Anonymity communication VPN and Tor: a comparative study

E Ramadhani¹,*
¹Department of Industrial Engineering, Faculty of Industrial Technology, Universitas Islam Indonesia
*Corresponding author: erika@uii.ac.id

Abstract. VPN and Tor is a technology based on anonymity communication. These two technologies have their advantage and disadvantage. The objective of this paper is to find the difference between VPN and Tor technologies by comparing their security of communication on the public network based on the CIA triad concept. The comparative study in this paper is based on the survey method. At last, the result of this paper is a recommendation on when to use a VPN and Tor to secure communication

1. Introduction
Anonymity communication is a communication that provides a hiding services on the Internet. The aim is to secure the communication line from an authorized user. Virtual Private Network (VPN) and The onion routing (Tor) are examples of anonymity communication. VPN and Tor have the same tunneling model communication, and they are also using encryption technology to reach the integrity of data. VPN usually implemented in an enterprise, while Tor tends to be used in a darknet side of the Internet.

The problem is although VPN and Tor have a similarity in their purpose, we cannot implement it arbitrarily. Inappropriate use may cause a fatal error in a network security system. We need to know on when to use between VPN and Tor; we need to do a comparative study between VPN and Tor regarding the security of communication. The comparative study is based on the survey method. The comparison covers the technology that has been used, the vulnerability of system so we can see the advantage and the disadvantages of the system, and the comparison based on the CIA triad concept in network security.

The result of this paper may be used as a recommendation when to use a VPN and Tor to get a secure communication based on anonymity communication.

2. Theoretical Background

2.1. Virtual Private Networks (VPN)
VPN is a network technology for securing communications lines between members or groups that together use public communications infrastructure that provides privacy services to communication lines using security and tunneling protocols. Characteristic of the VPN itself is the use of tunnels that provide security privacy to the communication path between nodes. VPN technology is usually called
VPN tunneling. Tunneling is a network technology that encompasses one type of protocol that contains packets and datagrams from different protocols [1]. For example, a Windows VPN uses point-to-point tunneling (PPTP) protocol package to complement and transmit private network traffic such as TCP / IP over public networks such as the Internet.

2.2. The onion routing (Tor)
The Onion Routing (Tor) is a computer network technology that uses the routing process to several hops to get to the destination. During the routing process to some hops, the encryption process occurs. The encryption process is done three times by the hops that passed. Tor provides the type of data delivery security from the anonymity side of the communication path. The client will be connected to the destination by passing through 3 relays namely entry node, middle relay, and exit relay. These three relays will then perform the process of encryption of the data [2].

2.3. CIA Triad Concept
Security components in the computer network system consisting of three kinds of confidentiality, integrity, and availability commonly abbreviated to the CIA. Essential components related to data communications security are confidentiality and integrity. Confidentiality is usually associated with data confidentiality. Data or information can only be read by an authenticated user. Usually, the implementation is using cryptographic techniques in the process of sending data. Two things to consider in confidentiality, are data confidentiality and privacy. Integrity relates to the authenticity of data that already transmitted, requires unmanipulated data. While the availability associated with the provision of services to access data or information by the user. Systems should always be available to provide services to users [3]. Two important things to note on this point are data integrity and system integrity.

3. Methods
This research method is done by doing a comparative review of previous research papers that talk about VPN and Tor. To compute the system against VPN and Tor, it is necessary to consider the security characteristics of data communications that have been discussed previously, namely confidentiality, integrity, and availability. The research flow is shown in Figure 1.

![Figure 1. Flowchart of research](image)

4. Result and Discussion
The result of security comparison of data communication between VPN and Tor is divided into two categories: based on security components and based on weaknesses in topology and technology used.
The following is the result of comparison of data communication security between VPN and Tor, shown in Table 1.

| Service | Encipherment | Digital Signature | Data Integrity | Authentication Exchange | Routing Control |
|---------|--------------|-------------------|---------------|-------------------------|----------------|
| Confidentiality | Y | | | Y | |
| Data Integrity | Y | Y | | | Y |
| Availability | | | Y | | Y |

4.1. Confidentiality
Confidentiality is one component of system security that maintains the confidentiality of a data. In this section includes two concepts of data confidentiality and privacy. In the data confidentiality that is concerned is the protection of data from access from outside that is not authorized. In the VPN, the aspect of confidentiality is shown in the use of tunneling encryption. Encryption tunneling on a VPN is an aspect that encrpts all data passing through its path. This encryption technology allows data confidentiality to be maintained. The existence of this encryption technology also prevents an unauthorized user from being able to read the contents of the transmitted data, even though the intruder can intercept the data. Tunneling technology used by the VPN is the routing process is done directly from the source to the destination. While the technology used by Tor, the encryption process is done by three layers. This is done to avoid sniffing the data contents by the attacker. Also, to achieve the goal of the Tor is anonymous communication. Tunneling used in Tor is a routing process done by passing through 3 relays [6].

4.2. Integrity
This section discusses how VPN and Tor can maintain data integrity. On VPN there are three types of protocols used for site-to-site connections: PPTP, L2TP over IPSec, and IPsec tunnel mode. In PPTP-VPN the technology does not provide a guarantee of data integrity. PPTP also does not provide Public Key Infrastructure (PKI) to check computer certificates [7]. While on the IP-Sec VPN there is a
process of authentication, data integrity and encryption services to protect data from unauthorized users and possible data modification. The protocols used are Authentication Header (AH) and Encapsulated Security Payload (ESP). For L2TP is a combination of Microsoft Point-to-Point Tunneling Protocol (PPTP) and Cisco L2F. Usually, L2TP does not provide encryption technology, so L2TP is often implemented in conjunction with IPsec. IPSec provides two of key management; they are Manual Key Management and Automated Key Management. HMAC–Message Digest 5 (HMAC-MD5) and HMAC–Secure Hash Algorithm 1 (HMAC-SHA1) is the two popular algorithm in a VPN gateway that uses for verifying the integrity of data. VPN also uses Diffie-Hellman Group 1 (DH-1) & Diffie-Hellman Group 2 (DH-2) as an encryption algorithms, but it is not a data integrity algorithms.

OpenVPN is an open source technology that uses OpenSSL encryption libraries and SSL v3 / TLS v1 protocols. The configuration allows using AES or Blowfish encryption technology [8]. A Hashed Message Authentication Code (HMAC) is a data integrity algorithm that ensures the integrity of the message.

| Table 3. Vulnerabilities Comparison between VPN and Tor |
|-------------------------------------------------------|
| **VPN** | **Tor** |
| Type of attacks: | Type of attacks: |
| • VPN – Hijacking | • End-to-end attacks |
| • Man – in – the – Middle Attacks | • Tagging attacks[9] |
| Lack of topology: | Lack of topology: |
| • In many enterprises provided a connection between wireless and wired based. Usually, the Ethernet jack is open, but 802.1X enabled authentication. This condition called the hidden wireless router (HWR) vulnerability. | • Entry node and exit node is the vulnerable part. According to [10], Tor exit node is the vulnerability section. One of many categories of attack is a malicious exit node modifies webpages, inserting JavaScript code that repeatedly connects to a logger server and sending a distinctive signal along the link. If the client uses a malicious entry node while JavaScript is active, the entry node can detect the signal and attacker can associate the client using his communication. |
| • The IP address is not restricted because ISP could see it as an exit point. | • We can not trust a relay in the onion network, one of them maybe can act as an attacker. |

In Tor, the integrity of the data draws much criticism and praise. Keep in mind Tor consists of many relays hosted by volunteers. You can imagine many relays if more hosts are willing to be a node inside a Tor network. So based on the exposure, the Tor topology will make the data becomes more difficult to know where it came from and where to go. The encryption technology used is three layers and passes the path using the TLS protocol. Here is a translation of Tor technology used regarding data integrity:

• Tor uses SOCKS proxy.
• Before establishing the inter-node communication circuit, Tor uses Public Key Crypto.
• Communication between circuits using Diffie-Helman crypto symmetric.
• SIG: a signature of a SHA256 hash and OAEP-MGF1 padding

Tor also uses RSA and Diffie-Helman as an encryption algorithms, these two is not a data integrity algorithms. In a study conducted by Seongmin Kim et al, they recommended an approach to improve
security and privacy on the use of Tor using the Intel SGX they call SGX-Tor. Systems created based on trusted computing. In a simple Tor topology, key pairs are stored as files, so there is the possibility of a key leak. SGX-Tor protects cryptographic operations and wraps keys before being stored in a file [11].

4.3. Availability
The more critical a service or component, the higher level of availability required. Interruptions that occur in the service will cause the user cannot access the computer resources. The assumption is when a system provides authentication services for a critical application then the system can guard the against the downtime and unreachable due to malicious actions. Based on table 2, the criteria reaching the availability of a system is to have data integrity and authentication exchange mechanisms. VPN and Tor have their data integrity and authentication exchange mechanisms that presented in section 5.2. VPN has their availability in one to one connection line straight from source to destination without a low latency. While Tor is more slow because of its low latency, but the system is never going down because the architecture is based on distributed system relay. The two has their advantage in this section.

Table 4. Advantage and disadvantage between VPN and Tor

| Communication | Advantage                                      | Disadvantage                          |
|---------------|------------------------------------------------|---------------------------------------|
| VPN           | • Fast                                         | • Not secure if the log could see     |
|               | • More secure than Tor if there is no log in    | by VPN provider                       |
|               |     VPN provider                                | • IP address is known as exit         |
|               | • Suitable for P2P filesharing                  |     point or server                   |
|               |                                                  | • Sometimes not free                  |
| Tor           | • IP address is completely secret               | • Free and open source                |
|               | • The topology is based on distributed network  | • Not suitable for P2P filesharing    |
|               |                                                  | • Inefficient because of the low     |
|               |                                                  |     latency                          |

As conclusion, in this section, we provide a recommendation when to use a VPN and Tor. Before we are implementing between VPN or Tor, we should know the vulnerability of that two systems. The vulnerability of VPN and Tor shown on table 3. These vulnerabilities based on the type of attacks and the lack of system topology. VPN is faster than Tor. Tor is very slow because the data is bounced randomly through many relays which could be anywhere in the world. We do not need to trust anyone while using Tor because it is completely anonymised. For such file sharing activities and streaming geo-restricted media content, using VPN is better than a Tor. VPN very secure as long as there are no logs at VPN provider. Tor is always oriented by mafia whistleblower or a dissident living under the regime. VPN provider knows your real IP address and can see the internet traffic at the exit point but not in Tor. To see the difference between VPN and Tor, we can see the summarized in table 4 based on advantage and disadvantage. The use of Tor and VPN depends on how you want to use it. According to [12] OnionCat is an application that using Tor's hidden services and implemented in a layer between a client application and the Tor proxy. OnionCat and Tor claimed that it is a new kind of anonymous VPN.

5. Conclusion
In this paper, we presented the difference between VPN and Tor based on their secure communication. The purpose of VPN and Tor is very similar, i.e., to maintain internet users' online anonymity and to
evade firewalls. The use of VPN and Tor depends on how you want to use it. Each has their advantages and disadvantages. We can combine it to get more secure communication. One thing to note is there is no such a thing as a fully guarantee of anonymity. Just use it wisely based on our necessity.

References
[1] Jha R, Kharga P, Bholebawa I Z, Satyarthi S and Kumari S 2014 International Journal of Computer Network and Information Security 6 49
[2] Ramadhani E and Luthfi A 2011 Adv. Sci. Lett. 4 400
[3] Kolkowska E, Hedström K and Karlsson F 2009 Information security goals in a Swedish hospital Secur. Priv. Organ. Challenges. Proc. 8th Annu. Secur. Conf., pp. 1–11,
[4] Gokulakrishnan J 2014 Indian J. Comput. Sci. Eng. 5 135
[5] Nawej M C 2016 Evaluation of virtual private network impact on network performance (unpublished article)
[6] Çalışkan E, Minárik T and Osula A M 2015) Technical and legal overview of the tor anonymity network (NATO Cooperative Cyber Defence Centre of Excellence)
[7] Behm B J, Roth G B and Rubin G A 2017 U.S. Patent No. 9,780,952. (Washington, DC: U.S. Patent and Trademark Office)
[8] Verma A, Kaur S and Chhabra B 2017 International Journal of Computer Science and Information Security 15 66
[9] Syverson P 2013 Practical Vulnerabilities of the Tor Anonymity Network (Advances in Cyber Security: Technology, Operation, and Experiences)
[10] Abbott T G, Lai K J, Lieberman M R and Price E C 2007 Browser-based attacks on Tor. PET’07 Proceedings of the 7th International Conference on Privacy Enhancing Technologies, pp. 184-199. Berlin, Heidelberg: Springer-Verlag.
[11] Kim S M, Han J, Ha J, Kim T and Han D 2017 Enhancing Security and Privacy of Tor's Ecosystem by Using Trusted Execution Environments In NSDI (pp. 145-161).
[12] Scaife N, Carter H and Traynor P 2015 OnionDNS: A seizure-resistant top-level domain. In Communications and Network Security (CNS), 2015 IEEE Conference on (pp. 379-387). IEEE.