Tor Network

Akash Patel (SJSU)

What is Tor? [1]

- Tor(The onion router) is an open source software used by many people for anonymous internet surfing
- Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory
- Primary purpose of the Tor was to protect U.S. navy's confidential communication.
- Today, it is used by Journalists, military people and corporate people for privacy and security purpose.

Why Tor is required?[2]

- Tor protects against Internet surveillance known as “Traffic analysis”. Traffic analysis is special kind of interference attack to deduce pattern information from patterns in communication.

- Internet data packet has two parts, The first is the header and the second is the body. Header contains basic information like source, destination, timing and some geographical information. The body part contains encrypted data. In traffic analysis interceptor focuses on the header part and tries to find a common pattern in the header. Header might not reveal person’s exact information but still reveal many details.

- Another very important reason for Tor is freedom of speech. In some countries there are so many restrictions on internet usage. People can not share their view and access some of the websites and if they do, it is very easy for government agencies to identify that person. Tor provides anonymous internet surfing.

How Tor Works?[3]

- Tor uses onion routing system. Tor uses thousand of volunteer networks to direct traffic over internet so user identity can be kept hidden from network interceptor.

- Tor helps to reduce risk of traffic analysis by distributing transaction over several places so no single point can link to senders destination

- For example user A wants to send a packet safely to user B using Tor network. Tor creates private network for this communication.

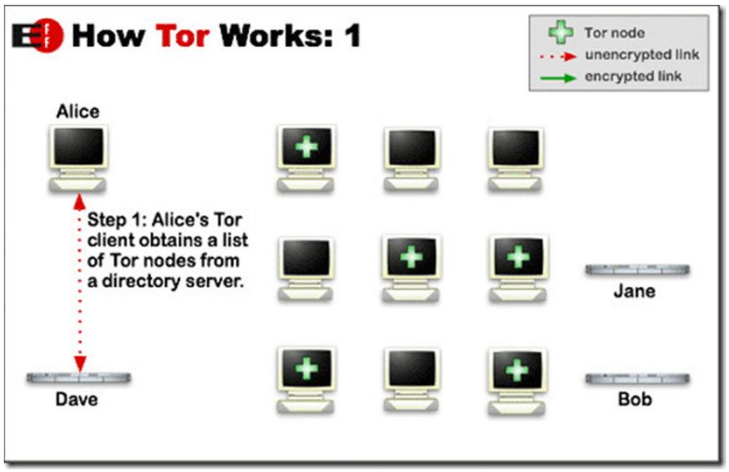
- First step is to identify available nodes. User A's Tor client obtains list of Tor nodes from server. It picks random node for each time so pattern cannot be observed by interceptor.

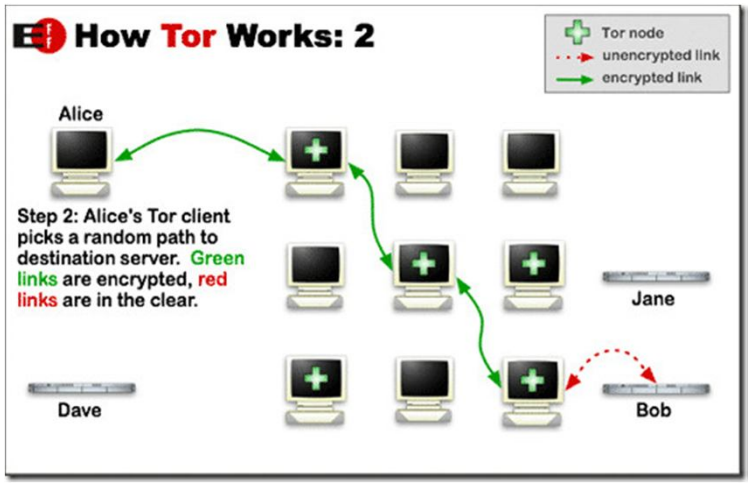
- Now client generates an encrypted message and which is sent to first node. The client on this node decrypts the first layer of encryption and identifies the next node.

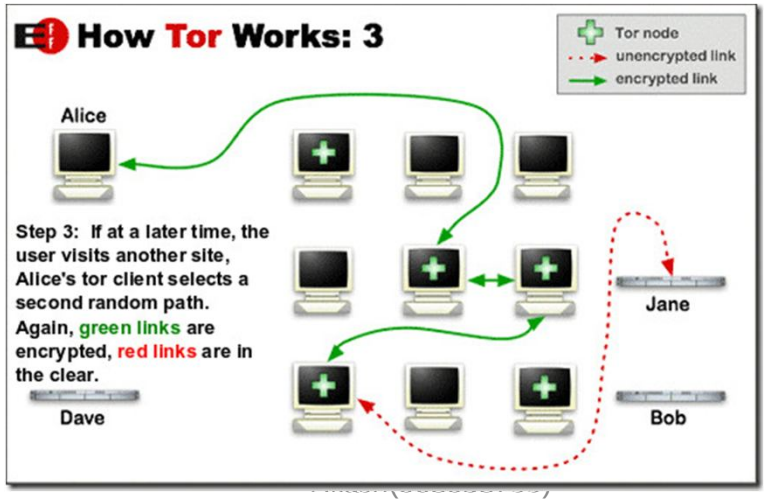
- This will continue until the final node receives the location of the actual recipient, where it transmits an unencrypted message to ensure complete anonymity.

How Tor works? [3]

- Now when the client computer want to send another packet Tor uses completely different path.
- Source: https://www.torproject.org/about/overview.html.en







How to use Tor?

- The Tor client is available for all major platforms e.g. Windows, Linux and Mac OS
- It is also available for smartphone platforms like Android and iOS
- It is normal software which user can install and use easily.

How onion routing works?[5]

- Onion Routing uses well known cryptography and networking technologies to provide anonymity and privacy on internet communication
- Onion routing connection has three phases: Connection set up, data movement and Connection tear down.
- First phase starts when initiator creates an onion, it is layered data structure which specifies properties of connection at each point.
- Initiator determines number of onion routers(nodes) to be used in the communication and creates Onion packet by having multiple encryption using public key of onion router(node).
- Each node has information about only 2 nodes: sender and receiver. Each node peels the layer of onion, they use their public key to decrypt the data and can obtain information about where they should send the packet.
- Receiver can use its public key and finally obtain plain text. Once connection is established bi-directional communication is possible. When data is sent back from the receiver to sender layering occurs in reverse direction.

Overhead and performance[6]

- In the Onion routing overhead is relatively small. Connection set up and identifying the onion router for the communication does not take much time
- Massive level of encryption is done at this stage but since the encryption is much more cheaper than the decryption, more burden is placed on the onion routers.
- Each onion routers needs to perform decryption which is a bit more costlier operation in terms of time.
- Overall Performance of the Tor network is slow due to extra bouncing of the packets as well as due to the decryption at each of the onion routers.
- Performance also depends on the bandwidth of each of the onion routers. If one of the router is slow then the overall time for communication will increase

References

1. http://en.wikipedia.org/wiki/Tor_(anonymity_network)

2. https://www.torproject.org/about/overview.html.en

3. Technical paper: Onion Routing for Anonymous and Private

Internet Connections by David Goldschlag Michael Reedy Paul Syversony on January 28, 1999

4. Technical paper: Onion Routing Efficiency for Web Anonymization in Various Configurations by Tomas Sochor:University of Ostrava, Ostrava, Czech Republic