Poster: COGS — Strengthening Anonymity in Tor with Guard Patience

Tariq Elahi, PhD Student
Kevin Bauer, Post Doctoral Fellow
Mashael AlSabah, PhD Student
Ian Goldberg, Associate Professor
Email: [mtelahi,k4bauer,malsabah,iang]@cs.uwaterloo.ca

Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario

I. Poster Abstract

Tor [2] is a **volunteer-resourced** anonymous communication network designed to provide communicating parties anonymity from their communication partners as well as passive third parties observing the network. As the network has grown, both in number of users and donated resources, there has been a need to capitalize on the available resources to both allow the network to scale and to **safeguard against resource donating adversaries**.

The idea of entry guard relays [5], [4] emerged as a solution to safeguard against specific threats to end user anonymity that also tangentially provides beneficial load balancing properties. Guards were adopted into Tor — with judicious parameters. This was six years ago.

Recently, there has been increased interest [1] in the use of entry guards in Tor and with it the need for the re-examination of the decisions that have driven entry guard implementation details. While there is consensus within the Tor community, on the most part, that entry guards provide a beneficial service, there is yet no empirical evidence of the effects and limitations inherent in their design and in their implementation.

To gauge the impact of entry guards in Tor, we thoroughly analyze guards from security and performance perspectives with a view to both identify the current strengths and shortcomings and to provide a proposal, COGS, to enhance end user anonymity.

Our empirical analysis has found **natural churn** in the Tor network, that is the propensity for network nodes to fail and recover, to provide a large threat to end user compromise rates. Since natural churn is inherent in realistic networks, especially those with volunteer run resources like Tor, we propose methods to mitigate the effects that it has on the anonymity properties of Tor as well its performance characteristics.

Our simulations — based on historical data provided by the Tor project — have given us a deep understanding of Tor relay, especially guard, churn characteristics. We find that end user guard churn can be handled with **patience**. By patience we mean that contrary to Tor's current design of picking a new guard immediately — and hence potentially exposing the end user to the adversary — the end user do nothing and continue using Tor with their remaining guards. The justification comes from empirical data which suggests that guards do not remain offline long enough to require replacement and that one can pick the patience duration according to certain statistical metrics.

Simulations show that a straight-forward version of this protocol — where the client simply waits a fixed amount of time picked from statistical analysis — reduces the amount of malicious guards in clients' guard sets, albeit with certain undesirable performance properties that we overcome with more sophisticated patient guard replacement protocols. We investigate three variations of the basic patience protocol.

Averaged Centralized Patience Meter: The directory service, which provides a consensus of the network state for end user consumption, provides a global patience duration that has been calculated using recent historical churn data of all guards. This timer lets the Tor client know that should one, or more, of its guards go offline that it should wait that amount of time before seeking a new guard. This method does not introduce changes other than the addition of this metric to the consensus document and which can be calculated with the currently collected data.

Individual Centralized Patience Meters: Similar to ACP above, the directory service provides the patience duration to all clients but instead of a global duration for all guards it provides patience durations for each guard. This finer granularity affords more sensitivity to each client's chosen guard set and hence it is expected that it performs better than ACP.

As always there is inherent tension between security and performance and so COGS seeks to balance end user security with load balancing, performance and service availability.

We investigate the load characteristics of the whole network under the above protocols to find the parameters that affect them most. Closed analysis suggests that not replacing offline guards and relying on the remainder will not have any adverse affects. In fact the situation would be no different than what occurs today.

A parallel line of enquiry establishes the limits of patience and the conditions that force us to ignore it and introduce further guards. The primary condition we try to avoid is no online guards at the time the end user wants to use Tor. We further parametrize by investigating end user set limits. Currently, we consider guard numbers and combined guard bandwidth as configurable parameters and search for the sweet spot of security, performance and scalability.

Recent progress [3] shows fruitful and illuminating nuances of guard use in Tor that may lead to a better network which enhances the end user experience, better manages network resources, and reduces the adversary's ability to compromise users.

REFERENCES

[1] R. Dingledine. Research problem: better guard rotation parameters. https://blog.torproject.org/blog/research-problem-better-guard-rotation-parameters, August 2011. Accessed May 2012.

[2] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, pages 21–21. USENIX Association, 2004.

[3] T. Elahi, K. Bauer, M. AlSabah, and I. Goldberg. Changing of the guards: Improving the selection of entry guards in tor. CACR Tech. Rep., May 2012.

[4] L. Overlier and P. Syverson. Locating hidden servers. In *Security and Privacy, 2006 IEEE Symposium on*, pages 15–pp. IEEE, 2006.

[5] M. Wright, M. Adler, B. Levine, and C. Shields. The predecessor attack: An analysis of a threat to anonymous communications systems. *ACM Transactions on Information and System Security (TISSEC)*, 7(4):489–522, 2004.