

June 16, 2005

Thomas Dübendorfer, Arno Wagner, ETH Zürich

Diploma Thesis:

Analysis and Detection of Denial of Service Attacks in the Internet Backbone

for Daniel Reichle <dani@reichle.li>

The Problem

Denial of service (DoS) attacks exist in many varieties. They are an increasingly larger annoyance of the current Internet. However, still most DoS attacks go by unnoticed by network operators, especially if they are executed only over a short time period or not that massive. Only few tools and algorithms exist to reliably detect and analyse such attacks.

The Setting

In the context of the project DDoSVaX we collect and keep a long-term (>1 year) archive of flow-level Internet backbone traffic data. The DDoSVaX team has created the online processing framework UPFrame, which supports plugins for near-real time detection of Internet worm outbreaks and attacks. Several plugins were already developed and successfully validated.

The Task

By using current Internet flow-level traffic data and by replaying traffic data of earlier minor and major denial of service attacks from our NetFlow archive, the student will develop an algorithm and implement it as a UPFrame plugin that can be used for the early detection of (D)DoS attacks. The DoS attack detection algorithm will be validated against known attacks in our recorded data.

This task is split into the following subtasks:

Understand the NetFlow data and its processing via UPFrame

Before writing a plugin for the UPFrame it is crucial to get familiar with the NetFlow data and the UPFrame system. Existing plugins will be contemplated to get an idea of

the complexity and the possibilities of a UPFrame plugin.

Develop an algorithm for (D)DoS attack detection

Taking into consideration existing algorithms for (D)DoS attack detection and earlier work on the subject within the DDoSVaX project, an algorithm will be developed aiming at a real-time detection of (D)DoS attacks by successively analysing NetFlow data.

Implement and test the algorithm

A design of the implementation of the detection algorithm will be developed. Then the program will be written for an offline analysis of NetFlow data. In the testing phase, the function of the program will be verified by processing archived NetFlow data of known DoS attacks of the past. As a last step, the algorithm will be implemented as a UPFrame plugin for real-time processing.

As a further optional component, the algorithm could be improved with the help of the test results.

Deliverables

During the work on this thesis the following deliverables are expected:

- Overview of related work on the subject: The relevant papers on the subject have to be described and categorised in a summary.
- Description of the algorithm to be implemented: Before the algorithm is implemented, it has to be presented along with performance estimations and a proposal of the software design.
- Real-time processing UPFrame plugin implementing the (D)DoS detection algorithm.
- Documentation: A written report will conclude this thesis.

Dates

This diploma thesis starts on June 6th, 2005 and will be finished on October 6th, 2005.

Supervisors

Thomas Dübendorfer, duebendorfer@tik.ee.ethz.ch, +41 44 632 71 96, ETZ G95
Arno Wagner, wagner@tik.ee.ethz.ch, +41 44 632 70 04, ETZ G95