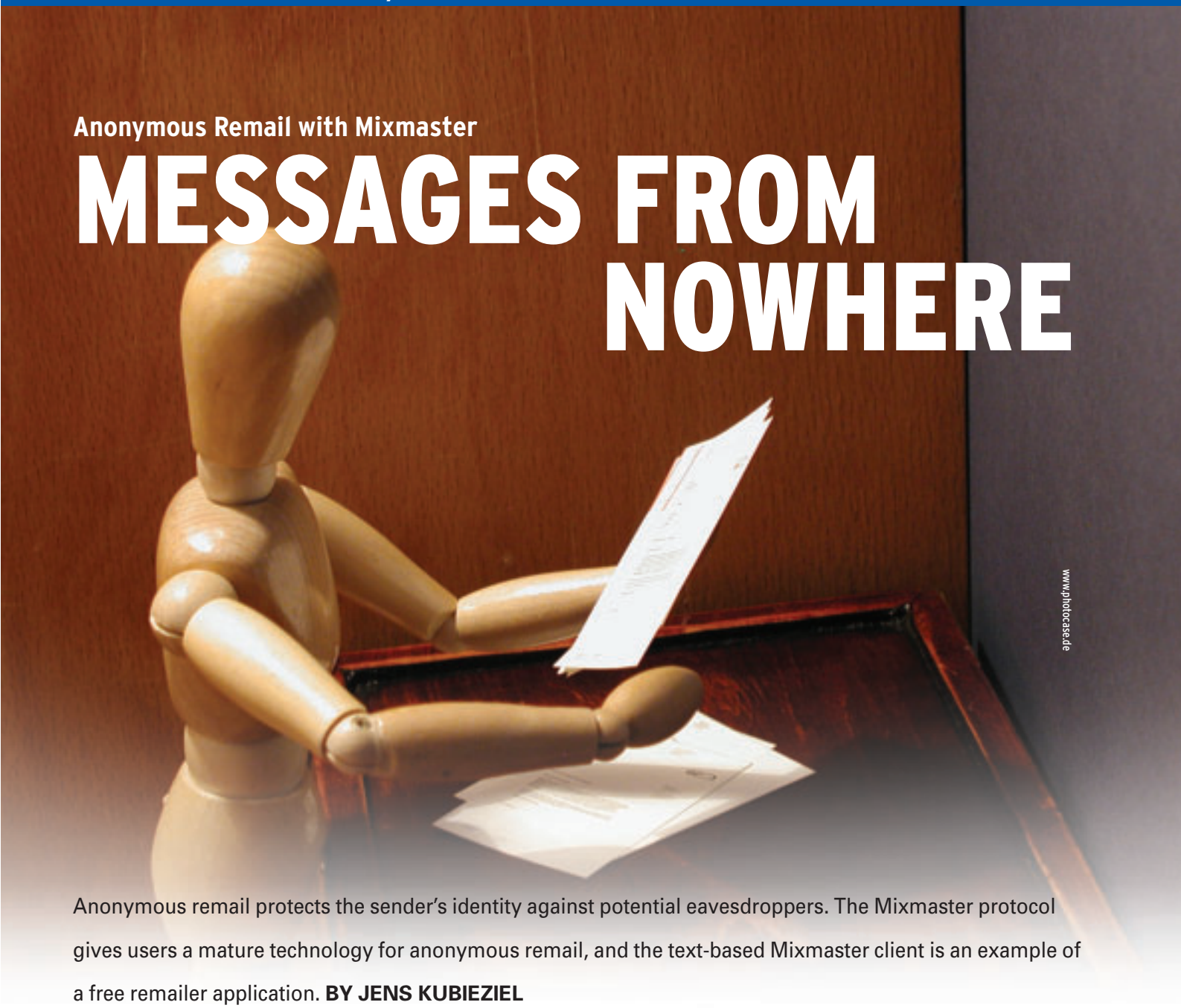

Anonymous Remail with Mixmaster

MESSAGES FROM NOWHERE

Anonymous remail protects the sender's identity against potential eavesdroppers. The Mixmaster protocol gives users a mature technology for anonymous remail, and the text-based Mixmaster client is an example of a free remailer application. **BY JENS KUBIEZIEL**

When Johan Helsingius started up an anonymization service for email back in 1993, he could hardly have anticipated the kind of trouble he would be in for. Despite, or maybe because of, the hostile reactions, Johan is now renowned for his pioneering work.

In the early 90s, mailing lists and USENET discussion groups had left the phase in which they mainly concentrated on scientific and computer-related subjects. USENET also supported a number of highly controversial political and religious discussions. Because these discussions were of interest to secret services and employers, users were looking for a way of expressing themselves anonymously. Johan Helsingius developed software for depersonalizing email messages and installed the software on his server.

The address of this server *anon.penet.fi* soon became known, and it is still spoken of with awe today. To use the service, users had to send an email message with a special entry in the header to the address. The server replaced the sender address with an address in the form of [anXXXX@anon.penet.fi] (where XXXX is a combination of numbers) and forwarded the email to the address specified in the additional header line.

The service was easy to use, and that attracted many users. By 1996, the software was handling around 10,000 messages a day. This was the year that the Scientology movement sued the operator, demanding the release of email addresses. A Finnish court decided email messages were not covered by the mail secrecy act and thus facilitated eavesdropping and the identification of the users. This, in turn, prompted Helsingius, to switch off the server [1].

Cypherpunk and Mixmaster

By the time Johan Helsingius switched off his anonymous mail server, development was progressing at lightning speed. The Cypherpunks, a group that focused on protecting privacy and the use of cryptography, developed a number of remailer models that did not rely on a central server. Their work was based on a paper published back in 1981 by David Chaum [2], describing mix networks that had been implemented with the idea of protecting the anonymity of the parties in email exchanges.

The principle is comparable with sending a letter in a number of envelopes. If Ralf Penn wants to send an anonymous letter, he originally addresses the letter to the recipient, but instead of sending the letter directly, he then adds a number of intermediate stations. He puts the letter in another envelope and writes the address of one of these stations on the envelope. The letter gets a new envelope for each of these stations.

The letter is then sent to the first intermediate address, where the external envelope is opened. The envelope is destroyed and the letter is sent to the address on the next envelope until, finally, the last intermediate station sends the letter to the actual recipient. The recipient can only trace the letter back to the last intermediate station, as all the other envelopes have been destroyed. This process guarantees the anonymity of the sender.

Figure 1: Mixmaster client start up screen.

First Generation Remailers

The first remailer model to be based on this principle was the Cypherpunk Remailer, also known as the Type I remailer. In contrast to Helsingius' model, there are a number of servers involved, all of which operate independently of one another. If one server is not accessible, users can fall back on one of the others. As the servers are located in different countries, with different legal systems, attackers would find it difficult to do anything about this kind of remailer.

Cryptographic techniques are used to wrap the message, as described earlier. This process involves the sender encrypting the message with the public key of each remailer in the chain. Users can request the key via email (Listing 1) or via the website of the server.

Each remailer in the chain can only decrypt the part of the message intended for its use. The decrypted part contains the address to which the server has to forward the message.

The remailer setup removes some of the weaknesses of Helsingius' service, but it still leaves a few problems. For example, each remailer forwards emails as soon as they arrive. This allows an attacker to deduce relationships between incoming and outgoing messages, and thus to draw conclusions about the identity of the sender and recipient. Also, an attacker could intercept a message and repeatedly reinsert it into the remailer chain.

Because each message is handled in exactly the same way, it takes exactly the same route. These were the weaknesses that Lance Cottrell identified in 1995 in "Mixmaster & Remailer Attacks" [3]; he also proposed a few changes, which led to the Type II Remailer, the Mixmaster.

How Mixmaster Works

Mixmaster does not forward incoming messages immediately. Instead Mixmaster waits until enough messages have been added to the queue. When the message pool is full, the server sends the messages to the next station in the chain in random order. To make it impossible for a potential investigator to identify messages by their size, the remailer also makes all messages a uniform size. If a message is too small, Mixmaster adds random fill characters; if a message is too big, Mixmaster splits that message into blocks of the same size. This technique makes it impossible for attackers to associate incoming packets with outgoing packets.

Also, each message packet is assigned a packet ID. Mixmaster checks if the ID is already registered, and drops the message if it is. Dropping registered message packets protects the server against reinsertion attacks. These steps remove some of the weaknesses of the Cypherpunk remailer. Additionally, Mixmaster remailers use symmetric encryption, which accelerates message processing.

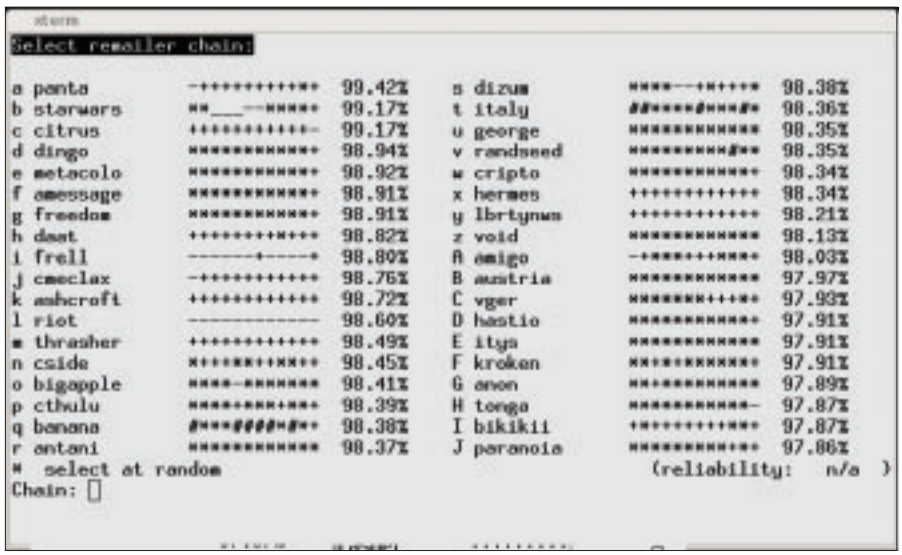

Figure 2: The Mixmaster client displaying an overview of available remailers.

In fact, the Mixmaster has a lot of advantages over the Cypherpunk remailer.

A detailed description of the way this works is far beyond the scope of this article. Readers might like to check out the RFC draft for the Mixmaster protocol [4].

Daily Operations

Mixmaster is also the name of a client software package that was developed by volunteer programmers as an open source project. Development work is hosted by Sourceforge [5]. Users can download the program sources from Sourceforge and build the program from the sources. Debian also has precom-

Listing 1: Retrieving a Remailer Key

```
01 From: Jens Kubieziel <jens@example.org>
02 To: Dizum Remailer <remailer@dizum.com>
03 Subject: remailer-key

Remailer Response:
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
   <remailer@dizum.com>
11
12 -----BEGIN PGP PUBLIC KEY BLOCK-----
13 Version: Mixmaster 2.9.0 (OpenPGP module)
14
15 mQCNAzkEMTMAAAEEAOa7vR4GZCRUukaoBqlGZbru6c6UlA
   gLOs8Od2I+UF1KTY5Z
16 XKClKK5UblHDiFgzJk+ONxVR3ePgJ56MJeK2iGPVZ/i8th
   C1gR6btrrSONzfK7rr
17 bW2aKlDfihyjz6emPYkHqPjOhAwxGQiTMkEPF5jmEdWeZ
   N4kph8q6DIxIOs3AAID
18 tCFOb21lbiBOZXNjaW8gPHJlbWFpbGVyQGRpenVtLmNvbT
   6JAJUDBRA5BDEzHyro
19 MjEjSzcBAWqABAC+6voEDspSDQUnORmLjy1zPsysx7Zdc7J
   /c4Ol6rGS9n1tZQiw
20 CTpILinXiCLP3I9Pu9T4kl1gHVYyIu2pqeNOJLOWz1w6Hk
   wQjGsGdxtFDyFCmfxe
21 cOhtDM5WQn1DqtIaG98mNcStkY2B5e7VNP2aVd66oTeDP
   LYD4VCsrITODw==
22 =RJCD
23 -----END PGP PUBLIC KEY BLOCK-----
24
25 Type Bits/KeyID    Date       User ID
26 pub  1024D/B1685FE7 2000-04-24 Nomen Nescio
   <remailer@dizum.com>
27 sub  1024g/B2547D80 2000-04-24
28
29 -----BEGIN PGP PUBLIC KEY BLOCK-----
30 Version: Mixmaster 2.9.0 (OpenPGP module)
31
32 mQGiBDkEMTMRBADqwatBmgC/yuOlyqrzFL1toAzDrSiHO6
   eZlo8eCRj+Uqw6lSuO
33 RxxhSZaBUIsuqogRHFiuxU+RqUia241vEjSNOx7ZV+LipT
   Zc282VbOPuDv7fL2Ll
34 Ez8QEJMz+zpMjICRFVNgHGRvhHUGu18i9BTmzigpyuMpM
   wwlB2HvTBO4CQCgwNPp
35 B/I45a4PZ2+zmZyVQUuAh+UD/je6OduoTwwq6176bUfcv
   CtVH9DP4DwoCgrVwd3c
36 r9KoR9hO7TAGL5Ah7eJ1GvndRH7KPBfuE6h/kMCohNgKGl
   uPn4je6vJ6NOJ/O3av
37 +jJ1mHN2TImOpO+VFXFPm1A7zqA/MWgOG7DWggfmguZ9E6
   TuAbfOIvy/Ksqnjt7O
38 JyelA/9YyKH56juAGYHdHbPQR/NAED3XLUuc8UzXNuL5VN
   AD4OSfbxVpNwJJPYM3
39 fA2RYOIbsMefKvotlXRkKZHzFbjOKcnkvFOdOWhXzCgTEd
   wYwhaQQJzWznvuVzqm
40 18GZoomfsbsgfYHwfDOCCTSqVj3GlMTXHO6ol7QOw69HGl
   NZYrQhTm9tZW4gTmVz
41 Y2lvIDxyZW1haWxlckBkaXp1bS5jb20+iQBNBBARAgANBQ
   I5BDEzAwsDAgIeAQAK
42 CRBos3tosWhf52NaAKCjS4nyqFvmq85a5HwGPHhTBhGPJw
   CdHrYGFeIVOh8OJJUR
43 vQiaIRNRG/W5AQOEOQQxMxAEAL5wXBX5gxZE4MDaUDE9TWR
   wo6VnE6dUvu6Ia45O
44 hyAVDp5AoquHpJv7PvhA/nLiDFJspm2eDdLglaUGcDIt6MJ
   EbXV/I9v/qQ7qnjh/
45 Cm84gsss+uKTWZjga2NRZ/Y4JGePImLWBlmapwPoHBhJEXs
   dp1zl/ODiDGmHdV12
46 xPHfAAMFBACB12J/HSJznAwpGsIBO3NrBz2Iw7NqrhepSfc
   ExGiWrGMJnAjAd98I
47 C84j5AYwMhGWMPmzcNqdcqWEI9Z2cWdOnXndt8GJAUCpfEb
   5T2snTnoqaiIB4nYq
48 vyG1HwBM7OMXw9k13smo+5PgE3EHyQ2pvIuAMoOZz6o/zq6
   dOxH6XokAPwMFGDkE
49 MTNos3tosWhf5xECVYOAoJcXnCHayCkFAE17SXU33cc3R1q
   nAKCpVZkKbuQSphYg
50 M4wRXciYWpAoyw==
51 =Vkzl
52 -----END PGP PUBLIC KEY BLOCK-----
```

piled binaries of the Mixmaster client for its users [6].

After installing the software, users should download the public keys and availability statistics for the remailers. Many remailer operators publish this data on their websites [7]. The Debian Mixmaster package includes a Perl script called *mixmaster-update*. The script automatically downloads the required files and is designed to run as a cron job or *ip-up* script. After downloading the files and storing them in */var/lib/mixmaster/stats/*, you can go on to type *mixmaster* and launch the program (see Figure 1).

Within the program, users can compose, read, and send messages. For example, if you need to send an email message, you are prompted to enter the recipient and subject line of the message when you press the [M] key. Pressing [E] in the send menu allows you to compose the message; you are returned to the menu after completing the message. By default, the program automatically selects a chain of four remailers, although users can type [C] to define a chain of remailers themselves (Figure 2).

Figure 2 shows remailers and their reliability values. These statistics are only snapshots, and some variation is expected, so use these values as a rough guide only. After selecting a chain, you can send the message to the message pool by pressing [M] and then go on to compose another message if needed. When enough messages have accumulated, or if a user issues a command to this effect, the program sends the messages to the other stations in the chain.

All in all, Mixmaster is very easy to use and has a self-explanatory user interface. Newcomers should have no problem getting accustomed to using the software and sending anonymous messages whenever they need to do so.

Pros and Cons of Anonymous Mail

In a pluralistic society, anonymous communication often has seedy connotations. People tend to think of denunciations, bomb threats, spamming, or illegal material. However, anonymous remailers simply comply with a requirement for a safe IT infrastructure; that is, they hide the fact that communication is taking place. There are many legitimate reasons for wanting to hide communications from public view. For example, a sudden increase in the volume of email between two companies may give listeners a clue that the companies are considering a partnership, even though the content of the messages might be encrypted. Members of radical groups, reform advocates in authoritarian countries, or people with serious, socially stigmatized illnesses also may wish to protect their anonymity.

On the other hand, there is no denying the potential for misusing the anonymous remailer. Lobbyists and email authorities are quick to point out the potential for abuse, and the resulting contraversy has provoked calls to ban anonymity services. Johan Helsingius, the man behind the remailer, claims never to have used the service he invented. It was, however, important for him to develop the technology to support anonymity, which allows users to exercise their right to freedom of speech. And this access to anonymous email is still available to remailers around the world today. ■

Box 1: Email Delivery via Cypherpunk Remailers

1. Compose message and add a header. The message is addressed to the recipient first. Two lines are inserted at the start of the message:

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

These lines give the last remailer the information it needs to send the message to its final destination.

2. Encrypt message and add the encrypted header. The message is now encrypted with the remailer's public key. Another line is inserted in front of the cipher text: *Encrypted: PGP*. This line tells the remailer that any following lines need to be decrypted.

```
01 ::
02 Encypted: PGP
03
04 -----BEGIN PGP MESSAGE-----
05 Version: GnuPG v1.2.5
   (GNU/Linux)
06
07 hQEOA1gu3H8UQS6IEAP/UgB5ZbyRS5
   Kkmi/mD4Vi4PHBg6XOOoS8BL/t6HGa
   CkMc
08 BHAB4YCnQGz1IEzxhrMnYxeFlOC
   a9BfsGTel1DjnHeLWypdW4XuPNn
   CiNA8fwdnu
09 C58rmBo2B8XTjcc1eGjD+SayRn/
   F3eGc3rdGw3EkwWpRxwgcXU/Sv
   HwE6vnOnTwE
10 +9fWwweS+WUFRCBNPqaUZkXqZ6j
   BpVe5fRAUZDRhqOhUcEAOnvRHn9
   D7QMJuqV9R
11 7CPEAb/+Dd2+hxqqezeXpTHOqJK
   iUiE8SqGnBBAw5uOpMffuGG120b
   LPEDfuM7yF
12 xaXWu6TQ94GTV/+2Inw9LufUPNs
   aTfrWWRxFNphWvTh9a+MRIIKb7a
   bSCee4qcwP
13 vjJsDM2f
14 =7HnR
15 -----END PGP MESSAGE-----
```

3. Repeat these steps for the given number of remailers. If the user wants to add another remailer, a new Anon-To: line is added at the start of the message. Then step 2 is repeated. These steps are repeated for the number of remailers in the chain.

4. Send message. The message is sent to the first remailer in the chain, which forwards the information described above.

INFO

[1] Press release on the closing down of 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] RFC Draft for the Mixmaster protocol, Version 2: *http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt*

[5] Mixmaster project homepage: *http://mixmaster.sourceforge.net*

[6] Information on the Debian Mixmaster package: *http://packages.qa.debian.org/m/mixmaster.html*

[7] Statistics for the Noreply.org remailer: *http://www.noreply.org/echolot/*