Network anonymity

Joel Paulsson Charlotta Westberg
Email: {joepa089, chawe049}@student.liu.se
Supervisor: David Byers, {davby@ida.liu.se}
Project Report for Information Security Course
Linköpings universitet, Sweden

Abstract

Due to recent happenings in the world, such as the implementation of Internet laws, network anonymity has become a highly controversial subject. This report is a brief inventory of technologies and reasons for anonymity, and is based on literature studies and some basic testing through existing tests. It also covers whether or not anonymous networks truly are anonymous and how difficult it is to create an anonymous network. While all of the different technologies that were tested have a degree of anonymity, some appear more secure than others. Within this report, it is found to be difficult, if not impossible, to create a completely anonymous network; though it is possible for the user to hide the fact that he/she is anonymous. The results of this report give an indication as to which technologies and features are available to someone who wishes for anonymity as well as how to choose between those options.

1. Introduction

The definition of anonymous is nameless and without identity. [1] This definition opens up lot of questions about anonymity on the Internet. Are anonymous networks really anonymous? Nowadays there are a lot of options for being anonymous and many users trust in the anonymity of these products. Is that trust misplaced? While many users want to be anonymous, there are also many that want to break this anonymity so that users, for example, will not be able to commit criminal acts. There are some difficulties in creating an anonymous network, but what are they? Is it possible to hide the fact that you are being anonymous? This report answers these questions and its purpose is to bring an objective view on the anonymity tools that are available today.

Our method for this project has been focused on literature research. This means that we have looked through sources, such as scientific articles, books and newspaper articles for answers to the questions we've presented above.

We start by describing what alternative technologies there are for anonymity, and then we take a closer look at specific software that uses the technology. We have limited this report to not cover all technologies and services for anonymity, for example we chose not to write about anonymous remailers and chose only to write about services that are free. We then discuss the difficulties in creating anonymous networks. Finally we present our conclusions.

2. Background

Anonymous means to be nameless and without identity. Essentially, this means that anonymity is untraceable, and the only way to discover such a person is by coincidence or by the user breaking his own anonymity. [2]

Pseudonymity means that communications are inherently traceable. It may seem that the user is anonymous but it is possible to determine the identity of the user. Today we live in an information society and where it is hard to create true anonymity. For example personal information is freely available to the public through the Internet. [2]

A pseudonym means "false name" [1] and in use of pseudonymity. Some examples are pen names, aliases, or working names. On the Internet, a pseudonym is any identifier that a user applies in a specific context. The purpose of the pseudonym is to identify the user in a specific context and not for any other context. [3]

Anonymity has been sought after for ages. An example is the use of pseudonyms by writers; such as Charlotte Brontë who used the pseudonym Currer Bell during the beginning of the 19th century. [4] There are also old works that have been posted anonymously, either under the name "anonymous" or without any given name. Sometimes a story was told orally so many times that no one remembered who the original storyteller had been when the story was written down. This was the case of the epic poem Beowulf that is known to have been recorded on paper sometime before the 16th century. [5]

As the world continues to evolve, so does the need for anonymity. As the internet grows larger so does the need for anonymity. Today, you can write a “blog” on the Internet where you can present your views, daily events, or anything else that you wish to share with others. If you want your views or actions to stay hidden from the people you meet everyday, or vice-versa, you may use a pseudonym, as writers have done for centuries. [6]

3. Analysis

This section covers the use of anonymity on the Internet, and why there are two camps; one that wants to be anonymous and another that wants to remain public.

3.1. Why use anonymity?

Online anonymity is a subject of privacy since so many things that are done on the Internet can be traced back to the user. There are a lot of different opinions on why one should be anonymous. Some more obvious opinions are: illegal activities [7], espionage [8] and as mentioned above, privacy [9]. A few less obvious ones are research purposes [8], protecting sources [10] and censorship [9]. The reasons for being anonymous are numerous, but unfortunately all of these cannot be covered in this report.

When performing illegal activities the reason for being anonymous is generally to hide from the authorities. Some normal illegal activities on the Internet are the uploading and downloading of copyrighted material, paedophilia, organized crime, and many more. [11]

A reason for being anonymous while spying is to avoid getting detected by the victim or outsiders. One reason for wanting to spy is that a company wants to get company secrets from a competing company. [8]

Privacy is one of the most common reasons why a person should be anonymous while browsing the internet. User history, search history and visited pages are saved and accessed by; for example, companies that are interested in selling products that the user seems interested in. Some claim that these things, and more, violate personal integrity and choose to be anonymous. [8]

Investigating reporters, companies, authorities, and others perform research on the Internet, and it could harm the investigation if it is known that they are the ones visiting these sites. That is why research is a big reason why anonymity is used. [8]

Papers and other media can get information from anonymous individuals that would not dare to give out this information otherwise. This is a reason why the media wants to be able to use encryption and anonymity software on their sites. [8]

Governments, other authorities, and companies might block sites from being visited or words from being searched. In order to bypass these censorships, users can use proxies and anonymity services to browse outside of the allowed area, and being anonymous makes it harder for the censoring party to know who bypassed their censorship. [12]

3.2. Why defeat anonymity?

While there are those who want to be anonymous there are also those who do not want anonymity. In the previous section it was stated that some of those who want to be anonymous want it because they want to perform illegal activities. On the opposite side we have law enforcers. What were also mentioned above were governments, authorities and companies that apply censorship. These accompanied with the law enforcement are the major parties that have an interest in breaking anonymity to uphold the law [13] and censorship [14]. One of the less obvious reasons is mainly a concern for companies that apply censorship on their computers. When the employees browse the net on “insecure” sites, or unapproved sites, there is as always the risk of the company computer getting infected by malware [14].

Another reason to why some people do not want anonymity is a new directive that EU has passed to its members, the IPRED (Intellectual Property Rights Enforcement Directive). The Swedish implementation of this directive means that copyright holders are allowed to go to the court with the IP-address belonging to the uploader of their work to attain information about this person from the Internet service provider. [15] It will be harder to gain information about an uploader if the criminal is using anonymous services since the IP-address is the only information the copyright holder has that can tie a specific individual to the alleged crime. [16]

There are also those with the opinion that anonymity makes people act irresponsible, while if they were identifiable they would feel more responsibility. [17][18] These irresponsible acts can be everything from death threats to hate e-mails. [19] The debate evolves into a question between anonymity and privacy, both the US and EU countries have strict laws for what you may and may not do with others personal information, all to uphold privacy to their people. Those against anonymity argue that privacy gives accountability while anonymity does not provide this and this is why law obedient citizens should seek privacy and not anonymity. What they mean is that with accountability, someone can be held responsible for their actions; this does not mean that personal information is accessible by the public, but by governments and law enforcers. [20][21]

Many journalists protect their sources by letting their sources be anonymous, but this type of anonymity can also be misused. For example it can be used to misinform the public or frame someone that in the end can lead to the destroyed privacy of the framed person or something worse. [22]

There are many more reasons one would like to break anonymity but unfortunately all of these can not be covered in this report.

4. Anonymity Technologies

There are many technologies that ensure anonymity. This section covers technologies as well as services that use the technologies. There have been several services over the years that have made it possible to be anonymous on the Internet. We do not cover all of these technologies and services in this section. Some that we have not looked further into are anonymous remailers such as anon.penet.fi and mixmaster. A remailer is a technology that lets you send e-mails without revealing your identity. E-mails leave a trail behind them in the machines that they have traveled through, such as Date, time and IP-address. An anonymous remailer wipes the header of this information. [23] This report does not look further into solutions that cost money. A company that offers different kinds of solutions to the public and to companies and governments is Anonymizer.com who is the global leader in online privacy and identity protection solutions. [24]

4.1. Anonymous proxies

An anonymous proxy is software that can be used to hide the IP address is used to identify the user. When a user that uses an anonymous proxy and tries to access a site; the request will go from the client to the proxy server. The proxy server then forwards the request to the target server (the site the user wants to access) and the response is sent back to the client. This part is in effect the same as an ordinary proxy. An anonymous proxy hides information about the client, so that the target server never sees the protected information. A good web proxy service will set up a secure tunnel, like SSL, with the user that wishes to be anonymous [25]. There are different types of anonymous proxy servers, what differs between them is the degree of anonymity they provide to the user. One of the simpler types is when the anonymous proxy server tells the target it is a proxy, but it hides the client's information. A more complicated type is similar to the one above, but it will provide the target server with a false client IP address. The last, and most complicated, will not reveal that it is a proxy, and it will not tell the target server any information about the client. [26]

There are some risks when using an anonymous proxy. If the user that is browsing through the anonymous proxy does not encrypt data when it is sent to the proxy server; the proxy server owner could record important information, such as credit card numbers and passwords that the user sends while using the proxy. Another risk is if the proxy server is not configured correctly; that would make it possible for others to break into the server and access the user's private information. [26]

4.1.1. Hide My Ass!

Hide My Ass! is an anonymous web proxy that offers the use of SSL encryption for users that want the added security. This anonymous proxy hides the users IP address and changes it to an address that is located in the US. When using Hide My Ass!, each web address the user visits has an encrypted URL that expires after the user quits the session. If someone later tries to look at the user's history they will only see a scrambled URL. As an alternative, Hide My Ass! has many other free proxy sites in case they would be blocked. [27]

4.2. Virtual Private Networks

Studying the name Virtual Private Networks one word at a time, is the best way to explain Virtual Private Networks. Network means a connection between different entities to share information and if this network is private it is a closed community that is protected from unauthorized users. Authorized users are allowed to access different network based services and resources. The traffic within the private network only travels through the nodes in the private network, this traffic is isolated, meaning that it does not affect or is affected by traffic outside of the private network. The last of the characteristics is that it is a virtual network, which means that it is built on a physical network infrastructure. A VPN has other advantages than just providing anonymity but in this report only the service that has most relevance for anonymity is covered, which is Dial-Up VPN. Companies usually use this service so that users will be able to connect to their company network from outside of the company. This service may also be used for anonymity purposes by connecting the VPN to a proxy. This means that it has the same functionality as an anonymous proxy, but the connection to the proxy is achieved through a VPN. [28]

4.3. P2P Network anonymity

A peer-to-peer network is a technology created for simplified file sharing between users. The files are located on the users' computers, and other users can connect directly to these users to get access to download the files.

To be able to use a peer-to-peer network the user normally has to download and install software. The software enables the possibility to search and download files from other users that have the same software installed. It also enables the possibility of sharing your own files with the other users. The downloading of the files is made possible through a direct connection between the user sharing the file and the user downloading the file. [29]

There are a number of different ways to make a peer-to-peer network anonymous. Freenet applies one of these ways.

4.3.1. FreeNet

Freenet is a P2P storage device created for freedom of speech. In Freenet you act as a node and only know yourself and your neighbours in the network and no one else. All files that are stored on the network are shared between all the nodes in Freenet and the user has very little control over what is stored on his node, but can control how much data that is stored on the node. The only way to delete a file from Freenet is to stop searching for it and hope that everyone else does the same. When you store a file on Freenet you get a key, which is used to retrieve the file from the network. There are four types of keys in Freenet: content hash keys, signed subspace keys, updateable subspace keys, and keyword signed keys. Content hash keys are used for files and are made in a way so that you can't alter a file without someone noticing that it's altered. Signed subspace keys are used for pages that are going to be updated by the author and the key makes it so that no one else can pretend to be you and update the site. The updateable subspace key and the keyword signed key exist to make Freenet user-friendlier. The updateable subspace key works as a user-friendly wrapper around the signed subspace key. The keyword signed key is a user-friendlier key than the content hash key, but with the drawback that people can add files with the same name. [30]

4.4. Onion Routing

Onion routing has gotten its name from onions; an onion is a recursive layered data structure that defines the properties of a connection at each router. This means that the onion is an encrypted data message and when a router receives an onion it decrypts it. The first onion is decrypted with the routers public key. This onion is a connection request onion and the decryption of it reveals the cryptographic control information, the identity of the next router and the embedded onion. The router then changes the embedded onion to maintain a fixed size and then sends it forward. When a connection is established after having sent the first onion, the next onion contains data and is encrypted and decrypted with the cryptographic control information that was defined by the first onion. As data moves forward from router to router each router decrypts one layer of the onion and the data will reach the receiver in clear text. If data should be sent backwards it uses a reversed order of the defined encryption. Each onion looks differently to each router because of the layered encryption that is used, which makes the onion routing strong when it comes to resisting traffic analysis. This prevents the routers in between from knowing where the message comes from, where it is going and what it contains, making the communication anonymous. [31]

4.4.1. Tor

Tor is free open-source onion routing software. Onion routing is easy to implement on already running systems, which is why the user only needs to care about installing the software locally for it to protect the user's identity. Tor is compatible with most operating systems and software that connects you to the Internet. The Tor network creates routes by being able to connect to over one thousand servers that are positioned all over the world. Tor also has a special function that lets you have a web-server running, but protects its location. [8]

4.5. Breaking anonymity

One of the oldest technologies for anonymity is Onion Routing, which is the popular service Tor uses. Since it is popular there will be users that use it for illegal purposes. Over time, there have been parties that have the desire to end Tor. Some examples of attacks that can end Tor are timing attacks and none-secure plug-ins.

Timing attacks means that when a client connects to a web server, that web server modulates the traffic back to the client in such way that is easily identified by an observer. This traffic is built up through a “timing” circuit through each Tor server and then sends traffic through them and measures the latency. By determining the Tor servers that have a similar traffic pattern as the web server, the attacker can map the entire Tor circuit that the user uses. [32]

Some of the none-secure plug-ins that can disrupt Tor are Java, Shockwave, and media plug-ins like Windows Media Player and Realtime. Most of these reveal the client’s identity when it uses Tor; though these attacks depend a lot on security of the client’s system. [33]

One attack that is known to disrupt Freenet is what they call “adaptive search”. In general this means that the attacker listens for inserts that are made by the author of some content. The attacker has to be able to predict the content or the keys to be inserted for this to work. At every request the attacker gets a data point that point closer to the author's location, in the end, the author has been found, thus losing anonymity. [34]

Anonymous proxies can be broken through vulnerabilities that exist on the proxy server. These vulnerabilities include, but are not limited to: SQL injection, cross-site scripting, and SSL PCT handshake overflow. If these vulnerabilities are exploited DDoS attacks or remote code execution may be possible, as well as other attacks [35]. If the server owner is malicious he can save the user's data and use it for his own means. [26]

Regarding VPN we did not find any actual attempts to break this service, but the level of security you get depends on which VPN software you use. [36]

4.6. Difficulties in creating an anonymous network

Even though the user is using an anonymous network, he might not be entirely anonymous. One of the most obvious difficulties in creating anonymous networks is the ignorance of the user. The creator of the anonymous network cannot feasibly foresee what kind of applications and vulnerabilities that exist on the client computer. [37]

5. Testing

Testing these anonymous services wasn't a priority; we used one basic type of test that is provided by Audit My Pc [38]. Their test displays the information that your computer gives away, while using some of the services mentioned. Without any service the test accurately provided a location, IP-address and the internal IP-address of the computer. The system we tested these services on was a computer that was running a fully updated version of Windows XP and the browser that was used was Mozilla Firefox 3.0.9. The system was behind a firewall.

We started by testing two proxies, Hide My Ass! and Kproxy [39]. Both of these showed another location and IP-address than the one we used to access the Internet. However, when we used Kproxy it found the internal IP-address of the computer.

We tested Tor with two different browsers. We began by testing it with the zero-bundle install from Tor, which has the browser Firefox 2.0.0.14. Secondly we tested the install bundle with the normal browser used on the system. In both cases the test showed a different location and IP-address than the original.

We tested a VPN service called Ivacy [40]. Ivacy is VPN service, where you connect through VPN to an anonymous proxy. The test showed a different location, IP-address and internal IP-address then the original.

6. Conclusions

By reading through the sources, writing this report, and performing tests we have come to several conclusions about network anonymity.

As we described earlier anonymous means to be nameless. Translating this for computer use means that it is impossible to make a connection between your physical person and your Internet identity. From what we have discovered we can conclude that this is a very difficult, if not impossible feat. A very low degree of anonymity is needed to hide your IP-address, but advertises you are anonymous. The closest we can get to complete anonymity is to hide the fact that we are being anonymous and hope that no one can make a connection to us in spite of this. However, even if an attacker realizes you are being anonymous it isn't obvious what kind of anonymity service you are using, which makes it harder to connect your Internet identity to your physical person. A clarification that we would like to make on the whole subject of anonymity is that normally only the IP-address is anonymous, not the traffic that is being sent.

When you decide to use an anonymity service you should trust it to a certain extent. You should probably test it to make sure you have anonymity where you want it, before you use it for sensitive services or sending of information. It also seems dangerous to write and do anything just because you are anonymous since no service provides complete anonymity. There is also the issue of malicious server owners that track everything you do and can even see things such as account numbers if you decide to send it over the anonymous network.

The main difficulty in creating an anonymous connection is the user. The service used might be good at what it is supposed to do but with a none-secure system it does not matter how secure the service is because there might be a leak somewhere else in that system. There is the risk that other parties might block anonymous services and therefore the user needs to hide the fact that it is using an anonymous service. It is technically difficulty to hide the fact that you are being anonymous. In addition to creating the anonymous service, you have to think about making the anonymous service anonymous. It is definitely possible to hide the fact that you are being anonymous. There are quite a few services that provide this feature. However, to completely hide the fact that you are being anonymous you cannot write your real name anywhere, but always have to use your Internet identity.

As described earlier the debate about anonymity evolves into a question about privacy and anonymity. Those against anonymity argue that what we want is privacy because it brings accountability while anonymity does not. They mean that someone who is law obedient should strive for privacy and not anonymity. A normal quote that is used for opposing anonymity is: “If you have nothing to hide, why hide it?” In conclusion to this debate we want to say that anonymity is needed for many legal and valid reasons, for example what about those reporters that report about the terrible things happening in countries where freedom of speech is not as obvious as it is in others? It is not viable that they should risk death because they report the truth.

There are many legal reasons as to one would want to use anonymous services, the illegal reasons almost always get more attention by the public. We consider it to be quite obvious that anonymity services will be used for illegal activities. We can compare it to the fact that a criminal that robs a bank uses a hood over his face; no one wants to get caught. However, because of this, there will always be a strong opposition against anonymity services, and the ones using them for legal reasons will be pushed aside.

In conclusion we can say that anonymity exists everywhere. Anonymity on the Internet exists in different degrees and when choosing a service, you should decide the level of anonymity you need. You probably should think hard about whether or not you really need to be anonymous. Regarding whether or not you should trust anonymous services our answer is maybe, but probably not. Always test the connection to see if it meets your needs for anonymity, and make sure that the server is one that you can trust, while keeping in mind that there are malicious server administrators. Also be aware of the fact that if someone puts real effort into finding you, they will; even though you are hiding behind what we call anonymity.

References

[1] Dictionary.com, http://dictionary.com, 09-04-24

[2] Computer Crime Research Center – Anonymity in cyberspace: finding the balance, http://www.crime-research.org/articles/2110, 09-05-01

[3] Bleumer G. (2004) Pseudonyms http://www.francotyp.com/research/bleumer/EncInfSec/GBl.Pseudonym.pdf

[4] The Literature Network – Charlotte Bronte, http://www.online-literature.com/brontec/, 09-05-03

[5] About.com – Beowulf - what you need to know about the epic poem, http://historymedren.about.com/od/beowulf/p/beowulf.htm , 09-05-03

[6] HASTAC – Anonymity and pseudonymity - building reputation online, http://www.hastac.org/node/1904, 09-05-03

[7] Svenska Dagbladet – Lagbrytarna har initiativet, http://www.svd.se/kulturnoje/nyheter/artikel_2596889.svd , 09-04-22

[8] Torproject, http://www.torproject.org/torusers.html.en, 09-04-22

[9] Dagens Nyheter – Många vill smygsurfa efter fildelardomen, http://www.dn.se/nyheter/sverige/manga-vill-smygsurfa-efter-fildelardomen-1.849472, 09-04-22

[10] Svenska Dagbladet – Stort intresse för anonym surfning, http://www.svd.se/nyheter/inrikes/artikel_2687187.svd, 09-04-22

[11] Wallace J.D. (1999) Nameless in Cyberspace Anonymity on the Internet CATO Institute Briefing Papers

[12] Reporters without borders – How to blog anonymously, http://www.rsf.org/article.php3?id_article=15012, 09-04-23

[13] Svenska Dagbladet – ”Ipred-lagen kan försvåra utredningar av barnporr”, http://www.svd.se/nyheter/inrikes/artikel_2038299.svd, 09-04-23

[14] Aladdin – Block anonymous proxies with esafe, http://www.aladdin.com/esafe/block-anonymous-proxies.aspx, 09-04-24

[15] Dagens Nyheter – Ipredlagen i korthet, http://www.dn.se/kultur-noje/ipredlagen-i-korthet-1.834782, 09-04-24

[16] Aftonbladet – Nya lagen full av hål, http://www.aftonbladet.se/nyheter/ipred/article3938506.ab , 09-04-24

[17] Townhall.com – Internet anonymity is as destructive as internet porn, http://townhall.com/columnists/DennisPrager/2007/10/23/internet_anonymity_is_as_destructive_as_internet_porn, 09-05-03

[18] Tim Courtney – Why anonymity on the Internet is bad, http://www.timcourtney.net/2007/07/28/why-anonymity-on-the-internet-is-bad/, 09-05-03

[19] BBC News – Call for blogging code of onduct, http://news.bbc.co.uk/2/hi/technology/6502643.stm, 09-05-03

[20] Bob Parsons – How anonymity hides the bad guys, http://www.bobparsons.me/WhyprivacymakestheInternetsaferHowanonymityhidesthebadguysp.html, 09-05-03

[21] David Lawrence Show – Privacy? Good. Anonymity? Bad, http://www.thedavidlawrenceshow.com/privacy_good_anonymity_bad_002281.html, 09-05-03

[22] Washington Post – Two bad cases for anonymity, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/09/AR2006060901552.html, 09-05-03

[23] Email Privacy, http://www.emailprivacy.info/remailers, 09-05-03

[24] Anonymizer.com, http://www.anonymizer.com/, 09-05-03

[25] Tech faq – What is anonymous surfing?, http://www.tech-faq.com/anonymous-surfing.shtml, 09-04-20

[26] Articlepool – Risks and benefits of using anonymous proxy servers, http://www.articlepool.com/risks+and+benefits+of+using+anonymous+proxy+servers-48226, 09-04-20

[27] HideMyAss, http://www.hidemyass.com/proxy, 09-04-20

[28] Venkateswaran R. Virtual Private Network Potentials, IEEE, February-March 2001 Vol. 20 Issue 1 on pages 11-15

[29] P2P World – How peer to peer works, http://www.solyrich.com/how-p2p-works.asp, 09-03-30

[30] FreeNet, http://freenetproject.org , 09-03-26

[31] Goldschlag D. Reed M. Syverson P. (1996) Onion Routing Communications of the ACM, February 1996 Vol. 42 Issue 2 on pages 39-41

[32] Hopper N. Vasserman E. Y. Chan-Tin E. (2007) How much anonymity does network latency leak? 14th ACM conference on Computer and communications security on pages 82-91

[33] Suess M. (2008) Breaking TOR anonymity http://www.csnc.ch/misc/files/publications/the_onion_router_v1.1.pdf

[34] Freenet Project, http://freenetproject.org/faq.html, 09-04-24

[35] Express Computer – Risks posed by anonymous proxies http://www.expresscomputeronline.com//20080317/technology02.shtml, 09-04-24

[36] Linux.com – SSL VPNs and OpenVPN: A lot of lies and a shred of truth, http://www.linux.com/feature/48330, 09-04-24

[37] Tor Project, http://www.torproject.org/download.html.en, 09-04-24

[38] Audit My Pc, http://www.auditmypc.com/, 09-04-24

[39] Kproxy, http://www.kproxy.com, 09-04-23

[40] Ivacy, http://ivacy.com/, 09-04-24