Network anonymity

Anders Hongslo Gabriel Jägenstedt
Email: {andho212, gabja964}@student.liu.se
Supervisor: David Byers, {davby@ida.liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

This report aims to observe the problems of accountability and anonymity in a technical setting. It lists a few of the possible ways to conceal the identity of an individual on a network. It also discusses why the properties are needed and who needs them. We also give a brief description of the actual problems that turn up when dealing with the area. We observe the chosen services with anonymity and accountability trying to determine who would have the upper hand if push comes to shove.

1. Introduction

Being anonymous is important for people for many reasons. The motives however are very morally diverse and ranges from freedom of speech and exposing injustices in oppressive regimes to planning terrorist attacks. If one wants to protect the anonymity of those with noble motives it is hard to hold criminals accountable for their actions since their anonymity is then protected as well. This dilemma of anonymity versus accountability is now more relevant than ever and this report investigates some of the practical methods to remain anonymous online in relation to these terms.

In order to hold someone accountable one must first find them. This makes anonymity and accountability hard to discuss without in some way touching on the other.

The question of who needs to be held accountable is not always as clear cut as one would think and is a matter of perspective. One man's "freedom fighter" is another man's "terrorist". But this report is not one of morals, it discusses the technical services and methods.

Under the headline “2. Background”, this report aims to first define anonymity and accountability and describe some of the actors on either side of the debate.

Under “3. Analysis”, we will give an overview of different methods available that aims to grant the user anonymity online. In “3.2 Evaluation and comparison” these services will be discussed in terms of anonymity and accountability.

The headline “4. Related work”, will contain a listing of works that have previously partly or in full covered the area and discuss how it relates to this report.

In “5. Conclusions”, we describe how the work has gone as well as the result of the evaluation.

2. Background

2.1 What is anonymity?

For the purpose of this report anonymity is when a person manages to conceal their true identity.
There are many facets to anonymity and different parts of one’s identity that can be concealed. It is also possible to attain different levels of anonymity, especially in regards to how easy it could be broken or subverted. For example one could successfully hide what address a certain mail originates from but still sign it with ones name.

True anonymity in any system would entail that given full knowledge of that system, the origin and destination of any message in the system cannot be determined. This however is not a goal that is easily reached in any system of reasonable size. At the same time, for any system of reasonable size it is hard to gain full knowledge. Since this is true it might still be possible to attain anonymity in regards to the difficulty in processing data surrounding the messages.

When we talk about messages in a system we refer to any passing of information between two parties within any set of communication channels. For example the sending of mail over SMTP or speaking face to face.

2.2 Motivations for Anonymity

There can be any number of reasons to conceal your identity. It is very common to focus on the fact that you might have something to hide, that you want to protect yourself from warranted or unwarranted persecution. However that is far from the only reason to be

anonymous. It is not possible to enumerate all the possible reasons a person may have but one could consider illegal activities, political persuasions, integrity or perhaps someone would just prefer if others stayed out of their business.

2.3 Actors of Anonymity

It's hard to put a label on those that are interested in anonymity. The group contains terrorists, governments, reporters, political activists and criminals as well as a myriad of others.

2.4 What is Accountability

In many ways accountability is the counterpoint of anonymity. Accountability means that on observing a message in a system the viewer can determine the source.

Accountability is a desired property of a system when there is a risk of someone using or abusing the system for criminal activities but undesirable when the user has a legitimate reason for concealing their identity, such as freedom fighters, political activists and for that matter ordinary people protecting their integrity. The problem is that it is nigh on impossible to distinguish these from each other and that the line between the two groups is likely to have different placement in different countries and according to different people. This is likely the reason that most anonymizing services don't provide any ways to get accountability. There would of course be possible ways to do this; one could have backdoors in the servers and clients that would give any authorized person access to the relevant data needed for tracking criminals. But what is the guarantee that no unauthorized use of this occurs? Most certainly no such guarantee can be made using the current systems.

Perhaps it would be possible to implement using some form of shared key encryption protocols where say a company, a state and a human rights group would need to all work together in order to put together a working key to decrypt records. If this has been studied or done before we certainly haven't heard of it. Given enough knowledge about most systems it would still be possible to track who speaks with whom, but suffice to say it will be a very time consuming and expensive action that might well not be worth the effort and most people don't have that good knowledge of the system, especially when it gets to the size of the internet.

2.5 Motivations for Accountability

Some people's actions online might hurt others. Amongst these are slander, defamation, bullying or spreading lies.

Bringing child pornographers to justice is another reason to hold people accountable for the material they spread online.

Terrorism is another often cited reason to emphasize accountability over anonymity. Many laws and restrictions have been put in place to thwart terrorist activity.

2.6 Actors of Accountability

Governments try to make sure that its citizens are accountable for their actions according to the law. Other actors are law enforcement on both local and international levels, corporations and anti-terrorist efforts. But in any state it is also important that the state, the government, the law and all other factions of power be held accountable to the people.

2.7 Accountability vs. Anonymity

The culture and where you live decides much of what is morally and legally allowed. The Internet is global but the laws which hold the individual accountable are local.

An oppressive regime might label dissidents traitors or potential terrorists and deal with them accordingly. In that case it's the very authority they are criticizing which decides whether or not the criticism is allowed or not. Expressing certain opinions or exposing certain information might be viewed as a threat to the order of the country, a try to instigate chaos or undermine the authorities, even if the information is true. This is also a problem in democratic countries; an example is the leaking of Guantanamo Bay operating procedures or military information on Wikileaks. If such sensitive material is leaked one could either argue that a traitor puts the national security at risk and should be held accountable or one could argue that such whistle blowers must be allowed anonymity in order to hold governments accountable for their actions.

3. Analysis

Here we describe different anonymizing services, take a look at how they try to offer anonymity and if users can be held accountable using the service.

3.1 Services

3.1.1 Tor

Tor is an acronym standing for The Onion Router. It provides routing algorithms with intermediate encrypted hops. Tor is based upon Onion routing gets it name from the way an onion is layered, if you peel away one layer another is beneath it. In the same way Tor encrypts the

packet it is sending in several different layers. However Tor does not implement it in the same way as the original paper on onion routing described. Tor is implemented as a sort of proxy where you send an encrypted message to a node in the network. Only this node can decrypt the message and see what is within, the contents can either be the final message or another layer of encryption with another node as destination. In order to know how to encrypt the data Tor negotiates public keys for hops and these keys are subsequently deleted to protect from replay attacks and malicious nodes being able to compromise other nodes in a circuit. The big upside of Tor is that any TCP packet can be sent through it. This means it is quite easy to set it up so that any of your clients can use it. It is important to remember that encryption is not end to end in Tor. The communication between the final node in the chain and the final destination (somewhere on the internet) is sent unencrypted unless the user has ensured that this step is encrypted as well.

The Tor network consists of a set of Onion Routers that register with all other routers in the network via TLS connections. All Tor users run Onion Proxies that enable them to make connections to the network. The routers in the network maintain two keys. The long-term identity key is used to authenticate the router by signing TLS connections and the routers descriptor containing information that the network needs to know. The short-term onion key decrypts requests for setting up circuits. The short-term keys are cycled periodically to make attacks against single node (routers) less effective. When a user wants to communicate over the network they must negotiate keys for the transfer incrementally. This means that each hop that is to be included in the circuit must help in negotiating the key for the next hop so that the sender gets a full list of keys that only work between the intermediate nodes. These keys are then used to create the "onion" from the original data.

3.1.2 I2P

I2P is an anonymizing network with many similarities to Tor. It is a distributed and dynamic network that has no trusted parties. It uses a layered encryption method to conceal who the original sender or uploader was.

I2P differs from Tor in that it has end-to-end encryption if the server on the other end has support for it. It is just like in the case of Tor possible to set up a proxy to handle a diversity of communication. I2P can handle both UDP and TCP traffic whereas Tor is only designed to work with TCP. There are a few things that set I2P and Tor apart. The most notable is the way that they refer to concepts. I2P more consistently calls nodes routers and endpoints where in Tor it can vary. I2P has Tunnels that can be likened to the chains in Tor. But this is all quite petty; the biggest difference is probably what in I2P is called netDb. NetDb is a database of routers in the I2P network and is used to track routers, their guessed distance from each other and other things that help with deciding what nodes to use for the best balance between security and performance depending on what the user expects. In the netDb each router has an ID and a leaseset. A routers ID provided by three parts. These are a 2048bit ElGamal public key, a 1024bit DSA public key and a certificate. These are the keys used to negotiate paths between nodes and encrypt the messages sent through the network. The leaseset has a destination provided by a structure such as the router ID, it also has a list of leases and a pair of keys for encryption.

3.1.3 Freenet

Freenet is a decentralized censorship resistant data-store. That is it can be use to surf so called “freesites”, chat on forums, share information and so on.

It is only possible to access information that is stored in the Freenet. In other words Freenet can be seen as an application level network that provides anonymity.

Freenet provides, through its decentralization, a way to distribute your opinions without being held accountable. Although it provides great anonymity it is not widely spread and as such only so much information can be found on the network and only so many people can actually see your contributions to it. On the technical side of things Freenet consists on a set of Freenet clients, a client can query the network, upload data and so on. The Freenet Client Protol is a message passing protocol built on TCP that provides error handling, prioritization and standardized data types. All clients in the network give up an amount of their resources to the distributed storage.

3.1.4 OneSwarm

OneSwarm is a peer-to-peer tool which is used to share files online. It offers explicit control over privacy settings and the user can decide to make files public or to only share them with friends or only specific friends. Instead of transferring data directly from one user to another OneSwarm may relay the encrypted traffic through multiple other friends to obscure the identities of those involved.

The three basic categories for shared data are: public distribution, with permission and without attribution. Public distribution uses public means such as the built in Bittorrent functionality to exchange data with users outside the swarm which is a very easily tracked method

of sharing and provides in essence no anonymity at all. With permission allows users to restrict access to files to their added friends; all users with permission to access the files can recognize each other to create a swarming download of the permitted files. Without attribution is used for material the user deems sensitive. Unlike the other categories this data is not directly advertised as available from the user at all, rather it's found through keyword search for the data. The data is then sent through an unknown number of intermediary nodes in the swarm until it reaches its destination.

Each OneSwarm user generates a 1024 bit RSA key pair, one public and one private. The public key is used as an identifier allowing users to connect to each other when online. The public key is combined with IP and port numbers to create entries in a distributed hash table (DHT) which is used to tell clients how to connect to users where we know their public key. Distribution of public keys can be done for instance over existing social networks such as Google Talk or Facebook or by email invitations. Distribution can also be done by community servers which maintain and share peer lists via SSL. Community servers help users to get untrusted peers for sharing data without attribution. Peers are untrusted by default and the user can then choose to change their trust level. To locate data sources we flood object lookups through the overlay and then use the reverse paths to transfer the data, obscuring the identities of sender and receiver by address rewriting.

3.1.5 Anonymizing proxies

A proxy server works as an intermediary connection by forwarding traffic sent and received by the users' computer. So by relaying all Internet traffic through an anonymizing proxy the traffic can be traced to the proxy server and not the user. The normal way to implement an anonymizing proxy is through using pseudonyms. This means that when a connection request comes through a proxy, information about the sender is saved in a cache so that responses can be returned directly to the sender. Unless the user sets up some sort of proxy chain the single proxy is all the assurance you can gain and you have to trust that server not to give out information about who connects where to those who ask for it. Anonymizing proxies exist in an abundance on the Internet. They can be private or public, free or non-free. No matter which type of proxy is chosen you will have to take into account how easily information about the service can be gathered by someone that wants to know either what you are communicating with or who has accessed a certain site or service on the Internet.

3.1.6 Anonymous remailers

An anonymous remailer is a service with which it is possible to falsify or hide who originally sent an email. There are several types of anonymous remailers with differing levels of anonymity.

The simplest, which may not even be counted as anonymous in many cases is called a Pseudonymous remailer and is where the senders address is stripped away but stored in a cache on the service so that it is possible to reply to it at a later point. To find the sender of the email you typically have to get it from the service itself, which may be more or less simple. Another possibility is to track the incoming and outgoing connections.

More secure than the just mentioned is a Cypherpunk remailer, also known as Type I.

A remailer of this type fully strips the sender from the mail without storing a return address. It is good for sending emails that should not get responses. For example spam or ransom demands.

Mixmaster remailers, also known as Type II use a layered approach, much like that of Tor but without return paths. Mixmaster pads messages to a set size and splits them into chunks. Chunks are resent between a set of remailers known as mixers out of order to make traffic analysis much harder.

Mixminion remailers, Type III is an attempt to provide a greater degree of flexibility than that of Type I and II. One of the things that it does is to give a choice to the user about whether it needs to be able to receive responses to a message. When the answer to this is no a method called forward anonymity is used which pretty much means that a path in the mixminion network is picked out and no return address is specified. Each chunk of the message is given its own path that may or may not be the same as the path of other chunks. When a user wishes to allow replies to anonymous messages they create a SURB(Single Use Reply Block) that contains the path back to them encrypted using the mixes on the paths keys. As the name states this SURB can only be used once and will not allow tracing of the sender.

3.1.7 Secure VPN

Secure Virtual Private Network works by granting the user an encrypted tunnel to a VPN server which can relay Internet traffic. In this case all traffic in the tunnel between the user and the endpoint at the VPN server is encrypted and therefore it is safer for the user to use public access points to the Internet with a secure VPN than with for instance a proxy server where this traffic isn't necessarily encrypted. Obviously it is important that

you can trust your VPN provider not to monitor or log your connections in order to remain anonymous. Secure VPN technologies include SSL/TLS, IPsec and IPsec inside L2TP. In order to establish a VPN tunnel the endpoints must authenticate between each other. This can be done in a number of ways including, but not limited to passwords, biometrics and digital certificates. Most of the time the encryption over the VPN tunnel will be a lot harder to break than aquiring a password or other means of attacking the endpoints authentication method. Since there are a number of different ways that VPNs can be set up there can be a lot of different encrytion methods and ciphers that provide the actual tunnel security.

3.2 Evaluation and Comparison

Here we intend to compare the services we have chosen to evaluate. Among the chosen services there are a few that are in many respects very insecure if you are looking for anonymity in any viable sense. The biggest problems are the services that provide anonymity basically through pseudonyms. The only thing needed to subvert this anonymity is to subvert one single node, the place where the identities are switched. Specialized anonymous networks are much harder to find single points of failure in. But given full knowledge of the nodes in question as well as being able to draw conclusions from timing of packets, power usage and energy emissions for example it might still be possible to get a good idea of how messages are passes as well as which nodes are involved in any single communication.

Some services work with issues of trust, others disregard it entirely and yet others work on the basis of removing trust from the equation, which is done by trusting no single node.

3.2.1 Tor

Tor does not claim to provide perfect anonymity. Even though it is probable the most well known free alternative for getting anonymous communication they still tell the users that it should not be used for anything where you need total anonymity. But taking aside the fact that Tor might not be usable for business critical anonymity it still provides a great deal of assurance that your identity is not likely to be traceable.

Since the design of Tor has three types of nodes these must be taken into account when observing the security of the service. The nodes we speak of are entry nodes, exit nodes and intermediate nodes. Compromising a node has different effects depending on which type it is. Certainly a compromise in the entry node is the most problematic since this would mean that the person seeking anonymity's own computer has been compromised. In this case all is lost and accountability can be assured. In any of the internal nodes a compromise is not as dangerous because it is truly difficult to determine anything beyond which node the message came from and which one is next in the chain. If it is possible to know where in the chain an internal node is it might be possible to draw conclusions about the sender and receiver but since packages are uniform and provide no real indication to what they contain this should not be possible. The final type of node is an exit node, this type of node is the most likely to be able to break the anonymity of the system if compromised (apart from the entry point of course). The problem with the exit node is that it will have access to the actual packets that are to be sent to a target so if anyone subverts one of these it might be possible to track the source using information from their communication patterns. For example if you log in to Facebook from an anonymous connection and at the same time post some anonymous comments on a forum within the 10 minute period that a chain is used an attacker would be able to correlate the two connections and anonymity would be void. In short, don't expect anonymity if you give away your identity. Another problem with an exit node is that it would be possible that the owner of that node could be accused of being guilty of the actions of those that are behind the Tor network. In general it is possible to show that since you own and operate such a node you can't really be held accountable for what goes on over your network. This in itself might also be considered an added bonus for the person owning the node. It will be hard to distinguish traffic that originally comes from the node to traffic coming from some other node so the owner could possibly use this argument to negate attempts to hold him/her accountable.

3.2.2 I2P

Although some of the design of I2P differs a bit from how Tor provides the same service it still has the same basic set of nodes that can be compromised. The routers are untrusted and have about the same possibility to take control of communications as internal nodes in Tor. The endpoints are more vulnerable to attack but just as with Tor it is difficult to trace traffic just through owning one endpoint and it is truly hard to know what endpoints you need to subvert in advance so it's likely an attacker will be too late. I2P has a lot more traffic shaping functionality than Tor, where Tor decided to remove a lot of that functionality due to performance issues I2P is still a lot more secure in this area. Tracking traffic within the network is probably harder since it provides this traffic

shaping but it would most certainly bring down the performance of the service. Packet delays and padding of messages are very helpful in foiling attempts to analyze it. All in all the security of Tor and I2P is most likely equivalent, with only minor bonuses for the respective parts.

3.2.3 Freenet

The message passing part of Freenet is much like that of Tor and I2P and we won't discuss it here as hold the same problems as those services. The interesting part about Freenet is that it was designed primarily to enable anonymous distribution of data. To ensure accessibility, data that gets uploaded into the network gets tagged with unique IDs. These IDs are used by Freenet to locate a copy of the original data. Since the data is distributed and replicated it is hard for an attacker to locate and stop the data from spreading and therefore Freenet is very censorship resistant. When an upload has been made to the network it is no longer possible to find out where the data came from. Therefore the systems greatest weakness is when you upload to the network as well as when you download things from it.

3.2.4 OneSwarm

The degree of accountability and anonymity here is entirely dependent upon how OneSwarm is used. If used as a regular Bittorrent client the user is fully accountable since OneSwarm doesn't offer any anonymity then. If used to share and download files marked with without distribution the accountability is low because of the extensive anonymizing features in OneSwarm. Persistent peers limit the ability of attackers to arbitrarily inject nodes into the overlay; this limits for example pollution attacks. Using both trusted and untrusted links in the overlay makes it harder for an attacker to figure out the path based on timing information. OneSwarm introduces delays for queries from untrusted users; these delays are calculated from the content's hash. A client's limited view of the overlay and the inability to control path setup defends against correlation attack in which the attacker correlates performance to ongoing transfers. OneSwarm cites deterministic decision making as a way to foil statistical attacks, no information such as delays can be statistically inferred. Rapidly changing paths between users makes it more difficult to figure out user behavior.

Collusion attacks however are very effective when it comes to inferring data sources although it requires the colluders to be directly connected to the target. If an attacker has many colluding clients connected to a community server it might compromise the target's anonymity. However the accountability is going to be probabilistic since the collusion just shows a certain chance of the target being the data source for a search.

How much information an attacker can infer depends largely on how compromised the target is and the target's settings. If the attacker manages to become a trusted peer or has full access to a trusted peer then a lot of information is obviously exposed by design. A user concerned with privacy will thus avoid using the Bittorrent client, avoid public community servers and pick both his untrusted peers and especially trusted peers with great care.

3.2.5 Anonymizing proxies

Since anonymizing proxies depend entirely upon one single point of failure it is by far the easiest service to break. There exist proxies that are free and there exist those that cost money. In either case since there is a single point of failure any problems with the node could mean you lose your anonymity or that the service becomes unavailable. When you use a proxy you are putting a high degree of trust on the provider. You trust that they won't divulge your identity or abuse it. This makes for a simple target when you want to hold someone accountable for some action. You only need to go through one person. Of course it is possible to use proxy chains which would in many ways solve some of the problems but every single node could still make the service unavailable unless you have planned for it by having some sort of dynamic proxy chains. If you do this you are getting close to Tor in complexity but still lack the protection between nodes provided by an encrypted normalized transmission. Since there is still no encryption in proxies you can probably trace a single transaction just by observing traffic to and from the proxy. Also proxies generally don't have any traffic shaping functionality that can make traffic analysis extra difficult. But even if you don't control the network between the nodes you might be able to get at the original sender/receiver by following the chain and taking control of one node at a time.

3.2.6 Anonymous remailers

Anonymous remailers do not offer data anonymity. The main purpose is to hide the origin of the message and not the contents thereof. With that said the different types provide varying degrees of anonymity and accountability. All of the services do require some trust in the service provider since it is possible for them to log the traffic. Pseudonymous remailers logs traffic by design

and is therefore the by far least secure solution, defective by design unless you consider accountability a feature. Cypherpunk and Mixmaster remailers offer very good anonymity if correctly implemented; i.e. no logs of traffic and counter-measures against timing attacks or energy emission attacks such as delays and padding of messages. Neither Cypherpunk nor Mixmaster allow two way communication since no return address is stored. Mixminion however offers TLS tunnels instead of SMTP which provides a decent link encryption between mixes making identification of sent data harder to accomplish. The biggest difference between Mixminion and other remailer types is the way it handles replies. It is possible to reply once to a mail using a temporary key but only once.

3.2.7 Secure VPN

The security of the secure VPN depends a lot on which protocol you use. If one establishes a VPN with an outdated protocol it may be susceptible to known attacks, for instance version 1 of PPTP has known weaknesses such as weak password hashing algorithms which allows an eavesdropper to retrieve a password.

How anonymous or accountable one is when connected to a secure VPN is entirely up to those who control the VPN. For instance users would not be anonymous and could easily be held accountable if the VPN logged all traffic. Here it actually seems theoretically possible to have some kind of compromise between anonymity and accountability even if it would be hard to oversee that the agreed upon rules are followed. Such a compromise might consist of only logging data if it consists of child porn or is directly related to terrorism. Although there is always the matter of trusting your secure VPN provider not to log data you want to keep anonymous. However a secure VPN can be combined with other solutions listed in this article such as Tor, I2P or OneSwarm which can be run over the secure VPN.

4. Related work

Since this report is an overview of many different subjects there exist a lot of more specific work on the matters looked at here. For instance how anonymity and accountability affects the behavior of people in general, technical reports analyzing the specific services in depth and reports discussing the concepts of anonymity and accountability. We could not find any reports which discusses the broader issue of anonymity vs. accountability in networks. When attempting to find information on the area we find a bunch of small articles with no real references but web pages with small credibility so while it is a widely discussed topic it seems that it is sorely missing from peer reviewed research papers. This makes us think that the theoretic area would do well to be analyzed more thoroughly.

5. Conclusions

Anonymity and accountability seem to be diametrically opposed unless both parties truly trust some gatekeeper to enforce mutually agreed upon rules which strikes the authors as unlikely. Furthermore not only are the acts of anonymity and accountability opposed but in a great deal of cases the actors themselves have a great deal of difference in opinion about what is most important, we are not likely to come across a situation where the police(or public) agree with a child pornographer about his rights to do as he wish and an agreement between dissidents and an oppressive regime is equally unlikely to occur. This means that we will always have new services trying to provide anonymous communications and new attacks trying to get around the defenses. It is an ongoing and never ending race where neither side has been able to pull very far ahead of the other.

The services which we have written about in this report are not easily graded from best to worst but rather offer different features and degrees of anonymity. Tor offers a versatile and thoroughly tested service with a high degree of anonymity while I2P offers some other features such as UDP support at the cost of being less tested. The third service that lands in the same area of use is Freenet which also provides a way to communicate anonymously but adds distributed storage to the mix. Of these three it is hard to say which is best; they all seem to provide decent anonymity for regular communications, differing a bit in how they can be used, over what protocols and have different features. However in the end we have not been able to determine which would give the most secure communication.

Neither proxies nor remailers appear to provide any advantage over those three save for the fact that it may well be easier to setup and could be considered to give a higher degree of availability. Using proxies might be good if you wish to ensure that some provider should think that you are connecting from a certain country but it is possible to put such constraints on all of the anonymizing networks in some way. Anonymous remailers were once needed for posting anonymously on newsgroups but in this day and age you could just as well create an email address using Tor and always use that path for sending and receiving mail. Since the real identity of the mail owner would not be known, knowing the mail address is only a problem if you end up connecting to it without using the anonymizer. Secure VPNs just like proxies require a certain degree of trust,

certainly you could set some policies on the provider and try to find a way for both anonymity and accountability to exist at the same time but why would anyone trust another entity to ensure that their anonymity was not compromised unless they were forced to. VPNs are mostly useful for companies and other parties that want to enable connections to their internal networks that to the outside are unknown but can be tracked on the network. What you do on a network behind a VPN is unknown to the outside but never the fact that you are communicating with the network. A VPN could also be used in combination with several of the different services mentioned to create an additional layer of anonymity although the simultaneous use of two different services might create unknown complications in regards to security; this could warrant further study.

OneSwarm has a somewhat different purpose than the other services discussed since it focuses more on file sharing than regular communication. It offers a lot of options and allows the user to configure the service to find a balance between anonymity, speed and functionality. When properly configured it offers decent anonymity and when used improperly it provides none.

References

[1] T. Isdal et. al., "Privacy-preserving P2P data sharing with OneSwarm", Technical report, UW-CSE. 2009, retrieved from http://oneswarm.cs.washington.edu/f2f_tr.pdf on April 14 2010.

[2] I. Clarke et. al, "Protecting Free Expression Online with Freenet", 2002, retrieved from http://freenetproject.org/papers/freenet-ieee.pdf on April 16 2010.

[3] R. Dingledine et. al, "Tor: The Second-Generation Onion Router", Usenix Security 2004, retrieved from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf on April 12 2010.

[4] G. Danezis et. al. Mixminion: Design of a Type III Anonymous Remailer Protocol retrieved from http://mixminion.net/minion-design.pdf on April 10 2010.

[5] http://www.i2p2.de/how_networkcomparisons visited April 1 2010.

[6] http://www.i2p2.de/techintro.html visited April 16 2010.

[7] http://www.vpnc.org/vpn-technologies.html visited April 16 2010.

[8] http://www.schneier.com/pptp.html visited April 28 2010.

[9] http://new-wiki.freenetproject.org/Main_Page visited April 16 2010.

[10] http://mixminion.net/minion-spec.txt visited May 3