디지털산업정보학회 논문지 제10권 제4호-2014년 12월

연령 검증정보의 안정성을 위한 평가인자에 대한 연구*

김 태 경**

The Study on the Evaluation Factor for Security of Age Verification Information

Kim, Tae Kyung

〈Abstract〉

Some laws and regulations may require internet service providers to provide services based on the age of users. Age verification in the online environment should be used as a tool to provide service that is appropriate to child based on age. Using the minimum attribute information, processes on age verification provides the proper guidance to the internet services. However, there is a lack of a globally accepted trust framework for age verification process including evaluation factors for age verification information. In this paper the federation model of user attributes were described and evaluation factors for the age verification information were suggested. Also using the suggested evaluation factors, performance evaluation of federation model of user evaluation was performed. To meet the requirements of evaluation factors, framework of federation model should consider the unlinkability pseudonym support, eavesdropping protection and cloning protection.

Key Words : Evaluation Factor, Federation Model, User Attribute

Ⅰ. 서론

연령검증이란 서비스 제공자에게 사용자의 연령이 특정 연령 이상인지 미만인지에 대한 정보(정확한 연령 값은 제공하지 않음) 및 기존의 인증방식보다 향상된 인증기능을 제공하는 기술이다. 이 기술의 목적은 특정 웹 브라우저나 웹 브라우저용 플러그인 없이도 사용자의 연령을 검증할 수 있는 기능구조를 제시하며, 해외에서 외국인이 우리나라의 사이트를 이용하거나 우리나라에서 내국인이 해외의 사이트를 이용할 때, 각 국의 정해진 나이 기준에 의해 능동적으로 해당 나이에 맞는 서비스를 제공하는 것이다.

연령검증은 연령과 관련된 서비스와 웹 콘텐츠에 접근통제를 위한 정보를 제공하는 것으로, 연령과 관련된 서비스와 웹 콘텐츠에 비인가자들이 접근하지 못하도록 하는 것이다. 특히 청소년들이 성인 관련 콘텐츠에 접근하지 못하도록 하고, 제한된 물품의 구매, 부당한 금융 행위, 부적당한 행동 그리고 규정을 준수하지 않는 서비스 제공자에 접근하지 못하도록

* 이 논문은 2014년도 서울신학대학교 연구년 연구비 지원에 의한 논문임

** 서울신학대학교 교양학부 교수

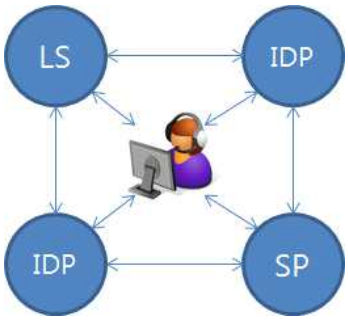
하며, 정해진 기간 동안 서비스 접속을 막는 것과 사이버 상에서 괴롭히기(cyber-bullying)를 방지하고, 고령자에게 저렴한 가격에 서비스를 제공받도록 할 수 있다[1-3].

연령정보는 서비스의 제공여부를 판단하기 위한 기본 정보를 제공하기 때문에 연령정보의 안정성을 확인할 수 있는 평가인자에 대한 연구가 필요한 상황이다. 본 논문에서는 인터넷상에서 연령정보의 안정성을 평가하기 위한 평가인자에 대한 연구를 수행하였으며, 2장에서는 연령정보를 제공하기 위한 속성정보 결합 모델에 대해서 기술하였다. 3장에서는 속성 결합 모델의 평가인자 및 필요성에 대해서 기술하였으며, 4장에서는 평가 인자를 통한 속성 결합 모델의 평가를 수행하였다. 마지막으로 5장에서는 결론으로 연구내용의 요약 및 향후 연구방향에 대해서 정리하였다.

Ⅱ. 연령검증을 위한 속성 결합 모델

연령검증을 위한 속성 결합 모델은 여러 다른 ID 속성 정보 제공자들(identity attribute)로부터 ID 속성 정보들을 수집하고 처리하기 위한 모델이다. 2장에서는 현재 연구되고 있는 연령검증을 위한 속성 결합 모델에 대해서 기술하였다.

현재까지 연구되고 있는 속성정보 수집 모델을 분류하기 위해서는 두 가지의 기준을 적용할 수 있다. 첫 번째는 속성 수집이 일어나는 위치에 대한 것이고 다른 하나는 어느 위치에서 전반적인 프로세스를 중재하는가이다. 여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이 이루어지는가의 기준에 의하면, 다음의 <그림 1>과 같이 SP(Service Provider)에서 수집, IdP(Identity Provider)에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류할 수 있다.



<그림 1> 사용자 속성 정보의 수집

여기서 SP(Service Provider)는 사용자에게 서비스를 제공하는 객체를 의미하며, IdP(Identity Provider)는 사용자의 ID를 등록하여 관리하는 객체로서 사용자의 속성 정보를 가지고 있다. LS(Linking Service)는 여러 IDP에서 동일 사용자들의 대한 속성 정보들을 매핑하기 위한 링킹 테이블(Linking Table)을 생성하는 역할을 수행한다.

수집이 이루어지는 장소에 추가하여 어디에서 수집을 중재하느냐 하는 기준을 추가하게 되면 SP에서의 수집은 SP 중재, IdP 중재로 나누어지며, IdP에서의 수집은 IdP 중재 한 가지만 존재하며, 클라이언트의 수집은 클라이언트 중재와 같이 나뉠 수 있다. 수집 장소, 수집 중재자를 고려한 여러 모델들을 정리하면 다음의 <표 1>과 같이 7개의 수집 메커니즘으로 분류할 수 있다[4-5].

2.1 응용 데이터베이스 모델

가장 단순한 모델로 SP가 로컬 식별자, 서비스에 특화된 선호도와 그룹 멤버십과 같은 이용자의 속성정보를 IdP가 제공하는 속성정보에 추가하여 저장할 수 있다. SP는 로컬 저장소에 SP가 생성한 식별자에 IdP가 제공하는 식별자와 연결하는 추가적인 속성정보를 저장하기 위한 매핑을 생성한다. 향후 이러한

<표 1> 속성정보 수집 모델

번호	수집 장소	수집 중재자	모델
1	SP	SP	응용 데이터베이스 모델
2			SP 중재 모델
3			링킹 서비스 모델
4		IdP	아이덴티티 연합/링킹 모델
5	IdP	IdP	아이덴티티 프로싱 모델
6			아이덴티티 릴레이 모델
7	Client	Client	클라이언트 중재 모델

로컬 속성정보는 특정서비스에 이용자가 접근 가능한지에 대한 결정하기 위해 참조될 수 있다.

2.2 SP 중재 모델

이 모델에서 SP는 다수의 IdP로부터 한 세션의 속성정보를 수집할 수 있도록 이용자에게 허용을 한다. 이용자는 순차적으로 IdP에 의하여 인증되며, 각각의 IdP가 제공하는 속성정보가 SP에게 전달된다.

2.3 링킹 서비스 모델

링킹 서비스 모델은 링킹과 아이덴티티 릴레이 모델의 조합 형태이다. 링킹 서비스(이용자는 링킹 서비스가 제공하는 식별자를 이용)라는 특별한 형태의 SP로 구성된다. 이 식별자는 링킹표의 링킹 식별자를 이용하는 IdP들을 연결하기 위하여 사용된다. SP의 어느 특정 서비스를 접근하기 위해서, 이용자는 SP를 방문하면, 첫 번째 IdP로 전달된다. 이용자는 인증이 이루어지고, 이용자 속성을 포함하는 주장과 링킹 서비스에 대한 식별자와 링킹 서비스에 대한 참조가 SP로 회신된다. 그러면 SP는 속성정보 수집을 위하여 링킹 서비스 식별자를 링킹 서비스에게 전달하다. SP는 링킹 서비스로부터 IdP들의 리스트를 회신 받은 후, 각 IdP로부터 속성정보를 검색한다. 수집된 속성정보로부터 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

2.4 아이덴티티 연합/링킹 모델

이 모델은 리버티 얼라이언스에서 속성 수집을 위하여 최초로 소개된 모델이다. IdP들은 이용자에게 두 개의 IdP사이에서 상호 링크를 생성할 수 있도록 허용하였다. 링크를 생성하기 위하여, 이용자는 첫 번째의 IdP를 방문하여야 하고 인증 받아야 한다. 첫 번째의 IdP는 이용자에게 다른 IdP와의 연합(Federation)을 할 것인지를 문의하며, 연합을 수락하면 두 번째 IdP로 연합을 요청하다. 이 시점에서 두 개의 IdP 간에 랜덤별명(Random Alias)를 만들기 위하여 상호 연동한다. SP로부터 서비스 접근 동안에는, 하나의 IdP는 속성정보를 포함하는 주장을 그 랜덤별명과 함께 SP에게 제공한다. SP는 다른 IdP로부터 속성정보를 포함하는 주장을 검색하기 위하여 랜덤별명을 사용할 수 있다. 두 개의 IdP로부터의 속성정보를 조합하여, SP는 이용자가 서비스에 접근 가능한지를 결정할 수 있다.

2.5 아이덴티티 프록싱 모델

이 모델에서 SP는 이용자가 매우 신뢰할 수 있는 IdP를 이용하여 다수의 IdP들로부터 속성정보를 수집할 수 있도록 허용한다. 첫째로 이용자는 신뢰하는 IdP로 전달된다. 신뢰 IdP는 이후 이용자를 해당 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 인증을 받은 후에 속성정보를 포함하는 주장을 신뢰 IdP로 회신한다. 이 시점에서 신뢰 IdP는 각 주장을 검증하고, 속성정보를 검색하여 최종 속성정보를 조합한다. 신뢰 IdP는 자신이 갖고 있는 사용자 속성정보를

더 부가할 수 있으며, 이것을 다시 주장으로 만들어 SP에게 전달한다. 전달된 속성정보를 기반으로 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

2.6 아이덴티티 릴레이 모델

이 모델은 프록싱 모델을 일반화된 케이스이다. 프록싱 모델은 SP로 하여금 신뢰 IdP하고의 강한 신뢰 관계를 요구하기 때문에, 프록시 IdP가 전적으로 요구하는 신뢰를 만족시킬 수 없으면 정상적으로 작동할 수 없다. 아이덴티티 릴레이 모델은 신뢰 IdP 대신에 중도적(Relay) IdP가 사용된다. 이용자는 처음에 릴레이 IdP에게 전달이 되고, 릴레이 IdP는 이용자를 다수의 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 개별적으로 인증을 받으며, 이용자 속성정보를 포함하는 주장과 함께 릴레이 IdP로 회신된다. 릴레이 IdP는 모든 주장을 하나의 주장으로 조합하여 SP에게 전달한다. SP는 전달된 주장 안의 각 주장들을 추출하고, 검증하여 속성정보를 검색한다. 조합된 속성정보를 기반으로 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

2.7 클라이언트 중재 모델

이 모델은 릴레이 모델과 유사하다. 릴레이 IdP의 기능들이 다수의 IdP들로부터의 속성정보 수집을 위한 능력을 갖는 이용자 에이전트 또는 응용으로 대체가 된다. SP는 클라이언트에게 자신이 신뢰하는 IdP들에 대한 정보를 제공한다. 클라이언트는 이용자를 이러한 IdP들에게 전달한다. 각 IdP로부터 인증을 받은 후에, 클라이언트는 모든 IdP들로부터 주장을 받으면 SP에게 조합된 주장을 제시한다. SP는 각 주장을 검증하고, 모든 속성정보를 검색하여 이용자가 서비스에 접근이 가능한지를 결정한다[6-7].

속성 결합 모델은 7개의 모델로 구분할 수 있으며, 이러한 다양한 모델 중에서 연령정보를 안정적으로 제공하기 위한 모델을 선정하기 위해서는 평가를 수행하기 위한 평가인자를 선정해서 각 모델들에 대한 성능을 검증해야 한다.

Ⅲ. 연령정보 제공 모델 평가 인자

3장에서는 연령정보 검증 모델을 평가하기 위한 연령정보를 평가인자에 대한 연구를 수행하였다. 연령정보 검증모델의 평가와 관련해서 다음의 사항들을 고려해야 한다.

3.1 데이터 보호(data protection)

연령정보를 제공하는 것은 개인정보와 밀접한 관계가 있다. 그러므로 서비스를 이용하기 위하여 가능하다면 최소한의 정보만을 이용해야 하며, 이용되는 정보 또한 최소한의 정보만 공개되어야 한다. 혹은 중간에 신뢰할 수 있는 제3의 기관을 이용하게 함으로 서비스를 이용하는 이용자의 익명성을 제공할 수 있도록 해야 한다. 데이터 보호와 관련하여 연령정보 검증모델에 필요한 평가인자들은 비연결성(unlinkability), 익명성 제공(pseudonym support), 도청방지(eavesdropping protection), 사용자 중심(user-centric system) 등의 요소들을 고려해야 한다.

3. 2 속성 정보 보안(security of attribute)

속성 정보는 여러 기관들 사이에 주고받기 때문에 보안성이 중요하다. 그러므로 속성값의 무결성과 공유 시 데이터의 노출 방지, 속성 복제 방지 등의 기능을 제공해야 한다. 따라서 속성 정보 보안과 관련된

<표 2> 속성정보 수집 모델 평가

번호	수집 장소	수집 중재자	모델	데이터 보호				속성 정보 보안			기능성	
				비연결성	익명성	도청방지	사용자 중심	무결성	공유 방지	복제방지	신원 확인	속성변경
1	SP	SP	응용 데이터베이스 모델	X	X	X	X	O	X	X	O	O
2			SP 중재 모델	X	X	X	X	O	X	X	O	O
3			링킹 서비스 모델	X	X	X	X	O	X	X	O	O
4		IdP	아이덴티티 연합/링킹 모델	X	X	X	X	O	X	X	O	O
5	IdP	IdP	아이덴티티 프로싱 모델	X	X	X	X	O	X	X	O	O
6			아이덴티티 릴레이 모델	X	X	X	X	O	X	X	O	O
7	Client	Client	클라이언트 중재 모델	X	X	X	O	O	O	X	O	O

평가인자로는 속성정보의 무결성(attribute integrity), 공유 방지(sharing protection), 복제방지(cloning protection) 등을 고려해야 한다.

3.3 기능성(functionality of the system)

연령검증 시스템의 주요 기능으로는 속성정보의 업데이트 발생 시 효과적으로 반영되어야 하며, 연령검증 주체에 대한 신원확인이 필수적으로 수행되어야 한다. 따라서 고려해야 할 평가인자로는 신원 확인(identity authentication)[8], 속성정보 변경(attribute update) 등이 있다.

Ⅳ. 평가 인자를 통한 속성 결합 모델의 평가

3장에서 기술된 연령정보 모델 평가 인자를 통하여 2장에서 소개된 연령검증을 위한 속성 결합 모델의 평가를 수행한 결과는 다음과 같다.

<표 2>는 연령검증을 위한 평가인자를 이용하여 속성정보 수집 모델을 평가한 것이다. <표 2>에서 알 수 있듯이 개인정보의 중요성이 높아짐에 따라 수집 장소 및 수집 중재자가 클라이언트에서 발생하는 클라이언트 중재 모델이 평가 인자 중에서 가장 많은 부분을 만족하는 것으로 나타났다. 즉 여러 속성정보 공유 모델 중에서 클라이언트 중재 모델이 연령 정보를 제공하기에 적합한 모델인 것을 알 수 있다.

그러나 연령검증을 좀 더 효과적으로 수행하기 위해서는 어디의 속성정보인지 파악할 수 없도록 비연결성의 제공 및 익명성을 제공해야 하며, 속성 값들을 복제할 수 없도록 암호화 혹은 복제방지 기능을 제공해야 한다. 즉 기본적으로는 클라이언트 중재 모델을 이용하되 여기에 보안기능을 추가하여 안정적인 연령정보 서비스를 제공해야 한다.

Ⅴ. 결론

연령검증이란 서비스 제공자에게 사용자의 연령에 대한 정보를 제공하는 것을 주목적으로 하며 특히 청소년들이 게임에 중독되는 것을 예방하거나 청소년들이 성인 관련 콘텐츠에 접근하지 못하도록 하고, 제한된 물품의 구매, 부당한 금융 행위, 부적당한 행동 그리고 규정을 준수하지 않는 서비스 제공자에 접근하지 못하도록 기능을 제공하는 역할을 수행한다.

본 논문에서는 연령정보 제공을 위한 다양한 속성 결합 모델에 대해 기술하였다. 또한 이러한 모델들 중에서 연령 정보 제공에 적합한 모델을 선택하기 위한 평가에 관한 연구를 수행하였다. 연령 검증정보 모델의 평가를 위한 평가인자들을 제시하였으며, 이를 통하여 속성정보 수집 모델들에 대한 평가를 수행하였다. 이러한 평가를 통하여 연령정보 제공에 가장 적합한 모델을 선택할 수 있으며, 보안에 관련된 추가적인 고려사항들을 파악할 수 있다.

추후 연구계획으로는 클라이언트 중재 모델이 비연결성, 익명성 그리고 복제방지 기능 등의 보안 기능을 제공할 수 있도록 만드는 연령정보 공유 모델에 대한 연구를 수행할 계획이다.

참고문헌

[1] 김태경, 나재훈, “온라인 아동 보호,” 정보보호학회지, 제24권, 제4호, 2014년 8월.

[2] 나재훈, 김태경, “청소년 아동보호 표준화,” 정보보호학회지, 23권, 3호, 2013년 6월.

[3] 김태경, “COP 보안기술 동향,” 정보보호학회지, 22권, 3호, 2012년 5월.

[4] 나재훈, “ITU-T SG17 웹 서비스 인증 강화 표준,” TTA ICT Standard Weekly, 2014년 11월.

[5] Md. Sadek Ferdous, Ron Poet, “Analysing Attribute Aggregation Models in Federated Identity Management,” 6th International Conference on Security of Information and Networks, 2013.

[6] David W. Chadwicka, George Inmana, Nate Klingenstein, “A conceptual model for attribute aggregation,” Future Generation Computer Systems 26, 2010.

[7] Tae Kyung Kim and Jae Hoon Nah, “Analysis on the Attribute Binding based Enhanced User Authentication,” International Journal of Security and Its Applications Vol. 7, No. 6, 2013.

[8] 김태경, “개인속성 정보의 결합을 통한 강화된 인증방안에 대한 연구,” 디지털산업정보학회 논문지, 10권, 2호, 2014년 6월.

■ 저자소개 ■

김 태 경
Kim, Tae Kyung

2008년 3월~현재
서울신학대학교 교양학부 교수
2006년 3월~2008년 2월
서일대학 정보전자과 교수
2005년 8월 성균관대학교 전기전자 및 컴퓨터공학과 (공학박사)
2001년 8월 성균관대학교 정보통신공학과 (공학석사)
1997년 2월 단국대학교 수학교육과(이학사)

관심분야 : 네트워크보안, USN, 클라우드컴퓨팅
E-mail : tkkim@stu.ac.kr

논문접수일: 2014년 11월 23일
수 정 일: 2014년 12월 5일
게재확정일: 2014년 12월 8일