Anonymous remailer

An **anonymous remailer** is a server that receives messages with embedded instructions on where to send them next, and that forwards them without revealing where they originally came from. There are Cypherpunk anonymous remailers, Mixmaster anonymous remailers, and nym servers, among others, which differ in how they work, in the policies they adopt, and in the type of attack on anonymity of e-mail they can (or are intended to) resist. *Remailing* as discussed in this article applies to e-mails intended for particular recipients, not the general public. Anonymity in the latter case is more easily addressed by using any of several methods of anonymous publication.

Types of remailer

There are several strategies that affect the anonymity of the handled e-mail. In general, different classes of anonymous remailers differ with regard to the choices their designers/operators have made. These choices can be influenced by the legal ramifications of operating specific types of remailers.[1]

It must be understood that every data packet traveling on the Internet contains the node addresses (as raw IP bit strings) of both the sending and intended recipient nodes, and so no data packet can *ever* actually be anonymous at this level. However, if the IP source address is false, there will be no easy way to trace the originating node (and so the originating entity for the packet). In addition, all standards-based e-mail messages contain defined fields in their headers in which the source and transmitting entities (and Internet nodes as well) are required to be included. However, since most users of e-mail do not have very much technical expertise, the full headers are usually suppressed by mail reading software. Thus, many users have never seen one.

Some remailers change both types of address in messages they forward, and the list of forwarding nodes in e-mail messages as well, as the message passes through; in effect, they substitute 'fake source addresses' for the originals. The 'IP source address' for that packet may become that of the remailer server itself, and within an e-mail message (which is usually several packets), a nominal 'user' on that server. Some remailers forward their anonymized e-mail to still other remailers, and only after several such hops is the e-mail actually delivered to the intended address.

There are, more or less, four types of remailers:

Pseudonymous remailers

A Pseudonymous remailer simply takes away the e-mail address of the sender, gives a pseudonym to the sender, and sends the message to the intended recipient (that can be answered via that remailer).

Cypherpunk remailers, also called Type I

A Cypherpunk remailer sends the message to the recipient stripping away the sender address on it. One can not answer a message sent via a Cypherpunk remailer. The message sent to the remailer can usually be encrypted, and the remailer will decrypt it and send it to the recipient address hidden inside the encrypted message. In addition, it is possible to chain two or three remailers, so that each remailer can't know who is sending a message to whom. Cypherpunk remailers do not keep logs of transactions.

Mixmaster remailers, also called Type II

In Mixmaster, you compose an email to a remailer, which is relayed through each node in the network using SMTP, until it finally arrives at your recipient. Mixmaster can only send emails one way. An email is sent anonymously to an individual, but for them to be able to respond, the reply address must be included in the body of the email. Also, Mixmaster remailers require the use of a computer program to write messages. Such programs are not supplied as a standard part of most operating systems or mail management systems.

Mixminion remailers, also called Type III

A Mixminion remailer attempts to address the following challenges in Mixmaster remailers: replies, forward anonymity, replay prevention and key rotation, exit policies, integrated directory servers and dummy traffic. They are currently available for the Linux and Windows platforms. Some implementations are open source.

Traceable remailers

Some remailers establish an internal list of actual senders and invented names such that a recipient can send mail to *invented name* AT *some-remailer.example*. When receiving traffic addressed to this user, the server software consults that list, and forwards the mail to the original sender, thus permitting anonymous—though traceable with access to the list—two way communication. The famous "penet.fi" remailer in Finland did just that for several years.[*citation needed*] Because of the existence of such lists in this type of remailing server, it is possible to break the anonymity by gaining access to the list(s), by breaking into the computer, asking a court (or merely the police in some places) to order that the anonymity be broken, and/or bribing an attendant. This happened to penet.fi as a result of some traffic passed through it about Scientology.[*citation needed*] The Church claimed copyright infringement and sued penet.fi's operator. A court ordered the list be made available. Penet's operator shut it down after destroying its records (including the list) to retain identity confidentiality for its users; though not before being forced to supply the court with the real e-mail addresses of two of its users.[*citation needed*]

More recent remailer designs use cryptography in an attempt to provide more or less the same service, but without so much risk of loss of user confidentiality. These are generally termed nym servers or pseudonymous remailers. The degree to which they remain vulnerable to forced disclosure (by courts or police) is and will remain unclear, since new statutes/regulations and new cryptanalytic developments proceed apace. Multiple anonymous forwarding among cooperating remailers in different jurisdictions may retain, but cannot guarantee, anonymity against a determined attempt by one or more governments, or civil litigators.

Untraceable remailers

If users accept the loss of two-way interaction, identity anonymity can be made more secure.

By not keeping any list of users and corresponding anonymizing labels for them, a remailer can ensure that any message that has been forwarded leaves no internal information behind that can later be used to break identity confidentiality. However, while being handled, messages remain vulnerable within the server (e.g., to Trojan software in a compromised server, to a compromised server operator, or to mis-administration of the server), and traffic analysis comparison of traffic into and out of such a server can suggest quite a lot—far more than almost any would credit.

The Mixmaster strategy is designed to defeat such attacks, or at least to increase their cost (i.e., to 'attackers') beyond feasibility. If every message is passed through several servers (ideally in different legal and political jurisdictions), then attacks based on legal systems become considerably more difficult, if only because of 'Clausewitzian' friction amongst lawyers, courts, different statutes, organizational rivalries, legal systems, etc. And, since many different servers and server operators are involved, subversion of any (i.e., of either system or operator) becomes less effective also since no one (most likely) will be able to subvert the entire chain of remailers.

Random padding of messages, random delays before forwarding, and encryption of forwarding information between forwarding remailers, increases the degree of difficulty for attackers still further as message size and timing can be largely eliminated as traffic analysis clues, and lack of easily readable forwarding information renders ineffective simple automated traffic analysis algorithms.

Web based mailer

There are also web services that allow users to send anonymous e-mail messages. These services do not provide the anonymity of real remailers, but they are easier to use. When using a web-based anonymous e-mail or anonymous remailer service, its reputation should first be analyzed, since the service stands between senders and recipients. Some of the aforementioned web services log the users I.P. addresses to ensure they do not break the law; others offer superior anonymity with attachment functionality by choosing to trust that the users will not breach the websites Terms of Service (TOS).

Remailer statistics

In most cases, remailers are owned and operated by individuals, and are not as stable as they might ideally be. In fact, remailers can, and have, gone down without warning. It is important to use up-to-date statistics when choosing remailers.

Remailer abuse

Although most re-mailer systems are used responsibly, the anonymity they provide can be exploited by entities or individuals whose reasons for anonymity are not necessarily benign.

Such reasons could include support for violent extremist actions[*citation needed*], sexual exploitation of children [*citation needed*] or more commonly to frustrate accountability for 'trolling' and harassment of targeted individuals, or companies (The Dizum.com re-mailer chain being abused as recently as May 2013[*citation needed*] for this purpose.)

The response of some re-mailers to this abuse potential is often to disclaim responsibility (as dizum.com does[2]), as owing to the technical design (and ethical principles) of many systems, it is impossible for the operators to physically unmask those using their systems. Some re-mailer systems go further and claim that it would be illegal for them to monitor for certain types abuse at all.[3]

Until technical changes were made in the remailers concerned in the mid-2000s, some re-mailers (notably nym.alias.net based systems) were seemingly willing to use any genuine (and thus valid) but otherwise forged address. This loophole allowed trolls to mis-attribute controversial claims or statements with the aim of causing offence, upset or harassment to the genuine holder(s) of the address(es) forged.

Archives

/Archive1
/Archive2
/Archive3
/Archive
4
/Archive5
/Archive6

Remailer software

- QuickSilver and QuickSilver Lite remailer software [4] are Windows e-mail client applications which send messages through Mixmaster anonymous remailer cascades. The newer Lite version is capable of SSL/TLS and with it's companion program QuickSilver Aam it supports nym servers.
- News2Remail [5] is an NNTP to remailer proxy for Windows.

References

[1] du Pont, George F. (2001) The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils (http://www.thsh.com/documents/JTLM.pdf)"Journal of Technology Law & Policy"

[2] https://dizum.com/help/usenet.html

[3] https://dizum.com/help/usenet.html

[4] http://www.quicksilvermail.net/

[5] http://www.cotse.net/news2remail/

- Remailer Vulnerabilities (http://freehaven.net/anonbib/cache/rprocess.html)
- *Email Security*, Bruce Schneier (ISBN 0-471-05318-X)
- *Computer Privacy Handbook*, Andre Bacard (ISBN 1-56609-171-3)

Article Sources and Contributors

Anonymous remailer *Source*: https://en.wikipedia.org/w/index.php?oldid=584455506 *Contributors*: Ahoerstemeier, Alphax, Ameins, ArnoldReinhold, Burpen, Chester Markel, Crooks, Cyberso, Davemcarlson, Davidgothberg, DouglasCalvert, Dr. Sunglasses, Dvehrs, Ehn, Evercat, F, Frecklefoot, Ghost51423, Gracefool, Gwern, Gzuckerwar, Haakon, Hakeem.gadi, HiEv, Imran, JAF1970, Jackzhp, Jaericho, Jaranda, John W. Kennedy, Jonathanbull, Joy, Kaizokuo, Kalkaska, Khazar2, LeoNomis, Marek69, Martarius, Marudubshinki, Matt Crypto, Meetsquiet, Mellery, MessaLec, Michigan Remail, Mild Bill Hiccup, Minesweeper, Minghong, Modemac, Mogism, Nikai, Nil Einne, No Guru, Nuwewsco, Peyna, Phantom784, PierreAbbat, Poolisfun, Rearden9, Rjwilmsi, Rusty.pole, S3ven, SWAdair, Santa Sangre, SebastianHelm, Sfan00 IMG, Shaddack, ShakespeareFan00, Simon D M, SimonP, Starblind, Stw, Superm401, TeaDrinker, Theycre, Uncle Milty, Warren, Wingman4l7, Wmahan, Wrs1864, Ww, Zanaq, Zoicon5, أحمد, 108 anonymous edits

Image Sources, Licenses and Contributors

File:Replacement filing cabinet.svg *Source*: https://en.wikipedia.org/w/index.php?title=File:Replacement_filing_cabinet.svg *License*: Public Domain *Contributors*: Anomie

License