International Journal of Information & Network Security (IJINS)
Vol.1, No.2, June 2012, pp. 105~109
ISSN: 2089-3299

Review on Attack and Defense in Tor

Muhammad Aamir
MS-IT (Computing), SZABIST

Article Info

Article history:

Received May21th, 2012
Accepted June 6th, 2012

Keyword:

Tor
Anonymity
Communications
Relay Network
Exit Node
Snooping

ABSTRACT

Tor is currently the most famous tool of anonymous TCP communications for clients who need security, privacy and anonymity in their low-latency communications over the public network such as Internet. For this purpose, Tor provides reliable ways of communication through randomly selecting relay network circuits on client's request to offer a secure communication path. However, several research papers are available which identify weaknesses of Tor that attackers can exploit to reveal a client's identity. This paper highlights a few such Tor's weaknesses through which attackers can launch snooping attacks on Tor. Some major attacks are discussed and it is observed that most attacks are launched at application-level protocols such as HTTP after compromising exit node or both entry and exit nodes of Tor relay circuits. Countermeasures against such attacks are also identified to increase security and anonymity over Tor based communications.

Corresponding Author:

Muhammad Aamir,
MS-IT (Computing),
Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST),
90 Clifton, Karachi, Pakistan.
Email: aamir.nbpit@yahoo.com

1. INTRODUCTION

Tor refers to an overlay network designed to provide anonymity to users who want to protect their identity as well as communication privacy. It is the most popular way of establishing anonymous communications over public network infrastructure such as Internet. Tor is designed to anonymize low-latency TCP (Transmission Control Protocol) communications through relay devices or routers referred as Onion Routers.

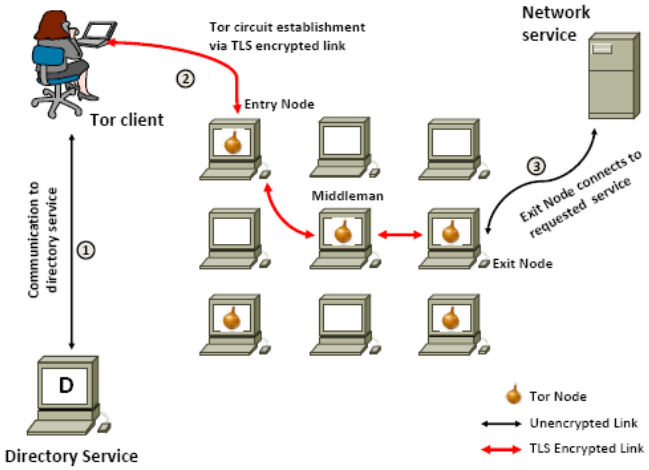

Figure 1. Communication through Tor

In figure 1, steps of communication through Tor are mentioned [1]. Before the start of communication through Tor, the client first makes a connection with Directory Service to obtain the list of available Tor nodes through which the communication can be established with the required host or service. This communication with Directory Service is not encrypted. Tor is a volunteer run relay network and its relay nodes are first identified by Directory Service to show their availability to users.

Once the client selects the relay network to be used for communication (three relays by default), the encrypted data starts to be sent over Tor relay network by the client browser through its proxy service to the first node on the relay network referred as Entry Node. This data is encrypted with TLS (Transport Layer Security). In fact, the feature through which Tor provides anonymity to users is the way it encrypts data and transmits it through the nodes (Onion Routers) of relay network. Layers of encryption are placed on data at the start of communication and each node or router through the path has to remove one layer of encryption to be able to forward the data. A node in the path of Tor can only know from which node it has taken data and to which it is providing it. It can never know the complete path of end-to-end communication. In this way, both identity and data content of the client are protected.

The last node in Tor relay network is referred as Exit Node. At this point, encryption layers placed for Tor communication are all removed and if end-to-end encryption is not used, this node can be compromised to fetch user's communication and identity. Therefore, Exit Node has been the best attraction for attackers who attempt to compromise client's anonymity over Tor based communications. Onion routing in Tor is designed to provide low-latency, bidirectional communications to users such as web browsing. The unit of transmission in Tor is called a *cell* which is a 512-byte fixed size packet and padded if required [2].

The aim of this paper is to provide an overview of different kinds of attacks on Tor that may currently be found in different papers and not in a single article. It may therefore be helpful for readers and researchers to get an insight of overall security position of Tor in terms of threats and kinds of major attacks it may face in recent times. Moreover, a review on attack mitigation techniques and countermeasures has also been presented to identify how Tor can be made more secure to prevent anonymity and data during the communication over Tor's relay circuits.

2. WEAKNESSES OF TOR

Tor has been designed to support anonymous TCP communications for low-latency data such as web browsing and instant messaging. However, the low-latency feature of Tor based communications has introduced a trade-off for its anonymity performance. The anonymity requires protection of both user's identity and data content. Since Exit Node in Tor relay network is responsible to forward data content to the destined host or server, its services can be tricked with malicious code by attackers to snoop the identity and data content of ongoing communications through different techniques. There are numerous attacks identified by researchers which exploit the weaknesses in Exit Node of Tor network. Most of the attacks are launched at application-level protocol such as HTTP (Hypertext Transfer Protocol) to get user's information of web browsing [3], [4]. Some attacks also target routing schemes of Tor to find its vulnerabilities and compromise user's anonymity [5].

3. ATTACKS ON TOR

In this section, a few attacks against Tor relay network to compromise user's anonymity are discussed.

3.1. Browser Based Attack exploiting Flash Active Content

Software pieces which plug into browsers such as Flash, Java and ActiveX controls impose the risk of compromising user's anonymity because these plugins do not necessarily use Tor relay network. Instead, they make direct TCP connections with the requested web server. These plugins are well known problems in anonymous web browsing and most of the anonymous communication systems warn users to disable these active contents in browsers.

A browser based attack has been discussed in [3] exploiting Flash active content in client's browser. It is based on the assumptions that web server is affected with malicious code and exit node is in the control of attacker. In this attack, malicious web page is responded by the server in which it also inserts an invisible *iframe* alongwith a unique cookie. The browser receives a malicious Flash application with web page and if Flash is enabled in the browser, the Flash movie is executed invisibly. As a result, browser will send the cookie associated with attack to malicious web server by making direct connection with the server and bypassing Tor. The web server will be able to identify pages sent to specific users after matching the cookies with direct Flash connections. The anonymity of clients is at risk as their HTTP traffic passing through compromised Tor exit node is associated with their respective IP addresses.

3.2. Browser Based Timing Attack exploiting JavaScript

Another browser based attack is discussed in [3] exploiting JavaScript content in client's browser. It is also based on the assumptions that web server is affected with malicious code and exit node is in the control of attacker to modify HTTP content destined for Tor client by the requested web server. It also assumes that the attacker has inserted a malicious entry node in the network which is used for traffic analysis or illicit snooping. In this attack, the compromised exit node modifies HTTP traffic destined for Tor client by the requested web server to include invisible JavaScript signal generator to generate a unique signal for each Tor client. When browser receives the traffic, it executes JavaScript code and sends a distinctive signal to malicious web server. This transmission is performed through Tor so the client is still anonymous at this stage. By default, Tor relay network circuit is changed for Tor clients approximately after ten minutes. Eventually, a Tor client can pick the malicious entry node to send data over Tor network. The attacker can snoop and perform traffic analysis to compare signals passing through the compromised entry node with numerous signals received by the web server. A match will disclose the user's identity and traffic history during the time he used malicious exit node.

3.3. Forged Web Page Injection Attack

In [4], two schemes of a potential HTTP-based application-level attack on Tor are explained which do not need to have browser plugins enabled, thus imposing a greater risk on Tor based communications. In forged web page injection attack, it is assumed that both entry and exit routers are under the control of attacker which are inserted in the Tor network. When client requests for a web page, exit node records the circuit identifier (CircID) and stream identifier (StreamID) values of the request cell and also injects forged web page with malicious code logging the current time after circuit is established with the client. Malicious web links are inserted in the forged web page with *img* tags for empty images. The client's browser is tricked to execute malicious web links to fetch images within a certain time during which the current Tor network remains established. The malicious entry node can carefully examine the flow of data for forward and backward cells within specified time. Although data content is encrypted, circuit identifier (CircID) and cell command can be checked by decrypting each cell and observing the distinctive traffic pattern. The distinctive traffic pattern is considered as detected if it matches with the expected one based on a similarity metric.

3.4. Target Web Page Modification Attack

In another attack scheme discussed in [4], it is assumed that both entry and exit routers are under the control of attacker which are inserted in the Tor network and the exit node modifies HTTP traffic content of web page provided by a web server on client's request, instead of injecting a forged web page itself. It is named as target web page modification attack. In this attack, a malicious Tor exit node is used to modify HTTP traffic to insert web links for empty images in addition to original web links contained in requested web page. The client's browser is tricked to execute malicious web links to fetch images along with executing original web links provided by the web server on requested web page. The malicious entry node can log cells passing through it to observe the distinctive traffic pattern. The distinctive traffic pattern is considered as detected through careful traffic analysis if it matches with the expected one based on web page modification time to establish a communication relationship between the client and the web server. The client's identity is thereby revealed.

3.5. Attack on Tor's Routing Algorithm

In [5], it is identified that attackers can launch routing attacks even with their low-resource machines (nodes or routers) by fake advertisements to Directory Service. Since Tor is designed to provide anonymity to communications of users for low-latency applications, it has compromised Tor's performance in terms of its privacy features and algorithms of node selection and information routing. Directory Service is configured to select fast and stable entry and exit nodes to establish a Tor circuit. For Directory Service, fast node is one which has significant bandwidth, whereas stable node is one which has significant uptime (greater than the median values of all routers). There are ways through which malicious routers can advertise their fake uptime and bandwidth to trusted Directory Service. Therefore, it increases the probability that malicious nodes can be chosen as entry or exit nodes for new client's Tor circuit. When entry and exit nodes are compromised in this way, it increases the chances for attackers to launch snooping attacks or other traffic analysis techniques.

3.6. Attack on Tor through Bridges

A list of clients or nodes exists for whom using Tor is prohibited by some official means. Users are censored for accessing Tor to protect illegitimate web content or communications being done anonymously to bypass several policies and rules. Such users seek help from bridges, serving as unlisted first-hop relays on Tor circuits. In this case, bridge is itself a client or user for Tor relay network. However, it is done on behalf

of a censored node to which the bridge is directly connected. Bridging is voluntary and being used widely to access Tor for enjoying benefits of anonymity.

As the censored node is directly connected to a bridge, it is compromised at first stage because if an attacker could snoop bridge's traffic through malicious entry and exit nodes on Tor circuits as discussed before, client's identity would also be revealed. The current bridge design makes it easy for attackers to locate *many* bridges [6]. Therefore, bridges cannot be considered as a trusted service always and their node configuration parameters might contain security flaws which attackers can exploit to further compromise the client's identity and data confidentiality.

4. COUNTERMEASURES TO PREVENT ATTACKS ON TOR

There are a few important countermeasures identified by earlier research papers to prevent illicit snooping and other attacks on Tor. Some papers also mention the detection of snooping attacks on Tor. In [1], a detection technique has been discussed using decoys. It was applied to detect illicit traffic snooping in Tor. Decoys are credentials which are controlled by users themselves to detect sessions made through such credentials, source and location of attacks etc. Decoy credentials are exposed to world through realistic sessions involving many client-server interactions so that they are nearly impossible to differentiate from real user sessions. In this way, attackers believe that they are real credentials and try to exploit Tor circuits and systems through such credentials for traffic analysis, illicit snooping etc. Since decoys are in the control of users, they can identify source IP address, attack location and sessions created through decoy credentials.

In [5], it is discussed that routing attacks on Tor can be mitigated by enhancing Directory Service algorithms to choose entry and exit nodes so that there may be a lesser chance of selection of malicious nodes for new client's Tor circuit. Verification of uptime and bandwidth through verification mechanisms should be performed in Directory Service's node selection algorithms so that fake advertisements of nodes regarding uptime and bandwidth can effectively be identified. Similarly, circuit establishment and cell routing algorithms should also be improved to prevent attacks launched through compromised nodes and routes.

In [6], it is discussed how attacks on bridge nodes can be mitigated through several defense mechanisms. There are ways through which attacker's discovery of bridge nodes can be mitigated. Moreover, different steps are proposed to protect bridge nodes, compromising which could easily reveal client's identity. Almost all attack mitigation mechanisms discussed in the paper require reduction of service level of bridge clients to improve the privacy of bridge operators. It is suggested that server activities should be separated from client activities to eliminate threats to the privacy of bridge operators. Limited service levels must be used while establishing Tor circuits through bridges.

In addition to above, earlier research papers also identify some general countermeasures regarding browser and protocol settings to prevent Tor clients from illicit snooping and traffic analysis attacks. They are mentioned as below:

4.1. Minimizing chance of malicious router selections

Chance of malicious router selections on Tor circuit can be minimized by preventing client's web browser using the same relay network. The same Tor circuit for a client's browser is maintained for at most 10 minutes as per specification of Tor protocol.

4.2. Disabling active browser contents

The most effective defense against browser based attacks on Tor can be disabling active browser contents and plugins such as Flash, JavaScript and ActiveX controls. However, disabling these contents also preclude many important web applications which can irritate a user.

4.3. Using HTTPS

Most snooping attacks on Tor are application-level attacks exploiting HTTP. Malicious exit nodes modify HTTP based traffic destined for specific user. In such cases, use of HTTPS (HTTP over SSL) prevents a malicious node to read or modify the data it is carrying for a user. Traffic analysis by malicious entry nodes can also be successful only if HTTP traffic could be modified by malicious exit nodes.

4.4. Detecting abnormal traffic through web browser plugin

There are some attacks discussed above which generate abnormal traffic that can also be detected by the client. For example, forged web page injection attack enables a malicious exit node to send a forged web page to the client with hidden web links to fetch images exploiting malicious entry node to examine flow of data cells. In such type of attacks, a secure web browser plugin installed at client side can detect abnormal

traffic and warn user to be careful and take further actions to defend the communication against an attack. A secure web browser plugin can be designed and installed like web proxies used as anonymity protection tools.

5. CONCLUSION

In this paper, weaknesses of Tor are identified and some major attacks on Tor based comunications are discussed. It is observed that most attacks are launched at application-level protocols such as HTTP. Some attacks exploit active web browser contents of client such as Flash, JavaScript and ActiveX controls. Some other application-level attacks do not need to use such web browser plugins whereas some are launched to exploit weaknesses in Tor's node selection and routing algorithms. A few other can make use of weaknesses in Tor's bridge nodes. Almost all attacks take the assumption that both entry and exit nodes or at least the exit node of Tor relay circuit are malicious and under the control of an attacker to launch traffic analysis and snooping attacks. The countermeasures for mitigating attacks against Tor are also identified in this paper and it is mentioned that some techniques may be employed at client side to protect user's identity and data over Tor based communications such as minimizing chance of malicious node selections, disabling browser's active contents, using HTTPS and detecting abnormal traffic through a secure web browser plugin. Finally, we are able to identify that major sources of attacks on Tor are malicious entry and exit nodes under an attacker's control. Directory services must make use of a secure algorithm to identify genuine nodes before offering the client a ciruit to establish through Tor. In addition, bridge operators should also evaluate the level of services running on bridge nodes and take corrective measures to secure the nodes in order to protect anonymity and communication data of clients.

REFERENCES

[1] S. Chakravarty, G. Portokalidis, M. Polychronakis and A.D. Keromytis, "Detecting Traffic Snooping in Tor Using Decoys," in *14th International Conference on Recent Advances in Intrusion Detection*, Springer-Verlag Lecture Notes in Computer Science, vol. 6961/2011, pp. 222-241, Sep 2011.

[2] S. Benmeziane, N. Badache and S. Bensimessaoud, "Tor Network Limits," in *International Conference on Network Computing and Information Security (NCIS), IEEE*, pp. 200-205, May 2011.

[3] T.G. Abbott, K.J. Lai, M.R. Lieberman and E.C. Price, "Browser-Based Attacks on Tor," in *7th International Conference on Privacy enhancing technologies*, Springer-Verlag Lecture Notes in Computer Science, vol. 4776/2007, pp. 184-199, Jun 2007.

[4] X. Wang, J. Luo, M. Yang and Z. Ling, "A potential HTTP-based application-level attack against Tor," *Future Generation Computer Systems*, Elsevier Science Publishers, vol. 27, issue 1, pp. 67-77, Jan 2011.

[5] K. Bauer, D. McCoy, D. Grunwald, T. Kohno and D. Sicker, "Low-Resource Routing Attacks Against Tor," in *ACM Workshop On Privacy in Electronic Society*, pp. 11-20, Oct 2007.

[6] J. McLachlan and N. Hopper, "On the Risks of Serving Whenever you Surf: Vulnerabilities in Tor's blocking resistance design," in *8th ACM Workshop On Privacy in the Electronic Society*, pp. 31-40, Nov 2009.

BIOGRAPHY OF AUTHOR

Muhammad Aamir is MS-IT (Computing) Student at Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST), Karachi, Pakistan. He has done his Graduation (Bachelors of Engineering in Industrial Electronics) from Institute of Industrial Electronics Engineering (IIEE) under affiliation of NED University of Engineering & Technology, Karachi, Pakistan. His topics of interest are Computer Networks, Communication Systems and Information Technology in Industrial Automation. He is a member of the IEEE and Computer Society of IEEE. He is also a reviewer of IEEE conference papers.