Statistical measures and attacks on anonymity networks

Lukáš Hellebrandt

ihelleb@fit.vutbr.cz

Faculty of Information Technology
Brno University of Technology

Abstract

In this paper, we are going to focus on chosen statistical phenomena in the area of anonymity networks.

First, we are going to describe a general anonymity network, what it is used for, why we need confidence in its anonymity ensuring properties and why there are attacks on anonymity being held. Then, we show how anonymity network's anonymity can be measured, using theoretical informatic properties of data. This is important to describe "level of anonymity" of different anonymity networks and mixing strategies. We will show different mixing strategies of circuit-based anonymity networks and compare them by the means of anonymity measurement.

Next, we are going to show two examples of attacks on anonymity networks, one for general anonymity networks and one specifically for The Onion Router (Tor) - one of the most used anonymity networks.

First of these attacks is a traffic confirmation attack described in George Danezis's paper [1]. It is a statistical attack described for general anonymity networks. The attack requires the attacker to be able to eavesdrop on the attack target's entry point to the anonymity network and on exit points. It allows the attacker to decide which exit point matches the entry point of the attack target - thus revealing the target's communications in an unobstructed form. As mentioned in a post [3] on The Onion Router's blog, this is a scenario Tor is not designed to protect against because an attacker needs to have control of both entry and exit nodes simultaneously. The attack is passive and allows a global adversary to match traffic of whole networks.

The second attack shown in this paper is a Predecessor attack described by Matthew K. Wright, Micah Adler, Brian Neil Levine and Clay Shields in their paper [4]. The paper shows a general approach for anonymity networks, rather than for Tor only. The attack is based on watching messages in the anonymity network over certain time and then probabilistically point out the message source. Computation of probability of attack success will also be shown. Apart from the general model, we will show one specific scenario for Tor. Attack in this scenario uses two Tor nodes and a timing attack to verify the nodes are on the same circuit and if there are some nodes in between them.

Finally, we are going to describe Mixminion - a message-based anonymous remailer protocol [2]. Mixminion aims at maximum anonymity possible, however, has a tradeoff of very high latency. Because of that, Mixminion can not be used for almost real time applications such as web browsing where a user expects almost immediate response - a user expects the website to load within seconds after entering an address or clicking a hyperlink. Mixminion is, however, useful for applications which are not latency-critical, such as electronic mail.

References

[1] George Danezis. The Traffic Analysis of Continuous-Time Mixes. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 35–50, May 2004.

[2] George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, May 2003.

[3] Roger Dingledine. "One cell is enough to break Tor's anonymity". https://blog.torproject.org/blog/one-cell-enough, 2009.

[4] Matthew K. Wright, Micah Adler, Brian Neil Levine, and Clay Shields. The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems. *ACM Trans. Inf. Syst. Secur.*, 7(4):489–522, November 2004.