Acceso ubicuo a recursos de información en Internet: El sistema PAPI

Diego R. López, Rodrigo Castro-Rojo

RedIRIS

E-mail: papones@rediris.es

Sumario: *PAPI es un sistema para facilitar el acceso, a través de Internet, a recursos de información cuyo acceso está restringido a usuarios autorizados. Los mecanismos de autenticación empleados para identificar a los usuarios se han diseñado para ser lo más flexibles posible, permitiendo que cada organización emplee un esquema de autenticación propio, manteniendo así los datos dentro de su propio ámbito, a la vez que los proveedores de información disponen de datos suficientes para realizar estadísticas. Los mecanismos de control de acceso son transparentes para el usuario y compatibles con los navegadores comúnmente empleados en cualquier sistema operativo. Dado que PAPI emplea procedimientos estándar HTTP, su uso para proveer servicios de identidad digital y control de acceso no requiere de ningún hardware o software específico, garantizando a los usuarios un acceso ubicuo a cualquier recurso de información al que tengan derecho.*

1. Introducción

En los últimos años, el acceso a través de Internet a recursos restringidos [1] (como publicaciones y bibliotecas digitales, informes on-line, y múltiples clases de formularios conectados a todo tipo de repositorios de datos) ha llegado a ser más y más común. El control de acceso a estos recursos ha sido realizado bien por medio del uso de los tradicionales pares usuario/contraseña, bien por mecanismos basados en la dirección IP origen de la petición, aceptando sólo aquéllas provenientes de determinados rangos.

El uso de una autenticación basada en usuario/contraseña tiene el principal inconveniente de los problemas de escala, especialmente importantes cuando los recursos que han de ser accedidos son proporcionados por otra organización (*un proveedor de información*). En este caso, lo normal es que el proveedor de información no esté dispuesto (en el caso de que debiera hacerlo) a mantener un registro más o menos detallado de los usuarios individuales de la organización cliente, ni a atender las diferentes incidencias relacionadas con el acceso de cada usuario. Por otro lado, tampoco suele resultar aceptable el empleo de un par usuario/contraseña general para toda la organización cliente, dado que esto limita la capacidad de obtener estadísticas significativas sobre el uso de los recursos y, más aún, lleva casi indefectiblemente a que se multiplique el uso de los recursos por medio de personas no autorizadas.

La respuesta tradicional a este problema ha sido el empleo de esquemas de autorización basados en la dirección IP origen: únicamente se permite el acceso a los recursos a un rango de direcciones IP definidas por la organización cliente [2]. Sin embargo, esta aproximación limita seriamente la movilidad de los usuarios y entra en conflicto con determinadas tecnologías muy comunes en la práctica actual de los proveedores de servicio Internet, como es el caso de los sistemas de proxy/cache.

La pretendida panacea de utilizar certificados derivados de una PKI presenta también serios problemas. Los certificados son, por su propia naturaleza, estáticos y de larga duración, mientras que la mayor parte de los derechos de acceso son mucho más dinámicos y de una duración más corta; el uso de tecnologías de PKI requiere el uso de software o hardware adicional, y , finalmente, los certificados suelen contener información personal que no debe ser entregada a terceras partes. Esto se traduce tanto en impedimentos para la movilidad de los usuarios como en complicaciones adicionales en la gestión de los derechos de acceso [3].

PAPI es un sistema que proporciona mecanismos de control de acceso a recursos de información a través de Internet. La identidad del usuario es establecida por medio de mecanismos de autenticación completamente locales a la organización con la que el usuario tiene establecida una relación específica, mientras que los proveedores de información mantienen un control absoluto sobre las condiciones de acceso a los recursos que ofrecen. Los mecanismos de autenticación están diseñados para ser abiertos y flexibles, de manera que cada organización pueda definir su propio esquema de autenticación, evitando la transmisión de datos privados, a la vez que se facilita la recolección de estadísticas de acceso por parte de los proveedores. Además, los

mecanismos de control de acceso son completamente transparentes para el usuario y compatibles con prácticamente todos los navegadores y sistemas operativos. PAPI emplea procedimientos HTTP estándar, por lo que sus mecanismos de autenticación y autorización no requieren ningún tipo de software o hardware específicos y proporcionan a los usuarios un acceso ubicuo a los recursos de información que tienen derecho a acceder.

2. Los componentes de PAPI

PAPI consta de dos elementos independientes: el servidor de autenticación (AS) y el punto de acceso (PoA). Esta estructura hace que el sistema tenga una gran flexibilidad y permite su integración en diferentes entornos operativos. No se requiere ningún tipo de correspondencia entre un determinado AS y un determinado PoA: un PoA es capaz de manejar peticiones desde cualquier número de ASs y dirigirlos hacia cualquier número de servidores web. El lema central de PAPI es: "La autenticación es un asunto local. Y la autorización también" [4].

El propósito del AS es ofrecer a los usuarios un punto único de autenticación y proporcionarles (de manera completamente transparente) todas las claves temporales que les permitirán acceder a los recursos para los que estén autorizados.

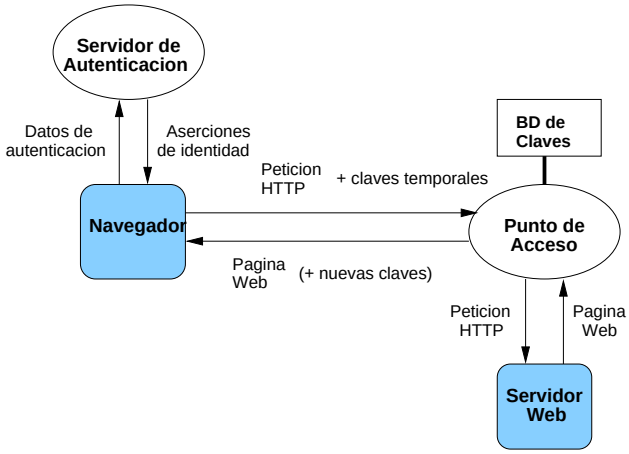

Figura 1: La arquitectura PAPI

El PoA realiza el control de acceso efectivo para un conjunto de localizaciones web dentro de un determinado servidor. El proveedor de información (o el operador de los servidores web) tiene la responsabilidad de gestionar el punto de acceso de acuerdo con su política. Un PoA PAPI puede ser adaptado a cualquier servidor web, con independencia de la plataforma sobre la que esté implementado. Es más, un servidor web puede contener más de un PoA, y también un PoA puede controlar el acceso a más de un servidor web. Los PoAs pueden ser combinados de manera jerárquica en grupos controlados por un *PoA de grupo* (un GPoA), a través del que se validan los intentos iniciales de acceso. De esta manera, el navegador del usuario debe únicamente cargar las claves temporales para los GPoAs en la raíz de la jerarquía.

Otra importante propiedad de este sistema es que ofrece una compatibilidad absoluta con cualquier otro sistema de control que se emplee, dado que no impone requisitos de ningún tipo en cualquier procedimiento adicional que se emplea para este propósito. En otras palabras, el control de acceso PAPI es completamente ortogonal a mecanismos como la protección por medio de contraseñas, filtros basados en direcciones IP, control de acceso por medio de TLS, etc.

El usuario establece su identidad por medio del servidor de autenticación de la organización con la que está directamente relacionado, posiblemente facilitando datos que no se desea proporcionar en ningún caso a terceras partes. Una vez autenticado, el usuario es automáticamente dirigido hacia el punto de entrada del PoA. Es importante insistir en el hecho de que el AS no tiene por qué enviar ningún dato proporcionado por el usuario hacia el PoA. El AS se limita a preparar una aserción sobre la identidad del usuario en los términos requeridos por el PoA y lo firma digitalmente usando su clave privada. El único requisito común a cualquiera de estas aserciones es que el identificador de la misma debe mantenerse único durante el tiempo que sean válidas las claves temporales proporcionadas por el PoA. Por supuesto que la información sobre el usuario debe ser suficiente como para satisfacer la política de control de acceso del PoA, pero en ningún caso es necesaria la entrega de información privada.

El PoA recibe esta información, firmada digitalmente por el AS, y en función de ella decide si permite el acceso del usuario o no. Es importante resaltar que cuando nos referimos a que "un PoA confía en un AS" no estamos realizando ninguna afirmación acerca de que el PoA va a aceptar, a priori, todas las solicitudes de acceso provenientes de ese AS, sino que el PoA confiará en la afirmación realizada por el AS acerca de la identidad del usuario. Esto significa que si un PoA confía en un AS, la aserción (firmada digitalmente) "Este es el usuario X del grupo Y" que transmite el AS será totalmente fiable para el PoA. Y el PoA debe decidir, de acuerdo con esta aserción y con su política de acceso, si debe dar paso a la petición o no. La autorización es, por tanto, un asunto decidido en el ámbito de la organización que opera el PoA.

Una vez que el PoA acepta el acceso para una aserción proveniente de un AS se genera un par de claves temporales, que se almacenan por medio de cookies HTTP en el navegador del usuario. Los sucesivos accesos al recurso que el PoA protege serán aceptados o denegados por medio de estas claves temporales. La Figura 1 ilustra el proceso.

3. El protocolo PAPI

El protocolo empleado por PAPI puede considerarse dividido en dos fases: autenticación y control de acceso. La fase de autenticación comienza cada vez que un usuario accede el servidor de autenticación para obtener claves temporales válidas. Durante el período que dura la validez de estas claves, este usuario no necesita volver a pasar por esta fase. El usuario debe reiniciar la fase de autenticación antes de la expiración de sus claves únicamente en ciertos casos específicos:

- Cuando las claves temporales son eliminadas del navegador. En la implementación actual, esto ocurre cuando las cookies son borradas explícitamente o cuando el fichero de cookies se ve dañado.
- Cuando ocurre una corrupción de las claves temporales.
- Cuando las claves temporales se copian a otro navegador y son empleadas por otro usuario.
- Cuando la clave simétrica principal (la *K1* descrita más adelante) del punto de acceso ha sido cambiada.

3.1. La fase de autenticación

Esta etapa se inicia en el Servidor de Autenticación, donde el usuario es autenticado y acaba, una vez todo se ha llevado a cabo de manera exitosa, cuando un conjunto de claves temporales (dos por cada uno de los (G)PoA para los que el usuario está autorizado) es almacenado por el navegador del usuario.

El usuario accede el Servidor de Autenticación por medio de un navegador Web y proporciona los datos que el AS requiere para reconocerlo como un usuario válido. Qué datos son estos y su validación es una cuestión local al AS. Si la autenticación es correcta se aplica la política que la organización utilice para proporcionar acceso a los recursos disponibles a través de PAPI para generar una lista de URLs que corresponden a los puntos de acceso que deben ser contactados para descargar las claves temporales. Esta lista de URLs se envía al navegador del usuario, integrada en una página que da cuenta del resultado positivo del proceso de autenticación. La política de acceso de la organización puede basarse en atributos tales como el tipo de usuario, su relación con la organización. su rango dentro de ella, el número de accesos que la organización puede hacer a un determinado recurso, etc.

Cada una de los URLs mencionados arriba incluyen una referencia al procedimiento que el PoA correspondiente emplea para generar las claves temporales, junto con tres parámetros que se pasan empleando el método GET de HTTP: el identificador del AS, un código de petición y una aserción encriptada acerca del usuario. Esta aserción contiene:

- Una cadena de texto que describe al usuario y sus derechos. Una descripción típica del usuario incluye referencias al usuario y a los grupos a los que pertenezca, anonimizados si es necesario.
- La duración que se solicita para la clave temporal principal que se va a generar.
- Una marca de tiempo, pera evitar ataques por medio de repeticiones de los datos.

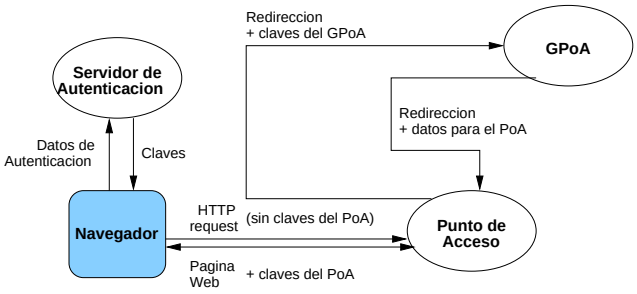

Figura 2: Interacción entre PoA y GPoA

Dado que el navegador del usuario recibe estos URLs incorporados en una página HTML, contacta de manera completamente transparente los puntos de acceso que están en la lista. Cada uno de ellos verifica la integridad y la marca de tiempo de la petición, empleando para ello la clave pública del servidor de autenticación. En este punto se verifican también las reglas de control de acceso aplicables a los datos que se reciben acerca del usuario. Si todo es correcto, se generan dos claves temporales: la clave temporal principal *Hcook* y la clave temporal secundaria *Lcook*. La clave temporal principal, junto con una cadena generada de manera aleatoria, se incluye en un registro de claves temporales mantenido por el punto de acceso. Ambas claves temporales se envían al navegador del usuario, codificadas como cookies HTTP.

Además de ser contactado directamente por un AS, un PoA puede también ser contactado por otros PoAs cuando éstos se hayan incluidos en un grupo controlado por un PoA de grupo (GPoA). Un GPoA recibe peticiones de sus PoAs subordinados por medio de redirecciones HTTP, como muestra la Figura 2. Si los procedimientos de control de acceso devuelven un resultado válido para el GPoA, éste construye un URL similar al descrito para el AS (empleando un código de petición distinto) y redirige el navegador de vuelta al PoA subordinado que contactó inicialmente al GPoA. En función de los datos que recibe por medio de esta redirección, el PoA subordinado decide si genera su par de claves temporales.

3.2. Claves temporales

El uso de dos claves temporales diferentes pretende un balance entre seguridad, con el objetivo de evitar accesos no autorizados por medio de duplicación de las claves, y eficiencia del protocolo, intentando evitar la repetición excesiva de cálculos criptográficos largos.

Hcook es la clave temporal primaria, criptográficamente más fuerte y que contiene más datos. Contiene un conjunto de campos con información de control de acceso, codificados con una clave simétrica (*K1*) que es exclusiva del PoA. Los campos de control de acceso son:

- Un código de usuario, derivado de la aserción recibida desde el AS.
- La localización a la que da acceso esta clave.
- El momento en que la clave expira.
- Un bloque generado de manera aleatoria.

Las entradas en el registro de claves temporales del PoA mantienen las claves temporales primarias que son válidas. Este registro se usa para evitar los accesos ilegales por medio de duplicación de cookies: cada vez que el PoA comprueba la validez de una Hcook recibida, compara el bloque aleatorio que contiene con el último que se generó para ella y que se almacenó en el registro.

Lcook es la clave temporal secundaria. Se emplea en la fase de control de acceso para realizar comprobaciones más rápidas y consiste también en un conjunto de campos de control de acceso, codificados con otra clave simétrica (*K2*), que también es exclusiva del PoA, aunque más corta que *K1*. Los campos que contiene son:

- La localización a la que da acceso esta clave.
- El momento en que la clave fue generada.

El tiempo de vida típico de una clave secundaria es de unos pocos segundos, mientras que las claves primarias son recalculadas en intervalos del orden de varios minutos. Una página primaria puede considerarse como una "clave de página", mientras que la secundaria pretende evitar retardos adicionales cuando se están cargando los elementos que componen la página.

3.3. La fase de control de acceso

En esta fase el punto de acceso se encarga de verificar las claves temporales asociadas con la localización que el navegador ha solicitado. El uso de dos claves temporales permite emplear la clave secundaria (cuya validez es muy corta) para reducir la complejidad de los cálculos criptográficos necesarios en cada decisión de acceso, incrementando así la capacidad de respuesta del sistema. Dado que *Lcook* tienen un período de validez muy corto, cuando expira se lleva a cabo una verificación larga: se decodifica *Hcook*, se genera un nuevo par de claves temporales y se actualiza el registro de claves temporales. Dado que las claves están almacenadas como cookies HTTP, cada vez que se intenta acceder una localización controlada, el navegador las envía automáticamente, sin necesidad de ninguna intervención por parte del usuario.

Cuando un PoA recibe una petición de acceso a una localización protegida, lleva a cabo los siguientes pasos:

1. Busca las claves temporales almacenadas en las cookies identificadas como *Lcook* y *Hcook*. Si no se han recibido las cookies, el PoA intenta redirigir la petición hacia su correspondiente GPoA (si está definido). En otro caso, la petición es rechazada.
2. El punto de acceso verifica la clave secundaria: decodifica *Lcook* usando *K2* y comprueba si son correctos la localización y la marca de tiempo. Si esta comprobación tiene éxito, la petición es aceptada.
3. Si el tiempo de validez de *Lcook* ya ha expirado es necesario proceder a la verificación de la clave primaria: *Hcook* ha de ser decodificada usando *K1*. La petición es rechazada si alguna de las siguientes condiciones no se satisface:
   - El período de acceso no ha expirado.
   - La localización codificada en la clave es válida.
   - El bloque aleatorio codificado en la clave coincide con el que se encuentra almacenado en el registro de claves temporales.
4. Si la clave primaria es correcta, una nueva clave (conteniendo un nuevo bloque aleatorio) es generada y almacenada en el registro de claves temporales. Asimismo, una nueva clave secundaria es generada, y los dos nuevos valores son enviados codificados como cookies hacia el navegador del usuario, a la vez que se envían los resultados de la petición original. A partir de este momento, si se reciben nuevas peticiones con el valor antiguo de *Hcook*, el valor de su bloque aleatorio no coincidirá con el almacenado en el registro, por lo que el PoA asume que se ha producido una duplicación de cookies y rechazará por tanto las peticiones.

4. Estado actual

Desde hace algún tiempo, una implementación estable de PAPI puede encontrarse en `http://www.rediris.es/app/papi/dist/`. Esta implementación incluye un

Servidor de Autenticación basado en Perl, que incluye soporte para diferentes métodos de validación de la identidad del usuario y de sus derechos de acceso, basados en LDAP, POP-3 o una base de datos interna derivada del formato Berkeley. Este AS puede emplearse como un CGI dentro de cualquier servidor Web y proporciona un interface para extenderlo por medio de métodos de autenticación adicionales. El Punto de Acceso incluido en esta distribución de PAPI se basa en el módulo *mod_perl* [5] de Apache. Puede ser integrado con cualquier servidor Web basado en Apache y configurado por medio de directivas específicas dentro del propio fichero de configuración de Apache.

PAPI está siendo empleado para controlar el acceso a zonas protegidas en los servidores Web de RedIRIS, y también es usado por diferentes instituciones de la Red Académica Española. Por ejemplo, la Unidad de Bibliotecas del CSIC emplea PAPI para facilitar el acceso de sus usuarios (dispersos por toda la geografía española) a los contenidos de los proveedores de información con los que tiene establecidos contratos de acceso. Para cada uno de estos proveedores se ha definido un PoA, y todos son controlados por un GPoA. Otros PoAs han sido definidos para controlar el acceso a la intranet de la Unidad, y a los propios mecanismos de gestión de los usuarios del sistema.

La tecnología PAPI está siendo empleada también en otros países para proporcionar un punto único de autenticación para acceder a contenidos digitales [6], o servicios para facilitar el intercambio inter-institucional de contenidos, como es el caso de [7] y [8]. En estos entornos, se han evaluado nuevos métodos de autenticación y se ha demostrado la aplicabilidad de PAPI a los diferentes sistemas de acceso a la información por medio de la WWW que emplean los proveedores comerciales de contenidos. PAPI constituye una de las componentes esenciales de la implementación de referencia de un sistema de autenticación y autorización que TERENA, la asociación de redes académicas europeas, está construyendo en el marco del proyecto TFAACE [9] y en colaboración con Internet2 [10].

5. Conclusiones

Esta ponencia ha presentado un sistema que pretende armonizar las necesidades tanto de productores como de consumidores de información y que facilita el establecimiento de relaciones de confianza entre los mismos. La arquitectura y los protocolos en los que se basa el sistema están diseñados para garantizar la independencia de los actores y preservar la privacidad de los usuarios. Todos los procedimientos son transparentes para el usuario, de manera que no se requiere formación adicional, por lo que el sistema puede ser fácilmente incorporado en cualquier organización.

El equipo que participa en el desarrollo de PAPI trata de mantener la evolución del sistema de acuerdo con las necesidades de las instituciones usuarias. Se mantienen reuniones periódicas con estas instituciones, con el objetivo de recopilar sus necesidades con respecto al sistema y de mejorar su funcionalidad y usabilidad. Como resultado de este proceso, los nuevos trabajos se concentran en:

1. Portar el PoA PAPI a diferentes entornos, especialmente a servidores basados en ISAPI, y mejorar sus prestaciones. Un interface común para los PoAs (con independencia de la implementación base) ha sido definida y se ha implementado como una librería ISAPI y como un módulo Apache.

2. Desarrollar el protocolo de manera que pueda emplearse una evaluación dinámica de los derechos de los usuarios, derivada a partir de las aserciones originalmente enviadas por el AS.

3. Extender la sintaxis y la semántica de las aserciones para poder transportar más información y permitir grados más finos de control, alineando el sistemas con las normas que están apareciendo en el campo de los lenguajes para la definición de niveles de seguridad [11].

Referencias

[1] E. Giabarra, "Licenses, contracts and intellectual property rights", *Jornadas sobre recursos electrónicos*, SEDIC, Madrid, Mayo 2000.

[2] I. Fuchs, "Remote Authentication and Authorization for JSTOR", *JSTORNEWS*, no. 2, Issue 3, Otoño 1998.

[3] D. R. López, M. Reina, “Providing secure mobile access to information servers with temporary certificates”, *Computer Networks*, Elsevier Science Press, vol. 31, no. 21, Noviembre 1999.

[4] A. Robiette, "Sparta: the Second-Generation Access Management System for UK Further and Higher Education. A discussion paper on the requirements", disponible en `http://www.jisc.ac.uk/pub00/sparta_disc.html`

[5] L. Stein, D. MacEachern, *Writing Apache Modules with Perl and C*, O’Reilly & Associates, Abril 1999.

[6] JISC, “Call for Projects in Authentication and Authorisation”, disponible en `http://www.jisc.ac.uk/pub02/c06_02.html`

[7] UNINETT, "FEIDE project”, disponible en `http://www.uninett.no/prosjekt/feide/index.en.html`

[8] SWITCH, "The SWITCH AAI concept", disponible en `http://www.switch.ch/aai/`

[9] TERENA, ”Task Force on Authentication and Authorization Coordination for Europe”, disponible en http://www.terena.nl/task-forces/tf-aace/

[10] Internet2, “Shibboleth”, disponible en http://middleware.internet2.edu/shibboleth/

[11] OASIS Security Services Technical Committee, "SAML 1.0 Specification Set", disponible en http://www.oasis-open.org/committees/security/