Analysis of Attack on Tor

Andrew Rosen

November 16, 2014

This document provides a short summary and analysis of the work presented by Bauer *et al.* [1] on compromising the anonymity of Tor [2] users by controlling entry and exit nodes in the system.

1 Attack Description

The Low-Resource Routing Attack (LORA for brevity), is an attack that can to compromise the anonymity of a sender using the Tor network. In a typical Tor setup, a client creates a circuit through the Tor network to communicate with a destination. The goal is to prevent a nosy individual or organization from snooping on the message contents, as well as hiding who the user is communicating with. The client selects three routers[1] for the circuit: an entrance node, a mix node, and an exit node.

Messages are sent through the Tor network to the destination along the circuit, encrypted in multiple layers, such that each hop in Tor removes a layer of that encryption, until the contents are sent unencrypted[2] from the exit node to the destination.

A client selects the entry nodes by obtaining a small list of fast and stable routers from a trusted directory server. Here, fast and stable mean having more bandwidth and greater uptime than the median of the routers. The directory server obtains this information by listening to advertisements from routers.

Mix and exit nodes are also picked based on their bandwidth and stability, although the selection is random to avoid all circuits going through the same router. The greater the router's advertised bandwidth, the more likely a node is selected as a router.

Only the message sender knows the complete circuit the message took in the Tor network. Thus, an observer at the sender's side could tell the client was sending messages, but not what or to whom. An observer at the receiver's end would just see a bunch of random messages. Naturally this entire arrangement is thoroughly upsetting to snoopy people.

2 The Attack

The issue with the above scheme is when an adversary controls both the entrance and exit of the network. The entry node knows who the sender is and the

[1] Three is the default number; the original paper explored the default Tor settings.

[2] Well, not encrypted by the Tor network; the message itself may be some ciphertext for the destination to decrypt.

mix server the message is being passed on to. The exit node similarly knows which mix server the message is coming from and the final destination of the message. An adversary controlling both would be able to tell who a client is communicating with, although not necessarily what about, but that's enough to break anonymity.

The idea behind LORA is to game the router selection process so, with uncomfortable levels of probability, users select malicious nodes as the entrance and exit nodes of a Tor circuit. As discussed, routers along the circuit in Tor are selected based on their speed and stability.

The issue is that information about each router is provided by that router. This information is trusted but unverified, which means an attacker can advertise false speeds and uptime, a technique also known as *lying*.

The adversary has multiple routes for launching this attack. If he has the hardware, he can deploy high performing routers on the network, which would be more likely to be chosen, but probably not likely enough. If the routers don't have the capability needed to have a high chance of being chosen, the malicious routers can lie and say they can handle a disproportionate high bandwidth to skew the exit node selection in his favor.

The adversary can also over-represent his routers in the network using a Sybil [3] attack. In a Sybil attack, a user lies and says that they are multiple nodes. For example, a malicious router could join the network multiple times along the same IP but different ports. A well-executed Sybil attack can turn a non-global adversary into a global-adversary.

Finally, if only one malicious node is chosen as part of the circuit, the adversary can force the user to attempt select a new circuit by deliberately dropping the connection. Experiments demonstrated that an adversary controlling 10% of the routers in this manner could compromise about a third of the circuits formed.

3 Proposed Defenses

The defenses focused specifically detecting

The proposed defense was to build a reputation system to detect adversaries.

3.1 Other Defenses

Snader et alṗroposes[4] a technique replacing self-advertisement with a distributed opportunistic measurement by other nodes. This was initially rejected by Bauer et al. due to the additional load on the network and the inability of the technique to . if probes are opportunistic, the bandwidth impact is miminmal

References

[1] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Low-resource routing attacks against anonymous systems,"

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," tech. rep., DTIC Document, 2004.

[3] G. Urdaneta, G. Pierre, and M. V. Steen, "A survey of dht security techniques," *ACM Computing Surveys (CSUR)*, vol. 43, no. 2, p. 8, 2011.

[4] R. Snader and N. Borisov, "A tune-up for tor: Improving security and performance in the tor network.," in *NDSS*, vol. 8, p. 127, 2008.