Timing attack on I2P web servers

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Thomas Jäggi (GIBB Gewerblich Industrielle Berufsschule Bern)

The Invisible Internet Protocol I2P is an anonymous peer to peer network. It promises discretion to its participants, both in hosting and browsing the I2P-websites called Eepsites. The goal of this thesis is to prove the feasibility of a timing attack on the I2P-network, which allows deanonymizing the hosts of certain Eepsites.

Invisible Internet Protocol - I2P

The I2P-network creates connections between two nodes using so-called tunnels. Each node has various inbound- and outbound-tunnels. Every tunnel consists of multiple nodes. After configuring the system, a client can access an Eepsite over the browser, by simply entering the domain name of the desired Eepsite (e.g. mud.i2p). The I2P-Protocol will then look for a matching entry inside the netDB. The netDB is a distributed database containing the domain and corresponding tunnel gateways.
By connecting an outbound tunnel of the client with one of the inbound tunnels of the server, I2P establishes a connection.
To the client, only the IP-Address of the inbound-tunnel is visible, the real IP-Address of the Eepsite-host remains hidden behind the tunnel. (fig. 1)

Deanonymize a host

As mentioned, the client should have as little information related to the host as possible. If we can link an Eepsite to the real IP-address of a node we consider that node/host deanonymized. And consequently, we know that said node hosts this Eepsite.
The information provided by the IP-Address can be location, VPN or name of the ISP. Therefore we can create a rough demographic about what kind of nodes are active in the I2P-Network.
To get the desired information, we execute a timing attack.

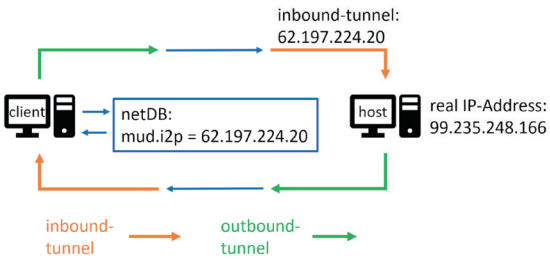

fig. 1: I2P-Protocol

Timing Attack

The attack consists of two parts. Collecting data and analysing that data.
By checking for a response every hour, we monitored the up- and downtime of a considerable amount of Eepsites and nodes, over a few months. We saved the results to a database for later analysis.

For every pair of Eepsite and node, we compare the up- and downtime and repeat this for all timestamps. We then calculate the ratio between matching timestamps vs total timestamps. The higher the percentage of matches, the bigger the chance, that the given node hosts that Eepsite.
This statistical analysis will get more precise with each new timestamp.

In the example below (fig. 2), we compare zeronet.i2p with the node 99.235.248.166. Throughout this analysis, the status for node and Eepsite was equal for 75 % of the compared timestamps, indicating a possible match.

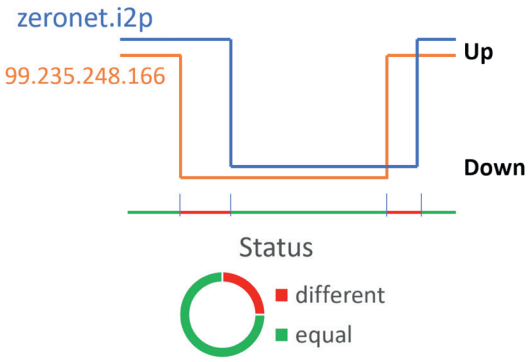

fig. 2: Status of an Eepsite and a node over time

Janek Bobst