Anonymity on the Internet: Darknet

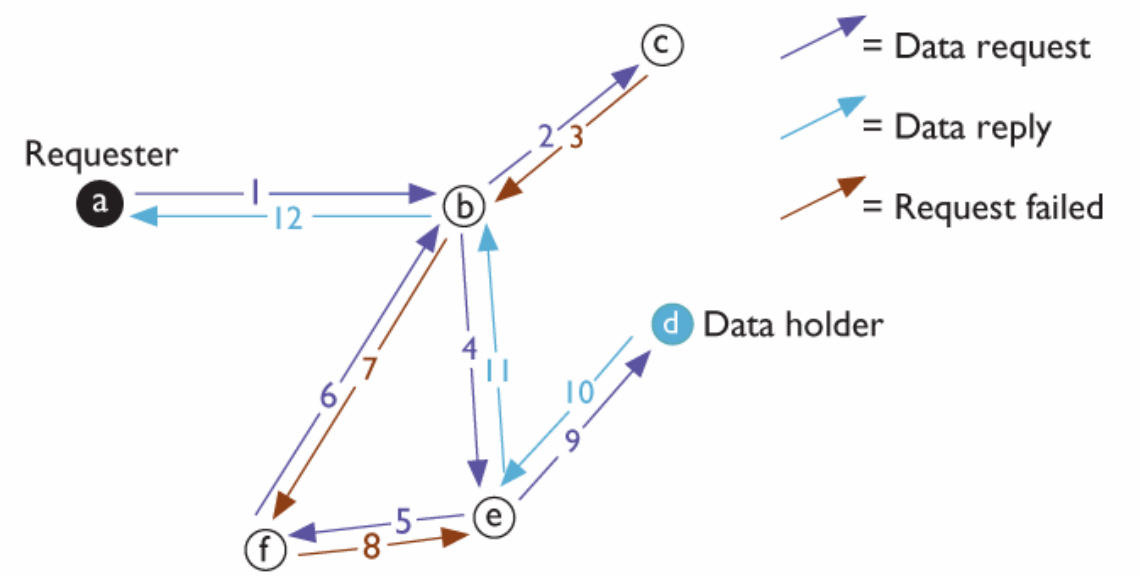
Abstract: An essay about anonymity on the Internet, why it is needed, how it can be achieved using darknets and a few examples of such networks.

By
Leon Ljunggren
Lelj1171@student.uu.se
841122-1412

"I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?'"

--

Mike Godwin, Electronic Frontier Foundation



An example of a request on Freenet.

Introduction
At first glance it might not be absolutely clear as to why anonymity on the Internet is needed. After all if you abide to the law and does nothing wrong there's no reason to hide, right? This is generally true (as long as it's possible to trust that the companies/individuals that gain information about your net activities doesn't misuse them, which they shouldn't since it's against the law) provided that you live in a functional democracy. Not everyone does however and even if you do anonymity is still a vital part in keeping a democracy functional. Without the possibility to speak up against injustice without fear of reprisal no democracy can exist. So clearly, not only is anonymity a nice thing to have when you don't want anyone to know you're buying adult entertainment but it is also a necessity for a democratic world.
The problem with anonymity on the Internet is that it is so hard to achieve, every computer connected has a unique address that makes it possible to track almost anything that this computer does on the net. One way of solving this problem and provide anonymity is the use of a darknet.

Darknet
In order to be totally anonym in a network no one can know anything about anyone. However this would make it impossible to communicate since if you don't know anything you don't know where to send the information you want to communicate. Darknets takes a slightly less strict path but still achieves pretty good anonymity.
The definition of a darknet is a virtual network of trusted computers that communicate with each others using strong encryption. It is still possible to see that a computer is a member of a darknet but it is impossible (provided that the encryption is strong enough) to tell what activities it is engaged in on that net. Most darknets provides some measure of anonymity among the members of the darknet by not routing traffic with a global end node, meaning that each node in the chain will transmit the information to the next one without knowing or caring if that node will retransmit it or not (more on this in the Freenet section).
There is several different kinds of darknets where some of the most popular are Freenet and Waste.

Freenet
Freenet is the largest darknet to date with a estimated user base of two million, and it is probably the most advanced, at least among those currently available to the general public. Freenet's main goal is to ensure freedom of speech and in order to do so it focus heavily on anonymity and attack resilience (so that information can not be removed by an attacker) at the cost of speed and the ability to search (although work is being done on improvements in both these areas). Freenet offers not only the ability to share files but also allows users to publish website like pages called freesites, however these pages are limited in the sense that it's not possible to use databases and scripting languages.
Since the goal of Freenet is freedom of speech it is not possible to remove files from the network, once a file has been added it'll remain on the network until it is no longer being accessed, in which case it'll removed through disuse.
Freenet is a peer-to-peer network with no centralized servers. As a participant in the Freenet network each user pitches in with a section of her own hard drive that can be used by the network for storing files (this is called the data store). The user has no direct control over what files get stored in her data store and in order to provide anonymity and plausible deniability the files are encrypted (this can of course be broken given enough computer power) so that the user doesn't even know what is on her data store.

Freenet uses something known as the small world phenomenon (the idea that a node is connected to any other node on the network through only a small amount of hops) as the basis of its network structure. Each node only knows of some neighbours and each of those only knows of a few others, but even though each node only knows a few others it is still possible to get from one node to any other in the network with only a small number of jumps, this kind of network is know as a small world network.
Freenet uses some of the most advanced routing seen in peer-to-peer networks, unlike systems like Gnutella and Kazaa, Freenet's routing system actually learns and adapts, proving faster services the more a certain object is requested (faster in the terms of lesser jumps). In order to provide anonymity each node in the routing chain are only aware of where it got the request from and where to send it, it does not know or care if the next node in the chain is the final destination or not. This does only provide rudimentary anonymity, it can (as with almost everything else) be broken if enough effort is put into it.
The scalability of Freenet is not known, however other similar topologies have been known to scale up to millions of users.

Waste

Waste is one of the few existing competitors to Freenet, although it appears that it is no longer under active development[1]. It was first released by Justin Frankel working at Nullsoft under the GNU General Public Licence, but was then withdrawn by Nullsoft's parent company AOL since the program wasn't part of the image they were trying to project to the public. However the program was picked up and continued by enthusiasts[2].
Waste is primarily intended for small groups of 10-50 participants and uses heavy encryption (RSA for authentication and Blowfish for the connection) to provide security from outsiders, however no protection is in place to prevent members of the group from eavesdropping on other members.
In order to make it harder for third party spies to realize that Waste is being used and how the protocol supports obfuscation and saturation (adding random traffic), this makes analysing the traffic more difficult.
Waste is based on the idea that only trusted computers should be allowed to connect to a certain group. To connect to the group you must have the IP, port[3] number and public key of one of the nodes already in the group and that node needs to know your public key and that it can be trusted. After connection to one node is established (provided that the node you connected to is able to authenticate you as a trusted user) the public keys of other nodes are exchanged and connections to other nodes will be established for more efficient routing.

Relakks

Relakks is the name of a service provided by the Pirate Party[4] and is advertised as being a darknet. However this is not true, it is actually a virtual private network that provides anonymous access to the Internet by letting the outside world (the net) see only that you're connected through Relakks' servers and not beyond that. Although this isn't entirely true either since by Swedish law the Pirate Party has to keep log files that can track your IP back to your ISP and thus back to you.

---

[1] The SourceForge.org version which is considered the main fork of the program haven't been updated since 2005. However no official statement has been made.
[2] An incident that is unseemly similar to what happened to Gnutella.
[3] The default port for incoming connections is 1337.
[4] A Swedish political party that failed to gain any significant amounts of votes in the resent election.

Ethical problems

While anonymity is crucial to the survival of our way of life (to put it the American way) it can also be a big problem when it's abused for malicious purposes. With anonymity on the Internet is becomes easier for child abusers and paedophiles to share their pictures and for terrorists to make their evil plans to destroy the world. This is an impossible problem, you can not have one and not the other. Either you accept the downsides and try to fight paedophiles and terrorist using other methods, or you do it the American way and forbid it outright[5].
The authors of Freenet and Waste obviously follows the previously mentioned philosophy, to them freedom of speech is more important than anything else, it is just unfortunate that what guarantees this can be abused (although some hard core freedom of speech fanatics claims that it should be everyone right to publish child pornography and plan terrorist attacks).

Conclusion

It is not possible to be entirely anonymous on the Internet, if someone wants to desperately enough and has the law on her side (or is willing to break it) then with enough work it is possible to track almost anything back to its source, just as it is possible to track almost any real life action back to the source within reasonable doubt. However it is possible to make it hard enough that tracking the source isn't practical.

Sources

Taylor, I. J. (2005). From P2P to Web Services and Grids: Peers in a Client/Server World. London
Freenet. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Freenet
Darknet. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Darknet
The Darknet and the Futre of Content Distribution. Retrieved 2006-10-19 From
http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm
WASTE. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/WASTE
Relakks. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Relakks
The Freenet Project. Retrieved 2006-10-11 From http://freenetproject.org/
Small world phenomenon. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Small_world_phenomenon
Small-world network. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Small-world_network
WASTE. Retrieved 2006-10-19 From http://waste.sourceforge.net/index.php
Pirate Party. Retrieved 2006-10-19 From http://en.wikipedia.org/wiki/Pirate_Party

Source critique

The book, From P2P to Web Services and Grids, is written by a trusted authority on the subject and should be fairly accurate, especially since the information is consistent with other sources. The web pages of different projects can be somewhat biased but for pure facts they should be trustworthy.
Wikipedia is a good source for information, especially on a technical subject, but one has to be on his guard in order to detect any errors or biased information.
It should be noted that the web page http://freenetproject.org/ could not be accessed when this essay was written. Instead Googel's cache, retrieved at 11th Oct 2006, was used.

[5] This could probably be used as an argument that Freenet isn't all that secure, since it's still in operation. However the main author, Ian Clarke, is Scottish so that might explain it.