Autonomous Institution Affiliated To VTU, Belagavi)

AN INTERNSHIP REPORT

ON

"HOW TO PROTECT YOUR SYSTEM USING TOR"

Submitted in partial fulfillment for the award of degree of Bachelor of Engineering in

INFORMATION SCIENCE AND ENGINEERING

Submitted by

NAGARJUN.P **1MJ21IS064**

Internship carriedout at
Plasmid Innovation
Bangalore, Karnataka

Under the guidance of

Internal Guide	External Guide
PROF. BINDU MADHAVI.P Professor, Dept of ISE MVJ College of Engineering Bengaluru-560067	**K PRAVEEN KUMAR** Senior Manager Plasmid Innovation Ltd Bangalore – 560103

DEPARTMENT OF INFORMATION SCIENCE MVJ College of Engineering
Whitefield, ITPB Main Road, Bengaluru -560067 ACADEMIC YEAR 2023-24

(Autonomous Institution Affiliated To VTU, Belagavi)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the internship titled **"HOW TO PROTECT YOUR SYSTEM USING TOR"** is a bonafide work carried out by **Nagarjun.P(1MJ20IS064)** in partial fulfillment for the award of degree of Bachelor of Engineering in Information Science and of the Visvesvaraya Technological University, Belagavi during the year 2023-24. It is certified that all corrections/suggestions indicated during the internal assessment have been incorporated into the internship report. The internship report has been approved as it satisfies the academic requirements.

Signature of Guide	Signature of HOD	Signature of the Principal
Prof. Bindu Madhavi. P Assistant Professor, Department of Information Science and Engineering MVJCE, Bengaluru-67	**Dr. Shima Ramesh** HOD, Department of Information Science and Engineering MVJCE, Bengaluru-67	**Dr. Suresh Babu V** Principal, MVJCE, Bengaluru

EXTERNAL VIVA

NAME OF EXAMINERS	SIGNATURE OF EXAMINER
1.	
2.	

MVJ COLLEGE OF ENGINEERING BENGALURU - 560067

(Autonomous Institution Affiliated To VTU, Belagavi)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

DECLARATION

I, **Nagarjun.P (1MJ20IS064)** student of sixth semester B.E., Department of **Information Science and Engineering**, MVJ College of Engineering, Bengaluru, hereby declare that the internship titled "**HOW TO PROTECT YOUR SYSTEM USING TOR**" has been carried out by me and submitted in partial fulfillment for the award of Degree of **Bachelor of Engineering** in **Information Science and Engineering** during the year 2023-2024.

Further I declare that the content of the report has not been submitted previously by anybody for the award of any degree or diploma to any other University.

NAGARJUN.P **1MJ21IS064**

Place: Bengaluru

Date:

CERTIFICATE

ACKNOWLEDGEMENT

I am in debted to our guide, **PROF. Bindu Madhavi.P** of **Information Science and Engineering** for her wholehearted support, suggestion and invaluable advice throughout the Internship and also for the help in the preparation of this report. I would also like to extend my gratitude to **Mr. K PRAVEEN KUMAR,** Senior Manager of **Plasmid Innovation Ltd** for his guidance in carrying out the internship.

Our sincere thanks to **Dr SHIMA RAMESH MANIYATH**, Professor and Head of **Information Science and Engineering**, MVJCE for her support and encouragement. I express sincere gratitude to our beloved Principal, Dr.Sureshbabu V for his appreciation towards the internship.

I thank all the technical and non-technical staff of the **Information Science and Engineering**
department, MVJCE for their help.

Thanking You.

ABSTRACT

Our project explores the integration of Tor, the Onion Router, as a strategic tool to enhance the security of computer systems in the face of growing online threats. It delves into fundamental and advanced strategies such as anonymous browsing, secure communication channels, and accessing. onion services

The papers suggest system-wide integration of Tor to anonymize applications and services, thereby minimizing vulnerabilities. Emphasis is placed on the role of Tor in thwarting traffic analysis attacks, providing an additional layer of defense against adversaries

The approach aims to fortify systems by combining Tor with traditional security measures. The paper advocates for the use of Tor Browser, designed for enhanced privacy, and highlights the benefits of accessing onion websites for heightened anonymity and security. The multi-faceted approach proposed seeks to protect sensitive information from interception and eavesdropping.

Overall, this project lays the foundation for a comprehensive exploration of Tor's potential in fortifying digital systems against diverse cyber threats.

TABLE OF CONTENT

TABLE OF FIGURES

CHAPTER 1

INTRODCTION

Tor (The Onion Router) is an internet networking protocol designed to secure the data relayed across it. Using tor's software will make it difficult, if not impossible, for snoops to see our webmail, search history, social media posts or other online activity. They also won't be able to tell which country we are in by analyzing our IP address, which can be useful for journalists, activists, business people and more.

AIM: Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their internet activities from being monitored.

Tor directs internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

The web browser stores the web-browsing history, while servers contain a log with an IP address and timestamp. In addition, an ISP can eavesdrop on the traffic and see what one is browsing. The Internet is no longer anonymous nowadays. Large IT companies, such as Google, Facebook, and Microsoft offer a variety of services for free. Most countries prosecute people for illegal actions on the internet. Tracking down a person works the following way: law-enforcing agencies make an inquiry to the owner of the resource where an illegal action has happened in order to acquire the IP address of the person who committed the illegal action. The IP address reveals the identity of the host who committed the illegal action. Technically, this means that all tracking is based on the IP address. In some countries, an illegal action can be a post or a comment about a hot political topic. That is why it is important to maintain privacy and anonymity online in order to preserve freedom of speech. In order to become anonymous on the internet, it is possible to use VPN, Proxy servers, I2P, Tor, Free net and many other software packages or technologies. The drawback of Proxy servers and VPNs is that these are centralized systems, meaning that in case the Proxy server or VPN gateway are compromised, it is possible to trace down the user. Tor is a distributed system and was designed to protect the user's identity as well it is

extremely popular.

The Tor browser works by moving your internet traffic between different worldwide Tor servers known as T-nodes. T-nodes provide Tor with millions of distributed worldwide proxies that use many different IP addresses to enhance web anonymity.

Tor is not meant to completely solve the issue of anonymity on the web. Tor is not designed to completely erase tracking but instead to reduce the chance that something will happen for sites to trace actions and data back to the user. The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.

Many workplaces use corresponding data to perform daily tasks, and information technology (IT) specialists are increasingly implementing client-server networks to manage information. Using a client-server network, you can efficiently access, share and secure data across devices. Understanding how this system functions in the workplace can help you perform routine tasks by hosting and managing resources and services that client computers need and allowing users to access information from a central server. A client-server model is a networking computing system design that illustrates a relationship between two or more computers, where the client computers request and receive services or resources from a powerful centralized server computer. It describes a specific way devices access the information we store in servers. It also allows multiple clients to open applications or retrieve files from an individual server, which helps maintain consistency across all devices. Many companies across various industries use servers to store and access information, offering more processing power and providing more extensive storage space.

Providing a usable anonymizing network on the Internet today is an ongoing challenge. We want software that meets users' needs. We also want to keep the network up and running in a way that handles as many users as possible. Security and usability don't have to be at odds: 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.

Ongoing trends in law, policy, and technology threaten anonymity as never before, as it weakens our ability to speak and read freely online. These trends also weaken national security and critical infrastructure by making communication among individuals, organizations, corporations, and governments more liable to analysis. Each new user and relay provide additional diversity.

CHAPTER 2

ABOUT THE ORGANIZATION

PLASMID is dedicated to providing individuals with the advanced skills and knowledge needed to excel in today's dynamic and competitive job landscape. The platform focuses on closing the gap between traditional education and the ever-changing needs of modern industries by offering targeted upskilling opportunities.

At PLASMID, the focus is on helping learners develop specialized skills that are in high demand in the job market. Recognizing the rapid changes in technology and industry standards, PLASMID designs programs to ensure that participants gain the critical expertise that employers are looking for. Whether individuals are seeking to progress in their current roles or transition to new careers, the courses given here provide the essential tools for success.

This company goes beyond standard training by offering personalized mentorship from seasoned industry professionals. Instructors here are experts with significant industry experience. These mentors guide participants through in-depth skill development, offering tailored advice and valuable industry insights. The mentorship program is designed to help learners overcome obstacles, refine their abilities, and reach their career goals.

PLASMID emphasizes learning through doing, with hands-on projects that simulate real-world challenges. These projects give students the opportunity to apply their knowledge in practical situations, helping them build a strong portfolio that showcases their skills to potential employers.

The motto of PLASMID is" Accelerating growth, for a secure tomorrow".

Fig 2.1: Logo of PLAMID

CHAPTER 3

INTERNSHIP DOMAIN

Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, unauthorized access, or damage. It involves a set of processes, practices, and technologies designed to safeguard computers, networks, programs, and data from cyber threats. These threats can include everything from hacking attempts and malware to data breaches and phishing attacks.

Cybersecurity is crucial for safeguarding valuable data from breaches and theft, which helps prevent financial losses and protects a company's reputation. It ensures businesses can operate smoothly without disruptions caused by cyber threats. Additionally, compliance with regulations like GDPR and HIPAA is essential, as non-compliance can lead to significant penalties. Strong cybersecurity measures also foster trust with customers, partners, and stakeholders, enhancing confidence and supporting long-term business success.

Some tools used in Cybersecurity are:

1. Network Security Tools : Firewalls,Intrusion Detection and Prevention Systems (IDPS),Security Information and Event Management (SIEM) Systems.
2. Endpoint Security Tools : Antivirus/Anti-malware Software,Endpoint Detection and Response (EDR).
3. Penetration Testing Tools : Vulnerability Scanners,Penetration Testing Frameworks,Password Cracking Tools.
4. Encryption Tools : Disk Encryption Software,Email Encryption Tools.
5. Web Security Tools : Web Application Firewalls (WAF),Content Management System (CMS) Security Tools.

Cybersecurity is a constantly evolving field that plays a vital role in protecting the digital world from a wide range of threats. As technology advances, so do the techniques used by cybercriminals, making ongoing vigilance and innovation essential in this domain.

CHAPTER 4

SYSTEM REQUIREMENTS

4.1 Hardware Requirements

1. Processor (CPU):A modern processor with at least 2 cores .For a relay node, a standard server CPU.For an exit node, a more powerful CPU may be needed depending on the expected traffic.
2. Memory (RAM):Minimum 512 MB (sufficient for a small relay node).Maximum 1 GB or more, especially for exit nodes or high-traffic relays.
3. Storage:1 GB of disk space.
4. Network:A stable and fast internet connection is crucial.
5. Rasberry Pi 3

4.2 Software Requirements

1. Operating System: Linux – Ubuntu 16.04 LTS.
2. Tor Software: Tor can be installed using package managers like APT (for Debian-based systems).
3. Configuration:**torrc File**: The configuration file where you define the node type (relay, exit, bridge), bandwidth limits, and other settings.
4. Google Cloud Platform

CHAPTER 5

SYSTEM DESIGN

5.1 ONION ROUTING

Onion Router connections are protocol independent and consist of three phases: connection setup, data movement and connection teardown.

- Connection setup: it is the first stage where the client machine or initiator creates a so called onion which defines the route of the packet, in other words, the initiator chooses the Tor nodes that the packet will travel through.
- Data movement: it is the second stage when the client pushes the data through the Tor network.
- Connection teardown: is the third phase when the connection is closing after the client chooses to not move the data through the Tor network.

Onion by itself is a layered data structure which defines the properties of the connection at each node along the path such as: cryptographic algorithms and keys that shall be used during data movement phase.

Every onion router along the path uses its public key to decrypt the entire onion that it receives and its duty is to pass data from one connection to another after applying some specific cryptographic operation. The Tor network consists of nodes. There are three types of nodes: guard node, relay node, and exit node.

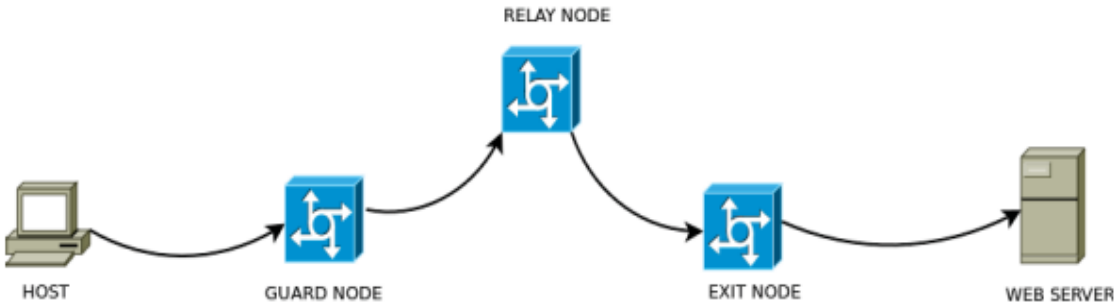


Fig 5.1: Tor topology

- The guard node is the only node that knows the host's identity. It acts as an entry point to the Tor network.
- The relay node is used to relay the packets to the exit node, which makes the system more secure to identity revealing attacks.
- The exit node is used to relay the traffic to the requested resource.

1. Host gets a list of available nodes from the Tor directory (request is encrypted).
2. Host selects the nodes and creates the circuit.
3. Host relays the packets through the Tor network.
4. The packets received by the requested resource have a source IP address of the exit node.

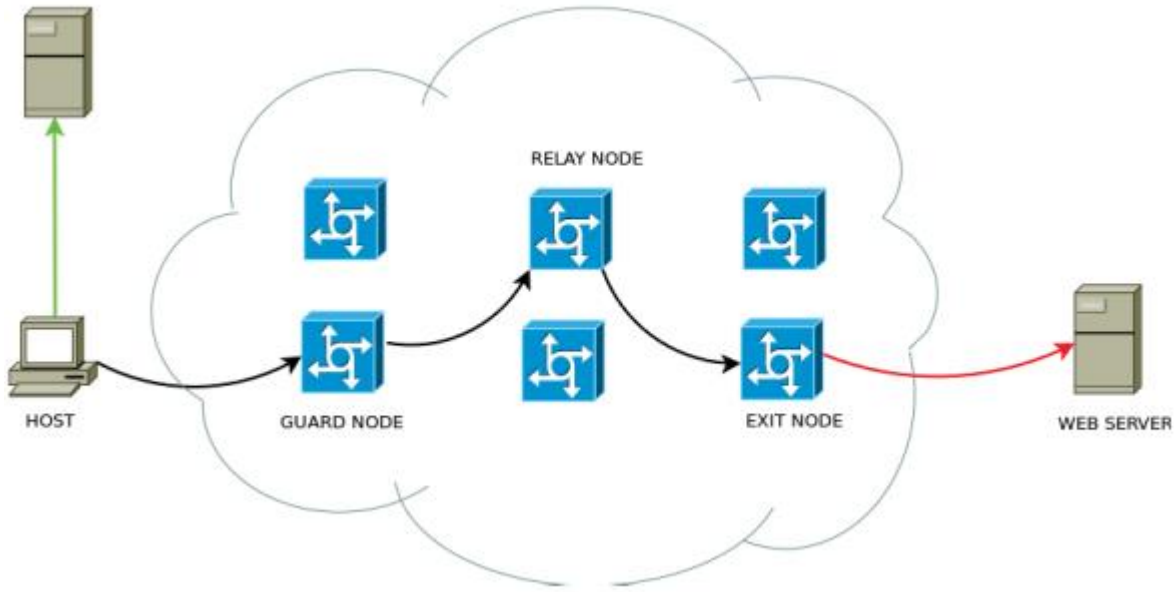


Fig5.2:Tor topology including Tor directory

In addition, Tor is used to hide the identity of the resource. This is called Hidden service. It has a special domain name. The logic behind the hidden service is that it uses a node called Rendezvous point which is used to secure the identity of the initiator and the resource as well. The initiator uses an identifier, which is a 16-character name derived from server's public key.

5.1.1HOW DOES ONION ROUTING WORK?

If we are browsing the internet on a normal web browser like chrome, firefox, etc you request webpages by making simple GET requests to servers without any intermediary. It's just a single connection between a client and a server and someone sniffing on your network can know which server your computer is contacting.

- Onion routing does this differently. In onion routing, the connection is maintained between different nodes i.e. the connection hops from one server to another and when it reaches the last server on this circuit it is the server that we wanted to contact and it will process our request and serve us the desired webpage which is sent back to us using the same network of nodes.

- Is it called the onion router because the message we send and the responses we receive are encrypted with different keys, with a unique key for encryption for every different hop or server visit.
- The client has access to all the keys but the servers only have access to the keys specific for encryption/decryption to that server.
- Since this process wraps our message under layers of encryption which have to be peeled off at each different hop just like an onion that's why it's called an onion router.

5.1.2 HOW DOES IT PROVIDE ANONYMITY?

Suppose if there is a sniffer listening at the first conversation(client – input node) all it can know is the address of the input node and the thrice encrypted message that doesn't make sense. So all the sniffer/attacker knows that we are browsing Tor.Similarly, if sniffing starts at the exit node all the sniffer sees is a server contacting another server but it can't track the client or the source of the request generated. But now if someone is listening in at Node 2 they will know the address of the input and exit and can trace the client and the destination server. But it's not that simple, each of these nodes has hundreds of concurrent connections going on, and to know which one leads to the right source and destination is not that easy. In our circuit Node 2 is a middle node but it can be a part of another circuit on a different connection where it acts as the input node receiving requests or an exit node serving webpages from various servers.

5.1.3 DEFENCELESS IN ONION ROUTING

The only security flaw in onion routing is that if someone is listening in on a server at the same time and matches the request at the destination to a request made by a client on the other side of a network by analyzing the length and the frequency of the characters found in the intercepted request or response at the destination server and using that to match with the same request made by a client a fraction of a second and then tracking them down and knowing their online activity and shattering the idea of anonymity. This is pretty hard to do but not impossible. But removing this flaw from Tor is virtually impossible.

5.1.4 FEATURES OF ONION ROUTING:

- **Encryption:** Onion routing encrypts each layer of data, making it difficult for an attacker to intercept and decode the data.

- **Anonymity:** Onion routing provides anonymity by masking the IP address of the sender and the receiver, making it difficult for an attacker to identify them.
- **Relays:** Onion routing uses a series of relays to route data through the network, with each relay only aware of the previous and next relays in the chain, adding another layer of anonymity.
- **Decentralized:** Onion routing is decentralized, with no central authority or control over the network.
- **Resistance to traffic analysis:** Onion routing makes it difficult for an attacker to analyze the traffic patterns and identify the source and destination of the communication.
- **Hidden Services:** Onion routing can also be used to provide hidden services, which allow websites and other services to be hosted on the network without revealing their location or IP address.

Onion routing provides a powerful technique for enhancing the security and privacy of internet communications, particularly in situations where anonymity and resistance to traffic analysis are important. It is commonly used by activists, journalists, and others who require a high level of security and privacy in their online communications.

5.1.5 ADVANTAGES OF ONION ROUTING:

- **Enhanced Security:** Onion routing provides enhanced security by encrypting data multiple times and routing it through several servers, making it difficult for attackers to intercept or tamper with the communication.
- **Anonymity:** Onion routing provides anonymity by masking the IP address of the sender and the receiver, making it difficult for anyone to identify them.
- **Resistance to Traffic Analysis:** Onion routing makes it difficult for attackers to analyze the traffic patterns and identify the source and destination of the communication, thereby enhancing privacy and security.
- **Decentralized:** Onion routing is decentralized, with no central authority or control over the network, making it more resilient to attacks.

5.1.6 DISADVANTAGES OF ONION ROUTING:

- **Slow Performance:** Onion routing can result in slow performance due to the multiple layers of encryption and the need to route data through several servers.

- **Limited Accessibility:** Onion routing is not widely accessible, and users may need specialized software to use it.
- **Malicious Use:** Onion routing can be used for malicious purposes, such as to facilitate illegal activities, making it a target for law enforcement agencies.
- **Vulnerability to Endpoints:** While onion routing provides enhanced security and anonymity during transmission, the endpoints of the communication may still be vulnerable to attacks, making it important to secure the endpoints as well.
- **Resource Intensive:** Onion routing can be resource-intensive, requiring a large number of servers to route data, which can result in high bandwidth usage and increased costs.

5.2 TOR CELL STRUCTURE

The traffic in Tor network is passing in fixed-size (512 bits) cells. The Figure represents the structure of a Tor cell:

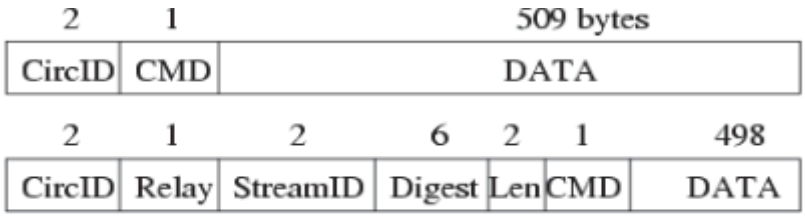


Fig5.3 : Tor control and relay cell structure.

The cell is divided into two parts: header and payload. The header consists of circuit ID which helps identifying which circuit this particular cell belongs to, because a single TLS connection can be carrying cells from multiple circuits and command which is used to tell the OR what particular action should it apply to the cell Based on the command, the cell can be either a control cell or a relay cell. The control cell commands are: create, destroy or padding. Create stands for creating a circuit, destroy for destroying it and padding is used for the keepalive messages. Relay cells have an additional streamID header, a Digest header (checksum) and a Len header (size of payload). The contents of the cell are encrypted or decrypted using the 128-bit AES cipher as the cell travels between the nodes. The CMD header contains a relay command which can be one of the following:

- Relay data
- Relay begin
- Relay end
- Relay teardown
- Relay connected
- Relay extend
- Relay truncate
- Relay drop

5.2.1 TOR CIRCUIT CONSTRUCTION PROCESS

- The initial design of onion routing implies that each TCP stream will have its own OR circuit. Building a circuit for each TCP stream is costly in terms of computing resources due to applying cryptographic operations. The Tor design implies that one circuit can be shared by multiple TCP streams. To minimize linkability between their streams, the user's OP builds a new circuit periodically, usually once in a minute.
- The below figure represents the way a user's OP constructs a circuit:

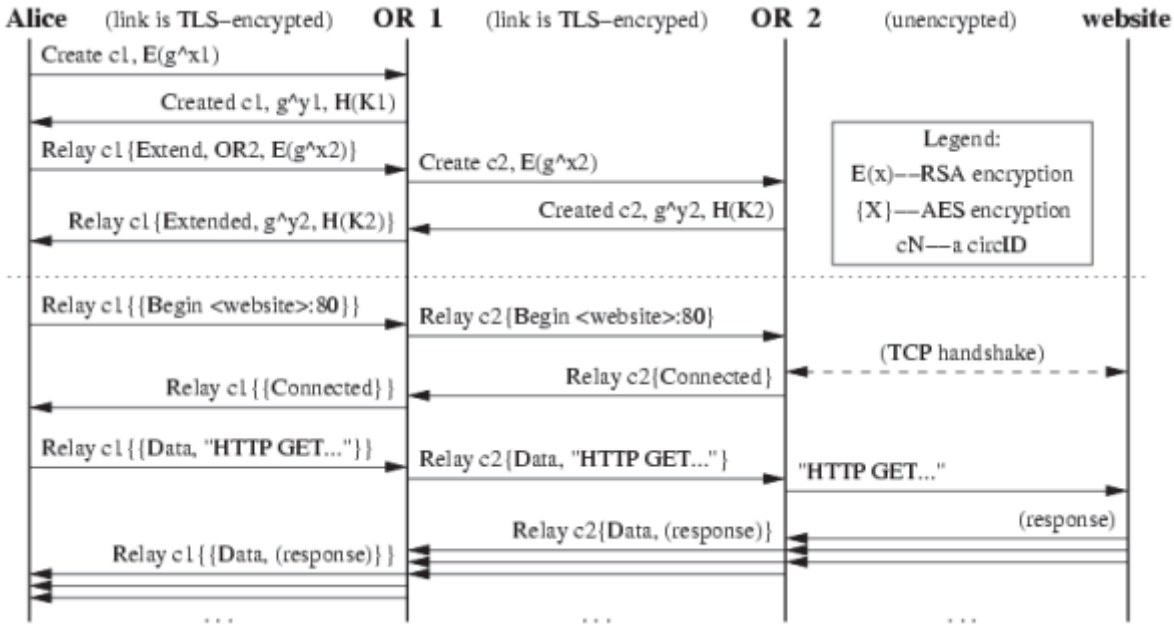


Fig 5.4: Tor key-exchange process

The circuit construction process is incremental. Each node has to negotiate a symmetric key with the other one. Firstly, Alice's OP creates a circuit with the OR1. Then OR1 creates a circuit with OR2 and forwards the information about newly created circuit to Alice. The only node which knows all the keys that are used to communicate between nodes is Alice. This is done to prevent man-in the-middle attacks, in case a node is compromised.

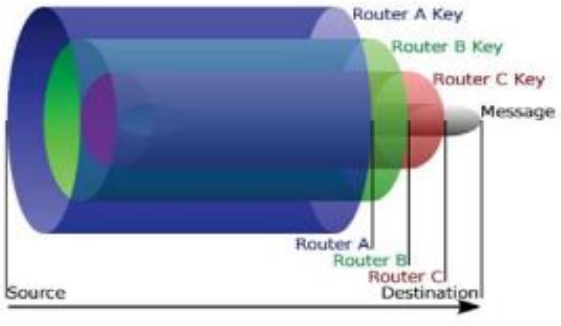


Fig5.5: Layered encryption concept

When Alice has established the circuit, she can start sending relay cells. When an OR receives a relay cell, it looks up the appropriate circuit and decrypts the cell header and payload in order to extract the session key for this particular circuit. Then the OR checks if the digest is valid. In case it is, the cell is processed further. OPs treat incoming relay cells similarly: they unwrap the relay header and payload with the session keys shared with every other OR in the circuit. If the digest is valid, the cell must have originated at the OR whose encryption has just been removed.

When the OR replies to Alice, it uses the key shared with Alice to encrypt the relay header and payload and sends the cell towards Alice along the circuit. The next OR to receive the cell adds a further layer of encryption. In order to tear down the circuit, Alice needs to send a destroy cell. When this cell is received by the OR, it closes the circuit.

5.2.2 CONFIGURING THE TOR NODE USING RASPBERRY-PI

Raspberry-Pi 3 is used to configure the Tornode. The first step is installing OS. It is possible to download a Debian Linux (Raspbian) distribution for R-Pi from the official website and write it to a microSD card which is afterwards plugged into R-Pi. If everything is configured properly, the user will be able to access R-Pi through SSH.

Fig 5.6: Raspberry-Pi 3

R-Pi is connected to the local router in the above figure and it has been configured so it could support the following topology :

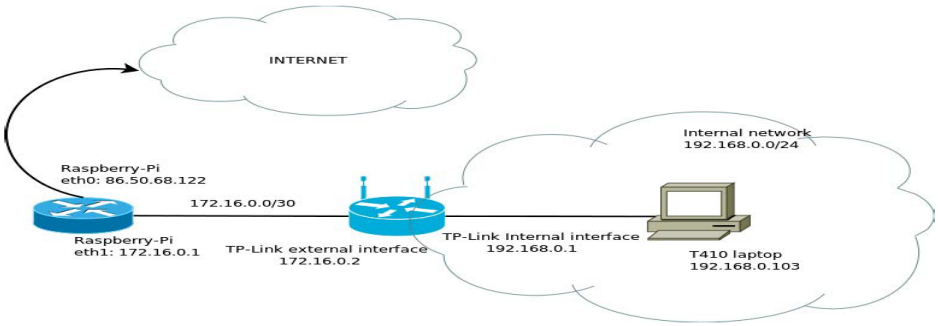


Figure 5.7: Home network topology

Configuring the network interfaces on Raspberry-Pi was carried out as follows:

```
pi@raspberrypi:~ $ sudo ifconfig eth1 172.16.0.1
pi@raspberrypi:~ $ sudo ifconfig eth1 netmask 255.255.255.252
pi@raspberrypi:~ $ ifconfig
eth0 Link encap:Ethernet HWaddr b8:27:eb:73:bf:3e
inet
addr:86.50.68.122 Bcast:86.50.69.255 Mask:255.255.254.0
inet6 addr: fe80::b0b0:9267:5b21:694a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23342 errors:0 dropped:32 overruns:0 frame:0
TX packets:448445 errors:0 dropped:0 overruns:0carrier:0
collisions:0 txqueuelen:1000
RX bytes:5116457 (4.8 MiB) TX bytes:28085876 (26.7 MiB)

eth1 Link encap:Ethernet HWaddr 00:b5:6d:00:98:db
inet addr:172.16.0.1 Bcast:172.16.0.3 Mask:255.255.255.252
inet6 addr: fe80::1a60:949c:5a93:9d72/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:373 errors:0 dropped:0 overruns:0 frame:0
TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:51985 (50.7 KiB) TX bytes:58301 (56.9 KiB)
```

It is required to edit the`/proc/sys/net/ipv4/ip_forward`file andchange the`0`to`1`in order to enable forwarding feature.

Second step is to configure the iptables to do the NAT:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o eth1 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Third step in the configuration process is installing the Tor:

```
pi@raspberrypi:~ $ sudo apt-get update
pi@raspberrypi:~ $ sudo apt-get install tor
```

5.2.3 CONFIGURING THE TOR NODE USING GOOGLE CLOUD PLATFORM

In order to successfully capture Tor traffic, we decided to use the Google Cloud platform by creating a virtual server with Ubuntu 16.04 LTS installed.

It is quite easy to create a virtual machine using the platform, it is possible to find the instructions on the Google Cloud platform web-site.

When the virtual machine is created, it is possible to ssh into it and install Tor. Afterwards, apply changes to the /etc/tor/torrc configuration file :

```
vitosinschi@instance-1$ sudo apt-get update
```

```
vitosinschi@instance-1$ sudo apt-get upgrade
vitosinschi@instance-1$ sudo apt-get install tor
vitosinschi@instance-1$ sudo vim /etc/tor/torrc


ORPort 9001
Nickname gcloudnodetest
RelayBandwidthRate 1024 KB
RelayBandwidthBurst 1024 KB
ContactInfo alexandr.vitosinschi@edu.turkuamk.fi
ExitPolicy accept *:20-23 # FTP, SSH, telnet
ExitPolicy accept *:53 # DNS
ExitPolicy accept *:79-81 # HTTP
ExitPolicy accept *:110 # POP3
ExitPolicy accept *:143 # IMAP
ExitPolicy accept *:194 # IRC
ExitPolicy accept *:220 # IMAP3
ExitPolicy accept *:443 # HTTPS
ExitPolicy reject *:*
```

CHAPTER 6

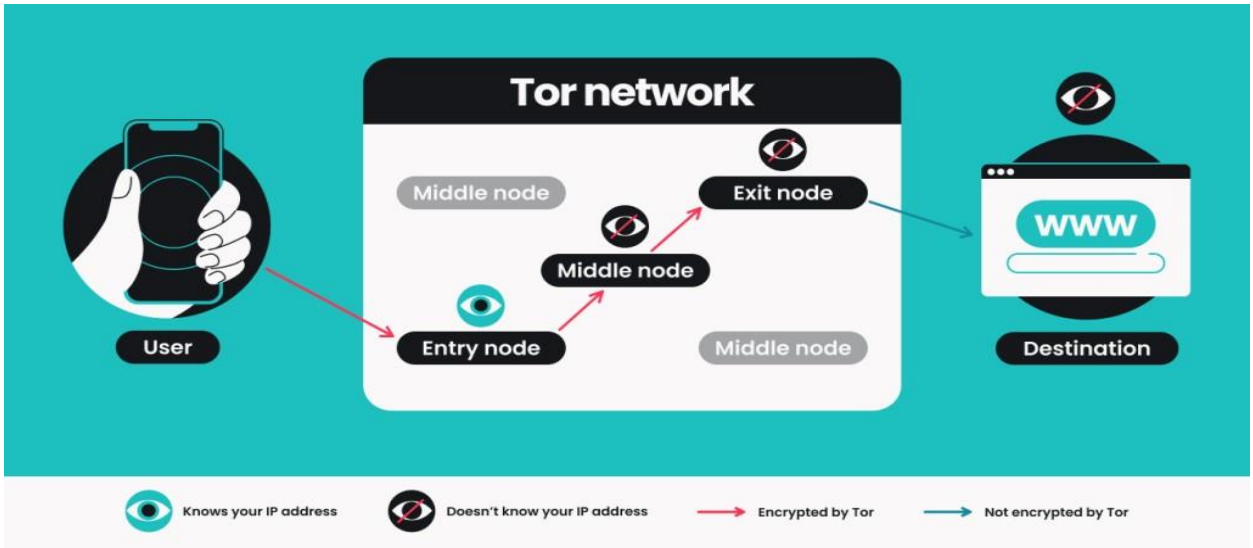
RESULTS

Using Tor for system protection provides anonymity, bypasses censorship, and enhances communication security through encryption. It allows access to onion websites for increased privacy and resistance to traffic analysis.

However, the final exit node poses potential risks as it can see unencrypted traffic. Latency is introduced due to data relay through multiple nodes, affecting activities requiring low latency. While Tor mitigates malicious exit node risks, users should exercise caution.

The system benefits from Tor's decentralized network design, making it challenging to trace online activities. Tor is valuable for protecting identity and privacy, particularly on public Wi-Fi networks. It is effective in circumventing restrictions imposed by governments or organizations.

Users must be mindful of their specific needs and threat models when incorporating Tor into their security practices.



CHAPTER 7

FUTURE ASPECT

The future scope of Tor involves enhancing usability, optimizing performance, and integrating with mobile devices and IoT. Ongoing research aims to strengthen security features and resist emerging threats, while advancements in cryptography contribute to overall resilience. Improved support for onion services fosters a more secure internet space.

Global collaboration and expansion initiatives address regional censorship challenges. User education and advocacy play a crucial role in increasing awareness and acceptance. Policies supporting the right to use privacy tools like Tor are essential.

Streamlining user experience and expanding Tor's reach contribute to wider adoption. Efforts to address latency issues for real-time applications are ongoing. Mobile integration and IoT support can extend Tor's capabilities. The continued evolution and adaptation of Tor remain pivotal in maintaining its relevance in providing online privacy .

CHAPTER 8

CONCLUSION

In conclusion, integrating Tor into a system can be a powerful tool for enhancing privacy, security, and circumventing censorship. The decentralized network design provides a robust mechanism for anonymizing internet traffic, protecting users' identities, and resisting traffic analysis. Tor's encryption capabilities contribute to secure communication, especially in scenarios where sensitive information is involved.

Access to onion websites further adds to the system's security by providing an avenue for more private online activities. However, users should be mindful of potential risks associated with exit nodes and the introduced latency in the network. The effectiveness of Tor in protecting against various online threats underscores its value for users seeking a heightened level of digital security.

Ultimately, the decision to use Tor in a system should be based on a thorough consideration of the specific security needs, potential risks, and the intended use cases. When employed judiciously and in conjunction with other security measures, Tor can significantly contribute to a more secure and private digital experience.

REFERENCES

1. **The Tor Project. (n.d.).** ***Tor Documentation*****.** Retrieved from https://support.torproject.org/
This is the official documentation provided by the Tor Project, offering comprehensive guides on installing, configuring, and effectively using Tor to enhance privacy and security.

2. **Dingledine, R., Mathewson, N., & Syverson, P. (2004).** ***Tor: The Second-Generation Onion Router*****.** In *Proceedings of the 13th USENIX Security Symposium* (pp. 303–320). USENIX Association. Retrieved from https://www.usenix.org/legacy/events/sec04/tech/dingledine.html
This foundational paper introduces Tor's architecture and discusses how it improves upon previous anonymity networks to provide secure and private communications.

3. **Electronic Frontier Foundation. (n.d.).** ***Surveillance Self-Defense: Using Tor*****.** Retrieved from https://ssd.eff.org/en/module/using-tor-browser
The EFF provides practical guidance on using Tor Browser to protect against surveillance and enhance online privacy.

4. **Murdoch, S. J., & Zieliński, P. (2007).** ***Sampled Traffic Analysis by Internet-Exchange-Level Adversaries*****.** In *Proceedings of the 7th Privacy Enhancing Technologies Symposium* (PET). Retrieved from https://www.cl.cam.ac.uk/~sjm217/papers/pet07ix.pdf
This paper analyzes potential threats to Tor and discusses methods to mitigate risks, providing insights into maintaining robust security while using Tor.

5. **AlSabah, M., & Goldberg, I. (2016).** ***Performance and Security Improvements for Tor: A Survey*****.** *ACM Computing Surveys*, 49(2), 32. doi:10.1145/2935417
This survey reviews various proposals and implementations aimed at enhancing the performance and security of the Tor network.