Retroshare

Retroshare is a free and open-source peer-to-peer communication and file sharing app based on a friend-to-friend network built by GNU Privacy Guard (GPG).[4] Optionally peers may exchange certificates and IP addresses to their friends and vice versa.[5][6]

History

Retroshare was founded in 2004 by Mark Fernie.[7] An unofficial build for the single-board computer Raspberry Pi, named PiShare, was available since 2012.[8]

On 4 November 2014, Retroshare scored 6 out of 7 points on the Electronic Frontier Foundation's secure messaging scorecard, which is now out-of-date. It lost a point because there had not been a recent independent code audit.[9]

In August 2015, Retroshare repository was migrated from SourceForge to GitHub.[10] In 2016, *Linux Magazine* reviewed security gaps in Retroshare and described it as "a brave effort, but in the end, an ineffective one."[11]

Design

Retroshare is an instant messaging and file-sharing network that uses a distributed hash table for address discovery. Users can communicate indirectly through mutual friends and request direct connections.[12]

Features

Authentication and connectivity

After initial installation, the user generates a pair of (GPG) cryptographic keys with Retroshare. After authentication and exchanging an asymmetric key, OpenSSL is used to establish a connection, and for end-to-end encryption. Friends of friends cannot connect by default, but they can see each other, if the users allow it. IPv6 was released in November of 2018.

File sharing

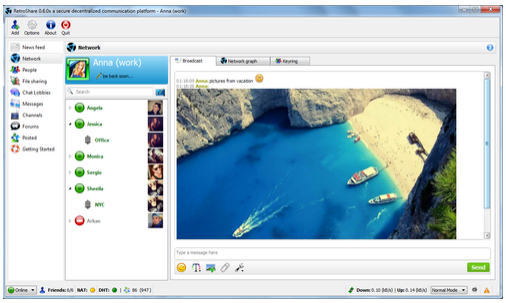
It is possible to share folders between friends.[13] File transfer is carried on using a multi-hop swarming system (inspired by the "Turtle Hopping" feature from the Turtle F2F project, but implemented differently). In essence, data is only exchanged between friends, although it is possible that the ultimate source and destination of a given transfer are multiple friends apart. A search function performing anonymous multi-hop search is another source of finding files in the network.

Files are represented by their SHA-1 hash value, and HTTP-compliant file and links may be exported, copied, and pasted into/out of Retroshare to publish their virtual location into the Retroshare network.

Communication

Retroshare offers the following services for communication:

- a private chat;
- a private mailing system that allows secure communication between known friends and distant friends;
- public and private multi-user chat lobbies;
- a forum system allowing both anonymous and authenticated forums, which distributes posts from friends to friends;
- a channel system offers the possibility to auto-download files posted in a given channel to every subscribed peer, similar to RSS feeds;

Retroshare	
	
	
Original author	Robert Fernie
Developers	Cyril Soler Gioacchino Mazzurco
Initial release	2006[1]
Stable release	0.6.7[2] / 30 November 2023
Repository	github.com/RetroShare (https://github.com/RetroShare)
Written in	C++
Operating system	Linux, Windows, macOS, Android, FreeBSD, OpenBSD, NetBSD, Haiku
Platform	Cross-platform
Available in	38 languages[3]
List of languages	[show]

- a posted links system, where links to important information can be shared;
- VoIP calls;
- Video calls (since version 0.6.0);
- Tor and I2P networks support, for further anonymisation (since version 0.6.0).

Type	Anonymous P2P, friend-to-friend, chat, instant messaging, newsgroups, voice over IP, email client and BBS
License	GNU General Public License
Website	retroshare.cc (https://retroshare.cc)

User interface

The core of the Retroshare software is based on an offline library, into which two executables are plugged:

- a command-line interface executable which offers nearly no control, but it is useful to run "headless" on a server
- a graphical user interface written in Qt is the one most users use. In addition to functions quite common to other file-sharing software, such as a search tab and visualization of transfers, Retroshare gives users the potential to manage their network by collecting optional information about neighbouring friends and visualizing it as a trust matrix or as a dynamic network graph. The appearance can be changed by choosing one of several available style sheets.

Anonymity

The friend-to-friend structure of the Retroshare network makes it difficult to intrude and hardly possible to monitor from an external point of view.[14] The degree of anonymity may be improved further by deactivating the DHT and IP/certificate exchange services, making the Retroshare network a real dark net.[15]

Friends of friends may not connect directly with each other; however, a user may enable the anonymous sharing of files with friends of friends. Search, access, and both upload and download of these files are made by "routing" through a series of friends. This means that communication between the source of data (the up-loader) and the destination of the data (the down-loader) is indirect through mutual friends. Although the intermediary friends cannot determine the original source or ultimate destination, they can see their very next links in the communication chain (their friends). Since the data stream is encrypted, only the original source and ultimate destination are able to see what data is transferred.

Caveats

While Retroshare's encryption makes it virtually impossible for an ISP or another external observer to know what one is downloading or uploading, this limitation does not apply to members of the user's Retroshare circle of trust; adding untrusted people to it may be a potential risk.[16]

In 2012, a German Court granted an injunction against a user of Retroshare for sharing copyrighted music files. Retroshare derives its security from the fact that all transfers should go through “trusted friends” whom users add. In this case, the defendant added the anti-piracy monitoring company as a friend, which allowed him to be traced through aggregation of bad Opsec.[17]

See also

- Comparison of file-sharing applications

References

1. "Retroshare aims to be a private F2F social network | SourceForge Community Blog" (https://sourceforge.net/blog/retroshare-aims-to-be-a-private-f2f-social-network/) . *Sourceforge.net*. 11 May 2010. Retrieved 4 December 2016.
2. "Release 0.6.7" (https://github.com/RetroShare/RetroShare/releases/tag/v0.6.7.2) . 30 November 2023. Retrieved 30 November 2023.
3. "Retroshare localization" (https://www.transifex.com/projects/p/retroshare/) . *Transifex.com*. Retrieved 4 December 2016.
4. Amato, Alba, Beniamino Di Martino, Marco Scialdone, and Salvatore Venticinque. "A negotiation solution for smart grid using a fully decentralized, P2P approach". *Ninth International Conference on Complex*.
5. "Anonymous, Decentralized and Uncensored File-Sharing is Booming" (https://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/) . TorrentFreak. 3 March 2012. Retrieved 4 December 2016.
6. Shen, Xuemin; Yu, Heather; Buford, John; Akon, Mursalin, eds. (2010). *Handbook of Peer-to-Peer Networking | Xuemin (Sherman) Shen* (https://www.springer.com/engineering/signals/book/978-0-387-09750-3) . Springer. doi:10.1007/978-0-387-09751-0 (https://doi.org/10.1007%2F978-0-387-09751-0) . ISBN 978-0-387-09750-3. S2CID 60783890 (https://api.semanticscholar.org/CorpusID:60783890) . Retrieved 4 December 2016.

7. Alkhulaiwi, Rakan; Sabur, Abdulhakim; Aldughayem, Khalid; Almanna, Osama (December 2016). "Survey of secure anonymous peer to peer Instant Messaging protocols" (https://dx.doi.org/10.1109/pst.2016.7906977) . *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE. pp. 294–300. doi:10.1109/pst.2016.7906977 (https://doi.org/10.1109%2Fpst.2016.7906977) . ISBN 978-1-5090-4379-8. S2CID 15496391 (https://api.semanticscholar.org/CorpusID:15496391) .
8. "PiShare download" (https://sourceforge.net/projects/pishare/) . *SourceForge.net*. 15 January 2014. Retrieved 4 December 2016.
9. "Secure Messaging Scorecard. Which apps and tools actually keep your messages safe?" (https://www.eff.org/pages/secure-messaging-scorecard) . Electronic Frontier Foundation. 4 November 2014.
10. Community, Retroshare. "History - Retroshare Docs" (https://retroshare.readthedocs.io/en/latest/about/history/) . *retroshare.readthedocs.io*. Retrieved 28 January 2018.
11. Byfield, Bruce (24 February 2016). "Is a private network useful for privacy and security?" (https://www.linux-magazine.com/Online/Features/RetroShare) . *Linux Magazine*. Retrieved 4 September 2022.
12. M, Rogers; S, Bhatti (2007). "How to Disappear Completely: A Survey of Private Peer-to-Peer Networks" (http://discovery.ucl.ac.uk/173455/) . *discovery.ucl.ac.uk*. Retrieved 28 January 2018.
13. Alkhulaiwi, Rakan, Abdulhakim Sabur, Khalid Aldughayem, and Osama Almanna. "Survey of secure anonymous peer to peer Instant Messaging protocols". *14th Annual Conference on Privacy, Security and Trust*.
14. Alkhulaiwi, Rakan, Abdulhakim Sabur, Khalid Aldughayem, and Osama Almanna (2016). "Survey of secure anonymous peer to peer Instant Messaging protocols". *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. pp. 294–300. doi:10.1109/PST.2016.7906977 (https://doi.org/10.1109%2FPST.2016.7906977) . ISBN 978-1-5090-4379-8. S2CID 15496391 (https://api.semanticscholar.org/CorpusID:15496391) .
15. "Anonymous, Decentralized and Uncensored File-Sharing is Booming - TorrentFreak" (https://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/) . *TorrentFreak*. 3 March 2012. Retrieved 28 January 2018.
16. "Increase online privacy with Retroshare" (https://dougvitale.wordpress.com/2013/07/29/increase-online-privacy-with-retroshare/) . *Doug Vitale Tech Blog*. 29 July 2013. Retrieved 28 January 2018.

17. " "Anonymous" File-Sharing Darknet Ruled Illegal by German Court - TorrentFreak" (https://torrentfreak.com/anonymous-file-sharing-ruled-illegal-by-german-court-121123/) . *TorrentFreak*. 23 November 2012. Retrieved 28 January 2018.

External links

- Official website (https://retroshare.cc)