Un modelo de control de acceso basado en la semántica

A Semantics-Based Access Control Model

M. I. Yagüe y A. Maña

Resumen

La web semántica es considerada la nueva generación de la web. El objetivo de esta nueva "web de los significados" es permitir que tanto máquinas como personas trabajen en cooperación. Para alcanzarlo, se codifican los datos de forma que los contenidos de la web sean más comprensibles por medios algorítmicos. En este trabajo se presenta la aplicación de los conceptos de la web semántica junto con sus tecnologías al área del control de acceso. En concreto, se presenta un nuevo modelo de control de acceso al que hemos denominado SAC, *Semantic Access Control Model*, el cual usa diferentes capas de metadatos para describir la semántica de los diferentes componentes que participan en una decisión de acceso.

Palabras Clave: Metadatos XML, web semántica, autorización, control de acceso.

Summary

The Semantic Web is considered the new generation of the Web. The objective of this new web, also known as the Web of meaning, is to enable computers and people to work in cooperation. To reach this, an objective is encoding data in forms that make web contents (meaning, semantics) more understandable by algorithmic means. In this paper, we present the application of Semantic Web concepts and technologies to the access control area. The *Semantic Access Control Model* (SAC) uses different layers of metadata to take advantage of the semantics of the different components relevant for the access decision. We have developed a practical application of this access control model based on a specific language, denominated Semantic Policy Language (SPL), for the description of access criteria. This work demonstrates how the semantic web concepts and its layers infrastructure may play an important role in many relevant fields, such as the case of access control and authorization fields.

Keywords: XML metadata, Semantic Web, Authorization and Access Control.

El objetivo de esta nueva "web de los significados" es permitir que tanto máquinas como personas trabajen en cooperación

1.- Fundamentos de SAC

El diseño de SAC [1] se basa en un modelo de metadatos que permite la integración semántica de una aplicación de control de acceso y una infraestructura de acreditación externa. SAC representa una solución al problema del control de acceso para entornos altamente distribuidos, dinámicos y heterogéneos. El diseño de este modelo se basa en la información semántica para lograr que se tengan en consideración las propiedades particulares de los recursos accedidos (lo que se conoce como "introspección de contenido").

Junto con el modelo de control de acceso se ha diseñado su correspondiente lenguaje de políticas, *Semantic Policy Language* (SPL), que se basa en el modelado semántico de la información contextual así como de los distintos recursos a proteger. Igualmente, y con el fin de que la integración de la entidad de autorización externa resulte transparente al resto del sistema de control de acceso, el lenguaje hace uso de las descripciones semánticas (modelado semántico) de las distintas autoridades de certificación que componen la infraestructura de autorización externa o PMI (*Privilege Management Infrastructure*).

1.1.- Un modelo basado en atributos

Los conceptos sobre los que se basa el modelo de control de acceso son determinantes en los niveles de interoperabilidad, flexibilidad, etc., alcanzados. El modelo de control de acceso basado en roles (RBAC), considerado como una tecnología madura y flexible, se define sobre los tres conceptos predefinidos de "usuario", "rol" y "grupo".

En el diseño y desarrollo del modelo SAC partimos de la base de que los conceptos tradicionales de 'usuario', 'rol' y 'grupo' pueden ser reemplazados por el concepto más general de atributo

La inclusión del concepto "usuario" implica el proceso de identificación como base para el control de acceso. De hecho, la asignación de roles y la pertenencia a grupos toman como base la identificación del usuario.

La definición de roles y la agrupación de usuarios puede facilitar la gestión, especialmente en sistemas de información corporativos. Pero en otros entornos donde la heterogeneidad y distribución de los recursos son sus principales características, estos conceptos dejan de resultar adecuados. De hecho, el concepto de grupo es un sustituto artificial de un concepto más general como es el atributo. En la práctica, los grupos se definen según los valores de determinados atributos como puede ser la posición del empleado dentro de la empresa, la función desarrollada, etc. El atributo usuario, por ejemplo, aparece en la mayoría de los modelos de control de acceso y, aunque la identidad constituye uno de los atributos más útiles, existen escenarios donde no es necesario (por ejemplo, si se quiere mantener el anonimato en el acceso) y por lo tanto no debería ser un componente predefinido de un modelo general.

Otro problema que tienen estos atributos tradicionales es, por ejemplo, que la estructura de grupos es definida por el administrador de seguridad del sistema de control de acceso y es normalmente una estructura estática. En el caso de sistemas más dinámicos en entornos como Internet (computación grid, servicios web, etc.), los administradores del sistema no pueden predecir las estructuras de los grupos, y además la estructura de grupos y los criterios de acceso pueden ser distintos para cada recurso. La heterogeneidad en cuanto a los requisitos de acceso de los recursos así como la incorporación dinámica y continua de nuevos recursos al sistema, unida a una mayor frecuencia de cambio en los requisitos de acceso, hacen poco adecuado el concepto de 'grupo' como base del control de acceso en estos nuevos entornos distribuidos, heterogéneos y dinámicos.

En el diseño y desarrollo del modelo SAC partimos de la base de que los conceptos tradicionales de 'usuario', 'rol' y 'grupo' pueden ser reemplazados por el concepto más general de atributo. En los sistemas de control de acceso basados en certificados de atributos, las condiciones de acceso se expresan en términos de conjuntos de atributos en lugar de usuarios o grupos. Los certificados de atributos se usan para demostrar que los usuarios presentan los atributos requeridos para ganar el acceso. Este esquema es muy escalable respecto al número de usuarios y también al número de factores diferentes (atributos) usados por el sistema de control de acceso.

2.- Visión general de SAC

El modelo SAC contempla la existencia de una serie de sistemas de control de acceso y un conjunto de entidades de acreditación confiables que actúan de manera independiente y dan servicio a los diferentes sistemas de control de acceso. El control de los recursos es independiente de su localización. De esta forma, los recursos controlados por un administrador no han de residir obligatoriamente en su propio sistema de información. Igualmente, algunos de los recursos almacenados por un sistema de control de acceso pueden no estar bajo el control de dicho sistema.

Cada sistema de control de acceso mantiene una descripción semántica de los recursos que controla. Asimismo, se tienen en cuenta propiedades acerca del contexto de aplicación. El nivel de granularidad no se limita a nivel de objeto (fichero, servicio, aplicación, componente software, etc.), pudiéndose especificar a un nivel más fino, como por ejemplo una operación de un objeto CORBA, una operación de un servicio web, de una aplicación o de un componente software, una operación sobre un fichero genérico o, en el caso de ficheros XML, una operación sobre uno de sus elementos, entre otros.

En nuestro modelo SAC, la identificación del usuario o cliente no es obligatoria. Esto es debido a que los clientes poseen una serie de atributos, y el acceso a los recursos se basa igualmente en la especificación de un conjunto de atributos que debe reunir el cliente para poder acceder a ellos. Estos atributos deben venir firmados digitalmente por una entidad de certificación confiable, externa al sistema gestor de control de acceso, constituyendo lo que se conoce por un certificado de atributo. De esta forma, se garantiza la interoperabilidad de los atributos que pueden ser comunicados de forma segura evitando la necesidad de ser emitidos localmente por el administrador del sistema. Dado que las entidades de certificación son externas al sistema de control de acceso, es necesario un mecanismo para establecer la confianza entre dichas entidades externas y el sistema de control de acceso. Para ello, se ha desarrollado un modelo semántico para describir la semántica de las distintas autoridades de certificación que componen la infraestructura de autorización externa o PMI. Este enfoque permite que el proceso de registro del cliente no sea necesario, y evita que un mismo atributo de un cliente deba ser emitido en cada sistema. Adicionalmente, el modelo contempla la realización de acciones condicionales, que deben realizarse para poder acceder al recurso.

Los requisitos de acceso a un recurso dependen de forma natural de sus propiedades y no de su localización

Como se ha indicado, el componente básico de las políticas es el conjunto de atributos que deben ser presentados para conseguir el acceso. Dichos atributos hacen referencia a propiedades de los clientes, mientras que el conjunto de atributos requeridos para el acceso puede depender de las propiedades semánticas de los mismos. De hecho, al contrario de lo que sucede en esquemas tradicionales, en nuestro modelo la determinación de la política que corresponde a un recurso no se basa en su estructura de almacenamiento. Esta asignación de políticas a recursos se basa esencialmente en las propiedades semánticas de los últimos, aunque también es posible considerar la estructura de almacenamiento.

Este enfoque responde al hecho de que los requisitos de acceso a un recurso dependen de forma natural de sus propiedades y no de su localización. Adicionalmente, el modelo desarrollado permite la definición de políticas genéricas de acceso que se adaptan en función de las características del recurso y el entorno. La política concreta a aplicar a un recurso se crea de forma dinámica en tiempo de acceso, lo que permite una mayor adaptabilidad a posibles cambios en los requisitos de acceso.

La semántica bien definida del modelo de control de acceso desarrollado [1] permite la validación semántica de los sistemas que lo implementan. Todo el diseño del modelo se ha realizado con el objetivo de facilitar la gestión del sistema de control de acceso resultante, así como de garantizar la corrección y simplicidad redundando en una mayor seguridad del sistema.

3.- Conclusiones

El control de acceso en sistemas abiertos, distribuidos y heterogéneos plantea una problemática que lo convierte en un escenario perfecto para demostrar el potencial de las infraestructuras de metadatos basadas en los conceptos de la Web semántica. La aplicación del modelo SAC propuesto ha permitido el desarrollo de un esquema de control de acceso escalable a un gran número de usuarios sin necesidad de una fase de registro y aplicable a distintos entornos con criterios de acceso complejos y heterogéneos, como por ejemplo bibliotecas digitales [2], servicios web [3], comercio electrónico [4], aplicaciones CORBA [5], DRM [6], etc. Además, gracias a la alta expresividad semántica del modelo y a los distintos niveles de metadatos representados, se consigue una total interoperabilidad entre los distintos componentes del sistema de control de acceso.

En definitiva, este trabajo demuestra cómo los conceptos de la web semántica y su infraestructura en capas puede desempeñar un papel muy importante en muchos campos relevantes, como ocurre en

este caso en las áreas de control de acceso y de autorización. La aplicación de tecnologías de la Web Semántica ha sido el origen del nuevo modelo de control de acceso SAC basado en la semántica.

Referencias

[1] Yagüe, M. I., "Modelo basado en metadatos para la integración semántica en entornos distribuidos. Aplicación al escenario de control de accesos". Dirigida por D. José Mª Troya. Dpto. Lenguajes y Ciencias de la Computación. 2003.

[2] Yagüe, M. I., Maña, A., López, J., Pimentel, E., Troya, J. M., "A Secure Solution for Commercial Digital Libraries". Online Information Review journal, 27(3), 2003, 147-159.

[3] Yagüe, M. I., Troya, J. M., "A Semantic Approach for Access Control in Web Services". Proceedings of Euroweb 2002 International Conference. W3C. 2002.

[4] A. Maña, M. I.Yagüe, V. Benjumea, "EC-GATE: Electronic Commerce based on E-gate Technology". *Golden Award of the E-gate Open Contest 2002*, París, 2002. http://www.axalto.com/press/news.asp?id=41

[5] López, J., Maña, A., Ortega, J., Pimentel, E., Troya, J. M., Yagüe, M. I., "Integrating PMI Services in CORBA Applications". Computer Standards and Interfaces Journal. Vol. 25(4). Elsevier Science. 2003, pp. 391- 409.

[6] Maña, A., Yagüe, M. I., Benjumea, V., EC-GATE: An infrastructure for DRM. IASTED Int. Conference. Special Session on *Architectures and Languages for Digital Rights Management and Access Control.* New York, December 2003.

Mariemma I. Yagüe
(yague@lcc.uma.es)
Antonio Maña
(amg@lcc.uma.es)
Dpto. de Lenguajes y Ciencias de la Computación
Universidad de Málaga