Hacia el *single sign-on* en la integración de herramientas externas en Entornos de Aprendizaje Virtual

Carlos Alario Hoyos, Eduardo Gómez Sánchez, Miguel L. Bote Lorenzo,
Juan I. Asensio Pérez, Adolfo Ruiz Calleja, Guillermo Vega Gorgojo
Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad de Valladolid,
Paseo de Belén 15, 47011, Valladolid, España.
{calahoy@gsic, edugom@tel, migbot@tel, juaase@tel, adolfo@gsic, guiveg@tel}.uva.es

***Resumen*—Uno de los aspectos más importantes que deben considerar las propuestas de integración de herramientas externas en Entornos de Aprendizaje Virtual (VLE), son los requisitos de seguridad que impone cada VLE y cada herramienta a la hora de permitir el acceso a su funcionalidad. El objetivo debe ser que los educadores y estudiantes puedan acceder de forma transparente a las distintas aplicaciones. Para ello, puede hacerse uso de los mecanismos de autenticación única o *single sign-on* (SSO). No obstante, las propuestas que tratan el SSO en la integración de herramientas lo hacen de forma muy específica o imponiendo una gran cantidad de requisitos. Por ello, este artículo presenta una solución que da soporte al SSO en la integración de múltiples herramientas externas en distintos VLE, basándose en los criterios de generalidad, y en la no imposición de requisitos a los proveedores de VLE y herramientas.**

I. Introducción

El uso de entornos de aprendizaje virtual (VLE - *Virtual Learning Environments*) para apoyar la realización de situaciones de aprendizaje es una tendencia en aumento a lo largo de los últimos años, gracias en parte al éxito de sistemas como Moodle[1], LAMS[2], .LRN[3] o Sakai[4]. Estos VLE suelen incluir algunas herramientas en sus distribuciones, tales como cuestionarios, *chats* o foros. Sin embargo, se ha detectado una limitación con respecto al número y tipo de herramientas que presentan, la cual dificulta el diseño y la realización de las situaciones de aprendizaje [1]. Por ello, numerosos autores se han inclinado por la integración de herramientas externas [2], [3], [4], [5]. A esto contribuye además la creciente cantidad de herramientas web para usos educativos [6]; por ejemplo, Google Apps[5], Twitter[6], o Delicious[7].

Uno de los principales problemas que se plantean en las propuestas de integración es la gestión de la seguridad. El motivo es que cada proveedor de VLE y herramienta puede definir diferentes mecanismos para permitir el acceso a los recursos. Uno de los más empleados consiste en solicitar las credenciales (normalmente en forma de usuario y contraseña) a los educadores y estudiantes, para que éstas sean validadas en los dominios del proveedor. En ocasiones, pueden utilizarse unas credenciales comunes para autenticarse en distintos VLE o herramientas, como las que se definen bajo el estándar de autenticación OpenID[8]. Otras veces, las credenciales de varios sistemas se validan contra una misma base de datos. En este sentido, es una política frecuente que distintos VLE dentro de una misma organización utilicen un servidor externo centralizado, accesible por ejemplo, mediante LDAP (Protocolo Ligero de Acceso a Directorios - *Lightweight Directory Access Protocol*) [7]. En cualquiera de estas situaciones se persiguen dos objetivos complementarios: facilitar el acceso y la autenticación de los usuarios en las diferentes herramientas integradas en los VLE, y minimizar la carga administrativa que supone la gestión adicional de la seguridad asociada a dicha integración. Ambos objetivos pueden cubrirse mediante una política de autenticación única (SSO - *single sign-on*) [8], la cual se incluye en bastantes de las propuestas de integración [9], [10], [14]. El problema es que estas soluciones son específicas para ciertas combinaciones VLE-herramienta, no pudiendo ser extendidas como una solución más general.

El objetivo de este artículo es realizar una propuesta que permita el SSO en la integración de múltiples herramientas externas en distintos VLE. Para ello, se parte de un escenario educativo en la sección II del cual se extraen los requisitos de diseño. A continuación, la sección III explora los mecanismos de autenticación que soportan los principales VLE y herramientas. En la sección IV se analizan las limitaciones de las propuestas de integración que consideran el SSO, para posteriormente proponer en la sección V una solución general. Finalmente, la sección VI recoge las conclusiones y líneas futuras.

II. Ejemplo de escenario educativo

Esta sección pretende ilustrar los problemas de seguridad asociados a la integración de herramientas externas en VLE. Para ello, se parte de una situación de aprendizaje inicial de la que se extrae un conjunto de requisitos de diseño para la propuesta de solución.

II-A. Situación de aprendizaje

Los profesores de uno de los últimos cursos de secundaria quieren que sus alumnos conozcan más detalles de la geografía española y a la vez fomenten sus capacidades de abstracción y discusión. Para ello, plantean una situación de aprendizaje utilizando las instalaciones de Moodle y MediaWiki[9] que posee su instituto. La clase se divide en varios grupos dependiendo de las ciudades a estudiar. Los usuarios de cada uno de los grupos deben consultar en primer lugar, información sobre su ciudad en Wikipedia[10]. Después deben

[1]http://moodle.org
[2]http://lamsinternational.com
[3]http://dotlrn.org
[4]http://sakaiproject.org
[5]http://google.com/apps
[6]http://twitter.com
[7]http://delicious.com
[8]http://openid.net
[9]http://mediawiki.org
[10]http://wikipedia.org

elaborar un texto con los puntos más importantes en una página de MediaWiki. Finalmente, han de hacer una breve presentación con Google Presentations[11].

II-B. Problemas de seguridad en la integración

El análisis de la seguridad parte de que los educadores y los estudiantes disponen de credenciales propias para acceder a su cuenta en Moodle. Una vez autenticados, es deseable que existan mecanismos de SSO que les permitan acceder a las herramientas mencionadas de forma transparente. En este sentido, Wikipedia no impone ningún requisito de seguridad para el acceso a la información que ofrece. Sin embargo, MediaWiki y Google Presentations requieren que los usuarios estén autorizados para acceder o modificar sus recursos. Esto genera la necesidad de disponer de credenciales adicionales, bien sean propias (una por educador/estudiante) o institucionales (compartidas por toda una clase/instituto/departamento). Disponer de credenciales propias para cada herramienta supone una sobrecarga de gestión, normalmente asumida por los propios usuarios. Disponer de credenciales institucionales puede ser una limitación importante a la hora de definir, desarrollar y evaluar actividades que incluyan grupos, ya que se dificulta la separación en el acceso a diferentes recursos dentro de una misma herramienta para cada grupo.

Las herramientas que componen esta situación de aprendizaje no aparecen actualmente en las distribuciones de los principales VLE, por lo que deben ser integradas. En esta línea, muchas de las propuestas que atacan el problema de integración lo hacen de forma específica para un VLE y una herramienta determinados [1], como por ejemplo los módulos desarrollados para Moodle [10]. El problema de este tipo de módulos es que suponen un gran esfuerzo de desarrollo para integrar múltiples herramientas en distintos VLE. Por ello, otras propuestas de integración se decantan por una arquitectura más modular en la que ciertos elementos pueden ser desarrollados y mantenidos por terceros [5]. Sin embargo, esto genera un problema de confianza [11], ya que para conseguir el SSO hay que atravesar dichos elementos.

II-C. Requisitos de diseño

A partir de la situación de aprendizaje inicial y de los problemas de seguridad detectados se establecen los siguientes requisitos de diseño.

1. **El VLE es el punto de entrada**. Los educadores y los estudiantes disponen de credenciales válidas en el VLE que les autorizan a desarrollar las situaciones de aprendizaje.
2. **Debe facilitarse el SSO a los educadores y a los estudiantes**. Las autenticaciones que se lleven a cabo para poder utilizar las herramientas han de ser transparentes, en la medida de lo posible.
3. **La solución propuesta ha de ser lo más general posible**. Se valora que se pueda conseguir el SSO en la integración de múltiples herramientas en distintos VLE, pudiendo haber sido éstas desarrolladas por distintos proveedores y con diferentes tecnologías.
4. **La solución propuesta no debe añadir requisitos a los proveedores de VLE y herramientas**. El motivo es que, en la mayoría de los casos, éstos no estarán dispuestos a modificar sus sistemas.
5. **Debe minimizarse la carga relacionada con la gestión de credenciales**. Es conveniente facilitar el trabajo de gestión de credenciales a los administradores de los distintos VLE.

[11] http://docs.google.com

III. Mecanismos básicos de seguridad

Los VLE y herramientas incluyen sus propios mecanismos para gestionar la seguridad. Esta sección analiza y discute su adecuación como parte de la propuesta de solución.

III-A. Análisis de los VLE

Los educadores y estudiantes que disponen de una cuenta válida en un VLE se autentican introduciendo sus credenciales en el sistema. Éstas pueden ser validadas contra la base de datos interna del VLE, o contra una base de datos o servidor externo. Por ejemplo, Moodle soporta, entre otros, servidores CAS (Servicio de Autenticación Centralizado - *Central Authentication Service*) o IMAP (Protocolo de Acceso a Mensajes de Internet - *Internet Message Access Protocol*). Sin embargo, LDAP es el único servidor externo soportado actualmente por las distribuciones de los principales VLE. De forma adicional, hay que mencionar que existen extensiones de Moodle, LAMS y Sakai para soportar Shibboleth[12], un mecanismo de autenticación SSO que puede utilizarse dentro de una misma federación u organización de confianza.

III-B. Análisis de las herramientas

Cada herramienta presenta sus propios mecanismos de seguridad, variando desde las que ofrecen libre acceso a su funcionalidad a aquéllas que requieren autenticación de usuarios. En este sentido, uno de los mecanismos de SSO más utilizado es OpenID, ya que permite autenticarse en una gran lista de sitios y herramientas web [12] con unas credenciales únicas proporcionadas por alguno de sus proveedores, entre ellos Google o Yahoo! De esta forma, los usuarios de Zoho[13] o Flickr[14] pueden autenticarse con las credenciales de cualquiera de estos dos proveedores. Algunas herramientas permiten también utilizar servidores o bases de datos externas. Por ejemplo, se han desarrollado extensiones para Wordpress o MediaWiki con el objetivo de soportar autenticación contra servidores CAS, IMAP y LDAP. Además, existen mecanismos de autorización delegada [9], que permiten el acceso a determinados recursos para un cierto usuario y generalmente durante un periodo de tiempo predeterminado. OAuth [13] es el protocolo estandarizado más extendido para proporcionar este tipo de autorización. Se basa en el intercambio de *tokens* o permisos entre el usuario final, el servicio que proporciona el acceso a la aplicación, y un tercero que es el que solicita y gestiona los permisos. Algunas herramientas como Google Apps, Yahoo! o Delicious implementan una interfaz OAuth. Además, existen otros mecanismos propietarios de autorización delegada, como AuthSub[15] de Google, BBAuth[16] de Yahoo! o la interfaz de autorización propia de Flickr[17].

[12] http://shibboleth.internet2.edu/
[13] http://zoho.com
[14] http://flickr.com
[15] http://code.google.com/intl/es-ES/apis/accounts/docs/AuthSub.html
[16] http://developer.yahoo.com/auth/
[17] http://www.flickr.com/services/api

III-C. Clasificación y discusión

Los mecanismos que permiten la **autenticación a través de un elemento o proveedor externo** pueden facilitar el SSO entre un VLE y una herramienta siempre y cuando ambos compartan el elemento que valida la autenticación (la base de datos, el servidor externo, OpenID). Aquí pueden surgir problemas de confianza dependientes de la arquitectura de integración, ya que utilizar elementos de terceros puede producir una suplantación de identidad de un usuario registrado en un VLE en las herramientas. Además, hay que considerar la confianza que se deposita en el elemento externo encargado de la validación. Esto se ejemplifica claramente en las herramientas que soportan OpenID, ya que la decisión de aceptar credenciales de uno u otro proveedor depende del nivel de confianza que ofrezca éste, siendo Google o Yahoo! los más aceptados.

Los mecanismos de **autorización delegada** también pueden facilitar el acceso transparente a un recurso en una herramienta integrada en un VLE durante un tiempo determinado. Para ello, este último debe conocer a quién solicitar los permisos correspondientes. En este caso, los problemas de confianza son menores, ya que los permisos se orientan a recursos concretos, en lugar de ofrecer libre acceso a una herramienta.

Los mecanismos que permiten el acceso a diferentes sistemas dentro de un mismo dominio se basan en la **federación de confianza**. Para ello, delegan la gestión y la autenticación de usuarios a una autoridad que pertenece al dominio y en quien se puede confiar. En este caso no los elementos que realizan la integración corren en máquinas del mismo dominio en el que se encuentran los VLE y las herramientas. El principal problema de estos mecanismos es que muchas de las herramientas de terceros que pueden ser integradas están disponibles en la web, y no pueden formar parte de una federación de confianza.

IV. Propuestas existentes para el SSO entre VLE y herramientas

Muchas propuestas de integración atacan el problema para una combinación VLE-herramienta. Por ejemplo, los módulos que permiten integrar Drupal[18] y Wordpress en Moodle requieren que el VLE y la herramienta compartan un mismo dominio y una misma base de datos [10]. En esta línea, Moodlerooms[19] ha desarrollado un módulo específico para integrar Google Apps en Moodle incluyendo SSO dentro de una federación de confianza. Su principal limitación es que requiere disponer de una cuenta de dominio de Google Apps, algo que no es asumible para la mayor parte de instituciones educativas. Otro caso concreto es la autenticación compartida de LAMS en su integración en Moodle o Sakai [14]. A pesar de ello, la especificidad del protocolo de intercambio de información definido, unido a la ausencia de estándares con una mayor aceptación hacen que sea difícil generalizar esta propuesta. Más genérica es la solución Crowd de Atlassian[20], pensada para automatizar la autenticación en ciertas herramientas web. Lamentablemente, a excepción de Google Apps, las aplicaciones que soportan Crowd han sido desarrolladas por la propia empresa que comercializa esta solución. Finalmente, merece la pena destacar *Reverse OAuth* [9], una modificación del mecanismo de autorización delegada OAuth, pensada para el contexto de integración de herramientas externas en VLE. Sin embargo, esta solución presenta varios problemas: el primero es que no considera aquellas situaciones de aprendizaje en las que se requiera el uso de grupos, ya que asume que se dispone de una única credencial institucional en la herramienta; además propone modificar un protocolo que se encuentra en proceso de estandarización, por lo que sus expectativas de implementación en los distintos proveedores es, a priori, muy limitado.

[18]http://drupal.org

[19]http://moodlerooms.com

[20]http://atlassian.com/software/crowd

V. Propuesta de single sign-on en la integración de múltiples herramientas externas en distintos VLE

Las limitaciones de las soluciones presentadas hacen que no puedan ser utilizadas, de forma general, en escenarios como el de la sección II. Por ello, esta sección realiza una propuesta de solución a partir de los requisitos de diseño iniciales.

V-A. Consideraciones previas

Las siguientes consideraciones han llevado a descartar otros trabajos relacionados.

- No puede suponerse que se dispone de una federación de confianza, ya que no es lo habitual en las instituciones educativas, especialmente si son de pequeño tamaño.
- Cada usuario debe tener unas credenciales propias en las herramientas que forman parte de las situaciones de aprendizaje.
- La solución propuesta debe ser válida independientemente de la arquitectura que dé soporte a la integración.
- Existen herramientas que a pesar de requerir autenticación para acceder a su funcionalidad no soportan ningún mecanismo de SSO ni ofrecen una API programática de autenticación.

V-B. Propuesta de solución

La propuesta consiste en combinar varios mecanismos de autenticación a través de un elemento externo, para facilitar el SSO con el mayor número de VLE y herramientas. Para ello, se utiliza un servidor LDAP que gestiona el almacenamiento, la publicación, y la utilización de credenciales. Esta decisión está condicionada por el hecho de que LDAP es el único protocolo soportado actualmente por los principales VLE.

- *Almacenamiento*. La base de datos asociada al servidor LDAP almacena un conjunto de credenciales válidas en distintos VLE y herramientas para cada uno de los estudiantes y educadores, asociando las cuentan de usuario en los VLE a las sus credenciales en las herramientas. Esta asociación incluye credenciales genéricas como las de OpenID, y específicas, para diferentes proveedores externos.
- *Publicación*. La información en el servidor LDAP debe almacenarla cada usuario de forma distribuida a fin de evitar el aumento de la carga del administrador. La interfaz de publicación de credenciales debe ser externa al VLE, de tal forma que no se introduzcan requisitos adicionales sobre estos proveedores.

- *Utilización*. Los elementos que componen la arquitectura de integración acceden al servidor LDAP para recuperar las credenciales correspondientes y utilizarlas para realizar el SSO. Únicamente se requiere indicar la referencia a la cuenta de usuario y a la herramienta concreta o al tipo de credencial.

El problema relacionado con el posible uso de elementos de terceros se resuelve incluyendo una lista de sitios de confianza en los módulos que extienden la funcionalidad de los VLE. Además, para probar su identidad y evitar cualquier tipo de suplantación, cada uno de estos sitios debe disponer de un certificado emitido por una autoridad certificadora externa, como por ejemplo CAcert.org[21] que ha de incluir en sus comunicaciones con otros elementos. La Figura 1 recoge la visión general de la propuesta.

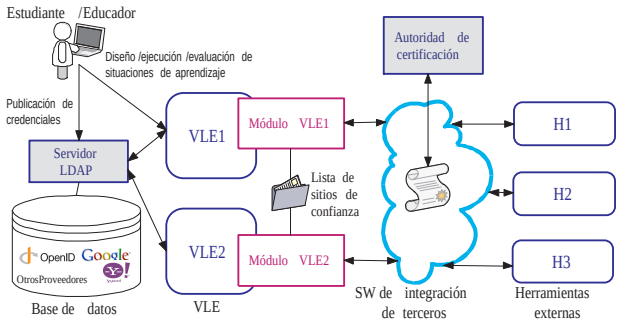

Figura 1: Propuesta de *single sign-on* en la integración de múltiples herramientas externas en distintos VLE

V-C. *Análisis de la propuesta*

El hecho de que los **VLE sean el punto de entrada** del SSO condiciona la decisión de sincronizar la información sobre las cuentas de usuarios en un servidor LDAP accesible desde los VLE, y relacionarlas con las credenciales en las diferentes herramientas. Esta relación es la que permite dar **soporte al SSO de educadores y estudiantes** a lo largo de las situaciones de aprendizaje. Para ello, se solicitan al servidor externo las credenciales de cada usuario en la medida en que sean requeridas por las herramientas. Es importante destacar que la solución es bastante **general**, ya que puede dar soporte al SSO en un gran número de herramientas. Para ello, se utilizan como base las credenciales de los usuarios en OpenID, Google o Yahoo!, pudiendo añadirse las de otras herramientas específicas. En este punto hay que comentar que el sistema debe estar preparado para seguir funcionando aun en los casos en los que los usuarios no hayan publicado aún sus credenciales; simplemente no podrá facilitarse el SSO. La solución propuesta **no impone requisitos a los proveedores de herramientas o de VLE**. Únicamente se debe añadir una lista de sitios de confianza y la capacidad de preguntar por los certificados como parte de la lógica de los módulos que extienden la funcionalidad de los VLE. Finalmente, el **administrador del sistema reduce su carga** ya que confía la gestión de credenciales a un elemento externo. Si bien es cierto que la propuesta requiere configurar y sincronizar el servidor LDAP, esta tarea se realiza una única vez, por lo que no supone un esfuerzo de administración considerable.

[21] http://cacert.org

VI. Conclusiones y líneas futuras

Este artículo presenta una propuesta que da soporte al SSO en la integración de múltiples herramientas externas en distintos VLE, utilizando un servidor externo y relacionando las credenciales de los educadores y estudiantes en distintas herramientas, con las cuentas en los VLE. Además, la propuesta cubre los problemas de suplantación que pueden surgir al utilizar *software* mantenido por terceros. Esta solución cumple con los requisitos de diseño iniciales y además, se diferencia de otras propuestas existentes en su generalidad, y en la no imposición de requisitos a los proveedores de herramientas y VLE. Su principal limitación es que impone que los estudiantes y educadores dispongan de credenciales propias en las herramientas que van a utilizar. Las líneas futuras pasan por la aplicación de esta solución a algunas propuestas de integración de herramientas ya desarrolladas [1], y su validación en situaciones de aprendizaje que incluyan múltiples herramientas que requieran seguridad.

Agradecimientos. Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación (TIN2008-03023) y por la Junta de Castilla y León (VA106A08).

Referencias

[1] C. Alario-Hoyos, J.I. Asensio-Pérez, M. Bote-Lorenzo, E. Gómez Sánchez, G. Vega-Gorgojo, y A. Ruiz-Calleja. Integration of external tools in Virtual Learning Environments: main design issues and alternatives. En *Actas de la Décima Conferencia Internacional en Advanced Learning Technologies, ICALT 2010 (aceptado para publicación)*, Sousse, Túnez, julio 2010. IEEE Computer Society.

[2] M. L. Bote-Lorenzo, E. Gómez-Sánchez, G. Vega-Gorgojo, Y. A. Dimitriadis, J. I. Asensio-Pérez, y I. M. Jorrín-Abellán. Gridcole: A tailorable grid service based system that supports scripted collaborative learning. *Computers and Education*, 51(1):155–172, 2008.

[3] C. Severance, J. Hardin, y A. Whyte. The coming functionality mash-up Personal Learning Environments. *Interactive Learning Environments*, 16(1):47–62, 2008.

[4] S. Wilson, P. Sharples, D. Griffiths, y K. Popat. Moodle Wave: Reinventing the VLE using Widget technologies. En *Actas del Segundo Workshop Internacional en Mashup Personal Learning Environments, (MUPPLE09)*, pp. 47–58. Niza, Francia, septiembre 2009.

[5] L. Fuente-Valentin, Y. Miao, A. Pardo, y C. Delgado-Kloos. A Supporting Architecture for Generic Service Integration in IMS Learning Design. En *Actas de la Tercera Conferencia Europea en Technology Enhanced Learning, (ECTEL08)*, pp. 467–473, Maastricht, Holanda, septiembre 2008. Springer-Verlag.

[6] Top 100 Tools for Learning 2009. URL: http://www.c4lpt.co.uk/recommended/. Última visita: marzo 2010.

[7] Lightweight Directory Access Protocol (LDAP): The Protocol. URL: Última visita: marzo 2010.

[8] A. Pashalidis y C.J. Mitchell. A Taxonomy of Single Sign-On Systems. En *Information Security and Privacy, Octava Conferencia de Australasia, ACISP 2003*, pp. 249–264, Wollongong, Australia, julio, 2003. Springer-Verlag.

[9] J. Fontenla, M. Caeiro, M. Llamas, y L. Anido. Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems. *Computers & Security*, en prensa, *corrected proof*, 2009.

[10] Moodle. Modules and Plugins. URL: http://moodle.org/mod/data/view.php?id6009. Última visita: marzo 2010.

[11] L. Kagal, T. Finin, y A. Joshi. Trust-Based Security in Pervasive Computing Environments. *Computer*, 34:154–157, 2001.

[12] OpenIDDirectory. URL: http://openiddirectory.com/. Última visita: marzo 2010.

[13] OAuth Core 1.0. URL: http://oauth.net/core/1.0a/. Última visita: marzo 2010.

[14] LAMS and 3rd Party App Integration Mechanism. URL: http://wiki.lamsfoundation.org/display/lams/LAMS+and+3rd+Party-+App+Integration+Mechanism. Última visita: marzo 2010.