Servicios Web – II

Fuente original: http://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf

Con la proliferación de los servicios web en Internet, surgió un problema de relevancia, la autenticación. Los servicios disponibles han crecido enormemente, y la mayoría de usuarios utilizan múltiples aplicaciones de terceros: por ejemplo, un usuario consulta su correo en un sistema de webmail, desde el teléfono o desde su cliente de correo. También es habitual la participación en redes sociales como facebook, linkedin, tuenti o twitter, etc. La mayoría de esas aplicaciones requieren que el usuario se autentique; es decir, que demuestre de algún modo (habitualmente usando un identificador de usuario único y una contraseña asociada) que es quien dice ser.

Al tratarse de aplicaciones independientes entre sí, en principio cada una de ellas utilizaría su propio sistema de autenticación y de gestión de datos personales, lo cual implica inconvenientes al usuario cada vez más graves a medida que el número de sistemas que utiliza crece.

Surge la necesidad de conocer cuales son las tendencias actuales respecto a la autenticación y autorización en Internet.

Autenticación vs. autorización

Antes de seguir, es necesario hacer una distinción clara entre dos tipos de servicios ofrecidos por las tecnologías que vamos a describir.

- **Autenticación**: consiste en un sistema para certificar que el usuario es quien dice ser; lo más común es utilizar una combinación de identificador de usuario único y contraseña.
- **Autorización**: consiste en dar acceso a una serie de recursos a un usuario o sistema (para ello, el usuario o el sistema previamente tendrán que haberse autenticado).

Protocolos y estándares ampliamente adoptados

Una primera solución evidente al problema de la autenticación sería el uso de algún tipo de **certificado personal** (basado, por ejemplo, en el estándar X.509) emitido y validado por alguna autoridad central de confianza. Si bien este tipo de certificados son útiles para gestiones con determinadas entidades, **no son prácticos en general para el acceso a servicios de Internet**. Por este motivo han surgido varios protocolos de autenticación y autorización en Internet.

OpenID

El protocolo abierto **OpenID**, cuya primera versión fue definida en 2005 para su uso en el sitio web LiveJournal, es un **protocolo de autenticación federada**, y consiste básicamente en que el usuario selecciona un servidor externo (el “proveedor” de OpenID) que va a ser el que va a validar su identidad en un sistema determinado (el “consumidor” de OpenID).

Problemas de OpenID:

- Complejidad: no se implementa fácilmente.
- Seguridad: es un protocolo muy vulnerable al phishing.
- Privacidad: los proveedores de OpenID tendrán mucha información del usuario.
- Confianza: ¿quién es realmente el usuario?.
- Usabilidad: puede ser incómodo y/o complejo para el usuario.
- Adopción: los proveedores de servicios tienen pocos motivos para aceptarlo como autenticación.
- Disponibilidad: se incrementa la dependencia de servidores.
- Patentes: no es un protocolo “tan” abierto.

OAuth

El protocolo abierto OAuth, a diferencia de OpenID, es un **protocolo de autorización**; más exactamente, **de delegación de acceso;** es decir, permite definir cómo un tercero va a acceder a los recursos propios. Empezó a definirse en 2006 y en 2007 se publicó la primera versión oficial. El propósito de este protocolo es, pues, que un usuario que tiene determinados recursos en un servidor (el “proveedor” de OAuth) pueda dar acceso a un tercero (el “consumidor”, usualmente un sitio web) a parte o todos esos recursos, sin necesidad de que ese tercero conozca su usuario y contraseña, ya que con esos datos tendría el control total de la cuenta.

Problemas de OAuth:

- Complejidad.
- Orientado a navegadores.
- Seguridad.

OAuth 2.0

OAuth 2.0 pretende ser una versión revisada y simplificada de OAuth. Aventaja a la versión anterior en una mayor simplicidad de implementación, y en una arquitectura más robusta y que da soporte a mayor número de plataformas.

Existe cierta confusión sobre si OAuth es o no un protocolo de autenticación de usuario. Estrictamente hablando no lo es, ya que no define ningún mecanismo explícito destinado a autenticar la identidad del usuario. Por tanto, cuando se habla del "mecanismo de autenticación de OAuth", en realidad se están refiriendo al mecanismo de autenticación propio del sitio web proveedor de OAuth, que puede ser cualquiera: autenticación http básica, OpenID, etc.

Nuevos Protocolos y estándares

OpenID OAuth Hybrid Protocol

Como hemos visto, OpenID y OAuth son protocolos con objetivos distintos aunque complementarios: autenticación de usuario (federada) y autorización, respectivamente. El protocolo híbrido OpenID OAuth combina ambos sistemas, integrándolos en una interfaz única.

Facebook Connect

Debido al enorme incremento de usuarios y, en consecuencia, de datos personales que ha experimentado Facebook en los últimos años, la compañía lanzó en 2008 su propio sistema conocido como Facebook Connect. Con ese movimiento, Facebook pretendía posicionarse como repositorio central de identidad de los usuarios en Internet. En la actualidad Facebook parece haber abandonado Facebook Connect para adoptar el protocolo 2.0 de OAuth.

OpenID Connect

El protocolo OpenID Connect es la última propuesta para reactivar OpenID. Su propósito es redefinir y simplificar el protocolo construyéndolo sobre el protocolo OAuth; de ese modo se aprovecha el trabajo desarrollado para OAuth, que parece estar extendiéndose rápidamente, dotándolo de una funcionalidad estándar de autenticación que, como hemos visto anteriormente, no posee.

Otros sistemas

Algunos de los grandes proveedores de servicios en Internet han definido, en algún momento, su sistema propio de autenticación y/o autorización. Sin embargo, la mayoría de ellos están adoptando estándares como OpenID y, especialmente, OAuth; es el caso, por ejemplo, de MySpace, Twitter o Yahoo!.

Otro estándar abierto para el intercambio de recursos de identidad es Security Assertion Markup Language (SAML). Está basado en XML, y su principal propósito es servir de marco para protocolos de autenticación federada. Este protocolo sirve de base para algunos sistemas propietarios de single-sign-on, pero no es utilizado por los grandes proveedores de servicios en Internet.

Resumiendo

Protocolo	Propósito	Última versión / estado	Ventajas	Inconvenientes
OpenID	Autenticación (federada)	2.0 (de 2007)	*Single-sign-on* sin depender de ningún proveedor específico (federado).	Protocolo complejo y antiguo; potenciales problemas de seguridad, privacidad, usabilidad. Pocos incentivos para ser consumidor.
OAuth	Autorización	2.0 (en borrador, pero muy utilizada)	Muy utilizado en servidores de Internet.	Dependencia de un servidor para la autenticación (delegada).
OpenID OAuth Hybrid Protocol	Autenticación (federada) + autorización; interfaz única	Borrador (pero adoptado por grandes proveedores)	Una única interfaz para autenticación (OpenID) + autorización (OAuth).	Depende de que los servidores implementen ambos protocolos.
Facebook Connect	Autenticación (delegada) + autorización + funciones red social	Abandonado en favor de OAuth 2.0	Parte de una amplia base de usuarios y datos personales.	Muy ligado a un único proveedor. Problemas de privacidad.
OpenID Connect	Autenticación (federada) a partir de OAuth	Propuesta (sobre OAuth 2.0)	Las mismas ventajas que OpenID con una implementación más sencilla; aprovecha las implementaciones de OAuth 2.0.	Similares a OpenID; pocos incentivos para ser consumidor.