Viable data channels for large anti-DDoS systems

Frank Uijtewaal
University of Amsterdam
February 29, 2016

Introduction

DDos attacks are an increasingly common thread. Various companies offer DDoS protection as a service, like CloudFlare and Akamai. Companies that intend to protect themselves can choose from a wide range of commercial solutions, usually in the form of (expensive) appliances. Not all companies have budget for these kinds of systems. In an attempt to help mitigate DDoS attacks, the “anti-ddos” project, also known as “OSAS”, was spawned [1] [2]. This project aims to both provide an affordable, open source, DDoS mitigation solution and to improve the level of expertise in the problem domain by providing academic researchers with data to work with.

The project is still in its infancy and thus most of the system still needs to be designed and created. This research will focus on the communication between the main components within the proposed system and do so in light of the feasibility of the anti-ddos project’s goals. For example, collected data may first need to be anonymized before being made available for public research. The named “main components” have not yet very strictly been defined so the research will hinge loosely around what the anti-ddos project has produced so far. In any case, the results may be equally applicable to similar systems.

Research Questions

For large anti DDoS systems, how may the data channels be set up with both effectivity and security in mind?

• What roles take part in the target system (sensors, analysis machines, stakeholders)
• What challenges exist in regard to security/privacy and how can they be tackled?
• How can the technical parts communicate both securely and effectively?
  – What data transmission methods are there and which suits our case best?
  – How can access control be implemented?

Related work

First of all the origin for this project is the anti-ddos project which can be found at [1]. [3] offers a good foundation on the topic of using NetFlow or IPFIX to for data capture and analysis systems. Furthermore, [4] and [5] show how network traffic can be anonymized.
Scope

The goal of this research is to come up with a viable, high level, architecture of how the major components in an anti DDoS system may interact. Given the little time that is at hand, there is no place to take actual performance measurements, nor to extensively reflect the proposed methods against theoretical performance on available hardware. In there's time a proof of concept will be created but only if it doesn’t negatively affect the main goal of the research, which is the data transmission and how this can satisfy the given needs. No work will be done in DDoS recognition or mitigation. The proposed architecture will assume these modules are already built and functioning. Wherever their interface would play a major role in the format of the transmission protocol, assumptions will be made and explicitly pointed out. At the same time, care will be taken such that the protocol could be modified in case future work on the DDoS related modules requires it.

Approach & Methods

As this is a new topic for the researcher, quite some effort needs to be put in getting up to speed in the field of network flows and anti DDoS solutions. When enough background knowledge is acquired the actual research questions can be addressed, in the same order as they are listed above. The roles will be extracted from the goals that the anti-ddos project has set and possibly others. Then it’s important to get a good grasp of who owns the data, whose privacy is at stake and who can access what data and when. This is an important question because security and privacy measures will have to be built in from the start. Finally, when these questions are answered, the actual architecture can be worked on. A couple of subquestions have already been written out but many more will probably come up while getting more background knowledge.

Requirements

For the theoretical part there are no requirements. In case there’s enough time to create a proof of concept, This will probably be built in a virtual environment for which the SNE’s personal server will suffice.

Planning

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feb 29 - Mar 6</td>
<td>Background research and first two subquestions.</td>
</tr>
<tr>
<td>2</td>
<td>Mar 7 - Mar 13</td>
<td>Third subquestion.</td>
</tr>
<tr>
<td>3</td>
<td>Mar 14 - Mar 20</td>
<td>Third subquestion, documentation and possibly proof of concept.</td>
</tr>
<tr>
<td>4</td>
<td>Mar 21</td>
<td>Presentation.</td>
</tr>
</tbody>
</table>

Expected products

A high level architecture for a large scale anti-DDoS solution. Major points of interest are confidentiality and privacy. Possibly a proof of concept for this architecture will be developed as well but only if time allows it.
Ethical issues paragraph

The research will take the ethical issues that arise when deploying a large scale anti-DDoS framework into account. The research itself doesn’t require much attention on this part, though.

References


