



Attacking I2P

Introduction

I2P is an anonymizing peer-to-peer network, offering a simple layer that identity-sensitive applications can use to communicate. Data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

The Challenge

The primary goal for the proposed thesis is the theoretical development, practical implementation and evaluation of an attack on I2P. This will be new research. Specifically, there is no concrete idea for an attack yet, we just believe that hardly any anonymous P2P network is actually safe.

Expectations

For the thesis, we expect to see five major milestones:

- 1) Proper technical description of the existing I2P protocol design with implementation details
- 2) Development of a theoretical attack against the system
- 3) Implementation of this attack
- 4) Execution of the attack and demonstration of its viability
- 5) Documentation of the attack in the style of a publishable research paper

Benefits

First of all, we expect that there will be frequent (at least weekly) interactions between the student and the mentors. We will jointly develop attack strategies and provide guidance for implementation and execution of the attack. It should be noted that the research group communicates primarily in English. In addition to the thesis itself, this work should result in a scientific publication, thereby significantly boosting chances for a future academic career.

Prerequisites

In order to start this project, you need to:

- Be able to program in Java
- Have a good background in networking and computer security
- be willing to write a thesis in English
- be interested in science and scientific publishing

Before applying, please study the I2P webpage at <http://www.i2p2.de/> (at least briefly).

