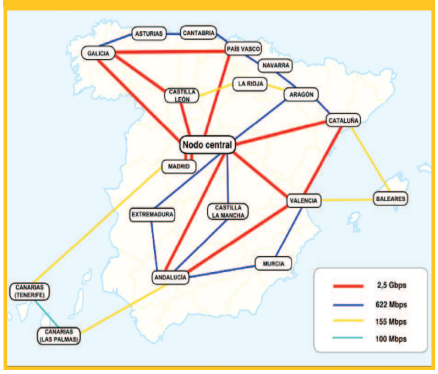
• RedIRIS2

Durante estos últimos meses se ha realizado una mejora en uno de los enlaces nacionales, aquel que une los nodos de Tenerife y Las Palmas de Gran Canaria. Este enlace es especial en cuanto a que el proveedor es el propio gobierno canario, el cual, tras realizar una importante inversión en las infraestructuras que interconectan dichas islas, ha hecho posible cambiar de un 34 Mbps (E3) a un enlace FastEthernet.

TOPOLOGÍA DE RedIRIS2



Sin embargo, se avecinan importantes cambios en la red y en los próximos meses comenzará una nueva e importante etapa. La actual insfraestructura nacional, RedIRIS2, resultado de un concurso público realizado en 2002 y en operación desde primeros de 2003, termina el 31 de octubre 2006. Para entonces, una nueva infraestructura de comunicaciones deberá estar desplegada que pasará a denominarse RedIRIS10.

Durante estos meses hemos estado trabajando en la redacción del pliego de claúsulas técnicas para el concurso público que convocará el Ministerio de Educación y Ciencia en breve. Las características técnicas de esta nueva red han sido determinadas tras analizar tanto las necesidades actuales y futuras de nuestros usuarios como el estado tecnológico de las redes de investigación de nuestro entorno y las necesidades de los servicios de red de nueva generación que están en fase de investigación actualmente.

El otro gran reto al que nos enfrentaremos en breve será al traslado del equipamiento de red de nuestro nodo en Madrid ubicado en la calle Serrano 142 y donde actualmente se encuentran alojados los equipos pertenecientes al núcleo de la red y aquellos donde se conectan las instituciones de Madrid. También se encuentran alojados allí gran cantidad de servidores que soportan los servicios nacionales. Por diversas razones este edificio no puede seguir alojando toda esta electrónica y se hace necesario trasladarla a un centro de especializado en este servicio. Carrier House 2 (CH2), situado en Alcobendas, fue seleccionado tras la realización de un concurso público.

El objetivo marcado es realizar este cambio antes de que comience el despliegue de RedIRIS10, de forma que los nuevos enlaces troncales ya vayan a CH2. Esta migración supone una gran complejidad y requiere de un alto nivel de coordinación, tanto con operadores como con fabricantes e instituciones directamente conectadas. Además, la comunicación e información con toda la comunidad RedIRIS será fundamental para generar confianza en el proceso y constituirá una de las actividades clave.

• Conexiones externas

En Espanix, a finales de 2005, el tráfico que intercambiabamos con algunos operadores comenzó a verse afectado por una degradación del rendimiento de los flujos a partir de cierto volumen de tráfico. Esta degradación era causada por el equipamiento que se utilizaba en la LAN del ESPANIX.

Tras detectar el origen del problema y encontrar que su solución (adquisición de nuevo hardware) no era inmediata, se decidió migrar las conexiones de RedIRIS a dos conmutadores 10G especiales. Son especiales porque son utilizados por un grupo reducido de operadores que necesitan intercambiar enormes volúmenes de tráfico, y cuentan además con una matriz de mayor rendimiento y capacidad para soportar conexiones de 10G.

Además de este cambio, tras verificar los niveles de ocupación de estos 2Gbps, se decidió duplicar la capacidad de conexión, con lo que la situación actual es una conexión de 4Gbps en la LAN de ESPANIX y una vez que la asociación adquiera nuevos conmutadores que reemplacen a los que presentan problemas de rendimiento, los cuatro enlaces GigaEthernet se moverán a dichos conmutadores.

En cuanto a las conexiones de tránsito (conectividad con la Internet comercial), contamos con dos enlaces GigabitEthernet: uno con Level3 y otro con Telia, y desde enero de 2006 se ha establecido una nueva conexión con un tercer operador, Cogent. La cantidad de tráfico cursado por estos enlaces en febrero fue de:

- ESPANIX: 300 TB, alcanzando el tráfico los 1,3Gbps
- Tránsito (Level3+Telia+Cogent): 200 TB y tráfico con niveles puntuales de 1.6 Gbps

ACTUALIDAD de RedIRIS

Se avecinan importantes cambios en la red con el despliegue de la nueva infraestructura RedIRIS 10

En breve el equipamiento de red del nodo de Madrid se trasladará a un centro de alojamiento especializado

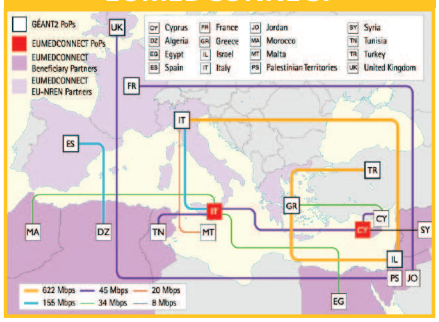
RedCLARA se ha extendido hasta los países centroameri-canos que estaban pendientes de los enlaces de conexión

La intranet de investigación mundial se ha complementado con el despliegue de una red entre países de Asia y Australia

• Proyectos internacionales para la creación de redes: EUMEDCONNECT, RedCLARA y TEIN2.

La red EUMEDCONNECT se ha extendido hasta Palestina y Siria y además, los enlaces troncales entre los nodos de EUMEDCONNECT y GÉANT2 se han aumentado a 622 Mbps tal y como se puede apreciar en la figura.

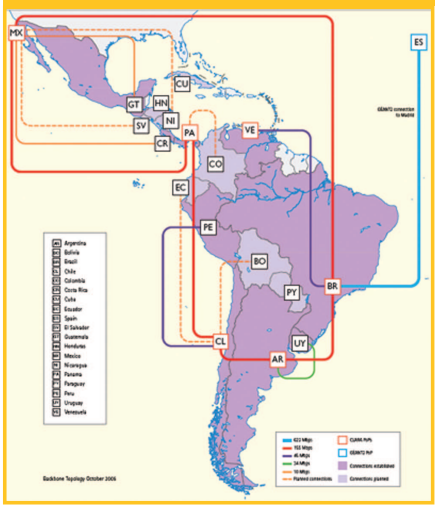
TOPOLOGÍA DE EUMEDCONNECT



RedCLARA se ha extendido hasta los países centroamericanos que estaban pendientes de los enlaces de conexión y Costa Rica, Guatemala, El Salvador y Nicaragua ya están en la red, con enlaces de 10Mbps al nodo de RedCLARA en Tijuana. Colombia y Ecuador también se han conectado; Colombia con un enlace de 10 Mbps al nodo de Panamá y Ecuador al de Chile con la misma velocidad. Aún siguen pendientes de su incorporación a la red Honduras, Paraguay y Cuba.

RedCLARA es Ipv6 nativa y soporta multicast y actualmente se está trabajando en el despliegue de Ipv6 mcast.

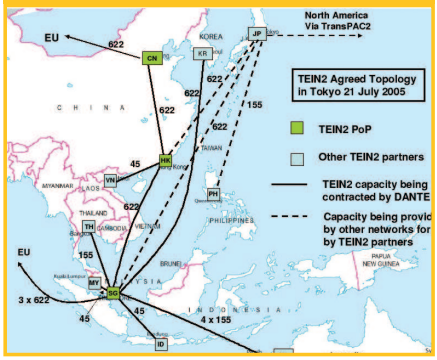
TOPOLOGÍA DE RedCLARA



La intranet mundial de la investigación se ha complementado con el despliegue de una red entre países de Asia y Australia, llamada TEIN2 (Trans-Eurasia Information Network, www.tein2.net). El despliegue de esta red pertenece a un proyecto financiado por la Comisión Europea cuyo objetivo es construir una infraestructura de red entre las redes de investigación de los países del área Asia-Pacífico y su interconexión con Europa (GÉANT2).

Se trata de una una red con 14 enlaces interconectando a 10 países que cuenta con un núcleo entre Tokyo-Singapore-Hong Kong a 622 Mbps. En estos puntos están situados los PoP de TEIN2 y a ellos llegan las conexiones del resto de los países: Australia, China, Indonesia, Corea, Malasia, Filipinas, Tailandia y Vietnam.

TOPOLOGÍA DE TEIN2



La conexión de esta red con GEÁNT es de 4x 622Mbps; uno de estos enlaces va por el Norte hasta Copenhague y los otros tres, a través de un enlace submarino, por el Sur hasta Frankfurt. El NOC de esta red está operado por la Universidad Tsinghua (Beijing) y los routers situados en los PoP de TEIN2 han sido donados por Juniper.

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red

GÉANT2

- Actualidad sobre la red paneuropea de redes académicas y de investigación

• Estado del despliegue de la red

Durante estos meses se ha estado desplegando la nueva infraestructura de red europea GÉANT2. El despliegue se ha divido en cinco fases comenzando por los nodos situados en Centro Europa y avanzando hacia nodos situados en los extremos. El nodo de GÉANT2 en España está situado en Madrid y las conexiones que tiene con el resto de la red son tres enlaces alquilados de 10Gbps (dos con el nodo de Francia en París y

uno con el nodo de Italia en Milán) y un enlace de fibra oscura Madrid-Ginebra.

En la fase IV se programó la puesta en producción del nodo en español, que se ejecutó duranta la última semana de febrero y primeros de marzo con la puesta en operación de los enlaces alquilados. Durante los dias 28 de febrero y 1 de marzo, RedIRIS migró su conexión de GÉANT a GÉANT2. La puesta en producción de la fibra oscura con Ginebra es más compleja técnicamente y está programada para abril.

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red

• Estado de las aplicaciones y actividades

Durante la última reunión celebrada en Cambridge se tomaron importantes decisiones de coordinación en cuanto al desarrollo de software propio de GÉANT2. Tanto desde la licencia que será aplicable al mismo como de los mecanismos de desarrollo colaborativo que se van a emplear. También se celebraron varias reuniones de coordinación entre los proveedores de la infraestructura de autenticación y autorización de GÉANT2 (liderados por RedIRIS) y las actividades usuarias dentro del proyecto.

Es de destacar también la contribución de RedIRIS en las reuniones de planificación de las actividades para el próximo periodo del proyecto, y en especial con los planes de proveer un conjunto de mecanismos de gestión de identidad para aquellas NREN que todavía no cuentan con una infraestructura propia. De esta manera, el nivel de desarrollo en estas tecnologías no impedirá su aplicación dentro de GÉANT2.

•Actividad JRA2

- Actividad JRA2 para la dotación de un marco de seguridad a GÉANT2

JRA2 (Joint Research Activity) es una de las actividades de investigación definidas en GÉANT2 enfocada a dotar de un marco de seguridad a la nueva red paneuropea, tanto en protección de equipos de red como en la cooperación entre las distintas redes para proporcionar una capacidad coordinada de respuestas ante incidentes.

Dentro del JRA2 se ha definido una serie de líneas de trabajo (Work Items, en adelante WI), que permitirán conseguir los objetivos marcados en esta actividad, entre ellos los más interesantes para la comunidad académica son los tres primeros:

- **WI1 (Protección de elementos y servicios de red de la red GN2)**. Actividad liderada por Dante en la que se pretenden elaborar recomendaciones y políticas de seguridad para el equipamiento y servicios de la red GÉANT2 y de las redes nacionales de investigación conectadas a ella, así como su posterior aplicación para asegurar dichos componentes. Dentro de esta línea de trabajo se ha incluido un nuevo servicio de filtrado y/o saneamiento de tráfico bajo demanda en el backbone de GN2 aún en discusión.

- **WI2 (Creación de servicios de seguridad)**. Liderada por SURFnet, pretende definir un conjunto integrado de herramientas, que podrán ser utilizadas por las distintas NREN, para monitorizar el tráfico de la red de cara a detectar y diagnosticar anomalías y ataques de seguridad.

- **WI3 (Diseño y establecimiento de una infraestructura de coordinación de incidentes de seguridad).** GARR lidera este apartado en el que se quiere fomentar el uso de las herramientas resultantes del WI2 y establecer canales de comunicación seguros entre los equipos de seguridad de las distintas redes de investigación para el intercambio de incidentes de seguridad, previo acuerdo de un formato unificado de intercambio y de una taxonomía, niveles de gravedad y procedimientos de manejo de información.

Se ha producido un cambio estratégico significativo en esta actividad; en un principio, las actividades estaban orientadas a hacer que los equipos de seguridad existentes en GÉANT fueran más efectivos sin centrarse en las necesidades de seguridad específicas de GÉANT2 como conjunto y, actualmente, los niveles de seguridad varían entre las distintas redes académicas nacionales dependiendo de múltiples factores. No existe un acuerdo acerca de unos niveles de seguridad mínimos a mantener y, dado que la seguridad de una red como conjunto es igual a la seguridad del más débil de sus componentes, esto puede tener un impacto negativo para el resto de las NREN conectadas a GÉANT así como para toda la red paneuropea.

El nodo de GÉANT2 en España está situado en Madrid

En Cambridge se tomaron importantes decisiones de coordinación en cuanto al desarrollo de software propio de GÉANT2

Se ha producido un cambio estratégico significativo en la actividad JRA2 para la dotación de un marco de seguridad a GÉANT2

eduGAIN es la arquitectura de la infraestructura de autenticación y autorización de GÉANT2

Este nuevo enfoque se puede conseguir prestando especial atención a las siguientes cuestiones:

- Obtener un compromiso de mínimos por parte de los comités de dirección de las distintas redes académicas.
- Que algunos aspectos de investigación que se llevan a cabo en el JRA2 pasen a ser servicios en operación para poder ser utilizados en el día a día de GÉANT2.
- Ayudar a la formación de nuevos equipos de seguridad en aquellas redes que no cuenten con uno establecido.

Actualmente se está trabajando en el plan de trabajo para el tercer año de vida del proyecto que intentará refinar las distintas actividades de investigación con el fin de obtener los mejores resultados al final del proyecto.

- **Actividad JRA5**

- Actividad JRA5 para la creación de una arquitectura de la infraestructura de autenticación y autorización

A lo largo de estos meses se ha definido la arquitectura de la infraestructura de autenticación y autorización de GÉANT2, que el equipo del proyecto ha bautizado como eduGAIN (GÉANT Authorisation INfrastructure); el documento que contiene esta definición se encuentra disponible como uno de los resultados de GN2 en la siguiente dirección: http://www.geant2.net/upload/pdf/GN2-05-192v6.pdf.

Esta arquitectura se centra en la capacidad de interconexión de diferentes infraestructuras nacionales (como es el caso de PAPI dentro de RedIRIS) utilizando perfiles específicos del estándar SAML para intercambiar de manera dinámica datos relativos a las interfaces de acceso a datos de identidad de los usuarios, establecer los mecanismos de confianza entre estas interfaces y garantizar que la privacidad de los usuarios se conserva cuando estos datos atraviesan los límites de la NREN. Ya ha comenzado el trabajo en la implementación de eduGAIN, cuya primera versión está planificada para septiembre de este año.

Las actividades relacionadas con la evolución de eduroam han producido una primera versión de la política del servicio tal como será proporcionado directamente por GÉANT2 y se han realizado diversos experimentos para evaluar las opciones de arquitectura disponibles para proporcionar a eduroam una arquitectura más flexible y con mayor tolerancia a fallos. Asimismo, se están iniciando experimentos para la conexión de eduroam con eduGAIN, lo que permitiría ofrecer a los usuarios de GÉANT2 una experiencia de acceso unificado (Universal Single Sign-On) tanto a la red como a sus servicios.

Diego López
(diego.lopez@rediris.es)
Coordinador de Middleware
Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de seguridad IRIS-CERT

III Edición del Reto de Análisis Forense

- III edición del concurso de Análisis Forense digital en castellano

La Universidad Autónoma de México (UNAM) y Red.es, a través del grupo de seguridad de la red académica nacional RedIRIS (IRIS-CERT), han convocado la realización del III Reto de Análisis Forense.

El reto consistirá en analizar un ordenador que ha sido atacado y averiguar cómo se produjo el ataque y a qué información accedió el atacante.

Con respecto a las ediciones anteriores, este reto de análisis forense cuenta con importantes variaciones ya que se analizará un sistema operativo Windows, de Microsoft, que tiene una gran difusión de uso entre los usuarios de Internet, de forma que las experiencias sobre este análisis puedan aplicarse en casos similares.

Los participantes han tenido hasta finales de marzo para analizar los datos y presentar un informe que en la actualidad está siendo evaluado por un Jurado de expertos de seguridad informática de diversos países.

En la página del reto, http://www.seguridad.unam.mx/eventos/reto se puede obtener información actualizada del concurso.

Francisco Montserrat
(francisco.monserrat@rediris.es)
Equipo de seguridad IRIS-CERT

Grupo de trabajo RTIR

- Actualidad sobre la herramienta utilizada por IRIS-CERT para la gestión de incidentes de seguridad

Como ya se ha comentado en pasados boletines, RTIR (Request Tracker for Incident Response

http://www.bestpractical.com/rtir) es la herramienta (*Open Source*) actualmente utilizada por IRIS-CERT, así como por multitud de equipos de seguridad en Europa y el resto del mundo, para realizar la tarea de atención y gestión de incidentes de seguridad.

Los objetivos del grupo de trabajo RTIR-WG, que se encuentra dentro del TERENA TF-CSIRT (CSIRT Coordination for Europe), han cambiado desde que se creó en enero de 2004. En un principio la principal tarea fue la especificación de un documento de nuevos requerimientos para el RTIR, teniendo en mente la obtención de nuevas mejoras y funcionalidades que permitiesen ampliar y hacer más flexible el flujo de trabajo del RTIR, así como que nuevos equipos pudiesen adoptar RTIR como su herramienta de gestión de incidentes de seguridad. En la actualidad el principal esfuerzo del grupo va dirigido a la gestión y supervisión del proyecto de desarrollo de la nueva versión.

Las cosas han cambiado mucho desde la última referencia efectuada en el número 73 del Boletín de RedIRIS (http://www.rediris.es/rediris/boletin/73/ACTUALIDAD.pdf); entre otras, cabe resaltar la firma del contrato entre TERENA y BestPractical.com para el desarrollo de la nueva versión del RTIR, basada en el documento de requerimientos escritos por este grupo de trabajo. Dicha firma se celebró el día 6 de septiembre de 2005 y, conforme a una de las cláusulas del contrato, la fecha de inicio del proyecto se fijaba un mes después, por lo que el proyecto arrancó de forma oficial el 6 de octubre de 2005. El contrato establecía además de la fecha de inicio, la división del proyecto en tres fases de seis meses de duración cada una; al final de cada una de las cuales los miembros del grupo tendrían un periodo de quince días para la revisión de la fase concluida; de esta forma podrían comprobar que el software entregado cumple con todos los requerimientos, que debían ser desarrollados según el contrato para ese ítem. La fecha de finalización, en principio, fue establecida, según el contrato, en mayo de 2007, aunque podría ser susceptible de cambios, debido a que en el contrato se fijó que durante los periodos de revisión, el grupo de trabajo podría no aceptar la versión del software entregado, y por tanto se pasaría a una fase de discusión entre BestPractical y el grupo para solucionar dichos problemas.

Durante este periodo se han celebrado dos reuniones del grupo de trabajo (http://www.terena.nl/activities/tf-csirt/ rtir.html). En la primera de ellas, el pasado mes de septiembre en Lisboa, coincidiendo con el TF-CSIRT, se eligieron a los miembros que desempeñarían funciones de coordinación, punto de contacto técnico y revisión establecidos por contrato. A raíz de esta elección, IRIS-CERT se hace cargo del liderazgo técnico del proyecto.

En esta reunión, también se presentó la guía de procedimientos y actuaciones que definían tanto la revisión del software en cada una de las fases, como los pasos previos que debían llevarse a cabo antes de iniciar el proceso de revisión.

La segunda reunión tuvo lugar en Ámsterdam, coincidiendo también con el TF-CSIRT, el pasado mes de enero. Debido a que la conclusión de la primera fase del proyecto se encontraba ya muy próxima (9 de marzo), el objetivo de esta reunión fue claro: acordar y finalizar los documentos que definen los procedimientos de evaluación del software de la primera fase, así como dividir el trabajo de test entre los integrantes del grupo de revisión.

Carlos Fuentes
(Carlos.fuentes@rediris.es)
Grupo de Seguridad IRIS-CERT

Informe de incidentes de seguridad año 2005

- Ya está disponible el informe de incidentes de seguridad de 2005

Está disponible en la página web de IRIS-CERT el informe de incidentes de seguridad de 2005 (http://www.rediris.es/cert/doc/informes/2005/), cuyo objetivo es dar un repaso detallado a los problemas más importantes de seguridad detectados en la Red Académica durante el pasado año.

En general, el año 2005 ha sido muy parecido al 2004. Aparte de los típicos gusanos, virus, bots, etc., los problemas que hemos tratado más habitualmente han estado relacionados con ataques de fuerza bruta SSH aprovechando contraseñas débiles y el acceso a equipos Linux debido a páginas PHP fácilmente explotables.

Precisamente, se ha dedicado una sección dentro del informe a las vulnerabilidades relacionadas con el web, además de la tradicional sección dedicada al spam.

Esperamos que encontréis el informe útil y nos mandéis vuestras sugerencias de mejora al buzón de IRIS-CERT (cert@rediris.es).

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de seguridad IRIS-CERT

IRIS-CERT se hace cargo del liderazgo técnico del proyecto

Respecto a incidentes de seguridad, el año 2005 ha sido muy parecido a 2004

La iniciativa ACRI nació para permitir el intercambio de firmas de IDS específicas para la detección de intrusiones en la red académica

RedIRIS está participando en eduGAIN a través de la implementación de una librería, que será utilizada por los distintos elementos de la infraestructura

Actualización de ACRI

- Actualización del Almacén Colaborativo de Reglas de Intrusión

La iniciativa ACRI nació en los Grupos de Trabajo de mayo de 2005 (http://www.rediris.es/cert/doc/reuniones/cord/gt2005/) para permitir el intercambio de firmas de IDS (Intrusion Detection System) específicas para la detección de intrusiones en la red académica, como complemento a las firmas oficiales.

Aunque el repositorio está disponible desde julio del año pasado, se ha realizado una serie de mejoras dignas de mención.

Para el repositorio utilizamos un wiki autenticado, de manera que todos los suscritos a la lista de coordinación IRIS-CERT (http://www.rediris.es/list/info/iris-cert.es.html) puedan acceder al mismo mediante el usuario/contraseña que se les ha proporcionado.

Para más informacion sobre la iniciativa, consultad su página web en http://www.rediris.es/cert/proyectos/acri.es.html.

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de seguridad IRIS-CERT

Reuniones de la XVI y XVII TF-CSIRT

- Últimas reuniones del equipo de respuesta de Incidentes de seguridad europeo

La XVI reunión del TERENA TF-CSIRT (CSIRT Coordination for Europe) se celebró en septiembre de 2005 en Lisboa, organizada por FCCN (Fundação para a Computação Científica Nacional) (http://www.terena.nl/tech/task-forces/tf-csirt/meeting16/) y la XVII se celebró en enero de 2006 en Ámsterdam (http://www.terena.nl/tech/task-forces/tf-csirt/meeting17/), organizada por CISCO y con una novedad: se trataba de la primera reunión organizada conjuntamente por TERENA y la secretaría del FIRST (*Forum of Incident Response and Security Teams*). En esta caso, durante la semana que duró el evento, hubo sesiones dedicadas exclusivamente al Task Force, y otras a temas relacionados con el FIRST, pero la organización de los seminarios del segundo día fue realizada de forma conjunta por ambas organizaciones, estando las sesiones abiertas a los miembros de ambos grupos, y fomentando el diálogo y la cooperación de las dos comunidades tan estrechamente relacionadas.

De los debates y conclusiones de las reuniones podemos destacar:

- El establecimiento de un marco de colaboración entre el TF-CSIRT y la iniciativa del CERT/CC CERT Development Team (http://www.cert.org/ csirts/).
- La puesta en marcha de la iniciativa CSIRT Mentoring Scheme (http://www.terena.nl/activities/tf-csirt/mentoring.html).
- Los aspectos y repercusiones en el trabajo diario de los CERT de la ley recientemente aprobada por el Parlamento Europeo sobre Retención de Datos que deberá ser traspuesta al derecho interno de cada país miembro en breve.

Para finalizar, tanto en Lisboa como en Ámsterdam se celebraron reuniones de equipos acreditados del servicio Trusted Introducer de TERENA (http://www.ti.terena.nl/) en las que se discutieron diversos aspectos operativos del servicio y posibles mejoras en el futuro.

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de seguridad IRIS-CERT

Desarrollo de eduGAIN

- eduGAIN la infraestructura de autenticación y autorización de GÉANT2

Dentro de los objetivos de la actividad JRA5 de GÉANT2, uno de los más importantes es definir y desarrollar una Infraestructura de Autenticación y Autorización común para la nueva red paneuropea, que al mismo tiempo integre infraestructuras ya existentes como PAPI o A-Select, como ya informábamos en el boletín de RedIRIS nº 73 (http://www.rediris.es/rediris/boletin/73/index.es.html).

Ya ha concluido una primera fase en la que se han definido tanto los requisitos de la infraestructura (http://www.geant2.net/upload/pdf/GN2-05-026v6.pdf) como la arquitectura de la misma (http://www.geant2.net/upload/pdf/GN2-05-192v6.pdf) y a esta infraestructura se le ha denominado eduGAIN. En este momento nos encontramos en una fase de implementación de los distintos componentes que forman parte de la misma.
RedIRIS está participando en este desarrollo a través de la implementación de una librería denominada eduGAINBase, que será utilizada por los distintos elementos de la infraestructura, y que sentará las bases del modelo de confianza

y de los distintos perfiles de funcionamiento que se contemplan para la arquitectura.

Diego R. López
(diego.lopez@rediris.es)
Coordinador del Área de Middleware
José M. Macías
(jmanuel.macias@rediris.es)
Área de Middleware

Servicio HelloSAML

- Herramienta de validación para sistemas de autenticación y autorización que utilicen SAML

Como parte de las actividades en las que viene participando RedIRIS dentro del Task-Force de Terena TF-MC2 (http://www.terena.nl/activities/tf-emc2/), se ha desarrollado HelloSAML (http://hellosaml.rediris.es). Se trata de una herramienta que permite comprobar el funcionamiento de infraestructuras de autenticación y autorización que utilizan el lenguaje de aserciones de seguridad SAML.

HelloSAML utiliza AARR (Authentication and Authorization Requester-Responder; http://www.rediris.es/app/aarr) y varios perfiles concretos que le permiten funcionar tanto en el papel de *contestador* de peticiones SAML como en el de *interrogador* de autenticación, autorización y atributos frente a infraestructuras ya existentes que usen este lenguaje.

El servicio se encuentra aún en fase de desarrollo, pero ya es posible solicitar una cuenta en el mismo y utilizarlo. Invitamos en este sentido a todos los miembros de la comunidad académica que trabajen con SAML a que lo prueben, y agradeceremos cuantas sugerencias nos hagan llegar al respecto.

Diego R. López
(diego.lopez@rediris.es)
Coordinador de Middleware
José M. Macías
(jmanuel.macias@rediris.es)
Área de Middleware

eduroam.es

- Proyecto de movilidad en el ámbito de la red académica española

En los primeros meses de este año ha habido un importante incremento en el número de organizaciones afiliadas a "eduroam.es" (la iniciativa "eduroam" http://www.eduroam. org en el ámbito de la red académica española), alcanzando a final de febrero las 35 organizaciones. La cobertura total de la iniciativa, organizada por ciudades y comunidades autónomas, puede consultarse en el mapa interactivo de la página http://www.eduroam.es. Además se ha incluido, enlazado a dicha página, un servicio de monitorización, "Estado de la jerarquía Radius", en el que se refleja el funcionamiento, tanto de servidores Radius de organizaciones finales, como de servidores Radius proxy, correspon-dientes a redes autonómicas, capaces de encaminar peticiones de autenticación entre organizaciones finales.

Para representar el estado de cada servidor en el mapa, se ha optado por un código de colores que refleja si un servidor no funciona (color rojo), que alguno de sus hijos no funciona (color amarillo), o bien que todo está correcto (color verde). A nivel de implementación, el test consiste en emular una autenticación contra un usuario de prueba "radius-test", configurado en cada uno de los servidores finales, con la peculiaridad de que este usuario no es un usuario válido de conexión, es decir, es un usuario que responde a la consulta de autenticación pero devuelve una serie de valores que no son válidos para obtener conectividad eduroam. En concreto, una consulta de autenticación contra este usuario responde un Access-Reject, con un atributo "Reply-Message" igual a "RADIUS OK", con lo que se consigue chequear el funcionamiento del servidor a través de un usuario no válido.

A nivel nacional, eduroam.es se ve reforzada con su inclusión en el proyecto "Campus Inalámbricos" (http://www.red.es/actividades/campus.html). Este proyecto surge de un acuerdo entre la CRUE (Conferencia de Rectores de la Universidades Españolas) y Red.es con objeto de impulsar el acceso inalámbrico a la red en los campus de las universidades públicas. Tras la convocatoria, se han presentado 34 proyectos, siendo uno de los requisitos esenciales en todos ellos la participación en la iniciativa "eduroam.es" o lo que es lo mismo, incluir en las propuestas medidas encaminadas a la creación de un espacio común WIFI entre universidades que facilite la movilidad de sus usuarios (permitiendo su conexión a Internet) y esté alineada con la iniciativa a nivel europeo "eduroam". Una vez ejecutados los proyectos englobados en "Campus Inalámbricos", se estima que 55 centros de la comunidad RedIRIS formen parte de "eduroam.es", lo cual daría como resultado uno de los mayores espacios de movilidad WIFI a nivel europeo, dentro de la iniciativa "eduroam" y permitiría disponer, a partir del año que viene, de un auténtico servicio interuniversitario para los usuarios.

Rodrigo Castro
(rodrigo.castro@rediris.es)
Técnico de Middleware

Ha habido un importante incremento en el número de organizaciones afiliadas a "eduroam.es"

A nivel nacional, eduroam.es se ve reforzada con su inclusión en el proyecto Campus Inalámbricos

pkIRISGrid, la infraestructura de clave pública usada en IRISGrid, ha sido acreditada internacionalmente

Ya se ha dado por finalizado el periodo de pruebas del software pkIRIS

pkIRISGrid

- Infraestructura de clave pública usada en IRISGrid

• pkIRISGrid acreditada en la EUGridPMA

pkIRISGrid, la infraestructura de clave pública usada en IRISGrid (http://www.irisgrid.es/pki/), ha sido acreditada, el 25 de enero, por la EUGridPMA, organización internacional dedicada a la coordinación de la red de confianza entre las PKI que dan servicio a la e-Ciencia europea.

La EUGridPMA (http://www.eugridpma.org/) establece unos requisitos mínimos exigibles a los proveedores de identidad, para temas relacionados con Grid, que permite crear una red común de confianza aplicable a la autenticación de las entidades finales para el acceso inter-organizacional a los recursos distribuidos en el Grid.

La EUGridPMA asegura que los certificados emitidos por las PKI acreditadas cumplen con los requisitos exigidos para el establecimiento de esta red de confianza.

Desde nuestra acreditación por la EUGridPMA, los certificados emitidos por la pkIRISGrid son aceptados por todas las organizaciones afiliadas a la EUGridPMA y a las de otras PMA afiliadas a la IGTF (International Grid Trust Federation).

• pkIRIS - software de PKI

RedIRIS y el CICA han colaborando para la generalización del código usado en la pkIRISGrid y próximamente verá la luz la primera versión del software pkIRIS. Algunas de las mejoras implementadas son:

- Ampliación del esquema LDAP pkIRIS con nuevos atributos para privacidad del correo electrónico, motivos de revocación de certificados, ...
- Extensión de los DTD usados en los ficheros XML para la intereconexión de la CA con los módulos auxiliares
- Modificación en diferentes módulos para compatibilidad con los requisitos de la EUGridPMA
- Mejoras en los sistemas de log y en las interfaces del administrador de la CA

Debido a la simplicidad de uso de la pkIRISGrid tanto para los usuarios como para los administradores de RA y CAS, algunas organizaciones afiliadas a la EUGridPMA, EELA y a RedIRIS han manifestado su interés en probar el software pkIRIS.

• pkIRISGrid - periodo de test

A finales de febrero se ha dado por finalizado el periodo de pruebas del software pkIRIS que comenzó en mayo del pasado año. Actualmente hay 11 autoridades de registro activas y el resultado del piloto ha sido satisfactorio.

Javier Masa
(javier.masa@rediris.es)
Técnico de Middleware

PAPI

- Sistema distribuido para control de acceso desarrollado por RedIRIS

La última versión disponible de PAPI es la 1.4.1, que incluye algunas mejoras y correcciones sobre la 1.4.0, en especial en lo relativo al manejo de conexiones por medio del esquema de proxies. En breve se encontrará disponible la versión 1.5, capaz de funcionar sobre Apache2 y que incorpora un esquema completamente nuevo de configuración, más flexible y fácil de usar.

También se encuentran disponibles versiones de PoAs PAPI para PHP y Tomcat, así como un GPoA capaz de ser ejecutado de manera totalmente independiente. Estos desarrollos simplifican la integración de los mecanismos de autenticación y autorización de PAPI con aplicaciones Web, así como también permiten independizar el uso de PAPI de un servidor o un conjunto de módulos concreto.

Diego López
(diego.lopez@rediris.es)
Coordinador de Middleware

Nuevo grupo de trabajo IRIS-Libre

- Creación de un grupo de trabajo para promover el desarrollo y aplicación de software libre en la comunidad académica

La comunidad académica y de investigación española ha iniciado el grupo de trabajo IRIS-Libre (http://www.rediris.es/gt/iris-libre/), con el objetivo de promover el desarrollo y la aplicación del software libre en esta comunidad.

IRIS-Libre nace como un foro eminentemente tecnológico con tres objetivos fundamentales:

1) Intercambiar experiencias en la aplicación y despliegue del software libre en la comunidad académica y científica.

2) Facilitar la difusión y coordinación de iniciativas relacionadas con el software libre dentro de la comunidad, tanto en el aspecto de desarrollo como en los de formación y cooperación.

3) Ofrecer una plataforma para dar a conocer y apoyar nuevos desarrollos basados en software libre por parte de los investigadores españoles.

La idea central del grupo de trabajo es la colaboración entre instituciones, con el fin de no duplicar trabajo ni esfuerzos y de este modo maximizar el rendimiento. Dentro de este espíritu, el grupo considera esencial la colaboración con iniciativas directamente relacionadas con sus áreas de actividad, como el grupo de interés en software libre auspiciado por la CRUE (CRUETIC-SL)

Diego López
(diego.lopez@rediris.es)
Coordinador de Middleware

Lanzamiento del proyecto OSIRIS

- **Proyecto para la implementación de una plataforma abierta para la integración de servicios en tiempo real**

El proyecto OSIRIS (Open Source Infrastructure for Run-time Integration of Services) se enmarca dentro del programa ITEA (Information Technology for European Advancement). Con una duración estimada de tres años, los participantes tuvieron su primera toma de contacto durante la reunión de lanzamiento celebrada en Sevilla los pasados 30 de noviembre y 1 y 2 de diciembre de 2005.
El objetivo de este proyecto es integrar tecnologías tales como el desarrollo basado en componentes, servidores de aplicaciones, middleware asíncrono, arquitecturas orientadas a servicios (SOA) y Web Services, creando una plataforma que permitirá la integración dinámica de plataformas, servicios y dispositivos para ofrecer servicios de valor añadido. RedIRIS participa liderando la tarea "Servicios básicos y seguridad" y colaborando en el diseño arquitectónico.

La página del proyecto está en:

http://www.itea-osiris.org/

y existe también un folleto informativo en ITEA:

http://www.itea2.org/public/project_leaflets/OSIRIS_profile_oct-05.pdf.

Ajay Daryanani
(ajay.daryanani@rediris.es)
Área de Middleware

Foro de Sistemas de Videoconferencia Avanzada

- **Reunión en Vigo sobre herramientas de colaboración síncronas**

RedIRIS organizó durante los días 23 y 24 de febrero, con la colaboración local de la Universidad de Vigo, un foro temático dedicado a sistemas de videoconferencia avanzada orientado principalmente a teledocencia y a grupos de trabajo distribuido y con el enfoque en la aplicación de la tecnología en el entorno académico y de investigación.

La colaboración síncrona a través de la red posibilita que el trabajo o la docencia se realicen de forma distribuida, evitando desplazamientos y brindando nuevas posibilidades de interacción.

Este foro ofreció a los asistentes la oportunidad de asistir a lo largo de un día y medio tanto a exposiciones teóricas como a demostraciones prácticas de las principales herramientas utilizadas en el entorno académico y científico. Se realizaron exposiciones de las siguientes tecnologías: ConferenceXP, ISABEL, XMPP, H.323, SIP, AccessGrid y VRVS-EVO.

Los datos ofrecidos por los asistentes al foro –que en su mayoría fueron responsables de los servicios multimedia de gran número de universidades y centros de investigación– consideraron como tecnología más interesante el AccessGrid seguida por ISABEL; los encuestados valoraron muy positivamente la reunión y expresaron su interés en la celebración de un foro de este tipo anualmente.

Durante la sesión final se trataron cuestiones que junto con las encuestas recogidas nos permiten obtener las siguientes conclusiones:

- La utilización de estos servicios ha de verse justificada en función de su utilidad, aunque hay que mostrar las posibilidades que ofrecen para que surja la demanda.

Lanzamiento del proyecto OSIRIS para la implementación de una plataforma abierta para la integración de servicios en tiempo real

Los asistentes al foro de videoconferencia avanzada consideraron el AccessGrid como la tecnología más interesante

Por las opiniones recogidas parece que en la actualidad no existe "la herramienta definitiva única"

Existe un porcentaje importante de usuarios que sigue utilizando la multiconferencia telefónica

- El modelo de utilización de salas resulta más simple que un modelo orientado a desktop que implica resolver multitud de problemas y exige la implantación de Centros de Atención a Usuarios (CAU).
- En caso de utilizar soluciones software, el coste marginal que supone añadir nuevos sistemas es poco importante en comparación con el coste del despliegue audiovisual de la sala.
- Es un requisito esencial para el despliegue de estos servicios incluir personal especializado que las atienda.
- Todos los cambios de configuración en el funcionamiento de las salas han de producirse sin que sea necesario cambiar el cableado.
- En la actualidad no existe "la herramienta definitiva única".
- En algunas instituciones (generalmente pequeñas) hay problemas de ancho de banda y esto es un *handicap* importante para la utilización de estas tecnologías.
- Existe la necesidad real de enlazar con teléfonos en el caso de reuniones de trabajo.
- Es interesante, para permitir cierta flexibilidad, la ubicación de los elementos audiovisuales y de comunicación en un rack como el que se utilizó en este foro perteneciente al CESGA para dar soporte a salas no equipadas.
- Se recomienda la realización de manuales. En RedIRIS tenemos información disponible al respecto en: http://www.rediris.es/mmedia/salas/salas.pdf.
- Durante la reunión se mencionó la posibilidad de aglutinar los contenidos digitales de las instituciones bajo un paraguas común (UVIGO.tv, UC3M-TV, URJC-TV, TELEUNED, UPV-RTV, etc.) y aunque esta posibilidad no era objeto del foro, que estaba orientado a comunicación síncrona, se tuvo en cuenta la posibilidad de que pudiera ser tratado en futuras reuniones.
- Entre los participantes en el foro se constató que existe un porcentaje importante de usuarios que sigue utilizando la multiconferencia telefónica y más alto aún a nivel directivo. Alrededor de un 40% está satisfecho con sus sistemas actuales, aunque una gran mayoría está dispuesta a evolucionar, mejorar o adquirir nuevos servicios de multiconferencia. La utilización principal de esta herramienta son las reuniones de trabajo, mientras que la utilización en docencia tanto de grado como postgrado es minoritaria.

  De entre los asistentes al foro menos del 60% de las instituciones disponía de personal dedicado a servicios de videoconferencia, un 45% no realiza grabación de las sesiones y es una característica muy importante para el 68%, siendo las sesiones grabadas accedidas mediante streaming (en directo o VoD) principalmente en abierto y de forma gratuita.

  El sistema más utilizado es H.323, seguido por videoconferencia RDSI (H.320) y una minoría utiliza SIP. Y la característica más extendida es la utilización de estándares, seguida por la interoperabilidad con otros fabricantes y la capacidad multiuso, la multiconferencia y la facilidad de uso.

  Existe más información al respecto en:

  http://www.rediris.es/mmedia/reuniones/hcs06/

José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia