Detection and Mitigation of DDoS Attacks at Internet Exchange Points

Marcin Nawrocki, advised by Matthias Wählisch
Freie Universität Berlin, Berlin, Germany
Email: {marcin.nawrocki, m.waehlisch}@fu-berlin.de

***Abstract*—DDoS attacks are a major threat to the Internet infrastructure and end-user systems. As this type of attack is increasingly distributed across Internet domains, an effective inter-domain approach is required to detect and mitigate it. This proposal motivates the utilization of Internet Exchange Points as central vantage points for effective DDoS countermeasures.**

I. Research Problem

Denial of service (DoS) attacks are a major threat to both Internet operators and end-users. A DoS attack attempts to exhaust resources of its target in order to disrupt the availability of Internet services. Typically, this is accomplished by simply flooding the target with a high volume of superfluous data packets (*volumetric attack*). This service disruption does not necessarily solely affect the target of the malicious packets but may also interfere with down- or upstream nodes. Possible variations are distributed DoS (DDoS) attacks, in which the attack is initiated by multiple IP addresses. Another currently very serious DoS extension is the amplifying reflection (DRDoS) attack. In this attack, an attacker sends data with an incorrect source IP address (*i.e.,* IP spoofing) and a third party is exploited to reflect initially small queries as much larger attack payloads. Even well-established protocols and services are susceptible to misuse, such as the prominent DNS [1]. Many Internet operators do not apply ingress filters to prevent IP spoofing.

Individual domains already implement monitors to identify this type of attack. However, DDoS attacks are an Internet-wide phenomena and cannot be detected or mitigated locally, *e.g.,* at a single domain. This is why popular commercial DDoS protection solutions use a distributed approach to monitor the Internet for arising threats. Effective mitigation of cyber security incidents thus mandates to take an inter-ISP view. In order to detect inter-domain attacks, it is necessary to view beyond individual ISP boundaries.

II. Research Proposal

This proposal introduces the utilization of Internet Exchange Points (IXP) data sources for the detection and mitigation of DDoS attacks. Related work already confirms that IXPs can be instrumented as a central vantage point to improve Internet measurements [2].

A. Objectives

Detecting DoS attacks *before* they take effect is challenging. Essentially, most approaches are based on monitoring the volume of traffic or the packet rate in a network. Those detection schemes assume ephemeral spikes in traffic volume instead of long-lasting peaks, or message flows that exhibit a balanced request-response pattern during normal operation. However, these methods still cause an increased load to the resources of an attacked domain. That is why DoS-attacks should be mitigated as early as possible, more precisely at an IXP.

Detect Aggregation of Malicious Flows: Considering network flows, IXPs can characterize customer ports and detect unusual traffic volumes or properties. Analyzing network flows by sampling can help to detect fingerprints that resemble DDoS attacks such as SYN, ACK, GET, POST floods. Suspicious, new flows that accumulate from several to one customer port should be handled with care. To make such analysis possible, a good sampling method is needed that depicts the current flows precisely and further an adapting real-time system that allows fast evaluation.

Detect Spoofing: We see unexploited potential for IXPs in the field of IP spoofing, which is one of the largest challenges to overcome in defending against reflection DoS attacks. Being a central transit point and having detailed knowledge about prefixes of their customers, IXPs have a higher chance of detecting doubtful packet origins.

Increase Reliability: If possible, the detection and mitigation process should be automated. If the envisioned toolchain is deployed by several IXPs, the detection results could be improved even more by a comparison of status reports for suspicious points in time across IXPs.

B. Research Questions

In this proposal, IXPs are envisioned as central vantage points for the detection and mitigation of DDoS attacks. The thesis will answer several research questions, including but not limited to:

1) Which resources and inter-domain knowledge can be instrumented by IXPs to detect DDoS attacks?
2) How can we mitigate the impact of DDoS attacks on the Internet as a whole and sub-domains with the help of IXPs?
3) How can IXPs deal with recent DDoS trends such as attacks from massively distributed IoT botnets?
4) How can IXPs check the integrity of IP source addresses in order to prevent spoofing, hence amplifications attacks?
5) Can we achieve better results by a close cooperation between several IXPs?
6) How do we produce precise real-time results, despite the high volume of traffic?

C. Advances of State of the Art

IXPs already collect measurement data such as traffic volume per (customer) port and detailed traffic statistics for the flows between different customers. Additionally, flow data is sampled. Typically, one in every 10,000 packets is captured at IXPs. However, this is rather done to ensure correct configuration of the infrastructure. Furthermore, some IXPs already have introduced an anti-DoS blackholing service that drops traffic flowing to the victim before entering the IXP platform. This effectively protects the victims resources. Moreover, it still requires manual BGP announcements triggered from the affected domain. Blackholing is an optional service, which is not enabled by all IXP members. Compared to the overall amount of data which is forwarded between IXP members, blackholed traffic is between 0.01% and 0.1% on average at one of the world-wide largest IXP.

This state of the art is likely to change in the near future. Several building blocks (*e.g.,* on-line learning algorithms, highly efficient packet capturing, real-time network analyzer) that can empower IXPs to take advantage of their inter-domain knowledge are close to be ready or already available. Developing a privacy-friendly methodology and a toolchain which can assess IXPs current network situation in detail will allow a precise, semi-automatic DDoS detection in real-time. This would increase the amount of blackholed traffic, which is currently very low, as we estimate the amount of the actual DDoS traffic traversing the IXPs to be much higher. The detection of spoofing will further inhibit amplification attacks, which will mitigate the impact of undetected DDoS incidents. IXPs are a central vantage point which will impose a low configuration and maintenance effort for new toolchains, hence solving two key problems of current distributed DDoS detection systems.

D. Practical Challenges

Measurements at IXPs for inter-domain security face several open challenges. The first challenge is to preserve the privacy of users whose data cross the IXP. A sophisticated data randomization or anonymity method has to be deployed. Moreover, IXPs forward very large volumes of data, hence analyzing it can be expensive in terms of resources and time. A data sampling process and an efficient, distributed computation should be introduced to make real-time results possible (*e.g.,* [3]). The Internet is an ever-changing network. This means, that the system has to adapt to hourly, diurnal, and even weekly patterns for traffic and domain features. The acquired data must not be made publicly available due to four major limitations: (*i*) privacy issues arise since IXPs forward end-user data, (*ii*) conflicting business interests of members might emerge if routing export policies are revealed, (*iii*) IXPs serve their members and must not compete with them by enabling similar services, (*iv*) legal rules may prohibit any kind of traffic analysis.

III. Research Environment

This PhD thesis is written within the project X-Check. X-Check is funded by the BMBF and part of the German Federal IT Security Programme with a special focus on incident response. The project involves universities, IXPs, and a security company. This project explicitly pursues the community-driven approach. The intended objectives will be implemented in close cooperation with the largest IXPs in Germany (DE-CIX and BCIX) and a well-established IT-security company (DFN-CERT). The solutions will be tested and refined during inter-regional field tests. This environment fosters precise and real-world applicable research results.

References

[1] F. J. Ryba, M. Orlinski et al., "Amplification and DRDoS Attack Defense - A Survey and New Perspectives," *in CoRR*, 2015.

[2] N. Chatzis, G. Smaragdakis et al., "On the Benefits of Using a Large IXP as an Internet Vantage Point," in *IMC*, 2013.

[3] M. Vallentin, V. Paxson, R. Sommer, "A Unified Platform for Interactive Network Forensics," in *NSDI*, 2016.