

Anonimowa poczta w technologii Mixmaster

WIADOMOŚCI ZNIKAJĄ

Systemy anonimowego przesyłania poczty elektronicznej służą do ochrony tożsamości nadawcy przed ujawnieniem. Protokół Mixmaster jest dojrzałą technologią tego typu; przykładem publicznie dostępnej aplikacji korzystającej z tej technologii jest tekstowy klient Mixmaster. **JENS KUBIEZIEL**



Kiedy w 1993 r. Johan Helsingius rozpoczął prace nad technologią zapewniania anonimowości poczty elektronicznej, chyba nie zdawał sobie sprawy, że otwiera puszkę Pandory. Dziś jednak, mimo wrogich reakcji – a może właśnie dzięki nim – Johan jest powszechnie ceniony za swój wynalazek.

Na początku lat 90. listy mailingowe i grupy dyskusyjne przestały być miejscami, w których dominowały tematy naukowe i informatyczne. USENET stał się także forum dla dyskutantów poruszających kontrowersyjne tematy polityczne i religijne. Ponieważ takimi dyskusjami interesowały się tajne służby oraz pracodawcy, powstała potrzeba wyrażania opinii w sposób anonimowy. Johan Helsingius opracował oprogramowanie do depersonalizacji wiadomości e-mail i zainstalował je na swoim serwerze.

Adres tego serwera, *anon.penet.fi*, stał się wkrótce dobrze znany i nawet dziś mówi się o nim z nabożeństwem. Aby skorzystać z usługi, użytkownik musiał wysłać pod ten adres wiadomość e-mail z odpowiednim wpisem w nagłówku. Serwer zamieniał adres nadawcy na format [anXXXX@anon.penet.fi] (gdzie XXXX była kombinacją cyfr) i przysyłał go na inny adres, podany w dodatkowym wierszu nagłówka.

Usługa była łatwa w użyciu i korzystało z niej wiele osób. W 1996 r. oprogramowanie obsługiwało ok. 10 000 wiadomości dziennie. W tym samym roku przedstawiciele ruchu scjentologicznego pozwali operatora do sądu, żądając upublicznienia adresów e-mail. Sąd fiński uznał, że wiadomości e-mail nie są objęte ustawą o poufności przesyłek pocztowych,

tym samym zezwalając na podsłuchiwanie i identyfikowanie użytkowników. To z kolei wpłynęło na decyzję Helsingiusa o wyłączeniu serwera [1].

Cypherpunk i Mixmaster

Kiedy Johan Helsingius wyłączał swój serwer anonimowej poczty, rozwój podobnego oprogramowania tego typu był już w zaawansowanym stadium. Grupa Cypherpunks, zajmująca się rozwiązaniami do ochrony prywatności i mechanizmami kryptograficznymi, opracowała metodę przesyłania poczty bez konieczności stosowania jednego, centralnego serwera. Prace oparto na artykule opublikowanym przez Davida Chauma [2], w którym autor – już w 1981 roku – opisał metodę ochrony anonimowości stron w wymianie listów elektronicznych w sieciach mieszanych.

Rozwiązanie przypomina wysyłanie listu umieszczonego w wielu kopertach. Nadawca anonimowego listu podaje adres odbiorcy, ale nie wysyła wiadomości bezpośrednio, lecz określa pewną liczbę stacji pośrednich. Następnie wkłada list do koperty, na której zamieszcza adres jednej z tych stacji. W każdej stacji list przenoszony jest do nowej koperty.

List dociera do pierwszej stacji pośredniej, gdzie otwierana jest najbardziej zewnętrzna koperta. Koperta zostaje zniszczona, a list jest wysyłany na adres podany na następnej kopercie; wreszcie, ostatnia stacja pośrednia przesyła list do faktycznego odbiorcy. Odbiorca może prześledzić drogę listu tylko do ostatniej stacji pośredniej, ponieważ wszyst-

kie inne koperty zostały zniszczone. Proces ten gwarantuje anonimowość nadawcy.

Remailer pierwszej generacji

Pierwszym modelem remailera (systemu przesyłającego pocztę w anonimowy sposób) był Cypherpunk Remailer, określane także jako remailer typu I. W przeciwieństwie do modelu Helsingiusa, w rozwiązaniu tym bierze udział wiele serwerów, z których każdy działa niezależnie od innych. Jeśli jeden serwer nie jest dostępny, użytkownik może skontaktować się z innym. Ponieważ serwery znajdują się w różnych państwach, posiadających różne systemy prawne, trudno jest dotrzeć do rzeczywistego nadawcy.

Wspomniane „opakowywanie” jest realizowane za pomocą technik kryptograficznych. Nadawca szyfruje wiadomość kluczami publicznymi poszczególnych remailerów na trasie przesyłki. Klucze takie można uzyskać pocztą elektroniczną (Listing 1) lub pobrać ze strony WWW danego systemu.

Każdy remailer rozszyfrowuje tylko tę część wiadomości, która jest dla niego przeznaczona. Rozszyfrowana część zawiera kolejny adres, pod który serwer ma przekazać wiadomość.

Opisywane rozwiązanie jest pozbawione wielu wad usługi Helsingiusa, ale pewne problemy wciąż istnieją. Na przykład każdy remailer przesyła wiadomość od razu po jej otrzymaniu. Atakujący może więc przeanalizować relacje między wiadomościami wychodzącymi i przychodzącymi, i na tej podstawie zidentyfikować nadawcę i odbiorcę. Może

Ramka 1: Wysyłanie listów przez remailery Cypherpunk

1. Piszemy wiadomość i dodajemy nagłówek. Najpierw należy zaadresować wiadomość do właściwego odbiorcy. Na samym początku listu muszą się znaleźć dwie linijki:

```
::
Anon-To: johannes.mustermann@example.org
```

Linijki te są informacją dla ostatniego remailera, który dostarcza wiadomość bezpośrednio do adresata.

2. Szyfrujemy wiadomość i dodajemy nagłówek o szyfrowaniu. Wiadomość jest teraz zaszyfrowana kluczem publicznym remailera. Przed zaszyfrowanym fragmentem dodajemy kolejną linijkę: *Encrypted: PGP*. Informuje ona system remailera, że kolejne linijki trzeba rozszyfrować.

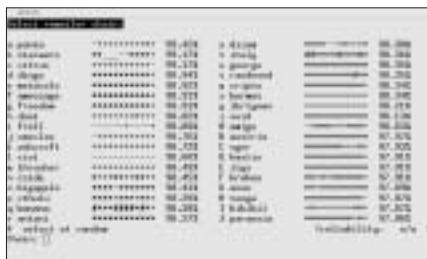
```
01 ::
02 Encrypted: PGP
03
04 ---BEGIN PGP MESSAGE---
05 Version: GnuPG v1.2.5 (GNU/Linux)
06
07 hQE0A1gu3H8UQS6IEAP/UgB5ZbyRS5K-
kmi/mD4V4PHBg6XOOoS8BL/t6HGaCkMc
08 BHAB4YCNQGz1IEzhrMnYxeFIOCa9B-
fsGTel1DjnHeLWypdW4XuPNnCiNA8fwd-
nu
09 C58rmBo2B8XTjcc1e-
GjD+SayRn/F3eGc3rdGw3EkWpRxxgw-
cXU/SvHwE6vnOnTWE
10 +9fWwweS+WUFRBNPqaUZ-
kXqZ6jBpVe5fRAUZDRhQOhUcEA0nvRH-
n9D7QMJuqV9R
11 7CPEAb/+Dd2+hxqzeXpTHOqJKiU-
iE8SqGnBBAw5uOpMffuGG120bLPEDfu-
M7yF
12 xaXWu6TQ94GTV/+2lnw9LufUPNsAT-
frWWRxFNphWTh9a+MRIKb7abSCe-
e4qcwP
13 vJJsDM2f
14 =7HnR
15 ---END PGP MESSAGE---
```

3. Powtarzamy powyższe kroki dla każdego remailera, przez który ma być przesyłana wiadomość. Aby dodać kolejny system remailera, na początku wiadomości trzeba umieścić nową linijkę Anon-To:. Następnie należy powtórzyć krok 2. I tak dla każdego remailera w łańcuchu.

4. Wysyłamy wiadomość. Wiadomość dociera do pierwszego remailera w łańcuchu, a ten przekazuje ją dalej.



Rysunek 1: Ekran startowy klienta Mixmaster.



Rysunek 2: Klient Mixmaster pokazuje listę dostępnych remailerów.

także przechwycić wiadomość, a potem wielokrotnie wstawiać ją w łańcuchu remailerów.

Ponieważ każda wiadomość traktowana jest dokładnie tak samo, podróżuje taką samą trasą. O tych wadach opisywanej usługi Lance Cottrell napisał w artykule „Mixmaster i ataki na remailery” [3] w 1995 r. Zawarte w tym opracowaniu propozycje zmian w architekturze rozwiązania stały się zaczątkiem utworzenia remailera typu II – rozwiązania Mixmaster.

Jak działa Mixmaster

Mixmaster nie przekazuje otrzymanej wiadomości natychmiast. Czeką dopóty, dopóki w kolejce znajdzie się wystarczająca liczba listów. Kiedy pula wiadomości jest pełna, wysyła listy do kolejnej stacji łańcucha w losowej kolejności. Aby uniemożliwić zidentyfikowanie wiadomości po wielkości, remailer przekształca je na paczki zajmujące tyle samo miejsca każda. Jeśli wiadomość jest zbyt krótka, dodaje do niej losowe znaki; jeśli zbyt długa – dzieli na kawałki równej wielkości. To uniemożliwia atakującemu odnalezienie relacji między wiadomościami przychodzącymi i wychodzącymi.

Ponadto każdy pakiet z wiadomością otrzymuje identyfikator. Mixmaster sprawdza, czy identyfikator został już zarejestrowany; jeśli tak – ignoruje wiadomość. Zabezpiecza to serwer przed atakami polegającymi na wstawianiu wiadomości do łańcucha remailerów. Wszystko to likwiduje wady remailera Cypherpunk. Dodatkowo w systemach Mixmaster stosowane jest szyfrowanie symetryczne, które przyspiesza przetwarzanie

wiadomości. Mixmaster ma więc liczne zalety w porównaniu z remailerem Cypherpunk.

Szczegółowy opis zasady działania Mixmastera wykracza poza ramy niniejszego artykułu. Czytelników zachęcamy do zapoznania się z roboczą wersją standardu RFC dla protokołu Mixmaster [4].

Mixmaster w praktyce

Mixmaster to także nazwa opracowanego przez programistów Open Source klienta korzystającego z opisanej usługi. Zasoby projektu znajdują się na serwisie Sourceforge [5]. Użytkownicy mogą pobrać kod źródłowy i samodzielnie zbudować program. Gotowe do użycia pakiety są dostępne dla użytkowników Debiana [6].

Po zainstalowaniu oprogramowania należy pobrać klucze publiczne i statystyki dostępności remailerów. Wielu operatorów umieszcza te dane na swoich stronach internetowych [7]. W pakiecie Mixmaster dla dystrybucji Debian znajdziemy skrypt w Perlu o nazwie *mixmaster-update*. Skrypt ten automatycznie pobiera wymagane pliki i można go wywoływać regularnie, jako zadanie usługi cron lub przy konfigurowaniu interfejsów sieciowych skryptami *ip-up*. Po pobraniu plików (ręcznie lub skryptem) i zapisaniu ich w katalogu */var/lib/mixmaster/stats/*, sam program uruchamiamy poleceniem *mixmaster* (Rysunek 1).

Program umożliwia pisanie, odczytywanie i wysyłanie wiadomości. Na przykład, aby wysłać wiadomość e-mail, musimy podać adresata i temat, a następnie wcisnąć klawisz [M]. Aby napisać wiadomość, wciskamy klawisz [E] w menu wysyłania; po napisaniu wiadomości następuje powrót do menu głównego. Domyślnie program wysyła wiadomości przez łańcuch czterech remailerów; aby samodzielnie skonfigurować łańcuch, należy wcisnąć klawisz [C] (Rysunek 2).

Na Rysunku 2 widzimy skrócone nazwy remailerów oraz informacje o ich niezawodności (dostępność, połączenie). Ponieważ dane te nie są uaktualniane na bieżąco, mają charakter tylko orientacyjny. Po zdefiniowaniu łańcucha wysyłamy wiadomość do puli oczekującej przyciskiem [M]. Po tym możemy już pisać następny list. Kiedy zbierze się wystarczająca liczba wiadomości, albo jeśli użytkownik wyda odpowiednie polecenie, program wysyła listy do kolejnych stacji w łańcuchu.

Program Mixmaster jest bardzo łatwy w użyciu i posiada intuicyjny interfejs. Nowy użytkownik nie powinien mieć problemu z wysyłaniem anonimowych wiadomości.

Listing 1: Pobieranie klucza remailera

```

01 From: Jens Kubieziel <jens@exam-
ple.org>
02 To: Dizum Remailer <remailer@di-
zum.com>
03 Subject: remailer-key

Odpowiedź systemu remailera:
01 From: Nomen Nescio <remailer@di-
zum.com>
02 To: „Jens Kubieziel” <jens@exam-
ple.org>
03 Subject: Remailer key for dizum
04
05 $remailer{"dizum"} = "<remailer@di-
zum.com> cpunk mix pgp pgponly reppg
remix latent hash cut test ek ekx esub inft50
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 No-
men Nescio <remailer@dizum.com>
11
12 ---BEGIN PGP PUBLIC KEY BLOCK---
13 Version: Mixmaster 2.9.0 (OpenPGP
module)
14
15 mQCNAzkEMTMAAAEEAOa7vR4GZ-
CRUuakobqLgzbruc6cUIAgL0s8O-
d2l+UF1KTY5Z
16 XKCKIKK5UbIHDiFgzJk+0NxVR3eP-
gJ56MJeK2iGPVZ/i8thC1gR6btrrSONzfk7rr
17 bW2aKIDfihyZ6emPYkHqPj0hA-
wxGQITMkEPF5jmEdWeZN4kph8q6Dlx-
0s3AAID
18 tCFOb21lbiBOZXNjaW8gPHJlbWFpb-
GVyQGRpenVtLmNvbT6JAJUDBRA5BDE-
zHyro
19 MjEjSzcBAWqABAC+6voEDspSDQU-
n0RmLjy1zPsysx7Zdc7J/c40l6rGS9n1tZQiw
20 CTplLinXiCLP3I9Pu9T4kl1gHVYylu-
2pqeNOJL0Wz1w6HkwQjGsGdxtFDyFCm-
fxe
21 c0htDM5WQn1Dqtlag98mNcStkY-
2B5e7VNP2aVd66oTeDPLYD4VCsrl-
T0Dw==
22 =RJCD
23 ---END PGP PUBLIC KEY BLOCK---
24
25 Type Bits/KeyID Date User ID
26 pub 1024D/B1685FE7 2000-04-24 No-
men 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 mo-
dule)
31
32 mQGiBDkEMTMRBADqwatBmgC/yoOly-
qrzFL1toAzDrSiH06eZlo8eCRj+Uqw6lSu0
33 RxxhSZaBUisuqogRHFiuX+RqUIa-
241vEjSN0x7ZV+LipTZc282Vb0Pu-
Dv7fL2Ll
34 Ez8QEJmZ+zpMjICRFVNgHGRvhHU-
Gu18i9BTmzigpyuMpMwwlB2HvTBO-
4CQCgwnPp
35 B/145a4PZ2+zmZyVQUuAh+UD/je6O-
duoTwwq6176bUfcvCtVH9DP4DwoCgrVw-
d3c
36 r9KoR9hO7TAGL5Ah7eJ1GvndR-
H7KPBfuE6h/kmCohNgKGLuPn4je-
6vJ6N0J/O3av
37 +jJ1mHN2TImOp0+VFXFPm1A-
7zqA/MWgOG7DWggfmguz9E6TuAbfO-
lvy/Ksqnjt70
38 JyelA/9YyKH56juAGYHdHbPQR/NA-
ED3XLUUc8UzXNuL5VNAD40SfbxVpNwJ-
JPYM3
39 fA2RY0lbsMefKvotlXRkKZHzFbj0Kcn-
kvF0d0WWhXzCgTEdwywhaQQJzWznu-
Vzqm
40 18GZoomfsbsgfYHwFD0CCTsqVj3GIM-
TXHO6ol7QOw69HGINZYrQhTm9t-
ZW4gTmVz
41 Y2lVdxyZW1haWxlckBkaXp1bS5j-
b20+IQBNBBARAgANBQI15BDEzAawsDA-
gleAQAK
42 CRBos3tosWhf52NaAKCjS4ny-
qFvmq85a5HwGPHhTBhGPJwCdHrYGF-
IVOh8OJJUR
43 vQiaIRNRG/W5AQ0EOQQxMxA-
EAL5wXBX5gxZE4MDaUDE9TWRwo-
6VnE6dUvu6la450
44 hyAVDp5AoaquHpJv7PvhA/nLiDFJsp-
m2eDdLglaUGcDlt6MEbXV/I9v/qQ7qnh/
45 Cm84gss+uKTWZjga2NRZ/Y4JGe-
PlmLWBlmapwPoHBhJEXsd-
p1zl/0DiDGmHdV12
46 xPHfAAMFBACB12J/HSJznAwpGsl-
B03NrBz2lw7NqrhepSfcExGiWrGMJnAjA-
d98l
47 C84j5AYwMhGWMpmezNqdcqWE-
I9Z2cWd0nXndt8GJAUCpFb5T2snTnoqa-
ilB4nyq
48 vyG1HwBM7OMXw9k13smo+5PgE3E-
HyQ2pvluaMoOZz6o/zq6d0xH6XokAPwM-
FGDkE
49 MTNos3tosWhf5xECVY0AojcXn-
CHayCkFAE17SXU33cc3R1qnAKCpVZkK-
buQSpHyg
50 M4wRXciYwPaoyw==
51 =Vklz
52 ---END PGP PUBLIC KEY BLOCK---

```

Zalety i wady anonimowej poczty

Anonimowa komunikacja niedobrze nam się kojarzy. Przywodzi na myśl donosy, groźby, spam i nielegalne treści. A przecież anonimowe remailery spełniają po prostu jeden z wymogów bezpiecznej infrastruktury komputerowej: ukrywają fakt wymiany informacji. Istnieje wiele powodów, dla których może zająć potrzeba ukrycia takiego faktu. Na przykład nagły wzrost wymiany listów elektronicznych – nawet zaszyfrowanych – między dwoma firmami może dać podsłuchującemu powody do podejrzenia, że firmy te planują nawiązanie partnerstwa. Często na anonimowości zależy aktywistom radykalnych grup, zwolennikom reform w państwach autorytarnych albo osobom cierpiącym na wstydlive choroby.

Z drugiej strony trzeba mieć świadomość potencjalnych niewłaściwych zastosowań anonimowych remailerów; to właśnie na te zastosowania chętnie zwracają uwagę lobbyści i przedstawiciele władz, którym wielokrotnie udaje się doprowadzić do zakazu udostępniania usług anonimowej poczty. Twórca remailerów Johan Helsingius twierdzi, że nigdy nie użył wymyślonej przez siebie usługi. Jego celem było tylko stworzenie technologii zapewniającej anonimowość, a więc zwiększającej swobodę wyrażania opinii. Dzięki istnieniu systemów anonimowych remailerów na całym świecie, technologia ta jest dostępna dla każdego z nas. ■

INFO

- [1] Informacja prasowa o zamknięciu serwisu 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/~fran/crypto/chaum-acm-1981.html>
- [3] Lance Cottrell, „Mixmaster & Remailer Attacks”: <http://riot.eu.org/anon/doc/remailer-essay.html>
- [4] Roboczy standard RFC dot. protokołu Mixmaster, wersja 2: <http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt>
- [5] Strona projektu Mixmaster: <http://mixmaster.sourceforge.net>
- [6] Informacje o pakiecie Mixmaster dla Debiana: <http://packages.qa.debian.org/m/mixmaster.html>
- [7] Statystyki remailera Noreply.org: <http://www.noreply.org/echolet/>