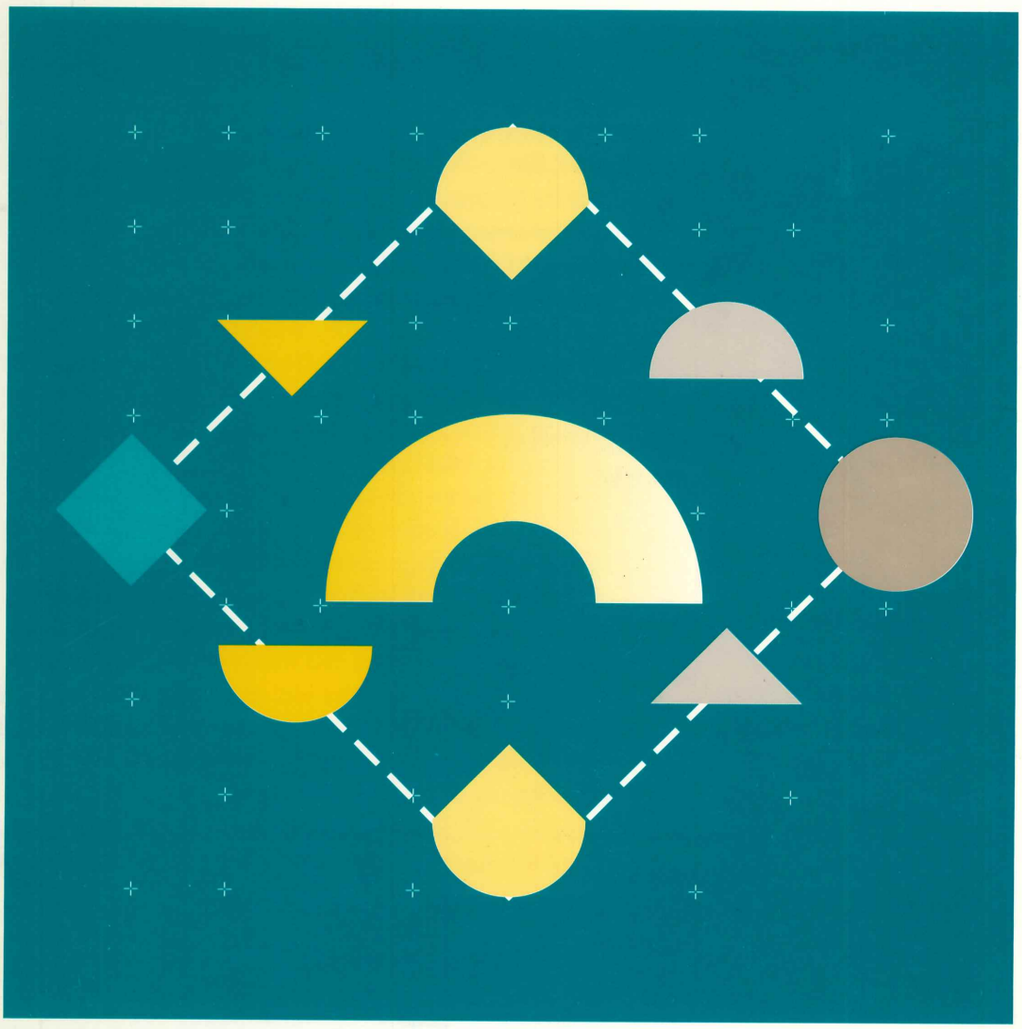
Red IRIS

Plan Nacional de I+D

Boletín de la red nacional de I+D, RedIRIS.

nº 22



nº 22
Marzo 1993

Boletín de la RedIRIS

Sumario

Publicación bimestral de la red nacional de I+D, RedIRIS.

Edita: RedIRIS
Alcalá 61, 1ª Plta. 28014 Madrid.
Tel.: 435 12 14.
Director Técnico: José Barberá Heredia
Coordinación: María Bolado
Filmación: BOCETTO, S.L.

Portada: TAU Diseño
Producción: Estudio 5
Autoedición: María Bolado
Imprime: ETS, S.L.
Distribución: B.D. Mail, S.A.
Depósito legal: M. 15844-1989

Presentación

J. Barberá

Una de las preguntas que constantemente rondan la cabeza de los que gestionamos redes teleinformáticas es ésta: ¿qué debe primar en una red, el ancho de banda disponible o los servicios ofrecidos?. O, de otra manera, ¿qué valoran más los usuarios: la capacidad de las autopistas electrónicas que les permiten transportar los bits de las diversas aplicaciones que ellos controlan, o los servicios de red, de aplicación y los sistemas de ayuda que se ponen a su disposición para facilitar su interacción con la red, o bien para acceder a diversas fuentes de información. La respuesta es en principio sencilla: ambas circunstancias unidas serán las que satisfagan a los usuarios de la red en mayor medida.

El problema surge a la hora de manejar recursos limitados, que habrán de distribuirse de forma equilibrada para poder mantener un grado de satisfacción general aceptable. El tema no es nuevo. Ya al surgir las primeras redes de conmutación de paquetes había dos puntos de vista enfrentados. El del usuario (al operador) era: a mí póngame una red rápida y barata que me permita enviar paquetes de un nodo a otro y despreocúpese de reordenarmelos o retrasmitirmelos, que de eso ya me encargo yo. El del operador (al usuario): yo ofrezco una red de calidad inmejorable y le garantizo la entrega en destino de todos los paquetes, debidamente ordenados y sin pérdidas ni duplicados (y cobro por ello también).

Al principio del Programa IRIS el esfuerzo se puso principalmente en uno de los servicios de aplicación, el más necesario y utilizado: el correo electrónico. El tema del ancho de banda no era una preocupación

En nuestro caso, el tema de las tarifas, o quizás más bien de la distribución de costes entre los diferentes servicios (de transmisión, de red, de aplicación), no ha sido relevante hasta ahora, por cuanto que todo ello ha venido siendo sufragado con fondos centrales. Sí lo ha sido sin embargo la distribución de esos fondos -limitados- en función de los diferentes servicios. En ese sentido podemos observar un proceso cíclico. Al principio del Programa IRIS el esfuerzo se puso principalmente en uno de los servicios de aplicación, el más necesario y utilizado: el correo electrónico. El tema del ancho de banda no era una preocupación: por un lado estaban las redes públicas de paquetes y, por otro, no se necesitaba gran ancho de banda. Al introducir luego los servicios basados en TCP/IP y conectar RedIRIS a la Internet, vemos que las redes públicas no sirven; se establecen así las redes ARTIX e IXI, con una capacidad incomparablemente superior a la *disfrutada* hasta entonces. Con más ancho de banda se pueden tener más y mejores servicios de aplicación, que, al extenderse como la pólvora, llenan los enlaces de 64Kbps que en su momento llamábamos de *alta velocidad*. Esto lo vemos no sólo aquí sino más allá de nuestras fronteras. En este momento parece que todos los enlaces internacionales están próximos a la saturación. Nuestro cuello de botella actual -el enlace Madrid-Amsterdam de Ebone- va a duplicar en breve su capacidad. Veremos si esto alivia la situación o bien encontramos a lo largo de nuestras rutas otros cuellos de botella internacionales. En Ebone los planes son aumentar asimismo la capacidad de los enlaces troncales a un mínimo de 1,5 Mbps. Seguramente esta situación mejorará la actual. Pero eso mismo llevará a la introducción de nuevas aplicaciones y servicios que volverán a congestionar las redes. Ese ha sido el patrón seguido hasta ahora. Esperemos que esta vez se retrase un poco más. Aquí este problema ya lo hemos sentido con uno de los servicios de información general de gran demanda: las *News*. Con pasos progresivos y seguros se extiende ese servicio piloto con condicionantes estrictos derivados de la necesidad de gestionar correctamente el ancho de banda de ARTIX. Los procedimientos y reglas de juego deben de respetarse escrupulosamente si no queremos que se colapse la red. Porque lo que no se ve por el momento es la posibilidad real de aumentar el ancho de banda.

Con más ancho de banda se pueden tener más y mejores servicios de aplicación

Lo que no se ve por el momento es la posibilidad real de aumentar el ancho de banda

El año pasado ha sido testigo de un significativo crecimiento de la Internet en Europa. Si hace dos años Europa apenas significaba un 5% de máquinas en la Internet, ahora ese porcentaje es ya del 30%. Ello se debe a la buena coordinación que se ha conseguido en el foro de RIPE y en la *cooperativa* Ebone, ambas informales y con medios escasos, pero vivas y activas a fin de

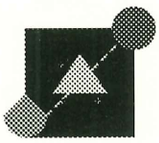
Diferencia entre "investigar en redes" y hacer "redes para la investigación"

cuenta, lo que ha llevado a los expertos europeos de las redes no sólo a ser tratados de igual a igual con los de EE.UU., sino a contar con ellos a la hora de tomar decisiones estratégicas sobre la evolución de la Internet.

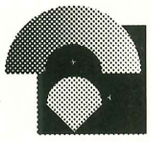
En cuanto a la sección Enfoques, se presentan esta vez dos temas avanzados que tienen relación con el correo electrónico y cuya aplicación, si no inmediata, promete mejorar la gestión del servicio y la aceptabilidad por el usuario de este sistema. Además, ambos temas hacen uso del servicio de directorio X.500, utilizado hasta ahora principalmente como un servicio de información de páginas blancas. Uno de los artículos se refiere al uso del directorio X.500 para encaminar la mensajería en X.400. Se destacan las pruebas hechas por RedIRIS con un MTA basado en una versión beta del PP, otro producto académico que mejora las prestaciones de nuestro conocido y bien amado EAN. El segundo artículo se refiera a temas de seguridad en correo electrónico, en concreto al servicio de mensajería privatizado que garantiza la confidencialidad y autenticidad de los mensajes. El grupo de investigación de la Universidad Politécnica de Cataluña que lo escribe está participando en el correspondiente subproyecto de COSINE. Su trabajo aportará una experiencia valiosa para poder ofrecer mejoras en el servicio en un futuro. Quede así patente la diferencia entre "investigar en redes" y hacer "redes para la investigación", distinción ésta a la que se ha aludido alguna vez en otros números de este boletín.

José Barberá
Director de RedIRIS
jose.barbera@rediris.es
C=es; ADMD=mensatex;
PRMD=iris; O=rediris;
S=Barbera; G=Jose

Actualidad de RedIRIS



Conexión de ARTIX con la red pública Iberpac



Conexión IP con la Agencia Espacial Europea

El Servicio Piloto de News de RedIRIS en 1993

Conexión de ARTIX con la red pública Iberpac

Según se anunció en las últimas Jornadas Técnicas RedIRIS 92 se ha procedido a la modificación del esquema original de interconexión de ARTIX con la red pública de datos Iberpac.

Hasta ahora la interconexión de ARTIX con Iberpac se basaba en un acceso por nodo con velocidades de hasta 9600 bps. El nuevo esquema de interconexión, acorde al tráfico actual, se basa en un único acceso para toda la red con una velocidad de 64 Kbps.

La reestructuración de los acceso a Iberpac tiene un doble objetivo:

- Adaptación al tráfico actual de la red.

- Disminución de costes innecesarios.

Para ello se ha instalado en Madrid un enlace Iberpac a 64 Kbps y se ha diseñado una transición suave que pasa por dos fases:

1.- Eliminación de los enlaces de interconexión con Iberpac en Madrid (antiguo), Zaragoza, Tenerife, Santander, Bilbao. Valencia y Valladolid, siendo encaminado el tráfico de estos nodos por el nuevo acceso a 64 Kbps.

2.- Eliminación de los enlaces de interconexión con Iberpac en Sevilla y Barcelona, pasando todo el tráfico ARTIX-Iberpac a estar encaminado por el enlace de 64 Kbps situado en Madrid.

En la elección de los nodos involucrados en la primera fase se han considerado razones de tráfico, obtenidos de las estadísticas mensuales de la red, mientras que en la elección de Madrid como único punto de acceso a Iberpac se ha tenido en cuenta la topología actual de la red, así como el tráfico generado por los distintos nodos.

El cambio en el esquema de interconexión ha obligado a la inevitable modificación de todas las direcciones Iberpac asignadas a cada uno de los ETDs registrados en ARTIX, cuyos responsables han sido debidamente informados.

El nuevo esquema de interconexión quedará operativo el 23 de Febrero.

Conexión IP con la Agencia Espacial Europea

En el último trimestre del año pasado RedIRIS y la Agencia Espacial Europea (ESA) llegaron a un acuerdo para el intercambio directo del tráfico IP existente entre ambas redes. La Estación Espacial de Villafranca del Castillo (cercana a Madrid), centro perteneciente a la Agencia en España, servirá de nexo de unión entre SIDERAL (servicio IP de RedIRIS) y ESINET (red IP de la ESA). Esta estación se encuentra englobada dentro de la infraestructura general de comunicaciones de datos de la ESA, conocida por ESANET[1], y, al mismo tiempo, conectada a la infraestructura de transporte de RedIRIS.

La conexión tuvo lugar en fechas recientes y para llevarla a cabo se hizo uso del enlace de 64 Kbps de ARTIX que conecta la Estación de Villafranca con el nodo de la red en Madrid, que hasta la fecha venía empleándose exclusivamente para tráfico DECnet y X.25. Por una parte esta conexión evitará que el tráfico IP entre los demás centros de RedIRIS y la Estación de Villafranca se curse a través de infraestructura de comunicaciones internacional; por otra parte, del intercambio bilateral de tráfico IP entre la ESA y RedIRIS se beneficiarán ambas partes, al acortar el camino entre las dos (o lo que es lo mismo, el "número de saltos" de los paquetes que viajan entre ellas) y evitar el tránsito por líneas externas, por lo general más cargadas, con lo que también se contribuye a descargar algo la infra-estructura IP común europea.

El Servicio Piloto de News de RedIRIS en 1993

Durante el segundo semestre de 1992 se realizaron una serie de pruebas para el inicio de un nuevo servicio de RedIRIS: Internet News. En dicho periodo se realizaron pruebas sobre ocupación en disco de noticias, carga de CPU, número de conexiones simultáneas al servidor, topología del servicio y administración de un

1. Ver número 18 de este Boletín (Julio 1992): "La Estación Espacial de Villafranca del Castillo. Comunicaciones y Redes de Datos"; D. de Pablo. J.J. Adán, F. Marcelo

software denominado ANUNEWS, desarrollado por la Universidad de Camberra en Australia, de dominio público. ANUNEWS funciona sobre VMS y está instalado en estos momentos en un VAX 4300, en los servicios centrales de RedIRIS. La versión instalada es la 6.1.Beta5 y dispone de un disco de 2GB para almacenamiento de noticias con un tiempo de expiración de 7 días.

Paralelamente, en SWITCH, red académica suiza, donde se encuentra situado el nodo que envia las noticias a nuestro servidor *rediris.es*, se han producido cambios de máquina, el nodo *scsing.switch.ch* es ahora un SUN 6/690, y de software, han cambiado de C-News a Internet Network News (INN), durante el pasado mes de Enero.

Por nuestra parte, se decidió ampliar desde el 1 de Enero, la posibilidad de acceder al servicio de News, a todos los centros de RedIRIS que lo soliciten, bajo una serie de condiciones que a continuación se detallan:

- Cada centro deberá cumplimentar la hoja de suscripción en la cual se determinan una serie de datos imprescindibles para habilitar el acceso al nodo de rediris, comprometiéndose a actualizar dicha información cuando corresponda. Así mismo, el centro deberá poner aquellos medios informáticos y humanos necesarios para que dicho servicio llegue a toda su organización. Por consiguiente, sólo un nodo accederá al servidor de RedIRIS por organización.

- Los centros accederán al servidor de noticias según un horario preestablecido y un número limitado de veces, si así fuese preciso, determinado todo ello por la carga del servidor.

- Igualmente, y dada la filosofía jerárquica del propio servicio de noticias, cada centro se compromete, a su vez, a permitir el acceso y distribución de su almacen de noticias a otros centros que así lo soliciten bajo la premisa de no duplicar el trafico de grupos y noticias en los enlaces de ARTIX.

- Inicialmente, no se limitará el número de grupos que reciba cada nodo, si bien, RedIRIS podrá establecer aquellas restricciones que considere necesarias para preservar el "buen uso" de la red y de los servicios que desde RedIRIS se ofrecen.

El motivo de tales requisitos viene originado por la falta de recursos de CPU que en estos momentos se disponen, estando previsto para el presente año mejorar los mismos en la medida de las posibilidades. La idea consiste en aumentar recursos de máquina UNIX que permitan iniciar las pruebas con el mismo software, INN(Internet Network News), que en la actualidad está funcionando en SWITCH, y que por la experiencia aportada por su personal parece una opción seria a considerar. Muy probablemente el servicio de News residirá, en un futuro, en un sistema UNIX que aglutine labores globales de servicios de información: Anonymous FTP, servidor de ficheros via mensajería electrónica, listas de distribución, servidor de News, servidor Gopher, servidor Archie,...

Para poder acceder al servicio de noticias de RedIRIS, el PER (Persona de Enlace con RedIRIS) deberá enviar a :

InfoIRIS
RedIRIS. FUNDESCO
c/ Alcalá 61
28014 Madrid
Telf 4351214
Fax 5781773
E-mail: infoiris@rediris.es

el fichero que se encuentra accesible en el servidor de RedIRIS (FTP anonymous y correo electrónico) INFO$ROOT:[REDIRIS.SERVICIOS.NEWS]: solicitud.news. Por correo se puede obtener como sigue:

```
EAN>co server@infoserv.rediris.es
TO: server@infoserv.rediris.es
send [REDIRIS.SERVICIOS.NEWS]SOLICITUD.NEWS
.
Send options? <RETURN>
```

Finalmente señalar que se han iniciado algunos grupos de interés local bajo el grupo principal es. En la actualidad estos grupos son: es.alt, es.earn, es.faenet, es.rec, es.rediris, es.talk, es.uniovi, es.upc, entre otros. Para abrir nuevos grupos se seguirán las normas al uso, que aparecerán en el servidor de información de RedIRIS (info$news) dedicado a todos estos temas, así como las propias noticias. La idea es establecer una pasarela entre dichos grupos de noticias y el servidor de listas de distribución Infoserv RedIRIS (ver noticia siguiente). A tal efecto se realizan diferentes pruebas con la finalidad de que

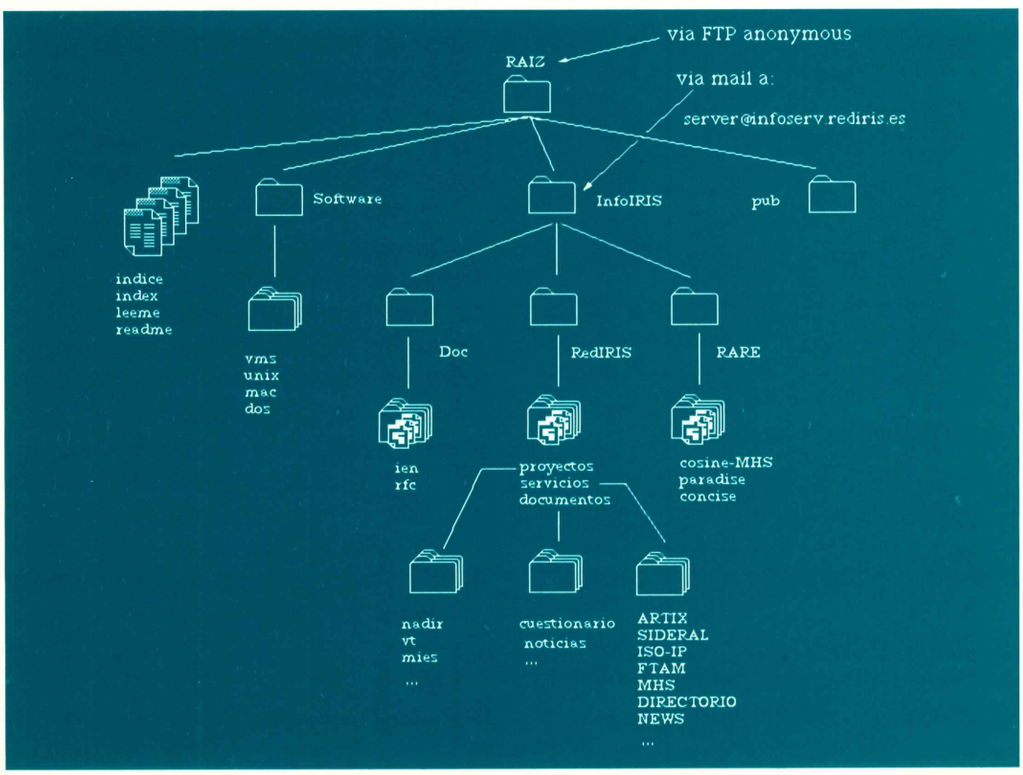
dichas aplicaciones se constituyan como herramientas para establecer comunicación a determinados *grupos de interés*.

INFOSERV: Nuevo servidor de listas de distribución y ficheros.

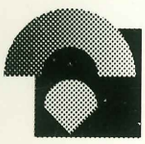
En la actualidad se encuentra disponible el nuevo *Infoserv* de RedIRIS. Se trata de un servidor de listas y ficheros mediante mensajería electrónica que incorpora el programa PMDF en su última versión (4.1). Dicho software funcionará paralelamente al servidor de EAN que hasta la fecha estaba desempeñando dichas tareas. Para enviar un mensaje a alguna de las listas de distribución del nodo de mensajería iris-dcp bastaba con enviar un mensaje a *nombre-lista@rediris.es* (anteriormente *nombre-lista@iris-dcp.es*) y el servidor se encargaba de expandir la lista enviando un mensaje a cada uno de los suscriptores de la misma, con el único inconveniente de que la suscripción debía ser realizada manualmente por el postmaster correspondiente. Por otra parte, para acceder a los ficheros ascii del servidor de RedIRIS bastaba con enviar un mensaje a una de las siguientes direcciones: *server@rediris.es*, *server@info.rediris.es* que incluyese algunos de los comandos permitidos (como **ayuda**, **envia**...) y automáticamente nos sería devuelta la información solicitada.

El nuevo servidor permite administrar listas abiertas o restringidas en cuanto a quien puede suscribirse a una de ellas. En el caso de listas abiertas (o públicas) cualquiera puede suscribirse, por el contario, en el caso de listas restringidas sólo uno o varios de los suscriptores autorizados pueden realizar nuevas incorporaciones. Ahora bien, tales listas pueden ser moderadas o no, en cuanto a quien puede enviar mensajes a la listas. En el caso de listas moderadas tan sólo el moderador/editor decide qué enviará a la lista (ejemplo revistas electrónicas), mientras que las listas no-moderadas admiten contribuciones de todo el dominio de suscriptores que contemple, en cuyo caso cualquiera puede enviar un mensaje a la lista con sólo enviar el mensaje a *nombre-lista@infoserv.rediris.es*, y las restringidas rechazarán todos aquellos mensajes no enviados desde algunos de los suscriptores de las mismas.

Ambos criterios son combinables de forma que pueden existir conferencias restringidas moderadas o no-moderadas y abiertas, igualmente, moderadas o no.



INFOSERV: Nuevo servidor de listas de distribución y ficheros.



Conexión con EBONE

Computer Networks for Research in Europe

El servidor de ficheros tal y como aparece reflejado en la figura, por su parte, permite una serie de órdenes, lamentablemente sólo en inglés (directory, encoding, help, index, lists,maximum, mode, send, subscribe, unsubscribe), que nos permiten desde conocer los ficheros disponibles a recibir un fichero, pasando por su posible compresión para el caso de ficheros de gran tamaño. En este caso será preciso utilizar la dirección de correo *server@infoserv.rediris.es* insertando todas aquellas órdenes que deseemos en el cuerpo del mensaje.

El servidor Infoserv dispone de una ayuda que contine la descripción de su funcionamiento en castellano y en inglés. Para conseguir dicha ayuda bastará con enviar un mensaje como sigue:

```
EAN> co server@infoserv.rediris.es
To:  server@infoserv.rediris.es
Subject: (no es necesario)
help
.
EAN>
```

Finalmente señalar que para mayor infomación o consultas bastará con enviar un mensaje a infoiris@rediris.es.

Conexión con EBONE

El nuevo enlace internacional de 128 Kbps. Madrid-Amsterdam, que conectará RedIRIS con la red EBONE, fue solicitado a finales de 1992 y está previsto que quede operativo en el mes de marzo.

Sustituye al enlace de 64 Kbps. que ha venido funcionando durante 1992.

Asimismo, en lo que respecta a los enlaces formales de EBONE, se producen los siguientes aumentos de capacidad:

Amsterdam - CERN	de 448 a 1,5 M (T1)
Amsterdam - Estocolmo	de 512 a 1,5 M (T1)
París - CERN	de 512 a 2 M (E1)

Computer Networks for Research in Europe

Las asociaciones RARE y EARN han decidido colaborar conjuntamente en una publicación denominada *Computer Networks for Research in Europe (CNRE),* conocida hasta ahora como *RARE/EARN Teletribune.*

CNRE tratará sobre todas aquellas cuestiones que en el mundo de las redes internacionales sean relevantes para la comunidad investigadora y académica europea. Esto incluirá actividades de RARE, EARN, EUnet, NORDUnet, Hepnet, etc... así como también de COSINE, la futura Unidad Operativa, EASInet y otros proyectos internacionales.

La publicación tendrá una orientación práctica, dirigida a los servicios y cubriendo los aspectos operativos más relevantes de las redes.

Los lectores a los que va dirigido son gestores y personal técnico de las organizaciones de redes nacionales, gestores de redes y servicios teleinformáticos en universidades y centros de investigación, así como usuarios avanzados de redes.

CNRE se distribuirá como serparata de la revista *COMPUTER NETWORKS and ISDN SYSTEMS* (CN&IS) publicada por Elsevier, con una periodicidad inicial de cuatro números al año. A las asociaciones RARE y EARN Elsevier les suministrará copias adicionales para la distibución entre sus afiliados y colaboradores. Asímismo estará disponible en servidores de información accesibles por redes de I+D.

CNRE cuenta ya con un comité editorial activo y competente que, al menos al principio, tendrá que trabajar sin compensación alguna, excepto la que supone el reconocimiento derivado del lanzamiento de esta nueva publicación. RARE y EARN ya han asignado colaboradores para la labor editorial de ayuda al comité, que de esta forma no necesitará ocuparse de los aspectos prácticos del proceso sino sólo de los aspectos científicos.

Aquellas personas interesadas en colaborar en esta publicación pueden dirigirse a:

Kees Neggers	<Kees.Neggers@surfnet.nl>
Frode Greisen	<Frode.Greisen@uni-c.dk>

Reunión de los socios de la Unidad Operativa

Las diferentes organizaciones nacionales de redes de I+D (más NORDUnet) que en su momento decidieron constituir una "Unidad Operativa" (UO) para la gestión y suministro de servicios internacionales de redes, se reunieron en Bruselas el 22 de enero de 1993. Hasta el momento 12 organizaciones de 16 países europeos se han agrupado para esta empresa común:

RENATER	(Francia)
DFN	(Alemania)
GARR	(Italia)
NORDUnet	(Países Nórdicos)
JNT	(Reino Unido)
SURFnet	(Países Bajos)
SWITCH	(Suiza)
RedIRIS	(España)
SPPS	(Bélgica)
ARIADnet	(Grecia)
FCCN	(Portugal)
ARNES	(Eslovenia)

HUNGARNET, la organización de la red nacional de I+D de Hungría, ha expresado asimismo su deseo de adherirse.

En su momento los socios actuales de la OU decidieron la elección de Cambridge (R.U.) como lugar para el establecimiento de las oficinas correspondientes. Actualmente se está en el proceso de selección del director y otros miembros del consejo de dirección.

Como se sabe la UO surge ante la necesidad de coordinar los diferentes servicios de redes en beneficio de los proveedores nacionales (bien sean socios de la UO o simples clientes), manteniendo de modo estable los servicios lanzados por el Proyecto COSINE y otros de interés para los usuarios de redes de I+D. De este modo la situación actual de dispersión de servicios internacionales (EMPB-IXI, Ebone, RIPE NCC, PARADISE, MHS-X.400, ...) podrá evolucionar bajo un techo común, en beneficio de los proveedores de servicios y de los usuarios finales.

Respecto al servicio internacional para la coordinación de dominios privados de mensajería basada en X.400 (MHS-X.400), que fue subvencionado por COSINE hasta diciembre del 92, se pretende ahora encontrar un sistema de financiación estable, basado en el uso del servicio que las diferentes redes MHS-X.400 hacen de él. En este sentido la UO está trabajando para encontrar un esquema equitativo para la distribución de los costes asociados. La red suiza SWITCH seguirá siendo responsable de este servicio proporcionado a las diferentes redes nacionales de I+D.

La Comisión de la Comunidad Europea (CCE) ha apoyado esta iniciativa aportando fondos a la UO, tanto para la puesta en marcha de la misma, como para la subvención de determinados servicios, incluyendo un *help-desk* para ayuda a los clientes. Las partidas destinadas a la subvención de servicios llegan a cubrir, durante el primer año, el 50% de los costes totales. En concreto esto afecta a los servicios MHS-X.400, coordinación de IP, pasarelas y seguridad. Asimismo la CCE subvenciona el 50% de los costes del servicio EMPB (infraestructura de transporte multiprotocolo) a 2 Mbps, sobre el que se informará más adelante.

Reunión de los socios de la Unidad Operativa

14ª Reunión de RIPE

14ª Reunión de RIPE

Con una periodicidad cuatrimestral vienen manteniéndose reuniones para la coordinación de los servicios Internet a nivel europeo en el marco de RIPE ("Réseaux IP Européens"). La última reunión tuvo lugar en Praga en la Facultad de Ingeniería Eléctrica de la Universidad Técnica Checa durante los días 25, 26 y 27 del pasado mes de Enero y a ella asistieron cerca de cien personas en representación de unas cuarenta organizaciones relacionadas con la provisión de servicios IP en Europa, entre ellas RedIRIS.

El primer y último día se dedicaron a sesiones plenarias en las que se presentaron y discutieron diversos temas de interés general tales como:

- Avances en la creación del "Global Internet Exchange" o GIX, que pretende armonizar y racionalizar la forma en que se llevan a cabo las comunicaciones intercontinentales.

- Coordinación entre RIPE y el Programa Técnico de RARE, a través de la representación de RIPE en el Comité Técnico

de RARE (RTC) y la colaboración en proyectos conjuntos que permitan una mayor participación europea en la evolución de la Internet. Así, ya se ha empezado a trabajar en la elaboración de dos documentos de gran interés: la especificación del servidor de rutas que será necesario en el futuro GIX para contener una visión unificada de las rutas a destinos europeos y la elaboración de una "Especificación Genérica de Servicio Internet" que sirva de guía tanto a proveedores como a centros usuarios cubriendo todos los aspectos importantes en relación a este servicio. Por otra parte, se va a hacer un seguimiento de las decisiones que se tomen en Internet acerca de la evolución técnica futura (IP versión 7), en las que se pretende que haya una mayor participación europea.

- Introducción de nuevos esquemas y protocolos de encaminamiento en Europa (CIDR y BGP-4), que permitirán, en conjunción con la nueva estrategia de asignación de direcciones que se viene aplicando desde hace ya varios meses, hacer frente a problemas acuciantes en Internet como son el agotamiento del espacio de direcciones y la explosión de las tablas de encaminamiento en los routers.

- Situación actual de EBONE y planes de actuación para 1993.

- Aspectos del servicio IP sobre EMPB, en especial se trataron aquellos relacionados con la interconexión entre EMPB/IP y la parte europea de la Internet. Los alemanes del DFN presentaron algunos datos sobre su experiencia corriendo IP encapsulado en X.25 sobre EMPB a 2 Mbps.

- Actividades llevadas a cabo por el Centro de Coordinación de Redes en RIPE (RIPE NCC) durante el último cuatrimestre del año 1992 (mediante su habitual informe cuatrimestral). También se analizó la situación actual de financiación de este imprescindible centro (pues sirve de soporte para todas aquellas actividades de RIPE que no pueden ser realizadas de forma efectiva mediante trabajo voluntario de miembros de las organizaciones participantes), siendo generalizado el sentimiento de que es necesario encontrar la forma por la que todos los actuales beneficiarios de su funcionamiento (fundamentalmente los distintos proveedores de servicio Internet europeos) contribuyan de forma equitativa a su mantenimiento.

Aparte de las sesiones plenarias, se dedicó un día completo para las reuniones de distintos grupos de trabajo de RIPE, a saber: routing, base de datos de RIPE, registros locales, DNS, mapas, conectividad de los Países del Este de Europa, relaciones entre redes académicas, educativas y comerciales, etc.

De las conclusiones de los grupos de trabajo únicamente resaltar un par de resultados importantes como son:

- Propuesta de modificación de la base de datos de RIPE en lo referente a datos de encaminamiento, de forma que pueda reflejar mejor la realidad y ser fácilmente usada con fines de "routing"; para ello, se redefine el concepto de Sistema Autónomo, dejando de ser prácticamente sinónimo de "dominio administrativo" para pasar a ser únicamente "un conjunto de redes con la misma política de encaminamiento de cara al exterior".

- Principio de acuerdo en el grupo de trabajo de registros locales entre los distintos NIC's para la utilización de un formulario de solicitud de direcciones IP unificado para toda Europa, lo que facilitará enormemente la coordinación de todas estas actividades. Es de esperar que este formulario y la documentación que lo acompaña sean aprobados para su uso durante la próxima reunión de RIPE que tendrá lugar en Amsterdam entre los días 27 y 29 de Abril.

Encaminamiento de correo X.400 utilizando el directorio X.500

Ignacio de los Mozos

Introducción

En este artículo se presenta la primera experiencia internacional de encaminamiento de correo utilizando el X.500, realizada entre la organización X-Tel Services Ltd del Reino Unido y RedIRIS.

En pasados boletines se ha puesto de relieve en reiteradas ocasiones la necesidad de encontrar mecanismos de encaminamiento X.400 basados en el directorio X.500. Por el momento, la ausencia de normas ISO / CCITT que regulen esta interacción exige un gran esfuerzo de coordinación entre los distintos responsables del servicio para la actualización y mantenimiento de tablas de rutas estáticas. [1], [2] y [3]

En este artículo se presenta la panorámica actual al respecto, así como la primera experiencia internacional de encaminamiento utilizando el X.500, realizada entre la organización X-Tel Services Ltd del Reino Unido y RedIRIS.

En ella veremos cómo obtener, e incluso superar, la funcionalidad que el servidor de nombres de la Internet (DNS) ofrece a su correspondiente protocolo de correo SMTP. Y esto a pesar de la mayor complejidad del X.400 y la posibilidad de utilizar indistintamente direccionamiento RFC-822 o X.400.

Lo que aquí presentamos es un modelo más de los posibles, que se encuentra en situación de draft de RFC del grupo de trabajo MHS-DS del IETF[1]. Aunque la normalización por ISO / CCITT está aún lejana, la aceptación de estos mecanismos en el seno de COSINE-MHS y PARADISE podría suponer su puesta en marcha en el plazo de uno o dos años. Hasta ese momento, están previstas situaciones intermedias que faciliten la operación del servicio, y que también introducimos aquí.

Hemos intentado, en la medida de lo posible, no realizar una presentación demasiado técnica, a pesar de lo específico del tema. En el peor de los casos, su lectura nos permitirá repasar algunos conceptos sobre mensajería y directorio introducidos en anteriores boletines.

Distintos usos del directorio

Desde el punto de vista de la mensajería electrónica, podemos identificar varios niveles de utilización del X.500 (cuando hablamos de "utilizar el directorio" nos referimos tanto a aplicaciones interactivas como intersistema):

- Buscar la ***dirección de correo*** de una persona a partir de su nombre, localización, foto, etc.

- Buscar las **características o *capacidades del Agente de Usuario***:
  Por ejemplo, si soporta multimedia, o uno u otro protocolo (IPM 1984, IPM 1988,...).

- Mantener ***listas de distribución***:
  Permite la gestión de las mismas de forma independiente al servicio de mensajería, lo que hoy es una carga adicional para el postmaster de un MTA.

- ***Autentificación***:
  Consiste en la identificación mutua de las entidades involucradas en una conexión X.400 (Agente de Transferencia - MTA, o de Usuario - UA).

1. IETF: Internet Engineering Task Force.

El encaminamiento dinámico puro constituye la única posibilidad de entender un servicio MHS X.400 a gran escala

- Distribuir y ***actualizar automáticamente las tablas*** estáticas de encaminamiento:
  El directorio posee mecanismos de actualización de copias, y puede ser utilizado como pseudo-base de datos distribuida.

- Buscar ***rutas de encaminamiento de mensajes***:
  Es el encaminamiento dinámico puro, sin utilización de tablas. Es la versión normalizada del DNS de la Internet. Incluimos aquí las tareas de conversión de direcciones RFC-822 en X.400 por atributos y viceversa.

Los dos primeros constituyen el servicio básico y ya están soportados por nuestro Servicio Piloto de Directorio. El mantenimiento de listas de distribución y la autentificación ya están contemplados en la norma X.400 de 1988, pero deben su retraso a la escasa implantación de este protocolo. [1]

La distribución automática de tablas constituye una de las tareas de mayor interés en los contactos entre COSINE-MHS y PARADISE, y será recogido en la nueva versión X.400 de 1992. En un futuro próximo se utilizará en el seno de COSINE-MHS, al menos entre WEPs[2] basados en PP.

El encaminamiento es la búsqueda de una serie de Agentes de Transferencia de Mensajes a través de los cuales podamos alcanzar el buzón del destinatario.

Finalmente, el encaminamiento dinámico puro constituye la única posibilidad de entender un servicio MHS X.400 a gran escala, y por tanto nuestro objetivo a medio plazo. Pasemos analizarlo en mayor detalle.

Encaminar un mensaje

El encaminamiento, en general, es la búsqueda de una serie de Agentes de Transferencia de Mensajes a través de los cuales podamos alcanzar el buzón del destinatario.

Para un MTA en particular, esta tarea de encaminamiento consiste en encontrar otro MTA más próximo al que "reenviar" el mensaje, salvo que el destinatario sea local.

En el caso de la Internet, en una sóla interacción con el servidor de nombres (DNS) se obtiene la dirección de red (IP) de un mailer que soporta de alguna forma el dominio asociado al destinatario. [3]

La extrapolación al caso X.400 no es inmediata, a pesar de contar con una herramienta mucho más potente: el directorio X.500. Las diferencias fundamentales entre ambos modelos son:

- *Menor conectividad* entre MTAs X.400.

- Utilización de *dos tipos de direccionamiento* RFC 822 y X.400. (De hecho se utiliza mucho más el primero)

- *Falta de equivalencia administrativa* con los dominios de la Internet no accesibles directamente por X.400. [4]

En los siguientes apartados veremos cómo afrontar cada uno de estos problemas, íntimamente relacionados.

2. WEP: Well known Entry Point: MTAs que coordinan el servicio de mensajería internacional de COSINE-MHS.

Información mantenida en el directorio

Para utilizar encaminamiento dinámico puro, el directorio X.500 debe contener información suficiente para realizar las siguientes tareas:

- *Representar direcciones X.400* por atributos, del tipo: "/G=ignacio/S=mozos/O=RedIRIS/PRMD=iris/ADMD= /C=ES/", o al menos parte de las mismas.

- *Obtener direcciones* de presentación y protocolos soportados a partir del *nombre distintivo* (DN) de un MTA.

- *Encontrar MTAs asociados* a cada dirección X.400 representada en el mismo.

- *Transformar direcciones* X.400 en RFC 822 y viceversa, según el RFC 1327.

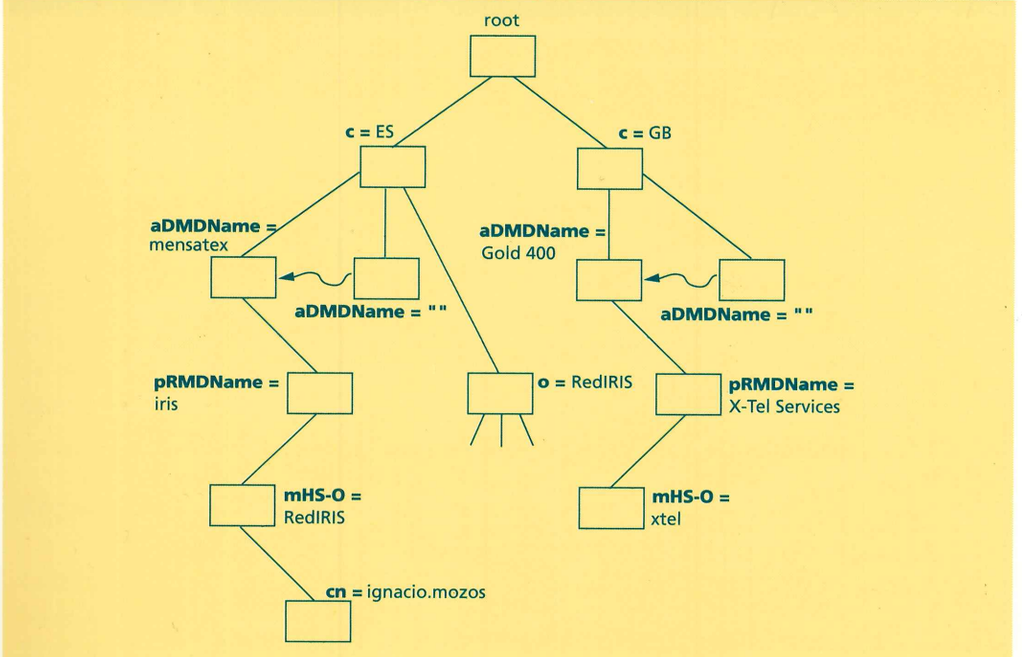
- *Encontrar pasarelas* adecuadas para buzones de la Internet.

RedIRIS, como responsable de la entrada c=ES, ha dado de alta en el directorio el dominio de gestión "mensatex"

Representación de direcciones X.400 en el directorio

La autoridad de directorio de cada país debe añadir bajo el mismo sendas entradas de una nueva clase **aDMD** para cada uno de sus ***Dominios de Gestión Administrativa*** (ADMD) correspondientes. RedIRIS, como responsable de la entrada "c=ES", ha dado de alta el dominio de gestión ***mensatex***, y un alias del mismo, para el convenio del <espacio en blanco>. [4]. (Ver figura adjunta).

REPRESENTACION DE DIRECCIONES X.400 EN EL DIRECTORIO



Con esta representación, cada parte de una dirección X.400 tendrá asociada una entrada en el directorio identificada por su nombre distintivo (DN)

Cada entrada del tipo aDMD se identifica por su atributo ***"aDMDName"***, de forma semejante a que una entrada del tipo *person* se identifica por su atributo *"commonName"*.

Bajo el aDMD correspondiente, se añaden entradas de tipo **pRMD**, identificadas por su "pRMDName" para representar los ***Dominios Privados de Gestión***. Y bajo estos, se dan de alta las ***organizaciones y unidades organizativas de correo***, de tipo ***"mHS-O"*** y ***"mHS-OU"***, respectivamente, y distintas en principio a su representación previa en el directorio.

Aunque esto es suficiente para mantener la información de encaminamiento necesaria, es posible añadir usuarios finales de mensajería, del tipo **mHS-user,** e identificadas por su ***"commonName"***. Esto permite la identificación del destinatario en el MTA originador, lo que no realiza por el momento ningún sistema actual de mensajería.

Con esta representación, cada parte de una dirección X.400 tendrá asociada una entrada en el directorio identificada por su nombre distintivo (DN). [2]. Por ejemplo, la dirección:

"/G=ignacio/S=mozos/O=RedIRIS/PRMD=iris/ADMD= /C=ES/"

Cada entrada del subárbol de direcciones del apartado anterior contiene nombres distintivos de MTAs asociados hacia los que encaminar los mensajes

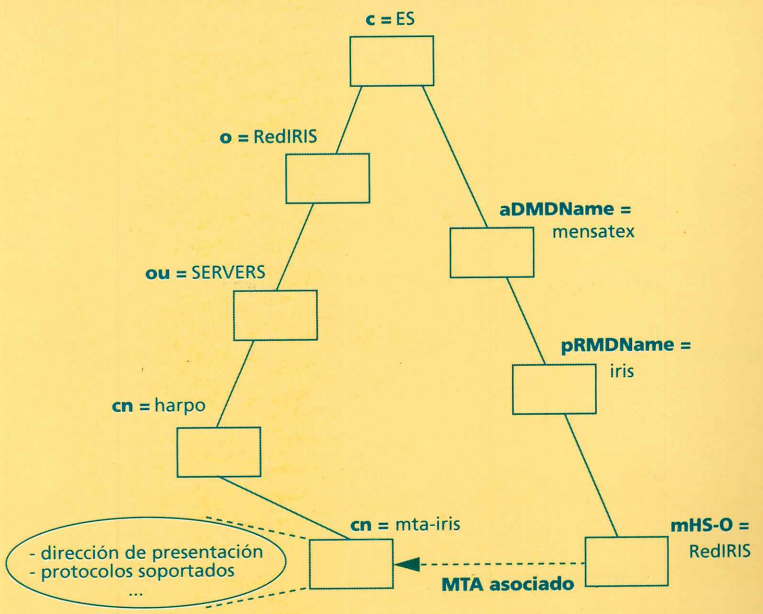
vendrá representada en el directorio por el nombre:

"c=ES@aDMDName= @pRMDName=iris@mHS-O=RedIRIS@cn=ignacio.mozos"

MTA asociado a una dirección X.400

Cada entrada del subárbol de direcciones del apartado anterior contiene nombres distintivos de ***MTAs asociados*** hacia los que encaminar los mensajes. (Ver figura adjunta).

MTA ASOCIADO A UNA DIRECCION X.400



En el caso de entradas de tipo mHS-user, mHS-O ó mHS-OU, los MTAs asociados pueden soportar directamente a los Agentes de Usuario. Es el caso de alta conectividad entre MTAs, análogo al modelo RFC-822.

Para entradas de tipo pRMD o aDMD, los MTAs asociados son pasarelas del dominio correspondiente. Constituyen el modelo opuesto, de baja conectividad entre MTAs, utilizado actualmente en el servicio internacional de mensajería COSINE-MHS.

Modelando el contenido del directorio podemos regular el grado de utilización de pasarelas para cada dominio u organización, tanto para el tráfico saliente como entrante, lo que no es factible con tablas estáticas.

Modelando el contenido del directorio podemos regular el grado de utilización de pasarelas para cada dominio u organización

Información mantenida sobre un MTA

En Internet, todos los "mailers" propuestos por el DNS para encaminar correo (MX records asociados a un dominio) son accesibles por cualquier otro mailer. Si el dominio no pertenece a mensajería SMTP, el mailer propuesto es una pasarela que sí será accesible directamente por SMTP, lógicamente sobre IP.

En X.400, el grado de conectividad es menor por las siguientes razones:

- Utilización de ***diferentes protocolos*** de transporte. Por ejemplo, TP4 sobre CLNP, TP0 sobre X.25 ó TP0 sobre TCP/IP (RFC 1006).
- Coexistencia de ***diferentes redes*** con el mismo protocolo pero no interconectadas, Por ejemplo, EMPB y PSDN X.25.
- Utilización de ***diferentes versiones*** de X.400: 1988 y 1984.
- Interacción con ***servicios no X.400***. La interoperabilidad con Internet no es simétrica.

En Internet, todos los "mailers" propuestos por el DNS son accesibles por cualquier otro mailer. En X.400, el grado de conectividad es menor

Con esta panorámica, cada MTA registrado en el directorio deberá mantener información suficiente para comprobar la conectividad con el mismo a diferentes niveles:

- ***Direcciones de presentación*** del MTA en las diferentes redes a las que esté conectado.
- ***Comunidades de transporte***: IXI (ahora EMPB), Int-X.25, Internet, ...
- ***Contextos de aplicación*** soportados: P1 1984, P1 1988, etc.

Aún así quedarían por resolver otros problemas de encaminamiento comunes al caso de utilización de tablas como son la falta de conectividad total en el backbone de ADMDs y el caso de registros de PRMDs no interconectados realmente con el correspondiente ADMD. Pero dejemos que estos problemas los aclaren primero los señores del MHS-sin-DS.

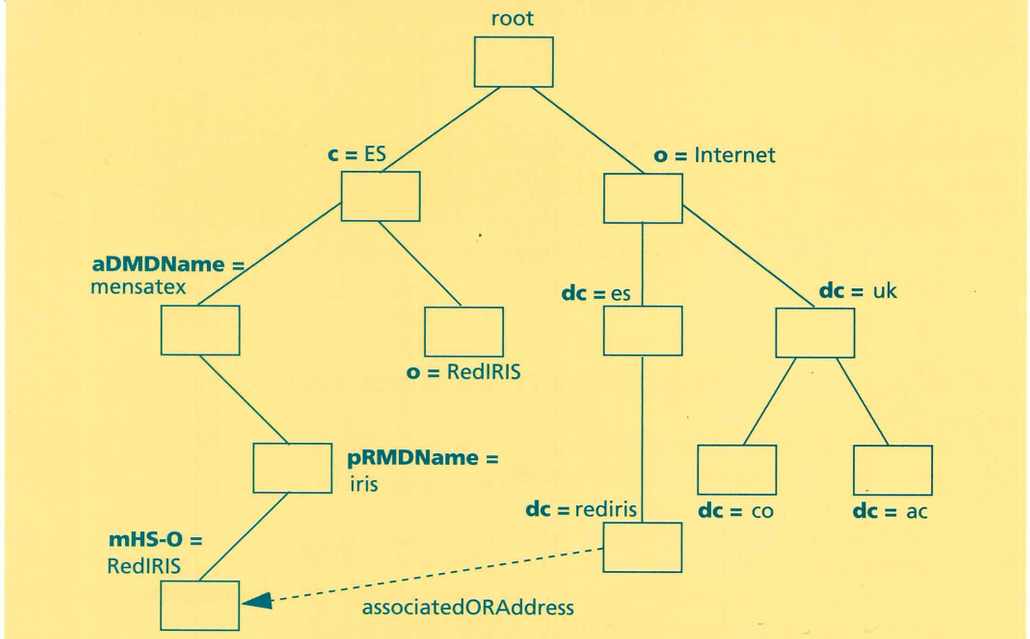
Representación de dominios RFC-822

Cada país debe registrar su dominio RFC-822 bajo una entrada global ***o=Internet*** destinada a tal efecto. (Ver figura adjunta). La autoridad sobre esta entrada la ejerce ahora el gestor de directorio para Estados Unidos.

Cada dominio registrado bajo o=Internet contiene información sobre la parte de direcciones X.400 que representa.

Los dominios representados en el directorio se identifican por el nombre "***domainComponent***", en abreviatura ***dc***. RedIRIS ha registrado allí el dominio "**dc=** *es*", y por tanto, se prodría volcar toda nuestra información del DNS bajo ese dominio. (Se buscan voluntarios :-).

REPRESENTACION DE DOMINIOS RFC.822



Conversión de direcciones RFC-822 en X.400 y viceversa

RFC-822 —> X.400

Sin entrar todavía en detalles sobre la equivalencia administrativa entre ambos espacios de direcciones [4], cada dominio registrado bajo *o=Internet* contiene información sobre la parte de direcciones X.400 que representa a través de un atributo ***"associatedORAddress"***.

Esto permite al MTA obtener la información suficiente para la conversión de direcciones con formato RFC 822 en direcciones OR por atributos separados por "/" sólo si el buzón correspondiente a esa dirección está situado en el mundo X.400. (Ver figura del apartado anterior).

X.400 —> RFC 822

De forma semejante, cada entrada del árbol de direcciones X.400 contiene información sobre su dominio RFC-822 asociado (si lo tiene), a través del atributo "***associatedDomain***". En este caso la conversión siempre es válida.

Interoperabilidad entre RFC 822 y X.400. La mensajería global

El soporte de la recomendación RFC 1327 [5] cuando no hay equivalencia administrativa entre un espacio de direcciones RFC 822 y otro X.400 es seguramente el mayor problema para el encaminamiento dinámico.

Recordemos que la no equivalencia administrativa entre espacios de direcciones se da cuando los dominios asociados están bajo distinta administración. El citado RFC 1327 especifica un mecanismo general de transformación de direcciones en ambos sentidos por encapsulación de la dirección de un sistema empleando notación correspondiente al otro. [4].

La información que se obtiene del directorio es independiente del punto de acceso, y por tanto no podemos hacer conversiones locales con el árbol global de dominios.

Sin embargo, por diversas razones cada país viene utilizando transformaciones locales diferentes para aquellos dominios RFC 822 no encaminables por X.400. Y así, por ejemplo, nos encontramos con conversiones tan dispares como:

Michaelson@cs.mit.edu ->

En España, /S=Michaelson/OU=cs/OU=mit/O=edu/PRMD=internet/ADMD=0/C=es/
y en Alemania, /S=Michaelson/OU=cs/O=mit/PRMD=edu/ADMD=dbp/C=de/

Por otro lado, la información que se obtiene del directorio es independiente del punto de acceso, y por tanto difícilmente podremos realizar este tipo de conversiones haciendo uso del árbol global de dominios presentado en apartados anteriores.

Este software incluye un MTA X.400 (84) de altas prestaciones, canales X.400 (88), SMTP y software X-Windows para la gestión del MTA.

Para mantener información de rutas local a un MTA, Steve Kille [6] propone un nuevo tipo de entrada denominada "***routingTree***", ó subárbol de rutas del directorio localizado en alguna parte bajo la entrada del país o PRMD, o incluso organización, que utilice estrategias de direccionamiento o encaminamiento locales.

Por el momento, este uso avanzado del directorio no ha sido probado en el seno de la experiencia desarrollada con X-Tel Services que a continuación pasamos a comentar, por lo que no entraremos en más detalle al respecto.

PP, la otra alternativa académica X.400

Desde sus orígenes, el software X.400 más extendido en IRIS ha sido EAN[3]. Con el paso del tiempo, y a pesar de sus limitaciones técnicas y de las expectativas creeadas en un principio sobre productos comerciales X.400, la realidad es que este software ha sobrevivido con dignidad hasta nuestros días.

En la actualidad, una alternativa real es el PP. Este software está desarrollado sobre ISODE e incluye además de un MTA X.400 (84) de altas prestaciones, canales X.400 (88), SMTP, JNT Mail, DECNET Mail-11 y UUCP, así como software X-Windows para la gestión del MTA.

Uno de los atractivos del PP para nosotros es su apuesta firme por desarrollar y probar nuevos

3. EAN: The EAN Message System. University of British Columbia. Canada.

mecanismos de interacción con el directorio, avalado por su orígen común a los impulsores de QUIPU, el software X.500 que soporta el Servicio Piloto de Directorio PARADISE.

Se ha podido transferir mensajes de prueba entre buzones de X-Tel Services y de RedIRIS sin utilizar los WEP de Reino Unido y España, ni el acuerdo explícito entre los respectivos postmaster

Es precisamente una versión *beta* del PP-6.4, aún no disponible en el dominio público, el software utilizado para nuestra experiencia. Es probable que esta versión aparezca en esta ocasión como producto comercial, soportado por X-Tel Services Ltd.

Nuestra experiencia

Esta ha consistido en la configuración de un MTA PP-6.4 (versión beta) de pruebas para el dominio *harpo.rediris.es*, así como la adición al directorio de la información suficiente para hacer encaminamiento dinámico y transformación de direcciones X.400 en RFC 822 y viceversa.

De esta forma se ha podido transferir mensajes de prueba entre buzones de X-Tel Services y de RedIRIS sin utilizar los WEP de Reino Unido y España, localizados en otras máquinas. Para ello no ha sido necesario el común acuerdo entre los respectivos postmaster de los MTAs PP-6.4 en pruebas, puesto que la identificación de MTAs también está soportados por el Directorio.

Un ejemplo sencillo es comprobar que la dirección de un buzón de X-Tel Services se alcanza directamente a través de su MTA, mientras el nuestro no posee información alguna sobre los dominios RFC 822 o X.400 del Reino Unido.

EJEMPLO DE ENCAMINAMIENTO UTILIZANDO EL DIRECTORIO

```
harpo# testroute "/i=j/s=onion/o=xtel/prmd=x-tel services/admd= /c=gb/"

For ORName /i=j/s=onion/o=xtel/prmd=x-tel services/admd= /c=gb/,
        best match at c=GB@aDMDName=\20@pRMDName=X-Tel Services@mHS-O=xtel
        route to MTA c=GB@o=X-Tel Services Ltd@cn=lancaster@cn=xtel-mta
        name UK.CO.XTEL
       presentationaddress "597"/Internet=128.243.9.1|Jnet=00002100102999|IXI=20433450210399|
                    JanetNS=0210021900015000|IXI=20433450210399
        transport communities:tc-cons, tc-internet,  tc-ixi, tc-janet
        Supported Application Contexts: ac-p1-1988
```

Referencias

[1] ISO 10021 / CCITT Recommendations X.400. 1988.

[2] Nombres y direcciones. Ignacio Martínez. Boletín de RedIRIS nº 11-12. Abril de 1991.

[3] ... y rutas. Ignacio Martinez y Celestino Tomás. Boletín de RedIRIS nº 13. Septiembre 1991.

[4] Sintaxis empleada en las direcciones de mensajería electrónica. Ignacio Martínez. Boletín de RedIRIS nº 18. Julio de 1992.

[5] RFC 1327 - Mapping between X.400(1988) / ISO 10021 and RFC 822. Hardcastle - Kille. May 1992

[6] MHS use of Directory to support MHS routing. Steve Kille. Internet Draft. November 1992.

Ignacio de los Mozos
Ingeniero de Sistemas de RedIRIS.
ignacio.mozos@rediris.es
C=es; ADMD=mensatex; PRMD=iris;
O=RedIRIS; S=mozos; G=ignacio

Seguridad en Correo Electrónico. Proyecto P8 de COSINE

Francisco Jordán, Manel Medina y Enric Peig

Resumen

Tras una introducción a los servicios y mecanismos de seguridad empleados en la comunicación de datos entre aplicaciones distribuidas, se describen los empleados en el servicio de mensajería electrónica privatizado (Privacy Enhanced Mail = PEM). Finalmente se describen las actividades realizadas dentro del proyecto P8, financiado por COSINE, para la puesta a punto de un servicio de comunicaciones seguras, en el entorno académico europeo.

Dentro del apartado de la seguridad en el intercambio de información entre sistemas informáticos existen varios niveles de servicio, desde el tradicional cifrado de datos o criptografía hasta la innovadora gestión de dominios de seguridad

1.- Introducción

El concepto de seguridad en computadores es muy extenso y abarca una gran variedad de temas, desde el más elemental control de acceso hasta la sofisticada auditoría informática. En particular, nosotros nos vamos a centrar en el apartado de las comunicaciones seguras entre computadores. También dentro del apartado de la seguridad en el intercambio de información entre sistemas informáticos existen varios niveles de servicio, desde el tradicional cifrado de datos o criptografía hasta la innovadora gestión de dominios de seguridad.

El artículo hace una revisión a los servicios de seguridad, centrándose después en el correo electrónico para explicar, a modo de ejemplo, los distintos servicios de seguridad ofrecidos. A continuación se describe la arquitectura, implementación y pruebas realizadas sobre estos servicios seguros en el marco del proyecto piloto P8 de COSINE. Por último y como conclusión se describe una posible extensión de los resultados del P8 en la comunidad académica española.

2.- Servicios de seguridad

De forma muy básica, las comunicaciones seguras introducen los siguientes servicios:

1) **Autenticación:** Corrobora la identidad de las entidades implicadas en la comunicación.

2) **Control de acceso**: Protege sistemas y recursos contra su uso no autorizado.

3) **Confidencialidad**: Protege los datos en la comunicación, de forma que para usuarios no autorizados sea prácticamente imposible interpretar dichos datos.

4) **Integridad**: Protege los datos en la comunicación contra cualquier intento de modificación, inserción, reordenación o destrucción de forma no autorizada.

5) **No rechazo**: Protege las entidades contra el rechazo del hecho de haber generado -enviado- o procesado -recibido- datos.

Aunque todos los servicios seguros mencionados son aplicables de forma análoga a la totalidad de las comunicaciones seguras, en este artículo usaremos, a modo de ejemplo para describir cada uno de estos servicios, una modalidad de comunicación muy extendida: el correo electrónico.

3.- Servicio de mensajería electrónica

En la actualidad el servicio de correo electrónico es quizás el servicio más utilizado por la comunidad académica y otras comunidades. Dicho servicio constituye el principal medio de comunicación e intercambio de información entre usuarios mayoritariamente humanos. Pensando en el grado de importancia de la información que es manejada, en estos momentos los usuarios de correo electrónico no tienen disponibles servicios suficientes para estar protegidos contra ciertos ataques. Por ejemplo, dados tres usuarios A, B y C del servicio de correo electrónico, supongamos que el usuario A quiere enviar un mensaje confidencial M a B, a partir de esta premisa se puede plantear lo siguiente:

En estos momentos los usuarios de correo electrónico no tienen disponibles servicios suficientes para estar protegidos contra ciertos ataques

a) ¿Puede A asegurar que el mensaje sólo lo leerá B? Por supuesto la contestación es no!!!, además, esto es más cierto cuantos más sistemas intermedios atraviese el mensaje; aún suponiendo que A y B sean usuarios locales, si C es el usuario postmaster, seguro que C puede leer el mensaje.

b) ¿Puede B asegurar que el contenido del mensaje recibido es el original y por tanto asumirlo como tal? Otra vez la respuesta es no!. Aun suponiendo que nadie modificara el contenido intencionadamente, puede ocurrir que algún agente intermedio realice alguna alteración o conversión (p.e. limitando la longitud de las líneas, de contenido, etc.).

c) ¿Puede B asegurar que el mensaje recibido ha sido efectivamente enviado por A? De nuevo la contestación es no!. Existen muchas y sencillas formas de suplantar la personalidad de otro usuario en correo electrónico, de forma que el usuario B reciba como remitente al usuario A y haya sido C el originador del mensaje (p.e. telnet -p 25, cualquier postmaster, etc.).

d) ¿Pueden A y B protegerse contra el rechazo unilateral o mutuo? Esto es, ¿Puede A asegurar que B ha leído el mensaje y por tanto aceptado su contenido (no rechazo de recepción)? y ¿Puede B asegurar que A le envió el mensaje (no rechazo de envío)? La respuesta es negativa. En ambos casos, los usuarios necesitan una prueba irrefutable del hecho, cosa imposible de conseguir con un sistema de correo normal, ya que A puede alegar fácilmente que el supuesto mensaje recibido por B ha sido generado por otro (hasta lo ha podido generar B), o al contrario, el usuario B puede leer el mensaje y después destruirlo y afirmar que jamás ha visto dicho mensaje.

Cada una de las preguntas anteriores pueden tener una respuesta afirmativa introduciendo los servicios de seguridad en el sistema de correo electrónico. La pregunta a) necesitaría de los servicios de confidencialidad, la b) de servicios de integridad, la c) de servicios de autenticación [1] y la d) de servicios de no rechazo.

3.1.- Mecanismos de seguridad

En la actualidad existen y conviven distintos mecanismos de seguridad capaces de proporcionar los diferentes servicios. Estos son:

1. Aunque la autenticación de entidades generalmente vaya asociada a un proceso de conexión de la comunicación, también puede entenderse como la corroboración de identidades en un proceso sin conexión como es el caso del correo electrónico a nivel de mensaje.

- **Cifrado simétrico o privado**. Técnica criptográfica en la cual las entidades a comunicar comparten un mismo secreto llamado clave o llave de cifrado (K). De esta forma, si el usuario A encripta (cifra) el mensaje M utilizando K para obtener un mensaje cifrado X -X=E(K,M)- a enviar a B, este podrá asegurar que sólo éste podrá leer el mensaje cifrado X, pues B es el único conocedor del secreto K y por tanto es el único capaz de desencriptar el mensaje -M=D(K,X)- para obtener el mensaje en claro M (figura 1).

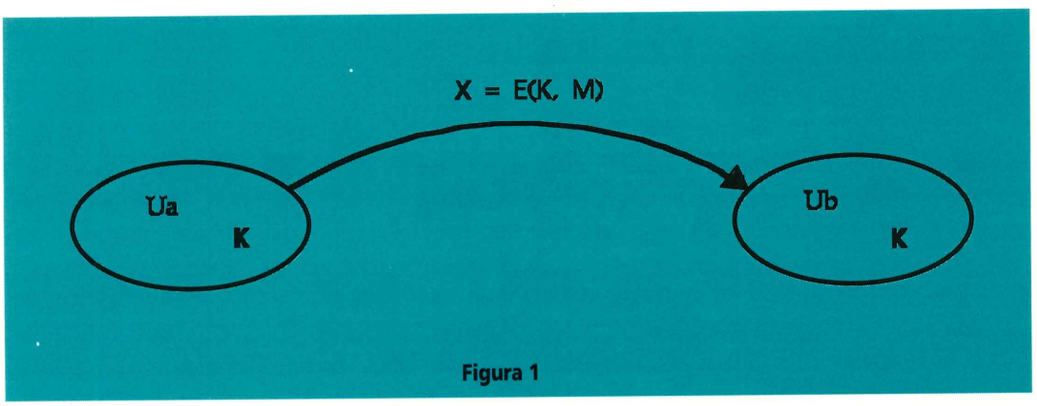


Figura 1

- **Cifrado asimétrico o público**. Técnica criptográfica en la cual cada entidad posee dos clases distintas de claves de cifrado, una clave llamada pública (Kp) compartida por todos los interlocutores para encriptar y otra clave llamada privada o secreta (Ks) conocida tan solo por una entidad para desencriptar, de manera que es prácticamente imposible deducir la una de la otra. De esta forma, si el usuario A envía un mensaje a B utilizando la clave pública de B KBp, sólo el usuario B podrá leer el mensaje ya que es el único que posee la clave secreta correspondiente KBs. La propiedad más importante de esta técnica se refleja en la siguiente relación: si X=E(Kp,M) entonces M=D(Ks,X) pero M<>D(Kp,X), y además también si Y=E(Ks,M) entonces M=D(Kp,Y) (figura 2).

- **Firma digital**. Técnica criptográfica en la cual el originador de un mensaje M genera un código F llamado firma, que depende del mensaje y de un secreto sólo conocido por él, de

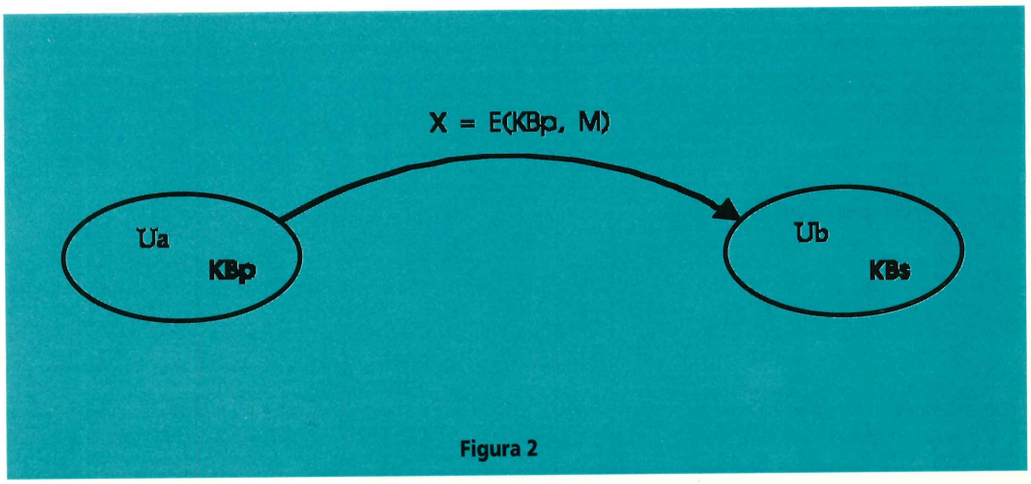


Figura 2

forma que F puede ser verificada por el receptor del mensaje. Una forma de implementar la firma digital es utilizando el mecanismo de cifrado asimétrico. Por ejemplo si A envía a B, M y F donde F=E(KAs,H(M)) y H() es una función hash pública, entonces B podrá asegurar y demostrar que A ha sido el generador del mensaje M ya que podrá verificar que H(M)=D(KAp,F) y por lo tanto que sólo A ha podido encriptar dicho mensaje (ya que es el único usuario que dispone de KAs). Además, B también comprueba que M no ha sido modificado ya que sino H(M) sería diferente (figura 3).

Uno de los problemas más importantes de las comunicaciones seguras es el de la distribución y gestión de claves

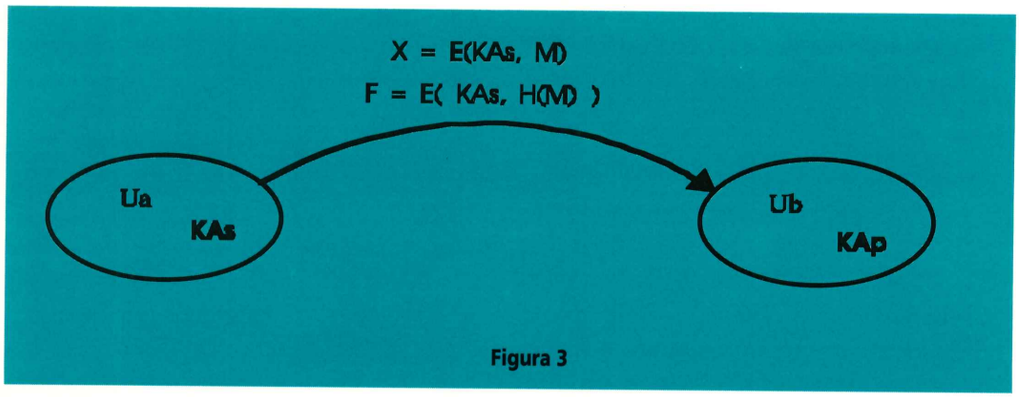


Figura 3

Con los mecanismos descritos se pueden implementar los servicios de seguridad arriba mencionados. La tendencia actual es utilizar algoritmos simétricos como el DES para los servicios de confidencialidad e integridad[2] algorítmos asimétricos y firmas digitales como el RSA y RSA-DSA para servicios de autenticación y no rechazo.

3.2.- Las claves de cifrado

Uno de los problemas más importantes de las comunicaciones seguras es el de la distribución y gestión de claves. Al utilizar una técnica criptográfica, se ha de conseguir que las entidades o usuarios implicados en la comunicación obtengan de una forma segura (confidencial e íntegra) las claves necesarias para poder encriptar/desencriptar los datos. Dependiendo de la técnica utilizada, esto es, simétrica o asimétrica, se tendrán una serie de ventajas y desventajas en cuanto a la gestión y distribución de claves, a saber:

- En cuanto a la distribución de claves, suponiendo una comunidad de N usuarios en la que se quiere insertar un nuevo usuario (N+1), es necesario distribuir la llave KN+1 al resto de la comunidad y a su vez entregar las N claves K1..KN al nuevo usuario. En el caso de una técnica asimétrica dicha distribución se realiza siempre de forma segura ya que las claves distribuídas son las públicas (K1p..KNp,KN+1p), pero en el caso de técnica simétrica es necesario hacer la distribución de forma privada a cada usuario. Por este motivo la técnica asimétrica es más conveniente para la distribución, pues esta es tan sencilla como publicar las claves Kp (p.e. utilizando el directorio) y la otra obliga a su vez establecer canales seguros para distribuir las claves que han de garantizar una seguridad posterior, cosa no tan sencilla a veces.

2. Aunque los algoritmos más utilizados son los llamados MDx (MD4,MD5,..).

En cuanto a la gestión de claves, el objetivo es establecer algún mecanismo que asegure la pertenencia de las claves distribuidas al usuario indicado en exclusiva, y en general, definir una política de seguridad para la comunidad de entidades y usuarios pertenecientes a un dominio gestionado por la misma autoridad

- En cuanto a la gestión de claves, el objetivo es establecer algún mecanismo que asegure (certifique) la pertenencia de las claves distribuidas al usuario indicado en exclusiva, y en general, definir una política de seguridad para la comunidad de entidades y usuarios pertenecientes a un dominio gestionado por la misma autoridad. En el caso de técnica asimétrica existen autoridades de certificación (Certification Authority, CA), cuya principal misión es la de generar el par de claves Ks-Kp para un usuario en particular, que se identifica por su nombre distintivo (Distinguished Name de X.500) y publicar lo que se conoce como certificado de usuario. Un certificado está formado básicamente, por la clave pública Kp, un tiempo de validez de la clave y la firma de la CA. Esto es, el certificado de un usuario B sería CB = KBp,T,E(KCAs,H(KBp,T)) -donde KCAs es la clave secreta de la CA-. De esta forma, cualquier usuario que desee enviar información a B sólo necesita: a) conseguir el certificado de B, cuya autenticidad podrá verificar analizando la firma de la CA (KCAp es conocida por toda la comunidad); y b) cifrar utilizando KBp. En el caso de técnica simétrica existen centros de distribución de claves (Key Distribution Center, KDC), los cuales almacenan de forma segura todas las claves correspondientes a la comunidad. Notar que en ambos mecanismos los usuarios dependen de -deben creer en- una entidad superior, CA o KDC, por lo cual estas entidades deben ser muy seguras ya que de ellas depende la seguridad de la comunidad. Debido a la naturaleza de ambos mecanismos, la seguridad de una CA es siempre superior a la de un KDC en cuanto la CA sólo debe mantener en secreto la KCAs, al contrario que un KDC que tiene que proteger todas las claves de la comunidad.

- Otra ventaja de la técnica asimétrica es que las claves suelen ser muy largas, al contrario que las simétricas que suelen ser cortas, por ello el período de validez de una clave asimétrica es siempre superior al de una simétrica, lo cual conlleva una mayor tarea de gestión en esta última. Esta ventaja se convierte en desventaja a la hora de generar y utilizar las claves, ya que los algoritmos de generación y cifrado asimétricos son mucho más complejos (y por lo tanto más lentos) que los simétricos.

3.3.- Servicio de Mensajería Privatizado (PEM)

Vistos los servicios y mecanismos de seguridad disponibles, no es difícil comprender por ...qué el método PEM (Privacy Enhanced Mail) de Internet se ha convertido en el método más usado para la seguridad en correo electrónico[3]. Las características de seguridad de PEM se pueden resumir en los siguientes puntos:

- Puede utilizar una técnica asimétrica (generalmente RSA) o simétrica (generalmente DES) para distribución y gestión de claves entre usuarios. En el caso asimétrico, un usuario A con nombre distintivo DNa tiene asociado un certificado CA generado por la autoridad de certificación a la que pertenece[4]

- Utiliza firma digital (generalmente RSA-DSA) para la generación de certificados. Existen definidas unas normas para la CA y la estructura del certificado (está basado en la X.509).

3. La seguridad en PEM está orientada al contenido del mensaje, al contrario que X.400/88 que está en el sobre (protocolo P1), esto hace que PEM sea compatible con cualquier sistema de correo electrónico, mientras que X.400/88 no.

4. La idea de CA es muy similar a la de dominio de gestión en la estructura jerárquica del directorio. Pueden existir muchos CAs que se encargan de gestionar los usuarios que serían nodos subordinados al nodo del CA en el directorio.

- Utiliza una técnica simétrica (generalmente DES) para el cifrado del contenido del mensaje.

En cuanto al tratamiento de los mensajes, el método PEM, a partir del contenido del mensaje de usuario realiza una transformación de éste y genera otro mensaje que contiene una cabecera PEM en la cual hay parámetros de seguridad (Originator-Certificate, Key-Info, MIC-Info, etc.) y el contenido original cifrado o no. Este nuevo mensaje PEM se puede enviar utilizando cualquier plataforma de correo, ya que tiene un formato imprimible (figura 4).

```
——BEGIN PRIVACY-ENHANCED MESSAGE——
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,F6F764CD8293D0C9
Originator-ID-Asymmetric: C=ES; O=UPC; CN=Francisco Jordan:C=IE;
O=Baltimore; OU=root-ca:408
Originator-Certificate:
 MIIBQjCB8AIBWTAKBgRVCAMBAgICADAzMQswCQYDVQQGEwJJRTESMBAGA1UEChMJ
 QmFsdGltb3JlMRAwDgYDVQQLEwdyb290LWNhMB4XDTkyMDkwODE1MTkzNVoXDTkz
 MDkwODE1MTkzNVowMDELMAkGA1UEBhMCRVMxDDAKBgNVBAoTA1VQQzETMBEGA1UE
 AxMKRW5yaWMgUGVpZzBYMAoGBFUIAwECAgIAA0oAMEcCQKxQbTZrDaeKIVtCQ9vj
 VvzOOyxt3c7Ta1jbfsWeq03o+vs9qQMsiLI/+Qh435JS670ERowTPwrPzQGJyGdT
 X2kCAwEAATAKBgRVCAMBAgICAANBABfahvxXiNI8FK9pK5iv+XAV0GQisrtBAEML
 MEPgJjh5VPZO5JqQpzbEJVR3rl8qMlYbmuDoMgpcXCdI1lTu9os=
MIC-Info: md5,RSA,
 AUnxmW9AZWsrMa3eocZUA3t38YtTgVPLXsNkSrtpErqpeLMtatSDZaepwH7b4FmX
 og1Bm/B598v2SykDSEHqwouVyQAjxb3V
Recipient-ID-Asymmetric: C=IE; O=BALTIMORE; CN=SUSAN:C=IE; O=Baltimore;
OU=root-ca:157
Key-Info: RSA,
 In2HaFSpeS9MiluofN+VHTYrP69IyAm6+vcJBViUPUdbSyvKfzr9slsr9csmcmMx
 NBJQV4+yPOk60VemKuNRVA==
Recipient-ID-Asymmetric: C=AT; O=GRAZ; CN=VESNA RISTIC:C=IE;
O=Baltimore; OU=root-ca:205
Key-Info: RSA,
 djsKFgY5wKf+B/UYvGsQgsrDAMm28o6+RHS8wmCRRdsf5jjmmwuCWVaI4+zeyyZh
 5vwX2btGa84UGEJKpXuOtA==

 d2ifLzCt/eeBDe2kQ01QDLWFB7wamhY4UZGcaQVikc3CNr/21LO5TF0oGbxtwH6G
 9xpiO8++JfCIuh3ulbJbNbT7CKnxqZpuF/ZiTRdEI9FPR4eFpp2lMA==
——END PRIVACY-ENHANCED MESSAGE——
```

Figura 4

Como se puede observar, PEM encapsula el mensaje seguro entre un principio y final de mensaje ("BEGIN/END PRIVACY-ENHANCED MESSAGE"). Entre estas marcas se encuentra primero la cabecera PEM que contiene, entre otros, los campos de:

- Proc-Type: Indica el tipo de procedimiento aplicado, sólo integridad o integridad y confidencialidad. En este ejemplo están ambas opciones.

- DEK-Info: Indica el algoritmo y **vector de inicialización** "(VI)" utilizados para aplicar confidencialidad sobre el contenido (texto) del mensaje. En el ejemplo se utiliza DES modo CBC con VI del valor indicado.

- Originator-ID-Asymmetric: Indica el originador del mensaje, en este caso utilizando mecanismo asimétrico para la gestión de llaves. En el campo se indica el nombre distintivo del usuario originador y el de la autoridad de certificación a la que pertenece dicho usuario.

- Originator-Certificate: Incluye el certificado del usuario originador. Este campo es muy útil mientras no se disponga de directorio ya que facilita la tarea de recepción.

- MIC-Info: Indica el algoritmo utilizado para generar el código de integridad del mensaje (MIC) -ejemplo es MD5-, el algoritmo para firmar el MIC -ejemplo es RSA con clave secreta del originador- y el MIC con la firma.

- Recipient-ID-Asymmetric: Pueden aparecer varios de estos campos indicando el nombre distintivo de un usuario destinatario y el de la autoridad de certificación asociada.

- Key-Info: Aparece después del campo anterior e indica un algoritmo de cifrado bajo el cual se ha encriptado la clave utilizada para cifrar el texto del mensaje (DEK-Info). En el ejemplo se utiliza RSA y la clave para encriptar el texto se ha cifrado con la clave pública del usuario destinatario. De esta forma sólo un usuario indicado como destinatario podrá descifrar la clave utilizada para encriptar el texto.

El proyecto piloto P8 es un proyecto práctico, cuyo objetivo es la definición, implementación y prueba de servicios seguros para la comunidad de usuarios bajo COSINE

Existen multitud de campos que se pueden incluir en la cabecera, pero con los mencionados, ya es suficiente para implementar los servicios de seguridad definidos anteriormente. Después de la cabecera y separada por una línea en blanco aparece el texto del mensaje, cifrado o no dependiendo del tipo de procedimiento. En el ejemplo aparece cifrado utilizando el algoritmo y vector inicial indicado en DEK-Info y la clave incluida en el campo Key-info.

4.- Proyecto Piloto P8 de COSINE

Originalmente, en el proyecto piloto se pretendía establecer servicios de seguridad para correo electrónico y acceso remoto, pero este último se limitó posteriormente.

El proyecto piloto P8 es un proyecto práctico, cuyo objetivo es la definición, implementación y prueba de servicios seguros para la comunidad de usuarios bajo COSINE. La participación en el proyecto fue restringida y por invitación, las instituciones participantes son Baltimore Technologies de Irlanda (contratados directamente por COSINE) y JANET de Reino Unido, SURFNET de Holanda, Trinity College Dublin de Irlanda,Technische Universität de Graz Austria, Fachhochshule Rheinland-Pfalz de Alemania y Universitat Politécnica de Cataluña de España (instituciones invitadas). El proyecto piloto se acabará a finales del primer trimestre de 1993, con posibilidad entonces de ampliación de participantes e implantación de los servicios en los países participantes y otros.

Originalmente, en el proyecto piloto se pretendía establecer servicios de seguridad para correo electrónico y acceso remoto, pero este último se limitó posteriormente. El servicio de correo electrónico seguro se basó en el PEM, utilizando el producto público SECUDE desarrollado por el GMD de Darmstadt, y sobre la infraestructura de X.400 MHS (1984) existente.

La arquitectura de seguridad adoptada en el proyecto piloto se definió dentro de un dominio de seguridad de COSINE (COSINE Security Domain, CSD) basado en mecanismos públicos (asimétricos) de criptografía, establecidos en la fase de especificación de COSINE. Todas las instituciones participantes están dentro de dicho dominio en el cual sólo existe una autoridad de certificación (CA) instalada y gestionada por Baltimore Tech. en Dublin (IE). Debido a la imposibilidad de utilizar servicios de directorio (X.500) para la distribución de certificados, los

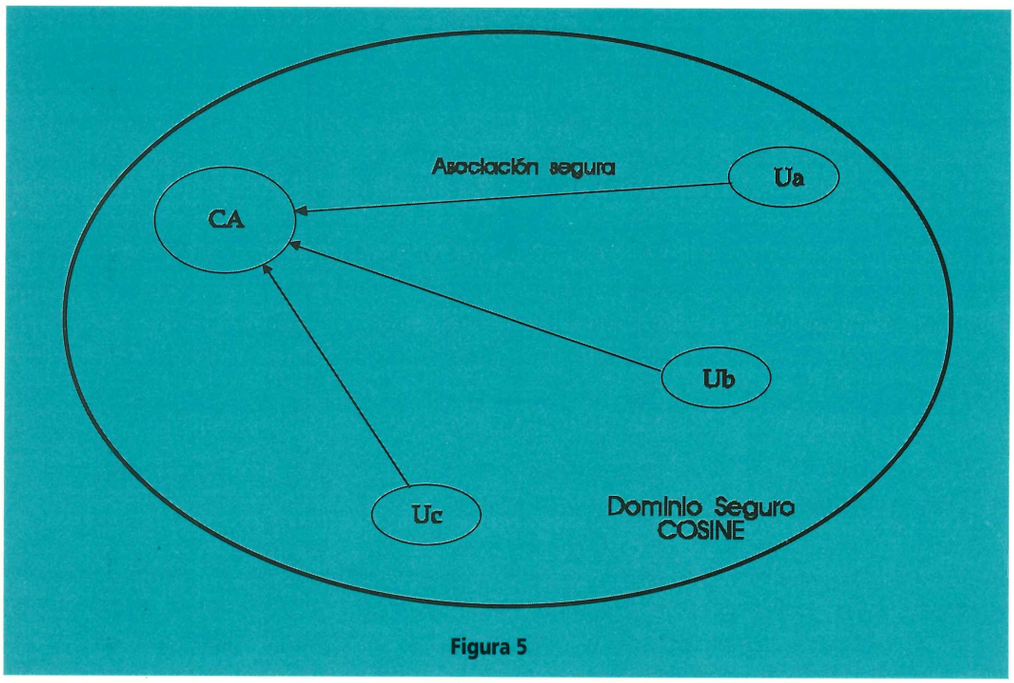


Figura 5

usuarios accedían al CA remótamente mediante una asociación segura (control de acceso seguro utilizando autenticación por medio de técnica asimétrica) para obtener los certificados públicos de los restantes usuarios -figura 5-. De todas formas, está previsto utilizar el directorio en otra posible fase del proyecto, así como aumentar el número de CAs, p.e. una por país.

Baltimore Tech. fue la encargada (bajo la supervisión del CPMU de COSINE con representación de las instituciones participantes) de la implementación y puesta en marcha de las pruebas de los servicios de seguridad. Entre todos los participantes se definieron unos requisitos mínimos de tráfico seguro para las pruebas, cuyas cifras se acordó que no fueran menores de: 40 usuarios, y un tráfico de 10.000 mensajes PEM entre todos los participantes durante el período de pruebas.

El resultado final del proyecto será un informe explicando la experiencia práctica de proveer servicios seguros a la comunidad, así como ofreciendo la posibilidad de ampliar los servicios dentro de cada institución o país participante.

5.- Extensión a nuestra comunidad

Como se ha mencionado anteriormente, la fase de pruebas del proyecto piloto P8 termina a finales del primer trimestre del 1993, teniendo en cuenta que la comunidad académica española dispone de la infraestructura necesaria (X.400 y acceso remoto X.25) para acomodar los servicios seguros de correo electrónico, podría ser ésta una buena oportunidad para introducir dichos servicios a los usuarios de correo. Como primer paso se podría definir un dominio seguro con una sólo CA gestionado por IRIS, cuya misión sería la de gestionar la generación y distribución de certificados a los usuarios. Esta arquitectura se podría mantener hasta que dispusiéramos de una implementación del CA basada en el directorio, con la cual se podría ampliar el número de CAs, distribuyéndolos entre diferentes instituciones, descentralizando y minimizando de este modo la gestión en IRIS.

Desde el punto de vista de recursos informáticos, para operar el CA se necesitaría una estación de trabajo UNIX conectada a X.25 o IXI, a ser posible protegida por medio de tarjeta inteligente (chip-card). En cuanto a los usuarios, necesitarían cualquier estación UNIX conectada a X.25 o IXI donde poder instalar los programas de seguridad para generar mensajes PEM y acceder al CA. Nuestra experiencia en el proyecto nos ha demostrado que una sola estación conectada a X.25 o IXI sería suficiente para una comunidad de usuarios no muy elevada.

En estos momentos estamos trabajando en un posible acceso a CA por correo electrónico, tal y como se define en PEM, que podría substituir el acceso remoto mientras no dispusiéramos de directorio de forma global. A largo plazo este método está destinado a sustituir al actual de acceso remoto a la CA, aunque al final también podrían convivir ambos métodos, directorio y acceso por correo.

6.- Conclusiones

En este artículo hemos realizado una breve pero completa descripción de los servicios básicos de seguridad, así como las distintas técnicas y problemas que se plantean en la gestión de la seguridad. Aunque los ejemplos y discusiones planteadas se hayan centrado en el servicio de correo electrónico, las conclusiones se pueden extender a cualquier otra modalidad de comunicación, p.e. seguridad en comunicaciones a nivel de transporte o de red (niveles 4 y 3 del OSI), a nivel de transporte Internet (TCP, UDP), etc.

Una vez introducidos los conceptos básicos de seguridad se ha descrito cómo conseguir un servicio de correo electrónico seguro utilizando el PEM, que es el método utilizado en el proyecto piloto P8 de COSINE descrito posteriormente y en el cual estamos participando activamente.

Por último se propone una aplicación práctica del P8 a nuestra comunidad académica, de forma que los usuarios de nuestro país puedan disfrutar también de la confidencialidad y otros servicios de seguridad, de la misma forma que utilizan el correo. ¿A quién no le gustaría estar seguro de que sus mensajes no serán leídos más que por sus destinatarios, o que llegarán hasta estos íntegros, etc.?.

Referencias

[1] CCITT Blue Book Fascicle VIII 8, Recommendations X.500 - X.509 (Authentication Framework).

[2] ISO 7498-2, OSI/RM, Security Architecture.

[3] ECMA TR/46 Security in Open Systems - A Security Framework Definitions.

[4] IS 9594, Information Processing System - Open System Interconnection - The Directory, ISO, 1988.

[5] Security and Authentication for COSINE, COSINE Specification phase (V5), RARE ,1988.

[6] S.Kent and J.Linn, Privacy Enhancement for Internet Electronic Mail, Internet RFCs 1113-1115, 1992.

[7] ANSI X3.92, Data Encryption Algorithm.

[8] R.L.Rivest, A.Shamir and L.Adleman, A method for obtaining digital signature and public key cryptosystems, Comm. ACM 21, 1978.

[9] R.L.Rivest, The MD5 Message Digest Algorithms, Internet Draft, 1992.

[10] M.Purser, Development and Proving of Security mechanisms - COSINE Sub-Project P8.

[11] R.Grimm et al., SECUDE, Principals of Security Operations (V1), GMD, Darmstadt, 1991.

Francisco Jordán, Manel Medina y Enric Peig
Universidad Politécnica de Cataluña
Departamento de Arquitectura de Computadores
jordan@ac.upc.es
medina@ac.upc.es
enricp@ac.upc.es

CONVOCATORIAS

4ª Conferencia Conjunta europea sobre redes: "Redes de investigación europeas en un contexto global."

◆ 4th JENC

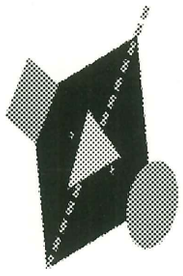
Trondheim-Noruega
10-13 mayo 1993

Organizada por RARE (Réseaux Associés pour la Recherche Européenne) en colaboración con:

EARN, Internet Society, IFIP TGC, NORDUnet, Internet Architecture Board y UNINETT.

El tema de la Conferencia - Redes de investigación europeas en un contexto global- admite el hecho de que las redes que cubren un área geográfica específica o sirven a un grupo de usuarios determinado sólo tendrán éxito si se conectan al resto del mundo. La conectividad global para un gran número de usuarios y aplicaciones aumenta el interés por la utilización de las redes. Hoy en día en Europa sólo un pequeño porcentaje de todo el personal académico e investigador son usuarios de redes; hay aún un largo camino por recorrer. En esta conferencia se pretende explorar los próximos pasos a seguir.

La conferencia va dirigida a los proveedores de servicios de redes, sea cual sea su tamaño, así como a las personas que desarrollan aplicaciones, representantes de los organismos de financiación, gestores, grupos de usuarios avanzados y organizaciones de estándares. Se hará mucho hincapié, una vez más, en la cooperación entre miembros de diferentes comunidades de redes, continuando con las experiencias positivas obtenidas en anteriores conferencias.



4th JENC

Esta conferencia constituye EL foro de las redes de investigación en Europa y ofrece una oportunidad única para el encuentro de las personas clave en este campo hoy en día.

A la vista del éxito de las conferencias anteriores se mantiene el mismo formato de la misma, excepto la inclusión de tutorías. La conferencia comienza el lunes 10 de mayo de 1993 a las 14:00 y durará hasta el jueves 13 a las 12:30. No habrá sesiones programadas para el miércoles por la mañana, con el fin de permitir a los participantes que organicen BoFs. De cualquier forma y como ocurre normalmente se organizarán reuniones internacionales en torno a la conferencia.

Para mayor información dirigirse a:

Secretaría de RARE
Singel 466-468
NL - 1017 AW Amsterdam

Tel.: +31 20 639 1131
Fax: +31 20 639 3289
EMail: raresec@rare.nl
C=nl; ADMD=400net;
PRMD=surf; O=rare;
S=raresec

Fundesco