Actualidad de Red

Durante estos últimos meses la red nacional ha permanecido muy estable en cuanto a cambios en enlaces o equipamiento se refiere. Dicha infraestructura ha soportado varios proyectos que requerían unas necesidades especiales. Este es el caso de *ATRIUM* proyecto que interconectaba Telefónica I+D en España con VTHD en Francia a través de la red GÉANT y RENATER (NREN francesa), utilizando una red privada virtual de nivel 2 configurada con MPLS (http://www.alcatel.be/atrium).

También el proyecto *Opera Oberta* finalizó su segunda temporada con la transmisión de la última ópera el pasado 24 de marzo. Estas transmisiones se realizan sobre la red multicast nativa con una demanda de ancho de banda superior a los 11 Mbps. Esta temporada han sido 27 las universidades que han participado en el proyecto (http://opera-oberta.liceubarcelona.com). Se han hecho pruebas de transmisión con la Universidad Nal. Autónoma de Méjico con resultados satisfactorios.

En enero de este año tuvo lugar un evento en Bruselas organizado por la Comisión Europea con ocasión del lanzamiento del servicio IPv6 (Global IPv6 Summit, http://www.global-ipv6.net/) Durante ese evento, como veremos más adelante, una de las demostraciones de uso de la red IPv6 nativa fue la transferencia de video de alta definición desde la UPC hasta la sede de la conferencia.

En los próximos meses nos esperan cambios importantes. Además de alguna actualización de hardware, el cambio más importante será la migración de los routers centrales de la red a otra ubicación, aún pendiente de determinar ya que su decisión será fruto de un concurso público que se lanzará próximamente. Actualmente estamos elaborando el plan de migración de forma coordinada con los operadores de los enlaces de todos los equipos de forma que se minimice el impacto en el servicio de la red y el tiempo de migración.

Seguiremos informando sobre este punto.

• GÉANT

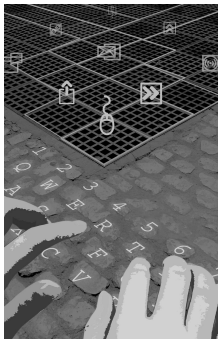
La conectividad con GÉANT se modificó significativamente mejorando tanto en capacidad como en fiabilidad. Así el pasado 7 de octubre entró en operación una lambda (sin protección) de 10 Gbps como enlace de conexión con GÉANT. El enlace que hasta ese momento teníamos de 2,5 Gbps (con protección óptica) se mantiene como enlace de respaldo, aunque eliminando la protección y proporcionando de esta forma no sólo una gran fiabilidad a nivel de enlace (ambas lambdas están configuradas por rutas físicas distintas) sino también a nivel de puerto físico en el router.

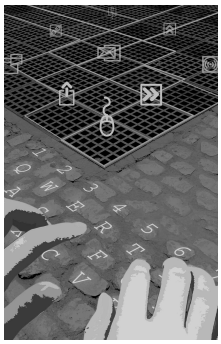
Este aumento de capacidad de conexión entre RedIRIS y GÈANT a 10 Gbps se soporta con la actualización de los dos enlaces de GÈANT que llegan a España; los enlaces Madrid-Milán y Madrid-París también se han visto aumentados a 10 Gbps.

La conectividad de GÈANT con otras redes mundiales de investigación también se ha visto incrementada. Anteriormente la red pan-europea proporcionaba tres enlaces de STM-64 (2,5 Gbps) para la interconexión con las redes del continente americano (ABILENE, CANARIE y Esnet) y desde finales del año pasado se puso en operación una lambda de 10 Gbps financiada por la National Science Foundation (NSF) de las que un enlace de 2,5 Gbps + 2 enlaces GE se utilizan para tráfico en producción con estas redes. Esta conectividad global se ve incrementada con el enlace 2,5 Gbps con SINET la red de investigación japonesa.

• Situación de la conectividad IPv6

Durante el segundo trimestre del año 2003 se diseñó, planificó e implementó el soporte IPv6 nativo en la red. La conectividad con GÉANT soporta IPv6 nativo. Las conexiones con la Internet comercial global también soportan IPv6 pero a través de un túnel (por limitaciones del operador) y -como se verá en el siguiente punto– son varios los operadores con los se ha establecido un peering IPv6 (a través de un túnel) en ESPANIX.





Actualidad de Red

El rango de direccionamiento IPv6 del 6bone, debe ser liberado y devuelto sustituyéndose por el perteneciente a RIPE antes del 6/6/2006. Aunque por un acuerdo global entre las NRENs europeas, por GÉANT ya no se enruta este rango desde enero 2004 (plazos anunciados en varias ocasiones por la lista IRIS-IP). Se puede solicitar direccionamiento en: http://www.rediris.es/red/iris-ipv6/direccionamientoipv6.html

Una vez que las redes de ámbito nacional e internacional soportan el protocolo, el siguiente paso es en las instituciones –en caso de no haberse dado ya–. Con el fin de obtener información sobre el despliegue de IPv6 en ellas, desde RedIRIS se lanzó una encuesta cuyo resultado fue el siguiente:

- 14 respuestas recibidas.
- 3 tienen conexión nativa o a través de túnel.
- 5 tienen direccionamiento IPv6 asignado (del bloque asignado por RIPE a RedIRIS).
- 9 no tienen nada.

En general de los que tienen conexión IPv6, entre el 0-6% de los usuarios tienen acceso a la red IPv6 (con una excepción, donde el 20% de los usuarios tienen acceso a la red IPv6)

Y si tomamos los datos reales del NOC en cuanto a conexiones funcionando y peticiones de direccionamiento realizadas el resultado es:

- 13 asignaciones realizadas a instituciones (del bloque asignado a RedIRIS por RIPE)
- 2 asignaciones a proyectos.
- 5 conexiones nativas (incluyendo dos redes autonómicas)
- 2 conexiones con túneles.

Estos resultados (tomando la referencia de las más de 250 instituciones a las que se da servicio) ponen de manifiesto que el despliegue en las instituciones en España es muy pequeño aunque prácticamente igual al que se observa en otras redes europeas de nuestro entorno, por lo que aún queda mucho trabajo por hacer en este campo.

• Multicast IPv6

Desde el pasado 15 de Junio, RedIRIS dispone de conexión multicast IPv6. Esta conexión se ha realizado a la red m6bone (www.m6bone.net), mediante un túnel, ya que en GÉANT no se dispone de IPv6 multicast nativo.

Los centros conectados a la red, que dispongan de conexión IPv6 unicast, se pueden conectar a la red IPv6 multicast también mediante un túnel a un router Cisco situado en Madrid.

De esta forma, se inicia la experimentación y familiarización con esta tecnología en la red, como paso previo a su puesta en producción.

Los centros interesados en la conexión pueden realizar su petición a noc@rediris.es

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

Los peerings establecidos en ESPANIX son los siguientes, ordenados según fecha de establecimiento apareciendo en negrita los que además tienen establecido un peering IPv6.

1.- COMUNITEL
2.- INTELIDEAS
3.- DATAGRAMA
4.- SARENET
5.- COLT
6.- LAMBDANET
7.- ONO
8.- RETEVISIÓN
9.- EASYNET
10.- BT
11.- TISCALI
12.- FLAGS
13.- ARSYS
14.- SERVICOM
15.- NTT/VERIO
16.- TELEGLOBE
17.- TELEFÓNICA DATA
18.- FUJITSU
19.- JAZZTEL
20.- YA.COM
21.- INTEROUTE

En CATNIX la situación es la siguiente:

1.- NEXICA
2.- ADAM
3.- ALTECOM
4.- ACENS

• ALICE y EUMEDCONNECT

El proyecto ALICE, cofinanciado por la Comisión Europea cuyo objetivo es desarrollar una infraestructura de comunicaciones para la interconexión de los países de América Latina con GÉANT, ha entrado en su Fase B, la de implementación y operación que se extiende hasta mayo de 2006.

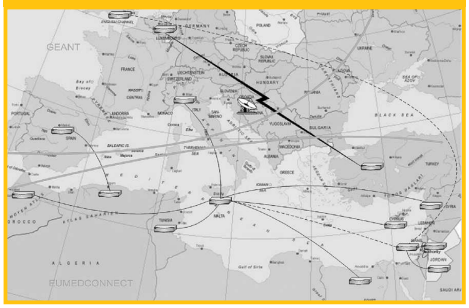
La selección de los operadores que soportarán la infraestructura de la red aún no es pública y está en la última fase. La futura red estará soportada por unos enlaces troncales con topología en anillo STM-1 (155 Mbps) que pasará a través de los Puntos de Presencia (PdPs) situados en Tijuana, Ciudad de Panamá, Santiago de Chile, Buenos Aires y Sao Paulo. El resto de países se conectarán a ellos con velocidades inferiores.

La conectividad internacional con GÉANT vendrá soportada por un enlace STM-4 (622 Mbps.) entre Sao Paulo y Madrid y se espera que con posterioridad esta red latinoamericana cuente con conectividad con Abilene a través de Tijuana.

Recientemente se ha realizado una llamada de interés, entre las redes nacionales latino-americanas más avanzadas para hacerse cargo de los grupos de: a) Ingeniería y planificación de la red y b) su operación respectivamente ganado por RNP (Brásil) y CUDI (Méjico).

EUMEDCONNECT también se trata de un proyecto cofinanciado por la CE y cuyo objetivo es desarrollar una infraestructura que interconecte los países de la Ribera Sur del Mediterráneo.

EUMEDCONNECT



Se encuentra en una fase más avanzada que ALICE y ya están entrando en operación algunos enlaces (p.e. Madrid). Dada la dificultad de tener una infraestructura entre los países de esta zona la topología inicial se basará sobre todo en enlaces directos entre los Puntos de Presencia (PdPs) de estos países y algunos de GÈANT, por ejemplo habrá un enlace directo contra Madrid (PdP de GÉANT en España) y Argelia. De momento el único PdP de esta red estará ubicado en Catania (Italia) y ya se está montando. El equipo que se va a utilizar es un 7512 con tarjetas de STM-1 (155 Mbps) y T3 (45 Mbps) que ha prestado GARR (NREN italiana) al proyecto.

- **XIII TF-NGN en Madrid**

Los pasados 22 y 23 de enero se celebró en Madrid la XIII reunión del grupo de trabajo TF-NGN (www.dante.net/tf-ngn) y las sesiones tuvieron lugar en las instalaciones del Centro de Proceso de Datos de la UCM. En este grupo se tratan nuevas tecnologías de red con aplicación inmediata en la red europea GÈANT.

El primer punto tratado fue el desarrollo de las actividades para este año centrándose los esfuerzos en la implantación, de forma definitiva, de una plataforma de monitorización multicast con acceso restringido por grupo monitorizable. El software utilizado es el beacon server (ver noticia al respecto).

Respecto a IPv6 la línea de trabajo a seguir es probar diferentes herramientas, desplegar looking-glasses y definir una política de seguridad de filtros. También se trabajará en definir e implementar multicast IPv6 en GÉANT.

En la actualidad se trabaja en la creación de un grupo de monitorización del rendimiento de la red (PERT: Performance Response Team) para GÉANT que será similar a un NOC.

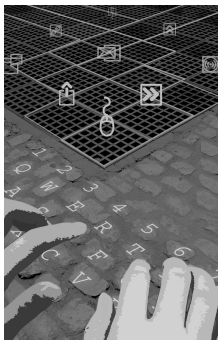
Por último se continuarán realizando pruebas de equipos (equipamiento de Alcatel) y se pondrá en producción la posibilidad de realizar VPNs de nivel 2, a lo largo de toda la red.

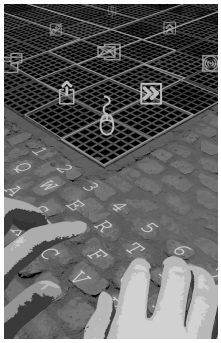
Seguidamente se discutió (a propuesta de Simon Leinen, de SWITCH) la posibilidad de soportar MTUs de tamaño grande (suelen tener un valor de 1500 octetos, siempre en algún punto del camino). Una MTU mayor proporciona mayor capacidad de salida y menor consumo de CPU en los hosts (según pruebas con Gigabit Ethernet) además de disminuir las interacciones con la memoria virtual. Respecto a routing, paquetes de mayor tamaño implican menos paquetes que conmutar en el router y menos trabajo a realizar. La propuesta es empezar a utilizar una MTU de 4470 bytes en los hosts con GigabitEthernet. Debe ser consistente y un inconveniente a tener en cuenta es que una MTU tan grande puede producir sobrecarga debido al proceso de 'MTU discovery' en el caso de caminos con MTU menor. Más información sobre estas pruebas se puede encontrar en www.abilene.iu.edu/jumboMTU.html

Respecto a la monitorización del rendimiento de una red se está trabajando en estos momentos en la implementación de los primeros elementos de la infraestructura de monitorización, considerando la instalación de dos cajas de medidas de RIPE. Asimismo se tendrá una base de datos distribuida en la que se recogerán todo tipo de medidas.

CESNET presentó su proyecto SCAMPI de monitorización de red donde se engloba la herramienta citada anteriormente. El proyecto consiste en un adaptador Hardware, con interfaces Gigabit Ethernet y 10 Gigabit Ethernet y se realiza monitorización del rendimiento de la red mirando el ancho de banda disponible y la pérdida de paquetes, 'jitter' y 'delay'. Todas las medidas se toman a velocidad de la línea.

Englobado en el área de monitorización también se presentó OpenIMP (www.ip-measurement.org/openimp); sistema distribuido de monitorización de Calidad de Servicio.





En IPv6 el siguiente paso es montar multicast en GÉANT. A Juniper se le han hecho diferentes peticiones para implementarlo en el JUNOS (su sistema operativo) y poder ofrecer dicho servicio satisfactoriamente. Las pruebas y evolución del trabajo se pueden seguir en: www.uninett.no/geantmc6/.

Se hizo un repaso a la actualidad de los proyectos europeos de IPv6. En 6NET, ahora están trabajando en movilidad y herramientas de monitorización y concretamente en el M6NET se trabaja para montar multicast IPv6. En este sentido están experimentando con versiones de routers que permitan RP embebido y 'scoped BSR'. Para usar multicast aunque un router no permita PIM se puede utilizar el proxy MLD (existen implementaciones para Linux). Así mismo, se trabaja en 'multicast fiable', utilizando códigos de error que se distribuyen para alcanzar dicha fiabilidad en la red.

Respecto a las líneas de trabajo a seguir en GÉANT se van a centrar en herramientas de monitorización, en seguridad y en multicast, en la promoción del IPv6 y en el servicio de su soporte por parte de las redes nacionales de investigación, con técnicas de transición, servicios preparados para soportar IPv6, gestión y monitorización con dicho protocolo.

- **Grupo de Trabajo ESPX-IPv6**

A finales del año pasado se inauguraron los grupos non-core de Espanix: correo, IPv6 y seguridad. En un primer momento RedIRIS se hace responsable de la coordinación de estos grupos para pasar más tarde el relevo a otros miembros del Espanix, la información acerca del grupo IPv6 está en: http://www.rediris.es/list/info/espx-Ipv6.es.html. Este grupo es la continuación natural del trabajo que se empezó a realizar con la interconexión IPv6 de sus miembros, aunque pretende ir más allá de la simple interconexión. Trata de ser un grupo de trabajo dinámico en el que se involucren los departamentos de I+D de las diferentes empresas y sirva como punto de partida para el despliegue total de IPv6 en la Internet española.

- **Global IPv6 Service Launch Event**

Los pasados 15 y 16 de enero se celebró en Bruselas el 'Global IPv6 Service Launch Event' (www.global-ipv6.net). El evento, patrocinado por la Comisión Europea, tenía como principal objetivo la promoción del IPv6 y dar un importante empuje en sus países miembros para acelerar su implantación. Durante el mismo tuvo especial importancia el trabajo realizado por las redes de investigación de los diferentes países y el realizado en GÉANT con soporte nativo de IPv6. Partiendo de este trabajo desde la Comisión Europea se promulgó el comenzar con el soporte de IPv6 en todo tipo de redes, teniendo en cuenta la importancia que va a tener en el desarrollo de los futuros dispositivos móviles (UMTS e incluso más allá).

Se contó con la asistencia de personalidades políticas de los diferentes países de la Unión, que comentaron las actividades llevadas a cabo dentro de su país con dicho protocolo. En el caso de España, Víctor Izquierdo (Subdirector Gral. de Empresas de la Sociedad de la Información), destacó la labor realizada en RedIRIS y en el Grupo de trabajo español (http://www.spain.ipv6tf.org/html/index.php).

Se aprovechó la ocasión para lanzar iniciativas privadas tales como el anuncio de Telefónica de comenzar a dar servicio IPv6.

- **Multicast Beacon**

Se acaba de poner en marcha una nueva herramienta de monitorización en el área de red: Multicast Beacon (http://dast.nlanr.net/Projects/Beacon/ y http://www.rediris.es/red/stats/IPmcast/beacon). Se trata de una aplicación cliente-servidor basada en perl que mide el funcionamiento de la red multicast. Esta última versión es más ligera que la anterior (basada en java) y el mismo software sirve tanto para el cliente como para el servidor. GÈANT utiliza también esta aplicación para monitorizar el tráfico multicast.

Funciona de la siguiente forma: los clientes envían tráfico basado en el protocolo RTP (RFC 3550, Protocolo de Transporte en Tiempo Real) que lleva asociado un protocolo de control que permite recoger información en tiempo real para poder monitorizar el servicio (retardos, congestión, pérdidas ...). Este tráfico se envía a un grupo multicast definido y los clientes son a la vez emisores y receptores, con lo que en cada momento cada uno de ellos obtiene datos acerca de la calidad de recepción de lo que emite el resto. Esta información se envía a un servidor que publica los datos.

- **Looking Glass**

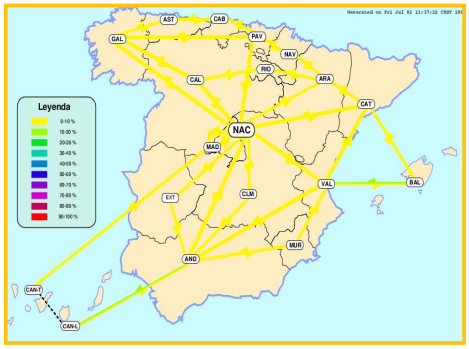
Asimismo, el «looking glass» de RedIRIS (http://www.rediris.es/red/lg/) ha ganado en funcionalidad. Actualmente, es posible realizar en cada router Juniper de la red comandos como

traceroute, ping, listas de AS por ruta, las sesiones SDR activas y el estado del árbol PIM de sesiones multicast existentes. Además, estas consultas pueden efectuarse contra direcciones tanto IPv4 como IPv6.

• Weather Map

RedIRIS ha desarrollado una herramienta para la monitorización de la red de características similares a las ya existentes en otras redes académicas y denominada Weather Map.

Éste mapa, enlazable desde la página web de red: http://www.rediris.es/red, permite visualizar el estado de ocupación de los enlaces nacionales en ambos sentidos en tiempo real, queda aun pendiente la incorporación del estado de los enlaces externos.

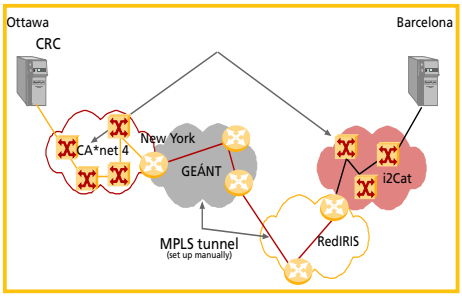


Actualmente, aunque está operativo, se sigue trabajando en la mejora e incorporación de nuevas utilidades que se consideran de interés para los usuarios y esperamos que estén en producción en breve plazo.

• Servicio de VPNs de nivel 2

Respecto a la puesta en producción de nuevos servicios, hay que destacar que recientemente y debido a la realización de una demostración como parte de un proyecto de colaboración entre la Universidad Politécnica de Cataluña y Canarie (red académica canadiense), se le solicitó a RedIRIS la configuración de una VPN (Virtual Private Network) de nivel 2 entre Barcelona y Canarie.

Esta solicitud implicó la configuración de MPLS (Multiprotocol Label Switching Path) y la definición de un LSP (Label Switching Path) redundando a través de la red nacional desde Barcelona hasta GEÁNT, permitiendo así, poner en producción el servicio de VPNs para el evento anteriormente citado y al mismo tiempo poder comprobar su comportamiento en un escenario real en producción. Actualmente el servicio de VPNs se encuentra en fase de pruebas para su puesta en producción.



• XLVII Reunión de RIPE

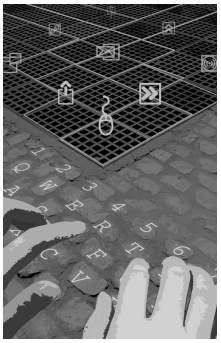
Durante la última semana de enero se celebró en Ámsterdam el cuadragésimo séptimo encuentro de RIPE (http://www.ripe.net /ripe/meetings/ripe47/presentations/index.html). Uno de los temas más interesantes presentados allí fue la creación de CRISP (Cross-Registry Internet Service Protocol) en el grupo de trabajo de base de datos. Se trata de un protocolo que pretende sustituir a WHOIS, cuyos ficheros de datos son inmanejables a partir de un determinado tamaño. De esta forma se unificarían los formatos de las bases de datos de los diferentes RIRs y sería mucho más sencilla su consulta ya que actualmente cada registro regional almacena sus datos en un formato distinto. Este protocolo está basado en XML y ya se ha presentado un draft en el IETF esperando que haya un piloto en funcionamiento para el verano de 2004. Ahora mismo se está estudiando dónde ubicarlo.

En el grupo de trabajo de IPv6, se anunció que RIPE es el registro regional que más prefijos ha asignado. En cuanto al grado de implantación en la red, cabe destacar que ya hay seis root-servers con dirección IPv6 asignada. Por último, se ha propuesto la elaboración de unas recomendaciones para aplicación de filtros.

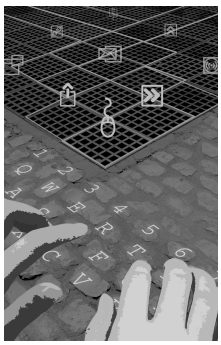
Se celebró la segunda reunión del grupo ENUM (todavía BoF), dirigido a coordinar la implantación de este protocolo. Se presentaron varias experiencias en Japón, Suecia, Polonia, Irlanda y Reino Unido.

En el grupo de routing, se presentaron varias herramientas de configuración remota de routers.

Finalmente, en el grupo de DNS se presentó el proyecto Reverse DNS (http://www.ripe.net/ reverse/rdns-project/) que pretende definir unos procedimientos más estables para la delegación



Actualidad de Red



Actualidad de Red

GN2

X y XI TF-CSIRT de TERENA

de zonas inversas que realiza RIPE. Hasta ahora se solicitaba la delegación y cambios sobre ella a través del buzón auto-inaddr@ripe.net, pero también se permitían, modificaciones en el objeto *domain* de la base de datos mediante el método habitual, lo cuál creaba inconsistencias. Asimismo se está estudiando un nuevo mecanismo de autorización específico para las actuaciones sobre los objetos *dominio*.

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

GN2

Se está preparando el proyecto GN2 (el anterior era GN1 y la red que se está utilizando GÈANT) que dará soporte a la nueva infraestructura de red europea y englobará una serie de servicios y actividades de investigación. Aunque está aún bajo negociación podemos avanzar cuáles son las actividades de investigación que cubrirá (Joint Research Activity, JRA) y en las que RedIRIS participa:

- JRA1: Performance Measurement and Management
- JRA2: Security
- JRA3: Bandwidth Reservation and Allocation
- JRA4: Technology and Service Testing
- JRA5: Ubiquity (Mobility) and Roaming Access to Services

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

X y XI TF-CSIRT de TERENA

La X reunión del TF-CSIRT de TERENA (http://www.terena.nl/tech/task-forces/tf-csirt/), tuvo lugar en Ámsterdam el pasado mes de septiembre y estuvo organizada por el Equipo de Atención de Incidentes de Seguridad de la Red académica holandesa (Surfnet), CERT-NL.

Las presentaciones de la primera jornada se centraron fundamentalmente en dar a conocer distintas iniciativas o desarrollos locales tales como el sistema de análisis de tráfico basado en flujos para la detección de ataques (NERD: Network Emergency Response & Detection) desarrollado por una universidad holandesa para Surfnet. También tuvieron cabida varias presentaciones de equipos de seguridad holandeses tales como la Agencia de Policía Nacional holandesa, el CERT gubernamental (GOVCERT.NL) o el Equipo de Seguridad de la Universidad Groningen. Todas las presentaciones están disponibles en la dirección: http://www.terena.nl/tech/task-forces/tf-csirt/meeting10/programme.html

El resumen de la reunión del Task Force de la segunda jornada, está disponible en http://www.terena.nl/tech/task-forces/tf-csirt/meeting10/TSec_03_120.pdf. Como viene siendo habitual, durante dicha reunión se hizo un repaso de los proyectos europeos en los que el Grupo está o ha colaborado (eCSIRt.net, EISPP y TRANSITS), así como a las diferentes iniciativas en materia de seguridad en las que el Grupo ha estado participando durante los más de tres años de vida del mismo con el fin de impulsar la colaboración entre los CSIRTs europeos y la adquisición de estándares y normas para facilitar el intercambio de información entre ellos.

La XI reunión del TF-CSIRT se celebró en Madrid en enero de 2004 y estuvo organizada por IRIS-CERT con la colaboración de la Universidad Complutense de Madrid que desinteresadamente nos permitió utilizar sus instalaciones en el Centro de Proceso de Datos. Desde aquí, nuestro más sincero agradecimiento.

Tanto las presentaciones de los seminarios del primer día como el resumen de la reunión del Task Force propiamente dicha se pueden consultar en: http://www.terena.nl/tech/task-forces/tf-csirt/previous-meetings.html.

Algo que echamos mucho en falta durante el primer día de la reunión de Madrid fue la escasa participación de instituciones y equipos de seguridad españoles. Esta corrió a cargo de Ricardo Marín, de Red.es y Matías Bevilacqua de la empresa CYBEX.

El segundo día se presentó la iniciativa del Grupo de Trabajo del EGC (European Goverment CSIRTs). Este Grupo que se reúne cada cuatro meses y está compuesto por CSIRTs de ámbito gubernamental de seis países europeos, tiene como finalidad tratar problemas e incidentes relacionados con el ámbito de actuación que afectan a este tipo de equipos, así como el

desarrollo de una serie de actividades paralelas como la implantación de sistemas de alerta, la cooperación de este Grupo con la futura Agencia de Seguridad Europea (ENISA), etc..

Tanto en Ámsterdam como en Madrid se celebró, de forma adyacente a la reunión del TF-CSIRT, una reunión de los equipos acreditados en el servicio de Trusted Introducer de TERENA (http://www.ti.terena.nl/). El acuerdo más importante al que se llegó en estas reuniones fue la propuesta de redacción de un código ético que deberán suscribir todos aquellos equipos que quieran llegar a obtener el grado de equipo acreditado en dicho servicio.

En Madrid, además, se celebraron el día anterior, y de forma paralela, dos reuniones: El Abuse Fórum y un Workshop sobre la utilización de la herramienta Request Tracker/RT for Incident Response, desarrollada por Best Practical (http://www.bestpractical.com/), por la que están apostando un gran número de Equipos de Seguridad como herramienta de gestión de incidentes. Como resultado de la reunión, se ha creado un Grupo de Trabajo entre los CERTs interesados en esta herramienta con la intención de discutir e implementar posibles mejoras y módulos adicionales a incluir en próximas versiones de la misma; por ejemplo un módulo PGP integrado en la propia herramienta o uno que permita el intercambio de incidentes siguiendo el estándar IODEF (Incident Object Description and Exchange Format). Tras esta primera reunión celebrada en Madrid la segunda se celebró en Londres el pasado 10 de febrero. Os seguiremos informando en siguientes números de los progresos y conclusiones alcanzados por el Grupo.

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

Resumen de incidentes de seguridad 2003

En las páginas web del Equipo de Seguridad de RedIRIS se encuentra el informe de los incidentes de seguridad del año 2003 (http://www.rediris.es/cert/doc/informes/2003/).

Se trata de un informe corto y fácil de leer en el que se presentan las estadísticas de los incidentes atendidos durante el 2003 por IRIS-CERT (http://www.rediris.es/cert) y que permite tener una visión general de cuáles han sido los problemas más importantes de seguridad que se han sufrido en la Red Académica y de Investigación española, así como algunos enlaces de interés a los problemas más comunes.

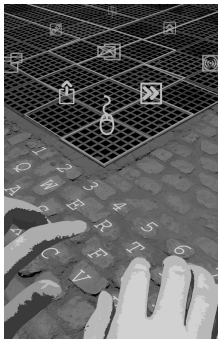
Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de Seguridad IRIS-CERT

I reunión del Grupo de Trabajo sobre RTIR

El pasado 14 de enero se celebró en Madrid la primera reunión del grupo de trabajo sobre el RTIR (Request Tracker for Incident Response, http://www.bestpractical.com/rtir), bajo el marco del grupo de trabajo de TERENA TF-CSIRT (Coordination and Support of Computer Security Incident Response Teams). El RTIR es un módulo de la herramienta RT (Request Tracker, http://www.bestpractical.com/rt) para la gestión y administración de incidentes de seguridad, desarrollada por Best Practical (http://www.bestpractical.com), dicho módulo fue creado a petición del grupo de seguridad de la red académica del Reino Unido (JANET-CERT), para adaptar RT a su "workflow" de atención de incidentes. A lo largo del pasado año, IRIS-CERT tomó la decisión de migrar a esta herramienta de atención de incidentes y abandonar su actual sistema con el fin de mejorar el servicio que se viene ofreciendo.

A la reunión asistieron algunos de los CSIRTs europeos que están utilizando la herramienta (JANET-CERT, CERT-Polska, CERT.PT,...) o están en vías de migrar a ella pronto (IRIS-CERT, SURFNet, CARNet, ACONet-IRT, ...), junto con responsables de BestPractical. Los objetivos iniciales eran definir los requerimientos para nuevas funcionalidades a añadir en RTIR, la prioridad en la implementación; la búsqueda de un marco adecuado para la creación de un consorcio, que bajo el paraguas -por ejemplo- de TERENA, tuviese como objetivo encontrar la financiación necesaria para afrontar dicho desarrollo y por último compartir los desarrollos que algunos CSIRTs habían estado realizando, de forma que se pudiese llegar a un grado importante de coordinación entre todos y evitar así repetir implementaciones.

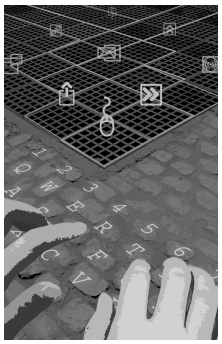
Todo esto trajo consigo una serie de discusiones sobre las funcionalidades a añadir y se decidió



X y XI TF-CSIRT de TERENA

Resumen de incidentes de seguridad 2003

I reunión del Grupo de Trabajo sobre RTIR



I reunión del Grupo de Trabajo sobre RTIR

Proyecto eCSIRT.Net

finalmente la implementación de un módulo PGP, para verificar la integridad y la autenticación de los mensajes que lleguen a la cuenta asociada al RTIR; integración de IODEF (Incident Object Description and Exchange Format) y módulo de contactos que permita búsquedas sobre BBDD de contactos de personas.

Carlos Fuentes
(c.fuentes@ukerna.ac.uk)

Proyecto eCSIRT.Net

En enero de 2001 arrancó el proyecto eCSIRT.Net (http://www.ecsirt.net) nacido en el seno del grupo de trabajo de TERENA TF-CSIRT (Coordination and Support of Computer Security Incident Response Teams: http://www.terena.nl/tech/task-forces/tf-csirt/). Se creó con el objeto de cumplir los siguientes objetivos:

- Definir un formato claro y estandarizado para el intercambio de incidentes entre los equipos involucrados.
- Permitir la elaboración de estadísticas claras y estandarizadas sobre incidentes y crear un acceso público a las mismas.
- Permitir la recopilación de información sobre incidentes, para posteriormente, generar una serie de alertas que puedan ayudar a los equipos involucrados.

A lo largo de los dos últimos años se han probado una serie de técnicas y se han definido una serie de formas de actuación para llegar a la consecución de los objetivos del proyecto. De esta forma se logró consensuar entre todos los equipos del proyecto un código de conducta (http://www.ecsirt.net/service/documents/code_of_conduct/coc.html) donde se establecían las formas de cooperar y compartir información y crear así una mayor confianza entre los equipos. Además se ha estado apoyando la estandarización y el uso del IODEF (Incident Object Description and Exchange Format: http://www.iodef.org/), para ello se definió un lenguaje común en el que se describían inequívocamente todos los campos del objeto así como su utilización eliminando por tanto cualquier ambigüedad que pudiera existir al utilizarlo. Además cada uno de los equipos adaptaron sus sistemas de gestión de incidentes para la recepción y envió de estos usando IODEF, probando de esta manera la tecnología que se había desarrollado para el objeto por parte del grupo de trabajo INCH del IETF.

El proyecto generó tres diferentes tipos de estadísticas que reflejaban la carga de trabajo y recursos gastados en la gestión de incidentes **(Tipo 1),** los incidentes gestionados por los equipos clasificados en base a la taxonomía de alto nivel definida en el proyecto **(Tipo 2),** y las estadísticas sobre ataques realizados en la red de sensores IDS desplegada por el proyecto **(Tipo 3).** Cabe resaltar que la recopilación de la información de los IDSs se realiza automáticamente utilizando como protocolo de intercambio de información de los logs **IDMEF** (Intrusion Detection Message Exchange Format).

Por último, se definió la Alert Function (http://www.ecsirt.net/service/documents/wp5-alert-policy-v11.html) de forma que los equipos dispusiesen de un mecanismo eficaz para enviar y recibir alertas sobre posibles nuevos incidentes detectados por alguno de los equipos integrantes. Para esto se definieron una serie de mecanismos para enviar y recibir dichas alertas, teniendo en cuenta que los integrantes de los equipos pudiesen estar en horario de oficina (In-Bound) o fuera de él (Out-Bound) y utilizando IODEF como formato para transmitir las alertas.

El proyecto acabó el 31 de diciembre y sus resultados fueron evaluados por los interventores de la Comisión Europea como muy satisfactorios. Se espera que todo el trabajo llevado a cabo sirva como punto de partida para futuros desarrollos en este campo.

En la actualidad y tras la conclusión del proyecto se están estudiando diferentes vías para continuar con los resultados obtenidos debido a la amplia aceptación que han tenido dentro del grupo de trabajo TF-CSIRT y de los beneficios que se podrían obtener a partir de ellos. El principal problema en estos momentos para poder seguir manteniendo la infraestructura creada es el monetario. Una de las soluciones más factibles sería la integración de los resultados del proyecto como nuevos servicios del Trusted Introducer (http://ti.terena.nl) de TERENA, de forma que todos los integrantes del mismo, la mayoría de los CERTs europeos se viesen beneficiados.

Durante el último semestre del pasado año se celebraron dos reuniones de coordinación del proyecto. En ellas se llevó a cabo el seguimiento del estado del mismo y el cumplimiento de las tareas que habían sido encomendadas a cada uno de los CSIRTs involucrados.

La primera se celebró el 18 de octubre en Londres. En ella cada uno de los CSIRTs presentó

el estado en el que se encontraba la implantación de IODEF dentro de sus sistemas de gestión de incidentes, informando sobre la librería utilizada para dicha integración. Posteriormente se estableció un calendario para la realización de una serie de pruebas de intercambio de IODEF entre los CSIRTs de forma que se pudiese probar que todos los equipos podían intercambiar incidentes de seguridad dentro de sus BBDD de incidentes. Se informó que el sistema de alerta estaba prácticamente operativo a falta de poner en marcha la parte de envío de alertas a través de mensajes SMS y se discutió sobre cómo se debían confirmar los diferentes tipos de alertas y cuáles debían ser los tiempos de respuesta para cada una de ellas.

La última parte de la reunión se centró en las estadísticas (http://www.ecsirt.net/service/documents/wp4-pub-userguide-v10.html) de tipo 1 (Información sobre operación de los CSIRT) y 2 (Información sobre incidentes) –generadas manualmente rellenando una serie de formularios web–, ya que algunos equipos mostraron su desacuerdo con los actuales formularios al considerar no recogían lo suficientemente bien la información requerida, además que no se ajustaba a la información que la mayoría de los CSIRTs almacenaban en sus BBDD. Toda esta discusión nos llevó a la modificación de la taxonomía de alto nivel (http://www.ecsirt.net/service/ documents/wp4-clearinghouse-policy-v12.html#HEAD6), de forma que se ajustase de mejor manera a las utilizadas por cada unos de los integrantes del proyecto para clasificar sus incidentes.

La segunda reunión fue el 10 de diciembre en Madrid, en la oficinas de RedIRIS. El principal objetivo fue evaluar el resultado de las primeras pruebas de intercambio realizadas con el IODEF unas semanas antes de la reunión así como ver los problemas que se habían planteado durante su realización. Se acordaron una serie de directivas para subsanar los errores encontrados, y para la implantación de la firma GPG de los objetos IODEF en las posteriores pruebas que iban a ser realizadas la semana siguiente a la reunión.

También por parte de Pre-Secure se mostró cómo quedarían los interfaces para cada uno de los diferentes tipos de estadísticas quedando así esta parte prácticamente concluida a falta de que algunos equipos introdujesen sus datos de los últimos meses del año.

La última parte de la reunión se dedicó a la función de Alerta, última fase del proyecto. Pre-Secure informó que todos los sistemas estaban totalmente operativos a falta sólo de realizar los tests definitivos que confirmasen dicho estado. Para ello se estableció un calendario de pruebas, tanto para la generación de alertas de seguridad a través del sistema, como para la recepción de las mismas en la modalidad In-Bound (en horas de oficina) y Out-Bound (fuera de horario laboral). Para estas pruebas el personal de Pre-Secure se comprometió a realizar una mini-guía *how-to* para la realización de las mismas.

Carlos Fuentes
(c.fuentes@ukerna.ac.uk)

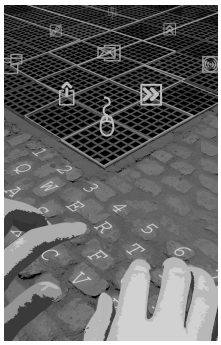
Resultados del reto de análisis forense

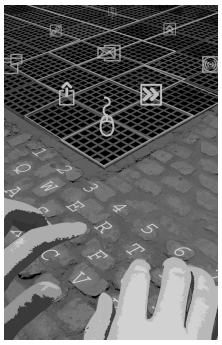
Con algo de retraso respecto a las fechas previstas –inicialmente a finales del año 2003– se desarrolló un reto de análisis forense organizado por RedIRIS (http://www.rediris.es/cert/ped/reto). El reto consistía en analizar la información contenida en un equipo previamente atacado para intentar obtener toda la información posible sobre las acciones realizadas por el atacante.

Este equipo formaba parte de una red de máquinas trampas (http://www.rediris.es/cert/ped) en una red dentro de RedIRIS, con una configuración de sistema operativo y servicios similar a la de otros sistemas instalados en instituciones afiliadas, y aunque externamente parecía un equipo normal en realidad se encontraba monitorizado y controlado para detectar cuándo se producía el ataque.

Como precedente de este reto se produjo en el año 2001 el *Honeynet Forensic Challenge* (http://www.honeynet.org/challenge/index.html), presentado por el grupo del proyecto HoneyNet, aunque esta es la primera iniciativa de este tipo que se realiza en castellano. El reto se realizó con dos objetivos:

a) Fomentar el empleo de técnicas de análisis forense para analizar los ataques que se producen en los equipos conectados a RedIRIS, de forma que los responsables de los centros estén familiarizados con las técnicas de análisis forense y tengan información sobre cómo actuar en estas situaciones.
b) Recopilar casos prácticos en castellano sobre cómo proceder a realizar un análisis forense, de forma que pudiera servir de guía práctica





Resultados del reto de análisis forense

Emisiones en alta calidad

Global Dialing Scheme

a todas aquellas personas interesadas en el análisis forense.

El reto solicitaba el envío de tres documentos a cada participante:

1.- Un fichero con la información de contacto de los participantes ya que el resto de documentos enviados deberían ser anónimos.
2.- Un resumen de tres a cinco páginas no técnico (informe ejecutivo) donde se comentasen los motivos de la intrusión, el análisis realizado y recomendaciones (lecciones aprendidas) sobre este incidente:
3.- Un informe técnico de la intrusión con la descripción en profundidad del análisis realizado; la longitud máxima de este informe no debería exceder las 60 páginas.

El jurado encargado de evaluar este resultado estuvo integrado por las siguientes personas:

- Rubén Aquino *(UNAM-CERT, Universidad Nacional de México)*
- David Barroso *(S21Sec)*
- Javier Fernández-Sanguino *(Germinus)*
- Jess García *(LAEFF-INTA/ SANS Institute)*
- Jordi Linares *(Cybex)*
- Borja Marcos *(Sarenet)*
- Francisco Monserrat *(IRIS-CERT, RedIRIS)*
- Jacomo Piccolini *(CAIS/RNP, red brasileña)*

Hay que destacar en primer lugar la calidad de los informes presentados por los participantes. Aunque al final ha habido algunos con una puntuación más elevada que otros todos los trabajos demuestran un profundo conocimiento de las técnicas a aplicar a la hora de analizar un equipo atacado de estas características.

Es interesante resaltar las diversas aproximaciones realizadas para llevar a cabo el análisis de un equipo, así por ejemplo para localizar los binarios instalados unos participantes emplearon los tiempos de modificación de los ficheros, (para averiguar qué ficheros habían sido modificados tras la instalación) y otros realizaron comparaciones de los ficheros con las huellas digitales (MD5) de sistemas con la misma distribución de Linux o emplearon las utilidades del sistema (base de datos rpm) para este fin.

Para todos los interesados en las técnicas de análisis forense la lectura de los documentos presentados aportará seguramente información valiosa a la hora de realizar un análisis.

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

Emisiones en alta calidad

Hace unos meses en colaboración con el CESGA y la UC3M iniciamos emisiones en pruebas en varios formatos, MPEG-1, MPEG-2, MPEG-4 y divX, con distintos bitrates utilizando tecnología multicast. El objetivo es hacer un banco de ensayo para probar nuevas posibilidades de la red. Como resultado hemos creado un canal en emisión continua que puede ser usada para que los receptores puedan comprobar sus configuraciones así como de demostración tecnológica de las capacidades de la nueva red.

Tanto para la emisión como para las pruebas de recepción hemos utilizado las herramientas *Open Source* (http://www.videolan.org) del proyecto francés Videolan .

En la actualidad se emite en bucle un vídeo en MPEG-2 a 8.6 Mbps procedente de un DVD sobre la red europea Geànt producido por Dante. Este vídeo ha sido doblado al castellano y al gallego por el CESGA.

Para recibir esta emisión es necesario soporte multicast y el cliente vlc que se puede bajar de la página de videolan para varias plataformas. Activar SAP al lanzar el cliente (opción—extraintf sap) y en la lista de reproducción al cabo de unos instantes aparecerá una entrada llamada RedIRIS-TV (http://www.rediris.es/mmedia/RedIRIS-TV.es.html).

En la lista de reproducción podremos ver otras emisiones como el canal UC3M-TV con emisiones continuas de vídeos grabados o en directo: cursos de humanidades del proyecto de docencia compartida ADAMADRID, actos institucionales, ... todo ello con calidad MPEG-2 a 3 Mbits.

Desde otras instituciones se ha mostrado interés en volcar sus canales de TV a la red y en breve podremos verlos anunciados en la lista de reproducción de la herramienta vlc.

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

Global Dialing Scheme

Global Dialing Scheme (GDS) es el plan de numeración utilizado para vídeo y audio sobre IP en la redes académicas y de I+D y en VideNet, una de las mayores redes de videoconferencia. Fue desarrollado por la organización europea

TERENA y se asemeja al plan de numeración internacional usado en el sistema telefónico con algunas diferencias. Si un terminal H.323 está registrado en un Gatekeeper conectado a la jerarquía GDS podrá alcanzar a cualquier terminal, MCU o gateway que use GDS en cualquier punto del mundo.

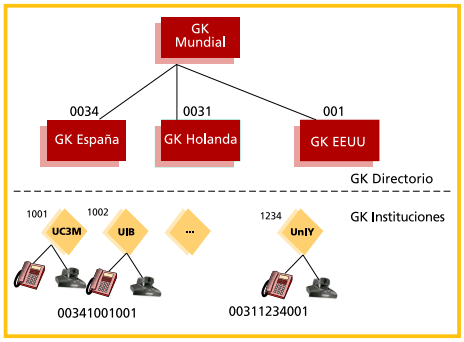
Un número E.164 en GDS consta de las siguientes partes:

1.- El Código de Acceso Internacional (CAI), también conocido como prefijo del gatekeeper mundial. Se define como 00.
2.- Un Código de País (CP). Éste se obtiene del sistema de códigos internacional definido por la ITU (International Telecommunication Unión). El prefijo para España es 34. Se puede encontrar la lista completa en: http://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_717.pdf
3.- Prefijo de la Organización (PO). GDS no dice cómo son asignados estos prefijos y existen varias alternativas, más adelante veremos cuál ha sido el plan que hemos adoptado.
4.- Número de Terminal (NT) Puede pertenecer a un terminal de videoconferencia, una MCU o un gateway. Éste se decide dentro de la organización y no está fijado ni por GDS ni por el plan nacional, aunque se pueden dar recomendaciones como por ejemplo la longitud del número.

El número completo queda así:
<CAI><CP><PO><NT>

Por ejemplo: 00(CAI) 34 (CP) 1000 (PO) 001 (NT)
GDS delega en cada país la utilización de su propio sistema de numeración, siempre que siga algunas reglas, de la misma forma que RedIRIS delega en cada institución la adopción del suyo propio siguiendo también algunas normas (http://www.rediris.es/mmedia/GDS/).

Los Prefijos de organización son asignados secuencialmente por orden de llegada a las instituciones afiliadas a RedIRIS.



GDS se implementa como una jerarquía de gatekeepers de una forma parecida al DNS:

- Hay un gatekeeper mundial; en realidad hay varios por redundancia pero se comportan como si sólo hubiera uno. En este gatekeeper no hay ningún elemento registrado (ni MCUs, ni terminales, ni gateways), funciona como directorio de gatekeepers reenviando mensajes de localización (LRQ, LCF y LRJ). Conoce sólo acerca de los gatekeepers nacionales.
- Un gatekeeper por cada país que suele ser operado por la red nacional de I+D. En RedIRIS se ha puesto en funcionamiento el gatekeeper nacional para España. Estos funcionan de forma análoga al mundial; en ellos tampoco hay terminales registrados, reencaminan mensajes de localización y saben acerca de los gatekeepers de instituciones.
- Gateepers de instituciones. En ellos los terminales están registrados y pueden implementar la política local. Pueden funcionar en varios modos: señalización directa entre terminales, con encaminamiento del tráfico H.225/H.245, y en modo proxy (todo el tráfico multimedia pasa por el gatekeeper). Estas distintas alternativas dependen de la política que quiera adoptar la institución, del grado de control y del tamaño del servicio, puesto que existen consideraciones de escalabilidad según la solución.

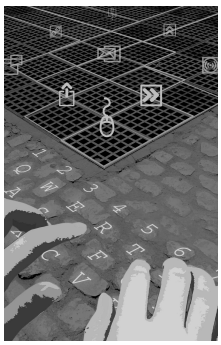
La implementación que hemos realizado consta de un router CISCO 2600 con MCM (que forma parte del IOS) como gatekeeper nacional y como gatekeeper de RedIRIS-institución un gnugk (www.gnugk.org)

GDS permite y hace fácil la utilización de servicios de videoconferencia o voz sobre IP (VoIP) constituyendo una infraestructura básica sobre la que se podrán desarrollar nuevos servicios avanzados.

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

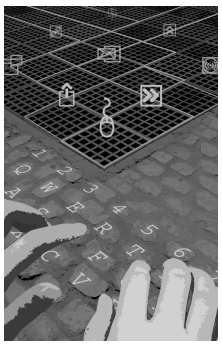
Piloto RDV

Desde que en 1996 se inició un servicio de multicast –entonces piloto– hasta el momento que se considera ya en producción, se ha visto que la tecnología multicast es la más adecuada para solventar los problemas de escalabilidad. No obstante, por varios factores, entre ellos consideraciones de seguridad y en ocasiones



Global Dialing Scheme

Piloto RDV



Piloto RDV

II Seminario sobre tecnologías de autenticación y autorización

Reunión del grupo TF-AACE

desconocimiento de la tecnología, ocurre que este soporte para IP multicast no alcanza al usuario final.

En el servicio de streaming existen momentos puntuales en que, debido a la emisión de eventos importantes en directo, la capacidad de los servidores y líneas de las organizaciones son puestas a prueba, mientras que en otros centros existen servidores ociosos, desde los cuales sería viable enviar el stream a las IPs más cercanas.

Para la entrega de contenido de vídeo en directo hace falta algún mecanismo que sea mínimamente escalable, una propuesta que surgió dentro del grupo IRIS-MMEDIA es desarrollar un software en principio simple, pero con posibilidades de crecimiento, que implementara ALM (Application Level Multicast). Los objetivos son:

- Desde el punto de vista de red: evitar congestión en los enlaces más cercanos a los servidores (por ej. accesos de las instituciones) en eventos en directo que sean seguidos desde el exterior.
- Desde el punto de vista de sistemas: balancear la distribución de vídeo entre distintos servidores, permitiendo la compartición de recursos ociosos entre instituciones.
- Extraer conocimiento que pueda ser usado para implementar un servicio en producción.

Existen varios mecanismos para implementar este comportamiento:

- Redirecciones DNS
- Información basada en distintas métricas (saltos, retraso, etc.).
- Mensajes de redirección: por ejemplo mensajes 302 de RTSP, estos mensajes no son soportados por todos los protocolos de streaming.
- Decisión basada en tabla estática.

Teniendo en cuenta las características de nuestra red y la facilidad de implementación se ha optado por el último mecanismo. Sabemos cuales son las subredes que conecta cada institución y estas cambian relativamente poco, con lo cual podemos generar un archivo que es compartido por todos los reflectores de la red.

El software ha sido desarrollado en la UC3M y en un principio se han utilizado servidores Windows Media, por ser lo más sencillo, no obstante sería simple adaptar a otros servidores de streaming.

Esta iniciativa está abierta a nuevos miembros dentro de la comunidad. (http://www.rediris.es/mmedia/rdv/)

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

II Seminario de tecnologías de autenticación y autorización

El segundo seminario sobre tecnologías de autenticación y autorización (AA), auspiciado por el grupo TF-AACE de TERENA, se celebró en la Universidad de Málaga los pasados días 20 y 21 de noviembre. Reunió a unas 40 personas, provenientes de Europa y Estados Unidos.

El primer día, las presentaciones y discusiones se concentraron en los escenarios de aplicación de estas tecnologías desde distintos puntos de vista: proveedores de contenidos, bibliotecas, grids, usuarios móviles, integración de servicios, videoconferencia y servicios multimedia. También se presentaron nuevas propuestas de tecnologías, en las áreas de modelos de autorización y de protocolos criptográficos.

El segundo día se dedicó a revisar el estado actual de las infraestructuras de AA en Europa y el resto del mundo, analizando las opciones para garantizar su interoperabilidad. El concepto de federación y su relación con las infraestructuras de clave pública fue considerada la clave para esta interoperabilidad. También se presentaron las iniciativas de proyectos europeos (GN2 y GRANDE) que, de una manera u otra, planean incorporar el uso de tecnologías de AA en el nivel de red.

Se puede encontrar más información al respecto en: http://www.terena.nl/tech/task-forces/tf-aace/AAworkshop/

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

Reunión del grupo TF-AACE

Con posterioridad al II seminario sobre tecnologías de AA (ya reseñado) se celebró también en Málaga una reunión del grupo TF-AACE (Task Force on Authentication and

Authorisation Coordination for Europe, http://www.terena.nl/tech/task-forces/tf-aace/). El trabajo del grupo se centró en los siguientes puntos:

- Aprobar la política del repositorio de CAs académicas de TERENA (TACAR, http://www.terena.nl/tech/task-forces/tf-aace/tacar/), una iniciativa que pretende facilitar el establecimiento de relaciones de confianza entre las diferentes PKIs académicas a nivel global. La política del TACAR se está aplicando ya, y cinco PKIs académica (española, holandesa, checa, griega y la de los grids del Dpto. de Energía de los EEUU) forman parte del mismo. La iniciativa ha despertado un gran interés entre los grupos que utilizan PKIs en el entorno académico y científico y el TACAR es mencionado como uno de los pilares para construir políticas comunes de acceso a los recursos de e-ciencia en el borrador del libro blanco del eIRG (e-Infrastructre Reflection Group), un grupo encargado de definir las direcciones del desarrollo de la e-ciencia y sus posibles aplicaciones en la Unión Europea.
- Discutir el desarrollo del AA-RR (AA Requester-Responder), un sistema para la validación de los requisitos de inter-operabilidad entre diferentes infraestructuras de AA que pretende ser el resultado final del grupo, cuyo mandato finaliza en mayo de este año. Una de las aplicaciones directas del AA-RR será la gestión de federaciones en el proyecto GN2 (http://www.terena.nl/tech/task-forces/tf-mobility/meetings/30-01-04/slides/JR-TF-Mob.pdf).
- Analizar las posibilidades de continuidad del trabajo del grupo. Se acordó recomendar a TERENA la organización de un grupo dedicado en general a la coordinación de las actividades de middleware de sus miembros, de manera similar al MACE de Internet2 (http://middleware.internet2.edu/MACE/).

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

Actualidad sobre PAPI

A lo largo del pasado invierno, el desarrollo del sistema de autenticación y autorización PAPI ha experimentado un significativo impulso. Se dispone de un nuevo portal que ofrece acceso a datos y documentación relativa al mismo, así como a las distribuciones de software (http://papi.rediris.es/). Además, y de manera muy significativa, el portal está orientado a facilitar el intercambio de información entre la creciente comunidad de usuarios del sistema.

El portal se estrenó con el anuncio de la reciente versión 1.3.0 de PAPI que incluye, entre sus nuevas características más significativas las siguientes:

- El soporte a la interacción directa entre un punto de acceso y un servidor de autenticación, permitiendo nuevos modos (más flexibles) de aplicación del sistema.
- La posibilidad de usar un motor de autorización externo SPOCP (http://www.umu.se/it/projupp/spocp/), lo que proporciona una mucho mayor riqueza a la hora de expresar reglas de control de acceso.
- Una importante mejora de las interacciones de PAPI con LDAP.
- Un conjunto más rico de operaciones disponibles en modo proxy.

Precisamente, el módulo proxy de PAPI ya ha sido empleado por la red académica suiza (SWITCH) para integrar en su infraestructura de autenticación y autorización el acceso a recursos con otros controles de acceso. Esta integración permitirá avanzar más rápido en la interoperabilidad de ambas infraestructuras y, en general, en la construcción de una AAI global.

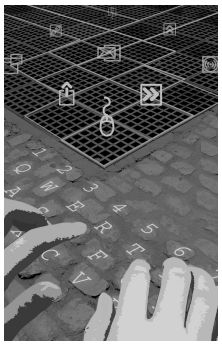
Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Aplicaciones

Creación del Grupo de Trabajo IRIS-XMPP

Anunciamos la creación de un nuevo grupo de trabajo sobre mensajería instantánea y presencia en la Red, que llevará por nombre IRIS-XMPP (http://www.rediris.es/im).

XMPP son las siglas en inglés para e**X**tensible **M**essaging and **P**resence **P**rotocol, es decir, protocolo extensible para mensajería y presencia en la Red. XMPP es conocido familiarmente como Jabber (http://www.jabber.org).

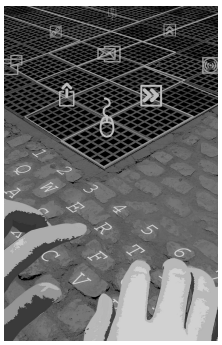
En el IETF existe un grupo (http://www.ietf.org/html.charters/xmpp-charter.html) trabajando en la edición de nuevos estándares para definir las características que habrán de tener este tipo de servicios. Fruto de este trabajo, se han aprobado



Reunión del grupo TF-AACE

Actualidad sobre PAPI

Creación del Grupo de Trabajo IRIS-XMPP



Creación del Grupo de Trabajo IRIS-XMPP

Iniciativa de movilidad en la red de I+D+I

recientemente –aunque aún se encuentran pendientes de recibir numeración–, las siguientes RFCs:

- Extensible Messaging and Presence Protocol (XMPP): Core (ftp://ftp.rediris.es/mirror/internet-drafts/draft-ietf-xmpp-core-22.txt)
- Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence (ftp://ftp.rediris.es/mirror/internet-drafts/draft-ietf-xmpp-im-21.txt)

No obstante, existen varios textos más (http://www.jabber.org/ietf/) pendientes de aprobación.

Los objetivos que nos marcamos al crear este grupo de trabajo son los siguientes:

- Intercambiar ideas y experiencias relacionadas con la implantación y explotación de sistemas de mensajería instantánea y presencia en la Red entre los miembros de la red académica.
- Estudiar la interoperabilidad entre los distintos servicios de mensajería instantánea dentro de la red académica, incidiendo en cuestiones como la identidad, autenticación y autorización de usuarios inter-organización.
- Estudiar la posibilidad de crear una federación de servicios de MI dentro de la red académica y/o a nivel nacional. Extensión de los servicios de MI para soportar tecnologías de indentidad digital como PAPI.
- Integración de Jabber con servicios existentes (directorios LDAP, multimedia, aulas virtuales, entornos colaborativos,...)
- Experimentación con nuevos servicios como los basados en localización *location-aware* y contexto *context-aware*.

Aquellas instituciones afiliadas que deseen formar parte del Grupo de Trabajo deberían comenzar por registrarse en la lista de correos que lleva el mismo nombre, enviando un mensaje a listserv@listserv.rediris.es, especificando en el cuerpo del mensaje:

subscribe IRIS-XMPP <Nombre y apellidos>

y devolvernos relleno el breve cuestionario que recibirá. En la página del grupo (http://www.rediris.es/im) se puede encontrar más información al respecto.

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

Iniciativa de movilidad en la red de I+D+I

Dentro de los grupos de trabajo englobados en las últimas Jornadas Técnicas de RedIRIS (2003) organizadas en Palma de Mallorca, se presentó el arranque de una iniciativa, cuyo nombre es MovIRIS, que coordinará la puesta en marcha de infraestructuras orientas a dispositivos móviles dentro de la comunidad RedIRIS. Su principal motivación es proveer servicios a usuarios que se encuentran localizados en organizaciones o localizaciones distintas a las de su organización origen, es decir, usuarios móviles que por diversas circunstancias se encuentran fuera de su organización habitual y necesitan diferentes servicios telemáticos. Dentro de estos servicios se puede pensar en conexión a Internet, acceso a servicios locales como impresión, etc.

Para conseguir este objetivo es necesaria una coordinación entre las diversas organizaciones englobadas en el proyecto a nivel de compatibilidad tecnológica en el equipamiento, sistemas de autenticación, autorización, registro, etc. de tal manera que se pueda dar estos servicios móviles con la mayor transparencia para el usuario, minimizando el esfuerzo de gestión en las organizaciones visitadas y maximizando el ámbito de movilidad. El objetivo último consistiría en que cualquier usuario móvil pudiera conseguir, de una manera sencilla y segura, conexión en cualquier otra organización dentro del ámbito nacional y europeo, así como acceso a una serie de servicios que le permitieran trabajar como si se encontrara en su organización origen.

Los objetivos del proyecto MovIRIS son:

- Coordinar la puesta en marcha de infraestructuras de movilidad en nuestra comunidad, sirviendo de punto de encuentro de problemas y soluciones.
- Homologar las soluciones tecnológicas a implantar en las diferentes organizaciones con las acordadas a nivel europeo e internacional en este sentido.
- Informar de todos los temas relativos a la movilidad: guías de apoyo, estándares, soluciones (tanto propietarias como de libre distribución), etc.
- Promocionar nuevas soluciones e iniciativas originadas en organizaciones de nuestra comunidad tanto dentro de nuestra red, como a nivel internacional.

A nivel de coordinación en el ámbito europeo, existe dentro de TERENA, el grupo de trabajo TF-Mobility (http://www.terena.nl/tech/task-

forces/tf-mobility/) que sirve de punto de apoyo a las diversas redes de investigación europeas para llevar a cabo la idea de un único espacio de movilidad en toda Europa. Dentro de los documentos elaborados desde este grupo se encuentran algunos que explican soluciones actualmente en funcionamiento en diversas redes de investigación, otros orientados a coordinar las diferentes soluciones haciéndolas compatibles entre sí, recomendaciones, terminología, etc. Así mismo, este grupo ha empezado a coordinarse con el grupo TF-AACE (orientado a soluciones de autenticación y autorización), para elaborar soluciones "Single Sign-on" que integren tanto el acceso de usuarios móviles a la red, como el acceso a cualquier recurso de Internet. Como apuesta firme a las iniciativas tanto de movilidad como de sistemas de autenticación y autorización en Europa, RedIRIS es uno de los principales participantes en la actividad JRA5 dentro de la propuesta para la próxima generación de la red académica europea, GN2 (http://www.terena.nl/tech/task-forces/tf-ngn/presentations/tf-ngn13/20040122_JR_GN2_JRA5.pdf).

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

eIRG White Paper

RedIRIS ha participado en la redacción de la última versión del "eIRG White Paper", contribuyendo con la experiencia acumulada en el desarrollo de infraestructuras de autenticación y autorización como PAPI, y en el despliegue de IRISGrid. En concreto, nuestra contribución se ha centrado en cuestiones de arquitectura, analizando el empleo de modelos de federación y la conexión entre las diferentes infraestructuras que tanto los proyectos de grid como las redes académicas nacionales han venido implantando en los últimos años para la gestión de identidades y derechos de los usuarios.

El documento fue presentado y aprobado en la última reunión del grupo, bajo los auspicios de la presidencia de turno de la UE, en Dublín, el pasado 16 de abril (http://www.heanet.ie/einfrastructures/).

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

TACAR

El repositorio de Autoridades de Certificación académicas de TERENA (TACAR: "TERENA CA Academic Repository" http://www.terena.nl/tech/task-forces/tf-aace/tacar/) se encuentra ya disponible. Se trata de una iniciativa para proporcionar una raíz común de confianza para la interconexión de Infraestructuras de Clave Pública académicas (PKIs) en Europa (e incluso más allá de nuestras fronteras).

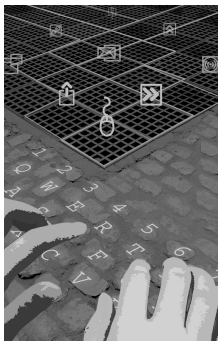
La idea tras el TACAR es poner a disposición de usuarios y, principalmente administradores de redes y sistemas, una relación fiable de certificados y sus correspondientes políticas de certificación, de manera que sea posible establecer vínculos de confianza entre una determinada PKI y otra(s). La gestión de los vínculos de confianza está depositada en los oficiales de TERENA, que se encargan de verificar la información publicada a través del repositorio por medio de encuentros personales con los representantes de las organizaciones participantes y por medio de mensajes de correo electrónico firmado (usando medios externos a los certificados gestionados por el repositorio).

El TACAR cuenta, en el momento de escribir esta noticia, con dieciséis certificados raíz, tanto de redes académicas nacionales (incluyendo a RedIRIS) como de proyectos transnacionales de grid. El repositorio ha sido oficialmente apoyado por el eIRG como una infraestructura básica para la e-ciencia en Europa, y es parte integral de los procedimientos de la EUGridPMA (la entidad que agrupa y valida las PKIs aplicadas en los grids europeos http://www.eugridpma.org/). Existen en la actualidad propuestas para experimentar la aplicación de TACAR en diversos mecanismos de gestión y uso de PKIs, en colaboración con la iniciativa "Evolvable PKI" de Internet2.

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

XPS

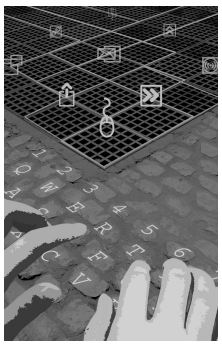
Ya se encuentra disponible la versión definitiva del XPS (X.509 Parsing Server), un front-end para el acceso LDAP a certificados digitales X.509, desarrollado por la Universidad de Salford con el soporte de TERENA y de varias redes académicas europeas: CESNET (República



Iniciativa de movilidad en la red de I+D+I

eIRG White Paper

XPS



XPS

TNC2004 en Rodas

Checa), SURFnet (Holanda), SWITCH (Suiza), UNINETT (Noruega) y RedIRIS. El sistema permite acceder a los certificados asociados a una determinada entrada en un directorio LDAP, obviando las limitaciones que el modelo de acceso a través de atributos imponía a la distribución de certificados por medio de LDAP. Está basado en las reglas definidas por el grupo PKIX del IETF y ya ha sido integrado en la versión 2.2 de OpenLDAP (http://www.terena.nl/tech/projects/AddingCertificateToOpenLDAP/). El equipo de middleware de RedIRIS está evaluando el software y preparando posibles aplicaciones del mismo, tanto en el entorno nacional como en iniciativas de colaboración internacional.

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

TNC2004 en Rodas

A comienzo del mes de junio se celebró la TERENA Networking Conference 2004 en la isla de Rodas (Grecia), junto con las habituales reuniones de los grupos de trabajo que se celebran al mismo tiempo que la conferencia. Los aspectos más relevantes en lo que concierne a las infraestructuras de middleware fueron:

1) En la reunión de TF-AACE se presentaron las conclusiones previas al informe final (que se redactará a lo largo del mes de junio) y los últimos resultados, en concreto el desarrollo del AA-RR a cargo de RedIRIS (http://www.terena.nl/tech/task-forces/tf-aace/Meet06-06-04/presentations/AARR-DL-TFAACE-Rhodes.pdf), para el que hemos recogido ofertas de colaboración de FUNET (Finlandia) y SURFnet (Holanda). Se presentó también el estado final del TACAR, que incluye 16 organizaciones (http://www.terena.nl/tech/task-forces/tf-aace/tacar/). El interés despertado es alto y se han planeado nuevas iniciativas para hacer evolucionar los servicios del repositorio, incluyendo su conexión con el proyecto XPS (http://www.terena.nl/tech/task-forces/tf-aace/).
2) Se presentó también la nueva propuesta del grupo EMCC (European Middleware Coordination Council), cuyos términos concretos serán remitidos al Comité Técnico de TERENA en septiembre. La propuesta incluye que Diego López actúe como Chairman del nuevo grupo.
3) En el grupo TF-Mobility se presentaron los resultados finales del trabajo del mismo, incluyendo la jerarquía de servidores RADIUS y los requisitos de interoperabilidad (http://www.terena.nl/tech/task-forces/tf-mobility/). Se anunció la integración de RedIRIS (a través de la iniciativa MovIRIS) en la jerarquía europea y se acordó proponer la prolongación de los trabajos del grupo por otros dos años.
4) En la conferencia propiamente dicha participamos directamente en:

   a) La coordinación de la misma, dentro del Comité de Programa.
   b) La presentación de la ponencia titulada "Distributed Metainformation Searching", elaborada por David Fernández Barrero, de la Universidad de Alcalá de Henares, bajo la dirección de Diego López dentro de la iniciativa PTYOC.

5) Se establecieron contactos muy interesantes para la colaboración en las áreas de:

   a) Diagnóstico de las capacidades de los servicios: NREN Detective de SURFnet.
   b) Análisis de flujos de red y su aplicación en temas de seguridad.
   c) Sistemas de recogida de datos de intrusiones basadas en "redes oscuras".
   d) La conexión de sistemas de AA (como PAPI) con los sistemas de acceso integrado a la información (JISC-IE).
   e) Taxonomías de sistemas de AA

6) Por último, tomamos parte activa (copresidiéndola) en la "Middleware Assembly" (http://www.terena.nl/conferences/tnc2004/meetings/#middleware), en la que se discutieron los aspectos comunes que las diferentes NREN encuentran en el despliegue de infraestructuras de middleware, y se tomaron algunos acuerdos con el objetivo de lanzar iniciativas de coordinación en el área de las autoridades de nombres, sistemas de autorización, esquemas de diagnóstico y aplicación de estas infraestructuras en servicios ya establecidos.

Se puede encontrar más información sobre las ponencias mencionadas en:

http://www.terena.nl/conferences/tnc2004/programme/presentations/

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

Incidencia de virus y spam en el Servicio de Listas

Nunca deja de sorprendernos el impacto de los nuevos virus en la Red. Si con los del pasado verano (Sobig.F, Mimail o Blaster) pensábamos que se había tocado fondo, la propagación del virus MyDomm (enero-febrero 2003) ha superado cualquier previsión y –lo que es peor– ha creado una gran desconfianza sobre la seguridad existente en la Red. Está claro que uno de los mayores problemas sigue siendo el usuario final que activa la propagación de los virus abriendo los ficheros adjuntos, sobre todo en ese periodo crítico del comienzo de la epidemia, cuando los antivirus todavía no lo detectan. Increiblemente los usuarios siguen confiando en esos mensajes desconocidos que abren por simple curiosidad y que, ya no sólo afectan negativamente a su propio PC, sino cada vez en mayor medida al resto de la Red dejando abiertos puertos traseros que son utilizados para la distribución de spam o de ataques a otros servidores. Es por lo tanto un requisito muy importante para mejorar la seguridad aumentar el nivel de conocimiento de los usuarios ofreciéndoles información fiable sobre estos temas.

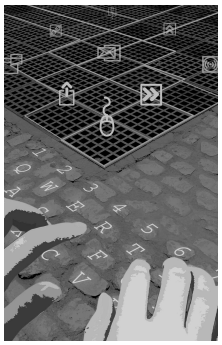
RESACA (Red de Sensores Antivirus de la Comunidad Académica) desde hace dos años viene aportando una serie de datos con una frecuencia diaria, semanal y mensual que permiten estimar la incidencia, tendencia y propagación de los virus en la Comunidad RedIRIS (http://listserv.rediris.es/resaca.html). Esos datos nos muestran que la propagación del MyDomm ha sido, aproximadamente, unas 10 veces superior a cualquiera de las mayores epidemias víricas del 2003. Si los niveles de dispersión de los virus ya es un hecho preocupante no podemos olvidar los efectos ocasionados en la Red y en los servidores de correo con el aumento de las conexiones SMTP, el tratamiento y análisis del tráfico de correo, etc.. A esto debemos añadir los puertos abiertos que dejan las últimas generaciones de virus y que quedan a disposición de los spammers para la distribución masiva de correo basura. Por último no podemos olvidar la enorme confusión y desconfianza que provoca entre los usuarios la falsificación de correos generados por los propios virus.

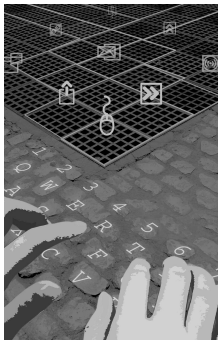
En un Servicio de Listas de distribución por correo electrónico los niveles de protección contra los virus y el spam debe ser máximo pues serían extraordinarios canales de propagación. Este servicio, LISTSERV, que nació antes que la propia Internet y que se diseñó para un entorno científico de confianza y donde era sencillo ir añadiendo mejoras y nuevas funcionalidades, se ha ido acoplando de forma exitosa a un entorno cada vez más agresivo, aunque por otra parte el incremento de los niveles de seguridad en el Servicio ha ido reduciendo algunas de sus funcionalidades.

El spam está golpeando duramente la única puerta abierta del Servicio de Listas de RedIRIS: la dirección genérica de contacto del administrador de cada lista (-request@, owner-@...) que es una redirección a su buzón personal. Esa dirección fue creada para gestionar una lista: recibir solicitudes de alta, de moderación, consultas, etc. pero igual que se recibe esa información necesaria se recibe spam y su volumen ya es muy superior. RedIRIS ha ido implementando cambios en la forma de atender estas direcciones y medidas parciales para reducir este problema, confiando en las medidas AntiSpam que se están implementando en las instituciones y en los propios usuarios para clasificar este correo basura.

Por otro lado los virus distribuyen mensajes infectados que de cara a un usuario son idénticos a los que suele distribuir el Servidor de RedIRIS en una determinada lista. Los usuarios reciben avisos de mensajes infectados que nunca enviaron igual que el servidor de listas y sus múltiples direcciones asociadas. Estos las responden de nuevo a direcciones que pueden llegar a ser la propia lista o direcciones de usuarios que nunca enviaron nada. Los servidores de listas se diseñaron para responder por correo-e a la dirección del emisor de todo lo que les vaya llegando. Se han implementado filtros de contenidos para evitar la distribución de mensajes procedentes de informes generados por antivirus y que se envían a las propias listas. Los virus envían mensajes a direcciones públicas del Servidor para intentar dar de alta o baja la dirección falsificada que lleva incorporada en el campo From. En definitiva un pequeño caos que provoca un aumento de tráfico y un trabajo adicional a los servidores y las personas que los administran. Pero lo más preocupante es la enorme desconfianza que se está generando entre los usuarios.

En definitiva, los virus y el spam están reafirmando los problemas del diseño del protocolo que regula el intercambio de correo (SMTP) que tanto afecta a un Servicio de listas de distribución. El problema más destacable es el uso ilegítimo que muchos spammers y virus están haciendo de nuestras direcciones de correo originando avalanchas de mensajes de





Incidencias de virus y spam en el Servicio de Listas

Actualidad de RACE

error y advertencias sobre virus enviados a personas inocentes. No podemos olvidar la falta de seguridad que implica que cualquier persona puede hacer uso de nuestras direcciones de correo. El IETF está evaluando soluciones para evitar el uso no autorizado del correo electrónico para que cada dominio especifique los servidores (Estafetas) que están autorizados a usarlo. Actualmente el sistema mejor posicionado es SPF (Sender Permited From) del que ya informaremos más adelante.

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

Actualidad de RACE

La iniciativa RACE (Red Académica de Correo Electrónico, http://www.rediris.es/mail/race) arrancó en junio de 2003 con tres objetivos ligados a la Coordinación del Servicio de Correo Electrónico en la Comunidad RedIRIS. Estos objetivos fueron: obtener calidad en el servicio, realizar auditorias interinstitucionales y desplegar una infraestructura privada de correo. La calidad del Servicio ha sido definida a través de 22 indicadores que forman un nuevo modelo de diseño del Servicio para las Instituciones, están agrupados en tres niveles: Básico, Medio y Avanzado. Estos indicadores se ajustan a cualquier institución independientemente de su tamaño (tráfico, usuarios, etc.) y nos permitirá disponer de información cuantitativa del estado del servicio en la Comunidad a través del Catálogo RACE.

RACE propone las líneas maestras para obtener un servicio moderno, seguro y fiable. Se pretende que de una forma consensuada se estructure la evolución del Servicio, se evalúen nuevas tecnologías, y se genere y comparta documentación y desarrollos. Los criterios RACE son variados y atienden a valores como:

- **Seguridad**: control del tráfico SMTP, anti-relay, cifrado, antivirus,...
- **Accesibilidad**: webmail, autenticación centralizada, redundancia,...
- **Usuario**: Documento Correo Electrónico (DOCE), gestión de incidentes, servicios de valor añadido...
- **Otros**: conservación de logs, sincronización NTP, criterios meritorios,...
- **Experimentales**: IPv6, etc.

El Nivel Básico de RACE es el inicial y más importante, todos sus indicadores son imprescindibles y de obligado cumplimiento. El Nivel Medio aporta criterios de valor añadido siendo dos de ellos imprescindibles. El objetivo del nivel Avanzado es cifrar y autenticar todas las transacciones entre el emisor y el receptor. Es evidente que estos niveles son consecutivos y por poner un ejemplo no sería razonable desplegar una PKI para el correo electrónico sin ofrecer a los usuarios un servicio de acceso a su correo vía web (WebMail).

El segundo objetivo RACE es evaluar el estado del servicio de correo electrónico en una Institución en función de los indicadores RACE. La evaluación la lleva a cabo de forma voluntaria el grupo de personas que gestiona el servicio de correo en sus instituciones. Este grupo se renueva periódicamente y desde la última referencia hecha en el Boletín (Boletín de RedIRIS nº 65, septiembre 2003, pg. 11) se ha incrementado la lista en 3 nuevas personas, de forma que actualmente está constituido por 11 postmasters de otras tantas universidades. Las incorporaciones más recientes han sido:

V. Giralt	Universidad de Málaga
J. Benjumea	Instituto de Microelectrónica de Sevilla (CSIC)
I. Bernal	Universidad de Navarra

La evaluación facilita un enriquecedor intercambio de experiencias interinstitucionales entre evaluadores y evaluados. Se genera un informe técnico con el resultado final y unas recomendaciones. RedIRIS, por su parte, envía a los responsables un certificado postal del nivel alcanzado y una serie de logotipos RACE para colocarlos en su web institucional. Con esta información se va creando un catálogo del estado del correo electrónico en la Comunidad RedIRIS (http://www.rediris.es/mail/race/cata.html).

En el periodo oct.-dic. 2003 se han producido las siguientes novedades en el Catálogo:

- Univ. Polit. de Cartagena que se incorporó al Nivel Básico en septiembre de 2003.
- Universidad de Navarra que se incorporó al Nivel Avanzado en noviembre de 2003
- La Univ. Carlos III de Madrid que en junio de 2003 fue evaluada como Nivel Medio y en febrero de 2004 alcanzó el Nivel Avanzado, claro ejemplo de la posibilidad de ir evolucionando de nivel.

El objetivo más ambicioso a largo plazo de RACE es la posibilidad de desplegar una infraestructura privada y de calidad para el intercambio seguro y fiable de correo electrónico entre las instituciones de RedIRIS con nivel avanzado RACE. Los objetivos serían:

a) Establecer una Autoridad de Certificación (CA) entre las Estafetas que permita la posibilidad de cifrar el tránsito de correo entre usuarios de diferentes instituciones.
b) Permitir la movilidad de usuarios.
c) Frenar la difusión de virus y spam interinstitucional. Ofrecer la máxima fiabilidad, tolerancia a fallos y redundancia.
e) Facilitar el uso e información al usuario.

Por último destacar las palabras de Pedro R. Benito, responsable del Servicio de correo electrónico de la Univ. de Burgos en la última reunión del Grupo de coordinación IRIS-MAIL/19 mantenido en Mallorca:

> "La iniciativa RACE nos ha ayudado a montar un sistema de correo electrónico que no solamente cubre todas nuestras necesidades, sino que también abre el camino para nuevas posibilidades. El esfuerzo merece la pena, ya que a partir de ahora todo lo que se aumente o mejore seguirá unos estándares, y se integrará con el resto de servicios gracias a nuestra experiencia anterior. Se han reducido drásticamente las incidencias en el servicio, y el nivel de satisfacción de los usuarios parece bueno, ya que incluso algunos han migrado sus cuentas de las estafetas de departamentos a las estafetas generales de la Universidad a petición propia, sobre todo por razones de movilidad"

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

I Reunión de proveedores de correo electrónico

A mediados del pasado año se formalizaron los objetivos y organización del grupo de interés de Espanix sobre correo electrónico (ESPX-MAIL). Actualmente el grupo está formado por 45 personas de 30 empresas proveedoras de servicio de correo electrónico (Wanadoo, Arsys, Sarenet, Telefónica, Ya.com, etc.). También han mostrado interés por la iniciativa entidades como la Agencia de Protección de Datos, el Instituto Nacional de Consumo o la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información. El grupo está moderado por Jesús Sanz de las Heras de RedIRIS el objetivo principal es la creación de un *clima de confianza* entre los técnicos de los diferentes proveedores que permita abordar los diversos problemas que afectan al correo electrónico en la Red.

La primera reunión del grupo tuvo lugar el pasado 25 de febrero en las instalaciones de Espanix. Asistieron 15 personas pertenecientes a 12 instituciones. Todos los representantes tienen un marcado perfil técnico, con menor o mayor poder de actuación en el ámbito de su empresa, a excepción de la Agencia de Protección de Datos cuya función en el grupo es sancionar el uso indebido de cualquier comunicación electrónica de carácter comercial.

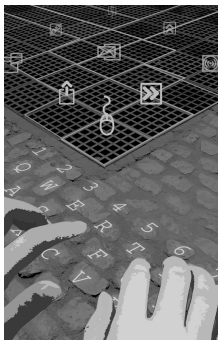
Una de las primeras conclusiones obtenidas es que el spam es mucho mayor en clientes residenciales que en corporativos dada la naturaleza del uso de Internet. Mientras que en el caso de los primeros se puede estimar en un 50% el spam respecto al total de correo, en los clientes corporativos se puede hablar cerca del 20%. Esto se debe a que la gente no suele usar la cuenta de correo de empresa para subscripciones, promociones, reenvío de correos en cadena y demás servicios susceptibles de ser punto de origen de spam. En las Universidades españolas el tráfico de spam se encuentra en un segmento intermedio cercano al 40%.

La reunión estuvo dividida en dos secciones; autorregulación y temas técnicos. Respecto al primer tema se consideró imprescindible acotar y disponer de una definición clara de lo que consideramos spam, denuncia, abusos, etc. Se descartaron esfuerzos en el tema de la coordinación de incidentes de spam debido a la falta de una definición clara de lo que es un "incidente de spam" y a los problemas relacionados con la protección de datos, etc. También se alcanzó consenso en definir una relación de buenas prácticas para usuarios finales y responsables del servicio de correo electrónico, incluidos los usuarios residenciales con ADSL en su casas, que actúan como servidores de correo con todos los puertos SMTP habilitados.

Red.es comunicó que en colaboración con RedIRIS está preparando el lanzamiento de un observatorio del correo electrónico donde se podrá centralizar información sobre el tema desde varias perspectivas: ESPs, usuarios, legislación, postmasters, etc.

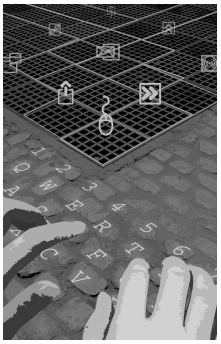
Como resultado se decidió elaborar tres documentos de buenas prácticas:

- BCP1: para delimitar y consensuar el significado de los términos que estamos tratando en este grupo: spam, queja, denuncia, abuse, etc.
- BCP2: Documento de buenas prácticas orientado a gestores de Servicios de Correo electrónico (postmasters).



Actualidad de RACE

I Reunión de proveedores de correo electrónico



I Reunión de proveedores de correo electrónico

XX reunión de IRIS-MAIL

- BCP3: Documento orientado a usuarios de Servicios de Correo electrónico

En los aspectos técnicos se abordó el tema de SPF (Sender Permited From) como una alternativa para paliar el problema actual del spam, no va a acabar con ello pero cualquier herramienta para reducirlo es bienvenida y su implantación no es en principio traumática ya que se puede comenzar a publicar registros SPF que no filtren. El problema radica en que si no se generaliza el uso de SPF, su ámbito de acción se reduciría a relaciones de confianza entre aquellos que lo usen. De las alternativas que se barajan SPF se muestra como la más cercana a adquirir status de RFC. Algunos asistentes se mostraron bastante reticentes a implementarlo sin antes haber hecho pruebas y se acordó informar sobre SPF a la comunidad española.

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

XX reunión de IRIS-MAIL

Esta última convocatoria de IRIS-MAIL celebrada el 18 de junio contó con la asistencia de unas 50 personas y se dividió en cuatro áreas de interés (http://www.rediris.es/mail/gt/jn04/):

- Aspectos generales: SAUCE, MailBackup y Libro Blanco anti-spam
- Proyecto SAnet: Modelo de sensores para la generación de estadísticas y gestión de denuncias (http://sanet.unizar.es)
- Proyecto Appliance de UNIZAR
- Presentación del Servicio de Correo Electrónico de la Universidad de Navarra

En los aspectos generales de IRIS-MAIL se analizaron los problemas que afectan a los Servicios de Mailbackup (http://www.rediris.es/mail/mailbackup) y SAUCE (http://www.rediris.es/sauce). MailBackup es un servicio operativo desde 1997 que está viéndose muy afectado por los graves problemas de incremento de tráfico y ataques que está sufriendo el correo electrónico en Internet. RedIRIS propuso una serie de medidas correctoras para mitigar estos problemas y que se evolucionara hacia un nuevo modelo. Respecto a SAUCE, es un servicio de acceso al correo vía Web creado en el año 2000 para ofrecer movilidad en el Servicio de Correo a todos los usuarios de la Comunidad RedIRIS y fomentar así progresivamente el despliegue de servicios WebMail en sus instituciones. Desde hace un tiempo el servicio está sufriendo una considerable carga en los sistemas de RedIRIS por parte de usuarios procedentes de instituciones que disponen de su propio servicio WebMail. Por este motivo se hace un llamamiento a las instituciones para que difundan entre sus usuarios sus servicios de WebMail y no necesiten utilizar el de RedIRIS. La evolución propuesta es ofrecer un modelo de SAUCE bajo demanda institucional para uso exclusivo de los usuarios de dichas instituciones.

También se hizo referencia a las actividades externas llevadas a cabo por los coordinadores del grupo IRIS-MAIL: la colaboración en el *II European Forum Abuse*; la coordinación del *Grupo ESPX-MAIL* de Espanix y la administración del *Foro Nacional de Postmasters* (MAIL-ES). A mediados de abril se llevó a cabo una sesión de videoconferencia con trece universidades de la Red académica chilena (REUNA) en la que se expusieron las principales líneas de trabajo de IRIS-MAIL; se definieron los canales de coordinación entre ambas instituciones y se resumieron las tendencias internacionales de las múltiples soluciones que se están proponiendo para resolver el problema del spam.

Se expuso el estado actual de desarrollo de las actividades englobadas en el "Libro Blanco anti-spam en RedIRIS" extraído de las conclusiones de la anterior reunión mantenida en Mallorca. A partir de los objetivos estratégicos de este documento se ha avanzado en la comparativa de listas negras que tiene un documento en revisión. La línea más avanzada corresponde a la del desarrollo de un sistema de extracción de estadísticas y generación de denuncias de spam que se ha formalizado en el Proyecto SAnet (Red de Sensores AntiSpam) gestionado por el Servicio de Informática y Comunicaciones de la Universidad de Zaragoza. Se hizo un llamamiento urgente para que las instituciones se dieran de alta como sensores SAnet ya que el Proyecto y sus datos son muy dependendientes del número de mensajes procesados. Actualmente hay 10 sensores de 6 instituciones (UNIZAR, UVIGO, UPV, UAM, UPCO y RedIRIS).

Pascual Pérez de UNIZAR expuso las coordenadas de la política de correo en su Universidad y los desarrollos que han implementado y puesto a disposición de CRIBA: desarrollo basado en librerías Milter de sendmail que permite entre otras cosas gestionar flujos de tráfico SMTP e integrarlos

con productos anti-spam y anti-virus. Uno de los objetivos proyectados es independizarlo de sendmail para poder integrarlo en otro tipo de servidores de correo. También comentó las coordenadas de un proyecto llamado Hermes (Mail Firewall Appliance): solución empaquetada y completa para Estafetas de correo que facilita la implantación de un modelo de calidad RACE, independiente y compatible con cualquier software de servidor de buzones (MDA) y con mayor alcance que una simple solución anti-spam.

Esta solución es la idónea para organizaciones pequeñas o medianas ya que no requiere personal experto en correo electrónico. Su instalación permitiría de forma automática convertirse en sensor antivirus de RESACA y sensor antispam de SAnet.

La sesión se cerró con la presentación que hizo Ignacio Bernal del Servicio de correo electrónico de la Universidad de Navarra. Esta universidad tiene certificado RACE de Nivel Avanzado y como tal expuso el diseño de sus líneas estratégicas: escalabilidad, alta disponibilidad, movilidad, monitorización y seguridad e interoperabilidad con otros clientes/servidores.

Entre otros aspectos interesantes hay que destacar los escasos recursos empleados en su política anti-spam basada en listas negras, servicios de denuncias e implantación como cliente de correo electrónico de Mozilla. Esto permite desviar recursos a reforzar un potente servicio de atención al usuario: manuales, cursos, helpdesk telefónico, etc..

La política anti-spam descansa en la implantación de Mozilla que permite a cada usuario, de forma sencilla, utilizar su motor de filtros adaptativos anti-spam con un simple botón (junk). Además, este cliente permite funcionalidades interesantes tales como: Soporte POPs/IMAPs, SMTP+TLS+SMTPAUTH, LDAP, múltiples cuentas, etc.

Se puede encontrar más información sobre las comunicaciones presentadas en la Zona de Trabajo IRIS_MAIL:

(http://cvu.rediris.es/bscw/bscw.cgi/0/525143).

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

eInfraestructuras Conferencia de Roma

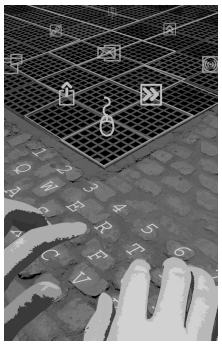
Después de una primera conferencia celebrada en Atenas en junio de 2003 bajo la Presidencia griega, el 9 de diciembre se celebró otra en Roma con el objetivo principal de intercambiar ideas sobre el concepto de *eInfrastructure* y cómo llevar a cabo su implementación en Europa (http://www.einfrastructures.org).

Se trata de un entorno donde los actores más importantes son los proyectos GRID, las redes de investigación y todo tipo de usos científicos, que empleando las redes de alta velocidad, elementos de almacenamiento y el middleware adecuado puedan permitir cambiar de una forma dramática los usos de las redes y su explotación en el campo científico y por extrapolación a usos en otros entornos industriales o domésticos.

En Roma se realizaron diversas presentaciones sobre la actividades en *eInfrastructure* y proyectos GRID de iniciativas nacionales propuestas al VI Programa Marco y la visión de la Comisión Europea al respecto. Todo ello con inclusiones de la cooperación internacional más allá de Europa: Japón, USA o Latinoamérica.

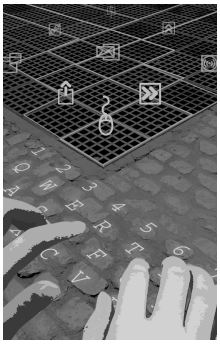
Lo que se constata en Roma es que existen proyectos en marcha, otros en preparación y un gran interés de cooperación de todos los implicados, pero que hace un grupo que coordine a nivel europeo estas actividades y que sea designado a nivel gubernamental por cada uno de los estados miembros (incluyendo los 10 nuevos miembros). El grupo recibe el nombre oficial de eIRG (*eInfrastructure Reflection Group*) y se marca en una fase inicial los siguientes objetivos:

- Identificación de los elementos, servicios y recursos necesarios para permitir una e-Science pan-europea
- Recomendación de líneas para el establecimiento de políticas de compartición de recursos:
  - Iniciativas de GRID nacionales
  - Proyectos regionales y europeos de *eInfrastructure*
- Contribución al establecimiento de un foro internacional de política en esta línea
- Ofrecimiento de elementos de entrada a otros foros de toma de decisión: ESFRI, NREN PC,....



I Reunión de proveedores de correo electrónico

eInfraestructuras Conferencia de Roma



eInfraestructuras
Conferencia de
Roma

- Establecimiento de una primera actuación hacia investigadores mediante eScience, pero también colaborar en su extensión a otros entornos: eLearning, eGovernment, eHealth, eCulture, eBusiness, etc.)
- Identificación, información y promoción del conocimiento GRID entre aquellas comunidades que se puedan beneficiar de la compartición de recursos.
- Control de aspectos administrativos en el despliegue de GRIDS.
- Utilización de la experiencia de la comunidad de las redes de investigación (estructura, operativa, Políticas de uso aceptable,...)

El eIRG estará formado por representantes de los estados miembros oficiales de la CE y apoyado por un grupo de técnicos que aportarán sus recursos desde los proyectos más emblemáticos: EGEE, DEISA y tal vez GN2.

En definitiva, se presenta una gran actividad en este entorno con la existencia de foros en los que RedIRIS, el MCYT y otros agentes deben estar presentes de cara al desarrollo de toda una base estructural y de conocimiento, que permita construir un sistema estable y operativo y que es deseable que esté disponible lo antes posible para que nuestros usuarios científicos puedan utilizarlo.

Más información en: https://cagraidsvr06.cs.tcd.ie/grid-event-2004/einfra/

Víctor Castelo
(victor.castelo@cti.csic.es)