



# IP PREFIX HIJACKING

## HIJACKING EXPERIMENTS IN THE NAME OF SCIENCE!

### Motivation

The world wide network is designed to be a fault-tolerant system. Failure of nodes or links is unproblematic for the network as a whole: routing protocols will adjust the traffic flow to take a different path through the network.

Internet-scale routing is based on the exchange of route knowledge between its participants, and implicitly assumes global trust. This allows attackers and misconfigured routers to inject illicit routes into the routing system, and thus to redirect traffic of other networks into their own.

Up to this day, there is no protection against such hijacks, and it is even harder to discover a hijacking attempt. In this thesis, you will learn about different hijacking scenarios, analyze known real-world incidents and develop techniques to infer attacks out of routing data. You will finally test your methods by Internet-wide hijacking experiments on your own!

### Your Tasks

#### Getting in touch with data sources

First, you have to make yourself familiar with available data sources. These are mainly routing table dumps of Internet border routers.

#### Analysis of real-world incidents

For the development of a hijack detection system, you have to carefully study known real-world incidents like the Pakistan attempt of hijacking YouTube traffic. You will analyze those events in the given data sources and try to identify their characteristics.

#### Hijack detection models

Your main goal is to develop techniques which are capable of detecting hijacks out of the given data sources. Analyses of changes in Internet graphs are an integral part for those techniques.

#### Evaluation of developed methods

Finally, you will get access to border routers of our own autonomous system in order to hijack prefixes on your own. You will then study the effects on the global routing system, and test your detection models in practice.

### Requirements

- Explorative nature
- Knowledge on global routing and graph analysis
- Programming skills (scripting, object-oriented)

### Keywords

Internet routing, border gateway protocol, autonomous systems, graph analysis

