Proyectos de Red

• MUPBED

En este proyecto (http://www.ist-mupbed.org) se han creado 5 testbeds a nivel europeo, uno de ellos en Telefónica I+D. De su conexión se ha encargado RedIRIS, así como del establecimiento el próximo septiembre de conexiones de nivel 2 con el resto de testbeds sobre GÉANT. Con estos testbeds, se va a integrar y validar las tecnologías ASON/GMPLS (Automatically Switched Optical Network/ Generalised Multi Protocol Label Switching).

De esta forma, en el proyecto se trabaja también en la integración de aplicaciones avanzadas con la red, mediante un plano de control, que en este caso puede ser UNI1.0 ó UNI2.0, aunque se están evaluando las diferentes tecnologías y el acceso directo de las aplicaciones a la configuración de dispositivos de red.

• Tecnología VPLS

Siguiendo con la línea de trabajo iniciada hace unos meses, y tras la puesta en producción del servicio de VPNs de nivel 2 punto a punto, RedIRIS, en colaboración con el personal del área de red del CESGA ha realizado las primeras pruebas europeas en entorno entre proveedor sobre tecnología VPLS (Virtual Private Network). Esta tecnología, permite proporcionar conexiones de nivel 2 multipunto y aunque por el momento no está soportada por GÉANT y no se encuentra en producción en RedIRIS, estas pruebas han sido presentadas en diversos foros de discusión y congresos y se han hecho varias publicaciones al respecto.

Una descripción completa de las pruebas realizadas puede encontrarse en la ponencia presentada en la pasada reunión anual de Terena que tuvo lugar en Poznan: (http://www.terena.nl/conferences/tnc2005/programme/presentations/show.php?pres_id=54).

Estas pruebas han despertado el interés de otras redes académicas de investigación, que están comenzando a trabajar en esta tecnología.

Miguel Ángel Sotos
(miguel.sotos@rediris.es
Laura Serrano
(laura.serrano@rediris.es)
Área de Red

• ALICE: Proyecto América Latina Interconectada Con Europa

RedCLARA (www.redclara.net) continúa creciendo y conectando a nuevas redes nacionales de investigación latinoamericanas. En junio 2005, las redes conectadas eran las de Argentina, Brasil, Chile, Méjico, Perú, Venezuela y Panamá y en breve se conectarán las de Uruguay y Guatemala para continuar con las de Costa Rica, El Salvador y Nicaragua.

Recordamos que el anillo principal de RedCLARA está formado por enlaces STM-1 (155 Mbps) entre Buenos Aires (Argentina), Santiago de Chile (Chile), Panamá, Tijuana (Méjico), Sao Paulo (Brasil) y Buenos Aires. En estos puntos se ubica un nodo de RedCLARA al cual se conecta bien la NREN del propio país o la de otro que no tenga nodo de RedCLARA, como por ejemplo, es el caso de Uruguay conectado a Buenos Aires.

El grupo técnico de RedCLARA se reunió los pasados 25 a 27 de abril en Veracruz (Méjico) y desafortunadamente en esta ocasión RedIRIS no pudo participar. Durante el evento, los propios técnicos de estos países dieron tutoriales y descripciones técnicas, destacando el impartido sobre IPv6 por nuestros colegas portugueses.

Durante esta reunión se elaboró la propuesta del Reglamento de la Comisión Técnica de CLARA para su aprobación por parte de su Consejo Directivo y surgió la iniciativa de crear una serie de grupos de trabajo por cada una de las tecnologías que se desea configurar y soportar en RedCLARA.

Las pruebas realizadas por RedIRIS en tecnología VPLS han despertado el interés en otras redes académicas

RedCLARA continúa creciendo y conectando a nuevas redes nacionales latinoamericanas

Incremento de velocidad en el enlace Argelia-Madrid de la red con los países del norte de África

El pasado junio tuvo lugar en Luxemburgo la presentación oficial de la nueva red académica

En el cuadro que aparece a continuación vemos los grupos de trabajo creados y los líderes de cada uno de ellos.

Grupo de Trabajo	Nombre del Lider	Red
Medidas Rendimiento	Hans-Ludwig Reyess	(CLARA-NOC)
Routing	Eriko Porto	(CLARA-NEG)
Seguridad	Juan Carlos Guel	(CUDI)
VoIP	Iván Morales	(RAGIE)
Video Conferencia	Alexander Valerín	(CR2NET)
IPv6	Azael Fernández	(UNAM/CUDI)
Multicast	Guillermo Cicileo	(RETINA)

Los pasados 28 y 29 de julio tuvo lugar en Antigua (Guatemala) la 4ª reunión del proyecto ALICE, a la que acudieron los representantes de 16 redes académicas y de investigación latinoamericanas, de dos de las cuatro redes europeas que participan en el proyecto (la portuguesa FCCN y RedIRIS) y de DANTE, la asociación formada por varias redes académicas europeas (incluyendo a RedIRIS) que se hace cargo de la gestión del proyecto.

En la última reunión del proyecto se trataron, entre otros temas, el de la inminente conexión a RedCLARA de las redes académicas y de investigación de Nicaragua, El Salvador, Guatemala, Costa Rica y Uruguay, que se sumarán a las redes, ya conectadas, de Brasil, Argentina, Chile, Panamá, México y Venezuela, lo que pone de manifiesto la buena marcha del proyecto.

RedIRIS presta un apoyo decidido al proyecto ALICE y a RedCLARA, y en la reunión de ALICE que tuvo lugar en Guatemala se comprometió a participar en la próxima reunión técnica de RedCLARA, y a acoger en las próximas Jornadas Técnicas de RedIRIS a los responsables de los grupos técnicos.

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red
Alberto Pérez
(alberto.perez@red.es)
Subdirector

• EUMEDCONNECT: Proyecto de interconexión entre el área Sur del Mediterráneo y GÉANT

En cuanto a la red con los países del norte de África (www.eumedconnect.net) debemos destacar el incremento de velocidad llevado a cabo en el enlace entre Argelia y Madrid, pasando de 45 a 155 Mbps. El enlace de 34 Mbps de Egipto con el Punto de Presencia (PdP) de EUMEDCONNECT en Catania está ya operativo. El enlace de 8 Mbps de Siria con el PdP de EUMEDCONNECT en Chipre va con retrasos y el de 45 Mbps de Jordania se está implementando.

Los socios de este proyecto estamos trabajando en el próximo entrenamiento que los socios europeos darán a los técnicos de las NRENs de estos países del norte de África. Tras expresar sus intereses, el entrenamiento será muy práctico y estará enfocado en multicast: análisis del despliegue y configuración y solución de problemas. Las fechas que se barajan son el próximo mes de noviembre. La parte de IPv6 quedará cubierta con otro entrenamiento ofrecido bajo el proyecto 6DISS (www.6diss.org) del que RedIRIS no forma parte.

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

GÉANT2

• Nueva red pan-europea de redes nacionales académicas y de investigación

Los días 14 y 15 de junio tuvo lugar en Luxemburgo la presentación oficial de la nueva red académica y de investigación paneuropea, GÉANT2 (www.geant2.net). El acto organizado por la asociación de redes académicas DANTE (de la que es accionista RedIRIS) contó con la presencia de más de 200 personas, entre las que se encontraban responsables de las principales redes académicas y de investigación a nivel mundial y de varios destacados centros de investigación europeos, así como representantes políticos nacionales y comunitarios, destacando la presencia de Viviane Reding, la Comisaria responsable de Sociedad de la Información y Medios de Comunicación (http://www.geant2.net/server/show/ conWebDoc.1267).

GÉANT2 interconecta las redes académicas y de investigación europeas entre sí, permitiendo que más de 3.000 centros académicos y de investigación europeos dispongan de una red de comunicaciones avanzada y de alta capacidad para comunicarse entre sí, lo que, en particular, resulta imprescindible para

determinados experimentos europeos que requieren transferencias masivas de datos. GÉANT2 permite además a esos centros acceder a otras redes académicas y de investigación internacionales, como las americanas Abilene y ESNET, la canadiense Canarie, la latinoamericana RedCLARA, etc.

La red GÉANT2 es financiada al 50% por la Comisión Europea y por un consorcio formado por las redes académicas y de investigación de 30 estados europeos (entre las que se encuentra RedIRIS). DANTE, asociación formada por algunas de esas redes académicas, se hace cargo de su gestión en nombre de ese consorcio.

En general, GÉANT2 (http://www.geant2.net/) presenta una arquitectura mixta donde se combina la conmutación de paquetes con la de circuitos. Esta combinación de tecnologías dotan a la red de una gran flexibilidad a la hora de satisfacer necesidades específicas de investigadores, a los cuales se desea proporcionar el mejor de los servicios.

La nueva red ofrecerá velocidades hasta 4 veces superior a las que se ofrecen ahora a través de su predecesora GÉANT. GÉANT2 tendrá la topología que se muestra en la siguiente figura, donde el punto de presencia (PdP) en España se conecta con el resto a través de tres rutas físicamente diversificadas: por el Este de la península, el PdP de España se une con el de Ginebra con fibra oscura; por el Norte hacia París, se cuenta con dos enlaces de 10Gbps cada uno y por el Este con Milán. La conexión de fibra oscura de España con esta red, significa que las instituciones conectadas a RedIRIS tendrán acceso a la red de conmutación de circuitos que soportará los enlaces extremo a extremo (configurados a nivel 1 ó 2) también conocidos como lighpaths. La capacidad, prácticamente, no está limitada, ya que la infraestructura física pertenece al consorcio de redes europeas y sobre esta infraestructura se pueden configurar nuevos enlaces de 10 Gbps.

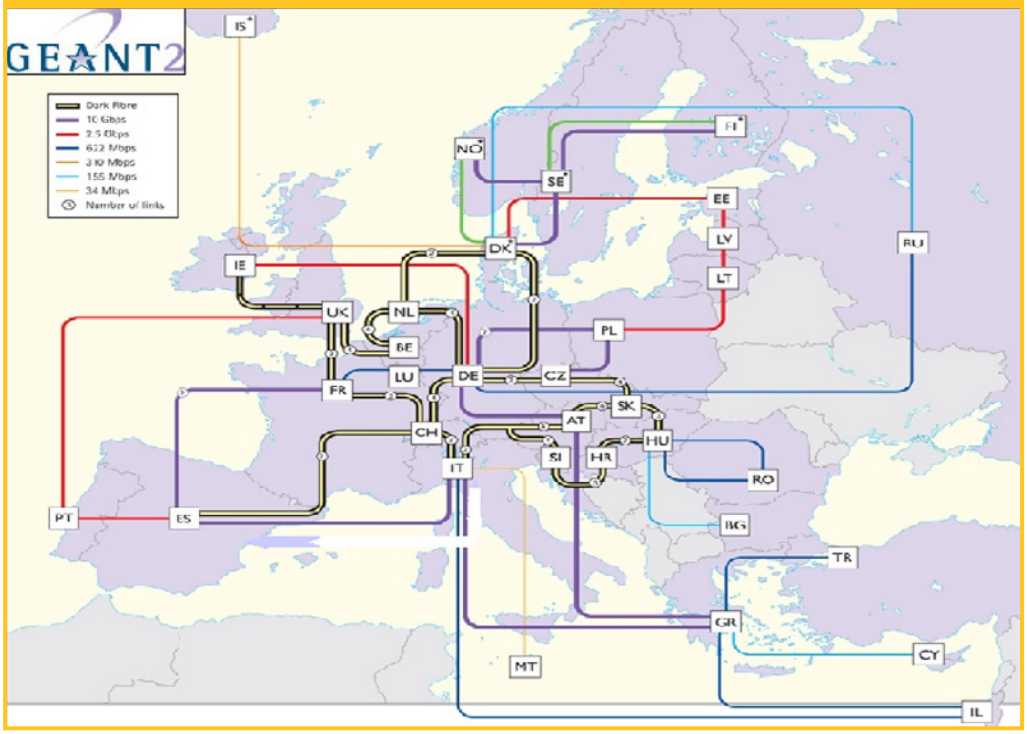
Aunque en la actualidad la conectividad del punto de presencia español a la red de fibra oscura europea no es total, ya que de momento sólo tenemos una ruta provista con fibra oscura –está en preparación un nuevo concurso para sustituir los enlaces alquilados con París por fibra oscura–, este es un paso muy importante para España al tratarse de un país de gran extensión situado en un extremo de Europa, donde la disponibilidad de fibra oscura por parte de los operadores para ser alquilada es limitada. La situación en cambio en el centro de Europa es la opuesta ya que la fibra oscura está disponible para alquilar a precios asequibles.

La planificación realizada estima que el PdP de GÉANT2 en España estará operativo en noviembre de este año, los trabajos ya han comenzado. Realmente no se trata de una

GÉANT2 presenta una arquitectura mixta donde se combina la conmutación de paquetes con la de circuitos

La nueva red ofrecerá velocidades hasta 4 veces superior a las que se ofrecen ahora

TOPOLOGÍA DE GÉANT2 (www.geant2.net/server/show/nav.941)

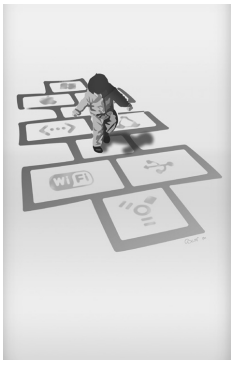


migración sino más bien de una complementación y mejora de la red actual, ya que a la red IP de conmutación de paquetes existente se la van a añadir enlaces de fibra oscura.

Además de routers IP, el equipamiento de GÉANT2 incluirá equipos ópticos y *switches cross connect*. El pasado 14 de junio se hizo público el fabricante ganador del concurso de este tipo de equipos que será Alcatel.

• Iniciativa de fibras transfronterizas o Cross Border Fibers

Nueva estrategia de conexión transfronteriza a través de redes de fibra oscura propia de algunas redes académicas



Como ya hemos comentado, la disponibilidad de fibra oscura en los países del Centro y Este de Europa es muy significativa. Es más, algunos de nuestros colegas del Este de Europa han optado por desplegar su propia red de fibra oscura allí donde no hay infraestructura para ser alquilada o los precios son demasiado elevados.

La iniciativa de conexión transfronterizas significa que estas NRENs pueden conectarse con sus propias infraestructuras sin utilizar las de GÉANT2

Esta estrategia seguida ha llevado a que redes nacionales académicas y de investigación de países colindantes posean fibras hasta sus respectivas fronteras o incluso hasta ciudades del país vecino, lo que significa que estas NRENs pueden conectarse utilizando sus propias infraestructuras sin utilizar la de GÉANT2.

Hay que enfatizar el hecho de que no se busca sustituir la red GÉANT2 sino optimizar recursos. En este sentido, si estos dos países se conectaran a nivel físico y proporcionaran los circuitos necesarios a GÉANT2 para ser construida, no sería necesario pagar el alquiler a un operador ni de capacidad ni de fibra oscura. Pero la tan buscada flexibilidad para tener lighpaths y ofrecer servicios extremo a extremo a los investigadores se mantendría, ya que la infraestructura física pertenece a las NRENs.

Esta nueva filosofía requiere de un profundo análisis de todas sus implicaciones tanto políticas como económicas, técnicas y de gestión. Con el propósito de iniciar este trabajo se ha creado un grupo de discusión entre las NRENs interesadas del que RedIRIS forma parte ya que tiene dos países europeos fronterizos con los que ya se han iniciado las conversaciones para analizar la viabilidad de una futura interconexión directa. Quizá a largo plazo, RedIRIS podría sacar ventaja de su proximidad con ciertos países de la Ribera Sur del Mediterráneo.

• Actividad JRA3

Actividad perteneciente al proyecto GÉANT2 para el desarrollo de un servicio de banda garantizado bajo demanda

Respecto a la actividad JRA3 (http://www.geant2.net/server/show/nav.00d00a003) cuyo objetivo es el desarrollo de un servicio de ancho de banda garantizado bajo demanda, RedIRIS constituye una de las redes académicas nacionales con la responsabilidad de diseñar la arquitectura del mismo, fase en la que actualmente se está trabajando.

Las reuniones recientes se han concentrado en la definición de los módulos que van a constituir el sistema, la interacción entre los mismos y la especificación de sus funcionalidades. En este sentido hay que destacar la problemática subyacente a este propósito principalmente derivada del proceso de automatización y del hecho de que sea un servicio punto a punto entre dominios.

Estas circunstancias plantean dificultades que deben ser tenidas en consideración, dificultades referentes al plano de control, de sincronización, de ámbito político, de priorización, referentes a mecanismos de backup, monitorización... que son vitales a la hora de diseñar una arquitectura completa en la que el servicio en sí mismo quede perfectamente definido.

Muchos de estos puntos siguen en estos momentos siendo objeto de discusión y cuestiones tales como disponer de rutas alternativas para proporcionar el servicio y poder así ofrecer backup; garantizar algún otro parámetro como el retardo o permitir algún tipo de reserva anticipada (preemtion) son algunas de las cuestiones que, aunque no se implementarán en una primera fase (manual y dentro del dominio), se han tenido en cuenta para próximas fases del proyecto.

Se trabaja para concluir la definición de la arquitectura de los sistemas de autenticación y autorización

• Actividad JRA5

Actividad que trabaja en la definición de la arquitectura de los sistemas de autenticación y autorización

Los trabajos de la actividad JRA5 (Roaming and Authorization) de la nueva red paneuropea GÉANT2 continúan de acuerdo con los planes previstos. En estos momentos el grupo trabaja en terminar la definición de la arquitectura de los sistemas de autenticación y autorización.

Esta arquitectura está basada en Web Services y orientada a la integración de infraestructuras ya existentes tales como PAPI o A-Select. El uso de Web Services garantiza la evolución futura de la infraestructura y su extensibilidad, al mismo tiempo que simplifica su integración con las aplicaciones usuarias potenciales, desde mecanismos de gestión de ancho de banda hasta las infraestructuras Grid.

Respecto a las diferentes actividades de GÉANT2 hay que destacar los contactos que se han establecido entre ellas con objeto de coordinar sus actuaciones. De esta manera, por ejemplo, los requisitos del grupo SA3 en cuanto a autenticación y autorización de usuarios han sido incorporados en la definición de arquitectura de la actividad JRA5.

• Actividad SA3

Creación de un servicio de conexión extremo a extremo de tráfico IP de máxima prioridad

En esta actividad (SA3: http://www.geant2.net/server/show/nav.00d00a006) se va a crear el servicio *Premium IP extremo a extremo* dentro de GÉANT y en las redes nacionales conectadas a ella, mediante el cual, sus usuarios podrán solicitar una conexión extremo a extremo de tráfico Premium IP (tráfico IP de máxima prioridad).

Otro de los objetivos de esta actividad es crear un PERT (Performance Response Team), un equipo similar a un NOC o un CERT encargado de resolver los problemas relacionados con el rendimiento de las aplicaciones. En una primera fase se creó un PERT en pre-producción en el que cada semana cada red académica nacional ponía a disposición de este equipo a un responsable, encargado de trabajar unas dos horas diarias y resolver los casos iniciales.

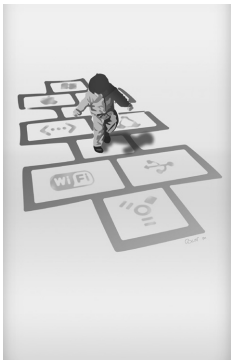
En esta primera fase se solucionaron varios casos, y se empezó a crear el sistema de tickets para gestionar incidencias. También se creó una base de datos de conocimientos donde se guarda información útil relativa a cualquier aspecto que pueda influir en el rendimiento de una aplicación. Hay que tener en cuenta que si el rendimiento es bajo, la causa puede estar provocada por múltiples factores: la red, la aplicación, sistemas operativos, red local, mala configuración de alguno de los elementos anteriores... Una vez finalizada esa fase con el sistema de tickets acabado, estamos ahora en una etapa de puesta en producción del PERT, con un encargado a tiempo completo cada semana.

Para que el PERT tenga éxito en la resolución de casos, es necesario que la recopilación de información para resolver el problema sea lo más extensa posible, así como poder contactar con expertos en diferentes materias (Sistemas Operativos, configuración de aplicaciones de red, etc...) que puedan ayudar en la resolución de los problemas.

Alberto Pérez
(alberto.perez@red.es)
Subdirector

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red
Miguel Ángel Sotos
(miguel.sotos@rediris.es
Laura Serrano
(laura.serrano@rediris.es)
Área de Red

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones



Creación de un equipo para resolver los problemas relacionados con el rendimiento de las aplicaciones

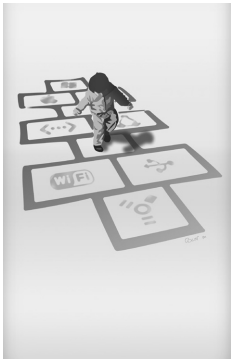
TNC 2005

• Reunión anual de la Asociación trans-europea de redes académicas y de investigación (TERENA) en Poznan

Reunión anual de TERENA el pasado junio en Poznan

A principios del pasado junio se celebró en Poznan (Polonia) la Conferencia Anual de TERENA 2005 (http://www.terena.nl/conferences/tnc2005/). Dentro de la misma podemos destacar:

- El que el elemento principal de la discusión del TAC (Technical Advisory Committee, encargado de definir las actividades técnicas de la asociación) se centrara en las actividades dirigidas a las tecnologías con las que establecer redes de confianza



En la reunión anual de TERENA se contó con dos presentaciones por parte de RedIRIS

Nuevas iniciativas de seguridad en marcha

dentro del espacio académico y de investigación europeo, actividad coordinada por RedIRIS.

- Dos presentaciones realizada por personal integrante del equipo de RedIRIS: Laura Serrano (http://www.terena.nl/conferences/tnc2005/programme/people/show.php?person_id=892) y Diego López (http://www.terena.nl/conferences/tnc2005/programme/people/show.php?person_id=890).

- Una presentación realizada por un miembro de la comunidad RedIRIS, Victoriano Giralt, de la Universidad de Málaga (http://www.terena.nl/conferences/tnc2005/programme/people/show.php?person_id=923).

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red
Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Nuevas iniciativas lanzadas desde el servicio de seguridad de RedIRIS

• Iniciativas relacionadas con la detección de intrusiones y su análisis

En los últimos Grupos de Trabajo celebrados en Málaga el pasado mes de mayo, se presentaron diversas iniciativas que poco a poco y previsiblemente antes de la finalización del presente año, se van a ir lanzando en nuestra comunidad, siempre contando con la inestimable colaboración y coordinación de diversos miembros de la misma.

A continuación vamos a describir brevemente estas iniciativas y su estado actual de desarrollo.

- **ACRI (A**lmacén **C**olaborativo de **R**eglas de **I**ntrusión**)**. El Repositorio ordenado de reglas para distintos IDSs (Intrusion Detection Systems) adaptadas a la comunidad académica y de investigación española, está en la actualidad disponible para los miembros de nuestra comunidad.

  De momento se contemplan tan sólo los ficheros de reglas correspondientes al snort (lhttp://www.snort.org/), al ser uno de los IDSs más ampliamente utilizado en nuestra comunidad, pero no obstante el repositorio está abierto a incorporaciones para otros IDSs.

  Toda la información acerca de la iniciativa y de cómo participar en ella está disponible en su página Web: (http://www.rediris.es/cert/proyectos/acri.es.html).

- **ANAMARIS (AN**álisis de **A**ctividad **MA**liciosa y **R**espuesta a **I**ncidente**S)**. Esta iniciativa, disponible en breve, pretende establecer un foro técnico especializado, integrado por técnicos en seguridad informática de la comunidad RedIRIS, con el objetivo de fomentar el análisis de la actividad maliciosa y dar respuesta a incidentes de forma coordinada en dicha comunidad.

  La idea es que a partir de dicho foro se fomente el intercambio de este tipo de información entre las instituciones participantes, para posteriormente, desplegar una serie de proyectos relacionados a medio/largo plazo (sondas de monitorización de espacio IP oscuro, investigación y uso de herramientas para la correlación de alertas, etc...).

  Más información disponible en nuestras páginas Web (http://www.rediris.es/cert/proyectos/ anamaris.es.html).

- **EnREDA (E**ntorno de **R**ecogida de **E**videncias **D**igitales y **A**nálisis**)**. La idea que se esconde detrás de esta iniciativa es la de disponer de una herramienta automatizada que facilite el análisis forense de máquinas comprometidas en nuestra comunidad, con el fin de aprender de los métodos y herramientas utilizados por los intrusos y que permita al mismo tiempo realizar una respuesta ante incidentes más efectiva.

  Las primeras versiones de EnREDA y los diferentes recursos asociados a esta iniciativa, estarán disponibles antes de finales de año.

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

Grupo de Trabajo sobre RTIR

• Herramienta utilizada en la actualidad por IRIS-CERT para gestión de incidentes

Como ya comentamos en la actualidad del pasado boletín (http://www.rediris.es/rediris/boletin/72/actualidad.pdf), estábamos perfilando los detalles del contrato que se suscribirá con *Best Practical* a través de TERENA, para la mejora y ampliación de funcionalidades de la herramienta de gestión de incidentes que en la actualidad estamos usando en el equipo de seguridad de RedIRIS, RTIR (Request Tracker for Incident Response, http://www.bestpractical.com/rtir/). Tras diversas discusiones en la lista, se ha llegado a un acuerdo entre ambas partes en cuanto a los términos de dicho contrato.

TERENA tras recibir los pagos correspondientes por parte de los equipos involucrados, firmará bilateralmente el contrato con *Best Practical*, que comenzará los trabajos al mes siguiente de su firma. Cada uno de los integrantes del grupo designará un representante que realizará el seguimiento de los desarrollos y módulos entregados por *Best Practical* con el fin de asegurar que el producto final cumple todos los requerimientos acordados.

Una vez finalizado el proyecto, con una duración estimada de un año y medio el producto resultante será de dominio público.

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

XV Reunión TERENA TF-CSIRT

• Para la colaboración entre los equipos de respuesta de incidentes de seguridad europeos y países limítrofes

La XV Reunión del Grupo de Trabajo de TERENA para promover la colaboración de los CERTs europeos y de países limítrofes, TF-CSIRT (http://www.terena.nl/task-forces/tf-csirt/) se celebró esta vez en Zurich (Suiza) el pasado mes de mayo.

La Jornada previa a la reunión del grupo de trabajo propiamente dicha resultó bastante interesante; cabe destacar la presentación realizada por Andrew *Cormack (JANET),* así como la forma en la que diferentes países están afrontando el reto de la protección de la infraestructura crítica nacional. Todas las presentaciones estás disponibles en: http://www.terena.nl/tech/task-forces/tf-csirt/meeting15/programme.html.

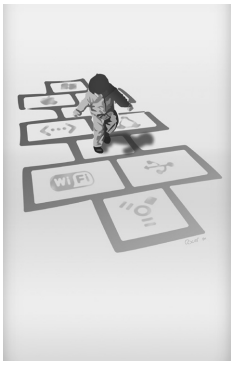
En cuanto a la reunión del grupo de trabajo celebrada al día siguiente, se tocaron uno a uno los diferentes frentes en los que los miembros del grupo están inmersos. De todas estas iniciativas podemos destacar la finalización del patrocinio europeo en el contexto del proyecto TRANSITS (Training of Network Security Incident Teams Staff) y la transferencia de todo el material generado al FIRST (Forum of Incident Response and Security Teasm) que está haciendo uso de este material para impartir cursos fundamentalmente en latinoamérica, aunque se ha llegado a un compromiso para la impartición de un par de cursos en Europa cuyas fechas todavía no han sido fijadas.

El Grupo de Trabajo también está decidido a colaborar de forma muy activa en la promoción de equipos CERT en Europa, realizando una función de concienciación y de diseminación de información sobre las actividades que los CERTs europeos están llevando a cabo con la recientemente creada Agencia Europea ENISA (European Network and Information Security Agency, http://www.enisa.eu.int/). Uno de cuyos miembros forma parte del Permanent Stakeholders' Group, que actúa como grupo asesor para la ENISA.

Se presentó en Zurich el *ENISA Work Plan 2005* y el borrador del año 2006, en el que se incluye la promoción de CERTs gubernamentales en aquellos países miembros que no dispongan de ellos, para posteriormente expandir la creación de dichos equipos a otros sectores.

Para finalizar es importante mencionar que RIPE ha incluido algunas modificaciones en el objeto IRT (http://www.ripe.net/ripe/docs/irt-object.html) y ha incorporado un nuevo atributo en las clases PERSON, ROLE, IRT, MNTER, ORGANIZATION, INETNUM Y INETNUM6 denominado abuse-mailbox, cuya función es especificar la dirección de correo electrónico a la que se deben redirigir los incidentes de abuse.

Para más información sobre lo discutido en la reunión de Zurich se puede consultar el acta que está disponible en:



Es muy importante ver cómo los distintos países europeso están protegiendo la infraestructura crítica nacional

Finalización del patrocinio europeo en el contexto del proyecto TRANSITS

http://www.terena.nl/ tech/task-forces/tf-csirt/meeting15/ TSec_05_043.pdf.

La próxima reunión del Grupo de Trabajo se celebrará en Lisboa (Portugal) el próximo mes de septiembre y estará organizada por el Equipo de Atención de Incidentes de la Red Académica Portuguesa, CERT.PT.

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

La pkIRIS Grid está formada por una autoridad de certificación situada en RedIRIS y varias de registro gestionadas por participantes en la iniciativa

II Edición del reto de análisis forense

pkIRISGrid

• Una infraestructura de clave pública para IRISGrid

pkIRISGrid (http://www.irisgrid.es/pki) es la infraestructura de clave pública usada en la iniciativa nacional de Grid IRISGrid (http://www.irisgrid.es). Está formada por una autoridad de certificación (CA) situada en RedIRIS y varias autoridades de registro (RA) gestionadas por los grupos de investigación participantes en esta iniciativa de Grid.

En el desarrollo de la PKI se han tenido en cuenta tres importantes objetivos:

- Cumplir los requisitos exigidos por la EUGridPMA para que se acredite a la CA de la pkIRISGrid como compatible con el resto de CAs de las PKIs de EUGridPMA (The European Policy Management Authority for Grid Authentication in e-Science: http://www.eugridpma.org)
- Simplificar las diferentes tareas existentes en el uso y gestión de una PKI
  - El usuario solicita y recoge su certificado desde su navegador.
  - El administrador de la autoridad de registro sólo ha de verificar los datos que el usuario ha introducido y validarlos para que de forma automática el sistema se encargue de hacer llegar a la autoridad de certificación, de forma segura, todas las peticiones de certificados.
- Uso de tecnologías desarrolladas en RedIRIS y otras basadas en estándares abiertos como por ejemplo:
  - OpenSSL para la gestión de certificados, solicitudes, revocaciones,...
  - LDAP, con el esquema pkirisgrid, como base para el almacenamiento de las RAs, entidades (usuarios, servicios/servidores), solicitudes de certificado y de revocación, certificados, listas de revocación,...
  - COPA (Codificación Optimizada Para el Acceso jerárquico a la información: http://www.rediris.es/ldap/copa/) para identificar un elemento dentro del directorio (ya sea entidad, autoridad de registro o certificado).
  - URNs para el almacenamiento de histórico de estados.
  - XML para el intercambio seguro de información desde las RAs a la CA.
  - LDIF para el intercambio de información desde la CA a las RAs.
  - PAPI como control de acceso a la zona privada de los administradores de las RAs.
  - PHP para la aplicación de las RAs.
  - Perl para la aplicación de la CA

Desde el mes de mayo la PKI se está usando en fase de pruebas con varias autoridades de registro.

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

II Edición del Reto de análisis forense

• II edición del concurso de análisis forense digital en castellano

En mayo de este año se entregaron oficialmente los premios de la segunda edición del Reto de Análisis Forense en castellano dentro de los actos del Congreso de Seguridad en Cómputo (http://congreso.cert.unam.mx), organizado por la Universidad Nacional Autónoma de México (UNAM).

En esta ocasión el concurso fue organizado por la Universidad Autónoma Nacional de Méjico y RedIRIS de forma conjunta, se contó con la colaboración de expertos informáticos de

diversos países como jurados para evaluar los trabajos presentados.

El interés que despierta este tipo de Retos es cada vez mayor, en esta edición los resultados de la inscripción fue de casi 1.000 participantes de todo el mundo.

El objetivo de estos concursos de análisis forense es fomentar el conocimiento de las técnicas de análisis forense digital existentes entre los administradores y técnicos de seguridad, de forma que puedan conocer los fundamentos necesarios para analizar los sistemas informáticos ante una intrusión en un momento dado.

El primer premio, una licencia del software Encase, fue para el equipo formado por José Ignacio Parra, Quique Martínez y Víctor Barahona.

El segundo premio, consistió en la asistencia a un curso dentro de las líneas de especialización en Seguridad de la Universidad Autónoma de México que fue obtenido por Juan Martín Galeote, y el tercer premio, un curso en línea de SANS que lo obtuvo Juan Antonio Fernández Gómez.

Hay que resaltar la gran participación llevada a cabo este año por los miembros de la comunidad académica española, Víctor Barahona perteneciente a la Universidad Autónoma de Madrid forma parte del equipo ganador y Juan Martín Galeote que consiguió el segundo premio, pertenece a la Universidad de Granada.

Los documentos presentados al concurso así como los participantes e imágenes del equipo atacado que se pueden emplear para realizar el análisis están disponibles en: http://www.seguridad.unam.mx/eventos/reto/.

Se pretende volver a preparar este año un tercer reto donde se vuelvan a poner a prueba las habilidades de los participantes para evaluar un compromiso informático.

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

Reunión anual del FIRST

• Foro Internacional de Equipos de Respuesta a Incidentes de Seguridad

FIRST (Foro de Equipos de Respuesta a incidentes de Seguridad, http://www.first.org) concentra a más de 170 equipos de seguridad de todo el mundo. El grupo de seguridad de RedIRIS, IRIS-CERT es miembro de esta organización desde 1977.

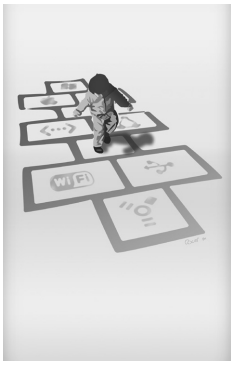
Todos los años FIRST organiza un congreso de seguridad global, cuyas ponencias pueden ser consultadas "online" transcurrido un tiempo de la realización del mismo y a lo largo del año se van organizando diversas reuniones técnicas cuya participación está restringida a los miembros de los grupos de seguridad integrantes en FIRST.

La conferencia de este año fue en Singapur y estuvo organizada en dos grupos paralelos, uno dedicado a aspectos organizativos de los grupos de seguridad y otro a cuestiones técnicas relacionadas con los incidentes.

A nivel organizativo cabe destacar las presentaciones donde se daban las pautas de organización de las distintas funciones de un CSIRT (Computer Security Incident and Response Team), tales como las herramientas para la creación de avisos de seguridad, la organización de un CSIRT a nivel gubernamental para la coordinación a nivel nacional de los incidentes de seguridad o las distintas métricas a la hora de evaluar la peligrosidad de una determinada vulnerabilidad.

En los aspectos técnicos se resaltaron las presentaciones orientadas a la monitorización de la red y a la detección de *bots* en ellas, al análisis de los programas desconocidos que se suelen encontrar en las intrusiones y a sesiones prácticas de configuración y detección de problemas de seguridad en una red.

A nivel de la organización de los grupos de seguridad, hay diversas iniciativas a la hora de fomentar la coordinación de estos grupos de manera similar a como se realiza en el TF-CSIRT europeo. Por una parte se encuentra la iniciativa de los países del Asia y Oceanía (ACEAN CERT) y por otra la de CLARA, que agrupa a las redes nacionales de I+D Latinoamericanas y está fomentando la creación de grupos de seguridad en cada una de las redes integradas.



En el II Reto de ánalisis forense con más de mil inscritos de todo el mundo el ganador fue un equipo español de la comunidad académica

IRIS-CERT es miembro de FIRST desde 1977

Extraordinario impulso de la iniciativa de movilidad eduroam

Ya está disponible el nuevo portal a los servicios de la Web of Knowledge

FIRST ha llegado a un acuerdo con TERENA para impartir de manera coordinada los cursos "TRANSIT" de formación de nuevos grupos de seguridad. La idea de estos cursos es ayudar al establecimiento de nuevos CSIRTs, proporcionando información necesaria para su creación así como los recursos necesarios,...

Coincidiendo con la reunión técnica de FIRST en Argentina, en Octubre está prevista la reutilización de un Curso TRANSIT para fomentar la creación de grupos de seguridad en Latinoamérica.

Hay que indicar que el próximo año 2006 la conferencia FIRST se realizará en Baltimore, se puede encontrar más información sobre esta conferencia y los plazos para la presentación de ponencias en las páginas web del FIRST.

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

Reuniones TF-EMC2 y TF-Mobility

• Grupos de trabajo sobre middleware y movilidad

Coincidiendo con la conferencia anual de TERENA en Poznan tuvieron lugar sendas reuniones de los grupos de trabajo TF-EMC2 (European Middleware Coordination and Collaboration, liderado por RedIRIS) y TF-Mobility.

Dentro de las actividades de TF-EMC2 (http://www.terena.nl/tech/task-forces/tf-emc2/) cabe destacar la iniciativa de experimentar con las llamadas "One Stament Policies" (1SP), orientadas a facilitar la comparación automática de certificados emitidos por diferentes autoridades, y la presentación de los primeros resultados de la iniciativa SCHAC, de la que hablamos en más detalle en otra noticia de esta sección.

TF-Mobility (http://www.terena.nl/tech/task-forces/tf-mobility/) constata el extraordinario impulso de la iniciativa eduroam (http://www.eduroam.org/), a la que ha decidido sumarse la red académica australiana, y que ha llevado a la constitución de un grupo específico de coordinación de servicios de acceso móvil a la red a nivel global. Precisamente este crecimiento está requiriendo una mayor formalización de lo que la marca "eduroam" significa, buscando un conjunto de criterios mínimos que permitan caracterizar los servicios de eduroam. La mayor parte de la reunión estuvo dedicada a analizar estos aspectos y a explorar mecanismos para coordinar la gestión de la infraestructura de movilidad.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Actividades del eIRG

• Grupo sobre e-infraestructuras de la Unión Europea

Una nueva versión del "whitepaper" del eIRG (e-Infrastructure Reflection Group: http://www.einfrastructures.org/) se encuentra ya disponible. Este grupo se está consolidando como el principal cuerpo asesor de la Comisión Europea en las actividades relacionadas con la e-ciencia.

RedIRIS viene colaborando activamente con este grupo, en el que participan responsables de la política científica de los estados miembros de la UE, contribuyendo a sus recomendaciones técnicas, en especial en las áreas relacionadas con los esquemas de autenticación y autorización y en la coordinación con las actividades de GÉANT2.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Portal de acceso a WoK

• Portal de acceso a la Web of Knowledge

El nuevo portal de la Licencia de Acceso Nacional a los servicios de la Web of Knowledge, gestionada por la FECYT (http://www.accesowok.fecyt.es/), se encuentra ya disponible. Este nuevo portal es fruto de la colaboración entre la propia FECYT, RedIRIS y la Universidad de Sevilla. Se

encuentra hospedado en las instalaciones del CICA y emplea la tecnología PAPI (http://papi.rediris.es/).

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Iniciativa SCHAC y esquemas iris

• Iniciativa para armonizar los esquemas de representación de datos para entidades académicas y de investigación; y los esquemas LDAP de RedIRIS

La iniciativa SCHAC (SCHema for Academia: http://www.terena.nl/tech/task-forces/tf-emc2/schac.html) nace dentro del grupo TF-EMC2 de TERENA (http://www.terena.nl/tech/task-forces/tf-emc2/) con la intención de armonizar los esquemas de representación de datos para entidades relacionadas con las instituciones académicas y de investigación.

Estos esquemas armonizados podrán aplicarse en multitud de situaciones, desde el control de acceso a recursos compartidos hasta facilitar procesos de movilidad interinstitucional (como el llamado proceso de Bolonia, que debe permitir a los estudiantes cambiar de centro universitario dentro de Europa).

El grupo ha producido ya sus primeros resultados, concentrados en la definición de los atributos correspondientes a las entradas que representan personas.

En los grupos de trabajo de Málaga se presentaron los resultados, hasta esa fecha, del comité de expansión del esquema LDAP iris (http://www.rediris.es/ldap/esquemas/iris/esquema-iris.es.html) cuyos puntos principales fueron:

- La versión estable del esquema LDAP iris (http://www.rediris.es/ldap/esquemas/)
- El esquema abierto a nuevas necesidades en nuestra comunidad

Es decir, el esquema LDAP iris se hace estable en su versión 20050323-1.1.14 y sólo se realizarán modificaciones en lo que se refiere a la incorporación de nuevos atributos.

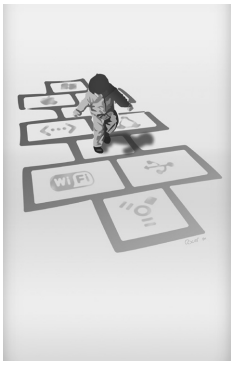
Se comentaron estos temas:

- La necesidad de potenciar el uso de URNs en algunos atributos para permitir extender la semántica de los mismos; realizar una normalización de manera simple y ofrecer una mayor expresividad. Además, esto facilitará la interoperabilidad entre los contenidos de los directorios corporativos de las instituciones afiliadas a RedIRIS.
- Se planteó la necesidad de crear vocabularios controlados para ciertos atributos del esquema LDAP iris como irisUserEntitlement e irisUserStatus y la posibilidad de definir un atributo irisEduPersonAffiliation (http://www.rediris.es/ldap/esquemas/iris/irisUserPrivateAttribute/).
- La necesidad de hacer hincapié en el uso de un estilo común a la hora de almacenar los componentes del nombre de una persona. En el esquema LDAP iris existen atributos para el apellido primero (sn1) y para el apellido segundo (sn2) por lo que se propone su uso. Esto, junto con el uso de givenName, para almacenar el nombre de pila, facilitará enormemente el desarrollo de aplicaciones que interoperen usando los directorios corporativos de las instituciones.
- Debido a la incorporación, en la última versión del esquema, del atributo irisClassifCode, dedicado específicamente a la clasificación de los objetos del directorio LDAP, se hace necesaria una actualización de las recomendaciones de uso que tenga en cuenta todos los aspectos relacionados con los sistemas de clasificación basados en la codificación COPA.

Asimismo se crearán muchos más ejemplos para que sea aún más cómoda la implantación del esquema LDAP iris dentro de nuestra comunidad.

En cuanto a la influencia de nuestro esquema en la comunidad internacional cabe destacar que se han exportado 6 atributos al esquema SCHAC en su RC2 y que se está haciendo una campaña para fomentar el uso de un atributo de privacidad al estilo del irisUserPrivate Attribute

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones
Javier Masa
(javier.masa@rediris.es)
Técnico de Middleware



En los Grupos de Trabajo de Málaga se presentaron los resultados del comité de expansión del esquema LDAP

La influencia de nuestro esquema LDAP en la comunidad internacional es actualmente muy importante

ACTUALIDAD de RedIRIS

Se está trabajando en la versión 1.4 de PAPI

Se está estudiando la colaboración entre las infraestructuras básicas de red de las NRNs y las actividades de e-ciencia

Actualidad de PAPI

• Actualidad del sistema distribuido para control de acceso desarrollado por RedIRIS

La version 1.4 de PAPI (http://papi.rediris.es/) se encuentra ya en versión beta y esperamos poder realizar el anuncio de la versión definitiva inmediatamente después del verano.

Por otra parte, el equipo de desarrollo de PAPI ha puesto a punto un punto de acceso (PoA) basado en PHP, que permite la implantación de la tecnología de acceso PAPI en entornos donde (por cualquier razón) no es posible o deseable desplegar toda la infraestructura PAPI. Este PoA permite pues, una extensión simple de la tecnología de acceso PAPI a prácticamente cualquier combinación de servidores y contenidos.

El equipo de PAPI ha comenzado también a trabajar en la integración de PAPI dentro del servidor Tomcat.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Seminario sobre NRENs y Grids

• Las redes académicas nacionales y los proyectos Grid

El pasado mes de mayo se celebró un seminario, organizado por TERENA, sobre aspectos de colaboración entre los proyectos Grid y las redes académicas (http://www.terena.nl/tech/grid/nren-workshop.html). En él se dieron cita representantes de ambos campos y se presentaron y discutieron las posibilidades de colaboración entre las infraestructuras básicas de la red y los servicios que requieren las actividades de e-ciencia.

El consenso común fue la necesidad de que las redes académicas prestaran servicios adicionales como parte de la infraestructura básica, mas allá de la estabilidad de la propia red y un ancho de banda suficiente.

Entre estos servicios se destacaron la gestión de la identidad digital, la localización de recursos y los mecanismos de colaboración en línea.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Reunión del TF-VVC

• Reunión del Grupo de Trabajo de vídeo, voz y colaboración de TERENA

El grupo TF-VVC (Task Force Video Voice and Collaboration: http://www.terena.nl/tech/task-forces/tf-vvc/) está auspiciado por el Programa Técnico de TERENA y tiene por objetivo investigar la utilización de tecnologías de voz, video y colaboración para su implementación en las redes europeas de investigación y educación.

Sus actividades están enfocadas a Europa y países limítrofes, empezó sus actividades el 1 de septiembre del 2004 y tiene prevista una duración de dos años.

El pasado 4 de junio tuvo lugar en Poznan (Polonia) la reunión presencial del grupo, se contó con la exposición de 13 presentaciones acerca de los avances en todas las áreas de actividad en las que está dividido el grupo. Estas áreas son guías para la provisión de servicios de colaboración basados en voz, video y datos, infraestructura para Content Delivery Networks, portal para el acceso a contenidos, metadata, netcasting channel (live.academic.tv), GDS, sistemas high-end/quality, control de acceso a recursos de video, desarrollos en telefonía IP y medidas extremo-extremo.

El catedrático del Departamento de Ingeniería Telemática de la UPM, Juan Quemada mostró en una presentación la herramienta de colaboración en grupo multipunto desarrollada por ellos: ISABEL.

En el área de actividad *J* presentamos un mecanismo de control de acceso a servidores de video cuya principal virtud es diferenciar la entidad de autenticación de la de autorización, permitiendo de esta manera separar cómo se sabe que alguien es dice quien dice ser, de los

contenidos a los que se puede o no acceder. El desarrollo que aun está en evolución se basa en tecnología PAPI.

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

Reunión anual del W3C en Gijón

• Reunión del World Wide Web Consortium

El pasado 28 de junio tuvo lugar la segunda reunión anual de miembros del W3C en España. A dicha reunión asistieron algunas de las instituciones afiliadas a la red académica que también son miembros, al igual que Red.es.

En la agenda de la reunión estaban incluidos numerosos temas de interés, distribuidos en cuatro mesas de trabajo sobre Accesibilidad, Web Móvil, Servicios Web, y gestores de contenido y Web Semántica.

Quizá la primera de las mesas fue la de más interés de cara a la comunidad académica, puesto que además de debatir sobre las tecnologías relacionadas con accesibilidad, como WCAG 1.0 (recomendación) y 2.0 (borrador); también se habló sobre la legislación aplicable para sitios web públicos. La LSSI establece que para final de 2005 los sitios web de organismos públicos deberán haber tomado medidas para adaptarlos de cara a cumplir con las directivas europeas en cuestión de accesibilidad.

En la mesa sobre Web móvil se debatió sobre el *'estado del arte'* de las tecnologías que permiten el acceso a la Web desde dispositivos móviles, así como sobre la posibilidad de diseñar *una-vez-para-todo* combinando las diversas tecnologías existentes y que ya son recomendación de W3C.

Por otra parte, la iniciativa *Mobile Web Initiative* del consorcio, en la que están los principales fabricantes de telefonía móvil y empresas de comunicación, está desarrollando una guía de "buenas prácticas" de desarrollo para la Web Móvil.

Las tecnologías relacionadas con Web Services centraron el debate de la tercera de las mesas.

Se habló de las posibilidades que ofrecen para el intercambio de información entre aplicaciones de una manera segura, así como de la gran cantidad de implementaciones que surgen a la vez que el estándar, lo cual hace que el ciclo de desarrollo y entrada en funcionamiento se acorte.

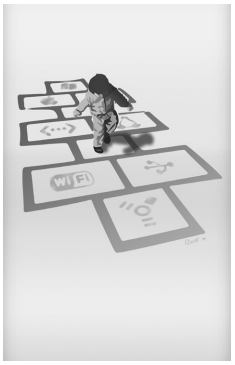
Por otra parte se hizo una invitación a la participación en las *I Jornadas Científico-Técnicas en Servicios Web: JSWEB 2005* (http://www.w3c.es/Eventos /ServiciosWeb), a celebrar en Granada los días 13 y 14 de septiembre.

La última sesión trató sobre gestión de contenidos y sobre web semántica. Respecto a gestión de contenidos, decir que el interés se centró en las herramientas que proporcionan una clara separación de aspecto y contenido, de cara a mejorar distintos aspectos como la usabilidad, accesibilidad o el visionado de la web desde distintos dispositivos, utilizando para ello los estándares ofrecidos por W3C. Respecto de Web semántica, se hizo un repaso sobre el estado de la materia y las distintas tecnologías y herramientas existentes.

Como colofón de la reunión se anunció el congreso *Fundamentos Web 2005 (http://www.fundamentosweb.org)*, que se celebrará del 22 al 24 de noviembre próximos, conjuntamente en Oviedo y Gijón. A dicho congreso asistirán las más importantes personalidades del mundo de la accesibilidad, usabilidad, y estándares web.

Por último, quisiera mencionar que el World Wide Web Consortium está abierto a nuevas incorporaciones de aquellas organizaciones de la comunidad académica que deseen participar como miembros. Creemos que esta comunidad tiene mucho que aportar en este foro e invitamos a las instituciones afiliadas a RedIRIS a seguir la actividad de la oficina del W3C en España (http://www.w3c.es/ ESmiembros), bien haciéndose miembro, o bien siguiendo la información a través de su sitio web.

José Manuel Macías
(jmanuel.macias@rediris.es)
Servicios de Información



La LSSI establece que para final de 2005 los web de organismos públicos deberán cumplir con las directivas europeas de accesibilidad

El 13 y 14 de septiembre se celebrarán en Granada las I Jornadas Científico-Técnicas en Servicios Web

El programa Sun SITE dona hardware a centros académicos para albergar repositorios de software y documentación de libre distribución

Nueva dinámica de minigrupos en el último Grupo de IRIS-MAIL

X Aniversario del SunSITE de RedIRIS y mejoras en el servicio de FTP

• Diez años de convenio con Sun para albergar repositorios de software de libre distribución

Se cumplen diez años del convenio firmado entre Sun MicroSystems y RedIRIS por medio del cual se acordó que RedIRIS hospedara un Zuñiste para España. El programa Sun SITE dona hardware a centros del entorno académico con objeto de que estos alberguen repositorios de software y documentación de libre distribución al mismo tiempo que sirve como canal de distribución de las distintas tecnologías de Sun. Cuando el SunSITE de RedIRIS (http://sunsite.rediris.es) nació en 1995, había 18 SunSITEs en el mundo, en la actualidad esta cifra asciende a 60 repartidos por los cinco continentes.

El servicio de FTP de RedIRIS (ftp://ftp.rediris.es) ha crecido en este tiempo ofreciendo sus contenidos a través del propio SunSITE RedIRIS y a lo largo de estos años se ha modificado la configuración inicial de hardware. En sus comienzos, estaba ubicado en una máquina SparcServer 1000E con dos microprocesadores SuperSparc, 128MB de memoria RAM y 6 GB de disco duro y coincidiendo con este décimo aniversario y aprovechando el relativo menor uso en la época estival del servicio de FTP, se ha procedido a realizar la última actualización a una máquina que pueda soportar mejor la demanda actual, así como también se ha incrementado la capacidad de almacenamiento actual hasta llegar a 3 Terabytes. Este aumento supone casi la duplicación del espacio dedicado hasta el momento a réplicas, y nos permitirá ampliar las existentes y añadir otras nuevas. Se ha realizado también un esfuerzo importante para racionalizar la estructura de directorios del servicio manteniendo sólo aquellos directorios que resultaban más intuitivos para los usuarios y creando alias que permiten acceder a rutas previamente existentes.

El sitio Web de SunSITE ha cambiado también su aspecto, para adaptarse mejor a los estándares de la Web, así como para mejorar la usabilidad y accesibilidad. Estamos trabajando de cara a mejorar las herramientas de búsqueda de información ofrecidas en la actualidad (rpmfind y buscador de ficheros en el propio servidor), que estarán integradas dentro del propio sitio Web de SunSITE RedIRIS.

David Fernández Barrero
(david.barrero@rediris.es)
Área de Middleware
José Manuel Macías
(jmanuel.macias@rediris.es)
Servicios de Información
Antonio Fuentes Bermejo
(antonio.fuentes@rediris.es)
Área de Sistemas

XXII reunión del Grupo de Trabajo IRIS-MAIL

• Reunión en Málaga del Grupo de Trabajo sobre correo electrónico

En esta última edición del Grupo de Trabajo IRIS-MAIL celebrada en Málaga (http://www.rediris.es/mail/gt/my05/) se han introducido cambios en la dinámica de la reunión con el fin de mejorar la participación, contacto e implicación de los asistentes y por lo tanto sus resultados. Para ello se introdujo en la agenda el concepto de **minigrupos**, una especie de *corrillos* entre los asistentes para debatir sobre temáticas concretas y cuyas conclusiones son expuestas y debatidas en el plenario. Estos minigrupos tuvieron una duración de 30 minutos, dispusieron de un moderador, una temática específica y un guión a debatir. La asignación de asistentes a cada uno de los minigrupos fue previamente pactada para hacer grupos heterogéneos.

En primer lugar agradecer a Carmen López (Universidad de Sevilla), Fernando Gozalo (UNED), Pedro Benito (Universidad de Burgos) y Daniel Magaña (Universidad Antonio de Nebrija) su predisposición, trabajo y colaboración directa como moderadores de los minigrupos en esta convocatoria de Málaga al final cada uno de ellos hizo una presentación de los resultados del debate de sus respectivos minigrupos cuyo contenido y tema fueron los siguientes:

- **Grupo I: Control de Flujos SMTP internos**

  Moderadora: Carmen López (US)

  a) Efectos colaterales del filtro en el puerto 25/out
  b) ¿Es necesario el control de flujos?
  c) ¿Qué mecanismos se suelen utilizar?
  d) Recomendaciones para este problema.

- **Grupo II: Cifrado de Tráfico SMTP entre MTAs**

  Moderador: Pedro de Benito (UBU)

a) ¿Cuales serían las ventajas para la Comunidad RedIRIS si se cifrara el tráfico entre MTAs?

- **Grupo III: Autenticación en el correo: Filtros 25/out + SPF + SMTP-AUTH**

  Moderador: Fernando Gozalo (UNED)

  a) ¿Es el filtro 25/out la solución a los *zombies* emisores de correo?
  b) SPF sí SPF no
  c) Pros y contras del uso de SMTP-AUTH y puerto 587
  d) ¿Es el forwarding un servicio necesario en la universidad?

- **Grupo IV: Formación, información y responsabilidad de los usuarios**

  Moderador: Daniel Magaña (NEBRIJA)

  a) ¿Son los usuarios responsables de sus irresponsables actuaciones?
  b) ¿Se dispone de Políticas de Uso en la universidad?
  c) ¿Están los usuarios suficientemente informados?
  d) ¿Se reducirían estos problemas con una adecuada formación?

Previamente al desarrollo de estos minigrupos, por parte de RedIRIS se hizo un repaso a los temas más importantes de IRIS-MAIL y se dió un tutorial sobre "Criterios de seguridad en los sistemas de correo electrónico" que se ampliará en futuras convocatorias. También se difundieron los resultados de la "Encuesta RACE" y los de una encuesta realizada a 40 instituciones de RedIRIS sobre los sistemas de Webmail más utilizados. Los resultados obtenidos son los siguientes:

1º.- IMP/HORDE (12)
2º.- SquirrelMail (9)
3º.- Postman (Universidad de Valencia) (8)
4º.- Exchange (5)
5º.- OWA, EmuMail, MailMan, IPlanet...

Se finalizó con el desarrollo de los minigrupos y la presentación de sus conclusiones donde se acordó poner en marcha las siguientes iniciativas:

Grupo I.- Control de Flujos SMTP internos

Conocemos los efectos que en nuestra red provocan los ordenadores comprometidos por virus (zombies): alto volumen de tráfico no deseado, phishing, distribución de virus, etc. así como el ingreso de dichas LPs en listas negras. Los beneficios para detener este uso abusivo pasan por definir unas políticas de filtrado del tráfico SMTP de salida con un correcto control ya que de lo contrario pueden provocar efectos colatarales más perniciosos como podría ser una excesiva sobrecarga de los servidores de correo y su consiguiente alta en listas negras.

Existen muchos tipos de mecanismos y cada institución definirá el que más se ajuste a sus necesidades. Se decidió crear un repositorio en la Zona de Intercambio de Ficheros para compartirlos entre todos.

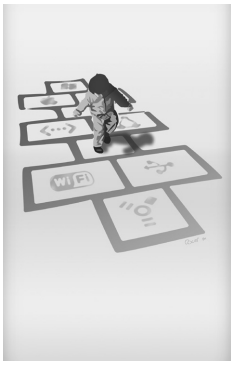
Grupo II.- Cifrado y autenticación entre MTAs de la Comunidad

Hubo consenso acerca de las ventajas del cifrado y autenticación entre MTAs de RedIRIS y se decidió plantear como objetivo el desplegar una red piloto de cifrado de tráfico SMTP entre instituciones de la red académica. Habrá que evaluar el tema de los certificados y la topología de la CA que se puedan utilizar. Si las conclusiones de este Grupo son correctas podremos poner en producción un modelo de Red de confianza inter-institucional para el intercambio de correo electrónico que pueda animar a otros entornos a utilizar estas tecnologías. Algunas de las ventajas y características de este modelo son:

- **Confidencialidad**: Serviría para trasmitir información sensible (investigaciones, datos personales, calificaciones, etc.).
- **Verificación del MTA origen**. Al reconocer un MTA como seguro se podrán evitar virus, spam etc., es decir MTAs no fiables.
- **Transparencia para el usuario**. Los usuarios no deben hacer nada en su clientes.
- **Inalterabilidad**. Los mensajes no podrían ser alterados durante su tránsito.

Grupo III.- Autenticación en el correo: Filtros 25/out + SPF + SMTP-AUTH

En este minigrupo se coincidió en la imperiosa necesidad de filtrar el puerto 25 (SMTP) de salida permitiendo exclusivamente establecer conexiones SMTP con el exterior a aquellos servidores legalmente establecidos. Esta medida reducirá notablemente los actuales problemas producidos por gusanos/virus/zombies. Por problemas administrativos su implementación no parece tan sencilla como cabría imaginar y se debatieron las diferentes tácticas para su definición.



Los beneficios para detener el uso abusivo del correo pasan por definir unas políticas correctas de filtrado del tráfico SMTP de salida

Se planteó como objetivo el despliegue de una red piloto de cifrado de tráfico SMTP entre instituciones de la red académica

SPF no tendrá éxito mientras los grandes operadores de correo electrónico no lo implementen

Sin responsabilidad e información por parte de los usuarios los problemas de seguridad son y serán imparables

Con respecto al tema de SPF (Sender Permited Framework), se debatieron los posibles motivos del escaso despliegue de esta tecnología. Uno de los motivos es que SPF no tendrá impacto mientras no se definan mecanismos de filtrado. Aunque el motivo más importante es la problemática del SPF con el *forwarding* mecanismo ampliamente utlizado en las universidades. Por otro lado se comentó que SPF no sería exitoso mientras los grandes operadores de correo electrónico no lo implementen. Casualmente poco después de esta reunión SPF dejó de ser una propuesta del Internet Engineering Task Force (IETF) para convertirse en un RFC en la categoría de estándar experimental. En próximos número intentaremos explicar con más detalle estas novedades.

Con respecto al tema del uso de SMTP-AUTH a través del puerto 587, pocos de los asistentes disponían de está tecnología. Varios no la requerían porque ofrecían Servicio de VPN (Virtual Private Network) dentro de su institución por lo que los usuarios eran considerados internos y necesitaban autenticarse frente al servidor de correo. Pero todos coincidieron en que es un servicio necesario que al final se acabará soportando. El gran problema de la implantación del uso del puerto 587 es la labor de difusión a realizar ya que es necesario que los usuarios configuren su cliente de correo.

Grupo IV.- Formación, información y responsabilidad de los usuarios

Este minigrupo debatió sobre las posibilidades que habría de informar y formar a los usuarios de forma cíclica a nivel de seguridad y de responsabilidad de Uso del Servicio en la universidad. Sin responsabilidad e información por parte de los usuarios los problemas son y serán imparables Se trataron algunos temas y se quedó como actividad realizar una pequeña Guía "Decálogo de buenas prácticas con el correo electrónico" con el mayor consenso posible. Se ha creado un repositorio común con las iniciativas de cada universidad sobre el tema: cursos, documentación, streaming, etc. También se fijaron algunas directrices estratégicas para intentar dar el suficiente peso a este tema.

Podemos decir que fue una reunión muy dinámica y productiva con bastantes iniciativas e implicación de los asistentes. Esta nueva dinámica de ***minigrupos*** probada en esta reunión se intentará introducir en futuras convocatorias, teniendo siempre presente los escasos recursos humanos necesarios para su correcto desarrollo.

Las presentaciones están disponibles en la zona de trabajo de IRIS-MAIL (login: iris-mail, clave:iris-mail) http://cvu.rediris.es/bscw/bscw.cgi/0/598718

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de correo electrónico

V Reunión de equipos abuse europeos (E-COAT)

• Reunión de equipos de resolución de acciones punibles llevadas a cabo por los usuarios de la red

E-COAT (E*uropean COoperation of Abuse fighting Team:* http://www.e-coat.org*)* es un grupo de reciente creación para el intercambio de información entre equipos abuse europeos. Esta V convocatoria se celebró el 11 de mayo en las instalaciones Swisscom en Zurich. El perfil de los asistentes se divide entre operadores europeos (KPN, Telia, Swisscom, Telefónica, France Telecom, etc.) y redes académicas nacionales (Alemania, Suiza, DK y alguna más). Por lo general los operadores tienen *equipos abuse* específicos y bastante bien estructurados dentro del organigrama de sus respectivas empresas y con bastantes recursos, la parte académica está más derivada a equipos CERT.

Por grupo de abuse entendemos los recursos encargados de recibir las quejas externas, sobre acciones punibles realizadas por los usuarios de la red y que toman las medidas apropiadas para contactar con estos usuarios o con los responsables de seguridad. Estas acciones pueden ser realizadas bien por un departamento (grupo de abuse) o estar descentralizadas dentro de la organización, como es el caso de RedIRIS.

Los objetivos de E-COAT se centran en el manejo y prevención de incidentes abuse, compartiendo problemas y aligerarando soluciones e iniciativas, definiendo buenas prácticas y estándares comunes de reporting, white/blacklisting,... en definitiva siendo el punto focal de la cooperacion anti-abuse en

Europa e interrelacionándose también con otros foros tales como: TF-CSIRT, FIRST, MAAWG, FIINA, RIPE, APWG, ENISA y otros.

Los temas a destacar de esta reunión fueron:

- La colaboración con el Messaging Anti-Abuse Working Group (MAAWG: http://www.maawg.org/)
- La aprobación y consolidación legal del Grupo ECOAT así como la elección de cargos.
- La definición de grupos de trabajo.

Se inauguró la Jornada con una presentación del grupo de Abuse de Swisscom que comenzó a funcionar en noviembre de 2003. Expuso su dinámica y áreas de interés y se abordaron temas como: Contenidos prohibidos, phishing, crackers, spam, malware, copyright, chat abuse y haresment. Es el operador más grande de Suiza y tienen varias decenas de miles de incidentes al mes. Cuentan con un grupo especial de temas de spam que ofrece soporte a sus clientes (residenciales y empresas) en estos temas.

Hubo un espacio reservado a uno de los problemas más candentes en la actualidad como es el phishing. Se contó con una presentación de Pierre Karsten, Interpay (payments transactions for Dutch banks) sobre sus experiencias y puntos de vista sobre los temas de spyware y phishing. Forman parte de una iniciativa internacional llamada ISAC (Information Sharing & Analisys Center http://www.fsisac.com) y disponen de protocolos para CERT gubernamentales y una serie de mecanismos para coordinar incidentes de seguridad.

El tema central de la reunión se centró en la aprobación de la Proposed Operational Framework para E-COAT que se consolidará como una organización que se tramitará antes de fin de año y la elección del comité técnico que estará formado por: Maria Rådström (TeliaSonera Abuse Team), Markus Weyrich (T-Online), Martijn van der Heide (KPN-CERT), Peter Quick (T-COM) y Francisco Monserrat (IRIS-CERT).

Hubo intervenciones y debates fuera de Agenda de interés para el Grupo, resaltar la de Huopio Kauto miembro de FICORA "Autoridad de Regulación de las Comunicaciones de Finlandia" que expuso las regulaciones aprobadas en Finlandia a finales del 2004 relacionadas con los Servicios de Correo electrónico proporcionados en redes públicas (http://www.ficora.fi/englanti/document/FICORA112004M.pdf). Estas regulaciones afectan a cualquier ESP (Email Service Provider) de Finlandia e incluyen aspectos técnicos como: Open-relays, tráficos smtp de salida, control de virus, uso de listas negras, etc.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de correo electrónico
Francisco Monserrat
(francisco.monserrat@rediris.es)
Equipo de Seguridad IRIS-CERT

Seguridad en las comunicaciones: RedIRIS, REUNA, RETINA y RNP

• Proyecto de Seguridad entre RedIRIS y redes latinoamericanas

El proyecto "Seguridad en las comunicaciones: Plataforma de Calidad en el Servicio de Correo Electrónico", desarrollado por RedIRIS y las redes latinoamericanas RNP (Brasil), RETINA (Argentina) y REUNA (Chile), fue uno de los 15 seleccionados por el Fondo Regional para la Innovación Digital en América Latina y el Caribe (FRIDA http://programafrida.net/sp/proyectos2005.html).

El objetivo es crear un escenario de colaboración que permita mejorar la calidad del correo electrónico en la comunidad académica latinoamericana y que sirva de inicio para trabajar de forma conjunta en otros aspectos de las comunicaciones en la Red. Este grupo de trabajo no será cerrado sino que buscará ir integrando poco a poco a otras instituciones latinoamericanas y españolas interesadas en participar en él.

El correo electrónico es una de las herramientas más utilizadas en el entorno académico e investigador para el intercambio de información; sin embargo este servicio está siendo amenazado de forma masiva en un ambiente agresivo y de enorme desconfianza convirtiéndolo en un instrumento vulnerable por sus innumerables problemas de seguridad: virus, fraudes, zombies, spam, etc. Las medidas utilizadas para frenar el caos tales como los filtros de contenidos, las listas negras locales, unilaterales o externas, está ocasionando un aumento de los recursos necesarios y del mismo problema. Este marco caótico provoca una degradación del servicio en los entornos académico-científicos en los que el correo es

Los objetivos de E-COAT se centran en el manejo y prevención de incidentes abuse

El objetivo del proyecto FRIDA es mejorar la calidad del correo electrónico en la comunidad académica latinoamericana

una herramienta vital para el desarrollo de muchas de sus actividades.

La falta de coordinación y disponibilidad de contactos entre los diferentes servidores de correo provoca que muchas veces no sea fácil resolver muchos de los problemas que existen resultando imposible abordar y debatir de forma conjunta las nuevas metodologías o protocolos que van apareciendo como puede ser por ejemplo el SPF (Sender Policy Framework) y que no son implementados por desconocimiento de muchos de los actuales responsables.

En resumen; los objetivos del proyecto son establecer modelos de Servicio de correo electrónico, implementar un modelo de evaluación y seguimiento de este servicio similar al existente en RedIRIS: RACE (Red Avanzada de Correo Electrónico: http://www.rediris.es/mail/race), evaluar estrategias bien de implantación de Modelos de Sensores en Red para problemas de seguridad (RESACA, SANET, etc.) como de nuevos protocolos tales como SPF (Sender Policy Framework), e incluso probar o definir un modelo de intercambio de tráfico IPv6. También se pretende construir herramientas de trabajo colaborativo para el desarrollo del proyecto y su continuidad en el tiempo de forma que permitan un intercambio fluido de información entre los participantes.

El proyecto beneficiará a operadores, universidades e instituciones del entorno académico latinoamericano y del Caribe. Comenzó el 1 de julio y la fecha de finalización marcada es el 30 de junio de 2006. Si su objetivo central es definir una plataforma de colaboración que permita mejorar la calidad del correo electrónico en la comunidad académica latinoamericana, mediante un foro de intercambio de comunicación sobre los problemas de seguridad del correo electrónico, establecido entre las diferentes instituciones académicas de América Latina y el Caribe debería traducirse en la construcción de nuevas prestaciones de valor añadido basadas en este servicio.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de Correo Electrónico

También se pretende construir herramientas de trabajo colaborativo para el desarrollo del proyecto

FRIDA beneficiará a operadores, universidades e instituciones del entorno académico latinoamericano y del Caribe