WASTE

WASTE is a peer-to-peer and friend-to-friend protocol and software application developed by Justin Frankel at Nullsoft in 2003 that features instant messaging, chat rooms, and file browsing/sharing capabilities. The name WASTE is a reference to Thomas Pynchon's novel *The Crying of Lot 49*. In the novel, W.A.S.T.E. is (among other things) an underground postal service.

In 2003, less than 24 hours after its release,[1] WASTE was removed from distribution by AOL, Nullsoft's parent company.[2] The original page was replaced with a statement claiming that the posting of the software was unauthorized and that no lawful rights to it were held by anyone who had downloaded it, in spite of the original claim that the software was released under the terms of the GNU General Public License.

Several developers have modified and upgraded the WASTE client and protocol. The SourceForge edition is considered by many to be the official development branch, but there are several forks.

Original author	Justin Frankel
Initial release	2003
Stable release	1.7 / 2008
Repository	waste.cvs.sourceforge.net/viewvc/waste/waste/ (http://waste.cvs.sourceforge.net/viewvc/waste/waste/)
Written in	C++
Operating system	Windows, Linux, OS X
Available in	English
Type	Darknet
License	GNU GPL
Website	waste.sourceforge.net (http://waste.sourceforge.net/)

Description

WASTE is a decentralized chat, instant messaging and file sharing program and protocol. It behaves similarly to a virtual private network by connecting to a group of trusted computers, as determined by the users. This kind of network is commonly referred to as a darknet. It uses strong encryption to ensure that third parties cannot decipher the messages being transferred. The same encryption is used to transmit and receive instant messages, chat, and files, maintain the connection, and browse and search.

WASTE networks

WASTE networks are decentralized (see social networks), meaning there is no central hub or server that everyone connects to. Peers must connect to each other individually. Normally, this is accomplished by having individuals sharing their RSA public keys, ensuring that their computers are accessible via the appropriate ports (one or more parties must have an IP address and port that can be reached by the other), and entering the IP address and port of someone on the network to connect to.

Once connected to the network, public keys are automatically exchanged amongst members (provided enough of the members are set to forward and accept public keys), and nodes will then attempt to connect to each other, strengthening the network (decreasing the odds that any one node going down will collapse or shut out any part of the network), as well as increasing the number of possible routes from any given point to any other point, decreasing latency and bandwidth required for communication and file transfer.

Since WASTE connects small, private groups rather than large, public ones, the network search feature is one of the fastest of all the decentralized P2P applications. Its instant messaging and file sharing capabilities are much closer to those of AOL Instant Messenger than more typical file sharing programs. Members of the network can create private and public chat rooms, instant message each other, browse each other's files, and trade files, including the pushing or active sending of files by hosts, as well as the more common downloading by users. Simple drag-and-drop to chat boxes will send files to their intended destinations.

The suggested size for a WASTE network (referred to as a *mesh* by users) is 10-50 nodes, though it has been suggested that the size of the network is less critical than the ratio of nodes willing to route traffic to those that are not. With original Nullsoft-client groups now exceeding ten years of age, it's not uncommon for stable meshes to host multiple terabytes of secure content.

By default, WASTE listens to incoming connections on port 1337. This was probably chosen because of 1337's leet connotations.

Since there is no central hub, WASTE networks typically employ a password or passphrase, also called a *network name* to prevent collision. That is, a member from one network connecting to a member of another network, thus bridging the two networks. By assigning a unique identifier (passphrase) to your network, the risk of collisions can be reduced, particularly with the original clients.

Nullnets

Nullnets are networks without a passphrase. It is impossible to know how many nullnets exist, but there is one primary nullnet. The best way to access the nullnet is to post your credentials to the

WASTE Key Exchange.[3][4] The nullnet can easily merge with other nullnets because there is no passphrase, which makes it a great place for public discussion and file sharing.

Strengths

- Secured through the trade of RSA public keys, allowing for safe and secure communication and data transfer with trusted hosts.
- The distributed nature means that the network isn't dependent on anyone setting up a server to act as a hub. Contrast this with other P2P and chat protocols that require you to connect to a server. This means there is no single point of vulnerability for the network.
- Similarly, there is no single group leader; everyone on the network is equal in what they can or cannot do, including inviting other members into the group, nor can any member kick another from the group, exclude them from public chats, etc.
- WASTE can obfuscate its protocol, making it difficult to detect that WASTE is being used.
- WASTE has a *Saturate* feature which adds random traffic, making traffic analysis more difficult.
- The nodes (each a trusted connection) automatically determine the lowest latency route for traffic and, in doing so, load balance. This also improves privacy, because packets often take different routes.

Shortcomings

- Trading public keys, enabling port forwarding on your firewall (if necessary), and connecting to each other can be a difficult and/or tedious process, especially for those who aren't very technically proficient.
- Due to the network's distributed nature, it is impossible to *kick* someone from the network once they've gained access. Since every member of the network will have that member's public key, all that member needs to do to regain access is to connect to another member. Coordinating the change of the network name is exceedingly difficult, so the best course of action is to create another network and migrate everyone over to the new network. This could, of course, also be seen as a strength.
- Since there is no central server, once someone disconnects from the network, they must know at least one network IP address to reconnect. It is possible that the network will drift from all the IP addresses used before so that none are known, and it becomes necessary to contact a network member and ask for address information to be able to reconnect. Indeed, it is possible that a

network could unknowingly split into two this way. It takes at least some coordination to keep a WASTE network intact; this can be as simple as one or more volunteers with a static IP address or a fixed dynamic DNS (DDNS) address (available free of charge from a number of providers) keeping their node up to allow people to reconnect to the network.

- While encryption is performed using the Blowfish algorithm, which is thought to be strong, the PCBC mode used has several known security flaws.
- Nicknames are not *registered*, which allows eavesdropping and spoofing. WASTE version 1.6 reduces the chances of eavesdropping by using public keys for communication, but as network members may choose any nickname a user must know and recognize the hash of the person they wish to communicate with to be sure of their identity.
- To connect from behind a firewall, one party must have the proper port forwarded to their computer; as WASTE networks do not depend on a central server there is no way around this. However, as long as one node accepts incoming connections it can act as a server, connecting nodes that cannot themselves accept incoming connections. Indeed, the long-term stability of a WASTE network depends on these hubs.

Versions

As of version 1.7, WASTE comes in an experimental and a stable release. The experimental branch implements a new 16k packet size, which improves overhead and transfer speeds, but is not compatible with previous versions which support a 4k packet size.[5]

WASTE 1.7.4 for Windows was released on 24 December 2008, and was current as of October 2009. This is a new branch on SourceForge created because of inactivity on the main WASTE development branch. This is the most fully featured version to date.[6]

A cross-platform (including Linux, OS X, and Microsoft Windows) beta version of WASTE called Waste 1.5 beta 4 a.k.a. wxWaste, using the WxWidgets toolkit is available.[7]

VIA Technologies released a fork of WASTE under the name PadlockSL, but removed the product's website after a few weeks. The user interface was written in Qt and the client was available for Linux and Windows.[8]

BlackBelt WASTE is a released fork of WASTE. Its build is labelled 1.8 to mark its significant improvements across its various areas of functionality. It supports Tor and i2p networks as well as clearnet. Its routing has been updated to provide even more obfuscated meta-data internally. It has uPnP support to automatically handle port forwarding. It also has automatic Anti-Spoofing

Technology to encourage unique users. Since May 2023, it also contains Conference VoIP. Under development since 2010, it currently (May 2023) has regular releases and improvements.[9]

See also

Free and open-source software portal

- Peer-to-peer (P2P)
- Anonymous P2P
- File sharing
- Friend-to-friend (F2F)

References

1. "AOL Execs Flush Nullsoft's WASTE" (https://betanews.com/2003/05/30/aol-execs-flush-nullsoft-s-waste/) . *BetaNews*. May 31, 2003.
2. "Nullsoft releases WASTE -- AOL pulls the plug" (https://www.afterdawn.com/news/article.cfm/2003/05/31/nullsoft_releases_waste_--_aol_pulls_the_plug) . *AfterDawn*.
3. "WASTE Key Exchange: WASTE 1.5 and 1.7 Nullnet Discussion" (https://wastekeyexchange.blogspot.com/2007/05/waste-15-and-16.html) . May 16, 2007.
4. WASTE Key Exchange Server (http://waste.nfshost.com/)
5. "WASTE again: Introduction" (https://wasteagain.sourceforge.net/introduction.shtml#whats-the-difference-to-original-waste) . *wasteagain.sourceforge.net*.
6. "WASTE again: Project News" (https://wasteagain.sourceforge.net/) . *wasteagain.sourceforge.net*.
7. "WASTE - Browse /wxWASTE Client_Server (POSIX) at SourceForge.net" (https://sourceforge.net/projects/waste/files/wxWASTE%20Client_Server%20%28POSIX%29/) . *sourceforge.net*.
8. "VIA Pulls PadLockSL - Slashdot" (https://slashdot.org/story/04/04/16/1215204/via-pulls-padlocksl) . *slashdot.org*. 16 April 2004.
9. "BlackBelt WASTE: Introduction" (https://sourceforge.net/projects/blackbeltwaste/) . *sourceforge.net/projects/blackbeltwaste/*. 2 August 2023.

External links

- WASTE again (https://wasteagain.sourceforge.net/) - a fork

- Original WASTE SourceForge site (https://waste.sourceforge.net/) - now defunct
- BlackBelt WASTE - Fork of WASTE with support for i2p and Tor as well as clearnet (https://sourceforge.net/projects/blackbeltwaste/)
- The World's Most Dangerous Geek(Rolling Stone interview with Justin Frankel) (https://web.archive.org/web/20100317095429/http://www.rollingstone.com/news/story/5938320/the_worlds_most_dangerous_geek) at the Wayback Machine (archived March 17, 2010)
- The Invisible Inner Circle (https://www.wired.com/wired/archive/12.04/start.html?pg=9)
- Anonymous Communication With Waste (https://web.archive.org/web/20050121093556/http://www.marktaw.com/technology/AnonymousWaste.html)
- 'Secure File Transfer With WASTE - Introductory video' (https://web.archive.org/web/20070804050303/http://www.showmedo.com/videos/video?name=sayersWaste000&fromSeriesID=63) by Russell Sayers at showmedo
- The Zer0Share Project (http://www.p2p-zone.com/underground/showthread.php?t=19077/) - Jack Spratts' Darknet