Anonymous remailer

A **privacy-focused remailer** is a server that receives messages with embedded instructions on where to send them next, and that forwards them while attempting to obscure their origin. There are cypherpunk remailers, mixmaster remailers, and nym servers, among others, which differ in their design and the level of privacy they were intended to provide. It is critical to understand that without integration with an anonymity network like Tor, these systems do not provide anonymity against powerful adversaries. *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 remailers

There are several strategies that affect the pseudonymity of the handled e-mail. These classes of 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 . 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.

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).[2]

Cypherpunk remailers

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 typically do not keep logs of transactions, but their design is vulnerable to traffic analysis.

Mixmaster remailers

In Mixmaster, the user composes an email to a remailer, which is relayed through each node in the network using SMTP, until it finally arrives at the final recipient. Mixmaster can only send emails one way. An email is sent pseudonymously to an individual, but for them to be able to respond, a 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. Mixmaster is vulnerable to long-term traffic analysis and is considered obsolete.

Mixminion remailers

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. Despite improvements, Mixminion shares the fundamental vulnerability to traffic analysis and requires protection by a network like Tor for meaningful anonymity.

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.[3] 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. 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.

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.

Modern Tor-based and Mixnet alternatives

Due to the inherent vulnerabilities of classical remailers to traffic correlation[4] and metadata surveillance, the modern approach to anonymous email relies on integrating remailer functionality with robust anonymity networks.

Tor-based remailers: Systems like the **Onion Courier Mixnet**[5] operate as Tor hidden services. This protects the user's IP address and the remailer's location from network observers. While Tor provides strong protection for network metadata, the mixnodes are adding additional layers of anonymity per hop.

Mixnet-based remailers: The Nym network is designed specifically to resist powerful traffic analysis attacks that threaten older remailers and even Tor in some scenarios. Nym uses a layered mixnet architecture with cover traffic to provide strong anonymity for message timing and metadata. Future anonymous email systems are likely to be built directly on top of mixnets like Nym to provide anonymity against nation-state adversaries.[6] For any meaningful anonymity, the use of such an integrated network is now considered essential; standalone classical remailers do not provide adequate security.

Web-based mailer

There are also web services that allow users to send anonymous email messages. These services typically do not provide the strong pseudonymity of cryptographic remailers, let alone anonymity, and they are often easier to use. When using a web-based anonymous email service, its reputation and privacy policy should first be analyzed carefully, since the service stands between senders and recipients. Many such services log the users IP addresses; others may offer superior privacy but still require trust in the operator.[7]

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, such as those provided by SEC3[8] when choosing remailers.

Remailer abuse and blocking by governments

While most remailers are used responsibly, their pseudonymity has been exploited for illegal activities. A prominent example is the **2012 University of Pittsburgh bomb threats**, where an Anonymous-linked remailer was seized by the FBI after being used to send over 100 threatening emails.[9][10]

Some remailers disclaim responsibility for abuse, citing technical and ethical limitations that prevent operators from identifying users.[11] Others argue that monitoring for certain abuses would itself be illegal under privacy laws.[11]

See also

- Anonymity
- Anonymous P2P
- Anonymous web browsing

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://ww

w.thsh.com/documents/JTLM.pdf) Archived (https://web.archive.org/web/20160305043023/http://www.thsh.com/documents/JTLM.pdf) 2016-03-05 at the Wayback Machine"Journal of Technology Law & Policy"

2. Froomkin, A. Michael (1995). "Anonymity and its Enmities". *Journal of Online Law*. **1**. Rochester, NY. art. 4. SSRN 2715621 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715621) .
3. "Johan Helsingius closes his Internet remailer" (https://web.archive.org/web/20160303221336/https://w2.eff.org/Privacy/Anonymity/960830_penet_closure.announce) (Press release). 1996-08-30. Archived from the original (https://w2.eff.org/Privacy/Anonymity/960830_penet_closure.announce) on 2016-03-03. Retrieved 2014-10-09.
4. Danezis, George; Syverson, Paul (2006). *Eclipse Attacks on Tor* (https://doi.org/10.1007/11957454_4) . Privacy Enhancing Technologies. doi:10.1007/11957454_4 (https://doi.org/10.1007%2F11957454_4) .
5. "Onion Courier: Anonymous email over Tor" (https://github.com/Ch1ffr3punk/oc) . GitHub. Retrieved 2025-06-30.
6. Dingledine, Roger (2004). "Tor: The Second-Generation Onion Router" (https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf) (PDF). *USENIX Security Symposium*.
7. "Amnesty Box" (http://www.amnestybox.com/) . Archived (https://web.archive.org/web/20120414030144/http://www.amnestybox.com/) from the original on 14 April 2012. Retrieved 29 March 2012.
8. "Current Remailer Statistics and Network Metrics" (https://www.sec3.net/misc/) . SEC3.
9. "FBI seizes activist's Anonymous remailer server in bomb threat investigation" (https://arstechnica.com/tech-policy/2012/04/fbi-seizes-activists-anonymous-remailer-server-in-bomb-threat-investigation/) . *Ars Technica*. 2012-04-06.
10. "2012 University of Pittsburgh bomb threats" (https://en.wikipedia.org/wiki/2012_University_of_Pittsburgh_bomb_threats) . Wikipedia.
11. "DIZUM FAQ" (https://web.archive.org/web/20100710023752/http://dizum.com/help/usenet.html) . Archived from the original (https://dizum.com/help/usenet.html) on 2010-07-10. Retrieved 2012-11-01.

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)