Location-Aware Onion Routing

Aaron Johnson
U.S. Naval Research Laboratory
aaron.m.johnson@nrl.navy.mil

The Tor network provides low-latency anonymous communication to over two million users daily. To be practical for widespread use, Tor uses onion routing, which does not protect a user against an adversary that can observe a user's traffic at certain vulnerable positions along the traffic's route through the Internet. A natural defense would be to choose Tor relays to minimize the chance that the resulting route can be observed by a network adversary. This idea has been explored to some extent [2, 1]. However, significant security and performance challenges remain. This talk will describe the work of the author and others on designing location-aware path selection algorithms in Tor and outline the challenges that remain to be solved.

There are several types of network entities whose network positions make them of particular concern to Tor users. Automous Systems (ASes), the subnetworks that comprise the Internet, and and Internet Exchange Points (IXPs), locations at which many ASes connect, are frequently on the routing paths to and from the Tor network [2, 4]. Groups of ASes controlled by the same organization or under the same legal jurisdiction are as well [3].

Several proposals have been made to defend against these specific entities by choosing Tor relays so that the resulting Internet routing paths to and from the Tor network do not put them into a position to deanonymize Tor users [2, 1]. These proposals suggest that the Tor network create models of Internet routing and that Tor clients choose Tor relays depending on the location of the client and the destination. This would be a significant change to Tor, which is currently ignorant of Internet routing and treats all clients and destinations the same. Moreover, it is becoming clear that major research challenges remain to make this approach viable.

One challenge is securely and accurately determining the Internet routing paths between clients, destinations, and the Tor network. It has been suggested to use BGP routing information and AS-level path-inference techniques to determine the ASes and IXPs between two hosts. However, recent work has indicated that such inference techniques are too inaccurate to provide security to Tor users over the long term [5]. Moreover, the BGP information itself is the output of an insecure protocol, and it is vulnerable to silent and transient rerouting attacks [6].

Another challenge to location-aware routing in Tor is that it may leak the client's location over time. The analyses of existing proposals consider individual Tor connections, but they do not consider the threat of an adversary who can observe multiple connections and link them to the same unknown user. This is a realistic threat. For example, a malicious web forum may observe the same pseudonymous user connecting over time, or a malicious ISP could observe connections to a server hosted by that ISP on a regular schedule. The well-known intersection attack shows that observations that each leak new information can quickly deanonymize users when linked.

A third challenge to location-aware routing is the interaction between Tor guards and mobile clients. In Tor, each client only connects directly to a small number (1–3) of *guards* to reduce the chance of being exposed to an adversarial relay. These guards are used for 2–3 months. Location-aware path selection may use the client's location to influence initial guard selection, but clients may then move to different network locations. Balancing between choosing new guards for new locations and preventing exposure to malicious guards remains to be explored.

Tor has become very popular in recent years, and it is more important than even to improve its security. A promising approach to solve some serious vulnerabilities is for Tor to become aware of Internet routing and for clients to take location into account when routing through Tor. This idea still has major theoretical and practical challenges to solve, however.

References

[1] M. Akhoondi, C. Yu, and H. V. Madhyastha. LASTor: A low-latency AS-aware Tor client. In *IEEE S&P '12*, 2012.

[2] M. Edman and P. Syverson. AS-awareness in Tor path selection. In *ACM CCS'09*, 2009.

[3] A. D. Jaggard, A. Johnson, S. Cortes, P. Syverson, and J. Feigenbaum. 20,000 in league under the sea: Anonymous communication, trust, MLATs, and undersea cables. *Proceedings on Privacy Enhancing Technologies*, 1, 2015.

[4] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson. Users get routed: Traffic correlation on Tor by realistic adversaries. In *ACM CCS '13*, November 2013.

[5] J. Juen, A. Das, A. Johnson, N. Borisov, and M. Caesar. Defending tor from network adversaries: A case study of network path prediction. *CoRR*, abs/1410.1823, 2014.

[6] Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal. Raptor: Routing attacks on privacy in tor. *CoRR*, abs/1503.03940, 2015.