Fuente:
IT Connect

Uno de los retos más difíciles de afrontar a lo largo de mi vida profesional como arquitecto y desarrollador, ha sido la seguridad y más concretamente los procesos de autenticación y de autorización.

Se trata de dos procesos que todo sistema con cierta envergadura debe tener, siempre que se deba controlar el acceso a la información y la ejecución de determinados procesos relacionados. Para ello, no solo se debe disponer de profundos conocimientos técnicos, sino también conocer con detalle el proceso de negocio en el que está envuelto el sistema en cuestión.

En la actualidad la autenticación/autorización no es algo que solo puedan realizar las personas: existen sistemas dotados de autonomía lógica con acceso a procesos y repositorios de información protegida, por lo que deben disponer del nivel de complejidad y calidad criptográfica adecuadas para lo que se desea proteger.

Tanto si lo que queremos autenticar/autorizar es una persona, como si se trata de un sistema o aplicación, debemos mantener un buen equilibrio entre la complejidad técnica de implementación y el proceso de negocio implicado. En cualquier caso, como anteriormente he adelantado, hay que tener un buen nivel, a fin de mantener ese imprescindible equilibrio. En caso contrario diseñaremos sistemas muy robustos pero tan complicados de implementar y usar que dejan de ser útiles. O, por el contrario, simplificaremos tanto el proceso de negocio que el sistema diseñado será en exceso frágil y, por tanto, la autenticación y/o autorización serán inútiles.

A día de hoy disponemos de múltiples estándares que nos facilitan la creación de nuestros sistemas. Pero son tres los principales actores en juego en esta área: OAuth, SAML, y Open ID. Aunque dos de sus principales funciones son la autenticación y la autorización, la más importante y por ello la más utilizada es la capacidad de federación de identidad con otros sistemas similares. Cualquier proveedor de aplicaciones o servicios de Internet, o que necesite ofrecer sus servicios por este medio ha de ser compatible con al menos uno de estos estándares o contar con el apoyo de todos ellos.

Generalmente, estos sistemas se utilizan para autenticar a las personas al usar aplicaciones de nube, en lugar de autenticar o autorizar a los componentes de software o subsistemas. Pero no hay nada que impida utilizar esta tecnologías para securizar la comunicación entre procesos o sistemas.
SAML

Actualmente se encuentra en la versión 2.0. Su utilidad se enmarca en la coordinación de los procesos de autenticacion y autorizacion en sistemas centralizados. Al tratarse de una definición que descansa sobre la especificación XML, toda su fortaleza reside en la aplicación correcta de sus pautas y en el adecuado uso de

terceras tecnologías, como son: SSL o TLS para el transporte de las conversaciones seguras, tecnologías de firma y cifrado de XML para garantizar la integridad de los datos, o el propio SOAP para extender determinadas funciones especiales.

OAuth

Tanto OAuth como el más nuevo OAuth 2.0 son protocolos comunes que se utilizan para autenticar y autorizar a los usuarios en las aplicaciones basadas en webs de terceros. Diseñado para HTTP, OAuth utiliza tokens de acceso como base de su funcionamiento y su verdadero potencial reside en la adecuada combinación de sus procesos básicos, como son: el perfilado y protección de la información a publicar, la generación del token y su relación con el propietario de la información o proceso y el consumidor final, y la definición de unas adecuadas reglas de consumo.

OpenID

La última versión de OpenID, OpenID Connect, se basa en OAuth 2.0 como un protocolo de autenticación. Es compatible con la firma y el cifrado fuerte. Principalmente se utiliza para la autenticación delegada, de forma que si el sitio a consumir es compatible con OpenID, el consumidor no necesita crearse una identidad para consumir la información, siendo únicamente necesario facilitar las credenciales obtenidas en cualquier otro sitio compatible, donde el que ofrece la información deberá verificar la credencial recibida. Este sistema requiere que la conversación entre el que solicita la autenticación y el que la ofrece sea de forma segura. Así mismo una de sus mayores ventajas reside en su facilidad de uso en los navegadores actuales mediante XRI.

CAS

Es un protocolo de inicio de sesión único para aplicaciones web. Se encuentra en su tercera versión y, como su nombre indica, consiste en un sistema de autenticación central, cuya principal funcionalidad es hacer de SSO entre múltiples aplicaciones de forma unificada. De este modo, el consumidor de los servicios solo ha de facilitar su credenciales una única vez. Al no tratarse de un sistema distribuido disfruta de gran solidez, no siendo necesario dotarlo de terceros sistemas para su correcto funcionamiento.

Con una sólida comprensión de estas cuatro tecnologías, así como un conocimiento adecuado del área de negocio al que desea aplicarlas, no será necesario que realice grandes y complicados desarrollos para construir un sistema robusto de autenticación y autorización. Únicamente aplicando “Buenas prácticas” en cada caso y un poco de lógica, obtendremos procesos usuales, seguros, fáciles de mantener y, por supuesto, económicos.

Disponible en:

http://itconnect.lat/latinoamerica/3741 [1]

Links

[1] http://itconnect.lat/latinoamerica/3741