Security Threats and Attacks on Tor

Maria Khan, Muhammad Saddique,
Umar Pirzada, Afzaal Ali, Bilal Wadud
Cecos University of IT & Emerging Sciences
Peshawar, Pakistan
Icrg.csit@gmail.com

Muhammad Zohaib
Electrical and Electronics Engineering Department
Near East University, North Cyprus
e.m.xohaib@gmail.com

Imran Ahmad
Faculty of Computing, Riphah International University
Lahore, Pakistan
imran.ahmad@riphah.edu.pk

Abstract

The Internet is in use nowadays all over the world. While using the Internet, the identities of the sender and receiver are not hidden; to hide the sender and receiver identities anonymous communication was introduced. There are many anonymous communication systems developed but, the Onion Router (Tor) is the most deployed anonymous communication system that provides online anonymity and privacy. There are vast security threats/attacks on Tor that are to be considered. In this article, the current attacks on Tor - an effort to categorize them for further analysis are discussed.

1 Introduction

David Chaum first introduced Anonymous communication networks as a building block for anonymity. In the sending and receiving of a message the mix acts as a keep-convey relay that is used to veil the link between sender and receiver [6]. Here the few mix based designs that have been proposed and carried out for secret email are the best particularly Babel [7], Mixmaster [8], and the fresher Mix minion [9]. For e-mail, their latency is acceptable, but for web, browsing it is un-suitable for communicating applications.

In: A. Editor, B. Coeditor (eds.): Proceedings of the XYZ Workshop, Location, Country, DD-MMM-YYYY, published at http://ceur-ws.org

Additional systems were also developed on the assumption that a mix will take low latency traffic. To anonymize the conversation of phone calls ISDN mixes [10], is designed, and for anonym zing web-mixes [12], it also follows the same pattern. At the University of Dresden the Java Anon Proxy (JAP) is based on this idea and it is fulfilled and running.

Tor is a connected network for anonymizing TCP streams over the Internet [1]. It can report boundaries in design of previous Onion Routing [2-5], by building up unspoiled forward confidentiality, then bottleneck control, then data purity or integrity, then customizable exit policies, then index servers, and then location-hidden services using meeting points. Tor works on real-world internet, which requires no special power or core adjustments, and needs little simultaneity or direction between nodes, and delivers a sane compromise between efficiency, usability and anonymity. With the constant and even ever increasing attention that TOR is witnessing, we provide, in this paper, a fresh view of the security threats and attacks on TOR. These attacks are groups in categories based on their types Section 2, provides a literature review. While the design goals and non-design goals of Tor are outlined in section 3. The threat model for Tor is presented in section 4. Section 5 overviews Tor design. And section 6 presents the different types of security threats/attacks against Tor. In section 7, we conclude the paper.

2 Literature Review

Before onion routing, an implementation based on a simple model by David Chaum of the University of California, Berkeley [13], was introduced to solve

the problem of source and destination identification through traffic analysis. To hide the identity of sender from the receiver entity, Chaum mix was introduced. In this approach, we have all sent back and forth all the traffic from sender to receiver which goes over a proxy that is able to disinfect the sender and/or the receiver information if needed; however, since the sender is the main focus of the problem then the receivers identity is kept as it. In this case to keep the path of sender and receiver identities, the only thing is the proxy. While sending the information to receiver the message is encrypted and decrypted by the series of public and private keys of Chaum mixes.

A. Onion routing: Onion routers are special proxies that forward/relay the data between sender and receiver. A normal user-level process is run by each router without any special privileges. There is a TLS connection between onion routers. The onion routers accept TDC data streams and mingle them through the circuits. The exit router of the circuit is linked to the destination.

B. TOR: The Second Generation Onion Routing: Tor [14, 15, 16], the onion router, is the largest and the most deployed anonymous communication system in the present era. It is used in more than 78 countries with 6755 relays to give online secrecy and privacy. In recent years, Tor has become a research hotspot in the anonymous communication systems world.

3 Design Goals/Non-Goals Of Tor

3.1 Design Goals:

Systems designed for anonymity are lowlatency, to follow to annoy attackers from joining communication partners, or from joining many communications to or from a specific user. For this purpose; however, some ideas have been introduced Tors development.

Simple design: In simple design the parameters of security and the protocol design are well-understood. In simple design extra features execute implementation and difficulty expenses; and by accumulation unverified methods to the design risks mobility, legibility, and simplicity of security examination. The purpose of Tor is to utilize a reserved and non-variant system that mingles the best known ways to protective anonymity.

Usability: Due to anonymity, systems hide users among users, and it is a weak system if it has a low number of users because a system which has less users; and thus, provides less anonymity. Usability is not only versatility but also a defense requirement [17, 18]. Therefore, Tor not only needs adapting to context aware applications. Moreover, Tor should not introduce prohibitive intervals. Tor requires few conformation decisions as potential. And finally, on all common platforms Tor should be easy to implement; No variation is required for the operating system to make it unidentified (Tor currently runs on Linux, UNIX, and others).

Mobility: In the real world it is used and its design is deployed. For example, asking more bandwidth than volunteers want to give so that it should not be costly to run, by giving permission to attackers to join onion routers in illegal events. Moreover, it should not put a burden on operators, for core patches, or different proxies for each protocol nor should it be problematic or expensive to implement. —In addition, there is no need for non-anonymous parties (just like websites) for our software to be run. This goal cannot be achieved for known users talking to unidentified servers.

Flexibility: The protocol is well identified and also flexible, so Tor could be a platform for future research. We have many open issues in low-latency anonymous networks, just like making dummy traffic or stopping Sybil attacks [19], it can be solved freely from the problems, which are dug up by Tor. Hopefully future systems will not be necessary to recreate Tors design.

3.2 Non-goals:

In preferring simple and deployable designs, it also has openly delayed numerous imaginable goals, because they are answered in some place, or because they have not been answered yet.

No protocol standardization: Tor has no-protocol normalization like Privoxy. If a sender wants to be unidentified from the other party while using difficult and random protocols e.g. HTTP, Tor has to be wrapped with filtering proxy like Privoxy to cover difference between clients and remove protocol features that reveal identity. With this portion Tor is capable of providing services that are not known to the network but enough to the server such as SSH. Similarly, Tor is unable to add tunneling for protocols like UDP; this should be provided by some other service if possible.

Not protected against end-to-end attacks: Tor doesnt completely resolve correlation attacks. Some solutions are still proposed such as running your own onion router.

Non steganography: Tor does not hide who is attached to the network.

Not peer-to-peer: In a non-peer-to-peer distributing surrounding where Tarzan and Morph Mix aim to scale with many small life servers, many of them are con-

trolled by an opponent. But there are still some debatable issues in this method [20, 21].

4 Threat Model

During the analytical study of anonymity designs a worldwide passive opponent is the most regularly assumed threat. But similar to other applied low-latency systems, In Tor we have no safety against such a strong opponent. As another possibility, we consider an opponent who can monitor some part of the network traffic. In Tor an opponent can remove, introduce, modify, or postpone traffic. And in Tor the opponent can control his own onion routers. In addition, an opponent can also adjust certain portions of the onion router. The objective of an opponent is to identify both the sender and receiver. In low-latency anonymity systems layered encryptions are used. While an adversary can observe both the ends so a passive attack can settle a doubt that client is communicating with server, but only if the effectiveness/timing and volume architectures of the traffic on the connection are sufficiently distinct. While active attackers can induce timing signatures on the traffic to compel distinct architectures.

Now an adversary wants to make a link with a client through her communication associates; an adversary can also try to make the profile behavior of client. The adversary can also accumulate passive attacks by detecting the edges of the traffic and correlating traffic coming and leaving the network by looking for packet size, timing. By negotiating routers or keys an adversary can also mount active attacks; or by reproducing traffic; particularly refusing service to trustable routers to move users to compromised routers, or refusing services to users to observe the data stoppage somewhere else in the network too; or through introducing designs into traffic that can be traced later. An opponent can compel and undermine the index servers to provide users opposing opinions of network status. Moreover, the adversary can exert an effort to minimize the networks reliability by compromising relays or by introducing damaging activities from coherent nodes and an opponent is struggling to make them reserve; thus making the network unreliable flushes users to other communication systems having minimum anonymity, where they can compromise them easily.

5 Thor Design

Tor works on the principle of onion routing [1]; the data is moved forward through a number of nodes with layers of encryption, one layer is removed by each node in the network. In a telescoping fashion the tunnel is constructed and routed across the network. In the tunnel each node knows only the previous node and the upcoming node in the path. In reality, the first entry node knows the beginning of the tunnel, but it does not identify the destination, and the exit node knows the destination but not the beginning. But if the nodes are observed they can do the traffic analysis to find the link of tunnel.

In Tor nodes are filed with the index service which is reliable. In Tor each node shows its own IP address, its public key and its exit policies for proving services. In a span of time one can find the bandwidth value that is found by looking for the highest bandwidth perceived by the node. Uptime of each node is also upheld by directory server. Tor route creation algorithm, implemented by the Tor beginner will have to choose all nodes with better policies and then it can choose a random node from the list, with the group influenced by the specified bandwidth.

Wright et al, [10, 11], firstly describes guard nodes which can defend against the predecessors attack. For its path each client can select three nodes and can select entry nodes from all of Guard nodes based on a high uptime that has a bandwidth over a certain threshold value.

6 Types of Security Threats/Attacks On Tor

6.1 Passive Attacks:

Tracking users traffic: by monitoring users connection show not show his/her data but will show the similar traffic patterns.

Monitoring users data: Data at the end is encrypted, not the connection. In order to hide application data traffic, Tor can use Privoxy and filtering services.

Selections distinguish ability: Tor allows clients to select configuration selection. With this clients who are fewer might give up maximum anonymity by looking different.

End-to-end timing correlation: the safety currently presented against such analysis to hide the link between the OP and the first entry node by running a Tor relay or behind the firewall.

End-to-end size correlation: observing the data packets will be useful in the analysis of end points of traffic.

6.2 Active Attacks:

Compromise keys: An attacker who comes to know a relays identity key replaces that relay forever.

Run a recipient: An opponent controlling a web server knows the timing outlines of the users who are linking to it, and can introduce random outlines in its replies.

Run an onion proxy: Sometimes, it might be necessary for the proxy to execute remotely. Identification of onion proxy is the identification of all the links that will occur as a consequence.

Denial of service: An attacker can over load the random nodes to cut off its link from the network.

6.3 Index Directory Attacks:

Destroy index servers: If some index servers vanished, the remaining can still convey the details of the network and create a consensus index. If most of them are destroyed, then the directory will not have enough signatures for the users.

Subvert an index server: By hijacking a directory server, an opponent can influence the last index to some extent.

6.4 Attacks against meeting points:

Make many requests: An opponent can cut off the Bob service by overloading his entry points with requests.

Compromise a meeting point: A meeting point is not going to respond further on a circuit, since all data traffic is encrypted going through the meeting point with a session key which is a mutual key of Alice and Bob [22, 23].

Circuit clogging attack: In a circuit clogging attack, the premise is that a client creates a circuit and connects to a server using that circuit. The server or parts of the content of the server (for example an advertising frame) is malicious. The malicious content alternates between sending a lot of data and sending very little data. The three Tor relays that show an increase in network latency in the monitoring are most likely: the three relays used in the circuit by the client. A detection scheme for clients is also proposed. If it detects a high and unexpected increase in network latency, the user can disconnect from the server and destroy the affected circuit [24].

Sniper Attack: Denial of service (DoS) attack against Tor that may be used to anonymously and selectively disable arbitrary Tor relays. The attack can be used to deanonymize hidden services by selectively disabling relays, heavily influencing paths to those in control of the adversary [25].

Entry and exit onion router selection attacks: The malicious onion proxy creates loops in circuits to target onion routers to create a denial-of-service attack. If the looping phase attack is successful, then the malicious onion routers are more likely to be selected in circuits, because the other legitimate onion routers are busy. This advantage of the adversary can be used to execute further attacks.

AS and global level attacks: An autonomous system is an independent network, and an Internet that consists of these ASes. For instance, when sending a message using Tor, the traffic goes through different multiple autonomous systems. More importantly, if both the entry and exit onion routers are located at the same AS, then a statistical correlation attack can be performed on the AS-level [26], [27].

6.5 Traffic and time analysis based attacks:

Low-Cost Traffic Analysis of Tor: presents an attack that includes traffic-analysis techniques and how an initiators, otherwise, unrelated streams can be linked back. The term low-cost means that the attacker is not required to be a global adversary, in fact only a partial view of the network is assumed.

A cell counter based attack against Tor: introduces a traffic analysis based active watermarking technique that reveals the communication partners in a Tor circuit.

Browser-Based Attacks on Tor: presents a time based attack that exploits browser behavior when tampering HTTP traffic [28-32]. A Practical Congestion Attack on Tor Using Long Paths: is an attack that reveals an entire path of a user in a modern Tor network.

Passive-Logging Attacks against Anonymous Communications: Systems examine a predecessor attack and an intersection attack. The predecessor attack provides probability values to reveal the users identity. In intersection attack the adversary keeps a list of addresses that have been active when the victim has contacted his destination.

7 Conclusion

This paper described the complete architecture of Tor; i.e., its circuit establishment and workings. Moreover, some attacks are described, which had been conducted on Tor to confirm that when two parties are communicating with each other over Tor by observing patterns, such as timing and volume of traffic, they can disable Tors network

References

[1] Roger Dingledine, Nick Mathewson and Paul Syverson. *Tor: the second-generation onion*

router, in Proceedings of the 13thconference on USENIX Security Symposium - Volume 13, 2004, pp. 2121.

[2] David Goldschlag, Michael Reed and Paul Syverson. *Hiding routing information, information Hiding*, first international workshop, Springer Verlag LNCS 1174, on May 1996, pp. 137150.

[3] Michael Reed, Paul Syverson and David Goldschlag. *Anonymous connections and onion Routing*. IEEE Journal on Selected Areas in Communications, 16(4), on May 1998, pp. 482494.

[4] Paul Syverson, Michael Reed and David Goldschlag. *Onion Routing access configurations*. In DARPA Information Survivability Conference and Exposition (DISCEX 2000), volume 1, pp. 3440.

[5] Paul Syverson, Gene Tsudik, Michael Reed and Carl Landwehr. *Towards an Analysis of Onion RoutingSecurity*. Workshop on DesignIssue in Anonymity and Un observability, Springer-Verlag, LNCS 2009, on July 2000, pp. 96114.

[6] David Chaum. *Untraceable electronic mail, return addresses, and digital pseudonyms*. Communications of the ACM 24(2), on February 1981, pp.8488.

[7] George Danezis, Roger Dingledine and Nick Mathewson. *Mix minion: Design of a type III anonymous remailer protocol*. In IEEE Symposium on Security and Privacy, Berkeley, CA, 11-14 May 2003.

[8] Ceki Gulcu and Gene Tsudik. *Mixing E-mail with Babel*. In Network and Distributed Security Symposium, NDSS 96, San Diego, California, on February 1996, pp. 216.

[9] Ulf Moeller, Lance Cottrell, Peter Palfrader and Len Sassaman. *Mixmaster protocol version 2*. Technical report, Network Working Group, on May 25 2004.

[10] Andreas Pfitzmann, Birgit Pfitzmann and Michael Waidner. *ISDN-mixes: Untraceable communication with very small bandwidth overhead*. Conference on Communication in DistributedSystems, volume 267 of Informatik-Fachberichte, Springer-Verlag, February 1991, pp. 451463.

[11] Rainer Bohme, George Danezis, Claudia Diaz, Stefan Kopsell and Andreas Pfitzmann. *Mix cascades vs. peer-to-peer: Is one concept superior*. In Privacy Enhancing Technologies (PET 2004), Toronto, Canada, May 2004.

[12] Oliver Berthold, Hannes Federrath and Stefan Kopsell. *Web Mixes: A system for anonymous and unobservable Internet access*. Designing Privacy Enhancing Technologies, volume 2009 of LNCS, Springer-Verlag, July 2000, pp. 115129.

[13] David Chaum. *Untraceable electronic mail, return addresses, and digital pseudonyms*. ACM Communication, volume 24(2), on 1981, pp. 8488.

[14] https://www.torproject.org/ accessed on 24 December, 2017.

[15] Roger Dingledine, Nick Mathewson and Paul Syverson. *Tor: the second-generation onion router*, in Proceedings of the 13thconference on USENIX Security Symposium - Volume 13, 2004, pp. 2121.

[16] David Goldschlag, Michael Reed and Paul Syverson. *Hiding Routing Information*, in Proceedings of Information Hiding: First International Workshop, Ed. Springer-Verlag, LNCS 1174, May 1996.

[17] Alessandro Acquisti, Roger Dingledine and Paul Syverson. *On the economics of anonymity*, in Springer-Verlag, LNCS 2742, 2003, pp. 84-88.

[18] Bassam Zantout and Ramzi Haraty. *I2P Data Communication System*. Proceedings of the Tenth International Conference on Networks (ICN 2011), St. Maarten, The Netherlands Antilles, pp. 401-409, January 2011.

[19] Michael Freedman and Robert Morris. *Tarzan: A peer-to-peer anonym zing network layer*. In 9th ACM Conference on Computer and Communications Security (CCS 2002),Washington, DC, on November 2002, pp. 193-206.

[20] Marc Rennhard and Bernhard Plattner. *Practical anonymity for the masses with morph mix*, in Springer-Verlag. LNCS (forthcoming), 2004, pp. 233-250.

[21] John Douceur. *The Sybil Attack*. In Proceedings of the 1st International Peer To Peer

Systems Workshop (IPTPS), on Mar 2002, pp. 251-260.

[22] Roger Dingledine, Nick Mathewson and Paul Syverson. *Tor: the second-generation onion router*, in Proceedings of the 13thconference on USENIX Security Symposium - Volume 13.USENIX Association, 2004, pp. 2121.

[23] Juha Salo. *Recent Attacks On Tor*. Aalto University, T-110.5290 Seminar on Network Security Fall 2010, updated on 2012-05-06.

[24] Chan Tin, Jiyoung Shin and Jiangmin Yu . *Revisiting Circuit Clogging Attacks on Tor Availability*. Reliability and Security (ARES), 2013 Eighth International Conference on 2-6 Sept. 2013, pp. 131 140.

[25] Rob Jansen, FlorianTschorschz, Aaron Johnson and Bjorn Scheuermannz. *The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network*. NDSS 14, on 23-26 February 2014, San Diego, CA, USA.

[26] Steven Murdoch and George Danezis. *Low-cost traffic analysis of Tor, Published in Security and Privacy*. 2005 IEEE Symposium, on 8-11 May 2005, pp. 183 195

[27] B. Zantout and R. A. Haraty. *A Comparative Study between BitTorrent and NetCamo Data Communication Systems*. International Journal of Computational Intelligence and Information Security. March 2010. Volume 1, Number 2, 2010.

[28] R. A. Haraty and B. Zantout. *The TOR Data Communication System*. Journal of Communications and Networks. ISSN 1229-2370. Volume 16, pp. 415-420, August 2014.

[29] Abdul Nasser El-Kassar and Ramzi A. Haraty. El Gamal *Public-key Cryptosystem Using Reducible Polynomials over a Finite Field*. Proceedings of the 13th International Conference on Intelligent & Adaptive Systems and Software Engineering (IASSE-2004). Nice, France. July 2004.

[30] Ramzi A. Haraty, Abdul Nasser El-Kassar and Bilal Shebaro. *A Comparative Study of RSA-based Digital Signature Algorithms*. Journal of Mathematics and Statistics. ISSN: 1549-3644. Volume 2, Number 1. 2006.

[31] R. A. Haraty and B. Zantout *A Collaborative-based approach to Avoiding Traffic Analysis and Assuring Data Integrity in Anonymous Systems*. Computers in Human Behavior Journal. Volume 51, Part B, October 2015, Pages 780791.

[32] Ramzi A. Haraty and Bassam Zantout. *The TOR Data Communication System A Survey*. Proceedings of the Sixth IEEE International Workshop on Performance Evaluation of Communications in Distributed Systems and Web based Service Architectures (PEDISWESA2014). Madeira, Portugal. June 2014.