[정보보호] ITU-T SG17 웹 서비스 인증 강화 표준

개요

대부분의 온라인 서비스는 이용자가 서비스에 접근을 하기 전에 인증을 요구한다. 개념적으로는 글로벌 환경에서 단일한 아이덴티티(Identitity)가 모든 온라인 서비스들을 처리할 수 있다고 생각한다. 그러나 현실에서는 이용자들의 서비스에 따라 아이덴티티 제공자(IdP: Identity Provider)가 제공하는 여러 개의 아이덴티티를 사용하고 있다. 아이덴티티 연합(Identity Federation)환경에서 속성정보를 수집하는 것에 대하여 최초로 관심을 갖은 그룹은 리버티 얼라이언스(Liberty Alliance)이다. 현재까지 많은 메커니즘이 개발되었지만 진화하는 웹 서비스의 요구사항을 모두 만족하기에는 표준개발이 후진성을 보이고 있다. 웹 자체가 서비스 선 구축하고 표준은 후 공개하는 것이 웹 산업의 생존 생리이기 때문으로 사료된다.

새롭게 대두되고 있는 이슈는 크게 두 가지로 분류된다. 하나는 속성정보의 수집 및 바인딩인데, 즉 네트워크 상에 있는 속성정보를 신뢰성 있게 수집을 하고, 필요한 정보를 추려서 향후 안전하게 사용할 수 있도록 토큰 형태로 바인딩하는 것이 필요하다. 이러한 기능은 도메인에 속한 아이덴티티의 속성정보에 대하여는 수집 및 바인딩이 가능하나, 다수의 도메인에 속한 아이덴티티의 속성정보의 수집 및 바인딩은 아직 미제의 이슈(Open issue)인 것이다. 예를 들면, 이북(eBook) 상점에서 IEEE 멤버에 대하여 20%의 책 세일을 계획하고 있다. 이러한 경우에 본 상점은 두 개의 아이덴티티 공급자로부터의 속성정보들이 제공되어야 한다. 즉 결재를 하는 단계에서 20%의 할인을 하려고 하면, 하나의 도메인에서는 신용카드 번호, 다른 도메인에서는 IEEE 멤버십 번호가 제공되어서 하나의 결재 작업에 사용되어야 한다.

또 하나의 이슈는 사용자 프라이버시 보장이다. 위의 상황에서 속성정보 제공자들 간에 이북 상점에서의 결재가 서로 연결되어 있다는 사실 자체가 인식되지 않아야 한다. 아이덴티티 연합환경에서 대표적으로 활용되고 있는 프로토콜들로 SAML2.0, Shibboleth, OpenID, OAuth와 같은 것들이 있다. 그러나 이러한 것들은 프라이버시 보호 정책에 의하여 그 활용 및 보급에 장애를 겪고 있다. 즉 백앤드에서 아이덴티티 공급자들 간에 속성정보를 전달하며, 이러한 행위가 사용자의 동의 없이 이루어지고 있는 것이 문제인 것이다. 이를 개선하기 위하여 여러 가지 모델들이 제안되었지만 아직도 춘추전국시대의 진행을 보이고 있는 것이 현시점이다. 다음은 이러한 두 가지의 이슈를 해결하고자 진행중인 기술적 모델들에 대하여 소개한다.

아이덴티티 연합환경에서 속성정보 수집 모델(Attribute aggregation models in federated identity management)

SAML2.0과 같은 연합관리 기술들은 속성정보를 주장(Assertion)에 내장한다. 그러므로 보편적으로 속성 수집(Attribute aggregation)은 두 개의 해석을 갖는다. 하나는 하나의 주장 안에 모두 속성정보가 내장되는 경우와, 하나의 주장 안에 다른 주장이 내장된 경우를 의미하게 된다.

현재까지 존재하는 속성정보 수집 모델을 분류하기 위하여 두 가지의 기준이 제시된다. 하나는 속성 수집이 어디에서 이루어지는가 하는 것이고 다른 하나는 누가 전반적인 프로세스를 중재하는가이다. 여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이 이루어지는가의 기준에 의하면, 수집 메커니즘들은 SP(Service Provider)에서 수집, IdP에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류된다. 또한 수집이 이루어지는 장소에 더하여 누가 수집을 중재하느냐 하는 기준을 부가하면 SP에서는 SP 중재, IdP 중재, IdP에서는 IdP 중재, 클라이언트는 클라이언트 중재와 같이 분류할 수 있으며, 최종적으로 <표 1>과 같이 7종의 수집 메커니즘을 분류할 수 있다.

<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	아이덴티티연합/링킹 모델
5	IdP	IdP	아이덴티티 프록싱 모델
6			아이덴티티 릴레이 모델
7	클라이언트	클라이언트	클라이언트 중재 모델

1. 응용 데이터베이스 모델

이것은 가장 단순한 모델이다. 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 로컬 속성정보는 특정서비스에 이용자가 접근 가능한지에 대한 결정을 하기 위하여 참조될 수 있다.

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.

3. 링킹 서비스 모델

링킹 서비스 모델은 링킹과 아이덴티티 릴레이 모델(아래 글에서 언급)의 조합형태이다. 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.

4. 아이덴티티연합/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, 그렇다면 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.

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.

6. 아이덴티티 릴레이 모델

본 모델은 프록싱 모델을 일반화된 케이스이다. 프록싱 모델은 SP로 하여금 신뢰 IdP하고의 강한 신뢰관계를 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.

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.

향후 전망

ITU-T SG17 9월 회의에서 제안된 아이템은 사용자 중심의 속성정보 수집을 기반으로 강화된 인증 프로토콜 개발을 내용으로 담았다. 그러나 ITU-T SG17의 아이덴티티 관리 표준 개발 그룹은 SAML2.0의 연장선 상에서 본 제안서를 검토하고 있으며, 특히 개인정보보호에 있어서 사용자가 제어를 하는 것이라 할지라도, 사용자의 정보는 네트워크에 담겨지게 되므로, 공급자 측면에서의 개인정보의 프라이버시 보장도 같이 검토를 하여야 한다는 주장이 제기되어, 최종 사용자를 엔티티라는 용어로 수정하고, 범위도 사용자 중심이라는 키워드를 삭제하여 포괄적인 표준 개발을 협의하여 신규아이템(X.eaaa: Enhanced entity authentication based on aggregated attributes)이 승인되었다. 향후 본 표준은 연령검증과 같은 영역에 확대 적용이 가능한 메커니즘으로 사이버공간에서 이루어지는 전자상거래에 대한 신뢰성 제고에 필수적인 표준이라 사료된다.

나재훈 (한국전자통신연구원 사이버보안연구본부 전문위원, jhnah@etri.re.kr)