

Tor - A tool to disguise Internet communications

Victor A. Clincy, and Padmaja Mudiraj
Computer Science and Information Systems Department
Kennesaw State University
Kennesaw, Georgia 30144
vclincy@kennesaw.edu, 770-420-4440

Keywords: *Network Security, Security, Privacy, Cyber Crime*

1. Abstract

In present world of internetworking, the network administrator, an intruder, or a normal person (provided with sophisticated tools) could easily observe the traffic passing through a particular network. In spite of deploying some encryption techniques, it is possible for the intruders to capture the traffic and analyze when, how and with whom the users communicate.

The content of a message can be sufficiently hidden by end-to-end encryption. However, an attacker can still investigate on who sent the messages to whom and at what time. To prevent the intruders from identifying the actual source and the destination, we need to employ the tools that provide the anonymous communication.

There are some well known measures allowing users themselves to decrease their observability. Through this paper, we have made an attempt to summarize the prevention techniques that provide privacy to the Internet communication, thereby keeping the communications between the recipient and sender unobservable. This paper focuses on an anonymous Internet communication system called “Tor”, and describes the facilities the tool provides, and also highlights the strengths and weaknesses of the tool.

2. Introduction - How Tor works

Tor prevents the intruders from peeping into your communications by distributing your conversations over several routes on the Internet. The main idea behind using the different paths is to use an indirect, inaccessible route in order to obstruct somebody from

sneaking your discussions. Instead of taking a direct route from source to destination, data packets on the Tor network take a random path through several servers, so no observer at any single point can tell where the data came from or where it's going.

In simple words, the client station which wants to communicate through the Tor network gets the list of available nodes, and selects the random path to its destination, from the available route's list. When the client employs Tor, then the client's IP address is changed to a different IP address. As a result, anybody capturing your data will never know your actual IP address. Therefore you create anonymity to your conversations. The snapshots shown below were captured during our testing process. The first snapshot (refer to snapshot-1) displays the actual IP address. This snapshot was taken before configuring the applications to use the "Tor". The second snapshot (refer to snapshot-2) displays the spoofed IP address. This snapshot was taken after configuring the applications to use the "Tor".

The screenshot shows the IPID | Your IP Info website. At the top, it says "Your IP address is:" followed by the IP address "68.19.109.197" in large red text. To the right, there is a warning: "Do not use this page as an automated IP checker! Please use [IPID Lite](#)." Below this is a banner for "Blue Virtual" web hosting. At the bottom, there is a table with the following data:

Host Information	
Your host address:	adsl-19-109-197.asn.bellsouth.net
Your browser version:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Where you came from:	
Your browser's language:	en-us
Files your browser accepts:	*/*
Connection:	Keep-Alive
Your "HTTP in" port	50775

Below the table, there is a section for "Proxy Information" which is currently empty.

(Snapshot-1: Displays actual IP address)

Your IP address is:

IPID | Your IP Info

209.89.209.129

Do not use this pa
automated IP ch
Please use [IPID](#)

Host Information	
Your host address:	d209-89-209-129.abhsia.telus.net
Your browser version:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Where you came from:	
Your browser's language:	en-us
Files your browser accepts:	image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Connection:	close
Your "HTTP in" port	2836

(Snapshot-2: Displays spoofed IP address)

3. Technology behind Tor

Tor is a network of onion routers. The client's software called an onion proxy (OP) negotiates the connection with the directory server to fetch the nodes/routers list. The server provides the client with the list of routers that are available to support/direct the communication. From the list, the onion proxy software creates a virtual circuit over the Tor network, and manages the connections. In this virtual circuit, no node knows information about other nodes, except the node from which it receives messages, and the nodes to which it sends. These onion proxies accept TCP streams and multiplex them across the circuits. The onion router on the other side of the circuit connects to the requested destinations and dispatches the data (Dingledine & Nick, n.d).

As mentioned before, to create a private network path with Tor, the user's software should develop a virtual circuit from the available list of the routers. But each of the connections in the circuit should be encrypted. So, each recipient should decrypt the symmetric key at each node. The decrypted content will then reveal the next node/recipient to which the data should be sent. The client negotiates a separate set of

encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

Since the circuit is extended one hop at a time, and each server along the way knows only which server gave it data and to which server it should pass the data. Because each server sees no more than one hop in the circuit, neither an eavesdropper nor a compromised server can use traffic analysis to link the connection's source and destination. (Tor: An Anonymous Internet Communication System, n.d.) No individual server ever knows the complete path that a data packet has taken.

Tor only works for TCP streams and can be used by any application with SOCKS support. Tor implements a SOCKS proxy to support the idea of a generalized anonymous communication protocol. A SOCKS proxy accepts requests for connections to other computers and decides whether to forward the connection or not. (Jones, 2004). Their original purpose was to allow users to reach resources that may otherwise be unreachable. In the case of Tor, the SOCKS proxy serves as an entry point into the network. Any application that can use a SOCKS proxy can communicate anonymously.

4. Vulnerabilities in Tor

The four kinds of attacks that can be used by a trespasser to degrade the anonymity of the clients are described below (Jones, 2004).

1. **Predecessor Attack:** In this attack, the attacker targets any one particular node, and observes it from the receiver point of view. The attacker keeps track of all the clients who initiate a request to send, and identifies the client who appears the most number of times. This is possible because, in an anonymous environment, the list of all available nodes changes whenever an existing node leaves or when a new node joins. So, the client has to make a new connection, and to do so, it might contact the same node (which the attacker is observing) for a new request. But the probability of success is very less because there is very small chance that the client initiates the new request with the same node that is being observed.
2. **Denial of Service attack:** There is a high chance that an attacker might act as a malicious node in the anonymous group. So, if that malicious node plays the denial of service attack on the directory server which provides the clients with the list of available nodes or routes, then no other client's request can be processed. As a result, the entire network fails.

3. Sybil attack: This is an extension of the denial of service attack. An attacker creates multiple virtual identities, and all act as malicious nodes. Within a time period, all these malicious nodes flood the server with the requests of joining the group, and by doing so; they obstruct the legitimate clients from joining the groups.
4. Local Eavesdropping: When a client wants to communicate with others, it initiates a new connection. So, an eavesdropper sitting there can detect it, but he/she cannot determine the content as the “tor” uses encryption technology. However, the initiator’s/sender’s anonymity will be compromised, and the attacker can determine the probable list of the recipients by using the timing of the sender’s message.

5. Conclusion

Tor helps to reduce the risks of both simple and complicated traffic analysis. The main intention in developing this tool is to provide protection only for the normal people who obey the law, because they don't typically have the knowledge to figure out the good way to achieve the Internet privacy. But unfortunately, in this present online world, the cyber crimes are increasing tremendously, and so are the cyber criminals. The intention of these criminals is to break laws. They do this by cracking into other’s computers, and using them as a staging area to launch attacks. They capture the conversations over the Internet, and spoof those conversations.

Therefore, these cyber criminals as well as other bad people have the motivation to learn the process of acquiring anonymity so that their illegal activities cannot be traced by the cyber police. So, there is a high chance of criminals using the “Tor” tool to disguise their illegal activities. But, since they already have better options, taking Tor away from the world will not stop them from doing their cyber crimes

6. References

- 1) Jones, Andy. (2004, September). Anonymous Communication on the Internet. Retrieved September 24 2005, from <http://www10.cs.rose-hulman.edu/Papers/Jones.pdf>
- 2) Tor: An Anonymous Internet Communication System. (n.d.). Retrieved September 24 2005, from <http://tor.freehaven.net/overview.html>

- 3) Dingedine, Roger, Mathewson, Nick & Syverson, Paul.(n.d). Tor: The Second-Generation Onion Router. Retrieved September 24
<http://www.onion-router.net/Publications/tor-design.pdf>

- 4) Mubix. (2005, July). Tor: the Ying or the Yang?. *WhiteDust Security*. Retrieved September 20, 2005, from
<http://www.whitedust.net/article/28/Tor:%20The%20Ying%20or%20the%20Yang?/>