Onions for Sale: Putting Privacy on the Market

Aaron Johnson, Rob Jansen, and Paul Syverson

U.S. Naval Research Laboratory
{aaron.m.johnson, rob.g.jansen, paul.syverson}@nrl.navy.mil

Problem Overview Onion routing, and in particular the Tor network, is technically well-designed to provide communications privacy. However, the resource constraints of a volunteer network result in unacceptable performance for many users. As a consequence, many users turn to paid services, but even when available they aren't ideal solutions. For example, Virtual Private Networks (VPNs) are often used for anonymous communication and censorship avoidance. However, VPNs are not designed to work against an active or state-level adversary and present a fragile single source of trust, as well as suffering from more subtle flaws [1]. As another example, users hide peer-to-peer file sharing via "seedboxes" that run the P2P protocol at a paid host. However, accessing such services is recognizable, and these solutions again present a single source of trust.

Proposed Solution We propose that Tor supports the optional purchase of its services to simultaneously provide communications privacy to a new population while improving privacy for the old. In this approach, the existing Tor network infrastructure will be used to provide both paid and unpaid service, but paid service will be prioritized to deliver acceptable performance. Users migrating their activity from existing services will improve their communication anonymity and privacy while at the same time providing additional cover traffic and additional resources for Tor's existing user base.

Technical Approach There are several technical components needed to incorporate payments into Tor's main services. To provide incentive to pay for service, traffic from users who pay is prioritized over traffic from those who don't using a new circuit scheduling architecture [2]. Communication between hidden service providers who pay and their clients is similarly prioritized. To enhance censorship evasion, users paying for this service are provided with access to a special reserved pool of bridges. To allow anonymous payments, we can take advantage of Bitcoin, although there are other possibilities. Similarly, there are multiple options for investing those payments into Tor network improvement without centralizing control or liability, such as using trusted third-parties that take direct payment. We feel that the challenges in this approach are surmountable and that the benefits outweigh the associated risks.

References

1. Appelbaum, J., Ray, M., Koscher, K., Finder, I.: vpwns: Virtual pwned networks. In: the 2nd Workshop on Free and Open Communications on the Internet. (2012)
2. Jansen, R., Johnson, A., Syverson, P.: LIRA: Lightweight Incentivized Routing for Anonymity. In: the 20th Network and Distributed System Security Symposium. (February 2013)