J. A. Montenegro and J. Lopez, "Taxonoma de las Infraestructuras de Autorizacin y Autentificacin", *XIII Jornadas TELECOM I+D 2003*, 2003.
NICS Lab. Publications: https://www.nics.uma.es/publications

Taxonomía de las Infraestructuras de Autenticación y Autorización

José A. Montenegro, Javier López
ETSI Informática, Dpto. Lenguajes y Ciencias de la Computación
Universidad de Málaga, 29071 Málaga
Telf: 952-13-1327, Fax: 952-13-1397
E-mail: {monte, jlm}@lcc.uma.es

Abstract

Los mecanismos de autorización y autenticación han dejado de ser elementos integrantes de los sistemas pasando a ser gestionados por elementos externos al sistema. Esta nueva filosofía se basa en el establecimiento de redes de confianza entre los sistemas que prestan servicio y los elementos encargados de la autenticación y autorización. Esta organización da lugar a una federación de sistemas que dependen de elementos que controlan el acceso, permitiendo al usuario aplicar técnicas de sing-on que facilitan la labor de autentificación, así como permite compartir la información de autorización entre los elementos integrantes de la federación. Existen distintas propuestas que dan vida a esta nueva filosofía, donde cada cual establece los elementos y los mecanismos que conforman el sistema. Este trabajo se centra en la realización de una taxonomía de las propuestas existentes, así como presenta una solución propia basada en la inclusión de técnicas biométricas, como elemento de autentificación, en estas infraestructuras.

1. Introducción

Durante las últimas décadas los mecanismos de autentificación y autorización estaban integrados en los sistemas como parte funcional del mismo. Esta situación hace que se presentara más inconvenientes que ventajas.

Los sistemas tradicionales mantienen su propio formato de intercambio de información, aunque el modelo que implementa se basa en el estándar. Este hecho hace que la interoperabilidad entre los sistemas sea más ardua y complicada de llevarla a cabo. De esta forma el paso de sistemas centralizados a sistemas distribuidos requiere de la modificación de los mecanismos utilizados, e incluso la aparición de algunos nuevos, que cubren la misma funcionalidad base que sus predecesores.

Esta diversidad de servicios, con la confusión asociada de los usuarios que supone, viene determinada por la poca flexibilidad que presentan los sistemas, a la hora de intercambiar los mecanismos que proporcionan los servicios. Normalmente los sistemas tradicionales siguen una administración centralizada que incide negativamente en la escalabilidad y en la movilidad de los usuarios.

Con la funcionalidad de salvaguardar estos inconvenientes nace el concepto de las *Infraestructuras de Autorización y Autenticación* (AAIs). La piedra angular de su funcionamiento es el establecimiento de redes de confianza entre los elementos de la infraestructura y los sistemas a los cuales presta servicio. Asociadas a estas infraestructuras aparecen tecnologías que permiten facilitar la tarea a sistemas y usuarios como es el caso de las técnicas de "sign-on".

A su vez estos sistemas favorecen la movilidad de los usuarios, debido a que el concepto de pertenencia de los usuarios a los sistemas resulta modificado, y de esta forma el usuario forma parte de una confederación, la cual agrupa un número de servicios distribuidos y heterogéneos.

2. AAIs existentes

La creación de una AAIs se basa en el establecimiento de los mecanismos necesarios para llevar a cabo el intercambio de la información entre los elementos de su confederación. Las distintas soluciones existentes difieren en los mecanismos implementados para el intercambio de la información, así como el establecimiento del formato de las credenciales intercambiadas entre los elementos del sistema.

Una posible taxonomía de las propuestas existentes viene determinada por la naturaleza de las AAIs, de esta forma destacamos los marcos teóricos, implementaciones propietarias y las soluciones mixtas.

2.1. Marcos Teóricos

Esta sección incluye las soluciones que establecen un marco teórico estándar, pero no define los mecanismos necesarios para el intercambio de la información, de esta forma estos modelos podrían formar la base de los restantes modelos, proporcionando una estandarización de los credenciales.

Una representación de esta categoría sería la fusión entre las *Infraestructuras de Clave Pública* (PKI) y las *Infraestructuras de Administración de Privilegios* (PMI), basada en la recomendación establecida por la ITU [3]. La propuesta establece la sintaxis de los certificados de atributos y los

certificados de identidad y su posible interacción, pero no establece los mecanismos de comunicación entre los elementos de un sistema que requieran utilizar estos elementos.

2.2. Implementaciones Propietarias

Actualmente existe una tendencia creciente de implementaciones de AAIs, que viene motivada por la utilización en aplicaciones relacionadas con la web.

El *modus operandis* de estas soluciones se basan en la utilización de redirecciones http y la utilización de *cookies* en el cliente para almacenar la información requerida en las sesiones.

Los proyectos que pueden incluirse dentro de esta categoría son los siguientes *Microsoft.NET Passport* [7], *PAPI* [8], *Shibboleth* [5]. Actualmente todas las propuestas cubren de forma más o menos eficiente la autenticación de los usuarios, aunque actualmente *Shibboleth* es la única que establece la interacción del sistema con una *Autoridad de Atributos* (AA) para administrar de forma eficiente la Autorización. La arquitectura de *PAPI* facilita la introducción en el futuro de AAs que permita hacer más completa la solución.

La definición del formato de las *cookies* y las secuencias de interacción entre los elementos del sistema, hace que a priori exista una incompatibilidad entre ellos. El siguiente paso será la realización de *Gateways* que se encarguen de procesar los distintos formatos e interactuar entre los elementos pertenecientes a distintas soluciones.

La desventaja que presentan estas soluciones es la dependencia que mantienen con los servicios web, debido a que su comportamiento se basa en características intrínsecas de este servicio.

2.3. Soluciones Mixta

Bajo este epilogo consideramos la inclusión de sistemas que mediante su implementación prestan un servicio y por su amplio uso se han establecido con el tiempo como estándares.

Ejemplo de esta clasificación sería el sistema Kerberos [4] y SPKI [1]. La inclusión de una nueva categoría, viene marcada debido a que estas soluciones establecen un estándar de facto, no sólo aplicable a servicios web y proporcionan mecanismos de interacción entre los elementos de un sistema, además del formato de la información de autorización y autenticación.

Además de las soluciones referenciadas previamente, existe el proyecto *Liberty Alliance* [6] que no ha producido implementación alguna, pero esta desarrollando especificaciones, con el propósito de estandarizarse posteriormente.

La mayoría de las propuestas implementadas se decantan por utilizar mecanismos de login-password para proveer autenticación al sistema. Otra posibilidad existente, es utilizar criptografía asimétrica como es el caso de la propuesta basada en PKI.

Dentro de los mecanismos de autenticación existen diferentes propuestas como es el caso de la biometría donde el usuario utiliza características físicas que le permiten autentificarse en un sistema de forma semejante al que se realiza en la vida real. La utilización de estas técnicas elimina la necesidad de poseer elementos adicionales para llevar a cabo la tarea de identificación.

3. BAAI

Las técnicas biométricas nos permiten realizar operaciones de identificación y autentificación en sistemas que requieran presencia humana eliminándose la necesidad de almacenamiento de secretos compartidos entre el sistema y el usuario, ya que utiliza características intrínsecas de los humanos para tal tarea. Una vez realizada la autentificación en el sistema del individuo es necesario saber que tareas le son permitidas realizar, para lo cual debemos especificar los privilegios que tiene el individuo en el sistema.

El trabajo expuesto en [Kon96] utiliza un sistema biométrico y asocia mediante un interfaz grafico los privilegios a las imágenes del usuario existentes en el sistema. Esta aproximación al problema aquí tratado, es insuficiente en el momento que trasladamos la asignación de privilegios de un sistema a un conjunto de recursos distribuidos, donde no es posible realizar una administración centralizada, utilizando para tal caso los servicios prestados por una PMI.

La idea principal del trabajo, definido de forma detallada en [2], es la de incluir el reconocimiento facial como técnica biométrica en las AAIs. De esta forma y mediante la utilización de la esteganografía se establece un nuevo concepto de certificado, denominado *Vision Attribute Certificate* (*VAC*) que almacena tanto la imagen del usuario, que será utilizada para verificar la identidad del usuario, y los atributos que marcan el proceso de autorización.

Nuestra propuesta se enmarca dentro de los marcos teóricos de la clasificación establecida en la segunda sección.

El siguiente subapartado muestra el funcionamiento detallado de la propuesta.

3.1. Descripción Técnica de la solución

Holder es el campo de los certificados de atributos X509 que representa la identidad del usuario o tenedor de los privilegios. Tal y como muestra la figura 1, codificado en ASN1 [10], el campo holder es una secuencia de campos que permite vincular el certificado de atributos con un certificado de identidad, proporcionarle un nombre o asignarle el hash de un objeto.

Nuestra solución utiliza los dos últimos campos de la secuencia *Holder* del certificado, y realiza el siguiente proceso.

Inicialmente obtenemos una imagen del usuario y le realizamos un hash de los bits más significativos de la imagen y seguidamente se almacenan en el campo *ObjectDigestInfo*.

El campo *entityName* almacenará opcionalmente el nombre del usuario relativo a la imagen. Este mecanismo permite que la las Autoridades de Autorización realicen las tareas propias de las Autoridades de Certificación, teniendo de esta forma una AAIs con una sola infraestructura, eliminándose en este caso el gasto que supone la administración conjunta de una PKI y una PMI, cumpliéndose en todo caso con los estándares.

Posteriormente la AA realizara las tareas relativas a la autorización, introduciendo los atributos o asignación de roles en el certificado, dependiendo de la identificación previa del usuario.

Una vez que hemos realizado la vinculación entre la imagen del usuario, que servirá como autenticación ante los biométricos, y sus atributos, que proporcionaran las acciones que el usuario este permitido realizar, el certificado será introducido mediante técnicas de estenografía dentro de la imagen, permitiendo de esta forma tener un simple elemento con toda la información requerida.

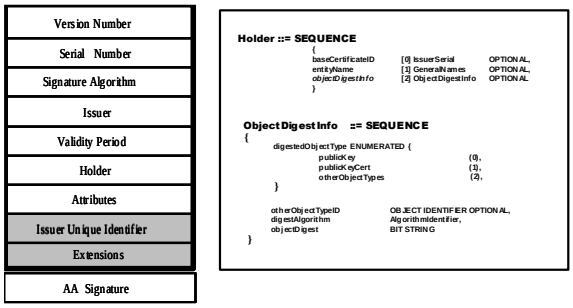

Fig. 1 Vinculación de los atributos con la identidad

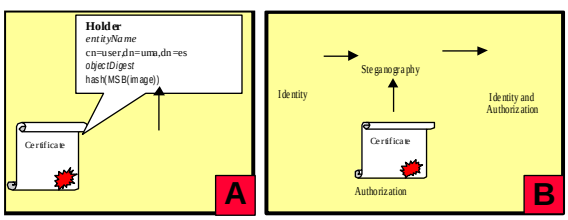

Fig. 2 Proceso de creación de los VAC

La utilización de estenografía permitirá que el certificado de atributos no interfiera en el reconocimiento de la imagen por el biométrico y que tengamos la información de autorización y autenticación almacenada de forma simultánea, obteniéndose finalmente el elemento básico de esta infraestructura o *VAC*.

La figura 2 muestra el esquema de operación del sistema en la creación de las credenciales. La figura 2a especifica el proceso de creación del certificado mediante la vinculación del nombre del usuario y su imagen, para la identificación biométrica, y finalmente la Autoridad de Atributo asigna los privilegios mediante el establecimiento de los atributos en el certificado.

La figura 2b muestra el proceso de introducción del certificado dentro de la imagen del usuario, mediante el uso de una aplicación de estenografía, de este modo mantenemos la información de autenticación y autorización unidas facilitando las tareas administrativas.

Una vez detallado el proceso de creación de los credenciales de los usuarios, pasamos a especificar los procesos de autenticación y autorización, que es realizado en tres pasos (figura 3):

1. Inicialmente una cámara CCTV recoge la imagen del usuario.
2. El sistema compara, mediante técnicas de biometría, la imagen recogida con las imágenes almacenadas, realizándose el proceso de identificación.
3. Una vez identificado el usuario, el sistema extrae mediante una aplicación de estenografía el certificado de atributo y permite obtener los privilegios del usuario identificado previamente.

Los VAC serán almacenados en un directorio X500, una vez que sean generados por la AA y estarán disponibles para todos los puntos de reconocimientos existentes en la infraestructura.

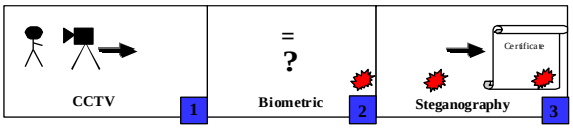

Fig. 3 Proceso de autenticación y autorización

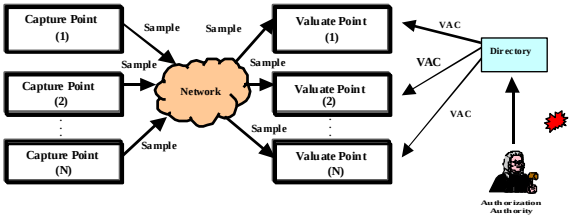

Fig. 4 Integración de la propuesta Sist. Distribuido

La figura 4 muestra como se integra la propuesta dentro de un sistema distribuido, permitiendo que los puntos de captura y evaluación no tengan que estar ubicados físicamente en el mismo lugar.

Los puntos de captura obtienen las características biométricas del usuario. Estas imágenes son transmitidas a los puntos de evaluación por medio de Internet.

Finalmente los puntos de evaluación comparan las capturas realizadas con los VAC almacenados previamente en un directorio por una Autoridad de Autorización.

4. Conclusiones

La clasificación establecida en este trabajo permite establecer las líneas de trabajo necesarias para avanzar el desarrollo de estas infraestructuras.

Las implementaciones propietarias permiten el avance de esta tecnología, los marcos teóricos establecen una solución base estándar para que sea usada en el futuro por las implementaciones, permitiendo una correcta interacción entre los elementos de diferentes implementaciones. Finalmente las soluciones mixtas son los pilares históricos de los cuales nace esta incipiente tecnología.

El proceso de autenticación ha sido cubierto por la mayoría de las tendencias de esta tecnología, pero queda un arduo trabajo en el campo de la autorización. La mayoría de las soluciones han dado prioridad a esta cuestión y dirigen sus esfuerzos en esta dirección.

A modo de ejemplo, las tareas que son necesarias realizar son, estandarización de los atributos necesarios para la autorización, establecer mecanismos que preserven la confidencialidad de los atributos utilizados de los usuarios, instituir las políticas que determinen los atributos que pueden ser utilizados por determinados sistemas, etc.

Por todo lo expresado en este trabajo el desarrollo de esta nueva tecnología abre la posibilidad de interacción entre sistemas, que anteriormente eran islas aisladas y ahora pasarán a formar parte de confederaciones que preservan la interoperabilidad entre sistemas dispares.

Referencias

[1] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, “SPKI Certificate Theory”, RFC 2693, September 1999

[2] E. Dawson, J. López, J.A. Montenegro, E. Okamoto, “BAAI: Biometric Authentication and Authorization Infrastructure”, IEEE, International Conference on Information Technology: Research and Education. Newark, New Jersey, USA, August 2003.

[3] ITU-T Recommendation X.509, Information Technology – “Open systems interconnection- The Directory: Public-key and attribute certificate frameworks”, 2000.

[4] J. Kohl C. Neuman, “The Kerberos Network Authentication Service (V5)”, RFC 1510, September 1993

[5] http://shibboleth.internet2.edu/

[6] http://www.projectliberty.org/

[7] http://www.passport.net

[8] http://www.rediris.es/app/papi/

[9] W. Konen and E. Schule-Krger, “ZN-Face: A system for access control using automated face recognition,” in Proceedings of the third annual SNN Symposium on Neural Networks, 1995.

[10] B. S. Kaliski, A Laymans Guide to a Subset of ASN.1, BER, and DER,1993.