2: DoS mitigation in Tor

Motivation

Tor is an anonymity system that allows users to hide their identities when browsing the Internet. Tor achieves this by separating the endpoints of the communication through a three-hop circuit. Such circuits are built using relays, which are voluntarily operated nodes that form a worldwide infrastructure. To build a circuit, Tor depends on a publicly available list of relays that documents the available nodes and their performance. While this public list creates transparency, it also opens the door for Denial of Service (DoS) attacks, as an attacker can simply pick nodes from the list and stress them. To prevent DoS attacks, Tor implements a DoS mitigation that blocks overly frequent requests from clients.

Instructions

Attack your own Tor relay. This is a hacky project in which you try to cause as much damage as possible! Please follow the steps documented below to structure your project.

1. Literature research: What is Tor and what open security issues are there? What is the current state of DoS attacks on Tor? What are the problems caused by a DoS attack?
2. Familiarize: Get the latest version of Tor and build it from source. Play with the configuration files, the control port, and scripts that allow you to control Tor through a script (Python is a good starting point).
3. Network setup: Create a virtual machine setup in which you run a Tor client on one machine and a Tor relay on another machine. Make sure that they can connect to each other and that the main functionality of Tor does not break.
4. Attack it: Try to trigger the DoS mitigation. Analyze the consequences of a triggered mitigation and its behavior. Review the code and relevant parts of the implementation to find out more about what is going on.
5. Break it: Get creative and try to break Tor. What can you achieve? What would be the consequences in a real-world setting? How could your attack(s) be mitigated?

Goals

- Setup a small test network in which you control a Tor relay and client.
- Analyze the DoS mitigation of the relay.
- Group presentation (∼10 minutes) at the end of the project where you elaborate on the findings of your research.

Ethics: Tor is a live system. Make sure to only attack your own relay. Avoid as much interaction with other nodes as possible. Don't record traffic that is not yours.