Actualidad de Red

Actualidad de Red

• RedIRIS-II

El pasado 3 de junio entró en operación el último enlace que quedaba pendiente de los veintinueve que conforman la nueva topología de Red.

RedIRIS-II proporciona una infraestructura avanzada de comunicación entre todos los centros académicos y de investigación españoles, así como con el resto de la comunidad internacional. El acceso a la red está altamente distribuido. El backbone está basado en enlaces ópticos, utilizando lambdas con una velocidad de enlace de hasta 2,5 Gbps.

RedIRIS-II

Para proporcionar redundancia en la conexión de los centros conectados en Canarias se continúa trabajando en la provisión de un enlace que una los nodos de Tenerife y Las Palmas. Se trata de un enlace especial que no formaba parte del concurso realizado el pasado año.

• Nuevo equipamiento

Para soportar las capacidades y los nuevos servicios de esta red se ha procedido a la actualización del equipamiento de todos los nodos. El nodo nacional/central está formado por dos equipos Juniper T-320. Estos chasis están redundados de tal forma que no exista un único punto de fallo que pueda hacer caer a todo el equipo.

En cada uno de los nodos con velocidades de troncal 622 Mbps o 2,5 Gbps, se han instalado equipos Juniper M20 o M40e (en función del número de interfaces). Así, el nodo de Madrid y el de Valencia cuentan con equipos M40e y el resto, con equipos M20. Al igual que los anteriores T320, los equipos están redundados. En los nodos con enlaces STM-1 se han reutilizado los equipos Cisco 7507 y 7505 más avanzados de la anterior infraestructura de red.

• Conexión con GÉANT a 10 Gbps

A primeros de octubre, la conexión con la red pan-europea de investigación GÉANT pasará de los 2,5 Gbps actuales a **10 Gbps**. De esta forma, RedIRIS se confirma como una de las infraestructuras de red situadas a la vanguardia de las redes de investigación internacionales.

Este cambio en la conexión con GÉANT, la actual infraestructura de red nacional, así como el establecimiento de los accesos de las universidades y redes regionales en el orden de los Gbps, configuran una infraestructura global capaz de satisfacer las demandas de la comunidad científica española, en particular, de aquellos grupos de investigadores con unos requisitos más ambiciosos en cuanto a necesidad de ancho de banda, retardo limitado y servicios avanzados como IPv6 nativo, redes privadas de nivel 2...

• Conectividad IPv6

Durante el mes de marzo se configuraron los routers de GÉANT con IPv6 nativo en *dual stack*. A primeros de abril, RedIRIS estableció una conexión IPv6 nativa con GÉANT, siendo la **primera red de investigación** europea en establecer esta conexión.

A nivel nacional, esta configuración en *dual stack* se está desplegando por todos los nodos

del backbone. El protocolo de routing dinámico que se está utilizando es IS-IS. A nivel de acceso, son ya varias las instituciones que tienen una conexión IPv6 nativa, en concreto: CESGA (Red Autonómica de Galicia), CESCA (Red Autonómica de Cataluña), UPV/EHU (Universidad del País Vasco), UV (Universidad de Valencia), UAM (Universidad Autónoma de Madrid).

El objetivo es ir eliminando las conexiones con túneles y configurar las conexiones IPv4 actuales como IPv4/IPv6.

• Intercambios en ESPANIX

El pasado 17 de junio se configuró el intercambio de tráfico con Telefónica Data sobre la infraestructura de ESPANIX. Hasta este momento, la conexión entre ambas redes se soportaba sobre un enlace STM-1, enlace que había alcanzado la congestión en salida desde RedIRIS desde hacía algunos meses.

Con esta nueva conexión se ha conseguido liberar tráfico de este enlace STM-1 y la conexión entre RedIRIS-Telefónica Data ya no presenta cuello de botella.

La lista de proveedores con los que intercambiamos tráfico, a primeros de julio, es:

COMUNITEL	TISCALI
INTELIDEAS	FLAG TELECOM
DATAGRAMA	ARSYS
SARENET	SERVICOM 2000
COLT	NTT/VERIO
LAMBDANET	IBERCOM
ONO	TELEGLOBE
RETEVISION	TELEFONICA DATA
EASYNET	BT

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

XI reunión del TF-NGN

Los pasados 8 y 9 de mayo se celebró en Poznan (Polonia) la XI reunión del grupo de trabajo TF-NGN (www.dante.net/tf-ngn). En este grupo se trata sobre nuevas tecnologías de red con aplicación inmediata en la red europea GÉANT.

Un apartado a destacar fue la arquitectura de monitorización del rendimiento de una red, arquitectura que se va a crear en GÉANT. En principio, consiste en la definición de unos dominios de monitorización, donde cada uno de ellos disponga de diversos puntos de monitorización. Se deben intercambiar la información entre sí, lo que plantea el problema de evitar el retardo en el transcurso del intercambio.

Las medidas que se pretenden tomar son: *One-way delay*, *IP delay variance*, *one-way packet loss*, reordenación de paquetes y el RTT (*RoundTtrip Time*), así como la información generada utilizando los conocidos comandos *traceroute* y *ping*. Respecto a los equipos de medida, en un primer momento se utilizarán las cajas de medida de RIPE (www.ripe.net), así como equipamiento de NTP y GPS. Se guardarán datos durante cuatro semanas. Los primeros experimentos para monitorizar el rendimiento de GÉANT empezarán en septiembre.

Dentro de este apartado, se está trabajando, como ya se ha comentado en anteriores boletines, en la creación de un PERT (Performance Enhancement Response Team). Se trata de un equipo de personas encargadas de monitorizar la calidad de una red y resolver problemas de rendimiento. Este equipo, aún en fase inicial, estaría formado por técnicos de distintas áreas: expertos de red, administradores de sistemas y desarrolladores de aplicaciones.

Respecto a IPv6, destacar la presentación realizada por Laura Serrano (RedIRIS NOC) sobre los experimentos realizados con NTP e IPv6 (www.terena.nl/tech/task-foces/tf-ngn/presentations11.html). La presentación muestra los resultados de los experimentos llevados a cabo bajo tres escenarios: IPv4 nativo, IPv6 nativo y túneles IPv6 sobre IPv4. Como cabía esperar, se ha comprobado que los mayores retardos surgen con el uso de túneles; este mecanismo se desaconseja a la hora de montar una infraestructura con servidores de tiempo. Los mejores resultados se obtienen con IPv6 nativo, lo que pone de manifiesto la optimización de la nueva versión de NTP para este protocolo.

Continuando con IPv6, señalar la disponibilidad del Gnome Meeting con soporte total para IPv6 (www.gnomemeeting.org), la portabilidad se ha realizado dentro del marco de este Task-Force.

Por último, respecto a multicast, destacar que el Centro de Supercomputación y redes de Poznan ha desarrollado el MUVI (Multicast Visualization Tool, http://muvi.man.poznan.pl), herramienta

que basándose en SNMP descubre el árbol multicast. Otra herramienta con un propósito similar es el Multicast Beacon que ha sido retocado y mejorado (http://noc.man.poznan.pl/noc/index/strony, apartado de "Applications"). Sobre IPv6+Multicast, cuando se dispongan de versiones estables el próximo año, GÉANT soportará este servicio.

Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de Red

RIPE 45 en Barcelona

Esta reunión tuvo lugar en Barcelona los pasados 12-16 de mayo. Durante la misma asistimos a los siguientes grupos de trabajo:

- Routing WG

Donde se realizaron diferentes presentaciones principalmente relativas a BGP (Border Gateway Protocol) realizándose una evaluación del tiempo de convergencia de este protocolo y un análisis de los intervalos de anuncios BGP.

En relación con este grupo de trabajo merece la pena destacar una presentación respecto a SBGP (Secure Border Gateway Protocol), extensión de BGP que haciendo uso de IPsec y Public Key pretende resolver los problemas de seguridad asociados a BGP. https://www.ripe.net/ripe/meetings/ripe-45/presentations/ripe45-routing-sbgp/

- Database WG

Merece la pena destacar el hecho de que en un plazo de tiempo muy reducido se va a disponer de un nuevo mirror de ARIN. Se aprovechó la ocasión para informar de que los objetos "persona" que no fueran referenciados durante 90 días serían borrados.

Paralelamente se está trabajando para modificar el método de acceso y formato de entrada de la base de datos con objeto de mejorar el ya existente.

Se ha planteado la necesidad de crear un objeto 'organización', que recoja más detalladamente los datos y contactos de la misma. Y para facilitar lo más posible el contacto con los responsables de las redes, se está estudiando la posibilidad de hacer obligatoria la introducción del correo electrónico en el objeto persona.

- LIR WG

RIPE NCC va a montar una infraestructura de clave pública (PKI) para la comunicación con los LIRs.

Por otro lado, se ha revisado la política de asignación de direccionamiento tipo PI. A partir de ahora no se asignarán rangos inferiores a /24, para controlar el crecimiento desmesurado que están sufriendo las tablas de rutas en los últimos años.

Y ya de forma general, se ha planteado una reestructuración de los grupos de trabajo según la evolución de las necesidades. Desaparecerá el grupo NETNEWS, y el grupo LIR se dividirá en dos: Policy WG y RIPE NCC Services WG. Los grupos DNS y DNR se unirán en uno solo.

Otro tema planteado y que se probará en el próximo meeting será la celebración del meeting general anual junto con el RIPE meeting, debido a que últimamente han surgido temas de carácter general, pero que se relacionan directamente con los técnicos que se discuten en el grupo de trabajo.

Laura Serrano
Maribel Cosín
(laura.serrano@rediris.es)
(maribel.cosin@rediris.es)
Área de Red

I Jornadas sobre ENUM

El pasado 24 de junio, la Universidad Carlos III organizó las primeras jornadas sobre ENUM, a petición del Ministerio de Ciencia y Tecnología. El objetivo fue hacer un sondeo acerca del interés y conveniencia de montar este sistema en España. El resultado fue positivo y se espera que próximamente se cree un grupo de trabajo que estudie a fondo la forma de implantarlo.

Asistieron representantes del ministerio así como de las distintas organizaciones del sector que podrían estar implicadas: operadores de telefonía fija y móvil, ISPs, usuarios, fabricantes, registradores de dominios...

ENUM es un sistema basado en DNS para asociar números E.164 a otros números E.164, como números fax y móvil, sistemas de correo vocal, una dirección de telefonía IP, una dirección de correo electrónico, un sitio web u otros recursos o servicios que pueden

XI reunión del TF-NGN

RIPE 45 en Barcelona

I Jornadas sobre ENUM

I Jornadas sobre
ENUM

IX Reunión del
TF-CSIRT
de TERENA

identificarse a través del esquema de direccionamiento Internet denominado Identificadores Uniformes de Recursos ("URI").

Maribel Cosín
(maribel.cosin@rediris.es)
Área de Red

IX Reunión del TF-CSIRT de TERENA

Entrega tras entrega os vamos informando a través de este boletín de las reuniones que, tres veces al año, se vienen celebrando en distintas ciudades europeas dentro de Grupo de Trabajo de TERENA TF-CSIRT. Este grupo fue creado para fomentar la colaboración y cooperación entre equipos de atención de incidentes de seguridad (CERTs o CSIRTs) europeos y de países limítrofes.

Esta vez le toca el turno a la IX reunión del mencionado grupo de trabajo celebrada los días 29 y 30 de mayo en Varsovia (Polonia) que tuvo como anfitrión al Equipo de Atención de Incidentes local, CERT Polska/NASK.

Una de las cosas que más llama la atención en este Task Force (TF) es que la representación de equipos de seguridad (tanto comerciales, como gubernamentales o de entornos académicos) es cada vez mayor, y se está convirtiendo en un grupo multitudinario (ha pasado de contar con 30 representantes en la primera reunión celebrada en mayo de 2002 a cerca de 60 en la de mayo de este año). Esperemos que este incremento no suponga cortapisas al trabajo tan interesante que se viene realizando en este foro desde hace 3 años.

Como en anteriores reuniones, el primer día se centró la atención en aspectos relacionados con el modo de operación de distintos CERTs. Entre ellos Govcert.nl –CERT del Gobierno holandés–, ACOnet CERT –el recién formado Equipo de Atención de Incidentes de Seguridad de la NREN austriaca–, SWITCH-CERT y Telia CERT. Otro de los objetivos de estos seminarios es dar a conocer los proyectos y equipos de seguridad del país anfitrión. El Polish Telecom Abuse Team realizó una presentación sobre sus procedimientos de actuación. Además, entre los temas tratados durante este primer día, cabe destacar una presentación sobre técnicas para saltarse la protección de los firewalls y una descripción sobre el European Abuse Forum, foro que trata de establecer una red de comunicación europea entre ISPs para el manejo de incidentes de abuse.

Asimismo es interesante destacar la consolidación, como herramienta de atención de incidentes más ampliamente utilizada por los CERTs europeos, del RT o Request Tracker (http://www.bestpractical.com/rt), a la cual muchos equipos están incluyendo modificaciones que probablemente estén disponibles para la distribución oficial en un futuro cercano.

Todas las presentaciones realizadas en esta primera jornada se pueden encontrar en la página web del TF (http://www.terena.nl/tech/task-forces/tf-csirt/).

En cuanto a la reunión del Task Force propiamente dicha, se presentaron tres proyectos financiados por la EC y en los cuales están involucrados distintos equipos participantes:

- eCSIRT.net (European CSIRT Network, http://www.ecsirt.net/). Para el desarrollo de formatos de intercambio y herramientas que faciliten la compartición de información relativa a incidentes de seguridad entre CERTs europeos, y en el que IRIS-CERT está participando activamente junto a otros seis Equipos de Atención de incidentes como JANET-CERT o CERT-Renater.

- EISPP (Europen Information Security Promotion Programme, http://www.eispp.org/). Este proyecto cuenta con la participación de importantes empresas europeas como SIEMENS o ALCATEL. El principal objetivo es crear una Red Europea de CERTs que colaboren en la generación de los avisos de seguridad ofreciendo un mayor nivel de calidad y confianza.

- TRANSIT (Training of Network Security Incident Teams Staff, http://www.ist-transits.org/). Del que ya os hemos hablado en más de una ocasión en el Grupo de Trabajo de Seguridad, y que permite la impartición de cursos de formación para nuevas plantillas de Equipos de Seguridad.

También vale la pena destacar una proposición de la Comisión Europea para la creación de una agencia europea para la seguridad de la información y las redes (European Network and Information Security Agency, NISA), como una acción consecuencia del eEuropa Action Plan 2003. Esta agencia, con un presupuesto de

24.3M de euros y una plantilla formada por 31 personas, no tiene a fecha de hoy demasiado definidas las funciones que desempeñará ni los objetivos a cubrir, pero si se cumplen las fechas previstas comenzará a estar operativa en enero de 2004. Tan pronto tengamos más noticias sobre la marcha de esta iniciativa publicaremos una nota en este boletín.

En septiembre del presente año, estará disponible la guía recopilatoria de información legal en los distintos países miembros de la Unión Europea como resultado del proyecto concedido por la EC a un consorcio liderado por Rand Corporation y en el que están participando activamente miembros del TF-CSIRT. Todos tenemos la convicción que esta guía cubre un aspecto poco conocido por los equipos de seguridad y puede ser de gran ayuda a la hora de emprender acciones legales ante incidentes en Europa.

Para finalizar, entre los proyectos que se están llevando a cabo en el Task Force podemos destacar:

- Asistencia en el establecimiento de nuevos CERTs.
- Estudio de los requerimientos a cumplir por los sistemas de manejo de incidentes.
- Estudio de la viabilidad para la construcción de una infraestructura de backup para CERTs europeos.
- Por supuesto, diferentes líneas de colaboración entre el TF-CSIRT y otros foros de seguridad como FIRST.

La próxima reunión tendrá lugar los días 25 y 26 de septiembre de 2003 en Amsterdam (Holanda).

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

XI Reunión del TF-CSIRT en Madrid

La XI Reunión del TF-CSIRT que se celebrará, previsiblemente el 16 ó 25 de enero de 2004 estará organizada por IRIS-CERT en Madrid. Como os hemos comentado en algunas ocasiones, los seminarios asociados a la reunión del Task Force propiamente dicha se aprovechan para dar a conocer el *modus operandi* de distintos CERTs que trabajan en el Task Force, pero también para presentar los proyectos y equipos de seguridad del país anfitrión. Por este motivo os animamos a poneros en contacto con nosotros (cert@rediris.es), si estáis interesados en contribuir con vuestras presentaciones en esta reunión.

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

II Jornadas CERES

Bajo el nombre "Un cambio de Dirección: Acercando la Administración al Ciudadano", se celebraron, los pasados 7 y 8 de mayo de 2003 en la Real Casa de Moneda y Timbre, las II Jornadas CERES (http://www.cert.fnmt.es).

Estas Jornadas tuvieron como objetivo exponer nuevas aplicaciones realizadas por Organismos que se han adherido al sistema de certificación ofrecido por la FNMT-RCM (tecnología Ceres), al mismo tiempo que presentar productos de empresas colaboradoras en el desarrollo de algunas de estas aplicaciones.

Un apartado que despertó bastante interés entre los asistentes fue el DNI electrónico, que aseguraron será una realidad en el próximo año, aunque no se ofreció ningún detalle sobre su implementación.

El uso de la firma electrónica conlleva importantes beneficios, tanto para la propia Administración como para los ciudadanos (ahorro en los gastos administrativos, reducción y automatización de tareas, acercamiento al ciudadano, eliminación de desplazamientos y tiempos de espera, etc...). Por esta razón y en este momento la FNMT-RCM se ha constituido como una de las Entidades de Certificación (o Tercera Parte de Confianza) con más renombre e importancia en España. Muestra de ello son la multitud de servicios que actualmente admiten firma electrónica basada en la tecnología Ceres (tanto en organismos de la Administración general, como autonómica o local):

- **Oficina virtual del Ministerio de Economía.** Presentación telemática de recursos y reclamaciones, compra-venta de Deuda Pública, cumplimentación de los datos del Censo de población y vivienda que elabora el INE, etc..
- **Agencia Estatal de la Administración Tributaria.** Presentación de declaraciones-

IX Reunión del TF-CSIRT de TERENA

XI Reunión del TF-CSIRT en Madrid

II Jornadas CERES

II Jornadas
CERES

Actualidad en
legislación sobre
firma electrónica
en España

autoliquidaciones, solicitud de cambio de domicilio fiscal, información on-line, etc..
- **Ministerio de Sanidad y Consumo**. Servicio de Gestión de Formación Sanitaria Especializada – MIR por Internet, etc.
- Envío de las disposiciones a publicar en los **Boletines Oficiales del Estado** de las distintas Comunidades.
- El **Ayuntamiento de Madrid** permite la consulta de inscripción en el Padrón Municipal.
- Etcétera.

Los certificados que emite la FNMT-RCM son de uso general y gratuitos, se pueden utilizar para la comunicación con cualquiera de aquellos organismos que hayan firmado convenio con la FNMT-RCM.

En la actualidad existen más de 300.000 ciudadanos certificados, que los utilizan en una amplia variedad de servicios en más de 30 entidades de las diferentes Administraciones.

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

Actualidad en legislación sobre firma electrónica en España

Como algunos de vosotros ya sabréis, el actual Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica será sustituido en breve por un nuevo Anteproyecto de Ley (26/julio/2002), elaborado por el Ministerio de Ciencia y Tecnología, en estrecha colaboración con los Ministerios de Administraciones Públicas, Economía, Interior y Justicia. Dicho Anteproyecto ha sido remitido ya a los servicios jurídicos del Estado para garantizar su ajuste constitucional.

En este nuevo texto están incluidas las modificaciones debidas al desarrollo tecnológico no tenidas en cuenta en el Decreto-Ley original. Entre las novedades más importantes incorporadas en la nueva redacción se encuentran:

- El Decreto-Ley hacía una definición muy estricta de Prestador de Servicios de Certificación (PSC), quedando extendida la definición de PSC en el nuevo texto.
- Se incluye el uso de atributos en los certificados (por ejemplo, el de representación).
- Se agiliza la obtención de sellos de calidad para los PSC.
- Se revisa la terminología y la sistemática del texto con vistas a facilitar su comprensión y aclarar los conceptos contenidos.
- Se amplia la titularidad de los certificados (por ejemplo, se contempla la emisión de certificados de personas jurídicas).
- Se avanza en el concepto de autorregulación de la industria, otorgando mayor libertad y protagonismo al sector privado
- Se elimina el registro obligatorio de PSC previsto en el Real Decreto-Ley de 1999 (existirá una página web en el Ministerio con un listado voluntario de PSC y sus sellos de calidad).
- Se establece un marco básico para la creación del Documento Nacional de Identidad electrónico.
- Se concentra y da importancia a los procesos de identificación de usuarios.

Además, el pasado mes de mayo se hacía pública la Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria. Mediante esta Orden, la Agencia Tributaria va a permitir el uso de las firmas digitales, basadas en criptografía de clave pública, realizadas mediante certificados de clave pública expedidos por otros PSC reconocidos distintos a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, siempre y cuando se cumplan determinados estándares y condiciones de publicidad.

Esta orden permite la liberación de la firma electrónica y abre una abanico de posibilidades muy interesantes para los PSC españoles (como el caso de RedIRIS con su RedIRIS-PKI). Están por ver todavía las condiciones y estándares requeridos, pero intentaremos por nuestra parte mantener las reuniones pertinentes con el fin de conocer las posibles actuaciones, dando cuenta de cualquier información que llegue a nuestras manos a través de las listas de distribución y de este boletín. Para más información: (http://www.rediris.es/cert/links/legal.es.html)

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

Grupo de Trabajo IRIS-CERT

Actualidad de correo electrónico

Grupo de Trabajo IRIS-CERT

En mayo de 2003 tuvieron lugar los grupos de trabajo de primavera y, dentro del grupo IRIS-CERT, se presentó un resumen de las actividades del grupo desde noviembre 2002. A continuación pasamos a entrar un poco en detalle

- Informe de incidentes:

  - Durante el periodo noviembre 2002-abril 2003 se atendieron un total de 1.171 incidentes, lo que refleja un incremento del 37% respecto al mismo periodo del año anterior. De estos, un 91% corresponde a incidentes en los que se ha visto implicada una institución afiliada a RedIRIS y en él se han visto implicados proveedores de Internet bajo el dominio ".es". De los primeros, el 66% corresponden a incidentes originados en una institución afiliada, el 30% la tienen como destino y el 3% restante tienen origen y destino en instituciones afiliadas a RedIRIS. A pesar del aumento en número, los porcentajes antes comentados se mantienen respecto a los mismos periodos del año anterior, lo que refleja un mismo comportamiento en los modos de notificación de incidentes. Dentro de estos números no se contemplan ni incidentes relativos a SPAM de correo, ni los relativos a problemas de copyright en contenidos detectados en ciertas máquinas. Esto se debe a que han quedado excluidos como incidentes a tratar por el CERT de RedIRIS, el primero de ellos por ser gestionado por el responsable de correo, y el segundo porque no se considera dentro de las funciones de IRIS-CERT el "control" de contenidos con problemas de copyright dentro de las instituciones afiliadas.

  - En cuanto a la tipología, siguen dominando los incidentes debidos a escaneos, esto en gran parte se debe a que es el primer síntoma típico de una máquina atacada, que normalmente saca a la luz otros problemas más serios. El segundo tipo en número, corresponde a "gusanos", que al igual que años anteriores, sigue siendo la mayor pesadilla para todas las organizaciones afiliadas.

  - Como puertos más escaneados en el periodo noviembre 2002-abril 2003 destacan:

    - 80/tcp: siguen los gusanos "CodeRed" y "Nimda", así como ataques a servicios WebDAV.
    - 137-138-139-445: Servicios relacionados con Netbios.
    - 443/tcp: gusano "Slapper" atacando a mod_ssl.
    - 1434/tcp: gusano "Slammer" atacando SQL Server.

- Foros Nacionales (ISPES):

  - Encargado a lo largo de los tres últimos años de coordinar los esfuerzos en materia de SPAM e incidentes de seguridad, entre los distintos ISPs que operan en España y RedIRIS. Después de la última reunión (mediados de febrero), se ha acordado su integración en los grupos de coordinación que funcionan dentro de ESPANIX. Asimismo, se acordó la integración dentro del futuro grupo, tanto a proveedores de red, como de servicios.

- Foros Internacionales:

  - Dentro del grupo TF-CSIRT de Terena (http://www.terena.nl/tech/task-forces/tf-csirt/), continúan abiertas líneas de trabajo tales como: desarrollo de un nuevo CSIRT para la Unión Europea y países del Este, estudio de procedimientos y requerimientos funcionales comunes para las herramientas de gestión de incidentes, estudio sobre infraestructuras de backup, cursos para nuevos miembros de CERTs,... Como novedad importante el nuevo objeto IRT dentro de RIPE que permite localizar grupos de gestión de incidentes para una determinada red.

- Novedades:

  - Se presentó el nuevo objeto IRT en la base de datos de RIPE, en el cual queda reflejada la información relativa a grupos de atención de incidentes, que están asociados a las distintas redes incluidas en RIPE. Como ejemplo, IRT-IRIS-CERT, objeto IRT en el que aparece información relativa a IRIS-CERT.

Rodrigo Castro
(rodrigo.castro@rediris.es)
Equipo de Seguridad IRIS-CERT

Actualidad de correo electrónico

• I reunión IRIS-MAIL por VRVS

Actualmente el Grupo IRIS-MAIL (Coordinación del Servicio de correo electrónico de la

Actualidad de correo electrónico

comunidad RedIRIS) cuenta con unos 265 postmasters pertenecientes a prácticamente la totalidad de instituciones afiliadas con sus datos mantenidos y actualizados desde 1993. Lo que une a todo este colectivo es el mundo del correo electrónico y el servicio que se presta a los usuarios de cada institución. El grupo se coordina a través de dos reuniones presenciales anuales (mayo y noviembre) y una lista de distribución para el intercambio permanente de información. Se trata de resolver dudas, se comentan noticias relacionadas con el servicio, se lanzan y debaten iniciativas, se recomiendan pautas, etc. Está claro que las reuniones presenciales (40-50 personas) son más productivas, pero llegan a menos gente que la lista de distribución. Con la lista aunque es más compleja la interacción y toma de decisiones, es útil para la resolución puntual de problemas y la ágil distribución de información o alertas.

Aunque esto pudiera ser suficiente, se pensó en la posibilidad de organizar reuniones periódicas con un sistema de videoconferencia estable y consolidado como es VRVS (*Virtual Rooms Videoconferencing System*). La idea era explotar al máximo las posibilidades que la Red ofrece con el fin de enriquecer la productividad y unión de este Grupo IRIS-MAIL y las reuniones periódicas por videoconferencia VRVS van en esta línea.

Los servicios de comunicaciones de las instituciones se han esforzado en difundir a sus usuarios la tecnología VRVS (http://www.vrvs.org), pero nunca se había pensado en ella como una herramienta de uso cotidiano. La primera reunión VRVS de IRIS-MAIL (I avIRIS-MAIL) se celebró el día 3 de junio de 2003 en la Sala Águila de 11.00 a 12.30 h. Los temas de la agenda de esta primera reunión fueron:

- MailBackup: Aspectos del Servicio y posibles alternativas
- Perspectivas de RACE (Red Académica de Correo Electrónico http://www.rediris.es/mail/race/)
- ¿Es adecuada la etiqueta "Nivel Básico" como nivel RACE?
- Documento descriptivo del servicio de correo electrónico

Realmente el temario de la agenda no fue lo más importante de esta reunión, sino la propia experiencia y su evaluación como complemento de futuro. Como resumen de los temas tratados, lo más destacable fue el apoyo unánime a la continuidad del Servicio MailBackup de RedIRIS operativo desde 1996 con la introducción de algunas modificaciones (http://www.rediris.es/mail/mailbackup/).

Cuando se convocó esta reunión se estimó una asistencia de 10 personas, aunque sin embargo la asistencia final fue de unas 50 personas, 15 en audio-vídeo y unas 35 en audio. Como conclusiones de esta primera experiencia podemos enumerar las siguientes:

- Que el debate fue dinámico y se demostró la validez de la herramienta para organizar posteriores eventos, aunque hay que mejorar.
- Organizativa y técnicamente la reunión fue buena. No se hicieron pruebas en la reunión, se respetó el turno y el audio y el vídeo eran de una calidad aceptable
- La excesiva gente conectada sólo en audio, por lo que si bien la calidad era buena se pierde contacto en este tipo de eventos.
- La necesidad de fomentar este formato para facilitar la compra e instalación de material adecuado para sesiones de videoconferencia: auriculares, cámara, tarjeta, etc.
- Hay que mejorar el aprendizaje para manejarse con este tipo de reuniones tanto por parte del moderador como de los asistentes
- El conocimiento de este tipo de herramientas facilita su divulgación a los usuarios internos.

El formato de esta primera reunión fue del tipo debate con moderador y cabe la posibilidad de hacer presentaciones cortas con transparencias. También se han puesto en marcha reuniones periódicas entre los miembros que forma parte del Grupo de Evaluación RACE (GA.IRIS-MAIL).

• IV Reunión extraordinaria IRIS-MAIL

El 7 de mayo se desarrolló una reunión en las instalaciones del CSIC en Madrid con el objeto de abordar dos de los actuales Proyectos IRIS-MAIL de RedIRIS: RACE (Red Académica de Correo Electrónico) y PUAS (Plataforma Unificada AntiSpam). A esta reunión asistieron 12 personas de varias universidades y tuvo lugar un día antes que los Grupos de Trabajo de Primavera. Se organizó un pequeño grupo con el fin de que fuera más dinámico y productivo y poder contar así con más tiempo.

Por la mañana se trató en profundidad el tema de PUAS y se analizó el desarrollo del piloto que comenzó en enero de este mismo año. Durante esta fase piloto, PUAS ha demostrado que es una iniciativa viable, efectiva y muy útil a la Comunidad RedIRIS y que habría que ponerla en producción. El sistema actual de PUAS se ha mostrado inestable para empezar a ser operativo y con

garantías. El actual desarrollo consume un gran cantidad de recursos cuando el número de denuncias es alto durante un periodo de tiempo, por lo que se propuso un nuevo desarrollo completo. Para ello se evaluó una serie de acciones que pasan por redactar unas especificaciones técnicas de lo que se quiere de esta nueva versión de PUAS y ver qué institución podría desarrollarlo. En principio la dirección de RedIRIS apostó por aportar una cantidad económica para cubrir los gastos del desarrollo de este Proyecto.

En paralelo se propusieron muchas ideas para incorporar a PUAS y fueron aprobadas ciertas actividades hasta llegar a la fase final de operación; algunas plantean seguir usando el actual sistema. Estas actividades son:

- Diseñar la estructura del portal informativo de PUAS del que hasta ahora no hay documentación.
- Crear los mecanismos para incrementar el número de denuncias y facilitar la labor a los usuarios finales de cada institución. En esta línea se presentó un desarrollo de Pablo Fernández Baladrón que recoge las denuncias internas, las comprueba y reenvía a RedIRIS para su procesamiento.
- Instaurar un plan de actuación para evaluar la aceptación de PUAS dentro de las instituciones. Se propusieron encuestas y documentación informativa.
- Organizar un grupo distribuido de gestión de PUAS para la atención de quejas, negociación con proveedores, información....

Seguiremos informando sobre el estado y evolución de PUAS a través de IRIS-MAIL.

Por la tarde se debatió el tema de RACE, se repasaron los criterios, la política el mecanismo, etc., y se decidió ponerlo en marcha cuanto antes como así ha sido. Se cerraron algunos temas pendientes acerca de los criterios, normativa de evaluación, etc.

• Actualidad de RACE

Después de un año de desarrollo y maduración, la iniciativa RACE (Calidad en el Servicio de Correo Electrónico http://www.rediris.es/mail/race) empezó a funcionar a mediados de mayo de este año. Se organizó y reforzó un pequeño grupo de postmasters para desarrollar este proyecto, del que forman parte en la actualidad las siguientes personas:

Pedro R. Benito	UBU
José L. Hernández	UC3M
Pascual Pérez	UNIZAR
José M. García	UPCO
Fernando Limón	FI-UPM
Víctor Hernández	UPO
Pablo Fdez. Baladrón	UVIGO
Jesús Sanz de las Heras	RedIRIS

El trabajo durante este mes ha sido bastante intenso, por lo que se agradece mucho la colaboración de los compañeros mencionados. A finales de mayo empezaron a llegar los primeros formularios RACE y se acometieron las evaluaciones. Se definió y ajustó el protocolo de actuación para facilitar las tareas de evaluación y garantizar sus resultados. Este protocolo lleva incluidos documentos, mensajes tipo, scripts de chequeo, formatos informes, etc. (http://www.rediris.es/mail/race/cata.html) También se han diseñado logotipos del Servicio para cada uno de los niveles RACE. Recordamos que en caso de superar alguno de los niveles:

- Se generan y envían informes técnicos sobre la evaluación.
- Se envían los logotipos RACE para colocarlos en páginas web institucionales y un certificado.
- Se da de alta a la institución en el catálogo RACE.

En caso de que alguna institución no supere los criterios, se enviará un informe técnico sobre el problema detectado. Hasta ahora han sido evaluadas las universidades de Burgos, Almería, Autónoma de Madrid, Carlos III, Pablo Olavide de Sevilla y el European Software Institute.

En definitiva, la evaluación RACE está siendo un trabajo riguroso y enriquecedor acerca de la calidad del servicio de correo de cada institución, una especie de auditoría de los mismos, un análisis crítico pero amigable por parte de técnicos de otras instituciones.

• Documento descriptivo del Servicio de Correo Electrónico (DOCE)

Desde hace tiempo en IRIS-MAIL se viene insistiendo en la necesidad de un documento o Política de Uso del Servicio, pero los problemas institucionales para su ejecución han sido siempre grandes. Ahora RACE ha incorporado un criterio imprescindible de Nivel Básico que obliga a disponer de un documento descriptivo del Servicio de correo electrónico.

Documento público describiendo el Servicio de Correo Electrónico. ***Explicación****: Se ha considerado que una descripción del servicio es imprescindible para que usuarios externos y*

Actualidad de correo electrónico

Actualidad de correo electrónico

sobre todo internos tengan conocimiento del Servicio que se les ofrece.

La experiencia actual de las evaluaciones RACE nos han demostrado que aunque las instituciones han ido documentado este tema, no es suficiente y existe un exceso de información acerca de configuraciones y servicios. Realmente este criterio RACE es uno de los más problemáticos para superar el Nivel Básico.

Para ayudar a las instituciones, el Grupo de Apoyo IRIS-MAIL ha redactado un documento genérico y descriptivo del Servicio de Correo Electrónico (DOCE) que ayudará a evaluar y definir los aspectos mínimos a tener en cuenta en la elaboración de este documento. A partir de ahí será labor de cada institución la redacción final del suyo propio (http://cvu.rediris.es/bscw/bscw.cgi/d378243/ServicioCorreoE.PDF). El documento (DOCE):

- Avala y apoya el trabajo de los responsables del Servicio.
- Informa a los usuarios de las características del Servicio.
- Informa de lo que se hace con un mensaje de correo-e desde que entra por Internet hasta que se deposita en el buzón y viceversa.
- Delimita las responsabilidades de cara a los usuarios internos y externos.
- Informa del correcto uso del servicio.

y por otra parte:

- Debe ser público y divulgado a todos los usuarios actuales y a los nuevos que se incorporen en el futuro para hacer uso del Servicio.
- Debe ser sencillo y claro para usuarios con otro tipo de formación y que usan el correo electrónico como herramienta de trabajo.
- Debe ser conciso y preciso en las necesidades de conocimiento de los usuarios.
- No sólo debe ser una descripción de configuración de los correspondientes clientes de correo.
- Debe ofrecer una panorámica técnica general del servicio de correo electrónico de una universidad además de informar de los servicios y utilidades de correo que se ofertan a la institución.

Los aspectos que se han considerado en este documento como imprescindibles son:

- Datos de contacto del Servicio
- Responsabilidades del Servicio
- Descripción básica del Servicio
- Procedimientos de usuarios
- Modos de acceso al buzón de correo
- Política Antivirus del Servidor de correo
- Política AntiSpam
- Política de MailBackup
- Política de Logs
- Limite del tamaño de mensajes o de buzón
- Puntos de contacto
- Recomendaciones para el correcto uso del correo electrónico

• Grupo sobre correo electrónico en Espanix

RedIRIS siempre ha tratado de crear foros de coordinación con los proveedores comerciales españoles como una de las mejores formas para mejorar la calidad de los servicios de red y proteger a la propia comunidad de posibles incidentes. Como se comentó en el Boletín de RedIRIS núm. 64, y a propuesta de RedIRIS la Asociación Espanix aprobó en su Junta directiva del 13 de febrero de 2003 el desarrollo de actividades llamadas "non-core" (actividades diferentes de las propias de un punto neutro de intercambio de tráfico). El primer grupo formado ha sido el ESPX-MAIL (http://www.rediris.es/list/info/espx-mail.es.html) cuyo coordinador es personal de RedIRIS y tiene como objetivo la coordinación entre proveedores de aspectos relacionados con el correo electrónico.

Después de un periodo inicial de divulgación entre los socios del Espanix, se alcanzó un nivel mínimo de 20 proveedores interesados y se pasó a una fase de desarrollo de actividades. La primera actividad fue consensuar un documento de buenas prácticas frente al spam (http://cvu.rediris.es/bscw/bscw.cgi/d262201/PolESPX-MAIL), definiendo unos criterios mínimos necesarios para evitar y gestionar incidentes de este tipo en el servicio de correo electrónico de los dominios y redes responsabilidad de los prestadores de servicios adheridos a la iniciativa ESPX-MAIL. Una política común que responde a la voluntad de contribuir en la generación de unas normas de conducta que faciliten el buen uso de Internet sobre la base del autocontrol y con el respeto más absoluto a la libertad de expresión y a la legislación vigente.

Este tipo de grupos, con proveedores comerciales y objetivos comunes, necesita de una gran dosis de confianza para ser productivos. El perfil de los participantes es técnico y un problema que hemos encontrado con los proveedores grandes es que los que tienen el poder de decidir tienen poco

conocimiento de los problemas reales, y los que conocen dichos problemas no pueden tomar decisiones al respecto. En consecuencia, estamos tratando de que los representantes del grupo tengan cierto poder de decisión. El grupo está en una fase incipiente y esperemos que en un futuro próximo surjan los primeros resultados de esta iniciativa

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

Reunión del grupo TF-AACE

El grupo TF-AACE (http://www.terena.nl/tech/task-forces/tf-aace/), englobado dentro de los grupos de trabajo de Terena, coordina y desarrolla actividades relacionadas con infraestructuras de autenticación y autorización de servicios en Internet. Se presta especial atención a los casos relacionados con: el acceso a recursos internos a una organización por parte de usuarios móviles, compartición de recursos entre organizaciones y acceso a recursos externos (proveedores de contenido) por parte de usuarios de una organización.

El pasado 18 de mayo, aprovechando la semana de conferencias de Terena, se organizó la reunión del grupo en Zagreb y se trataron los siguientes puntos:

- En primer lugar se presentó el informe realizado por Diego López de las respuestas al cuestionario "PKI Application and Requirement", que se ha utilizado como base de evaluación de la implantación de la PKI en las organizaciones. Como principales conclusiones, el informe destaca: la escasa participación a la hora de contestar el cuestionario (achacado a su poca difusión y al poco soporte para rellenarlo), la utilización de la tecnología de PKI, casi exclusivamente, para servicios de correo y web y la poca implicación de las organiza-ciones en proyectos GRID. En segundo lugar, se presentó el informe "Investigate the Different Approaches to inter and extra-Institutional A&A, Analyzing the Alternatives in Architecture and Protocols" realizado por Thomas Lenggenhager. En él se presenta una visión general y una evaluación de los sistemas de autenticación y autorización: AAI (SWITCH) A-Select (SURFNET), PAPI (RedIRIS), FEIDHE (Finnish Higher Education Identification), Grid, GSI y Shibboleth.

El 15 de abril en Amsterdam tuvo lugar una reunión entre organizaciones que están desarrollando soluciones AA. Se trató la problemática de la integración de las soluciones existentes (o nacientes) y la compatibilidad entre ellas. Otro de los aspectos que se discutieron fue el modo de establecer confianza entre instituciones a la hora de compartir recursos y la conveniencia de utilizar "federaciones bajo una misma política" para conseguirla. También se llegó a la conclusión de establecer un protocolo para la comunicación entre los distintos elementos que intervienen en un sistema AA acordándose tomar como base SAML.

Se estableció una serie de nuevas líneas de trabajo para conseguir centrar los esfuerzos en la consecución de una solución AA homogénea. Estas líneas son:

- Definición de una arquitectura como base de la integración de diferentes soluciones AA.
- Definición de esquemas LDAP y atributos comunes que permitan la compatibilidad entre organizaciones a la hora de definir reglas de acceso a recursos.
- Desarrollo de soluciones que permitan modelos de confianza entre instituciones. Como punto de partida, una iniciativa que contempla el mantenimiento por parte de Terena de un fichero que englobe los certificados raíz de las distintas redes I+D europeas.
- Recopilación y distribución de toda la información relativa a soluciones AA, tanto en funcionamiento como en vías de desarrollo.
- Presentación de una iniciativa para que Terena albergue un repositorio de certificados raíz, correspondientes a las CAs de las diferentes redes I+D europeas. La base de esta iniciativa es tratar de mantener en un fichero dichas CAs, de forma que siendo importado por un cliente, se consiga confianza en las estructuras de certificación de las respectivas redes académicas. Como punto de partida, Chelo Malagón y Diego López han redactado una política (no definitiva) que regula el funcionamiento de dicho repositorio.

Rodrigo Castro
(rodrigo.castro@rediris.es)
Equipo de Seguridad IRIS-CERT

Actualidad de correo electrónico

Reunión del grupo TF-AACE

Grupo de Trabajo sobre Middleware

Reto de análisis forense

Grupo de trabajo sobre Middleware

La tercera reunión del grupo de trabajo sobre Middleware (IRIS-MIDDLEWARE) que agrupa las iniciativas –hasta ahora dispersas– en esta área se celebró en Madrid el pasado 9 de mayo. La reunión se centró en aspectos relacionados con directorios, esquemas de metadatos y mecanismos de autenticación y autorización.

En lo referente a los directorios, se presentó la segunda guía básica sobre LDAP: "Recomendaciones acerca de estructura y nombres para entradas en servidores de directorio". En ella se ha pretendido agrupar las diferentes posturas existentes a la hora de estructurar un directorio de una manera común que permita desarrollar aplicaciones que interoperen de forma simple.

La guía propone un cambio en la estructura de las entradas. Hasta ahora se ha creado el directorio como reflejo de la estructura organizativa de las instituciones; es decir, un árbol jerárquico con los mismos niveles organizativos. A partir de ahora se apuesta por el uso de metainformación en las entradas del directorio para soportar esta estructura existente en los centros. Con ello obtenemos un directorio más plano en el que los DNs de las entradas son muy cortos e independientes de la localización física de la entrada. Asimismo, plantea el uso de interfaces de navegación inteligentes que basen la navegación en atributos especiales. De esta forma podremos ofrecer múltiples vistas virtuales diferentes del mismo directorio. Para ello se ha definido el esquema COPA.

Se ha definido también el esquema IRIS, con atributos específicos de nuestra comunidad tales como el uso de dos apellidos (atributos sn1 y sn2), lo que evitará la sobrecarga del atributo cn y simplificará enormemente la realización de interfaces de usuario.

También se presentó CATRE (Clasificación de Áreas Temáticas de REdIRIS). Clasificación basada en la relación de la UNESCO que usa codificación en formato COPA y que permite clasificar cualquier entrada del directorio en una/varias áreas temáticas añadiendo un campo a la entrada.

La última parte de la sesión estuvo dedicada a las infraestructuras de autenticación y autorización, lo que en nuestro entorno quiere decir hablar de PAPI. En ella presentamos la última versión de PAPI (1.2.1) y sus principales características. También anunciamos el acuerdo para el desarrollo de la versión 2 de PAPI con la Universidad de Málaga y la propuesta que ha hecho Athens para interconectar PAPI y sus sistemas de acceso.

Referencias

Grupo de trabajo sobre middleware:
http://www.rediris.es/gt/middleware/coord/gt2003/
Guías básicas LDAP:
http://www.rediris.es/ldap/doc/gb/
Esquemas LDAP:
http://www.rediris.es/ldap/doc/esquemas/
COPA: http://www.rediris.es/ldap/copa/
CATRE: http://www.rediris.es/rtr/catre/
PAPI: http://papi.rediris.es/
Athens: http://www.athensams.org/

Javier Masa
(javier.masa@rediris.es)
Responsable del Servicio de Directorio

Reto de análisis forense

El análisis de equipos previamente atacados es una de las actividades que más experiencia y tiempo requieren a la hora de analizar los efectos de una intrusión en un sistema informático.

Este análisis es fundamental para determinar las acciones realizadas por los atacantes, qué ficheros modificaron o instalaron y las posibles intenciones por las cuales se accedió al sistema.

Hasta hace unos pocos años se realizaba de forma no sistemática, basada sobre todo en la experiencia en la administración del sistema y orientada a eliminar las puertas traseras dejadas por los atacantes y las posibles vulnerabilidades que permitieron la intrusión, por lo que muchas veces se modificaban ficheros y se eliminaba información que pudiera ser usada después en acciones legales contra los atacantes.

En los últimos años han ido surgiendo diversas herramientas, como TCT (http://www.porcupine.org/forensics) y Task (http://www.sleuthkit.org), que han facilitado ir definiendo una metodología de análisis que permite conservar las evidencias y realizar un análisis más correcto de los equipos atacados.

Sin embargo, el problema que surge ahora es la dificultad de tener elementos de "muestra", que sirvan para formar a los administradores de

sistemas y seguridad en el uso de estas herramientas, de forma que puedan realizar correctamente su labor una vez que se detecta una intrusión informática.

Conscientes de estas dificultades, desde el grupo de seguridad de RedIRIS, IRIS-CERT, en colaboración con un grupo de expertos informáticos y empresas de seguridad especializadas, se ha promovido la realización de un reto de análisis forense que se desarrollará durante este verano.

El objetivo de este reto es analizar la información de una máquina previamente atacada (un sistema Linux perteneciente a la red de máquinas trampas de RedIRIS http://www.rediris.es/cert/ped), y contestar a una serie de preguntas relacionadas con esta intrusión.

Para más información sobre este reto, así como para obtener la copia de los datos del equipo atacado, se puede consultar la información que aparece en http://www.rediris.es/cert/ped/reto. Las conclusiones se comentarán en las próximas jornadas técnicas a celebrar en noviembre en Palma de Mallorca.

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

15 Reunión anual de FIRST

Del 22 al 27 de junio se celebró en la ciudad canadiense de Ottawa el congreso anual de FIRST (Forum of Incident Response and Security Teams http://www.first.org). Estas reuniones surgieron en 1989 como foro de seguridad a nivel mundial donde se tratan los diversos aspectos de la gestión de incidentes.

Durante los cinco días que dura la conferencia se combinan tutoriales con jornadas de ponencias y también se celebra la reunión general de los miembros de FIRST.

Los tutoriales de este año estuvieron centrados en los siguientes aspectos:

- Análisis Forense de Redes (Network Forensic) centrado en el uso de herramientas de análisis de tráfico de red para la detección de intrusiones. Se trató el empleo de la información de flujos generada por los router (netflow) con herramientas de dominio público y en concreto de una herramienta llamada Argus, que permite obtener una información similar a nivel de red local.

- La creación de un grupo de Seguridad, centrado primordialmente en aquellas organizaciones que no disponen de grupo de gestión de incidentes y que precisan formarlo.

- La creación de grupos de seguridad nacionales, donde se contó con la participación de representantes de los grupos de Seguridad Aus-CERT (Australia), GOVCERT.NL (Holanda) y CERT/CC, tratándose los problemas de creación de un grupo de coordinación de ámbito nacional que realice una función más proactiva de coordinación de alertas entre diversos grupos nacionales y ante nuevos problemas de seguridad.

- Los avisos de seguridad, tanto desde la perspectiva de un grupo de seguridad independiente como desde el enfoque de un fabricante, desde que se descubre un problema de seguridad hasta que se puede hacer pública la solución.

Los tres días siguientes se centraron en diversas ponencias que trataron aspectos relacionados con la seguridad en Internet:

- Worst Fears. Tratamiento de la evolución de los distintos gusanos que han ido surgiendo en los tres últimos años contra diversas plataformas y características que debería tener un gusano para colapsar Internet. Algunas de ellas se están viendo reflejadas en los últimos gusanos que han ido surgiendo.

- eCSIRT.net. Proyecto cofinanciado por la Unión Europea, en el que participa RedIRIS, destinado al intercambio de información sobre incidentes de seguridad entre los diversos participantes y a la creación de una red de alerta temprana ante problemas de seguridad.

- RTIR. Las modificaciones hechas en el programa de gestión de incidencias Real Tracker, para permitir manejar incidentes de seguridad. En la actualidad este programa está en estudio para adaptarlo a la gestión de incidentes de seguridad dentro de IRIS-CERT.

- Incidentes de privacidad en la información. Estos problemas de seguridad suelen ser especialmente problemáticos al tratar con información sensible (acceso a información médica, datos bancarios y de crédito, etc.). En

Reto de análisis forense

15 Reunión anual de FIRST

15 Reunión anual de FIRST

Internet2 Member Meeting

AA Developer Workshop

esta ponencia se realizó un estudio de algunos de los incidentes que ha habido de estas características y de los motivos que los causaron.

- Empleo de Redes Trampas en el entorno de grupos de seguridad para la obtención de información sobre las amenazas y ataques más frecuentes contra una red.

- Fire your Firewall (despida a su cortafuegos), donde se trataron los problemas que presenta el enfoque tradicional de instalación de un cortafuegos perimetral como único elemento de seguridad en una organización y la complejidad que introduce en determinados sistemas como, por ejemplo, las soluciones de videoconferencia.

- Sobre los sistemas de detección de intrusión. Destacar una ponencia que hubo sobre el empleo de herramientas de lógica difusa (fuzzy) a la hora de evaluar los diversos parámetros de una red y detectar cuándo se ha producido una intrusión en un sistema.

La política existente dentro de FIRST es hacer pública la información de las ponencias presentadas al año de realizarse el congreso, pudiéndose consultar la información de años anteriores (http://www.first.org/events/progconfs). Mientras tanto, los miembros de la comunidad académica pueden contactar con el grupo de seguridad de RedIRIS si necesitan más información sobre esta conferencia.

Por último, destacar que la próxima reunión se celebrará en Hungría y el plazo de solicitud de ponencias se abrirá en septiembre.

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

Internet2 Member Meeting

Durante los días 8 al 11 de abril se celebró en Arlington (EEUU) el Spring 2003 Internet2 Member Meeting, en el que una delegación de RedIRIS participó activamente en las áreas de middleware (dentro del MACE) y servicios multimedia.

En cuanto al middleware, como aspectos más destacados cabe resaltar los avances en la integración de las infraestructuras de autenticación y autorización (PAPI en RedIRIS y Shibboleth en Internet2), el acuerdo para colaborar en la definición de arquitecturas que permitan la integración del acceso a recursos cuyo acceso esté protegido por este tipo de infraestructuras, los esfuerzos por internacionalizar el esquema común eduPerson, y la implicación del grupo que trabaja en tecnologías de directorio en RedIRIS en la iniciativa SAGE, orientada a la definición, gestión y uso de grupos por medio de la federación de servidores LDAP.

En cuanto a los servicios multimedia, participamos en los grupos relacionados con la iniciativa GDS, anunciamos la apuesta clara de RedIRIS por VRVS y aceptamos la propuesta de compartir con toda la comunidad académica internacional los contenidos del curso virtual de VRVS que se describen en este número.

Referencias

MACE: http://middleware.internet2.edu/MACE/
PAPI: http://papi.rediris.es/
Shibboleth: http://shibboleth.internet2.edu/
eduPerson: http://www.educause.edu/eduperson/
SAGE: http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-sage-scenarios-00.html
Curso virtual VRVS:
http://www.rediris.es/mmedia/vrvs/

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

AA Developer Workshop

Convocado por TERENA en el marco de la iniciativa TF-AACE, el pasado 15 de abril se celebró en Amsterdam un encuentro de los grupos que, dentro de las redes académicas internacionales, se encuentran en la actualidad desarrollando infraestructuras de autenticación y autorización (AA). El objetivo era discutir las posibilidades de definir una arquitectura común e iniciar los pasos para garantizar la interoperabilidad de las mismas. A la reunión asistieron representantes de SurfNET (Holanda), JISC y Athens (Reino Unido), Switch (Suiza), Uninett (Noruega), Sunet (Suecia), Internet2 (EEUU) y RedIRIS.

Los resultados más destacados son:

- Se sentaron las bases de una arquitectura basada en tres fases (autenticación, autorización y control de acceso) que está

siendo refinada por un grupo de trabajo cuyas conclusiones se presentarán en TF-AACE.

- Se acordó el uso de SAML como protocolo básico de intercambio entre las diferentes IAA y se inició un grupo de trabajo para el establecimiento de un perfil mínimo de interoperabilidad.
- La oferta por parte de la mayor IAA operativa, Athens (con varios cientos de miles de usuarios y centenares de proveedores, aunque con una tecnología relativamente antigua), para abrir vías de integración con otras IAA que se están estableciendo ahora, como las basadas en PAPI, Shibboleth y A-Select

Referencias

TERENA AAI Developer Workshop: http://www.terena.nl/tech/task-forces/tf-aace/Meet15-04-03/AAMinutes.pdf
SAML: http://www.oasis-open.org/committees/security/
Athens: http://www.athensams.org/
PAPI: http://papi.rediris.es/
Shibboleth: http://shibboleth.internet2.edu/
A-Select: http://a-select.surfnet.nl/

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

TERENA Networking Conference 2003

Con ocasión de la celebración en Zagreb (Croacia) de la reunión anual sobre redes de TERENA, se han realizado dos presentaciones que implican directamente a las actividades actuales de RedIRIS en el área del middleware.

En primer lugar, se presentó la propuesta de integración de PAPI y PERMIS. PERMIS es un sistema de autorización distribuido basado en el uso de certificados de atributos y que ha sido integrado en la NMI (NSF Middleware Initiative). La propuesta pretende experimentar con el uso de los certificados de atributos y con la gestión dinámica de servidores LDAP como métodos de interacción entre los elementos encargados de autenticar a los usuarios y los encargados de autorizar el uso de los recursos en la red. Este uso está orientado a su implementación en entornos que requieran una configuración mínima, como pueden ser los grids. En la propuesta colaboran la Universidad de Salford (Reino Unido), la de Málaga y RedIRIS.

En segundo lugar, Jesús Vega (CIEMAT) presentó la ponencia invitada "Remote Operation in the TJ-II Fusion Device" en la sesión dedicada a sistemas de e-ciencia. Esta presentación da cuenta del entorno de participación remota para el reactor experimental de fusión TJ-II que se encuentra en las instalaciones del CIEMAT en Madrid. Por medio de este entorno (que emplea PAPI como elemento para el control de acceso y la identificación de usuarios) se ofrecen mecanismos para definir, conducir y explotar los datos de experimentos con el reactor a través de Internet.

Referencias

TNC2003: http://www.terena.nl/conferences/tnc2003/
Propuesta PAPI/PERMIS: http://www.terena.nl/conferences/tnc2003/programme/final-programme.html#2c
PAPI: http://papi.rediris.es/
PERMIS: http://www.permis.org/
NMI: http://www.nsf-middleware.org/
Presentación sobre TJ-II Remote Participation: http://www.terena.nl/conferences/tnc2003/programme/final-programme.html#4a
Laboratorio Nacional de Fusión: http://www-fusion.ciemat.es/

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

Grupo de trabajo sobre revistas electrónicas de ámbito científico

Durante el mes de mayo y dentro del foro de administradores de listas y redes temáticas de RedIRIS (ADMIN.-L), se produjo un intenso debate acerca de la necesidad de fomentar contenidos de calidad científicos en la Red a través de revistas electrónicas. El problema surge de la dificultad para conseguir esos recursos científicos propios y de calidad en el entorno de las redes temáticas científicas, y a esto se le añadía el eterno problema de la falta de metainformación en los escasos recursos existentes y su implicación en los sistemas de indexación y búsqueda. Por estos motivos se consideró que una alternativa que podría solucionar casi todos estos problemas sería

AA Developer Workshop

TERENA Networking Conference 2003

Grupo de trabajo sobre revistas electrónicas de ámbito científico

Grupo de Trabajo sobre revistas electrónicas de ámbito científico

I Curso Virtual del sistema de videoconferencia VRVS

fomentar los modelos de revistas electrónicas con criterios de calidad y su modelo funcional de comités científicos de redacción. Realmente es un modelo compatible con la actual dinámica de las redes temáticas y la plataforma de herramientas para la generación de contenidos que se oferta.

De este debate se concluyó que las publicaciones digitales posibilitan la comunicación entre usuarios de un mismo grupo temático, les permite tener acceso a una información común y abrir nuevos caminos a la colaboración científica. La realidad es que es un valor escasamente reconocido donde prima la publicación en papel sobre la digital en la Red. El problema parece agravarse con el hecho de que los miembros de la comunidad hispana se ven privados muchas veces del reconocimiento de la autoría de sus trabajos de investigación por no existir cauces de comunicación científica acreditados en castellano.

Para canalizar este problema e intentar evaluar las posibles alternativas, RedIRIS organizó un grupo de trabajo específico (RV-E) que se reunió por primera vez el 10 de mayo y donde se presentaron y evaluaron unas doce propuestas que recogen los aspectos más significativos del debate. A esta sesión se adhirió un representante de la Presidencia del CSIC y tres técnicos del CINDOC que le dio otro cariz a la iniciativa. De la reunión salió la idea de formalizar y poner en marcha un modelo de editorial electrónica en la comunidad científica con un proceso de evaluación de la calidad editorial de las e-revistas. El concepto "open" estuvo presente en todo momento como algo básico, y un punto de coincidencia importante fue la "visibilidad"; es decir, una publicación existe cuando "está presente", de forma que el concepto de "impacto" debe cambiar y vincularse al hecho real de que si "existe", "se ve", "se lee", "se analiza" y eso contribuye a su posterior "asimilación", cosa que debería ser el impacto. Visibilidad y calidad de contenidos son dos de los grandes objetivos que se deben conseguir con esta iniciativa

Se plantearon dos fases en el desarrollo de la iniciativa:

1ª Definición del marco, metodología y política de la Editorial Científica Electrónica en un documento de referencia que debería estar disponible antes de septiembre.
2ª Puesta en marcha del sistema de publicaciones en dicha editorial.

La segunda fase estaría planificada a más largo plazo y su ejecución dependería de la entidad que quiera recoger el relevo y ponerlo en marcha dentro del marco definido en la primera. Esta segunda fase pivotaría en una página web que incluiría un catálogo de revistas electrónicas que serían dadas de alta por el grupo coordinador de esta editorial en función de la evaluación, con unos rigurosos controles y criterios de calidad definidos en la fase anterior. A esto se añadirían otros aspectos como el alojamiento del portal de esta editorial, el de las revistas electrónicas si fuera necesario, el desarrollo de sistemas de búsqueda y navegación, la ágil difusión de artículos y servicios de alerta, plantillas o herramientas de metainformación, herramientas de apoyo, sistemas electrónicos de evaluación por pares, etc.

El eje principal de los objetivos del documento de la primera fase son los criterios de calidad, la estructura del grupo coordinador, la política editorial y el modelo de evaluación.

Jesús Sanz de las Heras
(jesus.heras@redirises)
Redes Temáticas Científicas

I Curso Virtual del sistema de videoconferencia VRVS

Durante las cuatro semanas comprendidas entre el 14 de abril y 6 de junio, dos personas de RedIRIS nos embarcamos en la novedosa e interesante iniciativa de organizar el Primer Curso Virtual del sistema de videoconferencia VRVS (*Virtual Rooms Videoconferencing System*), el cual no hubiera sido posible sin la inestimable colaboración de David Collados, miembro del equipo técnico del VRVS. Lo hicimos porque consideramos necesario que este tipo de herramientas no sólo se debían dar a conocer, sino que había que hacerlo de forma que se instruyera en su instalación y uso.

Por experiencia sabemos que en entornos académico-científicos, el mayor problema de cualquier aplicación o tecnología nueva de uso general que se ponga en marcha es su difusión y uso. Y el motor de difusión de información de RedIRIS al colectivo investigador a través de los PERs no suele ser tan efectivo como cabría esperar. RedIRIS a través de este curso virtual pretendía difundir, enseñar y dar soporte a esta útil herramienta para realizar videoconferencias. Queríamos intentar que los investigadores empezaran a conocer, instalar y utilizar esta segunda generación de nuevas tecnologías

I Curso Virtual del sistema de videoconferencia VRVS

–cosa que ya es posible con la actual capacidad de ancho de banda de la infraestructura de comunicaciones de RedIRIS– y al mismo tiempo intentar romper la actual inercia de difusión de información para que esta herramienta no llegara a ser de uso exclusivo por parte de una elite científica.

Otros objetivos perseguidos en este Curso Virtual de VRVS han sido:

1.- La creación de documentación sobre VRVS y metodología para organizar e impartir futuros cursos locales y presenciales en las respectivas instituciones.
2.- Los objetivos pedagógicos a impartir sobre VRVS eran:

- Conceptos y terminología básica de videoconferencia
- Nociones sobre el funcionamiento de la red de VRVS
- Instalación
- Conocimiento de los diferentes tipos de clientes para VRVS
- Forma de registro y reserva de salas
- Aprendizaje del servicio de texto conferencia
- Uso de aplicaciones añadidas
- Política y condiciones de uso de las salas
- *Netiqueta* en las salas y recomendaciones para organizar reuniones virtuales

Para poner en marcha la idea, se optó por un diseño *tipo curso* con su aula, temario y equipo de profesores. El aula era una lista de distribución moderada que serviría de vehículo de expresión para preguntar y opinar. El temario fue un documento dividido en ocho capítulos con información suficiente para comprender e instalar VRVS. El equipo de profesores estuvo formado por tres personas, los abajo firmantes y David Collados. La dinámica del curso consistía en ir publicando un capítulo por semana durante ocho semanas, al mismo tiempo que el equipo de profesores atendía las consultas acerca del tema correspondiente. Se intentó contener el flujo de mensajes para no molestar en exceso a los alumnos con correo innecesario o mal formateado. A medida que trascurría el curso, iban incorporándose nuevos alumnos a las salas VRVS, una minoría con audio-vídeo, otros con audio sólo y la mayoría al chat. El equipo de profesores atendía durante dos horas al día la Sala VRVS "Burro" para ayudar, charlar y probar el sistemas con los alumnos.

En el Curso Virtual VRVS se inscribieron unos 920 alumnos, sólo cuatro se dieron de baja antes de finalizar. Los alumnos procedían de 21 países diferentes, fundamentalmente España y .com pero también de Argentina, Cuba, Colombia, Brasil, Portugal, Chile, México, Paraguay, Perú, Venezuela, etc. El perfil de los usuarios era amplio, pero una gran mayoría procedía de la universidad o de entornos científicos.

Se comprobó que existían muchos problemas de acceso a VRVS para usuarios que intentaban conectarse desde lugares donde la conectividad no era la adecuada (Latinoamérica) y usuarios en España que lo hacían desde su casa con ADSL. Desde Latinoamérica sólo tenemos constancia de una persona que consiguió conectarse con plenas garantías de calidad desde una universidad mejicana. Los problemas con ADSL son debidos al escaso ancho de banda, problemas de filtros y NAT (traducción de direcciones públicas a privadas) en configuraciones multipuesto.

Además encontramos un problema conocido pero silenciado: muchas personas no podían hacer sesiones VRVS debido a los numerosos filtros existentes en puertos necesarios para la aplicación. Se escribió un documento ("VRVS un derecho para todos" http://www.rediris.es/mmedia/vrvs/portvrvs.es.html) y se difundió ampliamente para que se tomaran cartas en el asunto.

Esto solucionó muchos de los problemas de los alumnos, por lo menos de la Comunidad RedIRIS, aunque sólo un 10-15% consiguió establecer una sesión VRVS con plenas garantías, lo que se considera un éxito. Había otro porcentaje de alumnos que no disponía de alguno de los requisitos necesarios: PC con escasos recursos, cascos, micrófono, cámara, etc. A pesar de esto, el resto de alumnos que no consiguió acceder acabó el curso con ilusión y con el agradecimiento por estar informados de la existencia de esta herramienta, y muchos de ellos se comprometieron a ponerla en marcha en cuanto tuvieran oportunidad.

Como en otras ocasiones, este curso acabo con una "Fiesta de fin de curso" que consistió en celebrar una gran reunión por videoconferencia durante dos horas en dos salas VRVS para que "cupiéramos todos". Cada sala estuvo moderada por una persona de RedIRIS y moviéndose por las dos, David Collados. Asistieron a esta *fiesta* unas 120 personas perfectamente auto-repartidas en ambas salas.

Para dejar constancia de la "fiesta", se hicieron unas capturas de pantalla y uno de los

I Curso Virtual del sistema de videoconferencia VRVS

Mediateca del CSIC

asistentes grabó un par de vídeos que se han colocado para ser vistos por streaming (gracias a Francisco Ramos). Además, Mario Tomé, alumno de iniciativa y profesor de la Universidad de León, hizo otra *web-reportaje* con algunas capturas que realizó a lo largo del curso (http://www.rediris.es/mmedia/vrvs/repor/).

Realmente, organizar un curso de videoconferencia a través de web y listas era una apuesta arriesgada; no sabíamos si el resultado iba a ser satisfactorio, pero con los resultados obtenidos se ha despejado todo tipo de dudas, la participación ha sido masiva y los participantes lo han hecho muy ilusionadamente, haciendo realidad el ideal de cooperación en la Red.

Consideramos que la iniciativa ha cumplido todos los objetivos iniciales y se ha generado una documentación para que las instituciones cojan el testigo y lo utilicen para seguir formando a otros usuarios en el conocimiento y uso de esta útil herramienta.

Referencias

http://www.rediris.es/vrvs
http://www.vrvs.es

Jesús Sanz de las Heras
(jesus.sheras@rediris.es)
Redes Temáticas Científicas
José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia

Mediateca del CSIC

En el Museo Nacional de Ciencias Naturales ha sido inaugurada la Mediateca del CSIC. Se trata de un lugar donde se pretende digitalizar y ofrecer al público producciones de vídeo, audio y fotos de carácter científico y divulgativo, muchas de ellas olvidadas. La creación de la Mediateca es fruto de un acuerdo entre el Ministerio de Ciencia y Tecnología, la Comunidad de Madrid, el CSIC y la Asociación Española de Cine Científico; acuerdo por el que se comprometen a conservar y difundir y –en una segunda etapa– a promocionar la creación de nuevos productos multimedia de contenido científico.

En principio el acceso a los contenidos de la mediateca está limitado a las instalaciones locales existentes en el museo. En un futuro el objetivo es que éste sea el germen que permita su apertura a la Red. Habrá contenidos públicos y otros de carácter restringido, para preservar los derechos involucrados.

La solución adoptada para la implantación de la mediateca se ha desarrollado con la colaboración de profesionales de instituciones públicas que han definido la solución del proyecto: Jesús Dorda, Alfonso Marra y Rogelio Sánchez (MNCN-CSIC), Dolores de la Guía y Juan Manuel Bolaño (CTI-CSIC), Javier Álvarez (CISATER-ISCIII) y José María Fontanillo (RedIRIS).

Desde el punto de vista físico, el sistema está formado por un servidor conectado por un interface Gigabit Ethernet a un conmutador catalyst 3548; los 28 puestos clientes se conectan mediante fast Ethernet. El servidor guarda los contenidos en un raid de discos, por redundancia y velocidad de transferencia y contiene los siguientes elementos que están basados principalmente en software de libre distribución:

- Sistema gestor de base de datos Postgres que alberga metainformación de los contenidos
- Servidor Web Apache con páginas dinámicas PHP
- Servidor DHCP
- Compartición contenidos mediante SAMBA
- Software REMBO para arranque remoto de PCs clientes

El formato de los vídeos que alberga el servidor es MPEG4 a 1Mbps, pero el servidor está dimensionado para soportar alta calidad en MPEG2. El sistema es independiente del CODEC utilizado en los vídeos y audios, es suficiente con que los clientes lo puedan decodificar, pero se apuesta por formatos estándar como MPEG1, MPEG2 y MPEG4.

Los PCs clientes tienen el acceso físico restringido a la CPU por estar en una vitrina, tienen Windows 2000 Pro y están configurados en modo quiosco, para restringir la posibilidad de pérdida de configuraciones.

El objetivo de la Mediateca es ser un lugar de difusión de la cultura científica para todos los ciudadanos, al mismo tiempo que un sitio que sirva de promoción a todo tipo de producciones, con especial empeño en localizar aquellas, que por tratar temas menos comerciales, no son accesibles en las grandes cadenas comerciales, sin olvidar los títulos más populares para su consulta y estudio.

El carácter no lucrativo de la Mediateca facilita la participación en ella de todo tipo de instituciones, tanto públicas como privadas. Algunos de los fondos con los que cuenta en la actualidad son:

- El fondo documental de la Asociación Española de Cine Científico
- Documentales premiados en los certámenes de cine científico de Zaragoza, Ronda y Videomed
- Producciones del Centro Nacional de Educación Ambiental (CENEAM)
- Filmoteca Española
- WWF/ADENA
- Producciones del Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT)
- Documentales de diversas productoras: Transglobe Films, Madrid Scientifics Films, Trifolium, ATEI...

Referencias

http://www.asecic.csic.es/media.htm

http://www.fotosub.org/mediateca.htm

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

RedIRIS en CATNIX

El pasado 7 de mayo, y coincidiendo con la presentación de la nueva Anella Científica, se realizó la firma de la participación de RedIRIS en CATNIX. CATNIX es el Punto Neutro de Internet en Cataluña que tiene como objetivo realizar la interconexión en Cataluña de proveedores de Internet para reducir el transvase de información por los troncales y hacer posible el intercambio de tráfico lo antes posible en los extremos de la red. CATNIX se encuentra ubicado en las instalaciones del CESCA en Barcelona, que es a su vez la institución que las gestiona.

Lo antes posible se intentará intercambiar tráfico de RedIRIS, fundamentalmente regional, con los proveedores presentes en CATNIX.

Víctor Castelo
(victor.castelo)
Director

Red telemática de investigación de Madrid

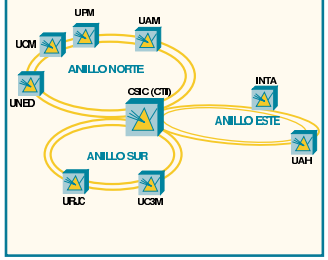
La nueva infraestructura nacional de RedIRIS junto con la necesidad de conseguir una calidad adecuada en las comunicaciones extremo a extremo hacen necesaria la existencia de infraestructuras, más allá del punto de presencia de RedIRIS, en cada una de las Comunidades Autónomas. Una de las formas de llevar esto a cabo es mediante redes autonómicas que se adecúen a las necesidades actuales de comunicación, con alta velocidad dentro de la autonomía, coordinación a todos los niveles y además la importante ventaja de su economía de escala.

Nos congratulamos de la aparición de una nueva red autonómica de investigación, la de la Comunidad de Madrid, recientemente presentada y que ofrece a los grupos de investigación de esta Comunidad una infraestructura de comunicaciones de primera línea.

En la primera fase de la red se incluyen las siguientes entidades:

- Consejo Superior de Investigaciones Científicas (CSIC)
- Universidad Politécnica de Madrid (UPM)
- Universidad Complutense de Madrid (UCM)
- Universidad Nacional de Educación a Distancia (UNED)
- Universidad Rey Juan Carlos de Madrid (URJC)
- Universidad Carlos III de Madrid (UC3M)
- Universidad Autónoma de Madrid (UAM)
- Universidad de Alcalá de Henares (UAH)
- Instituto Nacional de Técnica Aeroespacial (INTA)

RED TELEMÁTICA DE INVESTIGACIÓN DE LA COMUNIDAD DE MADRID



Mediateca del CSIC

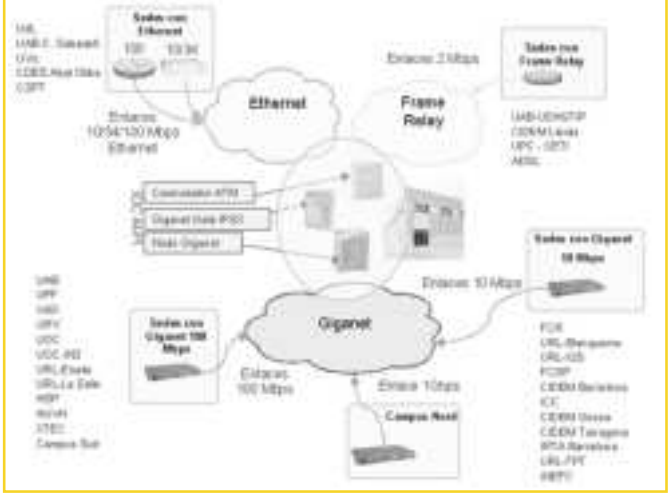
RedIRIS en CATNIX

Red telemática de investigación de Madrid

Red telemática de investigación de Madrid

Inauguración de la nueva Anella Científica

LA ANELLA CIENTÍFICA CON GIGABIT ETHERNET



La red se basa en un transporte DWDM con topología en anillo y con un enlace, en cada una de las entidades participantes, de una interfaz Gigabit Ethernet. El nodo central se configura en el Centro Técnico de Informática del CSIC, que a su vez es el que soporta las conexiones con RedIRIS.

Esperamos que la nueva red represente un cambio drástico, integrador y de alta calidad en las comunicaciones de la Comunidad Autónoma de Madrid.

Víctor Castelo
(victor.castelo@rediris.es)
Director

Inauguración de la nueva Anella Científica

El pasado 7 de mayo se celebró la inauguración de la nueva Anella Científica, la red de investigación autonómica de Cataluña, que ha pasado a utilizar tecnología Gigabit Ethernet. Esto supone una perfecta sincronización con la nueva infraestructura de RedIRIS, y por tanto un importante paso para mantener la capilaridad de la red hasta el usuario final pasando por la red estatal, la red autonómica y la red de campus.

Víctor Castelo
(victor.castelo@rediris.es)
Director