cert'의 고유번호를 기본키(P.K)로 하는 프라이버시 속성 정보 저장 데이터베이스이며, System DB는 유효성 검증 기관의 관련 정보, 등록 증명서 발급 기관 관련 정보, 프라이버시 속성 수집을 위한 시스템 환경 정보 등을 가진다.

각 구성 요소마다 기능의 확장을 위해 사용되는 PC Agent는 해당 구성 요소의 처리 모듈을 캡슐화하고 있다. PC Agent의 주된 역할은 Server의 인증서를 확인하고, 개인 정보 수집을 위한 PAMDB와 System DB를 관리한다. 그리고 등록 증명서 확인 시 각 개인 정보 수집을 위한 항목을 관리하며, Server Idle Time 및 회선 Idle Time 시 자동화된 개인 정보 수집을 통한 정보 수집의 부하를 최소화한다.

3.2 부분적 프라이버시 속성 참조

서버에서 부분적으로 프라이버시 속성 참조를 하기 위해서는 개인 정보 네트워크를 구성하는 각 구성 요소가 관리해야 될 개인 정보 DB의 범위가 결정되어야 한다. 우선 Server가 관리하는 DB는 비 식별자 속성 리스트와 서버 운영 정보이며, CO가 관리하는 DB는 등록 증명서 중계를 위한 시스템 운영 정보이며, RO는 프라이버시 필터링 속성 정보, 등록 증명서 발급 정보, RO 운영 정보 등을 관리한다.

RO에서 유지하는 프라이버시 속성 정보가 생성 및 추가되었을 때는 서버가 참조 가능하도록 하고, 접근이 가능한 속성 리스트를 서버에 제공해야 한다. RO 초기 설정시에는 RO가 초기에 개인 정보 네트워크와 연동될 때 개인 정보 보호 서비스 범위 내에서 서버에게 접근 가능한 비 식별자 리스트와 간접 접근 가능한 간접 식별자 리스트를 브로드 캐스팅한다. 그리고 신규 서버가 개인 정보 보안 네트워크에 추가되었을 때는 접근하고자 하는 비식별자/간접 식별자 속성을 가지지 못한 서버는 유효성 검증 기관을 통해 RO로부터 접근 가능한 프라이버시 속성 리스트를 가져온다.

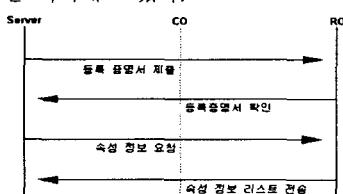
RO와 서버의 프라이버시 속성 정보 수집 시 기본적 인 프라이버시 속성 인증 작업에 대한 부하를 최소화하기 위해서는 서버가 서비스 요청 클라이언트 신원

을 확인하기 위해 유효성 검증기관에게 등록 증명서 제출시 서비스 요청자의 접근 가능한 비식별자 정보를 요청한다. 그리고 접근 시간 최소화를 위해 유효성 검증 기관의 비식별자 참조 속성 버퍼링 프록시 모듈을 이용한다.

그리고 서비스 이용자의 등록 증명서 폐기에 따른 간접 정책은 RO가 기발급된 인증서 리스트 정보를 보관한다. 그리고 기한이나 재발급 횟수/ 분실 등에 따른 추가적인 인증서 재발급시에는 직전의 인증서 고유번호를 등록 증명서에 추가한다. 검증자(서버)는 등록 증명서 제출시 재발급 여부를 확인하여, 재발급 시 기발급된 등록 증명서 고유번호를 현재의 등록 증명서 고유번호로 교체한다. 검증자는 등록 증명서 재발급 간접일자 정보를 서버에 기재하여 제출되는 등록 증명서 발급 일자의 비교 확인을 통해 작업 부하를 최소화한다.

3.3 프라이버시 속성 정보 수집을 위한 처리

개별적 프라이버시 속성 정보를 수집하기 위한 처리 과정이며, [그림 5]는 개별적 속성 정보 수집을 위한 프레임을 나타내고 있다.



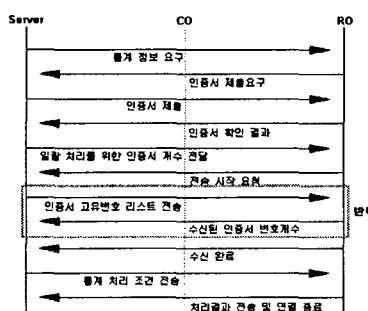
[그림 4] 개별적 속성 정보 수집을 위한 처리

> 프레임의 형태

프라이버시 속성 요청 프레임 : [인증서 고유번호 속성개수 요구속성]
요청에 따른 응답 프레임 : [인증서 고유번호 속성개수 속성값]

[그림 5] 개별적 속성 정보 수집을 위한 프레임

[그림 6]은 통계 정보 제공을 위한 일괄 처리 과정이며, [그림 7]은 통계 속성 정보 수집을 위한 프레임을 나타내고 있다.



[그림 6] 통계 속성 정보 수집을 위한 일괄 처리

> 프레임의 형태

프라이버시 속성 일괄 처리 프레임

서버 면밀 정보 헤더 | 증명서 순번1 | 증명서 고유번호1 | ⌂ | 증명서 순번n | 증명서 고유번호n

[그림7] 통계 속성 정보 수집을 위한 프레임

4. 결론 및 향후 연구 과제

본 논문에서는 기존의 프라이버시 속성 참조 기반 위에서 서버가 제한된 속성 정보에 접근 가능하도록 확장하였다. 이러한 서버의 개인 속성 정보 참조는 기존 논문의 개인 정보 보호를 위해 제공되었던 서비스 흐름의 단방향적 특성을 양방향으로 바꾸어 반드시 개인의 일부 속성 정보를 참조해야하는 배송이나 나이 제한 컨텐츠 사이트 등에 현실적으로 적용 가능하다.

그리고 정보 수집을 위한 참조 절차를 기존의 개인 인증 절차에 추가함으로써, 부가적인 기능 추가에 따른 처리 부하를 최소화하였다.

그러나 기존 모델의 구성이 복잡하고 개인 정보보호를 위한 네트워크 처리 모델의 부하가 커서 실용화에는 많은 비용과 노력이 필요하므로 비현실적이다.

향후 연구과제는 본 논문에서 제시된 확장된 개인정보 보안 모델을 간소화시키고, 실제로 구현 및 적용을 하고자 한다. 특히 본 논문에서 제시된 PC Agent 모델은 처리 부하와 전문성을 고려해 독립적으로 특성화하여 성능 향상을 극대화한다.

참고 문헌

- [1] T. Saito, K. Umesawa, and H.G. Okuno, "A Privacy-Enhanced Access Control", 日本電子情報通信學會論文誌, 2001. 11
- [2] M. Kaeo, Designing Network Security, Cisco Press, 1999
- [3] W. Stallings, Cryptography and Network Security Principles and Practice, 2nd, Prentice Hall. 1999.
- [4] C. Ellison, SPKI Requirements, RFC2692, 1999
- [5] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, SPKI Certificate Theory, RFC2693, 1999
- [6] Jonathan Knudsen, Java Cryptography, O'REILLY, 1999
- [7] H. Yagii, M. Yoshida, T. Fujiwara, "プライバシー保護を考慮した属性認証プロトコル", SCIS'03, 2003
- [8] R. Housley, W. Ford, W. Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, 1999.