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

Jessica Steinberger*†, Anna Sperotto†, Aiko Pras† and Harald Baier*

* da/sec - Biometrics and Internet Security Research Group
University of Applied Sciences Darmstadt
Darmstadt, Germany
Email:{Jessica.Steinberger, Harald.Baier}@h-da.de

† Design and Analysis of Communication Systems (DACS)
University of Twente
Enschede, The Netherlands
Email:{J.Steinberger, A.Sperotto, A.Pras}@utwente.nl

Over recent years, network-based attacks have become one of the top causes of network infrastructure and service outages. The reason is that attacks are getting larger, more sophisticated (e.g. multi-vector attacks) and frequent. At the same time it has never been easier to execute DDoS attacks, e.g., Booter services offer paying customers without any technical knowledge the possibility to perform DDoS attacks as a service.

Currently, mitigation of DDoS is performed using traditional security solutions such as firewall and Intrusion Prevention System devices [2]. These solutions are often not able to handle the large amount of traffic reaching the target network. One reason is that the monitoring equipment located at the victim side might exhaust its own resources as a side-effect of the attack. Further if a DDoS attack already reached the perimeter of the target network, it is often too late to start mitigation procedures, because the network link is already saturated. Therefore detection and mitigation need to be located closer to the source of these kind of attacks.

In accordance with van Eeten et al.[1], we believe it to be a promising approach to move mitigation from the target network to the network of Internet Service Providers. Additionally, ISPs should collaborate to share and exchange information in context of network security, in order to support proactive detection, real-time and automatic mitigation of current anomalies [3].

In this talk, we present the results of a survey that aims to gain insight into processes, structures and capabilities of ISPs to mitigate and respond to network-based attacks. Further, we 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 an 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.).

References

[1] van Eeten, M., Bauer, J., Asghari, H., Tabatabaie, S.: The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. In: OECD Science, Technology and Industry Working Papers. Volume 2010/05. Freeman, Rebecca and Auriol, Laudeline and Misu, Max (2013)

[2] Steinberger, J., Schehlmann, L., Abt, S., Baier, H.: Anomaly Detection and Mitigation at Internet Scale: A Survey In Emerging Management Mechanisms for the Future Internet Springer Berlin Heidelberg, 2013, vol. 7943.

[3] Steinberger, J., Sperotto, A., Golling, M., Baier, H.: How to Exchange Security Events? Overview and Evaluation of Formats and Protocols. In: IFIP/IEEE International Symposium on Integrated Network Management (IM2015), 2015. (May 2015) 261–269