Privacidad en el servicio de directorio

Privacy in Directory Services

J. A. Accino, V. Giralt y J. Masa

Resumen

En la actualidad, los servicios de directorio institucionales se ven abocados a un claro conflicto de intereses. Por una parte, está la necesidad de los miembors de la institución de encontrar a otros miembros de la misma u otra institución. Por la otra, están los derechos de los individuos a la privacidad.

Esto nos ha hecho desarrollar un mecanismo para solucionar este conflicto, utilizando controles de acceso que pueden ser gestionados tanto por la institución como por los individuos. Presentaremos nuestra implementación de tal mecanismo por medio de clases y atributos LDAP y Listas de Control de Acceso de OpenLDAP.

Palabras clave: privacidad, servicios de directorio

Summary

Modern institutional directory services nowadays are confronting a clear conflict of interests. On the one hand, there is the need of some members of one institution to find other members in the same or different institution. On the other hand, there are the privacy rights of individuals.

This has made us to develop a mechanism to solve this confrontation using information access controls that can be managed both by the institutions and the individuals. This presentation will discuss our implementation of such mechanism based on LDAP classes and attributes, and OpenLDAP Access Control Lists.

Keywords: privacy, directory services

Hemos desarrollado un mecanismo utilizando controles de acceso que pueden ser gestionados tanto por la institución como por los individuos

1.- El problema

Las instituciones públicas, como tales, están obligadas a dar servicio al público, uno de los cuales es ofrecer información sobre sus miembros que son, en la mayoría de los casos, funcionarios públicos. También, estas personas, en general, desean ser localizadas, localizar y tener contacto con, otras personas que trabajen en temas similares. El uso de las nuevas tecnologías de comunicación facilita estas tareas, pero esta misma explosión tecnológica ha hecho muy fácil obtener información e invadir la privacidad de los individuos, lo que ha llevado a un aumento de la sensibilidad de las personas y las instituciones en temas de privacidad.

Las preocupaciones sobre la privacidad han dado lugar, en muchos países, a leyes más restrictivas en cuanto a la diseminación de información

Estas preocupaciones sobre la privacidad han dado lugar, en muchos países, a leyes más restrictivas que las existentes en cuanto a la diseminación de información. La Unión Europea ha generado una serie de directivas sobre compartición y protección de datos personales, como por ejemplo la Directiva 95/46/EC del Parlamento Europeo y el Consejo de Europa, del 24 de octubre de 1995 sobre la protección de los individuos en cuanto al procesamiento de datos personales y sobre el libre movimiento de dichos datos.

Tales directivas han dado lugar a leyes como la LOPD española (15/1999, de 13 de diciembre) que indica que los individuos deben dar su consentimiento para la publicación de sus datos personales, de acuerdo con los artículos 6 y 11.

Las instituciones se encuentran en la encrucijada creada por su obligación de diseminar información y el derecho de las personas a ocultar sus datos personales. La solución más sencilla es la total eliminación de los servicios de directorio, que claramente no es la mejor posible, aunque algunas

instituciones han escogido ese camino. Ésta, desde nuestro punto de vista, no es una solución y sí un problema de mayores proporciones.

Otra forma de afrontar el problema es impedir el acceso al servicio de directorio desde fuera de la institución. Tampoco es ésta la solución, porque hace que aquellos individuos que desean ser localizados sean totalmente imposibles de encontrar y por lo tanto no protege el derecho a la privacidad.

Es completamente posible que una aplicación desarrollada internamente publique datos al exterior sin el consentimiento del individuo.

2.- La solución

Nuestro planteamiento para resolver el problema ha sido dar a los individuos el control total sobre la publicación de sus datos personales

Nuestro planteamiento para resolver el problema ha sido dar a los individuos el control total sobre la publicación de sus datos personales. Aunque, dicho control estará siempre dentro de la política establecida por la institución, que a su vez, debe estar definida dentro del marco de la legislación vigente.

El conjunto de información accesible no se verá afectado para el uso normal de la institución, cuando el acceso lo realicen aplicaciones desarrolladas internamente o individuos adecuadamente identificados.

El administrador del directorio define el conjuto de datos que pueden ser obtenidos por medio de búsquedas anónimas, de acuerdo con la política de la institución. Esto se puede hacer, por ejemplo, utillizando las listas de control de acceso de OpenLDAP. Entonces, los usuarios pueden controlar el acceso a los atributos, una vez que se ha definido la política.

3.- La implementación

El acceso a los datos se controla por medio de las Listas de Control de Acceso, lo que nos permite diferenciar tanto los tipos de acceso como sus niveles

Para implementar nuestro servicio hemos utilizado el servidor de directorio OpenLDAP, por tanto hemos usado las capacidades disponibles en dicho sistema para implementar la solución propuesta.

```
attributetype ( 1.3.6.1.4.1.7547.4.3.2.11
NAME 'irisUserPrivateAttribute'
DESC 'Set of denied access attributes'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )
```

El acceso a los datos se controla por medio de las Listas de Control de Acceso (ACLs, Access Control Lists), lo que nos permite diferenciar tanto los tipos de acceso (anónimos e identificados) como los niveles de acceso (lectura, escritura o ninguno).

Hemos introducido un nuevo atributo en el esquema común de RedIRIS, llamado **irisUserPrivateAttribute**. El uso de este atributo junto con las correspondentes reglas, nos permite mantener la privacidad de los datos personales a nivel del directorio, sin degradar la comunicación con otros servicios.

irisUserPrivateAttribute es un atributo multivaluado y contiene el conjunto de atributos que el usuario decide ocultar para las búsquedas anónimas. Estos son un subconjunto de un conjunto de nombre de atributos definidos por el administrador del directorio, como por ejemplo, *mail, telephone-Number, mobile or jpegPhoto*.

Hemos definido también, dos valores especiales: *all*, que indica que el usuario quiere ocultar el conjunto completo; y *entry* para indicar que será la propia entrada la que no estará disponible para ser recuperada.

El administrador del directorio define el conjunto de atributos controlables y los niveles de acceso por medio de listas de control de acceso, que decidirán si se devuelve un determinado atributo como resultado a una búsqueda, dependiendo de su presencia como valor de irisUserPrivateAttribute, el tipo de conexión, anónima o identificada, y en el caso de este último tipo, el usuario que la realiza. La definición de dichas listas de control de acceso debe hacerse en orden ascendente de granularidad, es decir, los granos más finos, se deben definir en primer lugar.

El siguiente ejemplo muestra el uso de este concepto para controlar el acceso a los atributos *mail* y *mobile*, así como a todo el conjunto de atributos disponible y a la propia entrada.

El administrador del directorio define el conjunto de atributos controlables y los niveles de acceso por medio de listas de control de acceso, que decidirán si se devuelve un determinado atributo como resultado a una búsqueda

```
[1]   access to *
      filter="(irisUserPrivateAttribute=entry)"
      by * none
[2]   access to *
      filter="(irisUserPrivateAttribute=mail)"
      attrs=mail
      by * none
[3]   access to *
      filter="(irisUserPrivateAttribute=mobile)"
      attrs=mobile
      by * none
[4]   access to *
      filter="(irisUserPrivateAttribute=all)"
      attrs=mail,mobile
      by * none
[5]   access to *
      by * read
```

- La regla número 1 controla el acceso a la entrada en sí misma.
- Las reglas 2 y 3 controlan el acceso a los atributos que el usuario puede decidir ocultar de las búsquedas.
- La regla 4 lista todos los atributos que puede controlar el usuario, de tal manera que no se muestran en los resultados de las búsquedas cuando **irisUserPrivateAttribute** vale all.
- Finalmente, la regla 5 permite el acceso a todos los atributos de la entrada si no se ha cumplido ninguna de las reglas que la preceden.

La regla 4 lista todos los atributos que puede controlar el usuario, de tal manera que no se muestran en los resultados de las búsquedas cuando irisUserPrivateAttribute vale all.

José A. Accino,
(acccino@uma.es)
Victoriano Giralt
(victoriano@uma.es)
Servicio Central de Informática,
Universidad de Málaga
Javier Masa
(javier.masa@rediris.es)
Área de middleware
RedIRIS