An Overview of Network Anonymity Technology

Jay Zimmermann
Email: jayzi926@sudent.liu.se
Suprevisor: David Byers, {david.byers@liu.se}
Project report for Information Security Course
Linköping Universitetet, Sweden

Abstract

This paper presents an overview of Network Anonymity Technology. It provides a look at current opinion concerning Anonymous Networked Communication. It then looks at what Anonymous communication entails and the technologies that go in to providing different forms of anonymous communication.

1. Introduction

Anonymity is not a new idea. There have always been activities and communications where those involved didn't want to be identified. Networked communication as a vehicle for communication has provided a new avenue for people who both want to communicate anonymously and people who want to gather information on others.

This paper will present an overview of some important aspects of anonymity as it relates to networked communication. First it will establish the environment in which anonymity technology exists by giving a brief look at who might desire anonymity and why as well as the groups that are against anonymity and there reasons. it will then present a brief introduction to how network infrastructure allows communication to be tracked and some base technologies that go into building anonymous communication tools. It will then look at different types of anonymous communications and the anonymous tools in each. This will focus on how these anonymity tools handle or fail to handle various means of tracking user communications.

2. Arguments For and Against Anonymity

Technology doesn't exist in a vacuum but is usually built to a purpose. The purpose can establish what it needs to be able to do. So to understand a technology it can be important to establish the environment it exists in. This section examines the who and why of anonymity. Who wants it and why, as well as who doesn't like it and why. Keeping ones identity private on the Internet is an issue that has generated a great deal of conflict and differing opinions. It is an issue closely linked to information privacy and cryptography so many arguments concerning the two overlap. There are good and bad reasons to keep ones identity private and different groups want to overcome this privacy for different reasons.

2.1 Pro

There are a number of good reasons for anonymity and groups that support it. Anonymity can benefit a wide range of people including dissidents, journalists, parents, children, law enforcement, companies, and criminals. One use for anonymity is it can support a general desire for privacy. This can be extended when one is looking into or speaking about sensitive issues like health, and sexual orientation which one might not only prefer to keep private, but be keeping private to avoid persecution. Free speech, also benefits greatly from the ability to keep ones identity private. In some countries governments oppress descanting views. Beyond descanting voices journalists and whistle blowers might need to keep from being associated with communications. Multiple anonymity tools have developed that can be used by these groups to facilitate communication anonymously. Physical protection can also be an important reason for anonymity. For someone who has had problems with physical harassment or has children using the web it can be important not to reveal their physical location. Further anonymity can have its uses in the prevention of Internet based attack like identity theft, and phishing [1]. Related to this could be attempting to avoid data brokers who collect information to sell and a lack of trust in companies keeping your information private and secure from people who might use it in these types of attacks [2][3]. Businesses can also benefit from anonymity when they want to hide company plans from competitors. Law enforcement agencies also might use anonymity software to hide or prevent the logging of known government IP addresses when they are gathering information[4].

2.2 Con

Anonymity in networked communication does have detractors as it can prove a hindrance to some of these same groups and a boon to criminals. Law enforcement and security professionals can find them selves frustrated by anonymity tools that can be used to conceal the identity of criminals performing network based attacks including information theft, and the distribution of spam and malicious software. A major area generating legal attacks on anonymity is companies attempting to fight the illegal distribution of copyrighted works. Claims have been made that anonymous networks are used predominately for peer-to-peer bit torrent traffic which is frequently associated with copyright infringement[5]. Law enforcement can further be frustrated by anonymous distribution of child pornography, and criminal communication. Additionally while anonymity can be an aid in physical security people can find themselves the target of anonymous harassment, or defamation over the Internet[1].

2.3 Legislation

In addition to technological responses, the good and bad sides of anonymity have lead to attempts to use methods outside of technology to handle anonymity. Beside technology, legislation can play a role in anonymity in the web. A broad array of laws exist both in support and attempting to prevent anonymous networked activity. These laws differ greatly from country to country and even within a country laws may not completely support or prevent anonymous communication. Some places have legislation requiring websites to protect user information. Some have laws restricting who can access electronic information. Conversely some places have laws requiring those who hold electronic information to store and provide information to the government. The United States provides an example of the mix of privacy that can appear with in a country. The Obama administration supports a privacy bill of rights [6], and the Electronic Communications Privacy Act offers limited protections, while courts have at times upheld that electronic communications are protected under the 4th amendment and the government needs a warrant to access these communications. However, the USA Patriot Act was passed into law to allow law enforcement easier access to electronic communications and courts have determined that an ISP is allowed to access private emails [7]. The United States is not alone in having a patch work of laws applied to electronic communication. While in some ways the European Union attempts to provide strong user defenses for electronic information the British Government Home Office allows remote searches of computers without a warrant and may provide this service to other members of the European Union[7].

There are a variety of arguments in favor of and against anonymous network communication. Legislation is one tool that can make it easier or harder for the use of anonymity in the Internet but isn't sufficient to address all issues. There will always be groups that are trying to keep information private and groups that attempt to collect information about who is doing what on the Internet. There are already many technologies that will support both these groups.

3. Overview of Technologies:

Some of the basic infrastructure and communication protocols used in networked communications have not conceptually changed over time and appear repeatedly in the sections below An understanding of some of this infrastructure is important to understanding how anonymity technologies function. When sending any packet over a network the packet will have the a sender and receiver address attached in the header to aid in delivery and response. These ip addresses are a useful tool in communicating over networks however they also can associate a message with a sender preventing anonymous communication. It is possible for an ISP to read the IP addresses and use them to track and log all data transmissions that pass through their servers. Further an attacker can also read IP addresses from communications on a network [1].

These problem for anonymous communication can be addressed through the use of several tools. A proxy server is a server that sits between a client and the server it is communicating with. A proxy server can have a wide range of uses including ip address hiding, hosting, and filtering[9]. Chaining involves sending a message to multiple proxies one after the other allowing for each computer to only knows who sent it to it and the next recipient [2][9]. Cryptography is also an important tool in network anonymity. Cryptography uses an algorithm and key to encode a message so that it is unreadable except by someone who knows how to decode it [10]. The section below examine how these tools are Incorporated into various anonymity systems and how they are used in creating anonymity.

4. Anonymity Services and Technologies

The remaining sections look at some network anonymity technologies and what exactly they do as well as how they work and how they can be attacked. First the history of some anonymity technologies is presented. The present builds on the past and the more complex technologies of the present tend to incorporate or be a

response to something that has come before. Computer Networks and there uses have developed and changed. As networks have grown and changed so have user needs and capabilities. The below paragraphs give an overview of some of the important developments in anonymity networks as they have changed.

4.1 Email

One of the primary uses of early networks was email communication and people who wished to communicate anonymously had to determine a way to send and sometimes receive messages without being identified as the sender. Anon.penet.fi was an early remailer that attempted to meet the challenge of anonymous communication via email. A remailer works is a type of proxy server that can be used to conceal an original sender by stripping away identifying technical information like the ip address of the sender and resending it. With the Penet remailer users could create a pseudonym that was kept in a table linking the original email address to the pseudonym. While this allowed for users to receive return emails it created a serious vulnerability since gaining access to this table could provide information as to who originally sent emails. After multiple attacks and legal pressure Penet eventually shut down, however other remailers had developed[1][2]. Cyberpunk type I remailers were a response to some of the problems observed in early remailers. Cyberpunk type I remailers dropped the user table and logging, sometimes allowed cryptography of messages, and introduced chaining. Because cyberpunk remailers dropped tables they did not allow for return messages [2][11]. Mixmaster or type II anonymous remailers, like nym.alias.net, built upon this model. They kept many of the features of Cyberpunk remailers retaining chaining and encryption. They also attempted to address passive correlation attacks, in which the attacker watches incoming messages and attempts to match incoming message size with outgoing message size. Mixmaster only sends messages of a fixed size and adds random ordering of messages. Mixmaster also reintroduced the ability to receive responses. It offered pseudo-anonymity by keeping a log for replies containing only the next link. This means that all links must be broken and connected to retrieve the users information[2][12]. Some other technologies development paralleled anonymous email development, while others appeared latter, but many tools that are used in email anonymity have been incorporated into other anonymity tools.

4.2 Hosting

Anonymous hosting originated as an attempt to meet the challenge of preventing the easy identification of information providers and the take down of those hosted works. In any hosting of a work a publisher publishes to a web server. The server then hosts the work. A user can access the server to view or use the work. For most anonymous web hosting attempts are made to keep the person publishing secret. They may also attempt to keep secret the location of the server and provide anonymous browsing services. There are a number of different groups that have supported anonymous web publishing including Publius, FreeHaven, FreeNet, and Tor. Each of these services adapts some of the previous examined technologies including, web proxy servers and chaining to hide the poster and person accessing a web site, and cryptography to hide the web site while it is stored. A proxy server hosts the work hiding the original publishers information from anyone accessing the site. Publius and FreeHaven attempted to use a set of static servers however were forced to close do to operating cost[13][14]. Alternately FreeNet and Tor emphasis volunteer storage, distributing the web page over a number of distributed volunteer proxy servers. Because volunteers are used to keep identities hidden the publisher publishes to the hosting server using chaining so that the hosting server isn't actually aware of who the publisher is. Additionally this makes it more difficult for a man in the middle to use incoming traffic and identify publishers. Since Tor and FreeNet rely on volunteers, redundancy and cryptography are also used. By placing the hosted work on multiple servers it makes it more difficult to take down all published copies and less likely to go off line because a volunteer server goes down. Both of these services also provide anonymous browsing of these hosted sites. This anonymous browsing acts to hide both the person accessing the website and the host server. The host is difficult to identify because the hosts information is stripped at each link in the chain that the information passes through on the way to a client trying to access it. FreeNet limits anonymous browsing to things posted on the FreeNet[15][16]. Tor can be used with both sites on its secure network and sites on the normal Internet [4]. Anonymous browsing will be looked at more in the next section. Along with the hosting of works some anonymous hosts have moved into hosting services. These hosts, like Tor Anonymous services or OTR, off the record instant messaging, may provide users with the ability to anonymously use services like instant messaging or VOIP. They function on the same basic principle as anonymous browsing with the person browsing being replaced by the person using the service so that the service user will connect anonymously to the service via chaining and use the service[4][17].

4.3 Browsing

Anonymous browsing has developed to serve as the complement to anonymous hosting and is sometimes

provided by the same group. Some early Anonymous email and hosting services were one way connections that required no response and simply involved one way transmission of a message. As a result didn't need to keep any information stored concerning who to reply to. Email services eventually incorporated technology to allow for safer storage of user information by making sure that each step in a chain new only the next. This would also be used eventually in browsing but like email other attempts were made before chaining was adopted. While in the technologies we have looked at so far anonymity has come at the user level some early attempts at providing anonymous browsing actually came from Internet Service Providers. Crowds were an attempt at hiding web requests by using random submission from a member of a crowd of users or sending the request on to another user. However, early implementations of crowds were not very strong anonymity and provided no cryptography[13]. The first attempts at user based anonymous web browsing had some similarities in form to the penet remailer. A user would log into a trusted server which replaced the users ip address with a substitute which it then stores with the users ip address to allow responses. While this is a simple, easy to use option, it is vulnerable to several types of attacks. Additionally one must trust the server not to keep logs and clear ip tables to avoid the theft of the form that would allow mapping ip addresses. Anonymizer.com's browsing service was an early example, of this type of single access point anonymity model, which has continued to develop and is still in operation [17]. This system will be examined in greater detail latter in the article . Onion routing introduced chaining to create a tunnel for web browsing. The initial computer encrypts the information so that each computer that the message reaches can peel one layer of encryption away so that each link only knows about the previous and next. Other groups like Freedom network and Tor would continue the onion routing concept with different models. Freedom network attempted to use a set of static servers however was forced to close do to operating cost [17][18]. Tor conversely implemented a volunteer run, free, open source service operating a distributed network This model does a better job of preventing user information theft and traffic analysis [4][17]. Tor will be examined more thoroughly below.

Browsing further creates vulnerabilities to identification as the user downloads content that may not be safe. Cookies are placed by websites on users computers to help access the website or store information for the website. They can therefore provide information about the user to someone who accesses them and undermine anonymity. One solution involves wrapper applications that redirect the cookies to another location [7]. Some Cookies can also be blocked through browser settings [19]. Proxy servers acting as filters, like privoxy, can also help against cookies. Additionally they can aid against spyware[20]. It is possible for users to be redirected to unsafe web sites. These web sites can download spyware on to a users computer and circumvent anonymity. There are filters that can block some spyware or prevent users from being redirected to these sites and anti phishing tools like Ebay account guard, which uses url matching for trusted and bad sites, and google safe browsing which uses google ranking to determine bad sites and helps block them [17]. Alternately tools exist that try to match known spyware. None of these tools can completely protect anonymity however they can help to preserve it.

5. Comparing Technologies

Different technologies may be better for different users. There are a wide range of technologies available for different anonymity goals. Comparing all of these is beyond the scope of this paper. This section discusses things one might examine when comparing two technologies without doing extensive testing. Then looks at how these criteria might differ in two of the technologies mentioned above and how one might compare them depending upon desired goals.

5.1 Things to compare

There are generally trade offs when looking at different anonymity systems. Some important characteristics when looking at an anonymity system include: services provided, ease of use, cost, accountability, community acceptance, speed, reliability, bandwidth, vulnerabilities or level of security. Some of these concepts are easier to compare than others, some of them may be more clear in their importance than others, and some may not be relevant to all users. The complexity of a topic is not always easy to tell. Community acceptance can indicate how trustworthy a product is and how well it has been tested. Haystack is a defunct project that never gained community acceptance as testing found it to have more vulnerabilities than stated[22]. Further with the abundance of proxy servers available on the Internet it is important to check the choice you make is trust worthy, otherwise you may be directing your traffic to an attacker. Community acceptance can be an indicator of trustworthiness. Vulnerabilities is also a complex topic do to the abundance of attack types and the different level of exposure and likelihood a system may have. Further there can be a trade off between security level and speed and bandwidth requirements. Additionally sometimes it is only possible to get serious detail on a product by running tests.

5.2 Anonymizer and Tor

Anonymizer.com and Tor are two of the more well established technologies available. Both provide a range of anonymity services but with two distinctly different models. Without examining the details of functionality of the two systems we are able to compare the services they provide, cost, accountability, and community acceptance. Both of these technologies are well established, but they have very different business models. Tor is volunteer supported and as a result free to use while Anonymizer costs a monthly fee. This also means that with Tor one must rely on volunteers for support while with Anonymizer the user can contact the company. Among its services Anonymizer offers users browsing and email, but excludes peer-to-peer file sharing. Anonymizer also includes other business tools like setting up a VPN that are more related to privacy than anonymous communication[23]. Tor offers users browsing, web hosting, and file sharing including peer-to-peer [4]. Based on these offerings if a user is looking for email, peer-to-peer file sharing, or hosting anonymity the choice between these two is clear and further analysis would need include other options that provide the same service.

Comparing Tor and Anonymizer's implementation of browsing and streaming of content can provide further insights into how they theoretically will perform. Speed, reliability, bandwidth, and vulnerabilities or level of security are all dependent on how a technology operates. To establish how these technologies compare the paper presents an overview of how each technology works and then a comparison on these points.

5.2.1 Anonymizer's Implementation

Anonymizer is a private, encrypted message, single point system that provides shifting proxies. When a user has Anonymizer running and sends a request that request is encrypted and redirected to Anonymizers proxy servers. Their some identifying information is stripped from the request, it is decrypted, a new ip address is attached and it is sent on to the desired address. Return information will have this process applied in reverse. The message is encrypted and sent to the user. The source address is also hidden. Anonymizer attempts to add protection by changing the users assigned pseudonym ip every 24 hours[17][23].

5.2.2 Tor's Implementation

Tor is a multiple layer, volunteer based, distributed network. When a user attempts to browse anonymously using Tor the first step is to get the computers it will work through. The user will connect to a trusted directory server which will have a list of available servers that can be used as entry points, exit points, and intermediary nodes. Along with providing available nodes these servers can be important in attempting to preventing too many untrustworthy nodes from entering the network. Tor uses an algorithm that provides some randomness but takes into account available bandwidth to determine which servers to send the traffic through. The user then establishes encryption keys with each of these servers. The message is then encrypted in the onion routing style. The request is then sent through each of the computers in the chain [4][24]. Replies are encrypted and routed back to the previous sender in the chain.

5.2.3 Performance

Looking at how these two systems work it is possible to theorize about how they should perform in certain areas. Anonymity services can slow things down as they add steps to the communication process. Looking at Tor and Anonymizer one can see Tor adds steps and may be slower do to multiple server steps and thus multiple encryptions as well as its establish connection step. Also important to speed and more difficult to determine without running tests on these technologies is how bandwidth will effect speed. Tor will rely on how many volunteers are available to feed information through as insufficient nodes to handle the load could slow Tor down. Tor does use an algorithm that takes into account load balance when determining what nodes to use which can help speed. Anonymizer conversely simply needs to provide sufficient bandwidth for the number of users it has. One can make some conclusions about how reliability might be affected by system architecture. Anonymizer is easier to make Denial of Service attacks against since it is at one, known location and this can affect reliability, however it is not an extremely common problem. Tor doesn't suffer from this problem but unlike Anonymizer relies on volunteers to provide entry, exit and, intermediary nodes. If insufficient volunteers are available this could cause problems with being able to use the service. Additionally as Tor relies on volunteers to provide nodes, if a user allows his computer to serve this function more traffic will flow through requiring greater bandwidth. The level of security provided by each system is the most difficult thing to be sure of as there are a wide range of attacks that could be used against each system, with different levels of ease to implement.

5.2.4 Attacks

Do to different implementations each of these technologies has different vulnerabilities. Anonymizer one point design makes it vulnerable to traffic analysis. and passive correlation attacks In traffic analysis the attacker watches the traffic coming into and going out of a proxy. By comparing the traffic it can be possible to

match incoming and outgoing packets providing. This breaks anonymity by allowing the attacker to match the incoming source IP and outgoing destination address. There are tools that a system can use to attempt to fight this. Large amounts of traffic can make it harder to pick out the correct match. One can introduce random delays to help prevent timing syncing. Random requests to web pages or hosting of web pages can also create messages that leave without entering matching and messages coming in without matching leaving messages [25]. Anonymizer is vulnerable to this sort of attack because there is only one location to watch all entry and exit traffic. Tor is designed to fight this kind of attack. While it is possible to use watch entry and exit nodes in Tor it is more difficult because there are multiple steps, distributed. It is more difficult to be certain which exit node receives a packet going into a specific entry node or to record entry and exit at all nodes, while recording at one node doesn't provide sufficient information to determine both sender and receiver[4]. Active attacks are also a greater problem for Anonymizer's single point network architecture. While neither of these systems keeps logs, if one might break into Anonymizers at one point they could have access to tables matching incoming and outgoing ip addresses, which when combined with recording of traffic can give browsing history. For Tor these would need to be recovered from each link to create the entire path. Encrypting these tables and regular deletion can help prevent this sort of attack. Tor is vulnerable to attacks based on placing untrustworthy nodes in the system. These nodes can then be used to determine the path of a communication [26]. This is not a problem for Anonymizer who controls the proxy server. Each of these networks has its vulnerabilities, however the resources required to perform these anonymity attacks will prove prohibitive for many attackers.

The architectures and business models these two technologies offer provide some insight into how they will function and provide for different user needs. However without doing a wide array of tests it is difficult to determine exactly how they will function. Further these two technologies by no means provides a complete view of anonymous browsing options. There are alternative free and pay services for browsing anonymously including JAP (Java Anon Proxy), Tarzan, MorphMix and many others [27][28].

6 Conclusion

This paper provides looks at some aspects of the current state of network anonymity. There are a host of technologies available that can provide different anonymity services. It may be noted that these technologies have varying uses and limitations. With enough money, time, and resources anonymity can usually be broken. Further there are trade offs. The ability to get responses creates a path back to the sender regardless of how well hidden and distributed it is. Further adding steps to a chain or hiding information through encryption add time to tasks slowing down the user [21]. Finally user awareness is always important. If while browsing the user downloads zero day spyware from a untrustworthy location then anonymity can be lost. If while sending email or posting to a anonymous server a user provides identifying information anonymity will be lost. Independent of laws and opinion users can through informed decisions find a network anonymity technology that will aid in a variety of anonymous network activities.

References

[1] Jacob Palme and Mikael Berglun. Anonymity on the Internet [Internet]. 2003 Jul 30 [cited 2011 Mar 20]. Available from: http://people.dsv.su.se/~jpalme/society/anonymity.html

[2] Ian Goldberg, David Wagner, Eric Brewer. Privacy Enhancing Technologies for the Internet [Internet]. 1997 Jan 21 [cited 2011 Mar 20]. Available from: http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html

[3] Wikipedia [Internet]. ChoicePoint [updated 2011 Jan 15; cited 2011 Mar 23]. Available from: http://en.wikipedia.org/wiki/ChoicePoint

[4] Torproject.org [Internet]. Tor:Overview[cited 2011 Mar 21]. Available from: https://www.torproject.org/about/overview.html.en

[5] Chaabane, A, P Manils, and M.A Kaafar. "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network." *Proceedings - 2010 4th International Conference on Network and System Security, NSS 2010*, 2010 (2010): 167-174.

[6] Computerworld [Internet]. Obama Administration calls for new privacy law. March 16 2011, [cited 2011 Mar 23]. Available from: http://www.computerworld.com/s/article/9214684/Obama_Administration_calls_for_new_privacy_law

[7] Wikipedia [Internet]. Internet Privacy [updated 2011 Mar 23, cited 2011 Mar 23]. Available from: http://en.wikipedia.org/wiki/Internet_privacy

[8] The Sunday Times [Internet]. Police set up step up hacking of home PCs, David Leppard. Jan 4 2009 [cited 2011 Mar 23]. Available from: http://www.timesonline.co.uk/tol/news/politics/article5439604.ece

[9] Wikipedia [Internet]. Proxy Server [updated 2011 Mar 14; cited 2011 Mar 23]. Available from: http://en.wikipedia.org/wiki/Proxy_Server

[10] Wikipedia [Internet]. Cryptography [updated 2011 Mar 15; cited 2011 Mar 23]. Available from: http://en.wikipedia.org/wiki/Cryptography

[11] Wikipedia [Internet]. Cypherpunk anonymous remailer [updataed 2010 Jul 11; cited 2011 Mar 21]. Available from: http://en.wikipedia.org/wiki/Cypherpunk_anonymous_remailer

[12] Quicksilvermail [Internet]. Instructions for Nym.Alias.Net [cited 2011 Mar 21]. Available from: http://quicksilvermail.net/help@nym.alias.net.html

[13] Ian Goldberg. Privacy Enhancing technologies for the Internet, II: Five years Later. Workshop on Enhancing Technologies 2002, April 2002.

[14] Publius [Internet]. Publius Censorship Resistant Publishing System [cited 2011 Mar 22]. Available from: http://www.cs.nyu.edu/~waldman/publius2/publius.html

[15] Wikipedia [Internet]. Freenet [updated 2011 19 Mar; cited 2011 Mar 21]. Available from: http://en.wikipedia.org/wiki/Freenet

[16] Freenet [Internet]. About: What is Freenet [cited 2011 Mar 22]. Available from: http://freenetproject.org/whatis.html

[17]Privacy Enhancing Technologies for the internet III: Ten Years Later, Ian Goldberg, Chapter 1 of "Digital Privacy: Theory, Technologies, and Practices", Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, Sabrina di Vimercati, editors, December 2007.

[18] The Register [Internet]. Freedom Network Source Code Now Available [updated 2002 Febr 15; cited 2011 Mar 23]. Available from: http://www.theregister.co.uk/2002/02/15/freedom_network_source_code_now/

[19] Mozilla Firefox [Internet]. Blocking Cookies [cited 2011 Mar 23]. Available from: http://support.mozilla.com/en-US/kb/Blocking%20cookies

[20] Privoxy.org [Internet]. Frequently Asked Questions; c2001-2010 [cited 2011 Mar 23]. Available from: http://www.privoxy.org/faq/general.htm

21] Zhang, J, H Duan, W Liu, and J Wu. "Anonymity Analysis of P2P Anonymous Communication Systems." *Computer Communications*, 34.3 (2011): 358-366.

[22] Wikipedia [Internet]. Haystack (software) [cited 2011 Mar 25]. Available from: http://en.wikipedia.org/wiki/Haystack_%28software%29

[23] www.anonymizer.com [Internet], FAQ [cited 2011 Mar 28] from: http://www.anonymizer.com/universal/#faq

[24] Yang, M, J Luo, and W Wu. "Modeling and Analysis of the Performance and Security for Anonymous Communication." *2009 Joint Conferences on Pervasive Computing, JCPC 2009*, (2009): 383-388.

[25] TheLivinInternet.com [Internet]. How Anonymizers Work [cited 2011 Apr 1]from: http://www.livinginternet.com/i/is_anon_work.htm

[26] R.Dingledine, N.Mathewson, and P.Syverson, "Tor: the second-generation onion router", in *Proceedings ofthe 13thconference on USENIX Security Symposium,* San Diego, CA, August9-13,2004.

[27] Ren, J, and J Wu. "Survey on Anonymous Communications in Computer Networks." *Computer Communications*, 33.4 (2010): 420-431.

[28] TheLivinInternet.com [Internet]. Anonymizer Sites and Services [cited 2011 Apr 1]from: http://www.livinginternet.com/i/is_anon_sites.htm