DDoS Attack Fingerprint, DDoSDB, and Their Usage[*]

Standing on the shoulders of giants for solving DDoS attack

Jair Santanna
University of Twente
j.j.santanna@utwente.nl

Koen van Hove
University of Twente
k.w.vanhove@student.utwente.nl

ABSTRACT

.

1 INTRODUCTION

Distributed Denial of Service (DDoS) attacks []

Why standing on the shoulders of gigants: existing solutions and stakeholders. Not reinvent the wheel but adding

The solutions against DDoS attacks are based on technologies (hardware and software) that monitors the network traffic and react upon a predefined event. There are mainly two types of events. The first is when occurs a match between the incoming network traffic (packet or flow) and a predefined rule or signature, called rule/signature-based Intrusion Prevention System (IPS). The second type of event is when the network traffic has an abnormal behaviour based on a predefined profile. This latter type of technology is called anomaly-based IPS.

An ideal scenario for the mitigation of a DDoS attack would be a distributed solution with a r connected to an anomaly-based IPS.

Different types of attacks requires different types of mitigation strategy.

The difference between an intrusion detection systems (IDS) and an is that the latter can launch an action after a detection event, while the former records an event after the detection. Sometimes these terms are interchangeable by the community.

There are two types of IDS/IPS: signature and anomaly-based. While the signature-based IPS is

For us, the DEFINITION of a DDoS fingerprint is an useful comprehensive summary of the characteristics of a single vector of a DDoS attack extracted from a network measurement.

*misunderstanding digital fingerprint, signature, rule, pattern, characteristics, profile

Law enforcement agencies do not like to call *digital fingerprint* because in their field a fingerprint leads to an unique individuo.

THE PROBLEM can be summarized as: (1) a lack of standard for fingerprinting DDoS attacks; (2) lack of an updated database with fingerprints; (3) lack of functions to convert DDoS fingerprints into applicable detection and mitigation rules;

Rule-based mitigation solutions (*e.g.,* firewall, BGP flowspec,) are an particular case of signature-based IDS.

Types of network measurements are: (1) packet-based (*i.e.,* pcap and pcapng), (2) (net)flow-based (*e.g.,* v5, v9, IPFIX), (3) sflow, and (3) log-based.

USAGE of the fingerprint: (1) improve existing detection and mitigation solutions, (2) attribution, (4) correlation among DDoS attacks and correclaation with other types of cyber threats, (5) accounting for attacks, and (6) notification to CSIRT/CERT's for cleaning misused machines, (3) reproduction of attacks (usually for academic purpose)

Detection and mitigation tools for DDoS attacks: (1) BGP Flowspec, (2) BRO, (3) SURICATA, (4) SNORT, (5) ModSecurity, (6) eBPF, (7) IPtables.

Unicast addresses

How much is needed to be collected (time, packets, flows)? How much is the impact of a mitigation rule (considering the ongoing traffic)? How to indicate spoofed IP presence?

We intend to solve the problem that DDoS attacks pose by ...

DDoS attacks are not likely to stop happening!

2 FINGERPRINT: CONCEPTS & CONTEXT

There are several words used by the academic and security community for defining DDoS attack fingerprint. The words are DDoS 'characteristics', 'fingerprint', 'profile', 'pattern', 'signature', and 'rule'. Oxford dictionary defines these words as the following.

- **characteristics**: "a feature or quality belonging typically to a person, place, or thing and serving to identify them";
- **fingerprint**: "a distinctive identifying characteristic";
- **profile**: "a graphical or other representation of information relating to particular characteristics of something, recorded in quantified form";
- **pattern**: "a regular and intelligible form or sequence discernible in the way in which something happens or is done";

[*] This document was not peer-reviewed.

- **signature**: “a distinctive pattern, product, or characteristic by which someone or something can be identified”;
- **rule**: “a principle that operates within a particular sphere of knowledge, describing or prescribing what is possible or allowable”;

3 OUR DDOS ATTACK FINGERPRINT

Requirements:

- .

4 THE DDOSDB

More than a database with DDoS attack fingerprints.

Requirements:

- flexible regarding the number and types of fields;
- flexible access control
- distributed fashion;
- enrich the fingerprint;
- facilitate queries;
- enable download of fingerprints and anonymized data;
- facilitate notification;
- distribute information;

5 USAGE OF DDOS FINGERPRINTS

6 CONCLUSION

DDoS attacks are not likely to stop occurring. However, we strongly believe that an community effort would extinguish the

REFERENCES

[1] Sally Floyd and Van Jacobson. Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on Networking (ToN)*, 1 (4):397–413, 1993.