http://dx.doi.org/10.3745/KIPSTC.2011.18C.6.389

신뢰적인 개방형 공유 인증 프로토콜 프레임워크

박 승 철†

요 약

최근 들어 현재의 인터넷에서 널리 사용되고 있는 서비스 제공자 중심적인(service provider-centric) 고립형(isolated) 인증 모델의 사용자 편의성 부족, 고비용 구조, 그리고 프라이버시 보호 어려움 등의 문제를 해결하기 위해 단일 사인온(single sign-on) 기반의 공유 인증에 대한 연구가 활발하게 진행되어 왔다. 인증 제공자(authentication provider)의 인증 결과가 다수의 인터넷 서비스 제공자(service provider)에 의해 공유되는 공유 인증(shared authentication) 모델이 실제 인터넷 환경에 적용되기 위해서는 사용자, 서비스 제공자, 그리고 인증 제공자간의 인증 보증 수준(level of authentication assurance)과 인증 정보 보호 수준(level of authentication information protection)에 대한 신뢰가 매우 중요하다. 본 논문은 사용자 중심적인(user-centric) 동작과 개방형 신뢰 제공자 네트워크(trust provider network)와 결합된 신뢰적이고 프라이버시 보호가 가능한 공유 인증 프로토콜에 대한 프레임워크를 제시한다. 제안된 공유 인증 프로토콜 프레임워크는 상호동작 가능한 개방형의 신뢰적인 인증 서비스를 제공함으로써 기존 공유 인증 연구들과 차별화된다.

키워드 : 인증, 공유 인증, 인증 보증, 프라이버시

A Framework for Trustworthy Open Shared Authentication Protocol

Seungchul Park†

ABSTRACT

Recently, researches on the shared authentication based on single sign-on have been actively performed so as to solve the problems of current service provider-centric and isolated Internet authentications, including low usability, high cost structure, and difficulty in privacy protection . In order for the shared authentication model, where the authentications of an authentication provider are shared by several Internet service providers, to be accepted in real Internet environment, trustworthiness among users, service providers, and authentication providers on the level of authentication assurance and the level of authentication information protection is necessarily required. This paper proposes a framework for trustworthy and privacy-protected shared authentication protocol based on the user-centric operation and open trust provider network. The proposed framework is differentiated from previous works in the points that it is able to provide interoperable shared authentication services on the basis of open trust infrastructure.

Keywords : Authentication, Shared Authentication, Authentication Assurance, Privacy

1. 서 론

웹 사이트와 같은 인터넷 서비스 제공자(service provider)가 자신의 인증 제공자(authentication provider)를 독립적으로 보유하는 기존의 고립형 인증 모델(isolated authentication)[1]과 달리, 최근 많은 관심을 끌고 있는 공유 인증 모델(shared authentication model)은 인증 제공자의 인증 결과를 다수의 인터넷 서비스 제공자가 공유할 수 있게 한다[2,3]. 공유 인증 모델에서 인터넷 사용자는 자신의 신원 정보(identity information)를 믿을 수 있는 인증 제공자에게 등록하고, 해당 인증 제공자에 한번 로그인(login)하면 인증 결과를 공유하는 인터넷 서비스 제공자들을 로그인없이 접근할 수 있다. 따라서 공유 인증 모델은 사용자 편의성을 높일 뿐만 아니라 많은 수의 서비스 제공자에게 사용자 신원 정보 노출에 따른 프라이버시 문제 발생 위험을 피할 수 있게 한다. 또한 인터넷 서비스 제공자는 복잡한 인증 서비스와 신원 정보 관리 서비스를 인증 제공자로부터 아웃소싱(outsourcing)함으로써 자체적인 인증 시스템의 개발과 유지.관리 부담으로부터 벗어날 수 있다[1,3]. 인증 제공자는 사용자와 서비스 제공자가 신뢰할 수 있는 인증 서비스를 효과적으로 제공함으로써 많은 수의 사용자와 서비스 제공자를 고객으로 유치할 수 있고, 서비스 제공자에 대한 인증 수준과 사용자 수에 따른 인증 비용 부과를 포함하는 다양한 비즈니스 모델을 개발할 수 있다[4].

† 정 회 원 : 한국기술교육대학교 컴퓨터공학부 부교수
논문접수 : 2011년 8월 19일
수 정 일 : 1차 2011년 10월 10일
심사완료 : 2011년 10월 24일

공유 인증 모델에서 인증 제공자의 인증 결과와 인증 정보가 다수의 서비스 제공자에 의해 공유되기 위해서는 사용자, 서비스 제공자, 그리고 인증 제공자간의 신뢰 관계 형성이 무엇보다 중요하다. 이 신뢰 관계는 인증 제공자가 제공하는 인증 서비스에 대한 신뢰 수준을 나타내는 인증 보증 수준(level of authentication assurance)에 대한 사용자와 서비스 제공자의 신뢰와, 인증 제공자로부터 인증 정보를 제공받는 서비스 제공자가 인증 정보 보호에 대한 신뢰 수준을 나타내는 인증 정보 보호 수준(level of authentication information protection)에 대한 사용자와 인증 제공자의 신뢰를 포함한다. 만약 인증 제공자의 인증 보증 수준을 신뢰할 수 없으면 서비스 제공자가 해당 인증 제공자의 인증 정보를 공유하기 어려울 것이다[4,5]. 또한 인증 제공자가 자신이 제공하는 인증 정보에 대한 보호 수준에 대해 신뢰할 수 없는 서비스 제공자에게 자신의 인증 정보를 제공하기가 어려울 수밖에 없다.

몇 년 전부터 Passport/Live ID, Liberty Alliance/SAML, OpenID, CardSpace 등 공유 인증 모델에 근거한 새로운 인증 프로토콜들이 개발되어 왔으나, 사용자-인증 제공자-서비스 제공자 간의 신뢰 관계에 기초한 신뢰적인 인증 공유 프로토콜에는 아직 이르지 못하고 있다[6]. 따라서 이러한 프로토콜들의 적용은 하나의 큰 조직 내(예, 마이크로소프트와 관련 업체), 상호간 계약에 의해 신뢰 관계를 형성한 그룹(예, 미국의 대학교와 관련 기관 그룹), 또는 낮은 인증 보증 수준을 요구하는 서비스 그룹(예, OpenID 지원 그룹) 등 특정한 그룹에 국한되고 있고, 전체 인터넷 차원의 글로벌한 적용에 이르지 못하고 있다. 뿐만 아니라 이들 프로토콜 간에 상호동작성(interoperability)이 제공되지 않기 때문에 이러한 프로토콜을 사용하는 인증 공유는 동일한 프로토콜을 사용하는 단일 도메인 내에서만 국한된다는 문제가 있다[4].

본 논문은 기존의 공유 인증 프로토콜들을 전체 인터넷 차원의 글로벌 적용이 가능한 개방형의 신뢰적인 공유 인증 프로토콜로 확장하는 방안을 제시하는 데에 목적이 있다. 본 논문이 제시하는 공유 인증 프로토콜 프레임워크는 신뢰 제공자 네트워크(trust provider network) 개념에 기초하여 신뢰적인 공유 인증 서비스를 제공한다. 신뢰 제공자 네트워크는 인증 제공자의 인증 보증 수준과 인터넷 서비스 제공자의 인증 정보 보호 수준에 대한 표준화된 공인 서비스를 제공하는 신뢰 서비스 제공자(trust service provider)의 연합체이다. 신뢰 제공자 네트워크에 의해 공인된 인증 제공자와 서비스 제공자는 제3자가 신뢰할 수 있다. 동일한 신뢰 제공자 네트워크에 의해 공인된 인증 제공자와 서비스 제공자의 표준화된 인증 보증 수준과 인증 정보 보호 수준은 신뢰 제공자 네트워크를 신뢰하는 모든 구성원에 의해 동일하게 공유된다. 제안된 공유 인증 프로토콜 프레임워크는 사용자 에이전트(user agent)가 표준화된 인터페이스를 통해 인증 제공자와 서비스 제공자간의 인증 정보 교환을 중재함으로써 다양한 공유 인증 프로토콜의 유연한 적용을 가능하게 할 뿐만 아니라, 인증 제공자와 서비스 제공자간의 직접적인 인증 정보 교환 과정에서 발생할 수 있는 불필요한 프라이버시 정보 노출을 회피할 수 있게 한다.

2. 공유 인증 관련 연구

2000년 대 중반 이후부터 본격적으로 진행된 공유 인증 프로토콜의 개발은 하나의 인증 서버(authentication server)를 통해 모든 인터넷 서비스 제공자들에게 인증 서비스를 제공하는 중앙집중형 인증 모델(centralized authentication model), 상호 협약을 통해 서비스 제공자들이 인증 서버의 인증 서비스를 공유하는 연방형 인증 모델(federated authentication model), 개방형 ID 기반의 OpenID 인증 모델, 그리고 서비스 제공자 중심(service provider centric)의 기존 인증 모델 대신 사용자 중심의 인증 모델(user centric authentication model) 등 다양한 방향으로 진행되어 왔다[6,7].

2.1 중앙집중형 공유 인증 모델(centralized shared authentication model)

Passport와 그 후속 모델인 LiveID는 마이크로소프트에서 서비스 제공자 중심의 고립형 인증 시스템 환경에서 발생하는 편의성 부족과 고비용 구조 문제를 해결하고, 사용자의 신원 정보를 안전하게 관리하기 위하여 개발한 웹 기반의 중앙 집중형 공유 인증 모델이다[8,9]. Passport/LiveID 모델에서는 사용자의 모든 인증 정보가 마이크로소프트에 의해 관리되는 Passport 서버에 등록되고, 유지되고, 관리된다. 그리고 사용자가 서비스 제공자에 로그온하고자 하는 경우 해당 사용자에 대한 인증 요구는 사용자의 웹 브라우저를 경유하여 Passport 서버에게 전달되고, 모든 인증 서비스는 Passport 서버에 의해 통합적으로 제공된다.

2.2 연방형 공유 인증 모델(federated shared authentication model)

Liberty Alliance에 의해 개발된 연방형 공유 인증 모델은 신뢰 동아리(CoT-Circle of Trust) 기반의 신원 연방화(identity federation) 개념에 기초하고 있다. CoT는 상호 사업적인 협약(business agreement)을 통해 미리 신뢰 관계를 형성한 Liberty 아키텍처를 따르는 서비스 제공자들과 인증 제공자들의 연방(federation)이다[10,11]. CoT에서 서비스 제공자는 효과적인 서비스 제공 등을 위해 일반적으로 자체적인 인증(authentication) 및 인가(authorization) 메카니즘을 포함하는 자체적인 인증 기능을 가지고 있지만, 단일 사인온 서비스(single sign-on)와 인증 정보의 안전한 관리 등을 위해 CoT내의 인증 제공자에게 인증 서비스를 의존할 수 있다. CoT내에서 사용자에 의해 선택되는 인증 서버는 사용자 신원 연방화 과정에서 서비스 제공자별로 사용자에 대한 필명/가명(pseudonym)을 지원하고, 인증 정보 제공에 대한 사용자 동의 및 제어(consent and control)를 통해 사용자의 프라이버시가 보호될 수 있게 한다. 그리고 보안 메카

니즘을 통해 인증 정보가 서비스 제공자에게 안전하게 전달되도록 보장한다. Liberty Alliance 연방형 인증 모델에서 인증 서버와 서비스 제공자간의 모든 인증 정보는 SAML (Security Assertion Markup Language)[12]을 통해 공유된다.

2.3 개방형 ID 공유 인증 모델(open ID shared authentication model)

OpenID는 사용자가 선택한 누구나 알 수 있는 URL(또는 XRI) 형태로 표시되는 하나의 신원 ID를 모든 웹 사이트에 사용할 수 있게 하는 간단하고 개방적이며 분산형의 신원 관리 모델이다[13,14]. OpenID는 인증 제공자인 OpenID 제공자(OP-OpenID Provider)에 의해 발급되고, OP에 대한 자격 제한은 없기 때문에 누구나 OP가 될 수 있다. OP는 서비스 제공자를 대신하여 자신이 발급한 OpenID에 대한 인증 서비스를 제공하고, 웹 사이트의 요청에 따라 사용자의 동의를 획득하여 사용자의 신원 정보를 제공할 수 있다. 목표 서비스 제공자는 사용자가 입력한 OpenID URL을 기초로 Yadis 프로토콜 또는 HTML 기반의 발견 메카니즘을 사용하여 OP의 URL을 발견한다. 서비스 제공자는 사용자의 접근 요청을 발견된 OP에게 redirect함으로써 해당 OpenID에 대한 인증을 의뢰한다. 인증 제공자인 OP는 해당 사용자에 대해 자신의 인증 메카니즘을 사용하여 인증을 실시한다. OP는 OpenID에 대한 인증 결과를 담은 어써션(assertion)을 서명된 redirect 메시지로 해당 서비스 제공자에게 전달한다. OpenID 2.0은 사용자가 사용자 ID 대신 자신의 인증 정보를 관리하고 있는 OP의 URL을 접근하고자 하는 서비스 제공자에 제시하고, OP는 해당 사용자에 대해 가명/필명(pseudonym) 형태의 ID를 발급하여 서비스 제공자에 사용하게 하는 것을 가능하게 한다. 이는 서비스 제공자 간에 해당 사용자의 접근 사실 공유를 어렵게 만들어 프라이버시 보호를 가능하게 하기 위한 것이다.

2.4 사용자 중심의 공유 인증 모델(user-centric shared authentication model)

CardSpace 시스템에 적용된 공유 인증 모델은 클라이언트의 선택장치를 사용하여 사용자가 서비스 제공자의 요구사항에 맞는 XML 파일 형태의 가상의 InfoCard를 선택하여 사용할 수 있고, 인증 정보의 제공을 제어할 수 있다는 점에서 사용자 중심의 공유 인증 모델이라 할 수 있다. InfoCard는 사용자에 대한 기본적인 인증 정보와 함께 InfoCard를 발급한 인증 제공자 정보와 해당 인증 제공자가 발행하는 신원 증명(credential)에 관한 정보(예, 신원 증명 유형 등)를 포함하고, InfoCard 사용자 사이트와 InfoCard를 발급한 인증 제공자간에 할당된 유일한 열쇠에 의해 자동 인증됨으로써 패스워드 사용 없이 InfoCard의 도용 위험을 방지한다[15,16]. CardSpace 사용자 클라이언트가 접근하는 서비스 제공자는 인증 요구사항을 클라이언트에게 전송한다. 인증 요구사항은 해당 서비스 제공자가 수용할 수 있는 보안 토큰(신원 증명 정보)의 유형 리스트(예, SAML 2.0 토큰), 필요한 인증 정보 리스트 등이 포함된다. 서비스 제공자의 인증 요구사항을 수신한 클라이언트의 InfoCard 선택 장치는 서비스 제공자의 인증 요구사항에 부합하는 InfoCard들을 선정하여 사용자에게 알려주고, 사용자는 자신이 서비스 제공자에게 제공하고자 하는 InfoCard를 선택한 후 카드를 발급한 인증 제공자에게 카드 정보를 제공하고 서비스 제공자에게 제공할 보안 토큰(security token)을 요청한다. 서비스 제공자는 클라이언트와 InfoCard에 대한 인증 작업을 수행하고 인증이 성공적이면 클라이언트가 요청한 보안 토큰을 제공한다. 사용자 클라이언트는 인증 제공자가 발급한 보안 토큰을 서비스 제공자에게 전달하고, 서비스 제공자는 수신한 보안 토큰을 확인하여 자신의 요구사항을 충족시키면 클라이언트에게 서비스를 제공한다.

3. 신뢰적인 개방형 공유 인증 프로토콜 프레임워크

3.1 기존 공유 인증 프로토콜의 문제점 분석

<표 1>은 기존 공유 인증 프로토콜들의 문제점을 요약하고 있다. 중앙 집중형 인증 모델인 Passport/Live ID 시스템은 모든 사용자의 서비스 제공자 접근 동작이 마이크로소프트의 Passport 서버에 노출되는 데 따른 프라이버시(privacy) 문제, 인터넷 서비스 제공자의 마이크로소프트에 대한 의존성 심화 문제, 그리고 중앙 서버의 확장성(scalability) 문제 등으로 인해 개방형 환경에서 적용되는 데는 어려움이 있다.

〈표 1〉 기존 공유 인증 프로토콜의 문제점 분석

공유 인증 프로토콜	문제점
Passport/Live ID[8,9]	- 프라이버시 문제 - Passport 서버에 대한 의존성 - 중앙 서버의 확장성
Liberty Alliance/SAML[10,12]	- 폐쇄형 신뢰 모델 - 인증 제공자의 관찰에 따른 프라이버시 문제
OpenID[13,14]	- 신뢰 인프라 부재 - 인증 제공자의 관찰에 따른 프라이버시 문제
CardSpace[15,16]	- 신뢰 인프라 부재 - 복잡한 클라이언트 소프트웨어 필요

Liberty Alliance의 연방형 공유 인증 모델에서 인증 정보를 공유하기 위해서는 미리 협약을 통해 인증 제공자와 서비스 제공자간의 신뢰 관계(CoT) 형성이 전제되어야 하고, 인증 제공자의 인증 서비스 공유는 CoT내의 서비스 제공자에 국한되는 문제점이 있다[17]. 즉, 객관적으로 신뢰할 수 있는 인증 제공자자 이미 존재하는 경우에도 접근하고자 하는 서비스 제공자와 해당 인증 제공자간의 신뢰 관계가 사전에 형성되어 있지 않다면 인증 제공자의 인증 서비스를

공유할 수 없다. 사용자의 서비스 제공자 접근 정보가 인증 제공자에게 노출되는 프라이버시 문제도 Liberty Alliance의 연방형 공유 인증 모델의 문제점 중의 하나이다.

OpenID 개방형 공유 인증 모델은 Liberty Alliance의 폐쇄적인 인증 공유와 달리 인증 제공자의 인증 서비스를 OpenID를 지원하는 모든 서비스 제공자에게 사용할 수 있는 개방성의 장점이 있는 반면, 사용자-서비스 제공자-인증 제공자(OP)간의 신뢰 확보의 어려움이 존재한다. 사용자는 서비스 제공자와 인증 제공자의 신뢰 여부를 전적으로 스스로 판단해야 하고, 서비스 제공자는 인증 제공자에 대한 신뢰 여부를 전적으로 자체적으로 판단해야 하며, 인증 제공자는 자신의 인증 정보를 사용하는 서비스 제공자의 신뢰 여부를 전적으로 자체적으로 판단해야 해야 한다. 이와 같은 신뢰 부족 문제는 개방적인 OpenID 공유 모델이 보안에 민감한 인터넷 서비스에 적용되는 데에 장애로 작용하고 있다. OpenID 개방형 공유 인증 모델도 사용자의 서비스 제공자 접근 정보가 인증 제공자(OP)에게 노출되는 프라이버시 문제를 안고 있다.

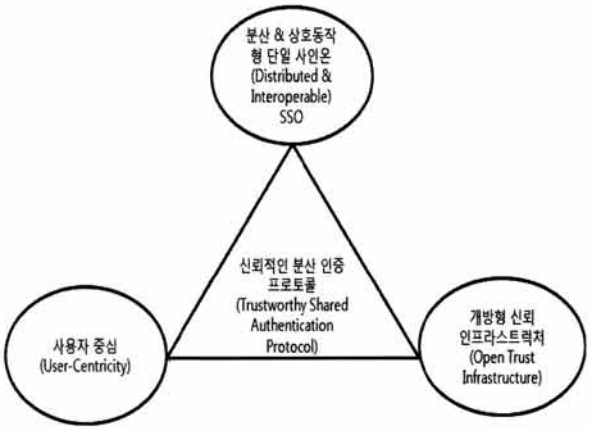
OpenID 공유 인증 모델과 마찬가지로 CardSpace의 공유 인증 모델에서도 특정 인증 제공자의 인증 서비스를 CardSpace를 지원하고 인증 요구사항을 충족하는 모든 서비스 제공자에게 적용할 수 있는 개방성을 지원하고, 사용자 시스템의 InfoCard 선택장치에 의한 인증 정보 교환 중재를 통해 사용자의 서비스 제공자 접근 정보가 인증 제공자에게 노출되는 프라이버시 문제 발생을 방지한다. 그러나 CardSpace 공유 인증 모델이 개방형 환경의 다양한 서비스에 적용되기 위해서는 여전히 사용자-인증 제공자-서비스 제공자 간의 신뢰 확보 문제가 선결되어야 한다. 서비스 제공자의 복잡한 인증 요구사항 처리와 대응되는 InfoCard 선택 등의 기능을 가지는 복잡한 클라이언트 소프트웨어(InfoCard 선택장치)를 사용자 시스템에 설치해야 하는 점도 CardSpace 공유 인증 모델의 문제점 중의 하나이다.

3.2 공유 인증 프로토콜 개선 요구사항

공유 인증 모델(shared authentication model)은 기존 인터넷 환경의 고립형 인증 모델(isolated authentication model)에 비해 사용자 편의성, 개인 정보 노출 회수 감소, 개발 비용 감소 등의 많은 장점이 있다. 그러나 앞 절의 분석에서 알 수 있듯이 공유 인증 모델이 전체 인터넷 차원의 글로벌 적용에 이르기 위해서는 아직 해결되어야 할 문제들이 남아있다. (그림 1)은 공유 인증 프로토콜의 발전 방향을 보여준다.

기존 공유 인증 프로토콜에 대한 분석을 통해 우리는 첫째, 단일 사인온(SSO - Single Sign-On)에 기초한 공유 인증 프로토콜은 Passport의 중앙집중형 모델이 아니라 사용자와 서비스 제공자가 선택할 수 있는 다양한 인증 제공자를 수용하는 분산형 공유 인증 모델(distributed shared authentication model)로 발전해야 함을 알 수 있다. 또한, 분산형 공유 인증 모델이 글로벌 환경에서 실질적으로 수용되기 위해서는 하나의 인증 제공자의 인증 서비스는 동일한 수준의 인증 서비스를 요구하는 모든 서비스 제공자에게 적용될 수 있는 상호동작성(interoperability)이 보장되어야 한다.

둘째, 미래의 공유 인증 프로토콜은 인터넷 환경에 존재하는 다양한 인증 제공자와 서비스 제공자에 대한 신뢰 서비스를 제공할 수 있는 신뢰 인프라스트럭처에 기초하여야 한다. 미래 공유 인증 프로토콜의 신뢰 인프라스트럭처는 Liberty Alliance의 폐쇄형 구조가 아니라 전체 인터넷의 글로벌 적용을 가능하게 하는 개방형 구조를 가져야 한다. 개방형 구조의 신뢰 인프라스트럭처(open trust infrastructure)는 어떤 서비스 제공자와 인증 제공자에 대해서도 신뢰 서비스를 제공하고, 필요할 때 언제든지 서비스 제공자와 인증 제공자의 신뢰 여부를 확인할 수 있게 해야 한다.



(그림 1) 공유 인증 프로토콜 발전 방향

셋째, 인터넷을 통한 민감한 데이터 공유가 더욱 활성화될 미래 인터넷 환경에서 프라이버시 보호는 공유 인증 프로토콜에서 매우 중요한 요구사항이 된다. 미래의 공유 인증 프로토콜은 CardSpace와 같이 사용자가 자신의 인증 정보를 제어하고, 사용자의 제어 영역 내에 있는 사용자 에이전트(user agent) 통해 인증 제공자와 서비스 제공자간의 통신을 중계함으로써 불필요한 인증 정보 공유를 차단할 수 있는, 사용자 중심(user-centric)의 인증 서비스를 제공함으로써 프라이버시 보호를 강화할 수 있어야 한다. 사용자 중심의 공유 인증 모델은 사용자 에이전트가 인증 제공자와 서비스 제공자의 신뢰 상태를 자동으로 확인할 수 있게 하는 장점도 기대할 수 있다.

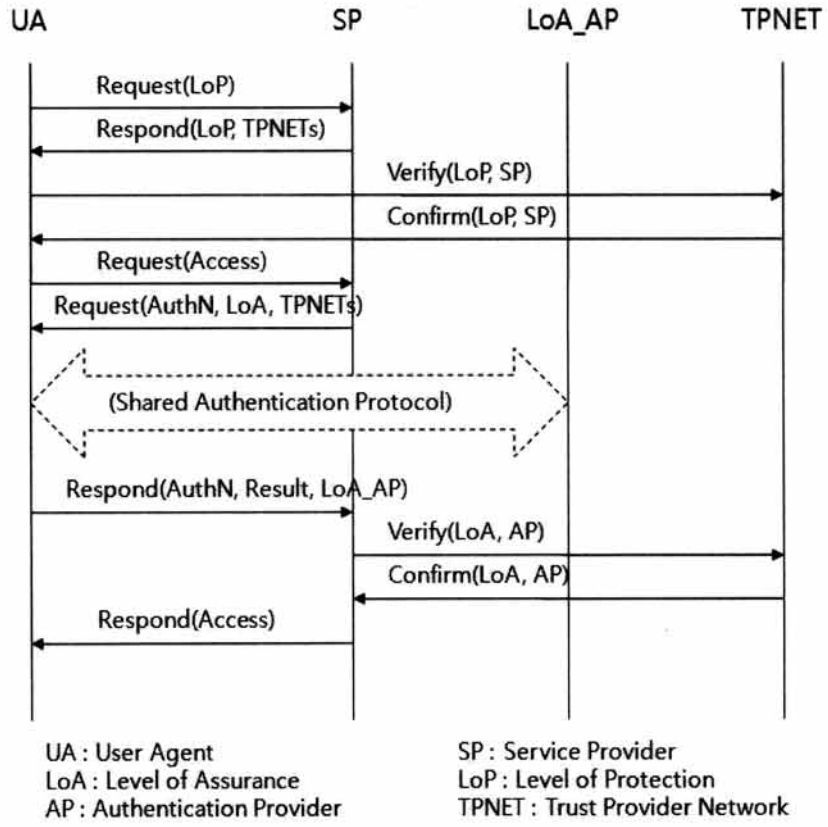
3.3 신뢰적인 개방형 공유 인증 프로토콜 프레임워크 제안

본 논문에서 제시하는 공유 인증 프로토콜 프레임워크는 인증 보증 수준(level of authentication assurance)과 인증 정보 보호 수준(level of authentication information protection)에 대한 표준화, 표준화된 신뢰 프레임워크(trust framework)에 기초하여 인증 제공자의 인증 보증 수준과 서비스 제공자의 인증 정보 보호 수준에 대한 공인 서비스를 제공하는 신뢰 서비스 제공자(trust service provider)의

연합체인 개방형의 신뢰 제공자 네트워크(TPNET - Trust Provider NETwork), 그리고 서비스 제공자와 인증 제공자가 표준화된 인터페이스를 사용하여 사용자 에이전트(UA - User Agent)를 경유하여 서로 통신하는 사용자 중심적인 동작에 기초하고 있다.

(그림 2)는 제안된 신뢰적인 공유 인증 프로토콜 프레임워크의 동작 과정을 보여 준다. 제안된 공유 인증 프로토콜 프레임워크에서 서비스 제공자는 신뢰 제공자 네트워크에 연결된 특정 신뢰 제공자를 선택하여 인증 정보 보호 수준 점검 절차에 따라 자신의 인증 정보 보호 수준에 대해 공인을 받을 수 있고, 신뢰 제공자는 해당 서비스 제공자의 신뢰 상태 정보를 유지한다. 신뢰 제공자에 의한 인증 정보 보호 수준(또는 인증 수준)에 대한 공인 절차는 신뢰 프레임워크(trust framework)에 정의되고, 공인 과정은 X.509 공인 인증서 공인 과정과 유사하게 정의될 수 있다. 제안된 공유 인증 프로토콜 프레임워크에서 신뢰 제공자 네트워크는 표준화된 신뢰 프레임워크를 따르는 신뢰 제공자는 누구나 구성원으로 가질 수 있고, 특정 신뢰 제공자는 동일한 신뢰 프레임워크에 의해 신뢰 서비스를 제공하는 다른 신뢰 제공자와 신뢰 서비스를 공유할 수 있기 때문에, Liberty Alliance/SAML의 폐쇄형 신뢰 모델과 달리 확장성 높은 개방형의 신뢰 인프라스트럭처에 기초한다. 신뢰 제공자 네트워크에 소속된 하나의 신뢰 제공자에 의해 공인된 서비스 제공자는 신뢰 제공자 네트워크의 다른 신뢰 제공자에 의해서 동일하게 공인된다. 신뢰 제공자 네트워크는 신뢰 서비스의 정확성 등에 의해 평가되는 경쟁 관계의 다수 체제로 유지될 수 있다.

사용자는 공유 인증 프로토콜을 통해 접근하고자 하는 서비스 제공자(SP)의 정보 보호 수준을 요구(Request(LoP))할 수 있고, 해당 서비스 제공자가 주장하는 인증 정보 보호 수준(Respond(LoP, TPNETs))을 서비스 제공자에 대한 신뢰 서비스를 제공한 신뢰 제공자 네트워크(Respond(LoP, TPNETs)에 의해 제시된 신뢰 제공자 네트워크의 목록 중의 하나)를 통해 확인할 수 있다. 사용자가 인증 정보 보호 수준이 확인된 서비스 제공자를 접근하면 서비스 제공자는 자신이 요구하는 인증 보증 수준(LoA)과 인증 보증 수준을 공인할 신뢰 제공자 네트워크의 목록(TPNETs)이 포함된 인증 요구 메시지(Request(AuthN, LoA, TPNETs))를 사용자 에이전트(UA)에게 전달한다. 사용자 에이전트는 서비스 제공자가 요구하는 인증 보증 수준을 지원하는 인증 제공자(LoA_AP)에게 자신을 인증하고 인증 결과와 인증 제공자의 정보가 포함된 인증 응답 메시지(Respond(AuthN, Result, LoA_AP))를 서비스 제공자에게 전달한다. 이와 같이 사용자 에이전트를 통해 서비스 제공자와 인증 제공자간의 통신을 중재함으로써 제안된 공유 인증 프로토콜 프레임워크는 서비스 제공자와 인증 제공자간의 인증 정보 교환에 대해 사용자가 통제할 수 있는 사용자 중심의 공유 인증을 실현할 수 있다.



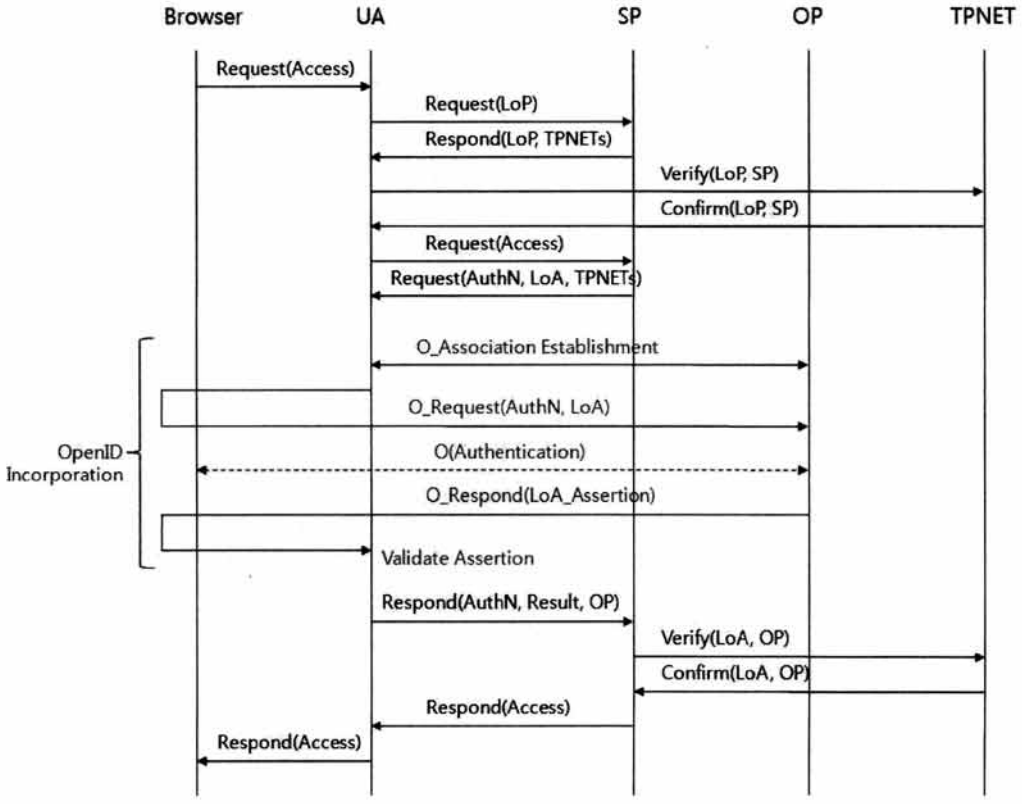
(그림 2) 신뢰적인 공유 인증 프로토콜 프레임워크의 동작 과정

사용자는 UA를 통하여 서비스 제공자의 인증 요구 수준을 충족할 수 있는 인증 제공자를 선택할 수 있기 때문에 분산형의 공유 인증 모델을 실현한다. 그리고 특정 인증 제공자의 인증 보증 수준은 사용하는 공유 인증 프로토콜의 신뢰성까지 고려하여 결정되므로 동일한 인증 보증 수준을 제공하면 어떤 공유 인증 프로토콜을 사용하든 관계가 없다. 즉, 제안된 신뢰적인 공유 인증 프로토콜 프레임워크는 표준 인증 보증 수준을 지원하는 다양한 공유 인증 프로토콜을 유연하게 수용할 수 있고, 동일한 인증 보증 수준의 인증 결과는 공유 인증 프로토콜과 무관하게 모든 서비스 제공자에 의해 공유될 수 있다. 따라서 제안된 공유 인증 프로토콜은 상호 동작형 단일 사인온(interoperable SSO)을 실현한다. 자신의 인증 보증 수준 요구에 맞는 성공적인 인증 결과를 수신한 서비스 제공자는 신뢰 제공자 네트워크를 통해 인증 제공자의 인증 보증 수준을 확인하고, 확인 결과가 성공적이면 해당 사용자에 대해 접근을 허용한다.

3.4 OpenID 기반의 구현 시나리오

(그림 3)은 본 논문이 제안하는 신뢰적인 공유 인증 프로토콜 프레임워크를 OpenID 공유 인증 프로토콜을 사용하여 구현할 때의 동작 절차를 보여준다. 서비스 제공자로부터 인증 요구 메시지(Request(AuthN, LoA, TPNETs))를 수신한 사용자 에이전트(UA)가 OpenID 공유 인증 프로토콜을 지원하고, 특정 OpenID 인증 제공자(OP)로부터 서비스 제공자가 요구하는 인증 보증 수준(LoA)을 제공할 수 있으면 OpenID 공유 인증 프로토콜을 사용할 수 있다. 이 경우 UA는 서비스 제공자를 대신하여 OP의 인증 서비스를 요청하는 프록시 서비스 제공자(proxy service provider) 역할을 수행하게 된다. UA는 OP와의 안전한 통신을 위한 association을 설정하고(O_Association Establishment) 브라우저를 경유하는 redirect 메시지를 통해 서비스 제공자가 요구하는 LoA가 포함된 OpenID 인증 요구 메시지를 OP에게 전달한다. OpenID 인증 요구 메시지(O_Request(AuthN, LoA))를 수신한 OP는 LoA에 적합한 인증 메카니즘(예, 사용자 ID/패스워드, X.509 Certificate 등)을 사용하여 사용자를 인증한다(O(Authentication)). 만약 해당 사용자가 이미 OP에 로그인되어 있으면 인증 과정을 생략하고 기존의 인증 결과를 사용할 수 있다. 사용자 인증을 완료한 OP는 인증 결과를 자신의 서명과 함께 redirect 메시지를 사용하여 프록시 서비스 제공자인 UA에게 전달한다(O_Respond(LoA_Assertion)).

OpenID 공유 인증 프로토콜을 통하여 인증 결과를 수신한 UA는 OP의 인증 결과(assertion)을 확인하여(Validate Assertion) 인증 결과와 OP의 정보가 포함된 인증 응답 메시지(Respond(AuthN, Result, OP))를 서비스 제공자(SP)에게 전달한다. 자신의 인증 보증 수준요구에 맞는 성공적인 인증 결과를 수신한 서비스 제공자는 신뢰 제공자 네트워크를 통해 OP의 인증 보증 수준을 확인할 수 있다(Verify(LoA, OP), Confirm(LoA, OP)). 따라서 SP는 안심하고 OP의 인증 결과를 사용할 수 있게 된다. 또한 UA를 통한 SP와 OP간의 인증 정보 교환 중재는 사용자의 SP 접근 정보가 OP에 의해 관찰되지 않도록 하기 때문에 OpenID의 프라이버시 문제도 해결할 수 있음을 알 수 있다.



(그림 3) OpenID 기반의 신뢰적인 공유 인증 프로토콜 동작 시나리오

4. 결론 및 향후 연구

인터넷 서비스 제공자들이 자체적인 인증 서버를 개발하고 운용하는 대신 제3의 인증 제공자의 인증 서비스를 사용하는 공유 인증 모델은 사용자 편의성, 개인 정보 노출, 개발 및 운용 비용 등의 측면에서 많은 장점이 있는 반면, 공유 인증 모델이 전체 인터넷 차원의 글로벌 적용에 이르기 위해서는 인증 제공자와 서비스 제공자간의 신뢰 문제를 개방적인 방법으로 풀 수 있어야 한다. 본 논문은 인증 보증 수준과 인증 정보 보호 수준에 대한 표준화, 인증 제공자의 인증 보증 수준과 서비스 제공자의 인증 정보 보호 수준에 대한 공인 서비스를 제공하는 신뢰 서비스 제공자의 연합체인 신뢰 제공자 네트워크, 그리고 서비스 제공자와 인증 제공자가 표준화된 인터페이스를 사용하여 사용자 에이전트를 경유하여 서로 통신하는 사용자 중심적인 동작에 기초하는 신뢰적인 개방형 공유 인증 프로토콜에 대한 프레임워크를 제안하고, OpenID 공유 인증 프로토콜 기반의 신뢰적인 공유 인증 프로토콜 구현 시나리오를 보였다. 제안된 신뢰적인 공유 인증 프로토콜 프레임워크는 신뢰 제공자 네트워크에 의해 공인된 어떤 서비스 제공자와 인증 제공자에게 적용될 수 있을 뿐만 아니라, 사용자 중심적인 동작을 통해 서비스 제공자와 인증 제공자 간의 불필요한 개인 정보 노출 방지를 통한 프라이버시 보장의 장점을 가진다.

본 논문이 제시한 공유 인증 프로토콜 프레임워크가 구체화되기 위해서는 먼저 공유 인증을 위한 인증 보증 수준과 인증 정보 보호 수준에 대한 표준화가 선행되어야 한다. 이를 위해 [18]의 연구 결과를 공유 인증 환경에 적합하게 확장하는 등의 표준화 노력이 요구되고, 기존 공유 인증 프로토콜들을 표준화된 인증 보증 수준과 인증 정보 보호 수준을 지원할 수 있도록 개선하여야 한다. 또한 표준화된 인증 보증 수준과 인증 정보 보호 수준을 지원하는 인증 제공자와 서비스 제공자를 공인하기 위한 신뢰 서비스 프레임워크도 표준화되어야 하고, 표준화된 신뢰 서비스 프레임워크에 따라 공인 서비스를 제공하는 신뢰 제공자들의 네트워크를 구축하는 방안도 마련되어야 한다. 기존 인터넷의 PKI(Public Key Infrastructure)와 오프라인의 신용카드 네트워크는 신뢰 제공자 네트워크 구축을 위한 좋은 모델이 될 수 있다.

참 고 문 헌

[1] A. Josang and S. Pope, "User Centric Identity Management", AusCERT Conference, 2005.

[2] T. E. Maliki and J.-M. Seigneur, "A Survey of User-centric Identity Management Technologies", Proc. of Int'l Conference on Emerging Security Information, Systems and Technologies, pp.12-17, 2007.

[3] E. Maler and D. Reed, "The Venn of Identity - Options and Issues in Federated Identity Management", IEEE Security & Privacy, March/April, 2008.

[4] P. Madsen and H. Itoh, "Challenges to Supporting Federated Assurance", IEEE Computer, May, 2009.

[5] M. I. Chehab and A. E. Abdallah, "Assurance in Identity Management Systems", 6th Int'l Conference on Information Assurance and Security, 2010.

[6] 박승철, "인터넷 신원 관리 2.0에 대한 분석과 3.0에 대한 전망", 해양정보통신학회논문지, 제15권 5호, 2011년 7월.

[7] T. E. Maliki and J.-M. Seigneur, "A Survey of User-centric Identity Management Technologies", Proc. of Int'l Conference on Emerging Security Information, Systems and Technologies, pp.12-17, 2007.

[8] D. P. Korman and A. D. Rubin, "Risks of the Passport Single Signon Protocol", IEEE Computer Networks, July, 2000.

[9] http://en.wikipedia.org/wiki/Windows_Live_ID

[10] Liberty Alliance Project, "Liberty ID-FF Architecture Overview", Liberty Alliance, 2004.

[11] Aries Fajar Dwiputera, "Single Sign-On Architectures in Public Networks(Liberty Alliance)", INFOTECH Seminar Communication Services, 2005.

[12] OASIS, "Security Assertion Markup Language(SAML) V2.0 Technical Overview", http://www.oasis-open.org, March, 2008.

[13] OpenID Foundation, "OpenID Authentication 2.0 - Final", http://openid.net/specs/openid-authentication-2_0.html, Dec., 2007.

[14] D. Chadwick and S. Shaw, "Review of OpenID", JISC Final Report(http://www.jisc.ac.uk/whatwedo/programmes/einfrastructure/reviewofopenid.aspx), Dec., 2008.

[15] K. Cameron and M. B. Jones, "Design rationale behind the Identity Metasystem Architecture", http://research.microsoft.com/en-us/um/people/mjb/papers/Identity_Metasystem_Design_Rationale.pdf, 2006.

[16] W. A. Alrodhan and C. J. Mitchell, "Addressing privacy issues in CardSpace", Proc. of 3rd Int'l Symposium on Information Assurance and Security, 2007.

[17] D. Thibeau and D. Reed, "Open trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies", A White Paper from the OpenId Foundation and Information Card Foundation, August, 2009.

[18] TTAIT-Xeaa, "개체 인증에 대한 보증 프레임워크(Entity Authentication Assurance Framework)", 한국정보통신기술협회, 2010년 12월 23일.

박 승 철

e-mail : scpark@kut.ac.kr

1985년 2월 서울대학교 계산통계학과 (학사)

1987년 2월 한국과학기술원 전산학과 (석사)

1996년 8월 서울대학교 컴퓨터공학과 (박사)

1987년 2월~1990년 10월 한국전자통신연구원

1990년 10월~1992년 2월 한국IBM

1992년 9월~2001년 4월 현대전자(현 하이닉스) 네트워크연구소장

2001년 5월~2003년 9월 현대네트웍스 연구소장/대표이사

2004년 3월~현 재 한국기술교육대학교 컴퓨터공학부 부교수

관심분야 : 멀티미디어 통신, P2P 컴퓨팅, 인터넷보안