Proceedings of International Conference on Technology and Social Science 2017
Invited Paper

Websites Identification Based on Fingerprinting attack against Tor Browser

Lu Kai Noriaki Yoshiura

Lu.k.625@ms.saitama-u.ac.jp yoshiura@fmx.ics.saitama-u.ac.jp

Information Science Department, Graduate School of Engineering, Saitama University,
Shimo-Okubo 255, Sakura-ku, Saitama-shi, 338-8570 JAPAN

Keywords: Network Security, Tor, Fingerprinting Attack

Abstract. Tor is the most popular anonymous communication tool around the world. its encryption mechanism protects users' privacy. Websites fingerprinting attack is designed to figure out websites which Tor browser may access. This paper proposes a suggestion that the capability websites fingerprinting dictionary should be extended when we implementing a WF attack. We explain two ways to improve the knowledge of dictionary: broadening the width and increasing the depth.

1. Introduction

Anonymous communication[1][5] provides users with secure communication environment by concealing contents of data transferred and hiding identities of both connecting ends. Anonymous communication also gives users the opportunity to bypass strict censorship from eavesdropper or even government in a totalitarian regime[1]. Usually, when users access web servers, they unintentionally expose their destination websites along the way. Some routers may collect information on client behaviors[2]; eavesdropping on an encrypted conversation can still figure out whose data and how much is being transferred by traffic analysis[3]. Furthermore, some countries in the world even have robust censorship like the GFW (the Great Firewall) to prevent access to servers in some foreign area. These reasons stimulate the popularization and the application of website proxy and VPN, which depend on one relay server outside and encrypted channels based on SSL[4]. Besides, proxy cache function leads to high-speed browsing service.[11]

Tor is known as the popular anonymous communication tool in the world. Its glorious encryption mechanism protects users' privacy and prevents the information leakage[5]. However, someone may abuse this tool for illegal activities. Websites Fingerprinting attac[2][6][7] is a method to identify websites which Tor Browser users may access by matching suspicious pages with a dictionary which is composed of monitored websites fingerprinting. In this paper, we pointed out that the scope of the dictionary should be extended.

We introduce the structure of Tor and mechanism of layered encryption in section 2. We simply review the Fingerprinting attacks and related research against Tor Browser in section 3. More detail of attacks implementation will be showed in section 4. We address several issues about the attacks and propose a new design in section 5 and conclude the paper in section 6.

2. TOR(The Onion Router)

Tor is one of the most prevalent anonymous communication tools used widely. Three nodes are randomly chosen from Tor directory servers, which are called as the entry node, middle node and exit node[5]. Clients build circuits, consisting of these three nodes, to communicate with destination websites (see figure 1). Tor uses TLS to communicate between nodes[6] (see figure 2).

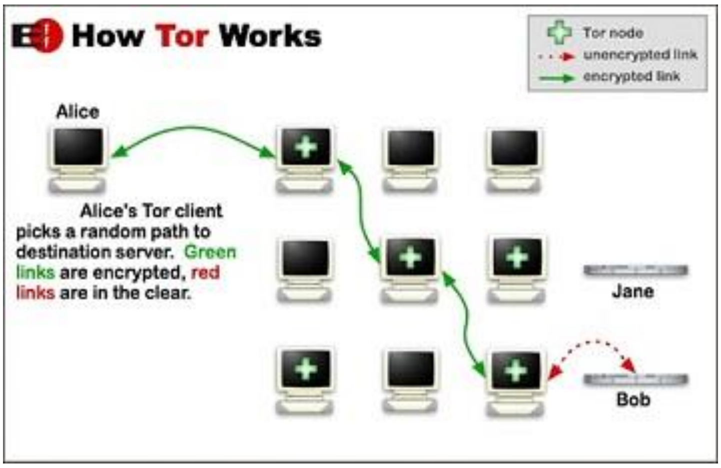
How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Figure 1: the structure of Tor network (cite from TOR homepage)

Although both two adjacent nodes including user's and his destination nodes know their address, they do not realize which parts of the communication circuit they belong to[2][7]. These nodes are contributed by thousands of volunteers. Each node can play every of those three main roles simultaneously in different connections. Furthermore, the data is encrypted which is transmitted respectively from users through these three nodes like structure of onion layers. These multiple layers of encryption processes achieve low latency and high security to prevent the leak of the data.

There is no doubt that these similar applications meet the demand of free speech and satisfy desires for information disclosure. However, someone may abuse these tools for malicious purposes and there should be ways to prevent or monitor his procedures. Fortunately, several attack methods have been found against the anonymity system for different goals, and requirements.

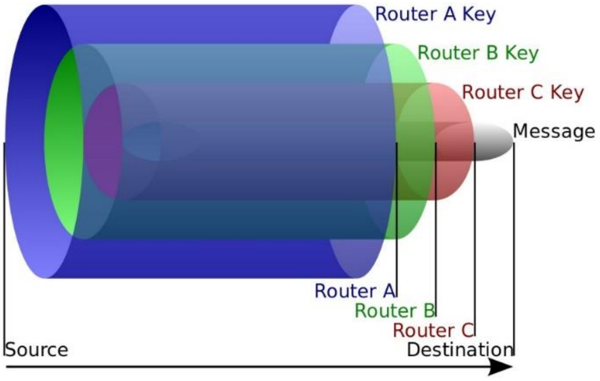

Figure 2: the encryption of Tor network(cite from TOR homepage)

If website fingerprinting is accurate, however, then Tor cannot protect client anonymity against an attacker who is able to monitor the connection between the client and the first relay of the Tor circuit (entry node). Furthermore, as Tor relays are operated by volunteers with no presumption of trust, they may act as attackers as well. Tor orders randomization defences to protect itself against website fingerprinting.

3. Related Research

3.1 Website fingerprinting

Website fingerprinting constitutes the identities of a website[7]. The site domain name, the look and feel of the content, and the lock icon (digital certificate) are the elements used to establish the identity of a website. However, in a real world scenario, a real attacker does not know these important properties in advance. The root problem is that there is no hard and fast definition or a distinctive property to identify a website, which is available to match and hard to duplicate, from the angle of the attacker[2][7].

Although layered encryption can hide whole contents of data sent on the Internet, someone can still estimate the volume of the data transferred, record the duration of the conversation and even learn the direction of the traffic flow between senders and receivers. This vulnerability allows an eavesdropper to recognize which certain page a victim is monitoring are visiting. Hence, the volume, time, and direction of the traffic should be analysed in order to refine the website fingerprinting distinctive to recognize a certain website.

3.2 Fingerprinting attack

In 2014, Wang et al[2][14] extract several features as websites fingerprints base on the Tor traffic information they observed from a victim. They consider this type of attack as a classification problem. They analyzed the numbers of incoming and outgoing packets or cells，the durations of communications and total transmission size to determine the weights in their k-nearest neighbor (k-NN) algorithm.

In 2016, Abe and Goto[15], conduct a new type way to classify the monitored websites by using deep learning algorithm on both closed world and open world test. They achieved high accuracy at 88% in closed-world test. They also got 86% true positive rate and control the false positive rate around 2%

3.3 Deep learning method

Recently, deep learning shows its superior ability in the artificial intelligence field[9][10]. Abe and Goto[15] utilized a layered neural network which called autoencoder. In their closed-world test, 100 monitored websites fingerprinting were able to classified as 100 labels. The packages were captured from victim side and matched with this 100 class to see if it belongs to one of these classes.

An autoencoder, an unsupervised learning algorithm, was conducted by setting the target values to be equal to its inputs in this fingerprinting attack scenario. Abe and Goto test many times to limit the hidden layer units to optimize their construction.

4. Implementation of WFA

In this section, we will introduce the way to implement a WFA and the key technics. We will discuss 2 types of tests.

4.1 traffic analysis

Due to the encryption of Tor, We hardly can in specify a website which Tor Browser Users may access. However, an attacker still can play a role of entry node while capturing useful traffic information[7]. Some researcher pointed that way was not realistic, because Tor protocol selects nodes randomly. If possible, an attack also would be monitored the data flow between Tor Browser and its entry node[6].

Captured packets are used to extract Tor cells which are the basic encrypted units for transmission through the Tor circuit. Each cell is limited to 512 bytes[6][15]. It is important to record the time stamp when observing income and outgoing data flow. Meanwhile, an attacker should access some suspicious websites under Tor anonymity environment and record their data size and time stamp to build a dictionary. Which is full of websites fingerprinting arguments.

4. 2 closed-world test

In closed-world tests, the dictionary contains 100 monitored websites fingerprinting arguments which were labeled as 100 classes[12][15]. Tor browser user was supposed to access to these 100 websites. Usually, some researcher chose machine learning methods such as SVM(support vector machine) or neural network to represent the difference and uniqueness of these 100 classes[8]. An attacker match the suspicious fingerprinting with each one in the dictionary to see if it belongs to one certain class. This kind of test was implemented to estimate the accuracy and sensitivity of machine learning method.

4. 3 Open-world test

In the open-world test, Tor browser user would be able to access to not only 100 monitored websites but also those of 9,000 non-monitored websites[7]. A non-monitored website fingerprinting never appears in the attacker's dictionary. In other word, the victim can access a new website that the attacker does not expect. Therefore, the result must be one of the classes in the dictionary or not in the dictionary. It is important to improve the true positive rate and control the false positive rate at a low degree.

5. New type of classification design

We propose a new method based on fingerprinting attack to identify a series of websites which users access. The previous fingerprinting attack aimed to identify a suspect website if it belongs to the monitored data set which contains many popular websites homepages from Alexa Ranking[3][4][7][15]. However, in a real world, we can hardly constrain the data set without knowing more information from Tor user.

For instance, if a Tor browser user can access News sites homepages, we can implement a fingerprinting attack to figure out the suspect page. However, sometimes we also need to know which kinds of news users may read and which kinds of information Tor users may be interested in.

5. 1 The coherence of websites fingerprinting

Many researchers[2][6][7] discussed the ways to improve the accuracy of their machine learning methods. Especially, in an open-world test, when we conclude a result that the suspicious fingerprinting is not in the dictionary, we usually check the true positive and false positive rate in the experiments[7]. However, they omit the importance of the structure of their dictionaries. If we expand the range of dictionary or add more monitored websites fingerprinting into dictionaries, it will relatively increase the possibility that the dictionary range may cover the one fingerprinting of a website which victims may access.

In this regard, we suggest that the top priority is to broaden the knowledge of the fingerprinting dictionary. There are two ways to attain our goal: Broadening the width and depth of the dictionary knowledge.

5. 2 Broadening the width of WF dictionary

The first way to expand the knowledge of websites fingerprinting in a dictionary is Broadening its width. In other words, increase the WF dataset both for training and testing. We could add our dictionary even into 1000 classes. However, in order to estimate how accurately a predictive machine learning model in practice, cross-validation(or rotation estimation) will be carried out completely during the whole phase. This process will create data as 10 times as the numbers in a dictionary for training and testing to prevent overfitting, which means that a large amount of data set may affect the processing time harshly.

Therefore, w0065 should take this fact into our consideration while expanding the knowledge of WF dictionary under good data process circumstance.

5. 3 Increasing the depth of WF dictionary

The second way is increasing the depth of knowledge of the WF dictionary. We would be able to build a new WF dictionary based on last results to implement a secondary or even more WF Attack. All the link pages can be used for a new dataset in a following open-world test.

For instance, when an attack concludes a result like news homepages from the dictionary, it is possible and necessary to collect fingerprinting of all the link pages to build a new dictionary. One major benefit is that the scope of the contents which users access to may be revealed step by step. For instance, if an attacker gets results like a certain video or news portal, it is meaningful to collect all links WF for the following test to know the specific resources are being exposed to the victim.

6. Conclusion

In this report, we design a new way to identify websites which a Tor browser user tries to access. We implement a deep-learning algorithm to improve the accuracy and efficiency of the websites Fingerprinting Attack on Tor browser. Furthermore, this paper shows the details and feasibility which may affect accuracy in both closed-world and open-world scenario.

References

[1] Daiyuu Nobori and Yasushi Shinjo, "VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls", Proceedings of the 11th ***USENIX Symposium on Networked Systems Design and Implementation,*** pp.229–241, 2014.

[2] Tao Wang, Ian Goldberg, "Improved Website Fingerprinting on Tor", *WPES '13 Proceedings of the 12th* ***ACM workshop on Workshop on privacy in the electronic society,*** pp.201–212, 2013.

[3] Andrew Hintz, "Fingerprinting Websites Using Traffic Analysis". ***Privacy Enhancing Technologies***, Volume 2482 of the series Lecture Notes in Computer Science, pp.171–178, 2003.

[4] Daniel Anderson, "Splinternet Behind the Great Firewall of China", ***Acmqueue,*** Vol.10, Issue 11, pp.1–8, 2012.

[5] Esra Erdin, Chris Zachor, Mehmet Hadi Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks", ***IEEE Communications Surveys and Tutorials***, Vol.17, Issue 4, pp.2296–2316, 2015.

[6] Andriy Panchenko, Lukas Niessen, Andreas Zinnen, Thomas Engel, "Website Fingerprinting in Onion Routing Based Anonymization Networks". ***Proceedings of the 10th annual ACM workshop on Privacy,*** pp.103–114, 2011.

[7] Marc Juarez, Sadia Afroz, Gunes Acar, Claudia Diaz, Rachel Greenstadt, A Critical Evaluation of Website Fingerprinting Attacks, ***Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security***, pp.263– 274, 2014

[8] Ariel Stolerman, Rebekah Overdorf, Sadia Afroz and Rachel Greenstadt, Drexel University, Classify, but Verify: Breaking the Closed-World Assumption in Stylometric Authorship Attribution, ***IFIP*** (International Federation for infromation Processing) Working Group 11.9 on Digital Forensics, pp.185–205, 2014.

[9] David Silver, Aja Huang, Chris J. Maddison, Arthur Guez, Mastering the game of Go with deep neural networks and tree search, ***Nature***, NO.529, PP.484-489, 2016.

[10] Ian Goodfellow, Yoshua Bengio and Aaron Courville, Deep Learning, ***Book in preparation for MIT Press***, 2016.

[11] Richard Clayton, Steven J.Murdoch, Robert N.M.Watson, Ignoring the Great Firewall of China, ***Springer***, Volume 4258 of the series Lecture Notes in Computer Science, pp.20-35, 2006

[12] Christopher Olston, Marc Najork, Web Crawling, ***Foundations and Trends in Information Retrieval***, Vol.4, No.3, pp.175-246, 2010.

[13] Marica Amadeo, Claudia Campolo, Jose Quevedo, Daniel Corujo, Information-centric networking for the internet of things: challenges and opportunities, ***IEEE Network***, Volume 30, Issue 2, pp.92-100, 2016.

[14] Tao Wang, Xiang Cai, Rishab Nithyanand, Rob Johnson and Ian Goldberg, Effective Attacks and Provable Defenses for Website Fingerprinting, ***23rd USENIX Security Symposium*** (USENIX Security 14), pp.143-157, 2014.

[15] Kota Abe, shigenki Goto, Fingerprinting Attack on Tor Anonymity using Deep Lerning, ISBN 978-4-9905448-6-7, *Proceedings of th*e ***APANReserch*** Workshop 2016.