# DoS attack against I2P network

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Daniel Voisard

The I2P network is part of the hidden face of the internet. Because of its anonymity, no one can control its content and know where the website hosting servers are. Is there still a way to put down I2P websites? The goal of this bachelor thesis was to find vulnerabilities in the I2P network and perform a DoS attack on a chosen website to make it unreachable.

## The I2P network

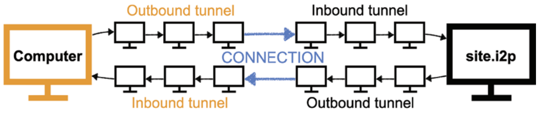
The Invisible Internet Project (I2P) is an anonymous network. It has similar services as the internet: websites, emails, etc. The difference is that all traffic is confidential and encrypted. Nobody is able to see who is communicating with whom and no one can read the communications. Since the first release in 2003, this open source project has grown and is used by more and more people.

Every computer which runs I2P is used as router in the network. It has its own network database which contains a list of other routers with different specifications called RouterInfos and a list of information how to access a website called LeaseSets. To achieve confidentiality, every router builds an inbound and outbound tunnel. Tunnels are made of other routers taken from the network database. These participant nodes will forward the encrypted data for a computer with knowing nothing else than the information of the next node where they have to send the data to. When a machine wants to access a website, the session is established by connecting its tunnels to the tunnels of the website router. Every router IP is known by the network but nobody knows which services a router requests.

## DoS attack

A Denial-of-Service attack is a network attack to make a service (e.g. a website) unavailable to its intended users. A typical DoS attack is done by sending a lot of requests to the service with the goal of an overload and a crash of the targeted machine.

Our goal was to perform a smarter DoS attack on an I2P website. When a router has published its website (by sending its LeaseSet to a router), it verifies shortly after that the LeaseSet has been flooded to other nodes by sending a request to a second router (not the one used for publication). We put some modified routers in the network so that the LeaseSet publication and verification of the website was done by our nodes. This allowed us to forward fake information to other routers by modifying the LeaseSet. Before storing and forwarding a LeaseSet, there is an integrity check. Thus, the modification forces legitimate routers to junk the LeaseSet. Because they do not have the right LeaseSet, they do not know the tunnel entry point. The website becomes unreachable.



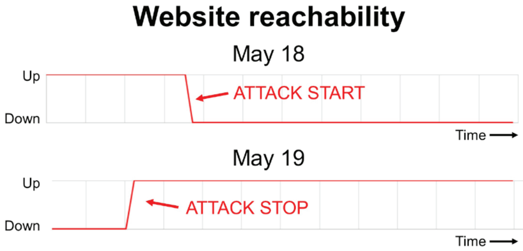
Connection to a website

## Results

We launched a test attack on May 18 morning until May 19 afternoon. All routers that we put in the I2P network used for this purpose were our own machines, even the targeted website hosting router. We had some routers which were continuously sending requests to the target website, to see whether it was reachable. With these statistics, we could deduce if the website was up or down. The results were successful. During all the time the attack was running, there was no single moment when the website was reachable. The attack was really stable without much need for resources.

Julien Laurent Burdet

Micaël Lerch


Website reachability
May 18
Up
Down
ATTACK START
Time
May 19
Up
Down
ATTACK STOP
Time