Tools and Protocols for Anonymity on the Internet

Azin Oujani, azinoujani@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract:

This survey focuses mostly on introducing anonymity systems, protocols, and some of the common tools that provide anonymity on the Internet. Privacy is one of the most important concerns of Internet users; thus numerous techniques have been deployed to offer security. The context of this paper will also address the most popular tools in use.

Keywords:

Anonymity, Anonymous communication, Mix networks, Onion routing.

Table of Content:

1.Introduction

Security and privacy have always been the most worrisome issue for people from the dawn of the history. Anonymity is something not only available via the Internet, but also has a significant history in the world. For instance, William Shakespeare chose to live anonymously on his entire life. However, the advent of the Internet and its rapid growth has soared up the demand of being anonymous in the cyber communication.

Anonymity has been requested for numerous purposes. The more sensitive information is transmitted through the Internet, the more people are concerned about their privacy. Therefore, anonymity systems and associated tools, which provide anonymity on the internet, are the central issue of this study.

This paper is organized as follows: First the difference between pseudonymity and anonymity, then anonymity systems and its components, and finally the two categories of anonymity system designs are being defined, in which it also introduces a few of the applicable tools in each design.

2. Pseudonymity vs. Anonymity

Before delving into exploration of anonymity, it is worth taking a quick look at pseudonymity and illustrating its differences from anonymity.

Pseudonymity with its Greek origin carries the "falsely named" meaning. It uses a pseudonym, a consistent disguised identity, which is linked to a single identifier keeping the real identity behind.

Publishing a public key is one of the simplest ways of deploying pseudonymity in which the confidentiality of the parties is provided, since the owner of the pair private key is the only one who can decrypt the message encoded. There are also Nym servers that use computer programs to give their users false identities as to post messages in newsgroups or send emails and have instructions on how to return messages to their real user.

Anonymity is also another Greek origin word meaning "name-less" which in turn is used where there is no identifiable information for an object or a person. The main difference between anonymity and pseudonymity is in anonymity the identity is unknown, whereas pseudonymity exploits the advantage of being unknown by using a pen name identity.

3. Anonymity Systems

Anonymity systems refer to an infrastructure that can provide anonymity on the Internet through allowing information to be transmitted from one party to another without leaking their identity. All possible nodes with the capability of being the sender or receiver of a particular message are referred to as Anonymity set. Anonymity set then is divided into Anonymity sender set and Anonymity receiver set.

3.1. Types of Anonymity

Anonymity sender: The anonymity sender terminology refers to a source that sends messages to recipients or any observer while could not be recognized. Consider hypothetical situation in which an employee wants to send a message to the employer. Passive observers cannot identify the employee that is included in anonymity sender set.

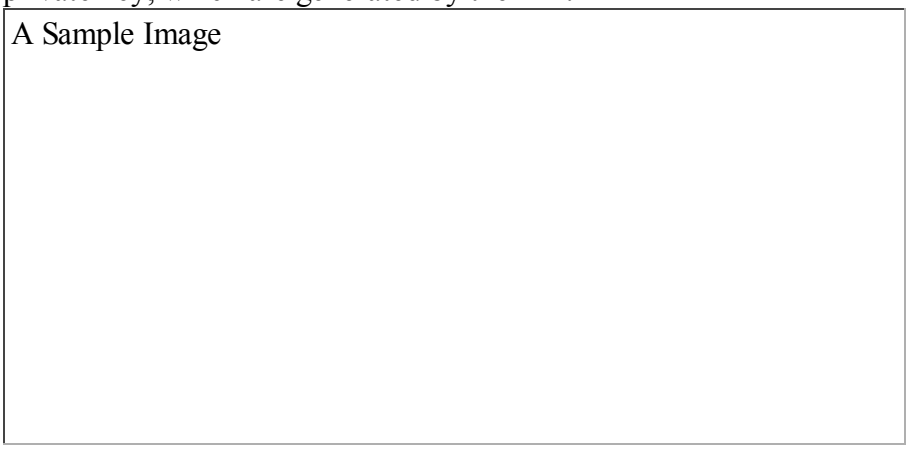
Anonymity receiver: No observer can identify the intended recipients of a message if the recipients are part of anonymity receiver set. Passive observers cannot identify other employers if the employee is to send a message to multiple employers that are included in anonymity receiver set.

Anonymity communication: Sender-Receiver anonymity is called anonymity communication, which makes the originator and recipient or even the whole communication unidentifiable from any observer. The employee and the employer are in the anonymity set, and any passive observer cannot identify the communication between them.

Anonymous communication design can be categorized into two general classifications: high-latency anonymity systems and low-latency anonymity systems. Before plunging into protocols and tools that offer Internet anonymity, it would be helpful to define the basic elements of most of the anonymous communications.

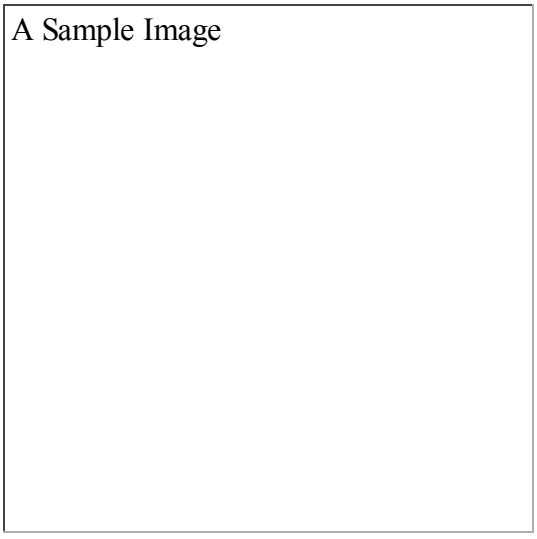
3.2. Mix Networks

Mix networks, was first outlined by Chaum in 1981, providing one-way or two-way anonymous communication. It is a process where a message gets encrypted using public key cryptography in a chain of gates or servers where the message has to go through. While being transferred through the gates, each gate will be able to decrypt the cipher using its own private key so that the last gate will be able to transfer the message to its destination. Public components transmit through the mix by creating a pair including public and private key, which are generated by the mix.



Illustrating the protocol, first client specifies destination of a message and selects an order of mixes. Then encryption algorithm proceeds in reverse order of the clientâ€™s path, and encrypts the message with the public key of the next hop in the mix. At last, each mix sends the message and detaches an encryption layer.

One of the most debated questions in the process of mix networks is the way to select the appropriate order of mixes. At the heart of much of the debate are mix cascade and free route. Both topologies are asymmetric while mix cascade is system defined and free route is user defined.



3.3. Batching Strategies

Mix uses batching strategies in order to determine which messages should be delivered to their destination at specific time defined by the mix. The succinct explanation of seven batching strategies is discussed below:

Threshold Mix: In this very simple algorithm, the messages will be forwarded in a random order to their next destination if the input of mix, cipher-text as mentioned above reaches to n packets, which n is defined by the mix. This is the original mix defined by Chaum, and is vulnerable to flooding attack.

Timed Mix: In this algorithm, the message will be forwarded in a random order to their next destination after t second which t is defined by the mix. This algorithm is vulnerable to the trickle attack.

Threshold Mix or Timed Mix: In this mixture algorithm message will be forwarded to their next destination, if either mix has received n packets or t seconds have passed. After sending the message mix resets the timer. This algorithm is vulnerable to blending attack, which is a combination of flooding and trickle attack.

Threshold and Timed Mix: Correspondingly, this combined algorithm will forward the message if t seconds have elapsed and mix has received at least n packets. Similar to previous algorithm, this one is also vulnerable to blending attack.

Threshold Pool Mix: In this algorithm after mix receives n packets other than f packets, which has been remained in the pool, it will randomly choose n packets, and forwards them to their next destination.

Timed Pool Mix: Similarly in this algorithm, mix collects packets after t seconds then adds them to f packets, which has been remained in the pool, and then randomly chooses n-f packets and sends them to their next destination.

Timed Dynamic Pool Mix: In this algorithm mix will randomly choose a fraction of whole messages in the pool, and forward it after t seconds have been elapsed. Pool mixes are vulnerable to blending attack.

Knowing these fundamentals will help to better understand the tools that provide high-latency anonymity systems.

---

4. High-latency Anonymity Systems

Strong anonymity can be provided by high-latency anonymity systems. However, it is normally applicable to applications like email that is tolerable for long time delays. Accordingly, some have called high-latency anonymity systems as message-based or message-oriented systems. Three types of remailer systems that provide high-latency anonymity systems are discussed below.

4.1. Cypherpunk Remailers

Cypherpunk remailers is called Type I remailers. Type I remailers chain multiple remailers; hence the message remains anonymous to each remailer. The mechanism can be illustrated as, a client selects an order of remailers then each remailer uses its private key to decrypt the message, strips the header away, and forwards it to its next remailer.

This tool is not strong since it uses PGP 2 for cryptography, and does not add random padding to messages for each hop. Anonymous replies could be supported in this type of remailers via reply blocks. Type I remailers are still in use.

4.2. Mixmaster Remailer

Mixmaster remailer that is called Type II remailer, is an enhanced construction of the Type I remailers. This improvement is achieved by adding batching, and random padding to the message. Moreover, mixmaster overcomes replay attack by keeping the packet IDs of the headers.

This protocol uses dynamic pool flushing algorithm, and SMTP for transport messages. In contrast to Type I remailers, anonymous replies are not supported in Type II remailer.

4.3. Mixminion Remailer

Mixminion remailer is called Type III remailer and it is also enhanced construction of the Type II remailer. Although mixmaster remailer exploit the methods of several ad hoc distributed servers, Mixminion makes use of smaller amount of synchronized redundant directory servers to present uniformly structured information about the network.

It uses TLS for forwarding messages. Additionally, in order to overcome anonymous reply problem, mixminion uses Single Use Reply Block (SURB) to secure reply messages as much as forward messages.

---

5. Low-latency Anonymity Systems

As mentioned above, high-latency anonymity systems make use of batching strategies that produce long time delay between sending and receiving messages. Thus, this design of anonymous communication is not applicable for interactive applications like SSH.

In contrary to high latency anonymity, low-latency anonymity systems are proxy based, which make them applicable for interactive or real-time applications. Accordingly some have called low-latency anonymity systems as connection-based system.

Lots of tools have been developed, on account of significant operation of low-latency anonymity systems on the Internet such as anonymizer.com, PipeNet, Tarzan, crowds, Java Anonymous Proxy (JAP), Morphmix, and so on.

The following part introduces the technique and a piece of software which employs that technique, most commonly in use for anonymous communication: Onion Routing and Tor.

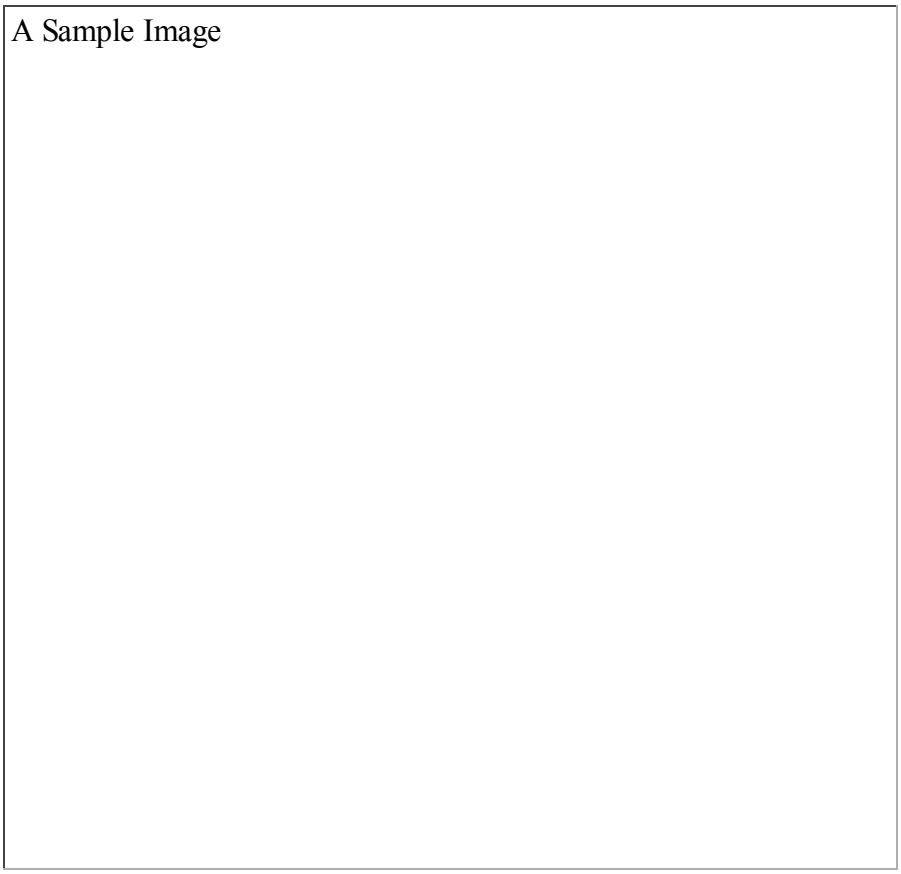
5.1. Onion Routing

Onion Routing is the most widespread and popular design for the low-latency anonymity systems based on a set of servers that delivers messages, like e-mail, World Wide Web, peer to peer applications, and so on.

Each server, which is called onion server, has a pair of public and private key, which the client gets to know the public key. Concentration of this proxy is to conceal the source and the destination of packets, although the message is encrypted with public key cryptography before transmission.

At first, a client selects a route to its desirable server, and then in a multi-layered model, encrypts its route with the public key of each node, in such a way that each node just knows the identity of its neighbor, and the interior layer contains the clear text message. Onion routing is not a two-way connection; however, reply onion, which is being sent all along with the message, makes it possible to respond to the client by setting up a reverse route.

Onion routed communications are at the risk of timing attack.

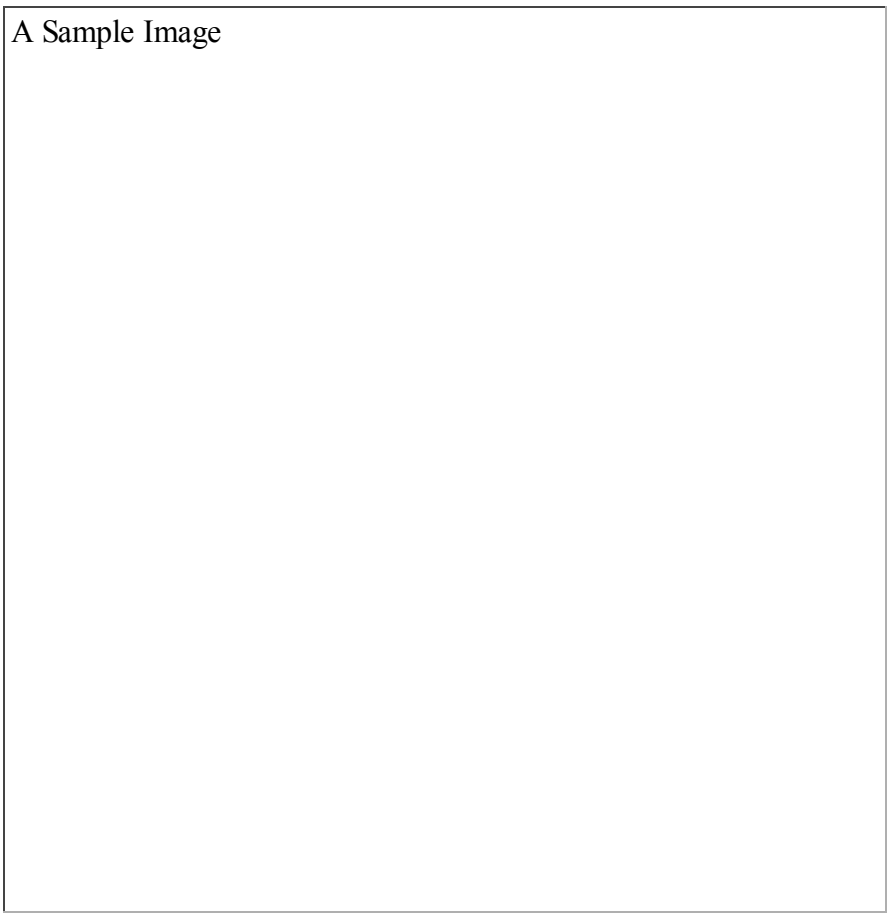


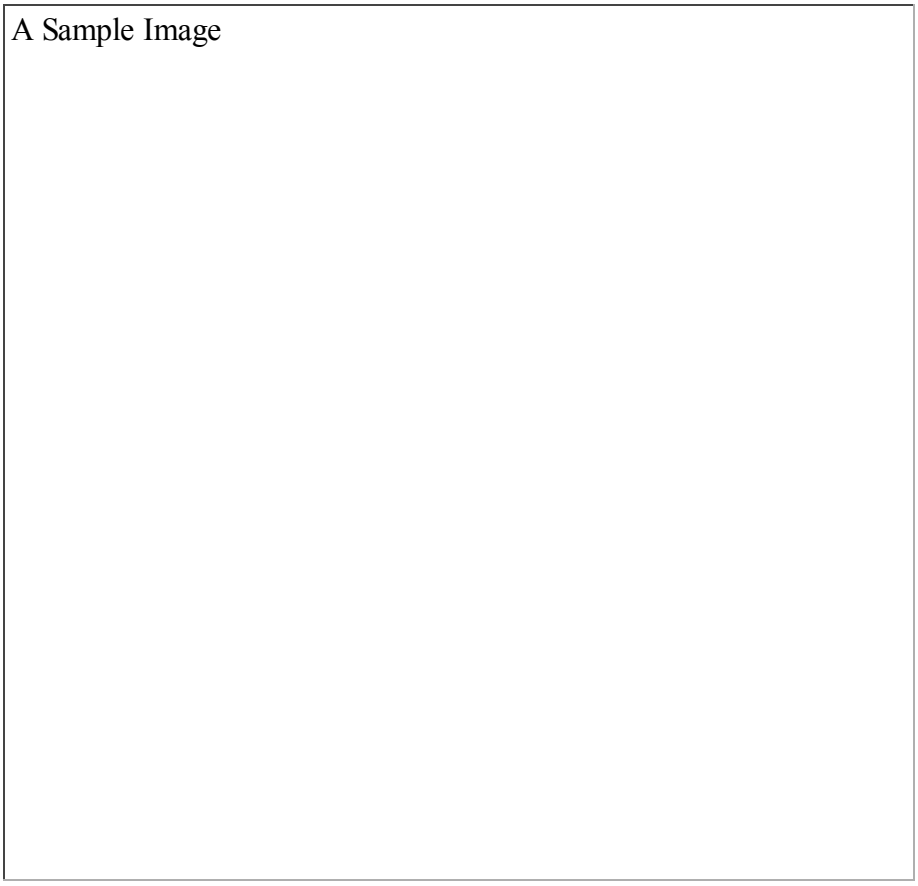
5.2. Tor

Tor is a software developed, as an onion router, to conquer the deficiencies of the original onion networks. The client side of the program will enable user to send traffic through volunteer networks and servers anonymously. It was basically developed to provide privacy and web surfing freedom to its users. The process starts by encrypting user traffic using private keys of Tor servers (relay points) and proceeds with each relay decrypting the traffic sent by the user and finally forwarding the traffic to its destination.

First, Tor establishes a circuit between the client and its destination by choosing a path of Tor nodes. Like Onion routing each node knows nothing about the path but the identity of its neighbors. The process of setting up a circuit is iterative, and is repeated around every 10 minutes in order to avoid traffic association to a specific user.

Given the description above, Onion routing techniques and inherently Tor; are limited in terms of area they cover to deliver the traffic as the final destination of the traffic is not part of the Onion network and needs the information to be delivered unencrypted.





Conclusion

Anonymity on the Internet can be used as a mean to protect data privacy and security or it can be used as a countermeasure to network security as to leave no trace for any unethical actions. In order to have anonymity on the net a set of systems as its elements are required so that the goal of anonymity can be achieved. Using this system a sender will be able to transfer information to receiver in anonymity communication in which at least one party of communication remains unidentifiable using techniques and tools available in the system.

Based on the application for anonymity communication, whether it is delay sensitive traffic or any type of file transfer not sensitive to delay and latency; choosing a proper tool to deploy anonymity is very important. A proper tool will then take use of the most appropriate technique and protocol so that the required security and performance is achieved.

As there are multiple techniques and tools to deploy anonymity, I have tried to address some of the most common ways and explained how they tend to differ from each other. There are different strength and weaknesses for all techniques and tools addressed in the context of this report as any other security technology, by the main concern is how practical a technique or tool can be. Tor as one of the very popular means of anonymity has been around for a period of time now and it seems to be responsive as of yet.

List of Acronyms

JAP Java Anonymous Proxy
SURB Single Use Reply Block

References

ARJAN DURRESI
Anonymous communications in the Internet
Published online: 24 March 2007
Springer Science+Business Media, LLC 2007.

CRANDALL, J. R., ZINN, D., BYRD, M., BARR, E., AND EAST, R.
ConceptDoppler: A weather tracker for Internet censorship. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCSâ€™07).
ACM Press, New York.2007.

CLARK, J., VAN OORSCHOT, P. C., AND ADAMS, C.
Usability of anonymous Web browsing: An examination of Tor interfaces and deployability. In Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS).
ACM Press, New York. 2007.

CLAYTON, R., MURDOCH, S. J., AND WATSON, R. N. M.
Ignoring the Great Firewall of China. In Proceedings of the sixth Workshop on Privacy Enhancing Technologies (PETâ€™06), G. Danezis and P. Golle, Eds.
Springer, Cambridge.2006.

DANEZIS, G. AND CLAYTON, R.
Introducing traffic analysis. In Digital Privacy: Theory, Technologies, and Practices, A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, Eds. Auerbach Publications, Boca Raton, FL. 2007.

DANEZIS, G., DIAZ, C., AND TRONCOSO, C.
Two-sided statistical disclosure attack. In Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PETâ€™07), N. Borisov and P. Golle, Eds.
Springer, Ottawa, Canada. 2007.

DINGLEDINE, R. AND MATHEWSON, N. 2007.
Tor protocol specification.
https://svn.torproject.org/svn/tor/trunk/doc/spec/tor-spec.txt

DINGLEDINE, R., MATHEWSON, N., AND SYVERSON, P.
Deploying low-latency anonymity: Design challenges and social factors.
IEEE Sec. 2007.

DINGLEDINE, R., SERJANTOV, A., AND SYVERSON, P.
Blending different latency traffic with alpha-mixing. In Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PETâ€™06), G.Danezis and P.Golle, Eds.
Springer, Cambridge, U.K.2006.

JONDOS GMBH. 2008. Jondonym.
https://www.jondos.de/en/.

MATTHEW EDMAN, BÃœLENT YENER, P.2009.
On anonymity in an electronic society: A survey of anonymous communication systems Vol. 42 Issue 1, December 2009.
ACM New York, NY, USA

MR. M.KRISHNAMOORTHY,G.JOTHIRAMAN, MS. S. KALAI ARAS
International Journal of Biotech Trends and Technology- May to June Issue 2011.
Tracing Traffic through Transitional Hosts by Mix Network against FlowCorrelation Attacks IJBTT - 17 - IJBTT
PFITZMANN, A. AND HANSEN, M. 2005.
Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. Draft. (Version v0.23 Aug. 25, 2005)
http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.23.pdf

Tor Anonymous Networks http://blag.cerebralmind.net/wp-content/uploads/2008/05/tor.pdf

ZBIGNIEW KOTULSKI, ANETA ZWIERKO 2005.
Secure protocol architectures through the concept of pseudonymization Deliverable reference number: D.WP.JRA.6.3.4
http://eurongi.enst.fr/archive/127/JRA634.pdf

Last Modified: December 6, 2011
This and other papers on latest advances in network security are available on line at
http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page