The Faithless Endpoint

How Tor puts certain users at greater risk

Len Sassaman[1]

Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
len.sassaman@esat.kuleuven.be

Abstract. We demonstrate that the decision to employ certain security solutions must be balanced against the additional risks that these security solutions introduce for a given user's situation, in the context of its specific threats. As an example case, we consider the anonymity network Tor and examine scenarios where the use of Tor decreases one's overall security. We then show that such trade-offs are reasonable for some, but not all, potential users of Tor. We then consider possible ways to mitigate these risks.

1 Introduction

Tor [4] is a distributed, low-latency anonymous communication service. Tor operates by use of a client application which tunnels the user's TCP traffic through a network of volunteer-operated Tor servers for the purpose of providing anonymity and unlinkability [5] for the user's network communications.

The Tor network consists of Tor servers operated by volunteer administrators. There is no central validation of an operator's trustworthiness; distributed-trust anonymity systems such as Tor assume that some portion of the network may consist of nodes operated by an adversary as part of the threat model they address.

Tor and other anonymity systems based on the mix-net primitive [3] route traffic from the client to its destination on the network through several nodes in the system, encrypting the traffic in a nested fashion such that the first node in the chain only sees encrypted data coming from the client, the next nodes in the chain see only encrypted data coming from the previous node and know neither the source nor the destination of this traffic, and the final node decrypts the plain-text network request, which it is able to read, but does not know the origin of the data.

Should a node in a user's chain be compromised, as long as enough of the other nodes in the selected chain are honest, the user's anonymity is still maintained.

This approach offers better anonymity protection than the "trust-base" approach offered by systems such as Anonymizer [2], where a single compromise of the trusted entity is enough to reveal the identity of its users.

2 Opportunistic end-point attacks

The problem of man-in-the-middle attacks on network protocols has been known for many years. Since performing a man-in-the-middle attack requires the ability to gain access to some point on the victim's network connection, indiscriminate attacks against large numbers of users have been uncommon due to the attention that network operators have paid to the security of their networks.

In recent years, as the use of wireless network connectivity has increased, the prevalence of this class of attack has also increased. Attackers looking for opportunities to steal user credentials, particularly for financial websites, now have a way to control a point in the user's network which facilitates active man-in-the-middle attacks: the wireless access point. Rogue access points can intercept network requests to sites of interest and redirect the traffic to impostor sites under the control of the attacker, allowing the attacker to learn login-credentials and other private information.

While users of the Tor system are protected against manipulation of their traffic by rogue access points due to the network traffic being encrypted to the Tor servers, Tor users are similarly susceptible to easily-performed man-in-the-middle attacks due to the untrusted nature of the Tor network. Should an opportunistic attacker want the ability to view and manipulate the traffic of large numbers of users without compromising key parts of the Internet infrastructure, he need only operate a Tor exit node. Existing man-in-the-middle and identity-harvesting toolkits currently used for rogue access points could be easily adapted to work on Tor exit traffic, putting Tor users at risk.

3 Threat analysis

Tor is designed to combat the threats of network monitoring, traffic analysis, and data interception posed by an adversary who is able to observe significant portions of the network. Users who are concerned about such attacks have traditionally been well-informed about network security in general, and are aware of the dangers of unencrypted traffic. The concerns in 2 are mitigated by good data security practices.

Naive users, who may not be fully aware of the various security threats the Internet poses, and who may be turning to Tor to provide a simple solution to all of their privacy and security problems, are the most likely to suffer. These users are, as a whole, less vigilant about ensuring that their web traffic is SSL encrypted, that their login credentials aren't submitted to an otherwise secure site via a URL argument, that SSL certificates are signed by a valid certificate authority, and so forth.

Ironically, it may be that the users most likely to fall victim to attacks by a malicious Tor endpoint should consider those opportunistic attacks a greater threat, both in terms of potential damage as well as likelihood of occurrence, than the traffic analysis attacks against which Tor aims to protect. As long as there exist security disadvantages to using Tor, this trade-off should be evaluated in the context of a given user's threat model.

Assuming that naive users will have the information necessary to perform a reasonable threat model analysis, however, is ill-advised. Furthermore, it is harmful to the anonymity of the Tor network if it has too few users [1]. A solution to faithless endpoint attacks must be found.

4 Partial Solutions

We propose two partial solutions to this attack.

4.1 Aggressive opportunistic encryption

The Tor client is able to aggressively seek opportunistic end-to-end encryption for the user's network data. The Tor client is bundled with Privoxy [6], a local proxy which sanitizes web traffic by removing identifiable information such as browser type. It is possible to modify Privoxy so that it attempts to connect to requested web sites via SSL first, reverting back to the requested form if the connection via SSL fails. If traffic leaving the last node of the Tor network is encrypted to the actual destination on the Internet, the attacker will not be able to intercept the data.

Should an opportunistic encryption attempt by the Tor client take place through an attacker's Tor node, the attacker could artificially cause the request to fail, forcing a request in the clear. In this case, the client would be no better off for having attempted opportunistic encryption. However, if a user obtains an encrypted session through a Tor chain with an honest exit node, and subsequent network traffic through the Tor system exits through a node operated by an attacker, the integrity of the data will be preserved by the existing encryption session.

4.2 Trusted endpoints

A more comprehensive solution to this problem is the introduction of "trusted endpoints" to the Tor security model. While a user of the Tor network may be unwilling to trust any individual entity to preserve her privacy or anonymity in many circumstances, it is reasonable to place some amount of trust in the assumption that an ISP or other reputable organization would not harvest information for the purposes of financial and identity theft.

The policy of permitting anyone willing to operate a Tor node to participate in the Tor server network should continue; the attack discussed in this paper is not one which can be performed at any point in the Tor chain except the exit point, and this policy provides insurance against the threat that the Tor network could come to be operated by a single adversary. However, if the Tor client were to be provided with a list of "trusted endpoints," the potential for the opportunistic attacks would be mitigated while the benefits of an open network are preserved.

5 Conclusions and future work

We have shown that under certain circumstances, using Tor may put one's security at greater risk than it would be otherwise. While we have offered some suggestions to mitigate these risks, the underlying problem remains: cleartext is dangerous to network users.

It is the lack of ubiquitous cryptography in network communication protocols that enables these attacks in the first place. Providers of network services should work to ensure that whenever possible, network communications are encrypted between the server and the client, and servers can be authenticated by the client, to avoid the potential for man-in-the-middle attacks in contexts where they are a likely threat.

Acknowledgments

We would like to thank George Danezis, Roger Dingledine, and Nick Mathewson for insightful discussions on Tor security trade-offs. We also thank Meredith L. Patterson for her comments on this paper.

This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy). Additional support was provided by the EU within the PRIME Project under contract IST-2002-507591.

References

1. Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the Economics of Anonymity. In Rebecca N. Wright, editor, *Proceedings of Financial Cryptography (FC '03)*. Springer-Verlag, LNCS 2742, January 2003.
2. Anonymizer. http://www.anonymizer.com.
3. David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), February 1981.
4. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.
5. Andreas Pfitzmann and Marit Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. Draft, July 2000.
6. Privoxy. http://www.privoxy.org/.