SCS: Superados los 1.000 certificados

- Hay expectativas de crecimiento por la comodidad y la eficacia del servicio

El pasado mes de julio se superó la cifra de 1.000 certificados emitidos, lo cual nos sitúa como una de las NRENs con mayor número de certificados emitidos de entre todas las NRENs que forman el acuerdo con GlobalSign.

Actualmente, el número de certificados es de 1.154 válidos, y con expectativas de crecimiento, ya que muchas instituciones, viendo la comodidad y la eficacia del servicio, han decidido dejar expirar los certificados emitidos de sus PKIs autofirmadas, para solicitar certificados del servicio SCS. Esto les permite no tener que dedicar personal exclusivamente para la gestión de una PKI, no reconocida por los navegadores web, con el inconveniente típico de los fastidiosos pop-ups.

En los últimos grupos de trabajo, celebrados del 26-27 de junio de 2007 en Madrid, lanzamos un nuevo procedimiento para la solicitud de certificados, que tiene como objetivo agilizar dichas solicitudes, ya que con este sistema se evita el uso del FAX. Con este nuevo procedimiento no pretendemos sustituir el que ya todos conocéis y que se encuentra descrito en *http://www.rediris.es/pki/scs/doc/userguide.es.html*

La variación que introduce este nuevo procedimiento reside en que evita el envío vía FAX de la documentación requerida para emitir los certificados solicitados. Para ello hacemos uso del correo electrónico firmado digitalmente según el estándar S/MIME con un certificado digital emitido por cualquier autoridad de certificación reconocida legalmente por el Estado español.

Antes de poder usar este nuevo procedimiento es necesario que el PER delegue la responsabilidad de la solicitud y validación de los certificados SCS en el solicitante. Así no es necesario la firma digital del PER, sino simplemente la del solicitante.

Esto es debido a que hemos estado desarrollando un piloto con dos instituciones, la Universidad Carlos III de Madrid y la Universidad Politécnica de Cataluña. Y queríamos tener suficiente experiencia para detectar los errores más comunes y documentarlos.

Daniel García
(daniel.garcia@rediris.es)
Área de Middleware

Reunión del proyecto ALICE en Guatemala

- Responsables de RedCLARA participarán en las Jornadas Técnicas de RedIRIS

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

ALICE es un proyecto, financiado por la Unión Europea, que tiene como objetivo la creación de la primera red regional de investigación de América Latina (RedCLARA) y su conexión directa con la red académica y de investigación paneuropea Géant2. RedCLARA *(http://www.redclara.net)* fue inaugurada oficialmente en noviembre de 2004, y hoy en día dispone de un anillo de 155 Mbps, conectado a 622 Mbps a la red paneuropea Géant2 a través de su punto de presencia en Madrid.

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

RedIRIS presta un apoyo decidido al proyecto ALICE y a RedCLARA, y en la reunión de ALICE que tuvo lugar en Guatemala se comprometió a participar en la próxima reunión técnica de RedCLARA, y en las pasadas Jornadas Técnicas de RedIRIS se realizó una sesión por video conferencia con CLARA.

Actualmente el número de certificados válidos emitidos es de 1.154

Las redes académicas y de investigación de Nicaragua, El Salvador, Guatemala, Costa Rica y Uruguay, conectadas a RedCLARA

La conferencia anual de TERENA se celebrará en Málaga en el 2009

Alberto Pérez, Subdirector de RedIRIS, es elegido miembro del Comité Ejecutivo de TERENA

Asamblea General de TERENA

- TERENA nombra a Alberto Pérez miembro del Comité Ejecutivo de la asociación

TERENA (asociación europea de redes académicas y de investigación) celebró en mayo su conferencia anual (TERENA Networking Conference 07) en Lyngby (Dinamarca). En esa reunión, TERENA adoptó dos decisiones relacionadas con RedIRIS: por un lado, confirmó que la conferencia anual de 2009 se celebrará en Málaga, corriendo la organización del evento a cargo de TERENA, RedIRIS y de la Universidad de Málaga; y, por otro lado, eligió a Alberto Pérez, Subdirector de RedIRIS, como miembro del Comité Ejecutivo de TERENA.

Alberto Pérez, como coordinador del grupo de trabajo de TERENA sobre ciclo de vida y gestión de la cartera de servicios de las redes académicas ("TF-LCPM" - Task Force on Life Cycle and Portfolio Management) realizó una presentación en esa asamblea general sobre las distintas áreas abordadas por ese grupo de trabajo: elaboración de un catálogo tipo de servicios y de un modelo de descripción de servicio; comparación de los compromisos de niveles de servicio asumidos por algunas redes académicas; la compartición de ideas sobre posibles proyectos de interés común (se debatió en esta ocasión la prestación de servicios de almacenamiento colaborativo), y el intercambio de mejores prácticas en materia de gestión de servicios de redes académicas y de investigación.

Colaboración en servicios de almacenamiento

- El objetivo de la reunión ha sido establecer líneas de trabajo comunes

El pasado día 29 de junio TERENA organizó un encuentro con las redes académicas y científicas europeas así como organizaciones adscritas a programas de e-Ciencia en la que estuvo presente RedIRIS.

El objetivo de la reunión era conocer qué servicios y proyectos relacionados con almacenamiento (o *storage*) están llevando a cabo cada una de las organizaciones y poder así establecer unas líneas de trabajo comunes. De esta forma, se podrán identificar qué servicios pueden ser aplicados en cada una de las redes, así como acometer proyectos más ambiciosos entre todas las organizaciones.

La siguiente reunión está prevista que sea para otoño 2007, en la que se espera elegir un proyecto piloto para ser implantado en todas las redes académicas y científicas dentro de un entorno federado por eduGAIN. Además, se trabajará en una política de uso del servicio que cumpla con los requisitos legales que existen en la transmisión de ficheros entre usuarios de distintos países.

Si alguna organización afiliada está interesada en colaborar en servicios de almacenamiento, como se está tratando en el grupo IRISLibre, puede ponerse en contacto con RedIRIS para lanzar un grupo de trabajo de esta área tecnológica.

TERENA TF-CSIRT

- La Universidad Carlos III de Madrid realizó una presentación en la reunión de Budapest sobre el sistema DesConll

Se han llevado a cabo dos reuniones del Grupo de Trabajo de TERENA TF-CSIRT (CSIRT Coordination for Europe, *http://www.terena.org/activities/tf-csirt/*). La primera de ellas se celebró en Budapest (Hungía) el pasado enero, patrocinada por Hun-CERT (Hungarian Nacional Computer Emergency Response Team), y organizada conjuntamente con el FIRST. Para la segunda, en mayo y celebrada en Praga (Republica Checa), fue CESNET-CERT (CESNET Computer Security Incident Response Team) quien actuó como organizador local.

Como viene siendo habitual, las reuniones se dividen en dos días, el primero de los cuales se dedica a seminarios de interés general, y el segundo a tratar temas específicos del Grupo de Trabajo y cuya asistencia está restringida a los miembros del mismo.

Las presentaciones de ambos seminarios se encuentran disponibles en*http://www.terena.org/activities/tf-csirt/ previous-meetings.html*

Cabe destacar que por primera vez una institución de nuestra comunidad, Universidad Carlos III de Madrid, realizó en Budapest una presentación sobre el sistema DesConll (*http://www.rediris.es/rediris/boletin/77/*

enfoque1.pdf), para la desconexión de sistemas comprometidos, presentando el sistema y las pruebas que desde RedIRIS se han realizado del mismo, en su modalidad de agregador de eventos de seguridad (sobre el nfsen).

Entre las actividades y proyectos discutidos en estas dos reuniones cabe destacar:

- El estudio realizado por el NISCC sobre los distintos formatos de intercambio de información sobre eventos de seguridad, incluyendo intercambio de incidentes, de alertas, recomendaciones, etc.

- Estudio encargado por la Comisión a la ENISA para examinar la posibilidad de crear un sistema a escala global de alertas y compartición de información a nivel europeo, propuesta que está incluida en el Communication COM (2006)-251. Actualmente, la ENISA está trabajando en determinar el impacto de este tipo de sistemas sobre la cultura de la seguridad, mediante el establecimiento y evaluación de una serie de indicadores.

- Inclusión del contenido del objeto IRT en las consultas básicas del whois de RIPE para aquellas redes que lo tengan enlazado.

- Continuidad de los cursos TRANSITs (*http://www.terena.org/activities/csirt-training/*), esponsorizados por diversas organizaciones, principalmente la ENISA y la ISPA.

- Conjuntamente a las reuniones del TF-CSIRT se celebraron las reuniones a puerta cerrada entre los miembros acreditados en el servicio TI (Trusted Introducer) de TERENA *(http://www.ti.terena.nl/)*. Entre los puntos más interesantes de dichas reuniones, podemos destacar:

  - Estudio de diversas propuestas para promocionar el conocimiento mutuo entre los equipos acreditados y pruebas paras comprobar la excelencia de los equipos.

  - Pruebas de los diversos sistemas de alerta ofrecidos por el TI a los equipos acreditados, entre los que se encuentran el sistema de alerta fuera y en banda.

  - Desarrollo de guías para manejar el estado de aquellos equipos acreditados en los que se produzcan cambios sustanciales en sus datos.

La última reunión de este año se celebró los días 20 y 21 de septiembre en Oporto (Lisboa), organizada por la Facultad de Ingeniería de la Universidad de Oporto (FEUP).

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

FS 2007

- V Foro de Seguridad de RedIRIS

La 5.ª Edición del Foro de Seguridad de RedIRIS se celebró en abril de este año en el Puerto de la Cruz (Tenerife), organizada conjuntamente por el Instituto de Astrofísica de Canarias (IAC) y RedIRIS.

El tema elegido en esta ocasión fue Detección de Intrusiones, como una pieza clave para la mejora de la seguridad de nuestras instituciones. El objetivo de las presentaciones era el de dar un repaso a las diferentes técnicas y modalidades de detección, incluyendo métodos y técnicas de correlación de eventos, desde las más tradicionales a las más novedosas, sin olvidar la casuística y características concretas de nuestra comunidad.

Para ello contamos con la participación de expertos tanto de nuestra comunidad como de fuera de ella, haciendo de esta nueva edición, según los resultados de las encuestas recibidas, un éxito.

Más información disponible en: *http://www.rediris.es/cert/doc/reuniones/fs2007/*

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

Reunión Internacional de CERTS

- IRIS-CERT participó en la reunión como punto de contacto de incidentes para todo el dominio.es

Del 23 al 25 de junio de 2007 se celebró en Madrid, organizada por el CERT/CC y esponsorizada por INTECO, la primera reunión internacional para la coordinación de CERTs con competencias nacionales.

Por primera vez, una institución de la comunidad de RedIRIS participa en el TERENA TF-CSIRT

El V Foro de Seguridad de RedIRIS se celebró en abril en el Puerto de la Cruz (Tenerife)

IRIS-CERT participó en la Reunión Internacional de CERTS como punto de contacto de incidentes para todo el dominio.es

En la Conferencia FIRST 2007, Francisco Monserrat, de RedIRIS, realizó una presentación conjunta con Picolini y Gilherme Venere, de CAIS

En ella se dieron cita Equipos de todo el mundo, algunos de países que cuentan con CERTs Nacionales como tales, como el caso de Brasil o Australia, y otros cuyas funciones asumen de manera completa o limitada CERTs de otros entornos como el académico o el gubernamental (Eslovenia y Holanda, por ejemplo).

IRIS-CERT participó en la reunión, como punto de contacto de incidentes (soporte limitado) para todo el dominio .es, tal y como aparece en la definición de nuestro ámbito de actuación. Durante la reunión se trataron diversos temas, como el SPAM, el Phishing, detección de botnes, análisis de malware, herramientas de soporte y coordinación entre equipos. De las discusiones y presentaciones surgieron diferentes líneas de trabajo. Entre ellas:

- Evaluación de herramientas de atención de incidentes.
- Evaluación de herramientas de análisis de malware.
- Identificación de datos a intercambiar sobre malware e incidentes.
- Identificación de mecanismos para el intercambio de información sobre ASs maliciosos.
- Monitorización pasiva de DNS.
- Correlación de información sobre eventos de seguridad procedentes de diversas fuentes.
- Intercambio de información de servidores de C&C de botnets y relaciones con las fuerzas de seguridad del Estado.

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

Conferencia FIRST. Sevilla 2007

- El equipo de respuesta e incidentes de seguridad de RedIRIS ha tenido un protagonismo destacado

Durante los días 16 al 22 de junio de este año se ha celebrado la conferencia anual FIRST de seguridad informática en Sevilla. FIRST, *http://www.first.org,* es un foro que engloba a distintos grupos de seguridad informática a nivel mundial, de diversos sectores, comerciales (Microsoft, Cisco, Juniper...), gubernamentales (GovCERT.nl, CERT-Polska...), proveedores de Internet (Deutche-Telekom, BT, KPN...) y también redes académicas como RedIRIS o Suftnet.

Al celebrarse la conferencia anual este año en Sevilla, IRIS-CERT, el equipo de respuesta a incidentes de seguridad de RedIRIS, ha tenido un protagonismo destacado, así ha participado como Patrocinador de Oro, al igual que otros equipos de seguridad españoles como e-LC, CCN-CERT e Inteco. Otras empresas españolas como Panda Software, S21sec y Telefónica fueron patrocinadores de diversos aspectos del evento.

IRIS-CERT también participó como anfitrión local del evento, proporcionando apoyo logístico a la organización de las conferencias.

Este año la conferencia FIRST ha tenido varios aspectos novedosos que han servido para que el número total de asistentes, aproximadamente 470, haya sido el mayor registrado desde que se organiza esta conferencia. Además el número de sesiones simultáneas se ha duplicado, pasando de dos sesiones a cuatro, e incluso algunas veces cinco sesiones, lo que hacía difícil escoger a que sesión asistir.

Ponentes de reconocido prestigio, como Wietse Venema (autor de Postifx, tcpdwrapper), José Nazario, de Arbor Network, o Joanna Rutkowaska, de Invisible things org., participaron en la sesión.

Durante la conferencia se realizó un concurso de seguridad informático en varias fases, en las que los participantes tenían que analizar un binario extraño para a partir de ahí obtener una pista que les permitiera acceder a la siguiente fase de este concurso, organizado por el equipo de seguridad de la red académica Brasileña, CAIS, en el que RedIRIS también colaboró y tuvo una gran aceptación.

En la conferencia se presentaron dos ponencias de la comunidad académica, una "Privacy matters in directory" fue presentada por Victoriano Giralt, de la Universidad de Málaga, y en una de las sesiones técnicas Francisco Monserrat Coll, del equipo de RedIRIS, realizó una presentación conjunta con Jacomo Picolini y Gilherme Venere, de CAIS, titulada "Botnet creation, usage, creation and eradication".

A destacar que el número de asistentes españoles ha crecido significativamente con

respecto a otros años, aunque todavía es un porcentaje bastante pequeño del total y más teniendo en cuenta que la conferencia se celebraba en España.

Toda la información de la conferencia, incluyendo gran parte de las presentaciones, se puede consultar en *http://www.first.org/conference/2007/presentations.html*

Por último indicar que la conferencia FIRST del próximo año se celebrará en Vancouver (Canadá). Ya se ha abierto el plazo de solicitud de ponencias. Se puede consultar más información en *http://www.first.org/conference/2008*

Grupo de Monotorización FIRST

- El grupo se reunió en junio en Sevilla aprovechando la 19.ª Reunión Anual del FIRST

Los Grupos de interés especial (en adelante SIG) del FIRST proporcionan a los miembros de los equipos de respuesta miembros del foro una plataforma donde discutir sobre temas de interés común. En la actualidad son siete los SIG definidos por la comunidad FIRST *(http://www.first.org/global/sigs/current/index.html)*. Uno de ellos, el MN-SIG *(http://www.first.org/global/sigs/ monitoring/),* está dedicado al soporte, desarrollo y promoción del conocimiento y las técnicas de recolección y análisis de datos de monitorización de red como herramientas de soporte fundamental para la detección de actividad maliciosa y la mejora de la seguridad de los sistemas y redes.

El grupo, del que RedIRIS forma parte, y que está liderado por el CERT Gubernamental Holandés (GOVCERT.NL), se reunió el pasado mes de junio en Sevilla, aprovechando la 19.ª Reunión Anual del FIRST.

Aparte de intercambiar información acerca de diferentes proyectos que se están o se han llevado a cabo por diferentes miembros del grupo, lo más destacado fue la aprobación de una propuesta para crear una Darknet para la comunidad FIRST, en cuya definición ya se está trabajando.

El objetivo primordial de este proyecto es el de proporcionar una visión general de la actividad maliciosa en la comunidad FIRST, mediante la donación de datos procedentes del espacio de direcciones de las darknets de los participantes en el proyecto. A partir de dichos datos, se establecerán una serie de servicios, a los que los miembros del FIRST y los donantes de datos podrán acceder en función a sus privilegios. Estos servicios irán desde estadísticas y gráficas, a búsquedas de datos específicos, pasando por la generación automática de alertas.

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

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

GEANT 2

- Actividad JRA1: Performance Monitoring and Measurement

- Actividad dentro del servicio de autenticación y autorización

A través de la actividad JRA1, se está desarrollando de manera colaborativa una herramienta de gestión de redes multidominio, llamado perfSONAR *(http://www.perfsonar.net),* entre diferentes organizaciones de redes científicas y académicas, como Internet2, ESnet o Geant2.

Uno de los objetivos principales para la próxima versión de perfSONAR es la publicación del Servicio de Autenticación y Autorización (AS), del cual es responsable de su desarrollo el equipo de Middleware de RedIRIS. Diseñado como un servicio web más de perfSONAR, cuando el resto de los servicios reciben una petición del cliente, envían una petición de autenticación al AS incluyendo un token de seguridad que ha debido incluir el cliente en su petición. Este token debe contener información de autenticación válido dentro del modelo de confianza de eduGAIN, y es transmitido en cada una de las peticiones a un servicio web de perfSONAR cumpliendo el estándar Web Services Security sobre SOAP 1.1 *(http://www.oasis-open.org/committees/wss/)* a través de sus perfiles X.509 security token *(http://www. oasis-open.org/committees/download. php/16785/wss-v1.1-spec-os-x509 TokenProfile.pdf)* y SAML security token *(http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-*

En el Grupo de Monotorización FIRST se ha aprobado una propuesta para crear una Darknet para la comunidad FIRST

El objetivo del proyecto es proporcionar una visión general de la actividad maliciosa en la comunidad FIRST

Se está desarrollando una herramienta de gestión de redes multidominio (perfSONAR) entre diferentes redes científicas y académicas

Se desarrollarán cursos de formación sobre el conjunto integrado de herramientas definidas en el JRA2

SAMLTokenProfile.pdf). Existen tres perfiles diferentes que deben ser integrados con el servicio de Autenticación:

- Automated Client (AC): este perfil define el proceso de autenticación que deben seguir aquellas aplicaciones o *scripts* que son ejecutadas sin ninguna interacción con un usuario, basándose en el uso de certificados válidos en el modelo de confianza de eduGAIN.

- User behind a Client (UbC): aquí se engloban todas aquellas aplicaciones no automáticas que no son ejecutadas en un servidor web, siendo por lo general aquellas que son de escritorio. En este perfil se utilizaran certificados de corta validez *(short life certificates)* obtenidos a través de SASL CA, una PKI *online* desarrollado por Internet2 con autenticación de usuario a través del protocolo SASL.

- Client in a Web containEr (WE): todas aquellas aplicaciones webs están integradas en este perfil y utilizar aserciones SAML para afirmar su identificación.

Durante la reunión que se celebró en Cambridge, los días 7 y 8 de junio *(http://wiki.perfsonar.net/jra1-wiki/index.php/JRA1_Meeting_-_Cambridge_-_June_2007),* se presentó una actualización del estado del desarrollo del servicio, el cual está ya en fase de pruebas, y también se realizaron diversos tutoriales de los diferentes perfiles que se encuentran en perfSONAR.

Cándido Rodríguez
(candido.rogriguez@rediris.es)
Área de Middleware

• Actividad JRA2: "Security"

• Actividad para la dotación de un marco de seguridad a GEANT2

Se ha comenzado la elaboración de la estrategia a seguir dentro de esta actividad para el cuarto y último año de vida del proyecto. Si durante los años anteriores se han puesto las bases para hacer de GEANT2 una comunidad tan segura como se necesite (definición de estándares de seguridad), es en este último año cuando dichos estándares se deben llevar a la práctica. Para ello:

- Es necesario ayudar a los socios de GEANT que así lo necesiten a alcanzar los estándares de seguridad acordados por el grupo. Se ha optado por trabajar en dos líneas:

  – El desarrollo de cursos de formación sobre el conjunto integrado de herramientas definidas por el JRA2 (nfdump/nfsen y FlowMoon).

  – El diseño de un sistema de mentoring para ayudar a los equipos de seguridad que lo necesiten a entrar en la red de confianza ("web-of-trust") de CERTS, incluyendo la ayuda en la creación de CERTs en aquellas NRENS socias de GEANT que todavía no dispongan de un equipo de dichas características. En el momento de escribir este artículo se han identificado aquellas NRENs susceptibles de ser beneficiarias de este servicio (7), así como la NRENs voluntarias para actuar como mentores, entre la que se encuentra RedIRIS.

  La financiación para la operación de estos dos servicios correrá a cargo de GEANT2, mediante la definición de dos NAs (Network Activities): NA8 para los cursos de formación y NA4 para el servicio de mentoring.

- Continuar trabajando en el conjunto de herramientas integradas, para conseguir una Toolset suficientemente madura para su utilización por parte de las NRENs, con el fin de monitorizar tráfico de red de cara a detectar y diagnosticar anomalías y ataques de seguridad. En este caso, el principal esfuerzo se va a invertir en añadir funcionalidades avanzadas de detección de anomalías, así como la incorporación de nuevas herramientas al Toolset (compuesto en la actualidad por el nfdump/nfsen y el FlowMoon Probe), a medida que éstas se demuestren maduras y de utilidad para la comunidad.

La información pública sobre las actividades de seguridad de GEANT2 se encuentra disponible en la URL *http://www.geant2.net/cert/.*

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

• Actividad: JRA3 (AutoBAHN)

• Actividad de asignación automática de ancho de banda en redes heterogéneas

A la vez que las actividades de desarrollo en GÉANT2 empiezan a ser estables, se están

concentrando más esfuerzos en tareas de integración entre ellas.

Una de ellas consiste en proveer al sistema de gestión de ancho de banda bajo demanda de soporte para autenticación y autorización federada. Es decir, integrar eduGAIN (desarrollado dentro del JRA5) dentro de AutoBAHN (JRA3). Para ello, es necesario el desarrollo de dos componentes por parte del equipo de eduGAIN: un filtro de servlets y un conjunto de clases para gestionar aserciones SAML.

El filtro implementa la interfaz JAVA javax.servlet.Filter, y se despliega en cada DM (Domain Manager). Se encarga de interceptar el acceso al primer componente usado para la reserva de ancho de banda, y de comprobar si el usuario se ha autenticado correctamente. De no ser así, éste es redirigido a su servidor de autenticación siguiendo el protocolo eduGAIN.

El analizador SAML (SAMLParser) se usará tanto en los DMs como en los IDMs (Inter-Domain Managers). Su objetivo es permitir incluir los datos de autenticación del usuario y sus atributos en todas las peticiones entre los componentes de AutoBAHN. Incorpora un perfil novedoso, que consiste en una confianza distribuida basada en 2 certificados X.509 por petición: el del emisor de la petición de reserva de ancho de banda y el del emisor de los datos de autenticación.

Ambos componentes deben servir para todos los casos de uso de AutoBAHN, distinguidos por quién realiza la reserva: en el perfil WebSSO (Web Single Sign On) el usuario es humano, y en el perfil AC (Automated Client) el usuario es un proceso automático.

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

• Actividad JRA5: Roaming and Authorisation

• Actividad relacionada con los servicios de movilidad e identidad digital

A lo largo de los últimos meses, tanto el software como la infraestructura de autenticación y autorización eduGAIN se han ido consolidando. eduGAIN se utiliza ya habitualmente en varias conexiones con acceso autenticado entre diferentes NRENs, incluyendo también a recursos y proveedores de identidad en Internet2, con lo que la infraestructura llega ya más allá de las fronteras europeas. El equipo de desarrollo de eduGAIN trabaja ahora en la consolidación del esquema de confianza, la integración del estándar SAML2 y la consolidación de la infraestructura.

También se han demostrado las capacidades del protocolo RadSec para el intercambio seguro de datos sobre usuarios móviles en la infraestructura eduroam. Basado en este protocolo, existe un proxy que permite extender la infraestructura eduroam a cualquier punto donde se encuentre una conexion a Internet y un punto de acceso con capacidades 802.1x. El protocolo RadSec se ha presentado al IETF para su estandarización y se encuentra en la fase de Internet Draft.

El trabajo del proyecto DAMe sigue su curso y contamos ya con un "testbed" para verificar el *software* que se ha ido desarrollando de acuerdo con las especificaciones que el proyecto acordó hace unos meses. Estas especificaciones se han alineado con otras iniciativas con objetivos similares, como la NAS-SAML de Internet2, y se ha propuesto su estandarización como perfiles de acceso a la red basado en identidad digital federada a OASIS. Estamos también en contacto con actividades relacionadas, como NEA en el IETF y la iniciativa TNC (Trusted Network Connect) de los grandes fabricantes.

Mas información:

http://www.geant2.net/jra5/
http://pki.edugain.org/
http://resolver.edugain.org/
http://www.ietf.org/internet-drafts/draft-winter-radsec-00.txt
http://dame.inf.um.es/
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
http://www.ietf.org/html.charters/nea-charter.html
https://www.trustedcomputinggroup.org/groups/network/

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

• Actividad: SA5

• Nueva actividad de servicio para eduroam en Geánt 2

Como resultado de las actividades del JRA5 de Géant2 (Roaming and Authorisation)y del Task-

El protocolo RadSec se ha presentado al IETF para su estandarización y se encuentra en la fase de Internet Draft

Contamos con un "testbed" para verificar el *software* que se ha ido desarrollando para el proyecto DAME

Se ha acordado la creación de una nueva actividad de servicio para eduroam, SA5

El servicio de videoconferencia europea proporcionará colaboración en tiempo real de alto nivel entre instituciones educativas y de investigación

Force de Terena sobre movilidad, se ha acordado la creación de una nueva actividad de servicio para eduroam, SA5.

Con la puesta en marcha de esta actividad se persiguen los siguientes objetivos:

- El establecimiento de una confederación, que contribuya a la consolidación del espacio europeo de movilidad —esto es, eduroam en Europa—, y que está apoyada en los siguientes estamentos:
  - Un comité de política (NREN PC) que actuará como autoridad política de la confederación.
  - Un grupo de servicio, en el que participan representantes de las redes académicas participantes.
  - Un equipo de operación, designado por el grupo de servicio.
- La puesta en marcha de un sistema común de gestión de incidencias, que será gestionado por el equipo de operación, y que ayudará a escalar tanto las incidencias que se produzcan en el servicio como los incidentes de seguridad o abusos que sean detectados.
- Desarrollar una serie de herramientas de monitorización para la jerarquía de servidores de la confederación, que permitirán obtener datos fiables de uso, así como detectar posibles fallos en la misma.

RedIRIS dio el primer paso para participar en la actividad de servicio ratificando la política de la confederación, y seguirá participando en las actividades de la misma, con el convencimiento de que los resultados obtenidos beneficiarán a la comunidad académica.

Actividad de servicio de eduroam:

http://www.geant2.net/server/show/nav.00d00600b002

eduroam Confederation Policy:

http://www.eduroam.org/docs/European%20eduroam%20confederation%20policy-v1.4.pdf

José Manuel Macías
(jmanuel.macias@rediris.es)
Área de Middleware

• Actividad SA6

• Servicio de videoconferencia Pan-Europeo

El 11 de julio fue aprobado por Geant2 la GN2 SA6, una actividad se servicio que trata sobre servicios de videoconferencia en la que participan las NREN europeas.

El objetivo principal de la Service Activity 6 (SA6) es crear un entorno que permita a los servicios de videoconferencia de las NREN's cooperar a nivel europeo, para mejorar la experiencia de los usuarios con respecto a las siguientes cuestiones:

- Tratar la ausencia de confianza del usuario final en los servicios de videoconferencia entre NREN.
- Acelerar y mejorar la eficiencia en la identificación y resolución de problemas entre NREN mediante una estructura organizativa adecuada y con la ayuda de aplicaciones y herramientas de gestión comunes.
- Suministrar una forma sencilla para localizar la información de contactos de equipos de videoconferencia en lugares remotos y soporte a la organización de videoconferencias mediante un proceso automático de envío de mensajes de invitación.
- Evitar la brecha digital mediante servicios de videoconferencia multipunto fiables para proyectos europeos, comunidades de investigación y NREN que de otra forma tendrían que depender de servicios *ad hoc* bajo una filosofía *best-effort*.

Descripción del servicio:

El servicio de videoconferencia europea proporcionará colaboración en tiempo real de alto nivel entre instituciones educativas y de investigación por medio de:

- Un servicio de soporte coordinado entre los servicios nacionales existentes.
- Facilidades de monitorización y gestión entre NREN para mejorar la identificación y resolución de problemas.
- Un directorio federado de terminales de videoconferencia desplegados, dedicados a cooperación internacional y al establecimiento de nuevas sociedades entre actores del mundo de la investigación y educación.

- Albergar un servicio centralizado para las NREN sin infraestructura de videoconferencia multipunto, evitando de esta manera la brecha digital entre partes de Europa y con el objetivo de proyectos de investigación y educación universitaria europeos e internacionales.

Jose M.ª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios Multimedia

Reunión de los proyectos EUMEDCONNECT y EUMEDGRID en Siria

- Estos proyectos permiten que los investigadores españoles puedan participar en proyectos de ámbito mediterráneo

Del 4 al 7 de septiembre tuvo lugar en Damasco (Siria) una reunión conjunta de los proyectos EUMEDCONNECT y EUMEDGRID, en los que participa RedIRIS.

EUMEDCONNECT es un proyecto de cooperación, financiado por la Unión Europea, que tiene como objetivo la creación de una red regional de investigación para la cuenca del Mediterráneo y su conexión directa con la red académica y de investigación paneuropea Géant2. EUMEDGRID es un proyecto de investigación enmarcado en el VI Programa Marco de la Unión Europea, cuyo objetivo es la extensión de la tecnología Grid a ese mismo entorno de la cuenca del Mediterráneo, para lo que hace uso de la infraestructura de comunicaciones desplegada a través de EUMEDCONNECT.

Estos proyectos permiten, entre otras cosas, que los investigadores españoles puedan participar en proyectos de ámbito mediterráneo en los que se requiera un ancho de banda significativo o la compartición de recursos de computación o almacenamiento.

Tanto el proyecto EUMEDCONNECT como EUMEDGRID están llegando a su fin y los participantes en ambos proyectos están concluyendo las tareas previstas, incluyendo el despliegue de la red a nuevos países mediterráneos o el incremento de su capacidad, o la "gridificación" de aplicaciones que se ejecutan sobre la plataforma Grid desarrollada.

Los miembros de ambos proyectos han planteado a las autoridades comunitarias su extensión temporal. Este tema se ha debatido de forma específica en unas Jornadas organizadas por TERENA, llevadas a cabo los días 23 y 24 de octubre en Bruselas, y en las que RedIRIS realizó una presentación.

Este encuentro se ha celebrado aprovechando una cumbre de Ministros de Sociedad de la Información europeos y mediterráneos que se celebró en Bruselas durante esos días.

pkIRISGrid y 10™ EUGridPMA

- El número total de certificados asciende a 997

En la actualidad, la infraestructura de clave pública de IRISGrid dispone de 25 Autoridades de Registro distribuidas por toda la geografía nacional. Siendo el Instituto de Física de Cantabria la última institución en solicitar y operar una RA.

El número total de certificados emitidos por la CA (Autoridad de Certificación) desde que fue acreditada por la EUGridPMA en enero de 2006 es de 997. De los cuales, 381 son certificados para personas válidos y 525 para servicios/servidor válidos.

A finales de mayo se celebró en Estambul la 10™ reunión de la EUGridPMA (European Policy Management Authority for Grid Authentication in e-Science). Como es costumbre, se presentaron varias CA para ser acreditadas, siendo los resultados de las presentaciones los siguientes:

Serbia - AEGIS CA
Fue acreditada.

Rumania - ROSA CA
No fue acreditada, debido a que necesitaba hacer pequeños ajustes al documento CP/CPS (Certificate Policy/ Certifica Practice Statement). La acreditación será aceptada vía e-mail cuando los revisores aceptaran las modificaciones

Marruecos - MaGrid CA
No fue acreditada, debido a que necesitaba hacer pequeños ajustes al documento CP/CPS (Certificate Policy/ Certifica Practice Statement). La acreditación fue aceptada vía e-mail cuando los revisores aceptaran las modificaciones.

Ucrania - Ukranie CA
No fue acreditada, y se le emplazó a presentar

Los miembros de EUMEDCONNECT y EUMEDGRID han planteado a las autoridades comunitarias su extensión temporal

Los miembros de la EugridPMA están muy interesados en definir un procedimiento de auditorías para CA

de nuevo su propuesta de CA en la próxima reunión de la EUGridPMA.

Entre otros, los temas más interesantes que se trataron fueron:

Acreditación de la CA de GlobalSign (del servicio SCS) por la EUGridPMA.

Se presentó un borrador de perfil para que se debatiese, con el objetivo de presentarlo a GlobalSign una vez que fuese aprobado por la EUGridPMA.

Actualidad sobre APGridPMA.

Se presentaron los resultados de los procesos de auditoría de CA que han realizado. Estos resultados fueron muy bien recibidos por todos los miembros de la EUGRidPMA y especialmente por las Relying Party, las cuales estaban muy interesadas en definir un procedimiento de auditorías para CA.

El perfil POCS se basa en registros de usuarios autenticados por "Portales" que actualmente usan muchos grid

Debate sobre el perfil POCS (Portal-base Credencial Services).

Este perfil se basa en los registros de usuarios autenticados por "Portales" que actualmente usan muchos sistemas grid, para identificar y autenticar los solicitantes. Siendo su mayor desventaja que el par de claves (pública y privada) no las genera/almacena el cliente, sino el portal. Y su mayor ventaja es que los usuarios no han de preocuparse por la gestión de sus certificados.

Implementación de cambios en los perfiles por parte de las CAs.

Se debatió sobre el procedimiento que se debe seguir para revisar las políticas de cada CA, con el objetivo de adaptarlas a los cambios de los perfiles. Esto llevó a plantear la posibilidad de realizar auto-auditorías de las CA según los criterios presentados por Yoshio Tanaca de APGridPMA.

Auditorías de Autoridades de Certificación.

Debido a que existen CAs que fueron acreditadas hace mucho tiempo, no se sabe si están cumpliendo su CP/CPS, por lo que se decidió que debe existir algún método para comprobar que realmente están siguiendo los requisitos mínimos de seguridad, así como respentando las extensiones KeyUsage.

Debe existir algún método para comprobar que se están siguiendo los requisitos mínimos de seguiridad para hacer acreditaciones

En este procedimiento se pretende:

- Proporcionar una fecha límite para que aquellas CAs que no cumplen se puedan poner al día.
- Si una CA no demuestra haber realizado una auto-auditoría sobre su CP/CPS en dos años, se le requerirá que la haga y presente los resultados en el próximo mitin, bajo riesgo de ser dada de baja.
- Si una CA no realiza una auto-auditoría en dos años, deberá sufrir una auditoría externa.
- Si una CA no cumple con los requisitos mínimos de seguridad, dispondrá de seis meses para adecuarse a ellos.

Hardware Tokens.

Se estudió la posibilidad de usar tokens criptográficos para manejar los certificados de entidades finales, pero se detectaron problemas en los proceso de certificación FIPS 140-2 de los fabricantes, por lo que se duda sobre su utilización.

Revisión de Grid IReland CA presentó los resultados de su auto-auditoría, basada en el documento presentado por la APGridPMA.

Revisión del perfil clásico de certificados x509.

Se puso mucho interés en mantener la reunión presencial entre el solicitante y el operador de la autoridad de registro. Incluso se planteó la posibilidad de requerir formularios en papel que almacenaría la RA con los datos de la verificación de la identidad de los solicitantes.

Las Relying Parties plantearon asignar a los certificados diferentes niveles de confianza, basados en el proceso de identificación del solicitante. Es decir, si ha sido mediante un encuentro cara a cara, o por conversación telefónica bajo previo acuerdo, etc.

Requisitos de las Relying Parties.

Se va a tratar de mapear los requisitos de las Relying Parties con los requisitos mínimos del perfil clásico x509.

Daniel García
(daniel.garcia@rediris.es)
Área de Middleware

I Reunión de administradores de autoridades de registros de pkIRISGrid CA

• La primera medida será la creación de políticas de uso de las RAs

El pasado 27 de junio, coincidiendo con los grupos de trabajo de RedIRIS, tuvo lugar la primera reunión oficial de administradores de registro de la pkIRISGrid CA en Madrid.

En dicha reunión se trataron diferentes temas, entre los que destacan:

• Descripción del escenario actual con las estadísticas de uso del servicio pkIRISGrid. CA cuenta en la actualidad con 25 autoridades de registro repartidas por toda la geografía española.

Hasta la fecha de la reunión se habían emitido 775 certificados, de los cuales aproximadamente 350 son certificados de usuario y el resto de servicio/servidor.

Se emitieron 67 CRLs, que han sido descargadas más de 24 millones de veces del repositorio oficial.

• Coordinación con los administradores de RAs:

Para el mantenimiento de los lazos de confianza entre la CA y las RAs se vio la necesidad de establecer varias reuniones presenciales cada año.

Se insistió en la necesidad de la colaboración para el establecimiento de unos procedimientos más formales a la hora de dar de alta una RA y para el proceso de auditoría de las mismas.

Se van a establecer mecanismos para mejorar la PKI teniendo en cuenta los nuevos requisitos de las RAs y de sus usuarios.

• Problemas detectados:

Se volvió a tratar el problema que tiene el software del CERN a la hora de dar acceso a los catálogos LFC a un usuario que tiene en su certificado el carácter punto (.) en el campo CN de su DN. Por lo que parece confunden el certificado de usuario con el de un servidor.

Están intentando arreglarlo pero no han proporcionado una fecha estimada para la resolución del problema.

El *software* de gestión de la pkIRISGrid CA soporta el guión (-) como carácter alternativo al punto (.) en el DN. De esta forma los usuarios no se ven afectados por dicho problema. Éstos podrán elegir un CN del tipo CN=javi-masa en lugar de CN=javi.masa en caso de que necesiten trabajar con los catálogos LFC del CERN.

Se comentaron los problemas relacionados con el proceso de acreditación de identidad de los usuarios a la hora de la reunión presencial con los operadores de las RAs y la importancia que tienen estos controles de cara a la EUGridPMA y a las relying parties.

• Mejoras en el servicio:

Se presentaron varias ideas para mejorar el servicio. Algunas de ellas relacionadas con las RAs, como la creación de herramientas de apoyo para el cumplimiento de los requisitos mínimos de identificación de solicitantes, herramientas estadísticas y reestructuración de las listas de correo.

A medio y largo plazo se crearon procedimientos de aviso de expiración, solicitudes pendientes, soporte de Subject Alternative Name, especificación de duración del certificado, importación de CSRs externas...

• Auditoría de las RAs:

Las relying parties, como dueñas de las máquinas que prestan servicios, han solicitado a la EUGridPMA que se realice un mayor control sobre el usuario final. Esto ha llevado a que se plantee la necesidad de realizar auditorías periódicas sobre las CAs, las RAs y sobre los mecanismo de control sobre el proceso que realizan las RAs en la verificación de los solicitantes.

La primera medida va a ser la creación de políticas de uso de las RAs donde queden reflejados los procedimientos que usa cada RA para la validación de los solicitantes de certificados.

RedIRIS preparará un borrador con los requisitos mínimos que debe cumplir la política de una RA y cada RA lo adaptará a sus procedimientos, pudiendo hacerla más restrictiva si así lo cree conveniente.

Se hace constar que será muy importante mantener los procedimientos y datos de las

Se ha celebrado la primera reunión oficial de administradores de registro de la pkIRISGrid CA en Madrid

Se presentaron varias ideas para mejorar el servicio. Algunas de ellas relacionadas con las RAs

verificaciones realizadas en un medio que sea auditable.

Más información:

http://www.irisgrid.es/pki/

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

Nuevas versiones del *software* y la web de PAPI

- Proyecto para implantación de nuevas tecnologías de red

A lo largo de los últimos meses, el equipo de desarrollo de PAPI ha realizado un importante esfuerzo para aumentar y racionalizar la oferta de *software* para el sistema de autenticación y autorización desarrollado por RedIRIS.

El equipo de desarrollo de PAPI ha realizado un importante esfuerzo para aumentar y racionalizar la oferta de *software*

Se ha actualizado el sitio web de PAPI para facilitar el acceso a la tecnología desarrollada

En la actualidad se encuentran disponibles módulos implementados en los siguientes lenguajes:

- Perl, como módulo del servidor Apache. El equipo de desarrollo ha finalizado una nueva versión, la 1.4.1, que será la última que se soporte para Apache 1. De hecho, la versión1.5.0 (adaptada a Apache 2) está ya en fase de pruebas, con un *software* bastante estable y a falta de redactar parte de la documentación.

- Java, en dos versiones. La primera como filtro para un servidor de aplicaciones, de acuerdo con el interface javax.servlet.filter, lo que lo hace utilizable en cualquiera de estos servidores: Tomcat, WebSphere, etc. La segunda ofreciendo un interface de acuerdo con el estándar JAAS, lo que lo hace compatible con cualquier mecanismo de control de acceso que emplee este estándar. La interconexión PAPI-Shibboleth está basada en este *software*.

- PHP, con un mecanismo de control de acceso que permite incorporar control de acceso basado en identidad federada de manera simple a cualquier nivel dentro de un servidorweb: desde árboles completos hasta ficheros individuales. Existen también módulos PHP de interconexión con otras infraestructuras de identidad digital (incluido OpenID), que se están desarrollando en colaboración con la red académica noruega UNINETT y Sun.

Para facilitar el acceso a la tecnología PAPI hemos actualizado el sitio web del mismo en consonancia con estos nuevos desarrollos.

Para más información:

http://papi.rediris.es/
http://perl.apache.org/
http://tomcat.apache.org/tomcat-5.5doc/servletapi/javax/servlet/Filter.htm
http://java.sun.com/j2se/1.5.0/docs/guide/security/jaas/JAASRefGuide.html

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

MAAWG

- Se pretende fomentar la colaboración y coordinación de esfuerzos para reducir el impacto del spam, botnets, phishing, virus, etc.

Los pasado dias 5 al 7 de junio RedIRIS asistió, en calidad de invitado, a la 10.ª reunión general del MAWWG, celebrada en Dublín. MAAWG es una asociación internacional con más de 100 miembros, incluyendo organizaciones internacionales, equipos abuse de operadores de red y proveedores tecnológicos del ramo. El objetivo principal es fomentar la colaboración y coordinación de los esfuerzos y capacidad de compartir información para reducir el impacto del spam, botnets, phishing, virus, etc. MAAWG organiza reuniones internacionales, trabajos en comités, informes métricos de correo electrónico y otras actividades centradas en la tecnología, colaboración industrial e iniciativas de políticas públicas.

En esta sesión del MAAWG se analizaron los problemas desde diferentes perspectivas, haciéndose especial mención al estado y evolución de los nuevos protocolos de SIDF & DKIM por parte de Eric Allman (Sendmail Inc.), bloqueo de IPs a otros niveles como BGP, la iniciativa DROP de Spamhaus y el fomento del despliegue de DNSsec.

Hubo sesión para el intecambio de direcciones IPs de relays de correo de los diferentes operadores para que cada uno los incluyera en

sus respectivas Listas Blancas locales asociadas a las personas de contactos. En el caso de RedIRIS se incorporaron a la zona MTAwl de la Lista Blanca.

RedIRIS desde principios de septiembre es miembro del MAAWG y esperamos que la experiencia y los documentos de Buenas Practicas generados por los diferentes grupos de trabajo sean de utilidad para la Comunidad RedIRIS.

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

Medalla al Mérito Militar

- Tomás de Miguel recibe la condecoración por su contribución a la UME

El Director de RedIRIS, Tomás de Miguel, ha recibido la medalla al Mérito Militar por su contribución a la Unidad Militar de Emergencias. El acto, llevado a cabo con motivo de la celebración del Día Institucional de la Unidad Militar de Emergencias (UME), se celebró el 7 de octubre en la Base Aérea de Torrejón. La ceremonia estuvo presidida por el Ministro de Defensa, José Antonio Alonso.

La Unidad Militar de Emergencias (UME) es un instrumento del Estado, aprobado en 2005 por el Consejo de Ministros, para garantizar la seguridad y el bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas.

La mayoría de los centros que pueden aportar datos están afiliados a RedIRIS: Instituto Nacional de Meteorología, Instituto Geográfico Nacional o el Instituto Español de Oceanografía, entre otros. Por este motivo se ha puesto en marcha una iniciativa que tiene por objetivo utilizar la Red Académica Española RedIRIS para transferir los datos de los centros que disponen de información relevante para la Unidad Militar de Emergencias.

La implantación de este sistema contempla estas ventajas:

- La red se ha podido desplegar en plazos muy reducidos, sin necesidad de contratar enlaces adicionales, aprovechando la conexión a RedIRIS de que disponen dichas instituciones en unos casos o conectando con el punto de presencia más cercano en otros.
- El coste del despliegue ha sido muy reducido.
- El impacto sobre la red académica ha sido prácticamente nulo, ya que la nueva red consume menos de la milésima parte de la capacidad disponible.
- La fiabilidad de la comunicación entre los centros es muy elevada, al aprovechar las características de red mallada y redundante de que dispone RedIRIS.
- Se garantiza la privacidad de los datos transferidos al utilizar la tecnología de red virtual, que permite aislar el tráfico de RENEM del resto de las comunicaciones de RedIRIS.

En RENEM participan instituciones de investigación que proporcionan datos meteorológicos, sismológicos, etc. y organismos ajenos a la investigación de todas las comunidades autónomas que intervienen o coordinan los servicios en caso de catástrofe como protección civil.

Más información: *www.rediris.es*

Cristina Lorenzo
(cristina.lorenzo@rediris.es)
Coordinadora de Relaciones Externas

Reunión de CSIRTs

- Pretenden reunirse periódicamente para lograr la mayor efectividad en sus servicios

El 24 de octubre los CSIRTs españoles se reunieron en las instalaciones de red.es, en Madrid, para presentar sus diferentes competencias, compartir experiencias y aunar esfuerzos y sinergias para conseguir establecer marcos de colaboración entre los diferentes organismos. Objetivo fundamental, sobre todo desde el nuevo marco establecido, ya que hasta hace año y medio solo existían en España un único CSIRT nivel nacional, IRIS-CERT, y en la actualidad hay seis equipos de seguridad.

Los CSIRTs pretenden reunirse periódicamente, para lograr la mayor efectividad en sus servicios.

En cuanto a funciones, aparte de atender incidentes, los CSIRTs tienen un catálogo de

RedIRIS desde principios de septiembre es miembro de MAAWG

El Director de RedIRIS recibe la Medalla al Mérito Militar por su contribución a la UME

servicios definidos que adaptan a las necesidades de las comunidades a las que sirven.

Cristina Lorenzo
(cristina.lorenzo@rediris.es)
Coordinadora de Relaciones Externas

JJTT Y GGTT 2007

• Se celebraron en el Campus de Mieres

Las JJTT de RedIRIS se celebraron en el Campus de Mieres del 21 al 23 de noviembre

El edificio Científico y Tecnológico del Campus de Mieres (Universidad de Oviedo) acogió del 21 al 23 de noviembre las XVIII Jornadas Técnicas de RedIRIS, red académica española dependiente de Red.es. En esta edición, se dieron cita más de 500 expertos en Tecnologías de la Información y la Comunicación (TIC) procedentes de las diferentes universidades y centros de investigación integrados en RedIRIS, y profesionales de empresas tecnológicas, con el objetivo de intercambiar información y experiencias.

Durante los tres días en los que se llevó a cabo el encuentro, se realizaron diversas sesiones paralelas con ponencias sobre diferentes temáticas, como modelos federados de identidad, colaboración y e-*Ciencia*, grid, seguridad, servicios multimedia, virtualización o monitorización. Además se realizó una sesión paralela, por videoconferencia, con CLARA (asociación de redes académicas y de investigación de América Latina).

Este encuentro estuvo precedido, como es habitual, por los Grupos de Trabajo, que se celebraron los días 19 y 20 en el mismo centro. Además, durante esos días, se llevó a cabo en paralelo un curso sobre Grids y una Reunión de RedIRIS con las Redes Académicas y de Investigación Autonómicas.

Cristina Lorenzo
(cristina.lorenzo@rediris.es)
Coordinadora de Relaciones Externas

Nombramientos

• Colaboración internacional

Chelo Malagón ha sido nombrada miembro del Trusted Introducer (TI) Review Board, en la pasada reunión de equipos acreditados del Servicio TI de TERENA. Ocupará el cargo durante los próximos tres años. Entre su labor destaca repasar las funciones del TI y dirigir las publicaciones especiales que podrían ser resultado del Trusted Introducer.

Francisco Monserrat ha sido nombrado miembro del Steering Committee del FIRST por dos años, y es miembro de la Junta Directiva del FIRST.INC, una organización sin ánimo de lucro de este organismo. En la actualidad está participando en la realización de un plan director para FIRST y también está centrado en temas de educación y de preparación de reuniones técnicas.

Cristina Lorenzo
(cristina.lorenzo@rediris.es)
Coordinadora de Relaciones Externas