Analysis of the I2P Network

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

Providing anonymous online communication is challenging and an important task. Similar to the well-known and -researched TOR project, I2P (Invisible Internet Project) aims to provide this inside its own network. But how secure and protected can a user feel when using I2P?
The main objectives of this thesis were to create I2P Observer, a Java program which gathers and publishes information about the I2P network, and to evaluate possible attacks on the software.

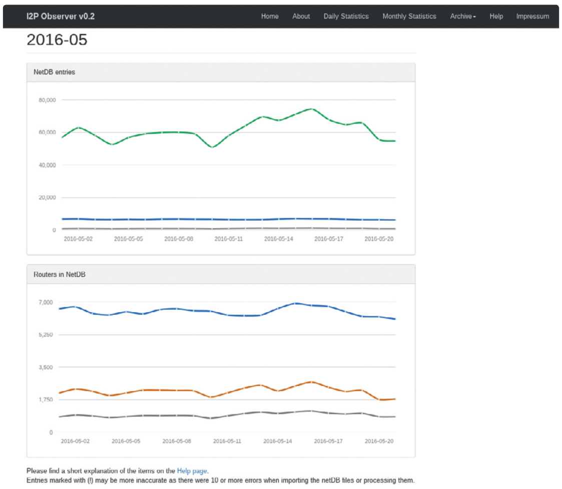
Jens Henning Müller
jens@jenix.net

The I2P Network

I2P aims to provide anonymous communication between participating systems inside an overlay network, separated from other Internet traffic. It is written in Java with versions for Windows, Linux and Mac, providing HTTP- and HTTPS-Proxies for browsing and APIs to adapt applications to communicate over I2P. Multiple layers of strong cryptography are used to protect the content of packets and a mechanism called Garlic Routing, where multiple messages for the same destination can be encapsulated, to hide meta data. Its NetDB, a database distributed across participating peers – so called floodfil routers – contains all information needed to contact other users and services.

I2P Observer

I2P Observer is a software written in Java to collect and publish data from the I2P network to provide historical data about it, with graphical representation of the most important facts to ease the detection of major changes. It extracts information from a locally running I2P instance including addresses, the number of floodfil routers, the amount of entries in the NetDB and the software version. It then creates a website with the collected information, split into daily overview pages with accurate data and monthly ones where the average for each day is computed. I2P Observer is also easily configurable to collect more and more accurate data.



Please find a short explanation of the items on the Help page.
Entries marked with (!) may be more inaccurate as there were 10 or more errors when importing the netDB files or processing them.

Screenshot of the I2P Observer Website

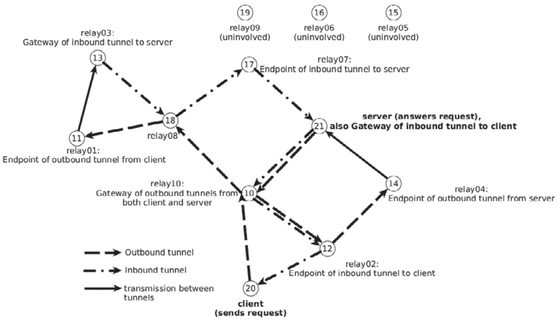
Theoretical Attacks on I2P

The main motivation for this thesis was an evaluation of I2P's security, which was researched with 4 different approaches:

- Impersonation of a service: Can a user be redirected to a malicious server without noticing it? A Clickjacking attack which allows this under certain circumstances was found.
- Identifying I2P traffic: Is it possible to find I2P packets inside a network stream?
- Is Garlic Routing working: Can individual packets be traced through the network if there is little traffic?
- Recap a «High Traffic Attack» in a test setup: Send a high amount of packets towards a target and use the possibility to monitor the whole network to identify all participating peers and the destination. The resulting graph is shown below.

Conclusion

The evaluation showed that I2P has many mechanism build-in to strengthen its security. Its traffic is encrypted and hard to detect, Garlic Routing hides individual packets very effectively and although some attacks seem possible, they depend on many constraints.


19
relay09
(uninvolved)
16
relay06
(uninvolved)
15
relay05
(uninvolved)
relay03:
Gateway of inbound tunnel to server
13
17
relay07:
Endpoint of inbound tunnel to server
18
relay08
11
relay01:
Endpoint of outbound tunnel from client
21
server (answers request),
also Gateway of inbound tunnel to client
relay10:
Gateway of outbound tunnels from both client and server
10
14
relay04:
Endpoint of outbound tunnel from server
12
relay02:
Endpoint of inbound tunnel to client
20
client
(sends request)
Outbound tunnel
Inbound tunnel
transmission between tunnels

Path of packets reconstructed with High Traffic Attack