**The Onion Routing Network**

**Divyanshu Shukla**

**Computer Science & Engineering (B.tech)**

**Babu Banarasi Das National Institute of Technology and Management**

**Lucknow, U.P. India (226028)**

[**divyanshushukl@gmail.com**](mailto:divyanshushukl@gmail.com)

Abstract— **Tor clients always build circuits with publicly listed volunteer relays to reach anonymously to their destinations. However, the relays are publicly listed, so they can be easily blocked by most of censoring adversaries when needed. If it is believed that TOR is always completely anonymous, private as well as secure way to access the internet (deep web sometimes) without being able to get monitored and tracing it back but it is not quite that simple and secure. TOR isn’t perfectly private and anonymous network.**

**It has several limitations and risks, which everyone must be aware. In this paper we are showing the flaws in the design-part and implementation part of TOR’s hidden network that allow an adversary to measure most of hidden services, taking down those hidden services and de-anonymize provided services.**

**So this second generation encrypted Onion Routing network addresses limitations due to which it is considered to be insecure network which can be easily compromised.**

**INTRODUCTION**

The Onion Router is a very low-latency based anonymous communication overlay network uses encryption methods. Tor directs Internet traffic through a free volunteered network of servers consisting thousands of relays to hide client’s location and usage from surveillance or traffic analysis and provide privacy as well as anonymity.

It mainly consists of client & relay nodes which together form a virtual tunnel through which the user configures TOR bundle to establish connection using the tunnel. In order to use TOR browser, clients contact publicly listed directory Servers, which is a fraction of TOR network responsible for tracking the network topology and node states. Directory servers allow users to fetch a list from volunteer relay nodes, also known as onion routers. The users then chooses some of these relays using TOR bundle and establishes a circuit through these nodes to its destination. Traffic is then routed through the TOR network over guard (entry), middle and exit node, hiding users’ identities and activities. TOR is considered as best project till date but if its encryption fails, nodes gets compromised. Such flaws can be utilized by an adversary resulting in revealing confidential information and privacy of user.

We here, focus both on attacks that allows to censor access to targeted hidden services as well as de-anonymization of hidden services. As the result it is believed that some components of the current TOR protocol should be improved and while short term may solve some problems but more complex approach is required in terms of efficiency as well as in terms of privacy.  
Ever since the TOR browser was introduced various attacks are made to de-anonymize the network through software loops like java script errors, mouse hovering & it’s also by network policies. To overcome such threats we can take measures at client side &in the TOR network preventing the adversaries from attacking on the network, firstly we will define the possible attack vectors & their deployment methods then realizing the defense mechanism to avoid attacks & make anonymity stronger.

**TOR and It’s Working**

The Onion Routing is a networking protocol designed to anonymize the data transferred across it. By using TOR Browser it is difficult, if not impossible, for any sniff into clients any online activity. It is even difficult to trace down the country and users IP from where TOR is operated.

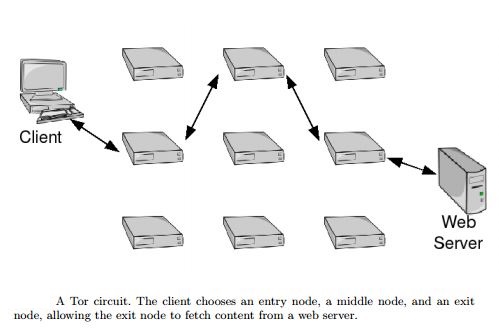
No online date collectors like Google, etc. can collect data and perform traffic analysis on Internet habits. Theoretically, it was designed to protect user from surveillance organizations like the NSA thus providing complete anonymity.

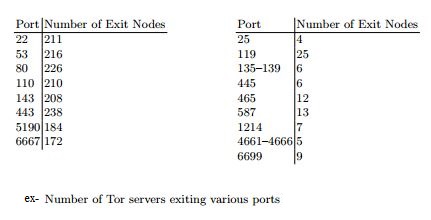
The Tor network runs over 7000+volunteerarily operated relay servers spread in the world. Data is bundled into an encrypted packet (512 byte cell) which enters into the Tor network. Then packet’s header is stripped, which stores the addressing information about the sender like OS information from which the data was sent.

Then, Tor encrypts other left addressing information, called as Packet Wrapper. Then this modified as well as encrypted data packet is then routed through many of these listed TOR servers, called relays, for its final destination. Each relay at its end only decrypts enough of the data packet wrapper to know from which relay the data came and to which relay it needs to be send next. Then relay rewraps the package in a new wrapper and transfers it forward. The layers of encrypted address information used to anonymize data packets sent through Tor are like an onion, hence the name given. Due to which data packet's path through the Tor network thus packets cannot be fully traced.

These Internet data packets are encrypted using a protocol called Secure Socket Layer (SSL) or Transport Layer Security (TLS). However, even SSL/TLS is used there are chances that those packets might be intercepted and sniffed to see information’s metadata like sender information, encrypted data information and who received that request in relay server because the addressing wrappers in SSL or TLS are not encrypted. But TOR hides the identity of sender and receiver of a given transmission.

If Tor Browser is used to visit a website that does not use encryption to secure users' connections, then that data packet will not be encrypted on reaching its final hop from last TOR relay because it lies outside the TOR. So try to use HTTPS websites so that data is encrypted and there are least chances of insecurity thus achieving high anonymity.





Some TOR terminology:

Let’s understand basic terms & concept of TOR networking. The Tor consist of the following components:

* Guard Node: Entrance node or the guard node is used as the entrance for user data via which it is encrypted & forwarded into the network.
* Relay Node: It forwards the data which received from entrance or other relay node to another relay or exit node, each relay node is chosen randomly.
* Exit Node: It marks the end of the network & exit nodes are chosen based on networks exit policy. It is the node which is unencrypted thus gets compromised.
* Client: User whose data is transmitted over proxy.
* Onion proxy: It is the application that allows to bypass. - Directory Server: Stores router’s information & public keys of all nodes.
* Cell: It is a Unit of transmission, fixed in size. Each cell is 512bytes.
* Onion router: An onion node that routes cells in network.
* Encryption: The cell which is encrypted in form of various layers, for each hop a layer is decrypted/removed & cell is forwarded, so the last layer is un-encrypted which is forwarded to destination.   
  During the forwarding or hopping the actual content is invisible to the relay/mix nodes, thus the name onion routing. Node to node communication is secured by TLS & public keys are used by communicating clients for establishing AES session keys for each hop.
* Rendezvous Point : Point at which two nodes meet where data is transferred from one node to another

**TOR Traffic Analysis**

Exit Nodes Can Be Sniffed While using Tor, Internet traffic is routed through Tor’s network and goes through several randomly selected relays before exiting the Tor exit node. Tor is designed in such a way that which is theoretically impossible to know which computer actually requested the traffic. Computers may initiate connections or it may be acting as a relay, relaying that encrypted traffic to another Tor node. But the last Tor node, where traffic leaves the Tor network and enters to internet destination, can be monitored by intruders. This node where traffic exits the Tor network is known as an “exit node” or “exit relay” here the node is unencrypted which is vulnerable to adversary using sniffing and website fingerprinting.   
To collect data regarding traffic exiting the TOR network, with default exit policy. During this time, router relayed TCP traffic exiting the Tor network. In order to gather statistics about traffic leaving the network, we ran Tcpdump on the physical machine as our Tor router. Tcpdump was configured to capture only the first 150 bytes of packet using the “snap length” option (-s). This limit was selected so that we could capture up to the application-level headers for protocol identification purposes.  
At most, total 96 bytes of application header data was captured, since an Ethernet frame is total 14 bytes long, an IP header is total 20 bytes long, & a TCP header with no options is totally 20 bytes long. Then the ethereal was used, another tool for protocol analysis and state-full packet inspection, for identifying application-layer protocols.

As a post-processing step, we filtered out packets with a source or destination IP address of any active router. This left only exit traffic.  
If you’re accessing an encrypted (HTTPS) website like Gmail account, this is okay – although the exit node can see that you’re connecting to Gmail. If you’re accessing an unencrypted website, the exit node can potentially monitor your Internet activity, keeping track of the web pages you visit, searches you perform, and messages you send.

**Common Threats and Countermeasures for TOR**

1. Traffic Analysis: Exit Nodes Can Be Sniffed

While using Tor, Internet traffic is routed through Tor’s network and goes through several randomly selected relays before exiting the Tor exit node. Tor is designed in such a way that it is theoretically impossible to know which computer actually requested the traffic. Your computer may have initiated the connection or it may just be acting as a relay, relaying that encrypted traffic to another Tor node. But the last Tor node, where your traffic leaves the Tor network and enters the open Internet, can be monitored. This node where traffic exits the Tor network is known as an “exit node” or “exit relay” here the node is unencrypted which is vulnerable to adversary using sniffing and website fingerprinting. To collect data regarding traffic exiting the TOR network, with default exit policy. During this time, router relayed TCP traffic exiting the Tor network. In order to gather statistics about traffic leaving the network, we ran tcpdump on the same physical machine as our Tor router. Tcpdump was configured to capture only the first 150 bytes of a packet using the “snap length” option (-s). This limit was selected so that we could capture up to the application-level headers for protocol identification purposes. At most, we captured 96 bytes of application header data, since an Ethernet frame is 14 bytes long, an IP header is 20 bytes long, and a TCP header with no options is 20 bytes long. We used ethereal, another tool for protocol analysis and state-full packet inspection, in order to identify application-layer protocols. As a post-processing step, we filtered out packets with a source or destination IP address of any active router. This left only exit traffic.  
If you’re accessing an encrypted (HTTPS) website such as your Gmail account, this is okay – although the exit node can see that you’re connecting to Gmail. If you’re accessing an unencrypted website, the exit node can potentially monitor your Internet activity, keeping track of the web pages you visit, searches you perform, and messages you send.

* Countermeasures:

If the site connected does not use HTTPS, the traffic will be sniffed from the exit node or even from other VPN using Man-In-The-Middle. Using websites which are having HTTPS rather than HTTP and other solution to this problem includes find a proxy that should be trusted for not sniffing data and thus preserves anonymity.

1. DNS Leak

Domain Name Service (DNS) is a mapping or translation of a domain name to an IP address i.e. (dotted decimal notation), so that humans can remember computer address by a url name instead of IP addresses. A DNS leak is a major problem to online users in terms of privacy and security due to the network which is supposed to be anonymous but it is not, thereby providing a false security to the user. A DNS leak is matching of TOR’s DNS IP to ISP’s real IP. Technically it is, leaking of user's real IP address while connected to a TOR service. A DNS leak occurs when computer is unknowingly accesses default DNS servers rather than using anonymous DNS servers provided by TOR network. This usually happens when any third party application tries to connect to internet and in some cases whenever a DNS query fails which is to be routed through the anonymity network, causing a DNS leak, and thereby user's real IP address is exposed to the public network.

DNS requests not sent through Tor network by default thus attacker could see what websites are being visited. External software such as Foxy proxy, Privoxy, etc that can be used to route DNS requests through tor network, but this is not default behavior.

* Check DNS Leak:

-To perform a DNS leak test simply go to [dnsleaktest.com](http://www.dnsleaktest.com/).   
-Check the results to make sure that you recognize the IP numbers.   
-In particular, any result that shows your ‘real’ location or that belongs to your ISP means that you have a DNS leak.

* Countermeasures

-Use a VPN client with built in DNS leak protection.   
-Change DNS severs and obtain a static IP.  
- Most VPN providers will be happy to give you their DNS server details, or you can route your requests through a public DNS server such as those offered by [Google Public DNS](https://developers.google.com/speed/public-dns/), [OpenDNS](http://use.opendns.com/) and [Comodo Secure DNS](http://www.comodo.com/secure-dns/). So that there are less chances of DNS leak and traffic sniffing from Local Service provider or ISP in some cases.

1. Rogue Exit Node

The Tor network works by connecting to a Tor node. A Tor node then connects to a deeper Tor node, which connects to a deeper Tor node, which connects to an exit node.

People must consent to run exit nodes, as running exit nodes puts them at more of a legal risk than just running a relay node that passes traffic. It’s likely that sometimes government investigators run exit nodes and monitor the traffic that leaves them, using what they learn to investigate criminals or, in repressive countries, punish political activists.

The last node via which traffic passes over TOR network has to be decrypted while communicating before reaching to its final destination. Someone operating that node can see the communication passing through this server. Criminals have also started using Tor network as a communicating channel for malware command and control (C&C) center, which means that its presence can indicate infection and compromise. For most organizations this will probably be the biggest worry of all.

Although Tor C&C is slower but is a tempting place for malware to hide its communications. The bandwidth of some of the weak exit nodes has resulted in Tor being hijacked for DDoS attacks.

* Countermeasures

-Open the location where your Tor browser is installed. Open the Browser folder inside Tor's directory. Double click on Tor Browser folder.

-Click on Data folder.

- Choose Tor inside the Data folder.

-Edit Torrc file.

-Set Exit Node for Tor, for example: ExitNodes {za} StrictNodes 1.

-Save Torrc file.   
By this we can make exit node by which traffic for particular user can be sniffed and it can be used to redirect the data to unwanted destinations and it can be used by investigation agencies.

* Reporting Malicious Node

-If the client does detect it is there a way to report and possibly block that particular exit node? Yes. If you suspect that an exit relay is interfering with your network traffic, you should report it to the Tor Project by creating a new ticket in the bug tracker.

1. De-anonymize Tor users from their Bitcoin transactions

It is considered that Bitcoin is one of the most secure and reliable systems to pay online without being tracked by law enforcement, the members of Tor Project warned about the recent **“Operation Onymous”** exploited the Bitcoin to identify the operators behind the seized black markets. In effect, it is possible to de-anonymize clients in a Bitcoin P2P network.

To exploit a built-in flaw in the Bitcoin architecture to reveal the IP address of a client who makes a payment with the virtual currency. The attacker generates a ‘malformed message (data)’, faking it to be sent by the user through the Bitcoin peer-to-peer network. These malformed data causes the unmasking of real IP address, and if fake messages exceed 100, the IP could be banned for 24 hours.

The mechanism is implemented as a DOS protection and could be abused to separate Tor from Bitcoin. The attackers force Bitcoin servers to refuse connections from Tor network and other anonymity services. This results in clients using their actual IP addresses while connecting to various destinations and thus being exposed to the attacker, which makes correlation with the pseudonyms with IP addresses.

Then every time a client makes a connection from a Bitcoin server, its IP address is revealed.  
If a Bitcoin client is using proxy for connecting over a Tor relay and sends malformed data messages, the IP address of this relay will be banned after a specific number of messages, and the Bitcoin users will continue to work with its original IP address. This technique isolates users from the entire Tor network, if the attacker is able to separate Bitcoin users from the entire Tor network by sending malformed messages to every Tor sever.

1. Not only de-anonymization but seizing directory authorities

Bitcoin Users reveals the IP addresses of Tor users, because there is also another possibility of compromising the entire architecture. The Tor network relies on 9 directory server authorities located in the United States & Europe, which provide a list of all the signed relays.

By attacking to these servers the overall TOR architecture can be compromised. The seizing of directory authorities (at least five) which belongs to the Tor network, could force Tor users to connect other relays. This attack could be conducted for disarming the Tor network.

Law enforcement investigation could run covert operations to interfere criminal crews that exploit the anonymizing system. Tor network also provides a safe network for millions of peoples.

**PROBLEM DEFINED: ATTACKS VECTORS FOR INVESTIGATORS**

These are the possible attacks & how the nodes get compromised.

1. Server attack: This is the basic attack where adversary compromises some server with high bandwidth & resources then it introduces it into the TOR system.   
Since the compromised server has high chances of being chosen as guard or exit is high, out of which guard node can be hacked for biased path and also these exit nodes where data is free from any encryption & internal contents is easily readable.

2. Illusion attack: The adversary compromises any randomly selected server because it wants to seize working network, intruder reports falsely to the TOR about the bandwidth allocation since directory, servers never actually verify the node capacity rather stores the information is given by node, where most of the cells are hopped to compromised node, thus server fails to handle the traffic and drops all data.

3. Application attacks: In this type of attack, adversary will analyses the system thoroughly for software flaws in system setting, JavaScript’s setting along with browser extensions & network. Using this loops the intruder bypasses the security and this type of attack can be performed at any of the node.

4. Circuit attack: This attack is performed only at entrance & exit node, adversary mostly compromises either entrance or exit & extends the attack in order to compromise nodes thus perform illusion attack creating a biased path and spread the attacks to sub-peers.

5. Timing attack: Adversary makes correlation between his timing & various flow characteristics with client through entrance and flow of data packets.

6. Cell based attack: The adversary first monitors both entry & the exit nodes & it must also have knowledge of who are user of that network. Then attacker selects a signal at appropriate time and then changes the cell counter of destination correlating to that signal.   
Signal embedding is done by adversary into destination, that signal will be transmitted along with actual messages to the entry node of onion router connecting to destination then at the entry onion router various variations received and embedded signals will be recognized, if found same pattern is matched.

7. Browser attacks: While using TOR, a client must use an HTTP proxy such as Privoxy, etc. So that all traffic of Tor is diverted via proxy rather than sending directly over the Internet, because most of the browsers will not automatically starts sending DNS queries through a SOCKS proxy. Sometimes software like as Flash, Java, and ActiveX Controls, do not use the browser’s proxy for network traffic. When any of these programs are executed by the browser then that traffic is not directed via TOR directly instead it establishes direct TCP connections compromising anonymity. This type of attack allows a website to identify its visitor.

8. Privacy Attacks: If TOR used as directed by the Tor Project can provide an effective layer of privacy, but undirected use causes information to leak. Mostly people don't utilize Tor button and browser information as agent strings was leaked potentially providing geo-location and host PC configuration. By stopping and properly using TOR button user can stop potential attacks.   
Also using HTTP requests via search engines provides information about user location, etc. The Tor button and other such user agent switching plug-ins prevents tagged geo-location information and OS details by spoofing details of defined-user. Measures to stop geo-locating via users searching would be user understanding like using HTTPS search engines

9. Circular attack: Adversary makes use of network as a normal user and transfers the packet in such a way that it forms a circular circuit inside the TOR network thus consuming lots of bandwidth to transfer same packet over and over. The onion Network never understands attack since every next node does not know about previous nodes.   
So actual address is never revealed as it is difficult in realizing that from where the packet actually came from the destination to which the node forwarded it.

10. Watermarking attacks: These attacks are very effective in TOR de-anonymization because it is a low latency as a unique signal can be embedded to identify the receiver to link with sender.   
The adversary adjusts inter packet delay between packets by manipulating the packet count then by checking population of packets within the intervals reveal about watermarking bit.

11. Cryptanalysis attack: For TOR, this attack is done by compromising keys. It is attack when attacker determines which key is used to encrypt and decrypt the data.

**Analysis and Results of Attacks**

Let’s estimate that the total probability of our attack. Suppose that Tor makes n entry guard nodes in a network of k nodes, out of which there are x exit port 80.

In our attack, the client uses one circuit which changes at every 10 minutes. Then let’s say that the attacker inserts y evil nodes in the TOR system, of which v are exit nodes modifying HTTP traffic. These exit nodes can be noticed by Tor users, but the other y - v servers only log data and are not malicious.   
At Any given bugged page will use one entry guard every ten minutes, so for any Tor user that has an evil entry guard the chance of being discovered in any ten-minute interval is 1 k ˜ 33%, and the probability of remaining anonymous over time is approximately the exponential distribution P(t) ˜ k-1 k t/10 min ˜ 0.66t/10 min . This means that a Tor user has a 0.4% chance of ever being vulnerable to the attack.   
Every 10-minute interval during which a vulnerable user leaves a webpage open, he has a 0.5% chance of leaving a signal generator running. If he leaves a bugged page open over an hour-long lunch break, he has a 92% chance of having this signal generator go through an evil entry node.

The probabilities that users are vulnerable or that they will receive a signal generator are low, but this is under the assumption that the attacker only controls a single Tor node.

**How to block Tor in your business from unauthorized activities.**

* Blocking by port: As mentioned below, Tor is partial to common ports such as 443 but it can also block HTTPS traffic as well if not configured properly.
* Blocking at the endpoint: Tor software should be stopped from installing by disabling external USB device by implementing privilege management. However, Tor can also be run pre-installed from a USB stick so in some cases these method can be bypassed.
* Blocking - from IP ranges to DPI:  Another method include checking LAN traffic but it is difficult because TOR uses SSL/TLS the traffic won’t be easy to spot and its content will be impossible to interrogate. By time the traffic inspected by firewall it will be difficult to inspect. A common techniques is SIEM logging by finding publically-known IP addresses used as entry nodes in TOR.

But this is temporary method because TOR list is dynamic in nature. Sometime innocent traffic may be blocked giving false positive. Second method is the Deep Packet Inspection (DPI) interface on firewall for unusual certificates used by TOR nodes along with checking ports.. Tor uses 443, but also 80 (HTTP), 9001 and 9030 but other ports can also be configured.

**Case Study**

CASE 1: Child Pornography Case

Jay Michaud, a public school teacher from Vancouver, Washington was arrested and charged with child pornography possession in July 2015. Michaud was monitored while accessing “Playpen,” a child pornography site hosted on the dark web. After Playpen’s servers were seized, then the agency hosted the site on its own servers for 13 days to spy.

For this FBI then carried out a Network Investigative Technique thus bypassed Tor and gathered MAC, IP and other information on the suspects. Judge then issued an order asking the FBI to explain how exactly it was able to subvert Tor. But the order was prompted partly.

CASE 2: Illegal Drugs Home Delivery

Mumbai cops were clueless when Indian Post delivered a regular business envelope to Shikhar’s\* door. Envelope consisted double vacuum-sealed package with five LSD stamps. For the unknown, LSD is a banned, semi-synthetic, psychedelic drug known for psychological effects that include hallucinations and an altered sense of time. It is colloquially referred to as acid. Indian Postal Service should not to be blamed. The consignment was ordered by Shikhar’s friend Ruhaan\* from online marketplace Silk Road, an underground site from where you can purchase everything from drugs to electronics to guns and fake passports. Given that in theory, you can order guns and other terror-related items from Silk Road and BMR, we hope our law enforcement agencies won’t be clueless for very long.

**Investigating Anonymously Using TOR**

To prevent & keep in check about the attacks following measures in network as well as client side TOR proxy:

1. Network Uptime verification: By sending periodic messages to the nodes we can keep the track of server’s uptime & downtime period, if the server are unavailable for very long time then there are high chances that it is compromised. Bandwidth scanning: The bandwidth of routers are measured & corrected in the directory server information for scanning the speed.
2. In Client software’s: There are default customization for TOR
3. TOR Buttons: Enable it
4. TOR Plugins: Disable this option.
5. Dynamic content Isolation: This function disables java scripts and doesn’t allow meta-data refresh and also blocks pop-ups.
6. Hooked java-scripts: This option masks the present time zone user agent & operating system.
7. No automatic TOR updates: TOR updates are never made from SSL websites, so if user receives any request then it might be a malicious program. Other options include blocking history read &. Using Firefox web browser extensions one can customize browser functionality & its component with XML & java-scripting.

**TOR ALTERNATIVES**

1. I2P: I2P is an anonymous peer-to-peer distributes communication layer which is built using the open source tools. It is a complete Tor alternative.

1. Tails: It is another Tor alternatives available, it is a Linux live operating system started using any USB drive, DVD or a SD card. It consist pre-configured apps that provides services of web browser, etc.
2. Subgraph OS: It uses the Tor network just like Tails but it focuses on usability. It is designed by Canadian security firm which calls this OS as “adversary resistant” designed to reduce attacks.
3. Freenet: It is a peer-to-peer to resist the censorship similar to I2P. Freenet uses the similar P2P technology of distributing data storage to deliver and keep the information.

1. Freepto: It is another Linux-based OS which could be booted using a USB disk on any computer. The data saved on the USB disk will be encrypted automatically.

**CONCLUSION**

Tor is available for Mac and Windows, but there are precautions for users when using it, Once the Firefox browser is running on Tor client can surf anonymously on social media sites and access areas of the deep web that are not indexed by Google. The Onion Routing provides anonymity but does not protect the exploitation of an insecure application to reveal the IP address of, or trace, a TCP stream.

Nowadays Law enforcement uses Tor to visit target websites without leaving government IP addresses in their web log, and for security during sting operations. Government officials can use above given attack vectors to find criminals using TOR networks and preventive methods could be used to secure their identity so that it is easy to search in locations like deep web & dark web without leaving IP traces. Investigators aims to de-anonymize hackers without the need of end-to-end decryption.

Thus, TOR should be considered as tool which is insecure and doesn’t prevent user’s anonymity. Attacks like website fingerprinting provides most of the information about TOR users. So, it should not be used for illegal purposes like using Silk route or BMR but it should be only for legal purposes.

“Because knowledge is no longer power but the way we use it is power”.

REFERENCES

[1] TheOnionRouter/TorFAQ.November2006.from: http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ

[2] Blackhat,(2007)“*Securing the Tor Network*” from: https://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-

perry-WP.pdf

[3] Cassandra Security, (2009) “*Onion Routing and Darknets*“ from: http://cassandrasecurity.com/index.php?s=onion+routing

[4] Torproject.org (2010) from: http://gitweb.torproject.org

[5] Vulnerabilities of TOR from: http://freehaven..net/~arma/slides-25c3.pdf

[6] watermarking TOR from: <http://dj.eas.aus.edu/snac/document>

<http://resources.infosecinstitute.com/hacking-tor-network-follow/>

[7]<http://web.mit.edu/k_lai/www/torpaper.pdf>

[8] Security against TOR Network: [hhttp://www.ijcset.com/docs/IJCSET12-03-01-072.pdf](http://www.ijcset.com/docs/IJCSET12-03-01-072.pdf)

[9] http://www.tomsguide.com/us/what-is-tor-faq,news-17754.html