Pseudonymous remailer

A **pseudonymous remailer** or **nym server**, as opposed to an anonymous remailer, is an Internet software program designed to allow people to write pseudonymous messages on Usenet newsgroups and send pseudonymous email. Unlike purely anonymous remailers, it assigns its users a user name, and it keeps a database of instructions on how to return messages to the real user. These instructions usually involve the anonymous remailer network itself, thus protecting the true identity of the user.

Primordial pseudonymous remailers once recorded enough information to trace the identity of the real user, making it possible for someone to obtain the identity of the real user through legal or illegal means. This form of pseudonymous remailer is no longer common.

David Chaum wrote an article in 1981 that described many of the features present in modern pseudonymous remailers.[1]

The Penet remailer, which lasted from 1993 to 1996, was a popular pseudonymous remailer.

Contemporary nym servers

A **nym server** (short for "pseudonym server") is a server that provides an untraceable e-mail address, such that neither the nym server operator nor the operators of the remailers involved can discover which nym corresponds to which real identity.

To set up a nym, one creates a PGP keypair and submits it to the nym server, along with instructions (called a *reply block*) to anonymous remailers (such as Cypherpunk or Mixmaster) on how to send a message to one's real address. The nym server returns a confirmation through this reply block. One then sends a message to the address in the confirmation.

To send a message through the nym server so that the *From* address is the nym, one adds a few headers, signs the message with one's nym key, encrypts it with the nym server key, and sends the message to the nym server, optionally routing it through some anonymous remailers. When the nym server receives the message it decrypts it and sends it on to the intended recipient, with the *From* address indicating one's nym.

When the nym server gets a message addressed *to* the nym, it appends it to the nym's reply block and sends it to the first remailer in the chain, which sends it to the next and so on until it reaches your real address. It is considered good practice to include instructions to encrypt it on the way, so

that someone (or some organization) doing in/out traffic analysis on the nym server cannot easily match the message received by you to the one sent by the nym server.

Existing "multi-use reply block" nym servers were shown to be susceptible to passive traffic analysis with one month's worth of incoming spam (based on 2005 figures) in a paper by Bram Cohen, Len Sassaman, and Nick Mathewson.[2]

See also

- Anonymity
  - Anonymous P2P
  - Anonymous remailer
    - Cypherpunk anonymous remailer (Type I)
    - Mixmaster anonymous remailer (Type II)
    - Mixminion (Type III)
    - I2P-Bote
  - Onion routing
    - Tor (network)
- Data privacy
- Penet remailer
- Traffic analysis

References

1. Chaum, David (February 1981). "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" (http://freehaven.net/anonbib/cache/chaum-mix.pdf) (PDF). *Communications of the ACM*. **24** (2): 84–90. doi:10.1145/358549.358563 (https://doi.org/10.1145%2F358549.358563) . S2CID 30340230 (https://api.semanticscholar.org/CorpusID:30340230) .
2. See The Pynchon Gate: A Secure Method of Pseudonymous Mail Retrieval (http://www.cosic.esat.kuleuven.be/publications/article-620.pdf) Sassaman, Len; Cohen, Bram; Mathewson, Nick (2005). "The pynchon gate: A secure method of pseudonymous mail retrieval" (http://www.cosic.esat.kuleuven.be/publications/article-620.pdf) (PDF). *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM Press. pp. 1–9. doi:10.1145/1102199.1102201 (https://doi.org/10.1145%2F1102199.1102201) . ISBN 1-

59593-228-3. S2CID 356770 (https://api.semanticscholar.org/CorpusID:356770) . Retrieved June 6, 2008.

Further reading

- Bruce Schneier (January 25, 1995). *Email Security* (https://archive.org/details/emailsecurityhow0000schn) . Wiley. ISBN 0-471-05318-X.
- Bacard, Andre (1995). *Computer Privacy Handbook*. Peachpit Press. ISBN 1-56609-171-3.

External links

- Anonymous Remailer FAQ (http://www.andrebacard.com/remail.html)
- Mixmaster FAQ (https://mixmaster.sourceforge.net/faq.shtml)
- Official I2P-Bote eepsite (http://tjgidoycrw6s3guetge3kvrvynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/) (I2P-internal)