# Real-time DDoS Defense: A collaborative Approach at Internet Scale

In the last years, Distributed Denial of Service attacks (DDoS) evolved to one of the major causes responsible for network infrastructure and service outages. Often the amount of traffic generated by DDoS attacks is such that, although traditional security solutions as firewalls and Intrusion Prevention Systems are deployed, the target network will lose connectivity, because the network resources are exhausted. To optimize mitigation and response capabilities and thus reduce potential damages caused by DDoS attacks, mitigation and response should be moved from the target network to the networks of Internet Service Providers (ISPs). Additionally, ISPs should collaborate and exchange information in context of network security. This poster proposes a framework for flow-based real-time and automatic mitigation of DDoS attacks in ISP networks. The framework collects and processes network flow-based data e.g. NetFlow/IPFIX from the network edge router of an ISP network. The collected data is used to perform anomaly detection, data fusion and classification. In case of a detected anomaly within the flow-based data a security event is raised. Based on this security event a collaborative process is initiated. The framework collaborates with third parties by gathering and processing security information e.g. from other ISPs, customers or available data e.g. Blacklists, Open DNS resolvers etc.).

## Speakers

Jessica Steinberger H-DA

## Authors

Jessica Steinbreger, Anna Sperotto, Aiko Pras and Harald Baier