International Journal of Engineering & Technology, 7 (4.29) (2018) 219-223

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Protecting Online Privacy by HeighteningCommunication Path Using Different Hops Path Tor

Amna Saad[1], Ahmad Roshidi Amran[2], and Awang Mohamed Fadli[3]

[1]Universiti Kuala Lumpur Malaysian Institute of Information Technology
[2]Universiti Kuala Lumpur, British Malaysian Institute
[3]Universiti Kuala Lumpur Malaysian Institute of Information Technology
**Corresponding author E-mail:amna@unikl.edu.my*

Abstract

The vulnerabilities within the internet cause unauthorized person to hack and steal our private data and spot our location within the cyber world. Some people do not think this as an issue. They would be more upset if the link is down, the connection is slow or when the link is intermittent. Hence, without their knowledge, their well- being is being monitored by an unknown person or group. The in- formation gained can later be used against their personal interests. Others are very concerned about this matter. They want to protect their privacy and identity in the cyber world. We proposed a solution to curb these activities by providing extra layers of internet connectivity protection, in order to create anonymouscommunication on demand. In this project we develop two, three and six hops security of the Tor wireless router on a Raspberry Pi 3. The client can choose to use, either hardware based 3-hops path standard security Tor or software based security Tor custom for 2-hops and 6-hops paths via application software rebuilding using MSYS2 and MNGW tool. Our result shows that there is no significant performance different in term of the connections response time regardless of the number of the Tor path lengths.

Keywords: *Prototyping; Privacy protection; Raspberry Pi; The Onion Router*

1. Introduction

When most communication happens on the internet, there will be higher requests from clients to secure their internet communication and protecting their privacy. The whole idea is to have a permeation of trust within each stage of our communication system. The permeation of trust is depended on the integrity of the chain of custody of each element in the system including its data [1]. Every day, when we surf the internet, create an account for the media-social and chat with others using instant messaging application, we would require our private communication to be protected. During our on- line communication on the internet, the IP addresses will be used to provide an identifier to address each party. The message might be encrypted to protect the data, however, the source and destination addresses are still contained in clear texts. These addresses are corresponding to the IP datagram headers of the source and destination of the encrypted message, which are exposed since they are in clear texts. This situation could not be avoided since otherwise messages could not be routed to their destination.

We could say that, such communication is not anonymous. An adversary monitoring the network traffic could easily identify the two parties communicating with each other. With the advancement of computer technology, the internet clients will be exposed to cyber-attacks.

That is why; anonymous communication has become more popular today. Anonymity is righteous and necessary in many scenarios, such as protecting internet client privacy, improving system security, bypassing the internet censorship body, satisfying some antivirus requirement, and protecting internet clients' computer from hackers' attack [2]. Without a good network security, our data will become a subject of interest to cyber attackers. Some of the attackers are passive. They monitored and sometimes scanned for open ports and vulnerabilities with the intention to gain information about the target. However, no data is changed on the target as yet. Our networks and data are vulnerable to these types of attacks, assuming we do not have a security plan in place [3].

Unencrypted network is everywhere and it can bring a hacker or an- other agency to snooping our privacies. According to a top-secret accounting journal dated January 9, 2013, the NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md. The report said, field col- lectors had processed and sent back a new record that included "metadata", which would indicate who sent or received e-mails and when, as well as content such as text, audio and video [4].

From this report, we could extract the following problems:

i. ***A private network is being analysed by someone without the owner's consent.***
That is a big problem because all the private data from an internet client will become insecure and someone can use it for their self-interest.

ii. ***Users are exposed to outside threat and easily detected if noanonymous communication is implemented.***
For example, a journalist who is on duty is very vulnerable to outside threat if his location is known by his rival.

iii. ***Lack of hardware development for protecting network security layer like Tor project.***
There is a lack of hardware development for portable devices that could be easily used out of the box to help curb clients from unathorised attack, a Tor project included. Basically, most of Tor project is developed via Software.

Our aim is to find a solution for commuters to secure their whereabouts by choice and on demand. We explore the possibility of using a portable device that could be used as a firewall on demand as to protect oneself from unauthorized personnel. Hence, we explore the Tor router capability for this purpose. Logically, more hops means the client will be more protected. Since the original Tor works on three hops, we would like to investigate whether less or more hops could provide similar outcomes as the original Tor setup.

The rest of this paper is organised as follows. In Section 2, we look at the related works done by other researchers. Section 3 discusses the prototype of two, three and six hops of Tor routers on Raspberry Pi 3. Finally, Section 4 briefly discuss on the testing and results, followed by the conclusion and suggestion in Section 5.

2. Related Works

2.1. The Onion Router (Tor)

In this new era, anonymous communications become popular around the world, in line with the advancement of network technologies. Due to this trend, mankind has developed highly anonymous communications with the reason to secure communications and to protect their data privacy from a common form of Internet surveillance device known as a traffic analyser. The Onion Router is a free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of thousand relays to conceal a client's location and us- age from anyone conducting network surveillance or traffic analysis. Tor project consists of a group of operated server that allows people to improve their privacy and security on the internet. Tor has been in operation for several years and has about a thousand nodes and a hundred thousand of anonymous clients. Tor works on the real-world Internet, requires little synchronization or coordination between nodes, and provides a reasonable trade-off between anonymity, usability, and efficiency.
Currently, most internet connections are less secure. With this vulnerable internet connection, hackers can easily hack and steal, then record our private data and location without our knowledge. Some people carelessly share their private life or information into a social media platform due to ignorance or on purpose. For example, their daily activities including information about their location, who they meet, information about their family, and more. The majority of these people takes it easy on what they consider as trivial matters and finally, it will bring a big problem later. They must know that someone outside there is watching them and trying to get information without their knowledge. In addition, any unauthorized person can use this information for their self-interest to exploit others [5]. A few individuals use Tor to keep remote websites from tracking them and their family members. On top of that, to connect to re- sources such as news sites or instant messaging services that are blocked by their local Internet providers. Activist groups like the Electronic Frontier Foundation (EFF) funds further the development of Tor to help maintain civil liberties online. Corporations are investigating Tor as a safe way to conduct competitive analysis, and are considering using Tor to test new experimental projects without associating their names with these projects. A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while being deployed in the Middle East recently. They use this Tor to secure a communication and also to secure a transportation information between two places. The journalists use Tor to communicate more safely and secure their locations, especially when they have been assigned to find stories at sensitive places such as a war zone country. Non-governmental organizations (NGOs) use Tor to allow their workers, while on duty, to connect to their home website while they are in foreign countries, without notifying their next of kin of their whereabouts and with what organization they are working with [6].

The function of Tor is to secure our network from traffic analyser. Tor also allowed the organization and individual to share their information over public network without compromising their privacy. Users can publish their website or some article without revealing their location. In other word, Tor also can become a better place for sensitive communication like chat and web forum for rape or people with illnesses.
The most important aspect of Tor would be to make it difficult, for any snoopers to see our webmail, search history, social media posts or other online activity such as online bank transactions [7]. They also would not be able to tell what country that we are in or locate us by an IP address, and this function is very useful for journalists, activists, business people and more. Tor works by bouncing connections from our computer to web server destinations through a series of intermediate computers that we call relays. Tor has thou- sands of relays that are run by volunteers around the world. Basically the theory of Tor is, any connection that bounced over more than three relays indicated that the connection is with tight security. One study showed that Tor implementation is intended to provide full privacy and are more trustworthy than VPN providers [8].

The following are the three categories of Tor relays:

Entry/Guard Relay- This is the entry point of the Tor net- work. Relays are selected to serve as guard relays after being around for a while, as well as having shown to be stable and having *high bandwidth* [9].
Middle Relay- Middle relays are exactly that - middle nodes used to transport traffic from the guard relay to the exit relay. This prevents the guard and exit relays from knowing each other.
Exit Relay- These relays are the exit point at the edge of the Tor network. These relays send traffic to the final destination intended by the client.

Tor developers have created Tor to bounce the connection through three relays. Each relay has their own specific function. The first relays are selected to serve as guard relays after being around for a while, as well as having shown to be stable and having high bandwidth. Then the intermediate relay is to transport traffic from guard relay to exit relay. The relay is very important because it will prevent a guard relay and an exit relay from knowing each other. The last relay will send a traffic into the final destination intended by the client. To increase Tor system efficiency, in every ten minutes, Tor provides a new circuit to keep hacker from linking to the client earlier action through the new route. In addition, Tor only works for TCP streams and can be used by any application with SOCKS support. There is one question that still being discussed in the Tor community, i.e. whether the path would be reversed. The path could be reversed but the complete path would not be revealed. The Tor nodes that retained the state of their successor and predecessor nodes would have enough information to simply reverse the headers and they do not need to use encryption to return the reply without exposing the complete path [10].

2.1.1. Tor Functionalities

Tor reduces risk of being hacked by distributing transactions over several places on the internet. With this method, there is no single point that can link clients to their destinations. Normally, most connection flow takes a direct route from source to destination. Unlike Tor, data packet on the Tor network take a random pathway through several relays that give an advantage to hide clients from any single points. This single point can tell where the data came or where it will go [6]. The client builds a circuit of encrypted connection relay on the network. This circuit is extended to one hop at a time. The client of the relay will never know the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop cannot trace these connections as they pass through. By default, Tor bounces connections through 3 relays. Each of the relays has their own role play in the Tor network.

2.1.2. Tor Path length trade-off

Tor's design like most low latency anonymizing networks. This design is vulnerable to end-to-end traffic correlation attacks. If the endpoints are compromised, an attacker can use any one of known traffic analysis attacks, to correlate the source and destination. Conventional wisdom indicates that 3-hops path gives an appropriate balance between security and performance. However, the 2-hops path is more about to improve the performance, though it is un- clear at the moment what security trade-offs that may incur for the 2-hops path [11].

Since 2-hops path offers better performance, it may focus on clients who need value performance over security to use the 2-hops path. Other clients who need a stronger security will use 3-hops path. Suppose that most client's value performance and consequently, Tor chose a default path length of two hops [12]. Security conscious clients could optionally use three hops to take advantage of the additional security that 3-hops path offer against adaptive surveillance. However, clients who choose to use longer paths may be identified as desiring additional security, which alone could draw an adversary's attention. Furthermore, it has been argued that most clients tend to keep default options, even when the defaults may not be optimally suited to their needs [13]. Allowing clients to con- figure their own path lengths assuming that, the clients understand the full security implications of their choice, which is very unlikely, particularly the novice clients. Thus, all clients should be encouraged to use the same path length. This type of rule can be set as an organization policy. The key here is for the organization to be consistent with its implementation.

3. System Prototyping and Instrumentation

As a proof of concept we develop two kinds of Tor routers, hardware based and software based. The 3-hops Tor router is developed using Raspberry Pi 3 that focus on hardware based Tor. On the other hand the 2-hops and the 6-hops Tor are developed using MSYS2 tool, these are software based Tor. For the hardware based Tor, the system is combined with Tor ARM, i.e. anonymising relay monitor. Tor ARM is a real time terminal monitor for Tor relays. It provides real time information of bandwidth, cpu, memory usage, relay configuration, connections, and other details relay operators might find handy for checking Tor's status.

3.1. ToR Paths

For this project, we use three different path-length, i.e. 3-hops path, 6-hops path and 2-hops path. The 3-hops path provides a standard security of Tor system. The 6-hops path is an improvement from the standard security into extra security of Tor system. On the other hand, the 2-hops path offers a better performance for client who need better performance over security. We configure and created a standard Tor network security in Linux terminal into Raspberry Pi. After that we use a compiler tool call MSYS2 tool, to download a source code from Tor developer and edit this source code to create the application software which support 2-hops, 3- hops and 6-hops Tor.
Then the system is tested to ensure that interfaces between modules work, the system works on the intended platform and with the expected volume of data. Finally, test was conducted to evaluate whether the system meet a client's requirements.

3.2. Hardware Based Tor

Figure 2, shows the flow of the 3-hops Tor from the initiation until the connectivity through the WIFI network. A user connects his LAN router to a Tor router. The user then switches on the Tor router. Then, the Tor router broadcasts a WIFI signal. The user now will be connected to the internet via the Tor router instead of his LAN router. In which case, the traffics to the internet will be relayed accordingly [14]. Since the user needs to connect his Tor router to a switch, hence, this solution is not the right solution for a commuter. Perhaps, the software based Tor is a more suitable solution for those who are on the move.

3.3. Software Based Tor

For a software based Tor, the application is installed on the device itself, i.e. notebook. The Tor router takes over the wireless router based on the setting, like any other application. Figure 1, shows the decryption process flow for N-hops software based Tor. In theory, N-hops Tor would perform N decryptions, where N is greater than 1. Assuming that the original data was encrypted N times. In addition, the number of node in a path for N-hops Tor is N+1.The final destination will be revealed once the packets bounced through N routers. The encrypted addresses will be revealed after each layer decryption. For example, for 6-hops path Tor, the packets will be encrypted six times. The final address will be revealed after the sixth decryption. Figure 3 shows the process for 6-hops Tor for a client named Awang.

1. Awang sends a 6 encrypted packet to Router 1.

2. Router 1 decrypts the first layer of encryption with his private key and then send only 5 encrypted packet to the Router 2.

3. Router 2 decrypts a second layer of encryption and then send only 4 encrypted packet to the router 3

4. Router 3 decrypts a third layer of encryption and then send only

3 encrypted packet to the router 4.

5. Router 4 decrypts a fourth layer of encryption and then send only 2 encrypted packet to the router 5

6. Router 5 decrypts a fifth layer of encryption and then send only 1 encrypted packet to the router 6.

7. Router 6 finally decrypts and decrypts the last packet and sends the packet to the Web server

The potential response of the receiver is sent to the last router in the circuit, i.e. Router 6, and is relayed back to sender most probably through the exact same circuit [14]. The last Onion Router, i.e. Router 6 of a circuit only knows the receiver or the destination of a message. However, he would not be able to see the data inside the traffic stream when an encryption like HTTPS is used. Each intermediate Onion Router, i.e. Router 2, 3, 4 and 5, only knows its predecessor and its successor, without even knowing which other Onion Routers are participating in the circuit.

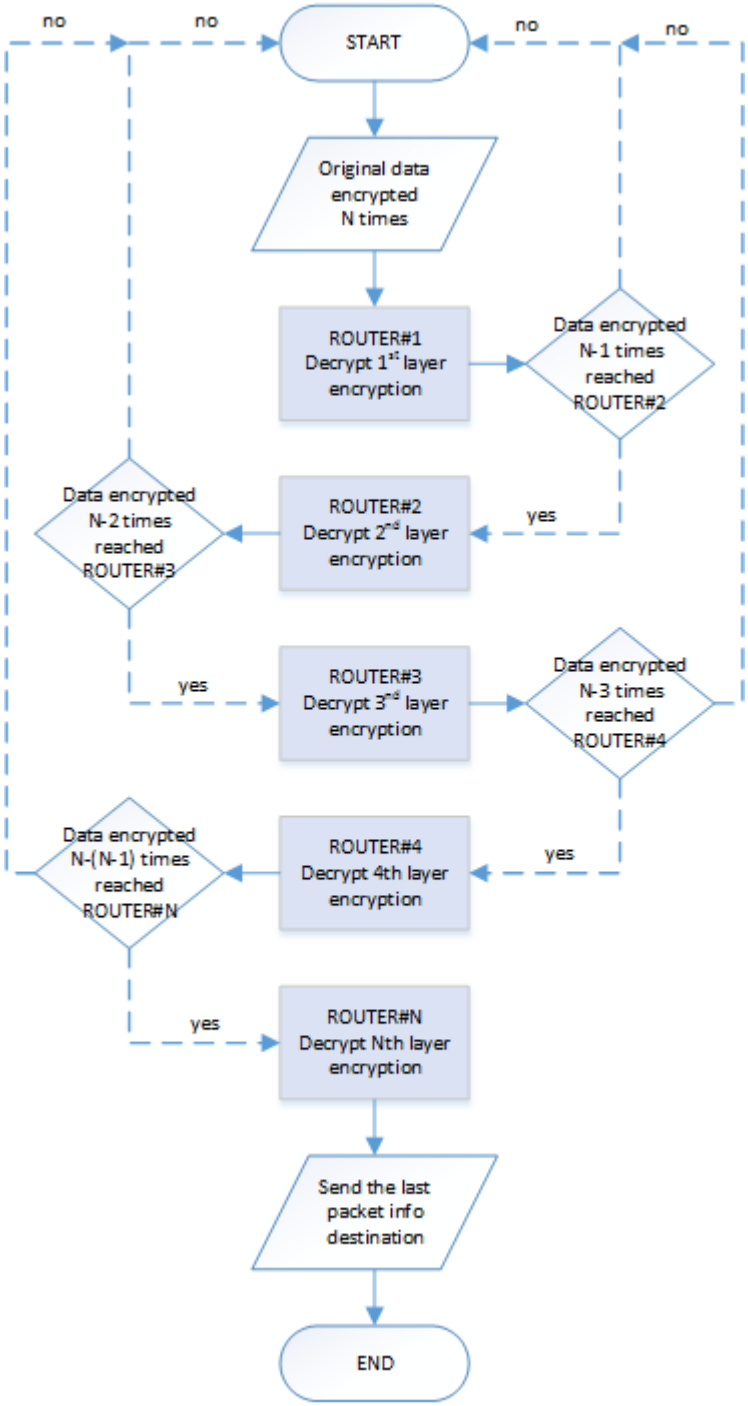

Fig. 1: Flowchart for N hops Tor

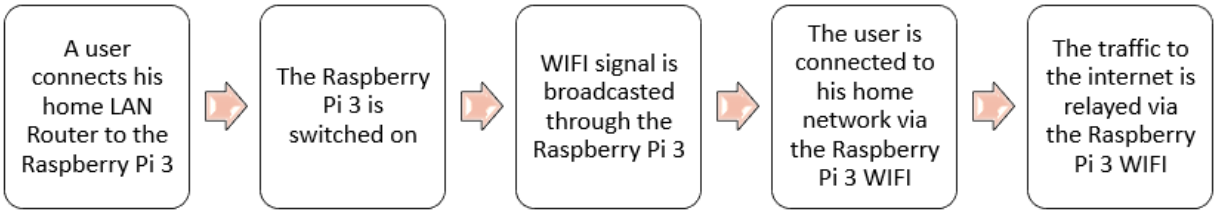

Fig. 2: Hardware based Tor: Process Flow

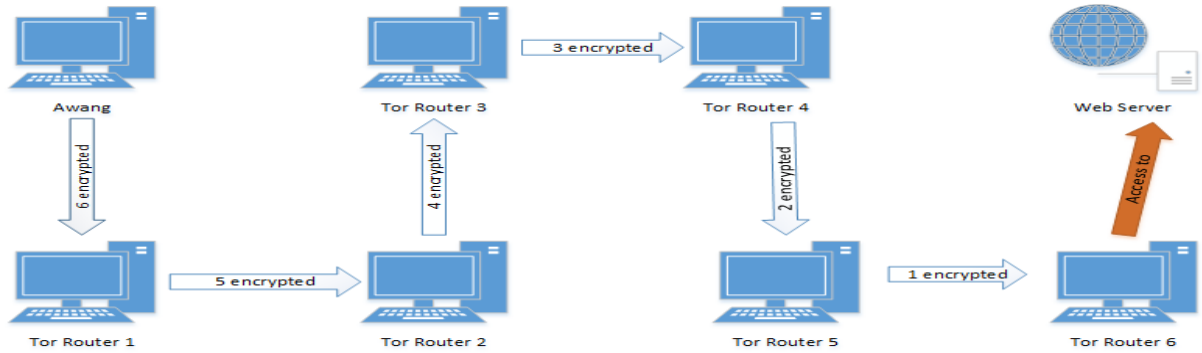

Fig. 3: Example of Software based Tor: from source to destination

4. Testing and Results

The following are our findings:

1. The state of the internet connectivity influence the performance of the system. The system requires stable internet connection for smooth execution.
2. The performance of surfing speed when using the Tor system depends on other Tor node routers around the world.
3. It is not suitable yet for common client usage. The client should be IT literate to monitor the network state. They must know the command like to run Tor ARM
4. There is no significant different in term of surfing speed regardless of two hops, three hops or six hops relay.

5. Conclusions and Suggestions

Everything is connected through Internet. Companies built fire-wall to protect their assets. However, what about the privacy of their employees? Many people commute from their homes to the offices and vice versa. Sometimes they work away from their homes and offices which they would like to keep it secret from others including their loved ones. However, they want to be able to connect to their families and friends on demand. So, how can the current technologies help such individuals?

A relay communications might be the solution. However the re-lay communications in theory would introduce some delays. This is the tradeoff of such communications, i.e. in term of performance, but it would ensure the privacy of such individuals would be protected. However, if the delay is manageable then why not. Tor has this solution, but at the moment the default relay path length is 3. In our research, we explored other path length like 2-hops path Tor and 6-hops path Tor. We choose 2-hops path because it is less than the default Tor path length. Theoretically, less relay means reduce security, but potentially better performance due to less delay. We also choose 6-hops path for a similar reason. However, in this case we would expect to see the improvement in security but reduce in performance. Our result shows that there in no significant performance different in term of response time and the security of the connections regardless of the number of path lengths.

Acknowledgements

Our gratitude to Universiti Kuala Lumpur and to our sponsor and parent company the Majlis Amanah Rakyat (MARA).

References

[1] 2015. Industrial Consortium. Industrial Internet of Things Volume G4: Security Framework. Technical report, CreateSpace Independent Publishing Platform, 2016.

[2] Yanchao Zhang, Wei Liu, and Wenjing Lou. Anonymous communications in mobile ad hoc networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1940–1951. IEEE, 2005.

[3] Microsoft. Common types of network attacks, Last visited June 2017.

[4] The Washington Post. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, Last visited June 2017.

[5] Marc Mendonca. *In Pursuit of Privacy on a Public Internet*. PhD thesis, 2012. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2016-03-11.

[6] Matthew Edman and Paul Syverson. As-awareness in tor path selection. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 380–389, New York, NY, USA, 2009. ACM.

[7] Yao Chen, Radu Sion, and Bogdan Carbunar. XPay: Practical Anonymous Payments for Tor Routing and Other Networked Services. In *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, WPES '09, pages 41–50, New York, NY, USA, 2009. ACM.

[8] Alexandr Vitosinschi et al. Protecting privacy using Tor. 2016.

[9] Arma. The lifecycle of a new relay, Last visited April 2017.

[10] Richard Horrocks. Is a server's response to a Tor browser query encrypted by the Tor nodes when it transits the Tor circuit in the reverse direction? Last visited November 2017.

[11] K. Bauer, J. Juen, N. Borisov, D. Grunwald, D. Sicker, and D. Mccoy. On the optimal path length for Tor. 3rd Workshop on Hot Topics in Privacy Enhancing Technologies, 2010.

[12] Kevin Bauer, Joshua Juen, Nikita Borisov, Dirk Grunwald, Douglas Sicker, and Damon McCoy. On the optimal path length for tor. In *HotPets in conjunction with Tenth International Symposium on Privacy Enhancing Technologies (PETS 2010), Berlin, Germany*, 2010.

[13] H. Teymourlouei. Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2015.

[14] E. Erdin, C. Zachor, and M. H. Gunes. How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys Tutorials*, 17(4):2296–2316, Fourthquarter