Actualidad de Red

• GÉANT

Nos encontramos muy próximos a la toma de las decisiones finales en cuanto a la infraestructura para la siguiente red pan-europea GÉANT2 (evolución de la actual GÉANT).

El modelo de red que hasta ahora hemos tenido se modifica, pasando a una nueva arquitectura que permitirá soportar servicios mucho más avanzados y que son descritos más adelante.

A nivel nacional, actualmente, estamos trabajando en la próxima infraestructura de red, que deseamos que incorpore el mismo nivel tecnológico que tienen otras redes de nuestro entorno así como la propia GÉANT2.

• Conectividad con proveedores comerciales

Durante estos últimos meses hemos estado trabajando junto con DANTE y otras NRENs europeas en el concurso para la conectividad comercial Global IP. Los actuales contratos expiran en el mes de abril aunque se extenderán hasta que los nuevos enlaces estén operativos.

Así, la situación actual es de dos enlaces STM-4 (622 Mbps) cada uno con un operador distinto (Telia y Global Crossing). Las estadísticas en abril arrojan valores cercanos a los 600 Mbps en picos por cada uno de los enlaces, es decir, que es necesario aumentarlos en breve.

De esta forma, estos enlaces pasarán a ser de dos conexiones GigabitEthernet (1 Gbps) con Telia y Level 3 y estarán operativos en mayo y junio respectivamente, fechas en las que se realizará la migración de estos servicios.

• Áreas de Investigación

a) VPLS

Desde principios de año, RedIRIS junto con el CESGA (www.cesga.es) han estado realizando pruebas con la tecnología VPLS (Virtual Private Lan Service) primero en entornos de un solo dominio, y posteriormente, en entornos multi-dominio. Esta tecnología (basada en MPLS) permite que máquinas en sitios remotos estén conectadas como si estuviesen en la misma red de área local. En una primera fase, se han realizado pruebas dentro de la red troncal de RedIRIS, y posteriormente se ha experimentado con dos dominios: el de RedIRIS y el del CESGA. Para realizar estas pruebas se ha buscado una solución escalable, utilizando BGP como protocolo de señalización.

Se trata de la primera vez que se configura VPLS en un entorno multidominio. Los resultados de las pruebas se han presentado en distintos Foros:

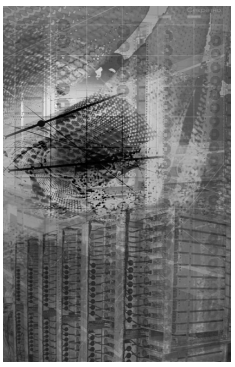
- El World MPLS Congress de París
  http://www.upperside.fr/mplsworldcongress05/mplsworld2005intro.htm
- El 17º TF-NGN de Zurich
  http://www.terena.nl/tech/task-forces/tf-ngn/
- El 4º Workshop GMPLS de Gerona
  http://bcds.udg.es/gmpls/ws4/index.php
- El Terena Networking Conference 2005
  http://www.terena.nl/conferences/tnc2005/

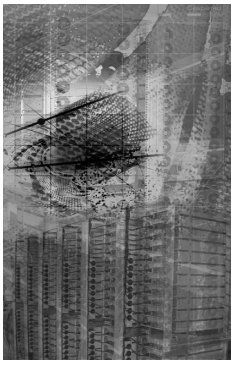
b) Actividades de Investigación en GN2 (Joint Research Activities y Service Activities)

JRA1

Dentro del proyecto GN2 para dotar a las redes de investigación europeas de una red avanzada, se han definido una serie de actividades de investigación en conjunción con las diferentes redes académicas nacionales. Éstas son las llamadas *Joint Research Activities* (en adelante, JRA). **JRA1** es la primera en esta serie (liderada por DANTE), y está enfocada a dotar de una infraestructura de monitorización y medida de rendimiento de red a la nueva red paneuropea. Actualmente es la actividad que se encuentra en una fase más avanzada.

Se está trabajando en un marco general para la aplicación que englobará a todo el mosaico de aplicaciones para medir distintos parámetros de la red, basados principalmente





Actualidad
de Red

en el grupo de métricas de IP conocido como IPPM (*Internet Protocol Performance Metrics*, http://www.advanced.org/IPPM/), y otros valores comúnmente utilizados. Entre ellas se encuentran:

1.- OWD (*One Way Delay*)
2.- RTT (*Round Trip Time*)
3.- Ancho de banda disponible
4.- Ancho de banda actual
5.- Flujos por segundo
6.- Paquetes por segundo

Aunque esta actividad ha partido de y para la red europea, la otra gran red académica, Internet2, está participando activamente en el desarrollo de esta actividad de cara a hacer compatibles los sistemas de monitorización y control de ambas redes y así conseguir un beneficio mutuo, amplificado por el gran número de usuarios comunes a ambas comunidades.

La aplicación que resulte del trabajo de la actividad JRA1 finalmente se llamará SONAR (*Service Oriented Network-monitoring ARchitecture*). La parte visible será una red de máquinas a lo largo y ancho de las redes académicas, con criterios de acceso y autorización regidos por los resultados de la actividad JRA5 (*Movilidad y autorización*). Se está trabajando en distintas áreas:

- Arquitectura general
- Esquema de la BBDD
- Visualización de los datos
- Elección de herramientas
- Elección de métricas
- Agregación de métricas de múltiples dominios
- Decisión sobre plataforma y software de desarrollo
- Licencia del trabajo resultante

A grandes rasgos, el diseño del marco general de la infraestructura (*General Framework Design, GFD*) está generando una gran cantidad de documentos de cara a conseguir, primero en papel y más tarde con un prototipo, un diseño con cimientos sólidos, usando las últimas tecnologías disponibles, y aprovechando gran parte de los desarrollos independientes que se han realizado hasta la fecha, tanto en forma de aplicaciones (*MRTG*, *Cricket*, *RRDTool, flow-tools*,...) como de métricas.

La arquitectura principal se basa en los siguientes objetos: MP (*Measurement Point*), DA (*Data Archive*), RP (*Resource Protector*), LS (*Lookup Service*), TS (*Topology Service*)

Un **MP** puede ser tanto una máquina con herramientas instaladas como un router al que se pueda consultar por SNMP. El **DA** se encarga de almacenar las estadísticas típicas de tráfico o retardos de líneas, el **RP** de proteger y planificar el uso de recursos de los **MP**s, y el **LS** y el **TS** de obtener una lista de recursos y una topología actualizadas.

Hay previsto un primer prototipo de SONAR para finales de junio de 2005, con capacidades mínimas, en el que se conseguirá una primera visión de los problemas y ventajas de las elecciones que se han realizado.

El foro de TERENA TF-NGN se ha estado aprovechando para realizar sesiones previas sobre JRA1, a fin de avanzar de forma rápida en algunos de los puntos más difíciles de tratar por correo electrónico. Asímismo, se ha producido un solapamiento con la actividad JRA2 (*Seguridad*) en el área de tratamiento de flujos, en la que se ha escogido la dirección que dicte el grupo de seguridad.

JRA2

El desarrollo de esta actividad se explica en esta sección un poco más adelante.

JRA3

Esta actividad está centrada en el desarrollo de toda la infraestructura necesaria para proveer ancho de banda bajo demanda extremo a extremo (http://www.geant2.net/server/show/nav.00d00a003). En estos momentos se está trabajando en la definición de la arquitectura inicial del servicio. Dicha actividad está liderada por RedIRIS. También se está avanzando en el estudio de la integración de diferentes tecnologías para proveer dicho servicio mediante el análisis de diferentes algoritmos de computación de caminos en una red. Estos dos aspectos son muy críticos en un entorno multidominio como es el entorno europeo al que pertenecemos.

SA3

El objetivo de este servicio es proporcionar la calidad de servicio definida como Premium IP (http://www.geant.net/server/show/nav.00700a003) extremo a extremo (end to end) dentro de GÈANT y en las NRENs conectadas a ella (http://www.geant2.net/server/show/nav.00d00a 006). En un primer paso se ha definido el marco y la arquitectura del servicio pasando ahora a la fase de implementación.

Asímismo, en esta actividad se ha creado el PERT (Performance Response Team), un equipo similar a un NOC o un CERT pero compuesto por expertos en diferentes ámbitos (sistemas, aplicaciones, redes) para buscar soluciones a los posibles problemas de rendimiento de las aplicaciones sobre la red. En una fase inicial, se ha montado un piloto de PERT, con una dedicación limitada aunque en estos momentos se está trabajando para crear uno en operación permanente.

c) Proyecto MUPBED

Su objetivo es integrar y validar las tecnologías ASON/GMPLS (Automatically Switched Optical Network/Generalised Multi Protocol Label Switching) en el contexto de testbeds (redes de prueba) de gran escala y administradas por el usuario (http://www.ist-mupbed.org/).

El trabajo hasta ahora se ha centrado en la interconexión de los testbeds que participan en el proyecto, centrándonos nosotros en buscar una tecnología de interconexión que permita al testbed de Telefónica I+D, conectado por un enlace ATM a RedIRIS, tener una conexión a nivel 2 sobre RedIRIS y GEANT, hasta los testbed de los otros participantes y teniendo en cuenta que en los otros extremos hay IP y Ethernet. Por otro lado, también se ha trabajado en evaluar las diferentes tecnologías respecto al plano de control, en el acceso directo de las aplicaciones a la configuración de dispositivos de red.

• Situación de conectividad IPv6

En estos momentos nos encontramos centrados en la puesta en operación del servicio multicast IPv6 nativo. No está siendo una tarea sencilla dada la dificultad que existe para analizar problemas con los protocolos multicast. Hemos involucrado a ingenieros de Juniper para descartar posibles problemas de las versiones JUNOS de los routers.

El peering multicast Ipv6 nativo ya está establecido y la red GÉANT, como red de tránsito, soporta este servicio.

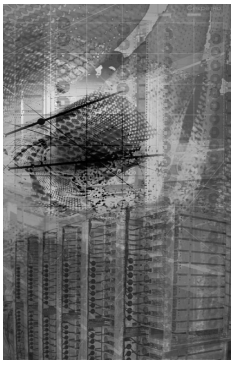
Por otro lado, en RedIRIS se han realizado dos asignaciones de direccionamiento, al CICA y a la UIB, conectándose esta Universidad a la red IPv6 mediante un túnel.

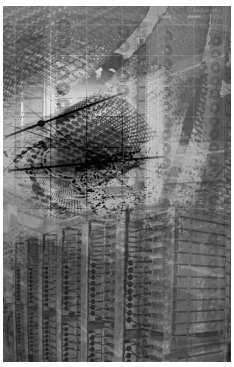
• I Foro IPv6 de RedIRIS

Los días 28 y 29 de abril se celebró en la Universidad de Valencia el primer Foro IPv6 de RedIRIS (http://www.rediris.es/red/jornadasipv6.es.html). Desde hace tiempo, la red dispone de IPv6 nativo y se ofrece a todos los centros conectados la posibilidad de usar esta nueva generación del protocolo IP. El objetivo de esta convocatoria fue eminentemente práctico y se intentó ofrecer a los asistentes –provenientes en su gran mayoría de universidades y grandes centros de investigación– la posibilidad de aprender a usar IPv6 junto con todos los aspectos relacionados con la configuración y puesta en marcha en redes, servidores y servicios para que empiecen a implantarlo en las redes de sus instituciones.

En las ponencias se trataron temas como:

- La Visión del Ministerio de Industria, Turismo y Comercio y de la Comisión Europea sobre el despliegue del protocolo en las redes. En este punto se explicó el esfuerzo realizado por la Comisión que se está canalizado a través de la financiación de proyectos de investigación relacionados con IPv6. El Ministerio de Industria también está impulsando la implantación del protocolo mediante su promoción a través de la participación en el Task-Force español de IPv6. La postura común es que, tras una inversión inicial enfocada principalmente a los entornos académicos y de investigación, ya ha llegado el momento de su despliegue en el sector privado.
- Configuraciones, problemas y soluciones en los routers de los principales fabricantes: Juniper y Cisco. Ambas empresas realizaron su presentación enfocada a sus principales líneas de producto, centrándose principalmente en el desarrollo de IPv6 en sus equipos para redes de campus.
- Ejemplos reales del despliegue de IPv6. La Universidad de Valencia nos mostró cómo han realizado la transición a IPv6 en parte de su red, así como en los principales servicios (web, FTP, DNS,...). La visión comercial del tema vino de la mano de Telefónica que presentó el despliegue en su red para el soporte de IPv6 y el servicio que ofrecen a los clientes.
- Proyectos y desarrollos que se están realizando actualmente con IPv6. La red portuguesa presentó el trabajo que ha realizado con IPv6 dentro del proyecto 6NET (http://www.6net.es). Al mismo tiempo, se presentaron proyectos de movilidad e IPv6, y ejemplos de transición, dentro del marco del proyecto Euro6IX (http://www.euro6ix.es). Se mostraron las experiencias con el uso del





nuevo protocolo en redes como i2CAT, y proyectos concretos de desarrollos de IPv6 sobre redes que sólo soportaban IPv4, por ejemplo, la reprogramación del firmware de un router wifi para soporte IPv6. Respecto a las aplicaciones en general, se presentó una guía para portar el código de aplicaciones hacia soporte IPv6.

- IPv6 en relación al registro de dominios. Desde Red.es se presentaron los planes futuros para poder registrar dominios.es con una dirección IPv6, si bien la demanda de usuarios es en la actualidad nula.

- Retransmisiones multimedia con IPv6. Gracias a las pruebas realizadas con CESCA, CESGA, UC3M y RedIRIS se ha configurado la red para el soporte de IPv6 multicast nativo. Aprovechando la infraestructura existente, en el Foro se realizó la retransmisión de un fragmento de ópera por IPv6 multicast de forma nativa y una transmisión en directo desde el Liceu.

- Se trataron los principales problemas de seguridad que existen con IPv6 y se valoraron ejemplos concretos como por ejemplo el desarrollo de una PKI sobre IPv6.

- Tuvo lugar una mesa redonda en la que se trataron temas como la perspectiva del usuario final sobre IPv6, lo que les puede aportar y por qué no se usa este protocolo.

  En la mesa redonda había representantes de una amplia gama de sectores: usuarios finales 'avanzados' (con conocimientos de redes), administradores de redes y sistemas del sector público y privado, representantes de la Administración –todos ellos con amplios conocimientos de IPv6–. Las principales conclusiones a las que se llegó es que realmente hoy en día no hay demanda suficiente para usar IPv6, y tampoco existe una necesidad real. Aunque el agotamiento de direccionamiento está lejos, la utilización real de IPv6 puede llegar cuando el número de dispositivos conectados a la red aumente de manera considerable, o bien cuando se produzca el despliegue masivo de voz sobre IP. Por otro lado, quizás ya se lleve demasiado tiempo hablando de transición y sea el momento de ir haciendo efectiva esta transición como una 'actualización de software' rutinaria. También es cierto que aparte de para administradores de redes y personas con cierto nivel técnico, IPv6 es un gran desconocido para los usuarios.

El foro lo inauguró el Réctor de la Universidad de Valencia y contó también con la participación de una importante experto de la Comisión Europea.

• Estado de la conectividad en los Puntos Neutros: ESPANIX y CATNIX

Los peerings establecidos en ESPANIX aparecen en la siguiente tabla ordenados por fecha de establecimiento. En negrita aparecen con los que además se tiene establecido un peering IPv6.

1.- COMUNITEL	14.- SERVICOM
2.- NTELIDEAS	15.- NTT/VERIO
3.- DATAGRAMA	16.- TELEGLOBE
4.- SARENET	**17.- TELEFONICA DATA**
5.- COLT	18.- FUJITSU
6.- COGENT	19.- JAZZTEL
7.- ONO	20.- YA.COM
8.- AUNA	21.- INTEROUTE
9.- EASYNET	22.- ACENS
10.- BT	23.- IBERCOM
11.- TISCALI	
12.- FLAG	
13.- ARSYS	

En CATNIX la situación es la siguiente:

1.- NEXICA	7.- AL-PI
2.- ADAM	8.- T-SYSTEMS
3.- ALTECOM	9.- SARENET
4.- ACENS	10.-EASYNET
5.- KAOS	11.- JAZZTEL
6.- BT	

• ALICE y EUMEDCONNECT

ALICE

La red latinoamericana que interconecta las redes de investigación nacionales de América Latina está operativa desde septiembre 2004. Las NRENs de Chile, Brasil, México, Argentina fueron las primeras en conectarse. En abril 2005, ya están las de Panamá, Venezuela, Perú y en breve Uruguay. Se continúa trabajando para interconectar al resto de países. La topología final es la siguiente:

También ha comenzado a funcionar el sitio web oficial de esta red, llamada RedClara, www.redclara.net.

Los próximos 25, 26 y 27 de abril se organizarán en Veracruz (MX) unas jornadas técnicas para los miembros de redclara y alice. En ellas se dará un tutorial de IPv6 y se discutirá la implementación dual-stack en la red y otros temas técnicos que afecten a la red.

• XVII TF-NGN en Zurich

Los pasados 14 y 15 de abril se celebró en Zurich la 17ª edición del grupo de trabajo TF-NGN (http://www.terena.nl/tech/task-forces/tf-ngn/).

Comenzó la reunión con un asunto de importancia crítica para todos los investigadores europeos y usuarios de las redes de investigación como es la actualización sobre el estado en el que se encuentra GÉANT2.

A continuación, se dio paso a presentaciones que trataban sobre desarrollos y pruebas en tecnologías de red. La primera parte versó sobre tecnologías de redes privadas virtuales, donde nuestra compañera Laura Serrano ofreció una presentación sobre las experiencias realizadas en RedIRIS junto con el CESGA.

Se siguió con temas de monitorización pasiva, y Sven Ubik de CESNET (NREN checa) presentó las últimas novedades del proyecto LOBSTER (sucesor del proyecto SCAMPI). IPv6 sigue siendo uno de los campos en los que se trabaja intensamente con el objetivo de acelerar su despliegue. Una vez que las redes europeas soportan IPv6 nativo, el siguiente esfuerzo se centra en IPv6 multicast. En este sentido, es crucial disponer de herramientas para la monitorización IPv6 multicast y por eso se ha creado una actividad dentro del TF-NGN para trabajar en este tema, actividad liderada por Steve Williams de UKERNA (NREN inglesa).

Se presentaron otras tres actividades de suma importancia: evaluación de nuevas arquitecturas hardware de routing y switching, protolos de transporte y Routing IP. En todas estas actividades RedIRIS forma parte.

A continuación, se mostraron los avances y desarrollos obtenidos en optical networking. La red checa presentó la implementación de CESNET2, una de las redes europeas más avanzadas en este campo. Felix Klueger de SWITCH (NREN suiza) presentó un nuevo servicio ofrecido por esta red a sus usuarios: LambdaTunnel, soportado por su red óptica. Finalmente, desde Dante se abre un nuevo campo de trabajo, Intelligent Control Plane Architectures, protocolos que veremos en un futuro funcionando sobre nuestras redes.

Para terminar, Juniper presentó una propuesta para distribuir reglas de forma dinámica entre redes pertenecientes a dominios distintos y controlar incidentes de seguridad.

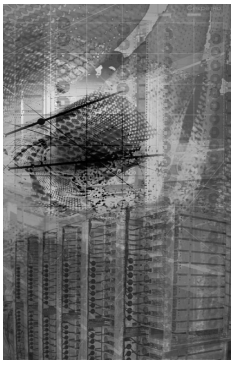
Esther Robles
(esther.robles@rediris.es)
Coordinadora Área de Red
Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de Red
David Martínez
(david.martinez@rediris.es)
Área de Red

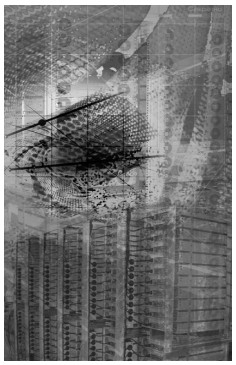
Informe de incidentes de seguridad año 2004

A principios de este año publicamos en las páginas Web del CERT de RedIRIS el informe anual de incidentes correspondiente al pasado año 2004 (http://www.rediris.es/cert/doc/informes/2004/). Se trata de un informe no muy extenso y fácil de leer que esperamos permita obtener una visión general de lo acontecido, a nivel de seguridad, en nuestra red.

Durante el año 2004 se ha confirmado la tendencia de ataques dirigidos a las plataformas más comunes y en concreto a usuarios finales, fundamentalmente con sistema operativo Windows. Aparecen por ejemplo, nuevos problemas asociados al uso, cada vez más extendido, de redes móviles en los centros afiliados a RedIRIS. Además, se confirma la tendencia ya observada durante el año pasado, de que muchos equipos finales son utilizados para fines ilícitos, normalmente mediante la instalación de un servidor FTP utilizado para distribuir material protegido por las leyes de copyright.

Vuelven a aparecer varios gusanos (Sasser, Kibuv, etc.) que tienen la peculiaridad de poseer un código altamente cambiante surgiendo diversas variaciones de un mismo gusano, lo que dificultaba en gran medida su detección y eliminación.





Sin duda alguna, lo más novedoso del 2004 lo constituyen la proliferación de botnets, redes de equipos "zombies" comprometidos y controlados remotamente desde un servidor central vía IRC, que son utilizadas para lanzar diversos ataques. Es previsible que durante el presente año continuemos viendo este tipo de redes de bots, cada vez más sofisticadas y utilizándose cada vez con mayor frecuencia para acciones ilegales.

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

Nuevos servicios para los equipos del *Trusted Introducer* de TERENA

IRIS-CERT es un equipo acreditado en el servicio *Trusted Introducer* (TI) de TERENA desde marzo de 2001 (http://www.trusted-introducer.nl/) y el propósito fundamental de este servicio es el de crear una red de confianza entre los CERTs existentes en Europa.

Desde su puesta en marcha, los equipos acreditados han contado con una serie de servicios de valor añadido, entre los que se encontraban el acceso a áreas restringidas de información en la Web del *Trusted Introducer*, listas de distribución restringidas para el intercambio de información, actualización y distribución de claves públicas de otros equipos, y difusión de información detallada de cada uno de los equipos acreditado como ficheros CVS.

A principios de este año, este conjunto de servicios se han visto ampliados de forma importante. Se ha incluido un sistema de alerta ante eventos de seguridad tanto en banda (mediante el uso de listas distribución con soporte criptográfico) como fuera de ella (mediante el uso de voz y SMS); servicios de recogida y distribución de estadísticas, y una infraestructura de clave pública (PKI) que permite la emisión de certificados digitales en favor de los equipos para el acceso a las zonas restringidas de la Web.

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

10 años de vida de IRIS-CERT

Fue hace 10 años (en noviembre de 1995), cuando nuestro entonces compañero Rubén Martínez presentaba en los Grupos de Trabajo de Tenerife el equipo de Atención de Incidentes de Seguridad de RedIRIS, haciendo una descripción general de las funciones de este tipo de equipos (prevención y actuación frente a incidentes de seguridad fundamentalmente) e informando de los servicios que el entonces recién nacido equipo iba a prestar (diseminación de información sobre seguridad, servicios de comunicaciones seguras, asesoramiento en prevención de incidentes y respuesta frente a ellos).

Mucho ha llovido desde entonces, muchos compañeros han ido y venido, y también se han lanzado algunos servicios nuevos durante estos años (varias ediciones del reto de análisis forense, red de máquinas trampa, auditorías bajo demanda, foros específicos de seguridad, ...). Incluso nos hemos encargado de servicios fuera del ámbito tradicional de un CERT como la PKI de RedIRIS o el servidor de claves PGP. En la medida en la que nuestros recursos nos lo permiten, hemos participado en diversas iniciativas de coordinación, foros y proyectos internacionales y nacionales, habiendo entrado en el más que preciado anillo de confianza entre CERTs por méritos propios y gracias al esfuerzo de cada uno de los integrantes del equipo en los últimos 10 años.

Tampoco podemos olvidar en esta celebración, a los muchos colaboradores que siempre hemos encontrado en nuestra comunidad, y que de una forma completamente altruista han compartido conocimientos y experiencias con todos nosotros.

Desde el equipo de seguridad os damos las gracias a todos y esperamos que los próximos 10 años contemos con los recursos adecuados para daros un servicio de calidad.

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

Nuevo teléfono de IRIS-CERT

Aparte de los teléfonos fijos publicados en nuestra Web, a partir de ahora, el operador en turno de incidencias de IRIS-CERT está localizable durante la jornada laboral (L-J de

09:00 a 18:00, V 09:00 a 15:00) en el nuevo móvil de IRIS-CERT (607156313).

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

XIII y XIV reuniones TF-CSIRT de TERENA

La 13ª y 14ª edición 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 celebraron en La Valeta (Malta) y Londres (UK), organizados por los principales Equipos de Atención de Incidentes de los mencionados países, mtCERT y JANET-CERT respectivamente.

Como viene siendo habitual, el primer día estuvo dedicado a presentaciones de carácter general, donde se intenta dar a conocer las distintas iniciativas o desarrollos en los países anfitriones. Pero además, se hizo una mención especial a varios temas de interés para la comunidad CERT europea tales como:

- La comunidad Grid y los problemas de seguridad que esta nueva infraestructura puede ocasionar y el establecimiento de mecanismos que permitan poner un solución coordinada y efectiva a los mismos.
- Propuestas para la presentación de proyectos relacionados con seguridad para el FP6 de la EU y para el PASR (*Preparatory Action Security Research Program*).
- ENISA (*European Network and Information Security Agency*) e interacciones con el TF-CSIRT. En este punto, contamos con una presentación en Londres realizada por su director, Mr. Andrea Pirotti, tras la cual se despertó un interesante debate sobre posibles vías de cooperación.

Todas las presentaciones está disponibles en:

- http://www.terena.nl/tech/task-forces/tf-csirt/meeting13/programme.html
- http://www.terena.nl/tech/task-forces/tf-csirt/meeting14/programme.html.

En las reuniones del Task Force propiamente dichas se trataron los temas habituales:

- CHIHT (*Clearinghouse of Incident Handling Tools*), que pretende ser un repositorio de herramientas y utilidades de uso generalizado por los equipos de seguridad, y que incorporará además descripciones de los workflows que siguen los CERTs, con la idea de que pueda convertirse en un recurso de utilidad para aquellas organizaciones que tengan pensado establecer un CERT (http://chiht.dfn-cert.de/).
- Firma de un MoU (*Memorandum of Understanding*) entre el TF-CSIRT y APCert (*Asia & Pacific Coordination Group*), que básicamente incluye el establecimiento de canales de comunicación eficaces entre ambos grupos, seguimiento de las actividades que se lleven a cabo por los mismos y cooperación en proyectos.
- Estrategias de colaboración entre el TF-CSIRT y la actividad de investigación sobre Seguridad en el proyecto GÉANT2, como por ejemplo el establecimiento de un grupo de expertos cuya función sea discutir y dar forma a la dirección estratégica de las actividades que se deben llevar a cabo durante la duración del proyecto.
- Se crea un nuevo Grupo de Trabajo dentro del TF-CSIRT sobre Formatos de Intercambio y Descripción de Exploits y Vulnerabilidades (VEDEF, *Vulnerability and Exploit Descripcion and Exchange Format*).

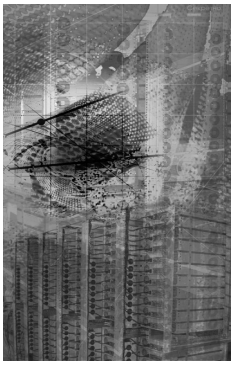
Las próximas reuniones del TF-CSIRT a celebrar durante el presente año se realizarán en Zurich (Suiza) en mayo y en Lisboa (Portugal) en septiembre.

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

Grupo de Trabajo sobre RTIR

En el pasado boletín os informamos de lo acontecido en la primera reunión de este nuevo grupo de trabajo impulsado por el TERENA TF-CSIRT (*CSIRT Coordination for Europe*) celebrada en Londres en enero de 2004. Mucho ha llovido desde entonces, y muchos han sido los progresos realizados de los que pretendemos informaros en esta noticia.

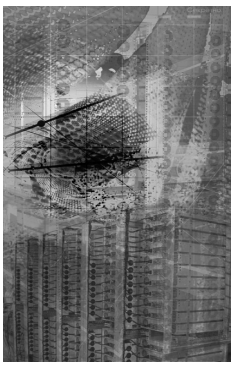
Sólo para refrescar la memoria a aquellos que lo necesiten, el RTIR (*Request Tracker for Incident Response*, http://www.bestpractical.com/rtir/) es una herramienta *Open Source*, construida sobre



Nuevo teléfono de IRIS-CERT

XIII y XVI TF-CSIRT de TERENA

Grupo de Trabajo sobre RTIR



una herramienta de propósito general para la gestión de incidencias denominada RT (*Request Tracker*, http://www.bestpractical.com/rt/). El RTIR fue especialmente diseñada por Best Practical (http://www.bestpractical.com/), a petición del Equipo de Atención de Incidentes de Seguridad de la red académica del Reino Unido, JANET-CERT, para cubrir las necesidades específicas de *workflow* que los CERTs tienen a la hora de atender incidentes de seguridad.

Han sido varias las reuniones que se han celebrado desde enero de 2004, en las que han participado diversos CERTs europeos, entre ellos IRIS-CERT, todos ellos con el interés de mejorar la herramienta que actualmente estamos utilizando en nuestro trabajo diario.

El objetivo del Grupo de Trabajo ha sido el de elaborar un documento de nuevos requerimientos con todas aquellas funcionalidades, mejoras y módulos que deberían presentar próximas versiones del RTIR y todo ello acompañado con la creación de un consorcio, bajo el paraguas de TERENA, con el fin de obtener la financiación necesaria para afrontar este desarrollo.

Tras diversas reuniones finalmente se ha conseguido elaborar el documento de requerimientos, el cual ha sido entregado a Best Practical y donde se especifican varios módulos que consideramos imprescindibles añadir a la herramienta, como por ejemplo el módulo cifrado/firma digital, atención de múltiples ámbitos de actuación, generación de informes ejecutivos, optimización en el manejo de contactos, mejora en el manejo de colas y visibilidad de colas entre RT y RTIR, utilidades de borrado de basura e información inútil de la Base de Datos subyacente, etc. así como una serie de mejoras generales en el interface de la herramienta y en los procesos de actualización del software.

El consorcio ha sido creado entre diversos equipos europeos interesados, entre ellos FCCN (Portugal), CERT-Polska (Polonia), GovCERT NL (Holanda), AcoNet-CERT (Austria), SUNET-CERT (Suecia), LITNET-CERT (Lituania), SWITCH-CERT (Suiza), JANET-CERT (UK) e IRIS-CERT (España). En estos momentos se están perfilando los detalles del contrato que se suscribirá con Best Practical a través de TERENA, y del cual IRIS-CERT formará parte.

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

Foro español y europeo de grupos abuse

A principios de 2004 se celebró en Madrid la I Reunión de equipos Abuse europeos que ha ido cristalizando en un propuesta de creación de un foro de coordinación similar al TF-CSIRT (Foro europeo de coordinación de CSIRTs), de hecho bastantes de los promotores son miembros de TF-CSIRT. Este foro de equipos abuse está dando lugar a un grupo más consolidado llamado E-COAT (European COordination Abuse Team http://www.e-coat.org) y pretende mejorar la gestión y el intercambio de los incidentes abuse entre los diferentes operadores europeos.

Para ampliar esta iniciativa a nivel nacional RedIRIS está alentando la creación de un foro de equipos abuse de operadores españoles (http://www.rediris.es/abuses/) que permita mejorar la coordinación a nivel nacional y europeo. Para ello, y en colaboración con el Grupo Nemesys de Telefónica España, a principios de marzo de 2005 organizó en Madrid la I reunión de equipos abuse españoles (http://www.rediris.es/mail/abuse-es.html) donde asistieron unas 50 personas pertenecientes a 30 operadores españoles.

La reunión se inauguró con la presentación de la dinámica de trabajo de uno de los Equipos Abuse más grandes, el de NEMESYS de Telefónica España (RIMA), que cuenta con centenares de denuncias diarias emitidas por equipos ADSL fundamentalmente residenciales, locutorios, cibercafés, etc. A continuación Francisco Monserrat Coll y Jesús Sanz de las Heras realizaron unas presentaciones que abrieron el debate de los siguientes temas:

- Gestión de incidentes abuse en cada uno de los operadores
- Aspectos de SPF
- Posibilidad de intercambiar IPs no deseables
- Denuncias de copyright
- Sistemas de intercambio de incidentes
- Medidas reactivas/proactivas de respeto a los usuarios
- Posibles vías futuras de colaboración
- Movilidad de usuarios maliciosos

Genéricamente los grupos abuse vienen siendo equipos encargados de gestionar cualquier tipo de incidencias de Red que se produzcan en los equipos de usuarios a los que el proveedor de acceso ofrece sus servicios. Estas incidencias se suelen producir como consecuencia de quejas provinientes del exterior de la organización por acciones realizadas por estos equipos. Algunos

ejemplos de las incidencias tratadas por estos grupos de abuse son:

- Envío de correo no deseado (SPAM) desde equipos del ámbito de actuación del grupo de abuse.
- Escaneos y mensajes provocados por la infección por virus, gusanos, bots, etc.
- Quejas de asociaciones de fabricantes de contenidos (informáticos, audiovisuales, etc.) por la distribución no autorizada de ficheros por parte de los usuarios.
- Acciones de denegación de servicio y ataques contra equipos de la misma u otra organización.
- En general todas las acciones de los usuarios que violen la política de uso de los sistemas informáticos y causen perjuicio intencionado a otra organización.

RedIRIS está promocionando la creación de equipos abuse en sus instituciones (abuse@dom.es) incluyéndolo en las Agendas de Grupos de Trabajo de RedIRIS, entre ellos IRIS-MAIL. La idea es ir cerrando los mismos modelos en sus diferentes niveles: europeo (E-COAT) nacional (ABUSE-ES) y de la comunidad académica (RedIRIS) con el fin de crear las bases de una colaboración más productiva.

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

Comité de expansión del esquema LDAP IRIS

Gracias a la creación, hace unos años, del repositorio de esquemas LDAP, se han detectado una serie de atributos en nuestra comunidad que –aunque tienen diferentes nombres– se usan con el mismo objetivo. Parece lógico pensar que estos atributos puedan unificar sus nombres para que en todos los centros se haga uso del mismo cuando nos refiramos al mismo atributo.

El esquema LDAP IRIS surge de la integración en un solo esquema de aquellos objetos y atributos que siendo definidos por alguna organización de la comunidad RedIRIS, para uso particular, puedan ser de utilidad a todas las demás.

Actualmente se utiliza un conjunto de atributos para la interoperabilidad de muchas aplicaciones multi-institucionales. No sólo basta con usar los mismos nombres de atributos, sino que se hace necesario utilizar una semántica común.

Es evidente que hace falta realizar un esfuerzo entre todas las organizaciones de la comunidad RedIRIS para actualizar y mantener al día este esquema (http://www.rediris.es/ldap/esquemas/). Para ello RedIRIS ha creado un pequeño Comité de Expansión (http://www.rediris.es/ldap/esquemas/iris/esquema-iris.es.html) del esquema que nace con los siguientes objetivos:

- Promocionar su uso dentro de nuestra comunidad.
- Crear y publicar las sucesivas versiones del esquema IRIS.
- Crear documentación que facilite la implantación del esquema IRIS en todos los centros haciendo especial hincapié en la semántica de cada uno de los atributos definidos.
- Coordinarse con iniciativas similares en otros países para la estandarización de objetos/atributos.

Desde su creación, en las Jornadas Técnicas de Toledo de 2004, el Comité se ha reunido en varias ocasiones para trabajar sobre las diferentes solicitudes de incorporación de elementos al esquema. Como fruto de este trabajo se han añadido al esquema IRIS atributos relacionados con:

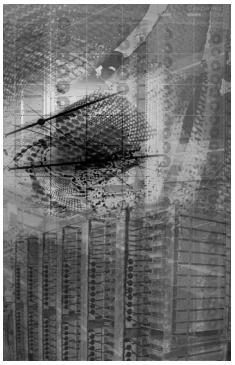
- Privacidad (irisUserPrivateAttribute)
- Correo electrónico (irisMailMainAddress, irisMailAternateAddress)
- Presencia en la red (irisUserPresenceID)
- etc.

A nivel europeo TERENA ha creado un Comité Internacional para la armonización de esquemas (SCHAC: SChema HArmonisation Committee) en el que vamos a participar para proponer que algunos de los atributos definidos en el esquema IRIS sean expandidos hacia un esquema europeo.

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

eduroam.es

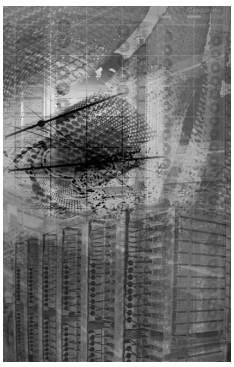
A lo largo de los últimos meses se han desarrollado una serie de actuaciones, tanto para el desarrollo del espacio de movilidad a



Foro español y europeo de grupos abuse

Comisión de expansión del esquema LDAP IRIS

eduroam.es



eduroam.es

Estado de la actividad JRA2

nivel nacional, como para el alineamiento de la iniciativa con su equivalente a nivel europeo. Conviene recordar, que el objetivo principal es crear un entorno europeo que permita a los usuarios que se desplazan a otros centros, poder acceder a servicios tanto de conectividad como a aquellos que les permitan continuar con su trabajo habitual.

La página web http://www.eduroam.org funciona no sólo como punto de referencia de la iniciativa europea eduroam, sino también a nivel mundial ya que se han incorporado centros de Australia y se está barajando la inclusión de algunos americanos. En esta página se puede ver un mapa que muestra los países (en verde) que actualmente integran eduroam, con enlaces a sus webs nacionales. La idea es que un usuario que se desplaza a un centro tenga una web de referencia donde consultar si el país al que pertenece se encuentra integrado en la iniciativa eduroam y cuál es su página de información, que en muchos casos corresponde a dominios "eduroam.x" en función de cada país.

En el caso de España, se ha asignado el dominio "eduroam.es" (http://www.eduroam.es) para su uso en los servicios relativos a la iniciativa a nivel nacional. En esta página se muestran las ciudades con centros integrados en "eduroam.es", y al colocar el ratón en cada una de ellas aparece información de dichos centros: url de la página del centro, SSIDs para cada uno de los modos de acceso wireless soportados y si el centro admite conexiones "Guest", es decir, de gente que les visita. De esta forma, el usuario posee un punto centralizado de información que le permite, por un lado conocer qué posibilidades de conexión puede encontrar en una determinada ciudad, y por otro información especifica del centro destino sobre cómo conectarse.

A nivel más técnico, en relación con la jerarquía de servidores radius sobre la que se cimienta actualmente eduroam, se ha implantado un servidor a nivel nacional (radius.rediris.es) basado en Freeradius (http://www.freeradius.org), que a nivel jerárquico cuelga de los servidores radius europeos, y cuelgan de él los servidores pertenecientes a redes autonómicas o centros adscritos a eduroam.es.

Actualmente el esfuerzo se vuelca en que cada vez más centros se adhieran a la iniciativa y hacer de eduroam y eduroam.es grandes espacios de movilidad que permitan a los usuarios de las redes académicas viajar a otros centros con la garantía de disponer de servicios adecuados para el desempeño de su trabajo diario.

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

Estado de la actividad JRA2 de GÉANT2

Dentro del proyecto GN2 para dotar a las redes de investigación europeas de una red avanzada, se han definido una serie de actividades de investigación en conjunción con las diferentes redes académicas nacionales. Éstas son las llamadas *Joint Research Activities* (en adelante, JRA). **JRA2** es la segunda actividad en esta serie (liderada por SWITCH). Está 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 de respuesta ante incidentes de seguridad de forma coordinada. Para ello se pretende: desplegar una infraestructura de monitorización de flujos y alarma, unificar los procedimientos de gestión de incidentes para que los equipos de seguridad reaccionen rápidamente, y crear recomendaciones de seguridad para equipos intermedios.

Teniendo en cuenta que GN2 no es únicamente una red, sino un conjunto de servicios; algunos de ellos no ofrecen un punto claro que delimite dónde empieza la responsabilidad de Dante y acaba la de la red de investigación, por lo que se requiere una cuidadosa planificación y coordinación para que no haya elementos que queden en «tierra de nadie». A este fin, en todas las actividades de JRA2 se hace un claro énfasis en una forma de pensamiento «global» que involucre a todos y cada uno de los participantes.

Se han definido varias líneas de trabajo (*Work Items, WI*) dentro de JRA2, que se describen a continuación:

- **WI1: Protección de elementos y servicios de red de la red GN2**

  En este apartado, liderado por Dante, se pretende crear recomendaciones y normativas de seguridad para las redes de investigación nacionales y la red GN2, y su puesta en práctica en los equipos de Dante. Dado que en otras actividades JRA se van a desplegar

equipos para ofrecer nuevos servicios, las recomendaciones irán evolucionando en función de las necesidades que se creen, para poder abarcar estos servicios. El desarrollo de la actividad se ha dividido en 3 planos: el de gestión/administración, el de control, y el de reenvío (*forwarding*).

- **WI2: Creación de servicios de seguridad**

  Esta línea de trabajo liderada por SURFnet pretende definir un conjunto integrado de herramientas que permita la monitorización del tráfico de red de cara a detectar y diagnosticar anomalías y ataques, así como la creación de contramedidas para paliar sus efectos.

- **WI3: Diseño y establecimiento de una infraestructura de coordinación de incidentes de seguridad**

  GARR lidera este apartado en el que se pretende fomentar el uso de las herramientas desplegadas en el WI2, y establecer canales de comunicación seguros entre los equipos de seguridad de las distintas redes de investigación, previo acuerdo de un formato unificado de intercambio de incidentes y de taxonomías, niveles de gravedad y procedimientos de manejo de información.

- **WI4: Establecimiento de relación con el grupo de trabajo de Terena TF-CSIRT**

  SWITCH lidera esta línea de trabajo en la que se intenta promover la colaboración entre GN2 y el grupo de trabajo TF-CSIRT de TERENA, que agrupa a un buen número de expertos en seguridad tanto de las redes de investigación como de otros ámbitos. Se pretende crear grupos de interés comunes a GN2 y el TF-CSIRT, así como aprovechar las reuniones periódicas del TF-CSIRT para organizar sesiones dedicadas exclusivamente a JRA2.

- **WI5: Creación de un comité de expertos**

  En este apartado se pretende formar un grupo de 10 expertos de GN2 y TF-CSIRT cuya función sea discutir y dar forma a la dirección estratégica de las actividades que se deben llevar a cabo durante la duración del proyecto.

Se han detectado interacciones entre distintos JRAs. En el caso de JRA2 hay una fuerte implicación de los resultados de JRA5 (*Movilidad y autorización*) en las acciones del WI1, dado que la infraestructura que se construya en JRA5 habrá de ser integrada en los sistemas de acceso de los elementos y servicios de red. Asimismo, dado que tanto en JRA1 (Monitorización y rendimiento de red) como en JRA2-WI2 se busca analizar flujos de red (aunque de forma diferente), los responsables de cada grupo de trabajo estarán en contacto para ahorrar esfuerzos y unificar criterios.

Hasta el momento se han celebrado dos reuniones presenciales en Malta y Londres, y están previstas al menos dos más en el presente año, en Zurich y Lisboa, coincidiendo con el TF-CSIRT, aunque no se descarta que se celebren reuniones adicionales para concretar aspectos relativos a la colaboración de dos JRAs o a un WI en particular.

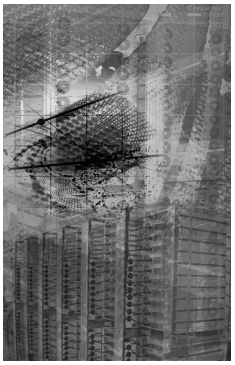
Existe una página en el web de Géant2 sobre JRA2: http://www.geant2.net/server/show/nav.00d00a002

David Martínez
(david.martinez@rediris.es)
Área de Red
Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de Seguridad de RedIRIS

Actividad JRA5 de GÉANT2

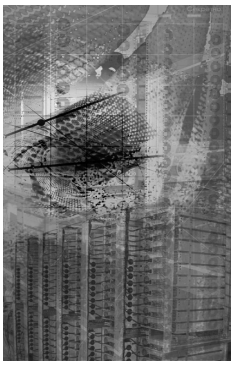
La actividad JRA5 (*Roaming and Authorisation)* dentro del proyecto GÉANT2 (http://www.geant2.net/) está orientada a establecer una infraestructura capaz de garantizar el acceso de los usuarios a la red y a los recursos que ésta ofrece desde cualquier lugar y en cualquier momento. Para ello, las primeras tareas se han concentrado en generalizar la infraestructura de Eduroam (http://www.eduroam.org/) dentro del objetivo de movilidad y en el establecimiento de una Infraestructura común de Autenticación y Autorización (AAI) que facilite la colaboración entre las redes académicas y sus instituciones afiliadas dentro de Europa. RedIRIS, dada su importante actividad dentro del área de las AAI (PAPI ha sido la primera AAI en producción a nivel mundial), lidera el objetivo del desarrollo de la AAI común.

En este momento, el grupo de JRA5 está trabajando en la arquitectura de esta AAI y en el análisis de requerimientos de la infraestructura de movilidad. Los resultados disponibles (un glosario de términos y el documento de requerimientos de la AAI común) han sido ya publicados en el sitio Web del



Estado de la actividad JRA2

Actividad JRA5 de GÈANT2



Actividades de la TF-EMC2

I EuroCAMP

Evolución de PAPI

proyecto (http://www.geant2.net/upload/pdf/GN2-04-111Final.pdf y http://www.geant2.net/upload/pdf/GN2-05-026v6.pdf).

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

Actividades de la TF-EMC2

Como ya comentábamos, se ha formado un nuevo grupo de trabajo de TERENA, TF-EMC2 (European Middleare Coordination and Collaboration), como continuación de los trabajos del grupo TF-AACE. Este grupo está de nuevo liderado por RedIRIS y su objetivo es avanzar en el desarrollo de las infraestructuras middleware y su interoperabilidad dentro del entorno académico.

A día de hoy, las tareas de la TF-EMC2 se concentran en las siguientes actividades:

- Desarrollo, evolución y aplicación del AA-RR (http://www.rediris.es/app/aarr/).
- Mantenimiento y desarrollo del repositorio de CAs académicas TACAR (http://www.tacar.org/).
- Contribución al desarrollo de las infraestructuras middleware dentro de los campus de las instituciones.
- Armonización de los esquemas para el intercambio de datos (en directorios, XML, etc.) entre las instituciones académicas.
- Coordinación de datos relativa al desarrollo y establecimiento de infraestructuras de autenticación y autorización.
- Coordinación con otras organizaciones internacionales en estas materias.

El grupo ha conseguido ya algunos resultados notables, como por ejemplo la organización del primer EuroCAMP, un documento sobre el uso de certificados en los Grids y un resumen de las prácticas comunes en cuanto a autenticación y autorización en Europa (http://www.terena.nl/tech/task-forces/tf-emc2/).

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

I EuroCAMP

Entre los días 2 y 4 de marzo se celebró en Turín el primer EuroCAMP (http://www.terena.nl/tech/eurocamp/) con el patrocinio de TERENA y dentro de las actividades de la TF-EMC2, una iniciativa tomada de la práctica habitual dentro de Internet2 para la difusión de las tecnologías middleware. El objetivo es juntar a personas dedicadas al desarrollo de infraestructuras middleware en las redes académicas nacionales y a los potenciales usuarios de las mismas dentro de las instituciones, con un triple objetivo:

- Facilitar la difusión de las nuevas tecnologías middleware en los campus.
- Obtener realimentación sobre las aplicaciones reales y las necesidades existentes en lo referente a estas tecnologías en las instituciones.
- Aumentar la participación en los grupos de desarrollo de estas tecnologías con grupos activos en ellas dentro de las instituciones.

Más de 120 participantes de toda Europa (con una notable representación española) acudieron al encuentro que, según las evaluaciones recogidas, fue un éxito completo: alrededor de un 92% de los asistentes expresó su interés en acudir a sucesivas ediciones del evento. El programa y las presentaciones se encuentran disponibles en http://www.terena.nl/tech/eurocamp/programme.html

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

Evolución de PAPI

Mientras el equipo de desarrollo sigue trabajando en la versión 1.4 del software (del que existe ya una versión beta), el número de instalaciones PAPI (http://papi.rediris.es/), tanto dentro de la comunidad RedIRIS como en otras redes académicas aumenta. Este aumento implica también un mayor desarrollo del software y del soporte de la comunidad de usuarios a la aplicación de PAPI en accesos basados en modo proxy y también de su extensión a otros mecanismos de autenticación (un ejemplo notable es el sistema de autenticación de la UOC) y otros ámbitos de aplicación como es el caso de los protocolos de streaming multimedia.

Es importante destacar también la integración de PAPI con:

- La infraestructura de control de acceso Athens (http://www.athens.ac.uk/), aplicada

en muchos proveedores de acceso a publicaciones científicas. Ahora es posible, para un usuario autenticado por PAPI, acceder a un recurso cuyo acceso esté controlado por medio de Athens sin necesidad de reautenticarse de nuevo.

- Los sistemas de gestión bibliotecaria de ExLibris (Aleph, MetaLib y SFX, http://www.exlibrisgroup.com/), lo que permite el uso de PAPI como fuente única de autenticación y derechos de acceso para las instituciones que gestionen sus fondos de publicaciones electrónicas por medio de estos sistemas.
- El nuevo portal de acceso a la Licencia de Acceso Nacional a la Web of Knowledge gestionada por la FECYT (http://www.accesowok.fecyt.es/)

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

Desarrollo de la herramienta AARR

Como parte de su actividad en el grupo de trabajo JRA5 (Joint Research Activity 5: http://www.geant2.net/server/show/nav.00d00a005) de GÈANT 2 (http://www.geant2.net) RedIRIS está desarrollando en la actualidad la herramienta AARR (Authentication and Authorization Requester-Responder: http://www.rediris.es/app/aarr).

La herramienta nació en un principio como una propuesta de PTYOC, y en la actualidad el código resultante del trabajo de dicha propuesta está siendo revisado, al igual que la arquitectura de la propia aplicación. Los primeros resultados están disponibles en la página del proyecto, así como el código fuente, a través de la interfaz WebCVS de RedIRIS.

AARR se concibe como una herramienta que ayudará a mejorar la interoperabilidad entre distintas infraestructuras de autorización y autenticación presentes en las distintas comunidades académicas, tanto a nivel europeo como internacional (Internet 2). Los siguientes pasos serán la conexión entre PAPI (http://papi.rediris.es) y Shibboleth /(http://shibboleth.internet2.edu) mediante AARR, haciendo que ambos sistemas puedan hablar entre sí.

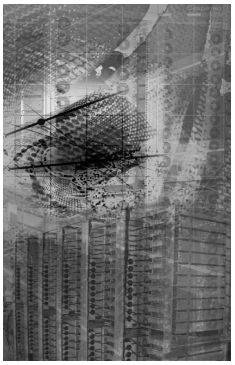
La idea de AARR ha suscitado gran interés tanto dentro de JRA5 como del grupo de trabajo sobre middleware de Terena, TF-EMC2.

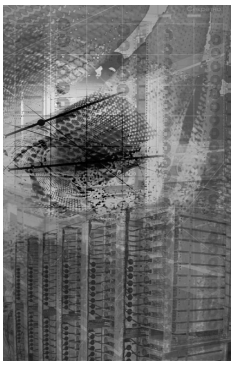
José Manuel Macías
(jmanuel.macias@rediris.es)
Servicios de Información

Actualización de los sistemas de monitorización

Para poder garantizar un nivel de calidad adecuado en los servicios gestionados por RedIRIS es necesario disponer de sistemas de monitorización que chequeen con frecuencia el correcto funcionamiento de los mismos. De esta forma estaremos informados en todo momento del estado de los servicios y podremos reducir el tiempo de respuesta en caso de tener que restaurar alguno de ellos. El principal sistema de monitorización que viene utilizando RedIRIS es Nagios (antiguo Netsaint). Este sistema de código abierto dispone de un conjunto de plugins para monitorizar muchos de los usuales servicios de red (ssh, http, ftp, pop, smtp, dns, ntp, nntp, etc.), además permite añadir tus propios plugins para otros servicios más específicos. La versión utilizada actualmente es la 1.2, aunque se está preparando la migración a la versión 2.0 que ha salido recientemente. Esta nueva versión introduce mejoras tales como la posibilidad de agrupar los servicios, la disponibilidad de nuevas macros en la definición de los comandos; de estadísticas sobre los procesos de Nagios; de API para integrarse con otros sistemas, etc., aunque habrá que probarla para conocer exactamente su alcance.

Existen dos sistemas Nagios en RedIRIS para hacer un chequeo cruzado y no perder información aunque uno de los dos sistemas falle. La nueva organización de los servicios monitorizados se basa en la estructura de la red de RedIRIS, de forma que cada host se agrupa según la subred a la que pertenece. Esto permite detectar rápidamente problemas de red cuando el conjunto de servicios con problemas se encuentran en la misma subred. Sobre algunos de los servicios monitorizados se hace un chequeo pasivo, de forma que desde el propio servidor donde reside el servicio se envía el estado del mismo a Nagios mediante el plugin NSCA. Este es el caso del chequeo de espacio en disco, del propio servicio de Nagios y de las news. También se han realizado plugins a





la medida como en el caso de la monitorización de PAPI y el sistema de acceso a recursos restringidos. Nagios además permite monitorizar otros servicios como LDAP, radius, mrtg, bases de datos como postgresql, mysql, oracle, etc.

En cuanto a la notificación de alarmas se han actualizado los contactos y los grupos, de forma que cada persona es considerada un grupo con dos contactos: su dirección de correo electrónico y su identificador de mensajería instantánea (Jabber). Así tenemos un sistema de notificaciones orientado a personas en vez de a contactos. También se han actualizado las dependencias entre servicios para no recibir multitud de alarmas cuando el origen del problema sea único.

Debemos comprobar que la nueva versión de Nagios mejora realmente el rendimiento de los chequeos y de los CGIs, puesto que los ficheros de configuración no sufren muchos cambios y los plugins son independientes del núcleo. Con respecto a los CGIs, se está pensando en sustituirlos por un interfaz web en PHP, esperemos que este cambio esté disponible en la versión 3.0.

David González
(david.gonzalez@rediris.es)
Aministración de Sistemas

Premio Nuevas Aplicaciones para Internet

El proyecto Searchy, nacido en el seno de RedIRIS y la Universidad de Alcalá dentro del programa PTYOC (http://www.rediris.es/app/ptyoc/), ha sido galardonado con el segundo premio de la IV edición del premio NAI (Nuevas Aplicaciones para Internet). El premio NAI está organizado por la Cátedra Telefónica para Internet de Nueva Generación en la Universidad Politécnica de Madrid. El objetivo de dicho premio es promover la creación y desarrollo de nuevas aplicaciones y desarrollos para Internet.

Searchy es un metabuscador de estado de arte cuya función es permitir búsquedas de recursos e integración de información dentro de entornos colaborativos, ofreciendo un elevado grado de flexibilidad y un mínimo coste de implementación. Utiliza tecnologías de agentes, junto con las últimas tendencias en la Web: los servicios web y la web semántica.

Actualmente se sigue desarrollando Searchy y se espera su entrada en producción a nivel europeo en los próximos meses.

Para más información se puede consultar la web del premio NAI (http://internetng.dit.upm.es/premio.htm) y la web del proyecto Searchy (http://jsearchy.sourceforge.net).

David Fernández Barrero
(david.barrero@rediris.es)
Área de Middleware

Reunión de administradores del Servicio de Listas

En abril de 1995 RedIRIS comenzó a ofrecer un Servicio de Listas de Distribución a la comunidad académica que relevaba al servicio que se venía ofreciendo desde la Universidad de Valencia a través de la desaparecida red EARN/BITNET. Este Servicio pretendía suministrar una herramienta, basada en el correo electrónico, destinada al desarrollo de grupos colaborativos de carácter científico. Las listas de RedIRIS han ido abriendo y consolidado caminos de colaboración entre científicos españoles y de otras partes del mundo, fundamentalmente de Latino América. En aquella época el correo electrónico era considerado una "*nueva tecnología*" y se preveía que futuras herramientas telemáticas fueran desplazándolo a un segundo plano, pero diez años después no se han percibido grandes cambios en las herramientas colaborativas, más allá de la concentración de herramientas en entornos web y del comienzo de las aplicaciones síncronas. A pesar de los múltiples problemas que afectan al correo, sigue siendo una herramienta habitual e imprescindible en la Red, si bien es cierto que hay que seguir apostando y promocionando por nuevas tecnologías ya no tan emergentes.

Inicialmente este Servicio se diseñó de forma distribuida para permitir que otras instituciones pudieran participar en él con el objetivo de optimizar recursos, mejorar rendimientos y sobre todo evitar duplicar listas con temáticas similares. Este modelo no fue posible por la falta de disponibilidad de servidores de listas en las instituciones y el escaso interés mostrado por la comunidad académica en este tipo de servicios. Actualmente es un servicio centralizado aunque siempre abierto a colaboraciones institucionales para evitar la dispersión de contenidos.

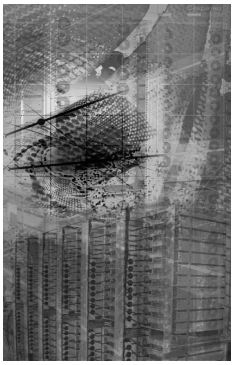
El Servicio de Listas de distribución ha intentado mantener el mayor nivel de calidad posible. Se ha creado una Política de Uso como marco de desarrollo y se han seguido unos rigurosos criterios de evaluación en la solicitud de listas donde priman los contenidos científicos. También se vienen exigiendo avales académicos a los administradores que gestionen los foros dando prioridad a los integrantes de instituciones pertenecientes a RedIRIS; puntualmente se ha ofrecido servicio a iniciativas científicas internacionales (Argentina, Uruguay, etc.) donde se ha contado con participación española. Las listas también vienen cumpliendo su misión de soporte a los habituales Grupos de Trabajo (IRIS-CERT, IRIS-IP, IRIS-MAIL, etc.), columna vertebral de las actividades de RedIRIS. El Servicio de listas está actuando como canal de distribución masiva de información de ofertas de empleo y becas (OFER-TRABEC), congresos o reuniones científicas (DISEVEN) y otros más específicos englobados en los Servicios de Distribución Científica de RedIRIS (http://www.rediris.es/list/sdis).

El Servicio de listas de RedIRIS no hubiera sido posible sin la figura y el trabajo voluntario del administrador, gestor o moderador de cada una de las listas que en la actualidad ascienden a unas 450 personas. Estas personas –docentes científicos en su gran mayoría– han trabajado por la calidad de contenidos de cada una de las listas; han dado soporte a sus usuarios y suscriptores; han recogido y divulgado las novedades de nuevas funcionalidades que el servicio ha ido generando en estos años; se ha preocupado de aspectos colaterales como seguridad, protección de datos, copyright, etc. y han sido valedores en los diferentes foros de las políticas de RedIRIS.

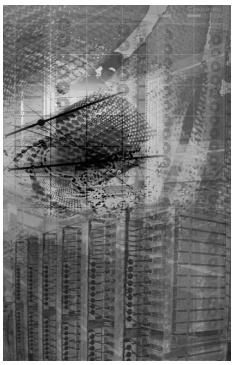
Desde el punto de vista estratégico de RedIRIS, este colectivo de administradores ha sido una pieza muy importante en la puesta en marcha de numerosos servicios y desarrollos tecnológicos como por ejemplo la iniciativa de Redes Temáticas Científicas de RedIRIS, desarrollo de bases de datos, la Guía de Expertos (canal de comunicación entre científicos y periodistas), SARAC (Servicio de Acceso a Recursos de Alta Calidad), Clasificaciones científicas (COPA), iniciativa de Revistas *open-acces,s* etc. Se trata de un foro inmejorable que dispone de información acerca de las necesidades de recursos de red, herramientas, servicios, etc. del colectivo de usuarios de la Comunidad de RedIRIS. Desde el punto de vista científico los administradores articulan la base de buena parte de la ciencia nacional y podría ser un punto de referencia en la política científica.

Para una mejor coordinación entre RedIRIS y este colectivo de administradores se vienen celebrando desde hace años unas Jornadas de coordinación de administradores de listas. En concreto la última se ha celebrado en la Universidad de Barcelona durante los pasados 11 y 12 de abril (http://www.rediris.es/list/jur05/). En esta reunió además de debatir y exponer los temas habituales del Servicio de Listas, se trataron temas y herramientas de trabajo colaborativo en la Red en el entorno científico, se dieron tutoriales de seguridad, sobre herramientas de trabajo colaborativo de nueva generación (streaming, VRVS, PODcasting, etc.), se abordaron temas colaterales tales como análisis y dinámica de grupos. Hubo un coloquio abierto donde todos los asistentes expusieron sus experiencias con listas de distribución remarcando las ventajas y problemas existentes para que RedIRIS disponga de información a la hora de definir estrategias futuras. Entre las conclusiones podemos destacar algunas palabras remitidas por José Luis Molina (docente del Departament d'Antropologia Social i Cultural de la Universitat Autonòma de Barcelona) asistente a este evento:

> *El Servicio de RedIRIS tienen sentido en sí mismo como mecanismo de difusión de información temática. El Servicio de RedIRIS es modélico. El correo electrónico con mensajes planos de una página bien estructurados y con al menos un hiperenlace, constituye un medio de comunicación perfecto. RedIRIS enlaza con iberoamérica y, en general, con el mundo de habla luso-hispana (http://revista-redes.rediris.es/webredes/sig/red_redes.jpg). Muchas de las listas de RedIRIS han dado lugar a nuevas iniciativas científicas tales como revistas electrónicas, proyectos de investigación, etc. Para la colaboración en la investigación o puesta en marcha de nuevos proyectos es necesaria la disponibilidad de herramientas colaborativas de mayor alcance que las suministradas por RedIRIS. Actualmente muchos proyectos de investigación están utilizando herramientas suministradas por proveedores comerciales (yahoo, MSN, etc.). Los grupos de investigación ya consolidados no necesitan de nada ni de nadie, ni dedican su tiempo a difundir el conocimiento, sólo son los grupos de áreas científicas poco*



Reunión de Administradores del Servicio de Listas



Reunión de Administradores del Servicio de Listas

XIX Grupos de Trabajo

reconocidas los que desde los márgenes, están empujando la innovación.

Uno de los aspectos que se debatieron fue la necesidad de herramientas *groupware* para trabajo colaborativo entre grupos y departamentos de diferentes instituciones académicas. Este tipo de servicios telemáticos actualmente no existen de forma estructurada en la Comunidad RedIRIS. Otros temas dignos de destacar de la reunión es la presentación de los Servicios de la Fundación Española de Ciencia y Tecnología (http://fecyt.es); la iniciativa de Revistas Científicas "Open-acces" que surgió en los foros de administradores en 2003 y ha cuajado en un servicio más amplio dentro del portal TECNOCIENCIA gestionado por el CINDOC (CSIC) y un debate de los aspectos tanto positivos como negativos de las diferentes alternativas tecnológicas complementarias a las listas de distribución por correo electrónico como Weblogs, wiki, mensajería instantánea, etc.

Como dato anecdótico destacar que en este X aniversario, el Servicio de Listas de RedIRIS ha recibido dos premios en la convocatoria internacional que lanzó L-Soft. Uno de ellos ha sido concedido a la innovación tecnológica del propio servicio (http://www.lsoft.se/news/choice5.asp) y el segundo al servicio OFER-TRABEC como mejor lista de distribución de anuncios dentro de su convocatoria internacional (http://www.lsoft.com/news/choicewinners.asp#five).

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Coordinador del Servicio de Listas

XIX Grupos de Trabajo

Los próximos días 26 y 27 de mayo tendrá lugar la celebración de las decimonovenas reuniones de coordinación de los Grupos de Trabajo de RedIRIS.

Este año los grupos se celebrarán con la colaboración de la Universidad de Málaga que nos acogerá en su magnífico edificio del Rectorado en el centro de la ciudad. De esta manera rompemos con lo que había venido a ser una suerte de tradición hasta ahora, de organizarlos exclusivamente en Madrid. Esperamos que esta nueva manera de organizar los grupos continúe en años sucesivos y nos permita acercarnos más a la realidad de las instituciones afiliadas y mejorar el contacto dentro de la comunidad.

Os sugerimos que consultéis periódicamente el programa (http://www.rediris.es/gt/gt2005/), que se irá actualizando a medida que la agenda de cada grupo vaya concretándose.

Como en ediciones anteriores, la inscripción se realizará a través del PER de cada institución, mediante el formulario de inscripción.

¡Nos vemos en Málaga!

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