Federando servicios de VoIP sobre eduroam

José Luis Hernández Ramos, Gabriel López
Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia
Email:{jluis.hernandez, gabilm}@um.es

***Resumen*—Este trabajo presenta una propuesta para enriquecer los mecanismos de gestión de identidad en el protocolo SIP (Session Initiation Protocol) para VoIP, así como su aplicación en un entorno ampliamente extendido como es la federación de red eduroam. El diseño propuesto se basa en los resultados obtenidos en el proyecto DAMe, posibilitando un proceso de SSO (Single Sign On) en SIP, desde el acceso a la red, además de proporcionar mecanismos de autorización avanzada. Se presentan distintos perfiles de uso y un análisis de rendimiento que analiza la viabilidad de la solución.**

***Palabras clave*: eduroam, SIP, DAMe, federación, SAML**

I. Introducción

Ante el incremento del número de servicios disponibles en Internet, así como del número de usuarios asociados a su utilización, la preocupación sobre la protección de recursos entre organizaciones ha motivado la proliferación de las federaciones de identidad [1]. Aunque en la última década varias iniciativas internacionales han intentado proporcionar diferentes soluciones, en el ámbito académico, eduroam se erige actualmente como el máximo exponente, interconectando miles de usuarios en instituciones académicas y de investigación de todo el mundo.

Una característica común de esos entornos es el uso de mecanismos de control de acceso basados en la identidad del usuario, referida normalmente a su nombre de usuario y contraseña, lo que imposibilita el desarrollo de un control de acceso preciso, así como la capacidad para ofrecer un servicio diferenciado a los usuarios. El proyecto DAMe [2] define un mecanismo aplicado a la infraestructura de eduroam para ofrecer, no sólo autenticación, sino también un mecanismo de SSO (Single Sign On) [3] que posibilita el acceso, por parte de un usuario itinerante, a los recursos de nivel de aplicación ofrecidos por la institución visitada, sin necesidad de volver a autenticarse en cada servicio. Además, DAMe ofrece a las instituciones que pertenecen a eduroam la posibilidad de aplicar decisiones de autorización avanzadas basadas en atributos de usuario, obtenidos desde la institución origen, y analizados en las instituciones visitadas por los usuarios.

Existen, además, tecnologías que permiten desplegar sobre eduroam servicios federados, es decir, servicios que mantienen una relación de confianza entre sí, como el Web (Shibboleth [4], PAPI [5], etc.). Sin embargo, todavía existen muchos servicios que no se pueden usar de manera eficiente en este tipo de federaciones, puesto que no existen procedimientos técnicos apropiados. Este problema ha sido recogido por diferentes iniciativas, que actualmente están planteando soluciones para la federación de cualquier tipo de servicio en la red (SSH, FTP, SMTP, XMMP, etc.), no sólo el acceso a la propia red o al Web.

Uno de estos servicios en los que se está trabajando es la VoIP (Voz sobre IP) [8]. Este servicio, con el protocolo SIP (Session Initiation Protocol) [9] como principal impulsor, ha transformado el panorama tradicional de las telecomunicaciones en todo el mundo. La incorporación de SIP a eduroam supone ventajas de cierta consideración, posibilitando que usuarios itinerantes realicen tareas tan cotidianas como llamadas de voz o videoconferencias de igual forma que si estuvieran en su institución origen.

Este trabajo define los mecanismos y entidades necesarias para poder hacer uso de SIP en una federación como eduroam. Tomando como punto de partida los resultados obtenidos por el proyecto DAMe, se proponen dos mejoras al proceso de registro en SIP, de modo que se permita la realización de un acceso al servicio de modo federado. Además, la propuesta descrita ofrece la ventaja adicional de posibilitar un mecanismo de SSO en SIP desde el acceso a la red, haciendo uso de tecnologías como SAML [10] y XACML [11]. Este último aspecto permitirá que tras la autenticación del usuario durante el acceso a la red eduroam, éste pueda acceder a diferentes servicios, en este caso SIP, sin necesidad de tener que realizar un nuevo proceso de autenticación que involucre al propio usuario.

El resto de este documento está estructurado del siguiente modo. La sección II describe DAMe, mientras que en la sección III se detalla el proceso de registro SIP en un escenario interdominio. En la sección IV se presenta el despliegue del servicio de VoIP en DAMe/eduroam. A continuación, la sección V describe algunas propuestas relacionadas con este artículo y la sección VI presenta un análisis de rendimiento que analiza la viabilidad de este trabajo. Finalmente, la sección VII presenta las conclusiones y vías futuras.

II. DAMe

DAMe extiende la infraestructura de eduroam, proporcionando un sistema de autenticación y autorización unificado para el acceso a la red y servicios web. Como se describe en [2], la autenticación del usuario para el acceso a la red se realiza de la forma tradicional en eduroam. Sin embargo, para ofrecer la funcionalidad de autorización y SSO a usuarios itinerantes, los servidores RADIUS deben ser extendidos y nuevas entidades deberán ser desplegadas en las organizaciones.

En la Figura 1 se muestra el diagrama de flujo detallado de la propuesta DAMe [12]. El proceso comienza cuando un usuario solicita acceso a la red eduroam desde una institución visitada. Así, el usuario presenta sus credenciales de autenticación (correo electrónico y contraseña). El servidor RADIUS visitado, basándose en el identificador de dominio de la dirección de correo, determina que ese usuario no pertenece a esa institución y, mediante la infraestructura de servidores RADIUS, redirige la solicitud de acceso a su institución origen. El servidor RADIUS de esta institución autentica al usuario siguiendo el proceso tradicional (normalmente basado en EAP-TLS o PEAP). A continuación, con el fin de obtener un token para el usuario que ofrezca SSO, el servidor RADIUS origen contacta con su proveedor de identidad (IdP) por medio de un mensaje SAML *SAMLAuthnRequest*. La consulta incluye el identificador del usuario (*subject*) y el método de autenticación usado por el servidor. El IdP genera entonces una sentencia SAML *SAMLAuthnStatement*, que conforma el token SSO, y se lo envía al servidor RADIUS. Este token se distribuirá al usuario final a través del canal EAP establecido anteriormente en la fase de autenticación (en modo seguro). Una vez recibido, el token será almacenado y protegido en el dispositivo del propio usuario, demostrando que ha sido autenticado por un miembro de confianza de la federación. Para ello, esta sentencia debe ir firmada digitalmente por la entidad que la emite (IdP). A continuación, el servidor RADIUS de la institución origen envía un mensaje *Access-Accept*, indicando que el usuario ha sido autenticado con éxito. Este mensaje incluirá un *handle*, que estará representado por el pseudónimo asociado al usuario y que será utilizado durante la siguiente fase de autorización de red.

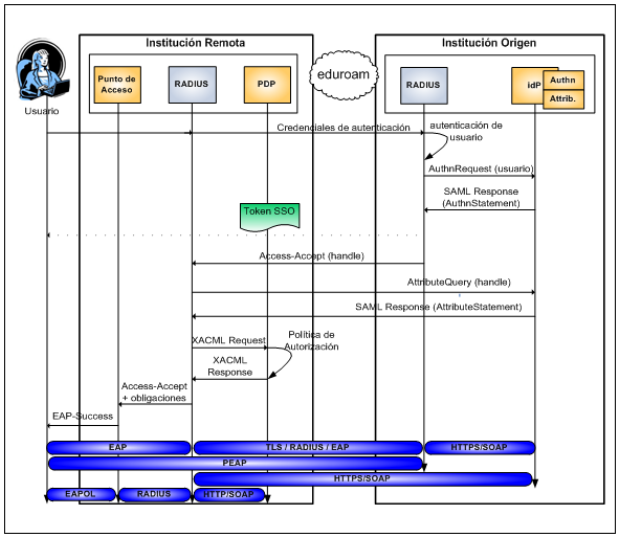

Figura 1: Autenticación y Autorización propuestos por DAMe

Una vez realizado el proceso de autenticación, antes de dar acceso al usuario a la red, la institución visitada podrá lanzar el proceso de autorización. Para ello, el servidor RADIUS, con el propósito de obtener información adicional del usuario (atributos), enviará un mensaje *SAMLAttributeQuery* al IdP origen del usuario. Esta entidad, haciendo uso del *handle* recibido en la solicitud, seleccionará los atributos del usuario que, según sus políticas de revelación de atributos [13], pueden ser enviados a la institución visitada. Es importante notar que el modo en el que el RADIUS visitado localiza al IdP de la organización origen puede basarse en dos mecanismos: o bien configuración estática; o bien mediante una entidad MDS (MetaData Service) que permite localizar las entidades de cada organización. Finalmente, el IdP genera una sentencia *SAMLAttributeStatement* que incluye los atributos visibles del usuario, enviada de vuelta al RADIUS visitado. Cabe destacar que, para proporcionar mayor seguridad, se debe establecer un canal seguro entre los servidores RADIUS y el IdP, normalmente mediante HTTPS/SOAP. A continuación, haciendo uso de los atributos recibidos, el servidor RADIUS de la institución visitada, enviará una consulta XACML de autorización a su entidad PDP (Policy Decision Point), con el fin de obtener una decisión final de acceso y conocer las propiedades (obligaciones) que deben ser aplicadas a la conexión de red del usuario (IP, QoS, VLAN, etc.). Finalmente, estas obligaciones son enviadas desde el servidor RADIUS hasta el punto de acceso y se notifica al cliente la decisión de autenticación tomada.

Es importante notar que la validación de sentencias SAML entre instituciones depende del despliegue de una infraestructura de confianza en eduroam. Para solventar este problema, se hace uso de una infraestructura de clave pública (Public Key Infrastructure o PKI) ya desplegada, eduPKI [14].

III. SIP

SIP (Session Initiation Protocol) [9] es un protocolo de señalización a nivel de aplicación que proporciona la creación, gestión y finalización de sesiones sobre una red IP. El término sesión hace referencia al intercambio de datos multimedia, como vídeo o voz. Una red SIP está compuesta fundamentalmente por dos tipos de entidades: agentes de usuario (User Agent, UA), elemento situado en los extremos de la comunicación; y un servidor SIP, dispositivo intermedio que asiste a los agentes de usuario en el establecimiento y gestión de sesiones.

El proceso de registro de SIP es imprescindible para que un agente de usuario pueda efectuar y recibir llamadas de otros clientes de la red, además de constituir el principal mecanismo para soportar la movilidad de los usuarios entre instituciones. Sin embargo, este procedimiento puede resultar muy costoso en ocasiones, ya que la solicitud de registro debe alcanzar la organización origen para validar las credenciales del usuario, todo ello atravesando varios proxys intermedios. Por consiguiente, este proceso debe llevarse a cabo de la forma más efectiva y eficiente posible, con el objetivo de que, tanto usuarios como instituciones, no se vean afectados en exceso por el coste de este proceso.

En este escenario, el registro comienza cuando el usuario itinerante conecta su cliente SIP a la red. Éste descubrirá, normalmente mediante DHCP [15], la dirección del servidor

SIP Registrar de la institución visitada. A continuación, enviará una solicitud *REGISTER* a este servidor. Éste, cuando recibe la solicitud, examina el campo *Request-URI* de la petición para determinar si el solicitante pertenece al dominio local o no. Si no es así, el servidor, actuando como SIP Proxy, envía la solicitud de registro al dominio del usuario, siguiendo el comportamiento definido en [9]. Cuando el SIP Registrar de la institución origen recibe la solicitud de registro, siguiendo el mismo mecanismo, descubre que dicha petición es de un usuario que pertenece a su dominio y utiliza un mecanismo de autenticación, normalmente HTTP-Digest [16]. Este proceso de autenticación puede ser realizado por el SIP Registrar, o bien, ser delegado en el servidor AAA de la institución origen, si se soporta [17]. HTTP-Digest se basa en el hecho de que, tanto UA como servidor, conocen un secreto compartido, en este caso la contraseña del usuario. La forma en la que se lleva a cabo este proceso es mediante un mecanismo de desafío-respuesta. Así, cuando el servidor recibe la solicitud de registro, emplea la cabecera *WWWAuthenticate* para enviarle este desafío al usuario a través del campo *nonce*. El UA, para determinar la respuesta al desafío, utiliza MD5 [18] sobre algunos campos de la solicitud. Una vez calculada la respuesta, el UA sitúa este valor en una cabecera *Authorization* y la envía mediante otro mensaje *REGISTER*. El servidor, cuando recibe la nueva solicitud, comprueba si el valor en la cabecera es el que espera y, en caso afirmativo, responde al UA con un mensaje *200 OK*, resultando en el registro del usuario.

IV. Despliegue de VoIP sobre DAMe

Como muestra la Figura 2, con el fin de hacer posible el despliegue del servicio de VoIP en la arquitectura propuesta por DAMe, existen algunas condiciones que deben ser cumplidas. Así, es necesario el despliegue de proxys SIP en las organizaciones para que usuarios itinerantes puedan hacer uso del servicio (este servicio ya está desplegado en la mayoría de instituciones). Además, dichas entidades deberán ser extendidas con el fin de interactuar con el IdP, para obtener información sobre el usuario y con el PDP, con el propósito de poder ofrecer un control de acceso avanzado y diferenciado dependiendo de la información del usuario recibida previamente. A continuación, se describe brevemente la funcionalidad requerida.

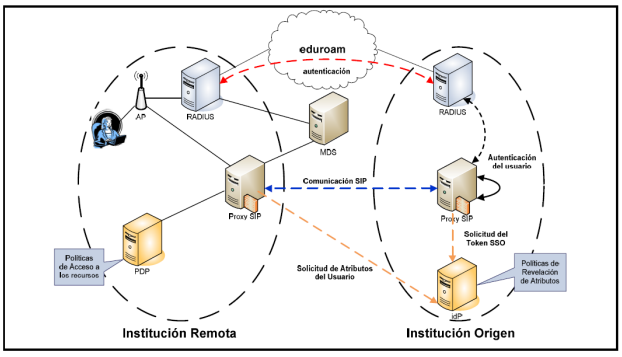

Figura 2: Arquitectura DAMe para el escenario de SIP

- RADIUS visitado. Encargado de redirigir peticiones de autenticación de usuarios a su institución origen.
- RADIUS origen. Recibe las solicitudes de autenticación enviadas por los servidores RADIUS visitados, validando las credenciales proporcionadas. Además, se encargará de distribuir la sentencia eduToken, según [12].
- Proxy SIP visitado. Se encargará de redirigir las solicitudes de registro SIP del usuario a la institución origen. Asimismo, se ocupará de llevar a cabo el proceso de autorización para el acceso al servicio SIP, haciendo uso del eduToken distribuido por la institución origen si está disponible.
- Proxy SIP origen. Este servidor recibirá las solicitudes de registro por parte de usuarios itinerantes. Si estas peticiones contienen el eduToken deberá validarlo. En caso contrario, se encargará de obtener un nuevo token SSO desde el IdP y distribuirlo al usuario.
- Policiy Decision Point (PDP). Entidad responsable de tomar las decisiones de autorización sobre los usuarios itinerantes para el acceso al servicio ofrecido por SIP, en base a los atributos recuperados.
- Identity Provider (IdP). Encargado de proporcionar información sobre los usuarios que pertenecen a la institución origen, generando sentencias eduToken para SSO o revelando atributos del usuario, según se requiera.

Para abordar las posibles situaciones del usuario itinerante en el momento de acceder al servicio de VoIP, se presentan dos escenarios: en el primero el usuario ha obtenido un token SSO (eduToken) durante el acceso a la red, y quiere hacer uso de éste durante el proceso de registro para SIP. En el segundo, el usuario no dispone de ese token porque no lo recibió durante el acceso a la red, o porque ha caducado. Así, deberá introducir sus credenciales de nuevo, pero el propio servicio de VoIP será el encargado de generar un nuevo token que permite el SSO en el acceso a futuros servicios. Una ventaja destacable de la infraestructura planteada es que no es necesario llevar a cabo cambios sustanciales sobre DAMe, permaneciendo tanto el PDP como el IdP inalterados ante el despliegue del nuevo servicio. A continuación se presentan ambos escenarios.

IV-A. Perfil de uso 1

Este perfil se basa en el hecho de que el usuario ya dispone del eduToken DAMe. La Figura 3 muestra cómo el usuario, mediante el uso de dicha sentencia, tiene la posibilidad de acceder al servicio SIP, sin necesidad de volver a autenticarse.

El proceso comienza cuando el usuario itinerante, a través de su SIP UA, intenta obtener acceso al servicio SIP en la institución visitada, haciendo uso de la solicitud *REGISTER*. Esta petición, con el fin de aprovecharse de la funcionalidad de SSO, incluye la sentencia de autenticación en la forma de una nueva cabecera llamada eduToken, según [19].

Cuando el SIP Registrar visitado recibe la solicitud de registro, comprueba, mediante el campo *Request-URI*, que ese usuario no pertenece al mismo dominio que gestiona. Así, basándose en información previamente almacenada, o bien mediante el uso de consultas DNS, ejercerá de SIP Proxy

siguiendo el comportamiento definido en [9] para hacer llegar la solicitud de registro a la institución origen.

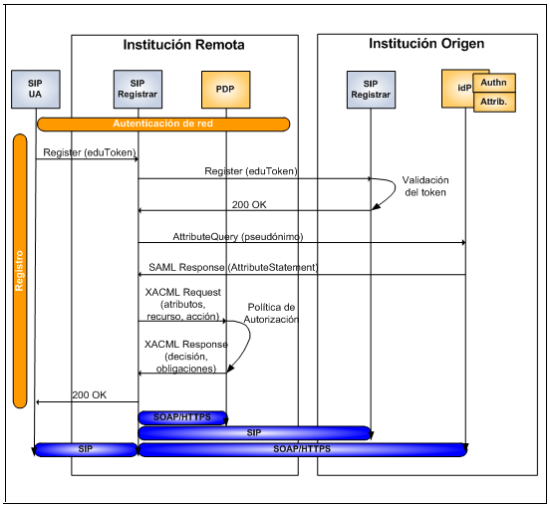

Figura 3: Perfil 1. El usuario dispone del eduToken

Tras recibir la solicitud de registro, el SIP Registrar origen descubrirá que dicha petición es de un usuario local. En ese momento, si detecta que la solicitud contiene un nuevo token de autenticación, validará la firma digital incluida en éste, que fue adjuntada por el IdP en el momento de la emisión de la sentencia. Además de validar la firma del token, comprobará su vigencia, asegurándose de que el instante de emisión de la sentencia, así como su periodo de validez continúan siendo válidos en el momento de recibir la solicitud de registro. En el caso de que la validación sea fallida por cualquier motivo, el SIP Registrar origen devolverá un mensaje de error *401 Unauthorized*, abortando de esta forma el proceso de registro SSO y lanzando el proceso tradicional descrito en la sección III. En caso contrario, si el token es validado correctamente, la entidad mencionada devolverá un mensaje *200 OK* al SIP Registrar visitado, incluyendo el pseudónimo asociado al usuario contenido en el eduToken según [19]. Este mensaje permitirá conexiones durante el tiempo de sesión asociado al token, que será determinado por el proxy.

Una vez que el proxy visitado recibe la respuesta a la solicitud de registro, deberá averiguar a qué sesión SIP está haciendo referencia dicho mensaje con el fin de lanzar posteriormente el proceso de autorización. Por ello, se ha seleccionado el campo *Call-ID* de SIP, que contiene un identificador único para todas las peticiones y respuestas de una sesión, resultando idóneo para esta tarea. De esta forma, el SIP registrar visitado, haciendo uso del pseudónimo recibido en el mensaje de respuesta, se encuentra en disposición de lanzar el proceso de autorización para el acceso al servicio de VoIP.

Una vez finalizado el proceso de autenticación basado en SSO, el proceso de autorización consta de dos fases. En primer lugar, el SIP Registrar visitado deberá obtener los atributos del usuario desde el IdP de la organización origen, del mismo modo que se describe en la sección II. En el caso de que no disponga de su ubicación, el SIP Registrar obtendrá esa información accediendo al servidor MDS. Para la obtención de los atributos del usuario, el SIP Registrar visitado utiliza el mensaje *SAMLAttributeQuery* siguiendo el profile SAML definido en [10]. Seguidamente, el IdP, según lo especificado en la consulta y su propia configuración de revelación de atributos, devolverá un mensaje *SAMLAttributeStatement* con los atributos pertinentes.

En la segunda fase del proceso de autorización, haciendo uso de la información obtenida en el paso previo, el SIP Registrar visitado deberá determinar si otorgar o denegar el acceso al usuario, y en qué condiciones debe hacerlo. Para ello, enviará una solicitud al PDP situado en la misma institución. Del mismo modo que se describe en la sección II, basándose en las políticas de las que disponga, enviará un mensaje indicando si debe permitir o denegar el acceso al usuario en cuestión, y contendrá una serie de obligaciones para las que el SIP Registrar deberá asegurar su cumplimiento (parámetros QoS, timeouts, propiedades SIP, etc.).

En base a la respuesta enviada por el PDP, si la respuesta de autorización es afirmativa, el SIP Registrar enviará un mensaje *200 OK* al usuario, dando por finalizado el registro. Ante cualquier otra respuesta del PDP, la contestación del SIP Registrar al cliente SIP será el mensaje *401 Unauthorized*, estableciendo que el proceso de registro no se ha podido completar. Sin embargo, en este caso, como el usuario sí está autenticado, este mensaje no contendrá la cabecera WWWAuthenticate del proceso tradicional de autenticación de SIP (sección III).

IV-B. Perfil de uso 2

En este perfil, Figura 4, un usuario itinerante intenta acceder al servicio SIP del modo tradicional, sin token de autenticación. El mecanismo utilizado es similar al descrito en la sección III mediante el registro de usuarios SIP entre dominios. Es decir, el SIP Registrar origen, haciendo uso de autenticación HTTP-Digest, insta al usuario a ser autenticado correctamente.

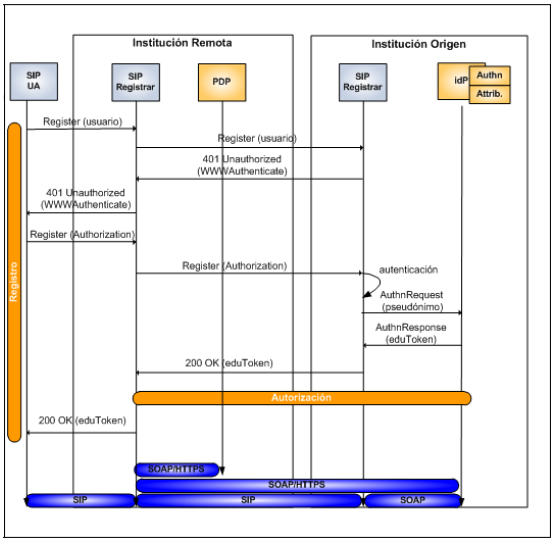

Figura 4: Perfil 2. El usuario no dispone del eduToken. Autenticación en SIP Registrar

Una vez concluido el proceso de autenticación, pero antes de devolver al usuario el mensaje *OK 200*, SIP Registrar

origen, con el propósito de obtener un nuevo eduToken, envía un *SAMLAuthnRequest* al IdP local, utilizando el nombre del usuario obtenido mediante la solicitud de registro. Puesto que la autenticación del usuario ya ha sido realizada, el SIP Registrar origen enviará la solicitud a un punto de entrada del IdP que, recibiendo la solicitud de una entidad confiable, tendrá la certeza de que el proceso de autenticación ya se ha efectuado y que únicamente debe generar un nuevo eduToken. El nuevo token será devuelto al usuario añadiendo una nueva cabecera al mensaje *OK 200*, del mismo modo [19].

Una vez obtenido el eduToken para el usuario, éste lo almacenará localmente, al igual que se propone en DAMe, para poder usarlo en posteriores accesos a servicios federados. Finalmente, el proceso de autorización podrá realizarse del mismo modo que se describió en el apartado anterior.

V. Análisis de rendimiento

Con el propósito de demostrar la viabilidad de este trabajo, los perfiles descritos en las secciones IV-A y IV-B han sido implementados. El escenario desplegado se compone de dos instituciones: una origen, a la que el usuario itinerante pertenece; y una visitada, donde se solicita el acceso al servicios. Ambas instituciones tienen desplegado el servicio de VoIP, al que el usuario intenta acceder. El escenario descrito se ha implementado sobre organizaciones reales pertenecientes a eduroam, en concreto, entre la Universidad de Murcia, actuando como institución origen, y la Universidad Técnica de Darmstadt, como institución visitada. La Tabla I detalla el hardware y software utilizado para el desarrollo de las pruebas.

Elemento	Hardware	Software
Institución Origen (Universidad de Murcia)		
Proxy home	Intel Core i5 2.27 GHz 4GB RAM	Jain-sip 1.2 Opensaml 2.3.2 Sun XACML
IdP	Pentium IV 1.5 GHz 512MB RAM	Shibboleth 2.3.2 Apache-Tomcat 6.0.32 MySQL 5.1.16
Institución Visitada (Universidad Técnica de Darmstadt)		
Proxy remoto	Intel Core i5 2.27 GHz 4GB RAM	Jain-sip 1.2 Opensaml 2.3.2 Sun XACML
PDP	Intel Core i5 2.27 GHz 4GB RAM	XACMLight

Tabla I: Hardware y software utilizado

Utilizando esos componentes, cada perfil ha sido ejecutado 100 veces. La mediana de estas pruebas se muestra en la Tabla II, junto con los tiempos de las fases parciales de cada perfil. Además, estas medidas son comparadas con los tiempos calculados en el trabajo [20], donde se obtienen los tiempos medios de acceso en eduroam (1568ms) y eduroam+DAMe (2817ms) en un escenario similar al propuesto en este trabajo.

eduroam	eduroam +DAMe	Perfil 1			Perfil 2		
		1865			2390		
1568	2817	Validar token	Obtener atributos	Consulta de autorización	Obtener token	Obtener atributos	Consulta de autorización
		327	749	109	414	749	109

Tabla II: Mediana de los tiempos obtenidos (ms)

Según los resultados obtenidos, el tiempo total del perfil 1 es de 1865 ms, que incluye los tiempos parciales:

- Validar eduToken: 327ms. Tiempo de validación de la firma contenida en el eduToken, haciendo uso del certificado contenido en la misma sentencia.
- Obtener atributos: 749ms. Tiempo que se consume desde que se genera la sentencia *AttributeQuery* en el proxy visitado, hasta que se obtiene una sentencia *AttributeStatement* del IdP origen. Es importante destacar que la consulta se realiza en un solo *round-trip* entre las instituciones y sobre un canal protegido HTTPS. Además, no se han realizado consultas al MDS, la información sobre localización del IdP se ha obtenido de modo estático en la institución visitada.
- Consulta de autorización: 109ms. Tiempo que se tarda en generar una sentencia *XACMLRequest* con los atributos obtenidos en el paso anterior, hasta que se recibe una sentencia *XACMLResponse* del PDP con la decisión de autorización tomada. Esta consulta se realiza en un *round-trip*, incluye la consulta de políticas XACML y la conexión se realiza sobre un canal HTTPS.

Hay que tener en cuenta que los intercambios SIP se realizan directamente sobre canales UDP y no se han utilizado conexiones seguras entre las instituciones (IPSec/SSL) que, aunque recomendables, no son normalmente desplegadas.

Las pruebas de rendimiento realizadas sobre el segundo perfil, ofrecen un tiempo medio de 2390 ms, lo cual representa un incremento del 28,15 % sobre el perfil 1. Este tiempo incluye los tiempos de autorización anteriores más el tiempo requerido por parte del SIP proxy origen para solicitar un nuevo token de autenticación al IdP. Este tiempo supone unos 414 ms, e incluye los mensajes de solicitud y respuesta SAML y el tiempo de generación y firma del token. Todo esto, igualmente, sobre un canal HTTPS entre SIP proxy e IdP. El incremento del tiempo es debido fundamentalmente al incremento en el número de mensajes intercambiados entre ambas instituciones durante el proceso de registro SIP.

La interpretación de estos resultados debe realizarse del siguiente modo. Según [20], el tiempo medio de acceso a la red eduroam para un usuario itinerante es aproximadamente 1,5 segundos, lo que se considera asumible para los usuarios. El intercambio de un token de autenticación adicional supone un tiempo total de acceso a la red de 2,8 segundos aproximadamente, incluyendo la recuperación de atributos y toma de decisiones. Suponiendo que se está ofreciendo un servicio diferenciado al usuario y que puede obtener una mejor experiencia en el acceso, se considera que este tiempo es asumible para los usuarios. Una vez que el usuario ha obtenido acceso a la red y tiene, o no, un token de acceso, decide realizar una llamada SIP. En este caso, el tiempo de registro de usuario si ya dispone del eduToken sería de aproximadamente 1,9 segundos, mientras que el tiempo de registro si no dispone de él sería de aproximadamente 2,4 segundos. Estos tiempos se consideran asumibles ya que se realizan previo establecimiento de llamada, y este proceso no se ve afectado por el uso o no del eduToken.

VI. Trabajo relacionado

Existen algunas propuestas relacionadas con la gestión avanzada de identidad en SIP y sus posibles aplicaciones. Así, los autores en Chavali et. Al. [21] hacen hincapié en

las carencias que ofrece el concepto de identidad en SIP y, haciendo uso de SAML, presentan dos perfiles en un escenario interdominio con el fin de que el destinatario de una llamada tenga la certeza de que el usuario origen de la misma se autenticó correctamente en su dominio. Sin embargo, el trabajo que aquí se presenta está centrado en la mejora del proceso de registro en SIP, pudiendo ser complementado por dicha propuesta. Por otro lado, los trabajos presentados en Khoury et. Al. [22] y Sisalem et. Al. [23] presentan diseños que tienen como propósito el de mejorar los esquemas de movilidad para usuarios SIP itinerantes, aunque no abarcan los problemas de SSO ni de autorización avanzada del usuario.

Nie et. Al [24] y Tschofenig et. Al [25], [26] consideran la incorporación de SAML a SIP con el fin de obtener un mecanismo de SSO, evitando la necesidad de procesos de autenticación adicionales para el acceso al servicio de SIP. Como se ha comentado, la gran ventaja de la solución que se ofrece en este trabajo es que el SSO no solo se ofrece este distintas conexiones del propio SIP, sino que se gestiona desde el propio nivel de red. Además, estas soluciones tampoco tienen en cuenta la incorporación de mecanismos de autorización avanzados basados en atributos del usuario.

VII. Conclusiones y vías futuras

Este trabajo pretende ofrecer un mecanismo para la federación de servicios de VoIP sobre federaciones de identidad, en concreto, eduroam. Para ello, se hace uso de la propuesta DAMe, aprovechando la gestión de sentencias de autorización, la toma de decisiones basadas en políticas XACML y la distribución de un token de autenticación que permita ofrecer SSO entre capas de red. Se han propuesto dos perfiles de uso, dependiendo de si el usuario tiene o no dicho token de autenticación. Se han analizado, desarrollado y desplegado ambos perfiles con el fin de realizar un análisis de rendimiento que permita establecer si la solución es factible o no desde el punto de vista de los usuarios finales. Los resultados indican que un proceso de registro para VoIP, en una institución visitada, entre 1,8 y 2,4 segundos, podría ser un tiempo asumible por el usuario, suponiendo que va a recibir a cambio una mejor experiencia en el acceso al servicio de voz, por ejemplo, mediante parámetros específicos de QoS, servicios de VoIP personalizados, etc.

Este trabajo se enlaza con el que se está realizando actualmente en el grupo de trabajo ABFAB del IETF [7], así como en el proyecto Moonshot [6], donde se intenta ofrecer una solución a la federación de cualquier tipo de servicio más allá del Web. La integración de las tecnologías propuestas en ABFAB y Moonshot, así como el estudio de implantación de arquitecturas como IMS en eduroam, son vías futuras de investigación sobre este trabajo.

Agradecimientos

Trabajo financiado por el proyecto MULTIGIGABIT EUROPEAN ACADEMIC NETWORK (FP7-INFRASTRUCTURES-2009-1) y el programa de excelencia de la Fundación Séneca (04552/GERM/06).

Referencias

[1] E.Norlin, A. Durand. “Federated identity management”. White paper, PingID Network, 2002

[2] O. Cánovas, A.F. Gómez-Skarmeta, G. López, M. Sánchez. “Deploying authorisation mechanisms for federated services in eduroam (DAMe)”. Internet Research, 17(5):479 - 494, 2007.

[3] R. Semancík. “Internet Single Sign-On Systems”. nLight, s.r.o., Mayo 2005. Research Report.

[4] T. Scavo, S. Cantor. “Shibboleth Architecture. Technical Overview”, Junio 2005. Working Draft 02.

[5] R. Castro, D.R. Lopez, J. Vega. “An authentication and authorization infrastructure: The PAPI System”. Fusion Engineering and Design, Volumen 81, Julio 2006.

[6] J. Howlett, S. Hatman. “Project Moonshot”. Briefing paper for TERENA Networking Conference, Junio 2010.

[7] K. Wierenga, L. Johansson. “Application Bridging for Federated Access Beyond web”. The Internet Engineering Task Force (IETF) – Working Group, 2011. http://tools.ietf.org/wg/abfab

[8] B. Goode. “Voice Over Internet Protocol (VoIP)”. Proceedings of the IEEE, Volume: 90, Issue:9, Septiembre 2002

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. “SIP: Session Initiation Protocol”. The Internet Engineering Task Force (IETF) - Network Working Group, Junio 2002. Request For Comments (RFC) 3261.

[10] OASIS. “Security Assertion Markup Language(SAML) V2.0 Technical Overview”. OASIS Committee Draft. , Marzo 2008.

[11] OASIS. “eXtensible Access Control Markup Language (XACML) Version 2.0”. OASIS Standard. 2005.

[12] O. Cánovas, M. Sánchez, G. López, R. del Campo, S. Neinert, J. Rauschenbach, I. Thomson. “DJ5.3.2: Architecture for Unified SSO”. Mayo 2008. Project Deliverable.

[13] M. Sánchez, Ó. Cánovas, G. López, A. F. Gómez-Skarmeta. “Managing the lifecycle of XACML delegation policies in federated environments”. 23rd International Information Security Conference (SEC 2008), Septiembre 2008.

[14] L. Florio, J. Howlett. “eduPKI Service Definition”. Febrero 2011.

[15] R. Droms. “Dynamic Host Configuration Protocol”. IETF RFC 2131. Marzo 1997.

[16] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. “HTTP Authentication: Basic and Digest Access Authentication”. IETF RFC 2617. Junio 1999.

[17] J. Loughney, G. Camarillo. “Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)”. IETF RFC 3702. Febrero 2004.

[18] R. Rivest. “The MD5 Message-Digest Algorithm”. IETF RFC 1321. Abril 1992.

[19] J. Rosenberg, H. Schulzrinne. “Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)”. IETF RFC 4485. Mayo 2006.

[20] M. Sánchez, G. López, O. Cánovas, A.F. Gómez-Skarmeta. “Performance Analysis of a Cross-layer SSO Mechanism for a Roaming Infrastructure”. Journal of Network and Computer Applications, 32(4):808-823, Febrero 2009.

[21] A. Chavali, D.C. Sicker. “Role-Based Authorization in the Session Initiation Protocol (SIP) based on SAML”. University of Colorado Boulder. 2003

[22] J.S. Khoury, H.N Jerez, C.T. Abdallah. “H-SIP Inter-Domain SIP Mobility: Design”. Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE, Enero 2006.

[23] D. Sisalem, J. Kuthan. “Inter-domain Authentication and Authorization Mechanisms for Roaming SIP Users”. 3rd International Workshop on Wireless Information Systems, Abril 2004.

[24] P. Nie, J. Tapio, S. Tarkoma, J. Heikkinen. “Flexible Single Sign On for SIP: Bridging the Identity Chasm”. IEE ICC’09 Proceedings of the 2009 IEEE international conference on Communications, Junio 2009.

[25] H. Tschofenig, R. Falk, J. Peterson, J. Hodges, D. Sicker, J. Polk. “Using SAML to Protect SIP”. Journal IEEE Network - NETWORK , vol. 20, no. 5, pp. 14-17, Octubre 2006.

[26] H. Tschofenig, J. Hodges, J. Peterson, J. Polk, D. Sicker. “SIP SAML Profile and Binding draft-ietf-sip-saml-08”. Internet Draft. Octubre 2010.