Paying the Guard: an Entry-Guard-based Payment System for Tor

Paolo Palmieri and Johan Pouwelse

Parallel and Distributed Systems
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands,
p.palmieri@tudelft.nl peer2peer@gmail.com

Abstract. When choosing the three relays that compose a circuit, Tor selects the first hop among a restricted number of relays called entry guards, pre-selected by the user himself. The reduced number of entry guards, that until recently was fixed to three, helps in mitigating the effects of several traffic analysis attacks. However, recent literature indicates that the number should be further reduced, and the time during which the user keeps the relays as guards increased. Therefore, developers of Tor recently proposed selecting only one entry guard, which is to be used by the user for all circuits and for a prolonged period of time (nine months). While this design choice was made to increase the security of the protocol, it also opens an unprecedented opportunity for a market mechanism where relays get paid for traffic by the users.
In this paper, we propose to use the entry guard as the point-of-sale: users subscribe to their entry guard of choice, and deposit an amount that will be used for paying for the circuits. From the entry guard, income is then distributed to the other relays included in circuits through an inter-relay accounting system. While the user may pay the entry guard using BitCoins, or any other anonymous payment system, the relays exchange I Owe You (IOU) certificates during communication, and settle their balances only at synchronized, later points in time. This novel deferred payment approach overcomes the weaknesses of the previously proposed Tor payment mechanisms: we separate the user's payment from the inter-relay payments, and we effectively unlink both from the chosen path, thus preserving the secrecy of the circuit.

Keywords: Tor, anonymous payments, economy of privacy enhancing technologies.

1 Introduction

The demand for privacy and anonymity is increasing in today's Internet, and many tools of varying effectiveness are available to the users: from simple web proxies and virtual private networks (VPN), to mixnets and onion routing. These different solutions, however, share a common strategy: achieving privacy by relaying one's traffic through one or more intermediary hops, so that the traffic

origin is concealed, and censorship can be bypassed. A simple web proxy can hide an IP address to a casual observer and bypass trivial forms of Internet blockades, but more advanced privacy preserving technologies are needed when confronted to powerful adversaries. One such technology are anonymous routing networks, where the user's traffic is encrypted and bounced off a number of servers before reaching the intended destination, to provide both sender and receiver anonymity. While many similar designs have been proposed, such as Freenet [7] of Tarzan [13], the most widespread and popular network, currently counting millions of users, is Tor, the onion router [9]. Servers composing the Tor network are called *relays*, and the user selects among them a path (called *circuit*) through which his traffic will be relayed. A circuit is usually composed of three relays: an entry node, a middle node and an exit node, so that no single node can learn both the origin and the destination of the communication it relays. The communication itself is concealed by the user using three layers of encryption, and each relay peels off the most external layer before passing it on to the next hop, in a way similar to peeling off an onion (hence the name).

While the Tor design does not prescribe whether users should be also acting as relays, or relays should instead be powerful, dedicated server, the latter is the most common configuration [18]. With a high number of users and a relatively limited set of available relays, especially in the exit node role, the network is mostly sustained by high capacity nodes, that can cope with a high number of connections. However, the very nature of dedicated relays introduces the problem of providing the necessary incentives (whether monetary or not) to operate one. In fact, operating a relay is generally a risky and unprofitable business, and operators currently have to rely on external motivations, whether altruistic or malicious, to run one. Moreover, the high costs associated with running a good capacity node further discourage potential providers from operating a relay. This results in a low number of nodes, which adversely affects the performance and reduces the privacy properties of the network.

Despite an ongoing effort in designing an effective payment system to remunerate node operators, this still remains an open problem. The complexity of the task is due to two main factors: the need to preserve both user anonymity and circuit secrecy, which translates into the need for a privacy preserving payment mechanism; and the complex and distributed nature of the network, which requires payments from each single user to be spread through a number of different relays. In this paper, we propose a novel approach to this issue, which leverages the distributed nature of the payments between relays to provide privacy against actors not directly involved in the transactions (whether they are external observers or other relays). By doing so, we allow the use of anonymous but public record currencies such as BitCoins to be used for payments, although our design strives to remain currency-agnostic.

1.1 Contribution

We propose a system in which users pay for the Tor network by "subscribing" to an entry node. Each user deposits an amount that will be used for future traf-

fic, and uses the entry node as starting hop in all circuits (which is consistent with the upcoming Tor protocol modifications as discussed in Section 2). During communication, the entry node and other relays in the circuits exchange I Owe You (IOU) certificates as promise of future payments, and all outstanding balances between relays are paid simultaneously at a later point in time, using an inter-relay payment mechanism. Both user-to-entry-node and relay-to-relay payments are currency-independent, and the payment mean can be agreed between the two parties. The novelty of our construction resides in the deferred and synchronized inter-relay payments, which enable a strong separation between the circuits used for communication and the related payments. At the same time, the user's advance payment prevents external observers from linking payments to generated traffic.

An open market for entry guards stimulates competition, and encourages operators to come out in the open and publicly advertise their services. This, in turn, enables users to make a more informed decision when selecting relays. A privacy-preserving payment mechanism provides economic sustainability to the Tor network and promotes the credibility of running Tor nodes as a legitimate business, thus leveling the playing field for operators not relying on external resources or motivations.

1.2 Related works

The need for incentives to run relays in anonymous routing networks has been frequently discussed in the relevant literature, leading to different proposals.

The main challenge of remunerating the operators is to design a payment mechanisms that preserves the privacy properties of the underlying anonymous routing network [15]. The first payment schemes date back to the late nineties, and were proposed for the classical mix-nets [11, 12]. More recently, Wendolsky proposed a volume-based accounting system for fixed-route mix cascade systems [19]. The first design to be proposed for Tor was PAR [1], in 2008. The scheme suffers, however, from a number of weaknesses [2]. A second payment mechanism is XPay [6], which aims at being a general privacy-preserving system for charging users of networked services. Similar systems have been proposed for BitTorrent [17], or designed for generic privacy enhancing technologies [14, 5]. However, privacy-preserving payment schemes do not necessarily protect the user's privacy when associated to anonymous relaying networks, as demonstrated by the case of AN.ON [20].

2 Design

In the current Tor protocol, users select during the first connection a set of three relays, which will later be used as the entry nodes of all circuits created for communication for 30 to 60 days. These relays are called *entry guards*, and help mitigating several attacks, including the predecessor attack [21], selective denial of service [4], and statistical profiling. The entry guard design provides a degree

of protection against attackers aiming at becoming the entry node of a particular user, and increases the start-up costs for such attackers by allowing only long-running and capable nodes to be selected as guards. However, a number of recent results indicate that the current design does not yet provide a sufficient level of protection, and may also introduce new vulnerabilities [3, 10, 16]. For these reasons, the Tor team recently proposed to switch to a single entry guard, to be used for a prolonged period of time (9 months) [8].

This design choice, primarily made to increase the security of the protocol, may also open the way for a payment mechanism for the Tor network. In fact, having a single point of entry to the network means that the user can pay directly the entry guard for all traffic. Our proposed mechanism takes advantage of this new setting, and relies on entry nodes as the interface to the users. Each user selects an entry node among the list of potential candidates (entry guards are a subset of the relays, based on larger bandwidth and higher reliability) and "subscribes" to it by making an initial deposit payment of an arbitrary amount. From then on, the entry node will be used as starting hop in all circuits, and will be responsible for indirectly paying the other relays used in the circuits created by the user. In order to deal with downtimes of single nodes, we assume users can connect to any node of the same *family* of the entry guard (families are publicly announced set of nodes run by the same operator). Since the entry node does not know the identity of the exit node, this happen through an inter-relay payment mechanism described in details in Section 2.1. The payment mechanism is based on promissory notes (a promise of future payment), called I Owe You (IOU) certificates. Relays pay to each other all the promissory notes issued during a time interval simultaneously, at a predetermined moment in time. We introduce therefore a risk element for relays holding IOUs, that we offset by introducing a reputation mechanism that affects the relays position in the public relay directory. Since we assume users to buy traffic in advance, the entry node will also keep a balance for the user.

2.1 Inter-Relay Accounting System

Once the user's payment has reached the entry node, and the circuit starts being used, non-entry relays in the circuit start relaying traffic for which they have not been paid yet. On the other hand, the entry node has availability of all funds paid by the user, including the amount owed to the following nodes in the circuit. Each node, starting from the entry node, issues to the following one the equivalent of promissory notes (or time bills), that we call I Owe You certificates. The certificates are relative to a specific interval in time, and are due to be paid at the next balance settlement deadline.

IOU Certificates An *I Owe You certificate* (IOU) is a certificate signed by the issuing node containing information on the amount of traffic to be paid to the receiving node (the *value* of the IOU) and the date and time it was created (the IOU *timestamp*). IOUs are issued at regular intervals (agreed between the sending and receiving node), encrypted and attached to the traffic sent to the

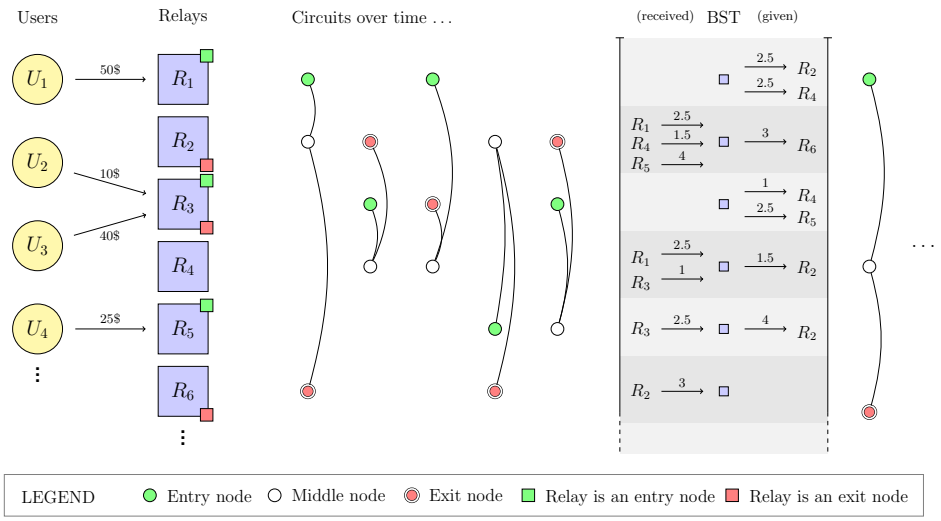

Fig. 1. The inter-relay payment mechanism. At the synchronized balance settlement (SBS) time, the relays settle their respective outstanding balances. This implies a reduced number of aggregated payments, where details of single transactions are lost. In the figure, for simplicity, we assume the same amount of traffic is exchanged in different circuits. Here, exit pricing is 1.5 times the regular traffic price.

receiving node. Each node in a circuit except the last issues IOUs to the following node, and each one except the first receives them from the previous one. As the position of a relay changes between different circuits, most relays will both issue and receive certificates during continued network operation.

Synchronized Balance Settlements All relays participating in the network agree to predefined intervals of time during which IOUs are exchanged but not yet paid . After the end of a time interval, open balances (that is, unpaid IOUs) between relays are settled (paid) at a specific, predetermined moment in time, called *balance settlement time* (BST). The process is illustrated in Figure 1. Aggregated, deferred payments are the pivotal property of the payment mechanism, contributing to enhance the privacy of the user and reduce risk-taking by relays. In fact, in a dynamic network, where relays are part of a significant number of circuits over a single time interval, most relays, taken two at a time, will both owe IOUs to each other. In fact, the duration of the interval itself can be calibrated to satisfy this assumption. This reduces the number of payments between relays (at most one of any two relays will pay the other), and obfuscates the actual amounts owed between relays to an external observer able to track payments.

Dealing with fraudulent or defaulting nodes A malicious entry node may perform a *hit-and-run attack* against other nodes by failing to pay to them the owed amounts at the following BST. We limit this risk by introducing a new

requirement when flagging nodes as "entry guards" in Tor public relay directory. Tor already selects entry guards when a number of parameters are met: uninterrupted up-time of the node and available bandwidth. This ensures that the node participates in a significant number of circuits for each time interval. Moreover, we require the node not to have any open (unpaid) or contested balance settlements from previous time intervals. A contested balance settlements is a settlement for which a node holding IOUs claims not to have been paid for them at the required BST. Such claim is sent to the relay directory, together with the contested IOU certificates, which are therefore publicly disclosed. Disclosed IOUs are nullified, and lose their value. Strategies to reduce the risk of an attacker trying to maliciously exclude honest nodes include allowing only nodes already trusted as entry to contest settlements, limiting the number of reports allowed per node over a time interval, and un-flagging a node already trusted only after multiple reports from different nodes. The accused node can also appeal to the relay directory by presenting proofs of payment for the contested IOUs: this is possible in particular when using public record currencies.

In order to avoid a situation in which the entry node receives a first user payment but drops the circuit without relaying any traffic, and therefore before issuing IOUs to the following node, we require nodes to issue a starting amount of IOUs to each other at circuit negotiation.

Traffic Pricing For the purpose of this work, we assume traffic to be paid the same amount independently of the node relaying it, and we leave to future works the task of investigating a market in which relays can freely set their own price. However, the role of exit node in Tor is generally considered a risky one, and only a subset of nodes are willing to provide this service. This is due to the fact that, if a user visits questionable material behind the protection of a Tor circuit, the user himself will remain anonymous, but the material will appear to have been visited from the IP address of the exit node. For this reason, we introduce the possibility to pay a premium price to exit nodes. A potential strategy to do that is increasing the price paid to earlier nodes by the ratio of exit nodes against all nodes: if N is the set of all nodes, and $E \subset N$ is the subset composed only of nodes allowing exit traffic, we calculate the standard exit price p_E as $|N| \,/\, |E|$ times the standard price.

Time interval duration The ability of the proposed system to hide the payments made for a single circuit by a single user relies on the aggregation of payments between relays imposed by the deferred balance settlements. The more relays owe to each other, the more difficult it is to reconstruct information on single transactions.

Based on the official Tor statistics[1], the average 2 million active users in the first 8 months of 2014 (number extracted from requests to the directories that clients perform periodically to update their list of relays) have been served by a number of relays that went up from more than 5000 in the first months of the year to more than 6000 in the month of August, with a slow but steady

[1] https://metrics.torproject.org/

increase except for a downward movement in the month of May that reached 4500 as the lowest peak. The number of exit nodes has been stable over the same period to around 1000, while entry guards have been increasing from around 2000 to almost 2500. Considering the standard lifetime of a circuit, 10 minutes, we estimate that most entry and exit relays will have been in a circuit with most other relays after a time-frame of around 10 days. This estimate considers that the 10% most popular relays are part of millions of circuits each day. We therefore suggest a conservative time interval duration of 15 to 20 days.

3 Conclusions

Anonymous routing networks are seeing an ever increasing interest, and the number of users went up from the few thousands early adopters of the first mix-nets to the millions of users of today's Tor network. Providing proper incentives to run relays is therefore crucial to ensure the sustenance and development of Tor. In this paper, we design a payment system that allows a relay to be remunerated by the users for the service provided. In particular, we propose users to select a single entry guard, and deposit to the selected node an amount that will be used for paying Tor traffic. In this system, inter-relay payments are strongly separated from both the user's payment and the circuits he creates, thanks to a mechanism based on I Owe You certificates and aggregated, deferred payments. Our design is currency-agnostic, and makes it possible to use anonymous but public-record currencies such as BitCoins while preserving the privacy properties of the system.

The market system we propose in this paper provides an effective platform for building an economy of Tor. Economic sustainability of relay operation will prompt more providers to run new relays or increase the capabilities of existing ones, which will positively impact the performance of the network. A better performing network will in turn increase the number of interested users, thus creating a virtuous circle that will allow anonymizing networks to thrive and prosper.

References

1. Androulaki, E., Raykova, M., Srivatsan, S., Stavrou, A., Bellovin, S.M.: Par: Payment for anonymous routing. In: Borisov, N., Goldberg, I. (eds.) Privacy Enhancing Technologies. LNCS, vol. 5134, pp. 219–236. Springer (2008)
2. Arnold, C., Jansen, R., Lin, Z., Parker, J.: On par for attack. Tech. rep. (May 2009)
3. Biryukov, A., Pustogarov, I., Weinmann, R.: Trawling for tor hidden services: Detection, measurement, deanonymization. In: 2013 IEEE Symposium on Security and Privacy, SP 2013. pp. 80–94. IEEE Computer Society (2013)
4. Borisov, N., Danezis, G., Mittal, P., Tabriz, P.: Denial of service or denial of security? In: Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007. pp. 92–102. ACM (2007)
5. Carbunar, B., Chen, Y., Sion, R.: Tipping pennies? privately practical anonymous micropayments. IEEE Transactions on Information Forensics and Security 7(5), 1628–1637 (2012)

6. Chen, Y., Sion, R., Carbunar, B.: Xpay: practical anonymous payments for tor routing and other networked services. In: Al-Shaer, E., Paraboschi, S. (eds.) WPES. pp. 41–50. ACM (2009)
7. Clarke, I., Sandberg, O., Wiley, B., Hong, T.W.: Freenet: A distributed anonymous information storage and retrieval system. In: Federrath, H. (ed.) Workshop on Design Issues in Anonymity and Unobservability. LNCS, vol. 2009, pp. 46–66. Springer (2000)
8. Dingledine, R., Kadianakis, N.H.A.G., Mathewson, N.: One fast guard for life (or 9 months). In: 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2014) (2014)
9. Dingledine, R., Mathewson, N., Syverson, P.F.: Tor: The second-generation onion router. In: USENIX Security Symposium. pp. 303–320. USENIX (2004)
10. Elahi, T., Bauer, K.S., AlSabah, M., Dingledine, R., Goldberg, I.: Changing of the guards: a framework for understanding and improving entry guard selection in tor. In: Yu, T., Borisov, N. (eds.) Proceedings of the 11th annual ACM Workshop on Privacy in the Electronic Society, WPES 2012. pp. 43–54. ACM (2012)
11. Franz, E., Jerichow, A.: A mix-mediated anonymity service and its payment. In: ESORICS. pp. 313–327 (1998)
12. Franz, E., Jerichow, A., Wicke, G.: A payment scheme for mixes providing anonymity. In: Trends in Distributed Systems for Electronic Commerce. pp. 94–108 (1998)
13. Freedman, M.J., Sit, E., Cates, J., Morris, R.: Introducing tarzan, a peer-to-peer anonymizing network layer. In: Druschel, P., Kaashoek, M.F., Rowstron, A.I.T. (eds.) IPTPS. LNCS, vol. 2429, pp. 121–129. Springer (2002)
14. Humbert, M., Manshaei, H., Hubaux, J.P.: One-to-n scrip systems for cooperative privacy-enhancing technologies. In: Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on. pp. 682–692 (2011)
15. Johnson, A., Jansen, R., Syverson, P.F.: Onions for sale: Putting privacy on the market. In: Sadeghi, A.R. (ed.) Financial Cryptography. LNCS, vol. 7859, pp. 399–400. Springer (2013)
16. Johnson, A., Wacek, C., Jansen, R., Sherr, M., Syverson, P.F.: Users get routed: traffic correlation on tor by realistic adversaries. In: Sadeghi, A., Gligor, V.D., Yung, M. (eds.) 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS 2013. pp. 337–348. ACM (2013)
17. Nielson, S.J., Wallach, D.S.: The bittorrent anonymity marketplace. CoRR abs/1108.2718 (2011)
18. Palmieri, P., Pouwelse, J.A.: Key management for onion routing in a true peer to peer setting. In: Yoshida, M., Mouri, K. (eds.) Advances in Information and Computer Security - 9th International Workshop on Security, IWSEC 2014. LNCS, vol. 8639, pp. 62–71. Springer (2014)
19. Wendolsky, R.: A volume-based accounting system for fixed-route mix cascade systems. In: Second Privacy Enhancing Technologies Convention (PET-CON). pp. 26–33 (2008)
20. Westermann, B.: Security analysis of AN.ON's payment scheme. In: Jøsang, A., Maseng, T., Knapskog, S.J. (eds.) NordSec. LNCS, vol. 5838, pp. 255–270. Springer (2009)
21. Wright, M.K., Adler, M., Levine, B.N., Shields, C.: The predecessor attack: An analysis of a threat to anonymous communications systems. ACM Trans. Inf. Syst. Secur. 7(4), 489–522 (2004)