TOR: Enabling Online Anonymity

Madhavi Dhingra

Abstract - Tor is an anonymity network that allows people on the Internet to safeguard their privacy. Now a days, it is used for a wide variety of purposes by several classes of people e.g., armed forces, journalists, law enforcement authorities, activists, and many others. In this paper, the working of the Tor and its concepts were studied. Also, various kinds of attacks to breach Tor have also been discussed.

Keywords – Tor, Tor attacks, Anonymity Network, Working of TOR

1 INTRODUCTION

Tor is a network of virtual tunnels that direct the internet traffic through several layers to conceal the user's location from the attackers. Tor is free software developed by Tor project that uses onion routing and encryption to provide network anonymity. It can also be used to hide originating IP address from remote servers. Onion routing is a technique for anonymous communication in which the message is transmitted through a series of routers. At each router, it is encrypted repeatedly till it doesn't reach to the last router. The intermediate routers don't know anything about the source and the destination, this prevents eavesdropping and traffic analysis attacks.

Tor was originally designed, implemented, and deployed as a third-generation onion routing project for the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is widely used for a wide variety of purposes [1]. To protect the data from intruders, tor distributes the tasks over several nodes on the internet, thereby

hiding the details of the real communicators. Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is trailing you — by periodically erasing your footprints[1].

The basic idea of this network is that all the routers involved in the communication only know its successor and predecessor. A circuit is constructed which consists of onion routers as nodes. User uses this circuit to transmit data. Data packets travel through a random path instead of a direct path to reach the destination, so that if any observer is analyzing it, can never know about where the packets are coming from and going to.

2 WORKING OF TOR

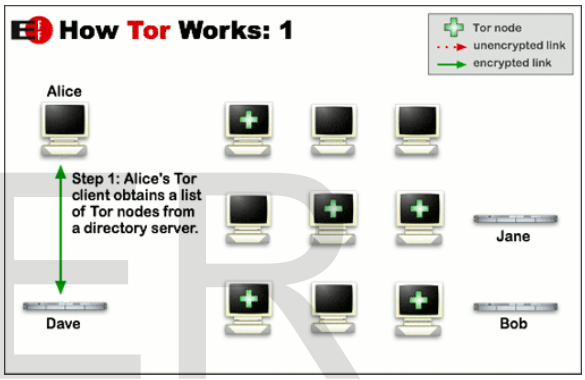

Figure 1.How Tor Works[1]

To create a private network pathway with Tor, the client incrementally builds a circuit of encrypted connections through routers on the network. The circuit is extended one hop at a time. Along the path, each router knows only which router has sent the data packet to it, and to which router, it is forwarding data packet to. No router knows the actual path that a data packet follows to reach its final destination. The client uses a set of encryption keys to encrypt the data packet so that no node can detect the path through which data packet is transmitted through.

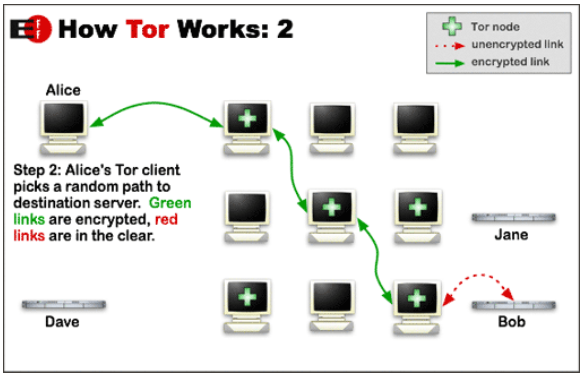

Figure 2. How Tor Works[1]

After setting up the connection, data can be transferred over the Tor. Because each router sees no more than one hop in the circuit, neither an eavesdropper nor a compromised router can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support[2].

After the transmission of all the data packets, the connection is terminated.

3 TOR ATTACKS

1) Like all current low latency anonymity networks, Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network, i.e., the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation).[3]

2) To browse the Internet anonymously using Tor, a user must use an HTTP proxy such as Privoxy so that traffic will be diverted through Tor rather than sent directly over the Internet. This is especially important because browsers will not automatically send DNS queries through a SOCKS proxy. However, pieces of software that plug into the browser, such as Flash, Java, and ActiveX Controls, do not necessarily use the browser's proxy for their network traffic. Thus, when any of these programs are downloaded and subsequently executed by the web browser, any Internet connections that the programs make will not go through Tor first. Instead, they will establish direct TCP connections, compromising the user's anonymity, as shown in Figure 2. Such browser attack allows a website to identify its visitors but does not allow a third party to identify Tor users visiting a given website. These active content systems are well-known problems in anonymous web-browsing, and most anonymizing systems warn users to disable active content systems in their browsers. [4]

3) The Tor Project suggests using two browsers; one for Tor, other unprotected. The unsafe browser probably doesn't have many of the restrictions or protections. The content from the unsafe browser can potentially target local Tor resources, for example, use Java same origin bypass.

4) Add-ons may launch external programs like Microsoft .NET Framework Assistant installed as system extension to support Click Once deployment. It is monitored for content that was returned with Content-Type: application/x-ms-application and re-requests content from external program, leaking the user's original IP address.

5)Locally saved HTML content is not safe - Any HTML content can be forced to be locally saved by specifying "Content-disposition: attachment" Content may be saved with an HTML extension and opened later from the web browser. The "Open" option opens a local temporary file. In Firefox 2, local HTML can read any file.

6) Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use Tor button while browsing the web to withhold some information about your computer's configuration.[5]

4 CONCLUSION

Understanding the working of Tor, and the attacks, it can be said that there is a large application attack surface in Tor. There are many attackable components between the user web browser, local HTTP proxy, Tor client and remote web server. Thus, new attack defense techniques are researched and refined all the time. We need a usable anonymizing network on the Internet today. Much secure defense techniques are required so as to make Tor a successful project. As Tor's usability increases, it will attract more users, which will increase the possible sources and destinations of each communication, thus increasing security for everyone.

REFERENCES

[1] Tor: Overview https://www.torproject.org/about/overview SOCKS , www.wikepedia.org
[2] "One cell is enough to break Tor's anonymity". Tor website; 9 January 2011.
[3] Browser-Based Attacks on Tor - Tim Abbott, Katherine Lai, Michael Lieberman, Eric Price {tabbott,klai,mathmike,ecprice}@mit.edu
[4] Attacking Tor at the Application Layer - Gregory Fleischer
[5] Tor (anonymity network) , Wikepedia.org
[6] "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise"; Zetter, Kim; 16 September 2007
[7] "Configuring Hidden Services for Tor". The Tor Project; 9 January 2011.