Reenvío anónimo de correo con Mixmaster

MENSAJES DESDE NINGÚN SITIO

El correo anónimo protege la identidad de los remitentes de las posibles escuchas en la red. El protocolo Mixmaster ofrece a los usuarios una tecnología madura para el envío anónimo y el cliente Mixmaster basado en texto es un ejemplo de una aplicación libre para el envío anónimo. **POR JENS KUBIEZIEL**

Cuando Johan Helsingius comenzó un servicio para el envío anónimo de correo electrónico en 1993, no podía prever en que clase de problema se estaba metiendo. Johan es ahora famoso por su trabajo pionero, a pesar de las reacciones hostiles, o precisamente debido a ellas.

Al comienzo de los 90, las listas de correo y los grupos de discusión de USENET habían dejado la fase en la cual principalmente se concentraban en temas científicos y relacionados con la informática. En USENET también se dieron numerosas discusiones políticas y religiosas muy polémicas. Como estas discusiones eran de interés para los servicios secretos y de los jefes, los usuarios buscaban una manera de expresarse anónimamente. Johan Helsingius desarrolló un software para despersonalizar mensajes de correo electrónico y lo instaló en su servidor.

Pronto se conoció la dirección de este servidor (*http://anon.penet.fi/*) y todavía se habla de él con reverencia. Para utilizar el servicio, los usuarios tenían que enviar un mensaje de correo electrónico con una entrada especial en la cabecera para la dirección. El servidor sustituía la dirección del remitente por una dirección con el formato [anXXXX@anon.penet.fi] (donde XXXX era una combinación de números) y remitía el correo electrónico a la dirección especificada en la línea adicional de la cabecera.

El servicio era fácil de utilizar y atrajo a muchos usuarios. Antes de 1996, el programa manejaba alrededor 10.000 mensajes al día. Éste era el año que el movimiento de la Cienciología demandó al operador, exigiendo la publicación de las direcciones de correo electrónico. Una corte finlandesa decidió que los mensajes de correo electrónico no estaban amparados por la ley de secretos del correo postal facilitando así la escucha secreta y la identificación de los usuarios. Esto, a su vez, impulsó a Helsingius, a desconectar el servidor [1].

Cypherpunk y Mixmaster

Para cuando Johan Helsingius apago su servidor de correo anónimo, el desarrollo progresaba a la velocidad del rayo. Los Cypherpunks, grupo que se centró en la protección de la privacidad y el uso del cifrado, desarrollaron un cierto número de modelos de servidores anónimos (*remailers*) que no dependían de un servidor central. Su trabajo estaba basado en un artículo publicado en 1981 por David Chaum [2], describiendo redes mezcladoras que habían sido implementadas con la idea de proteger el anonimato de las partes durante el intercambio del correo electrónico.

El principio es comparable a enviar una carta en varios sobres. Si Ralf Penn quería enviar una carta anónima, inicial-

mente dirigía la carta al destinatario, pero en vez de enviar la carta directamente, agrega un número de estaciones intermedias. Pone la carta en otro sobre y escribe la dirección de una de estas estaciones en el sobre. La carta consigue un sobre nuevo para cada uno de estas estaciones.

Entonces se envía la carta a la primera dirección intermedia, donde se abre el sobre externo. Se destruye el sobre y la carta se envía a la siguiente dirección del siguiente sobre hasta que, finalmente, la estación intermedia envía la carta al destinatario real. El destinatario solamente puede rastrear la carta hasta la ultima estación intermedia, ya que se han destruido el resto de los sobres. Con este proceso se garantiza el anonimato del remitente.

Primera Generación de Servidores Anónimos

El primer modelo de servidor anónimo que se basó en este principio fue Cypherpunk Remailer, también conocido como *remailer Tipo I*. Al diferencia del modelo de Helsingius, se involucran un cierto número de servidores, que trabajan independientemente unos de otros. Si un servidor no es accesible, los usuario pueden recurrir a cualquier otro. Como los servidores están situados en países distintos, con diferentes sistemas legales, los agresores lo tendrán difícil para intentar lo que sea contra este tipo de servidores.

Según se ha descrito anteriormente, se utilizan técnicas criptográficas para envolver el mensaje. Este proceso implica que el remitente cifre el mensaje con la llave pública de cada servidor anónimo de la cadena. Los usuarios pueden solicitar la llave vía correo electrónico (Listado 1) o vía el sitio web del servidor. Cada servidor anónimo en la cadena solamente puede descifrar la parte del mensaje previsto para su uso. La parte descifrada contiene la dirección a la cual el servidor tiene que remitir el mensaje.

La organización del servidor anónimo elimina algunas de las debilidades del servicio de Helsingius, pero todavía quedan algunos problemas. Por ejemplo, cada servidor anónimo remite los correos electrónicos tan pronto como llegan. Esto permite que un atacante deduzca relaciones entre los mensajes entrantes y salientes y de esta manera sacar conclusiones sobre la identidad del remitente y el destinatario. Un atacante también podía interceptar un mensaje y reinsertarlo reiteradamente en la cadena de servidores anónimos.

Debido a que cada mensaje se maneja exactamente de la misma manera, toma exactamente la misma ruta. Esta debilidad fue identificada por Lance Cottrell en 1.995 en "Mixmaster & Remailer Attacks" [3]; también propuso algunos cambios, los cuales condujeron a *remailer Tipo II*, el Mixmaster.

Como Funciona Mixmaster

Mixmaster no remite inmediatamente los mensajes entrantes. En vez de eso, espera hasta que se han agregado bastantes mensajes a la cola. Cuando el destinatario de mensajes está lleno, el servidor envía los mensajes a la siguiente estación en la cadena en un orden aleatorio. Para que sea imposible que un potencial investigador identifique los mensajes por

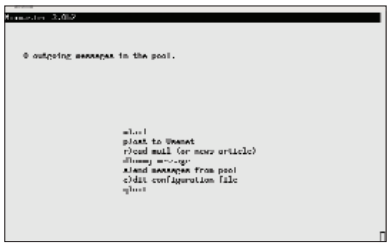

Figura 1: Pantalla de inicio del cliente Mixmaster.

su tamaño, el servidor anónimo también hace que todos los mensajes tengan un tamaño uniforme. Si un mensaje es demasiado pequeño, Mixmaster agrega caracteres de relleno al azar; si un mensaje es demasiado grande, Mixmaster divide el mensaje en bloques del mismo tamaño. Esta técnica hace imposible que los atacantes asocien los paquetes entrantes con los paquetes salientes.

Además, a cada paquete del mensaje se le asigna un ID. Mixmaster comprueba si el ID del paquete ya se ha registra-

Cuadro 1: Correo en Servidores Anónimos Cypherpunk

1. Se compone un mensaje y se añade la cabecera. El mensaje se direcciona al primer destinatario. Se insertan dos lineas al comienzo del mensaje:

```
::
Anon-To: john.smith@example.org
```

Estas lineas proporcionan al ultimo servidor anónimo la información que necesita para enviar el mensaje a su destinatario final.

2. Se cifra el mensaje y se añade la cabecera cifrada. Ahora se cifra el mensaje con la clave pública del servidor anónimo. Se inserta otra linea delante del texto cifrado: *Encrypted: PGP*. Esta linea indica al servidor anónimo que debe descifrar las siguientes lineas.

```
01 ::
02 Encypted: PGP
03 03
04 -----BEGIN PGP MESSAGE-----
05 Version: GnuPG v1.2.5
   (GNU/Linux)
06 06
07
   hQEOA1gu3H8UQS6IEAP/UgB5ZbyRS5
   Kkmi/mD4Vi4PHBg6XOOoS8BL/t6HGa
   CkMc
08
   BHAB4YCnQGzlIEzxhrMnYxeFlOCa9B
   fsGTel1DjnHeLWypdW4XuPNnCiNA8f
   wdnu
09
   C58rmBo2B8XTjcc1eGjD+SayRn/F3e
   Gc3rdGw3EkwWpRxwgcXU/SvHwE6vnO
   nTwE
10
   +9fWwweS+WUFRCBNPqaUZkXqZ6jBpV
   e5fRAUZDRhqOhUcEAOnvRHn9D7QMJu
   qV9R
11
   7CPEAb/+Dd2+hxqqezeXpTHOqJKiUi
   E8SqGnBBAw5uOpMffuGG12ObLPEDfu
   M7yF
12
   xaXWu6TQ94GTV/+2Inw9LufUPNsaTf
   rWWRxFNphWvTh9a+MRIIKb7abSCee4
   qcwP
13 vjJsDM2f
14 =7HnR
15 -----END PGP MESSAGE-----
```

3. Se repiten estos pasos por cada uno de los servidores anónimos. Si el usuario quiere añadir otro servidor anónimo, se añade una nueva linea *Anon-To:* en el comienzo del mensaje. Después se repite el paso número 2. Este paso se repetirá para cada uno de los servidores de la cadena.

4. Enviar el mensaje. El mensaje se envía al primer servidor anónimo de la cadena, el cual reenviará la información indicada más arriba.

do y si es así, descarta el mensaje. Al descartar los mensajes con paquetes registrados se protege al servidor contra los ataques por reinserción. Estos pasos eliminan algunas de las debilidades del servidor anónimo de Cypherpunk. Además, los servidores anónimos de Mixmaster utilizan el cifrado simétrico, que acelera los proceso con los mensajes. De hecho, Mixmaster tiene un montón de ventajas sobre el servidor anónimo de Cypherpunk.

Aunque una descripción detallada de cómo funciona todo esto está lejos del alcance de este artículo, los lectores que lo deseen pueden comprobar el borrador del RFC para conocer el protocolo de Mixmaster [4].

Listado 1: Recuperación de claves de un Servidor Anónimo

```
01 From: Jens Kubieziel
   <jens@example.org>
02 To: Dizum Remailer
   <remailer@dizum.com>
03 Subject: remailer-key
Respuesta de Remailes:
01 From: Nomen Nescio
   <remailer@dizum.com>
02 To: "Jens Kubieziel"
   <jens@example.org>
03 Subject: Remailer key for
   dizum
04
05 $remailer{"dizum"} =
   "<remailer@dizum.com> cpunk
   mix pgp pgponly repgp remix
   latent hash cut test ek ekx
   esub inflt50 rhop20 reord post
   klen64";
06
07 Here is the PGP key:
08
09 Type Bits/KeyID Date User ID
10 pub 1024R/31234B37 2000-04-24
   Nomen Nescio
11 <remailer@dizum.com>
12
13 -----BEGIN PGP PUBLIC KEY
   BLOCK-----
14 Version: Mixmaster 2.9.0
   (OpenPGP module)
15
16
   mQCNAzkEMTMAAAEEAOa7vR4GZCRUuk
   aoBqlGZbru6c6UlAgLOs8Od2I+UF1K
   TY5Z
17
   XKClKK5UblHDiFgzJk+ONxVR3ePgJ5
   6MJeK2iGPVZ/i8thC1gR6btrrSONzf
   K7rr
18
   bW2aKlDfihyjz6emPYkHqPjOhAwxGQ
   iTMkEPF5jmEdWeZN4kph8q6DIxIOs3
   AAID
19
   tCFOb21lbiBOZXNjaW8gPHJlbWFpbG
   VyQGRpenVtLmNvbT6JAJUDBRA5BDEz
   Hyro
20
   MjEjSzcBAWqABAC+6voEDspSDQUnOR
   mLjy1zPsysx7Zdc7J/c4Ol6rGS9n1t
   ZQiw
21
   CTpILinXiCLP3I9Pu9T4kl1gHVYyIu
   2pqeNOJLOWz1w6HkwQjGsGdxtFDyFC
   mfxe
22
   cOhtDM5WQn1DqtIaG98mNcStkY2B5e
   7VNP2aVd66oTeDPLYD4VCsrITODw==
23 =RJCD
24 -----END PGP PUBLIC KEY
   BLOCK-----
25
26 Type Bits/KeyID Date User ID
27 pub 1024D/B1685FE7 2000-04-24
   Nomen
   Nescio<remailer@dizum.com>
28 sub 1024g/B2547D80 2000-04-24
29
30 -----BEGIN PGP PUBLIC KEY
   BLOCK-----
31 Version: Mixmaster 2.9.0
   (OpenPGP module)
32
33
   mQGiBDkEMTMRBADqwatBmgC/yuOlyq
   rzFL1toAzDrSiHO6eZlo8eCRj+Uqw6
   lSuO
34
   RxxhSZaBUIsuqogRHFiuxU+RqUia24
   1vEjSNOx7ZV+LipTZc282VbOPuDv7f
   L2Ll
35
   Ez8QEJMz+zpMjICRFVNgHGRvhHUGu1
   8i9BTmzigpyuMpMwwlB2HvTBO4CQCg
   wNPp
36
   B/I45a4PZ2+zmZyVQUuAh+UD/je6Od
   uoTwwq6176bUfcvCtVH9DP4DwoCgrV
   wd3c
37
   r9KoR9hO7TAGL5Ah7eJ1GvndRH7KPB
   fuE6h/kMCohNgKGluPn4je6vJ6NOJ/
   O3av
38
   +jJ1mHN2TImOpO+VFXFPm1A7zqA/MW
   gOG7DWggfmguZ9E6TuAbfOIvy/Ksqn
   jt7O
39
   JyelA/9YyKH56juAGYHdHbPQR/NAED
   3XLUuc8UzXNuL5VNAD4OSfbxVpNwJJ
   PYM3
40
   fA2RYOIbsMefKvotlXRkKZHzFbjOKc
   nkvFOdOWhXzCgTEdwYwhaQQJzWznvu
   Vzqm
41
   18GZoomfsbsgfYHwfDOCCTSqVj3GlM
   TXHO6ol7QOw69HGlNZYrQhTm9tZW4g
   TmVz
42
   Y2lvIDxyZW1haWxlckBkaXp1bS5jb2
   O+iQBNBBARAgANBQI5BDEzAwsDAgIe
   AQAK
43
   CRBos3tosWhf52NaAKCjS4nyqFvmq8
   5a5HwGPHhTBhGPJwCdHrYGFeIVOh8O
   JJUR
44
   vQiaIRNRG/W5AQOEOQQxMxAEAL5wXB
   X5gxZE4MDaUDE9TWRwo6VnE6dUvu6I
   a45O
45
   hyAVDp5AoquHpJv7PvhA/nLiDFJspm
   2eDdLglaUGcDIt6MJEbXV/I9v/qQ7q
   njh/
46
   Cm84gsss+uKTWZjga2NRZ/Y4JGePIm
   LWBlmapwPoHBhJEXsdp1zl/ODiDGmH
   dV12
47
   xPHfAAMFBACB12J/HSJznAwpGsIBO3
   NrBz2Iw7NqrhepSfcExGiWrGMJnAjA
   d98I
48
   C84j5AYwMhGWMPmzcNqdcqWEI9Z2cW
   dOnXndt8GJAUCpfEb5T2snTnoqaiIB
   4nYq
49
   vyG1HwBM7OMXw9k13smo+5PgE3EHyQ
   2pvIuAMoOZz6o/zq6dOxH6XokAPwMF
   GDkE
50
   MTNos3tosWhf5xECVYOAoJcXnCHayC
   kFAE17SXU33cc3R1qnAKCpVZkKbuQS
   phYg
51 M4wRXciYWpAoyw==
52 =Vkzl
53 -----END PGP PUBLIC KEY
   BLOCK-----
```

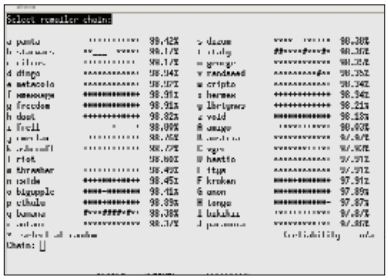

Figura 2: El cliente Mixmaster muestra un resumen de servidores anónimos disponibles.

Operaciones Diarias

Mixmaster también es el nombre de un paquete software que ha sido desarrollado por programadores voluntarios como un proyecto de fuente abierta. El desarrollo está hospedado en Sourceforge [5]. Los usuarios pueden descargar el código fuente desde Sourceforge y construir el programa desde las fuentes. Además Debian ha precompilado los binarios del cliente Mixmaster para sus usuarios [6].

Después de instalar el software, los usuarios deben descargar las claves públicas y las estadísticas de disponibilidad para los servidores anónimos. Muchos operadores de un servidor anónimo publican estos datos en sus sitios web [7]. El paquete Mixmaster de Debian incluye un guión de Perl llamado *mixmaster-update*. El guión descarga automáticamente los archivos necesarios y está diseñado para trabajar como una tarea *cron* o como parte de del guión *IP-up*. Después de descargar los archivos y de almacenarlos en */var/lib/mixmaster/stats/*, ya puede teclear *mixmaster* y arrancar el programa (véase el Cuadro 1).

Dentro del programa, los usuarios pueden componer, leer, y enviar mensajes. Por ejemplo, si se necesita enviar un mensaje de correo electrónico, se le pide al usuario que rellene los campos remitente y asunto del mensaje cuando se pulsa la tecla [M]. Pulsar [E] en el menú de enviar permite componer el mensaje. Se vuelve al menú tras terminar el mensaje. Por omisión, el programa selecciona automáticamente una cadena de cuatro servidores anónimos, aunque los usuarios pueden teclear [C] para definir una cadena de servidores anónimos (Cuadro 2).

El Cuadro 2 muestra servidores anónimos y sus valores de fiabilidad. Esta estadística es solamente una instantánea y se puede esperar una cierta desviación, así que estos valores se deben utilizar solamente como un indicador aproximado. Después de seleccionar una cadena, se puede enviar el mensaje o el conjunto de mensajes presionando [M] y después pasar a componer otro mensaje si fuese necesario. Cuando se han acumulado bastantes mensajes, o si un usuario emite un comando a tal efecto, el programa envía los mensajes a las otras estaciones en la cadena.

En definitiva, Mixmaster es muy fácil de usar y tiene un interfaz de usuario auto-explicativo. Los recién llegados no deben tener ningún problema para conseguir acostumbrarse a usar el software y a enviar mensajes anónimos siempre que necesiten hacerlo.

Pros y Contras del Correo Anónimo

En una sociedad plural, la comunicación anónima tiene connotaciones sórdidas. La gente tiende a pensar en acusaciones, amenazas de bombas, correo basura o documentos ilegales. Sin embargo, los servidores de correo anónimos solamente cumplen con un requisito para la seguridad de la infraestructura de TI, que es, la que oculta el hecho de que la comunicación está teniendo lugar. Hay muchas razones legitimas para querer ocultar la comunicación a la opinión pública. Por ejemplo, un repentino incremento del volumen de correo electrónico entre dos compañías puede dar pistas sobre que las compañías estén considerando una posible asociación, aunque el contenido de los mensajes esté cifrado. Miembros de grupos radicales, defensores de reformas en países autoritarios o personas con enfermedades graves estigmatizadas por la sociedad, también desearán proteger su anonimato.

Por otra parte, no hay que negar el potencial que tiene el envío de correo anónimo para hacer cosas inadecuadas. Los grupos de presión y las autoridades de correo electrónico se apresuran a precisar el posible abuso y la controversia resultante ha provocado llamamientos para prohibir los servicios de anonimato. Johan Helsingius, el hombre detrás del remailer, afirma que nunca ha utilizado el servicio que inventó. Sin embargo, para él era importante desarrollar una tecnología que diera soporte al anonimato y que permitiera a los usuarios ejercitar su derecho a la libertad de opinión. Y este acceso al correo electrónico anónimo aun está disponible en los servidores anónimos alrededor del mundo. ■

RECURSOS

[1] Nota de prensa sobre el cierre de anon.penet.fi: *http://www.fitug.de/news/1997/penet.html*

[2] David L. Chaum, "Untraceable Electronic Mail, Return addresses and Digital Pseudonyms": *http://world.std.com/~franl/crypto/chaum-acm-1981.html*

[3] Lance Cottrell, "Mixmaster & Remailer Attacks": *http://riot.eu.org/anon/doc/remailer-essay.html*

[4] Borrador del RFC para el protocolo de Mixmaster, Version 2: *http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt*

[5] Página principal del proyecto Mixmaster: *http://mixmaster.sourceforge.net*

[6] Información en el paquete Debian Mixmaster: *http://packages.qa.debian.org/m/mixmaster.html*

[7] Estadísticas para el servidor anónimo Noreply.org: *http://www.noreply.org/echolot/*