1 Introduction

DDoS in general

Distributed Denial of Service (DDoS) attacks are a threat to Internet services ever since the widely published attacks on ebay.com and amazon.com in 2000. ETH itself was the target of such an attack six months before these commercial sites where hit. ETH suffered repeated complete loss of Internet connectivity ranging from minutes to hours in duration. Massive DDoS attacks have the potential to cause major disruption of Internet functionality up to severely decreasing backbone availability.

The DDoSVax Project

In the joint ETH/SWITCH research project “DDoSVax”\(^1\) abstract Internet traffic data (Cisco Netflow) is collected at all four border gateway routers operated by SWITCH. This data contains information about which Internet hosts were connected to which others and how much data was exchanged over which protocols.

2 The Task

A generic robust realtime UDP Netflow (Internet connection data) processing framework was developed in a diploma thesis. However, for efficient traffic analysis in the DDoSVax project we need to have various realtime and near-realtime statistics available. The task of the student is split into three major subtasks: understand the Netflow data and its possibilities, implement a sample plug-in like packet-size distribution, and develop one or two own attack detection methods.

\(^1\)See http://www.tik.ee.ethz.ch/~ddosvax/
Understand the Netflow data and its possibilities

In a first step it is required to understand how the relevant data is stored in a Netflow record and how it can be used to detect attacks.

Implement a sample plug-in like packet-size distribution

To get familiar with the realtime framework and its plug-in support it would be wise to start by writing this simple data gathering plug-in. It is also a good starting point to see which performance bottlenecks in realtime processing must be considered.

Develop one or two own attack detection methods

A common pattern of DDoS attack is the increased traffic originating at hosts which where mostly inactive in the past. Analyzing Netflow records and collecting traffic statistics per IP subnet should expose these attacking hosts. In combination with filtering Netflow records by port numbers (e.g: 25 for internet worms implementing their own MTA) this gives a powerful tool to recognize DDoS attacks.

3 Deliverables

The following results are expected:


2. Attack detection plug-ins Based on the experience with the sample plug-ins one or two attack detection methods should be developed. In an implementation their realtime capability is tested and the output is verified.

3. Written report A concise description of the work conducted in this thesis (task, related work, environment, results and outlook).

Further optional components are:

- More sophisticated attack detection methods and their implementation.

Documentation and Presentation

A documentation that states the steps conducted, lessons learnt, major results and an outlook on future work and unsolved problems has to be written. The code should be documented well enough such that it can be extended by another developer within reasonable time. At the end of the thesis, a presentation will have to be given at TIK that states the core tasks and results of this semester thesis.
Dates

This semester thesis starts on November 17th, 2003 and should be finished by May 10th, 2004.

Milestones

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample plug-in</td>
<td>22.3.2004</td>
</tr>
<tr>
<td>Progress Report</td>
<td>8.4.2004</td>
</tr>
<tr>
<td>Attack detection plug-in</td>
<td>12.4.2004</td>
</tr>
<tr>
<td>Final presentation</td>
<td>29.4.2004</td>
</tr>
<tr>
<td>Documentation</td>
<td>10.5.2004</td>
</tr>
<tr>
<td>Delivery of Semester Thesis</td>
<td>10.5.2004</td>
</tr>
</tbody>
</table>

Supervisors

Thomas Dübendorfer, duebendorfer@tik.ee.ethz.ch, +41 1 632 71 96, ETZ G64.1
Arno Wagner, wagner@tik.ee.ethz.ch, +41 1 632 70 04, ETZ G64.1