DDoS Security Metrics

Alexandru Babeanu
Samarjeet Patil
Thanasis Pagiavlas

September 24, 2018

1 What security issue does the data speak to ?

A denial-of-service (DoS) attack is a cyber-attack in which a malicious party seeks to make a machine or network resource unavailable to its users by disrupting services of a host connected to the Internet. This is usually accomplished by spamming the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS), the attackers make use of multiple devices, usually machines infected with malware throughout the network. This type of attack is harder to stop because the requests originate from multiple sources.

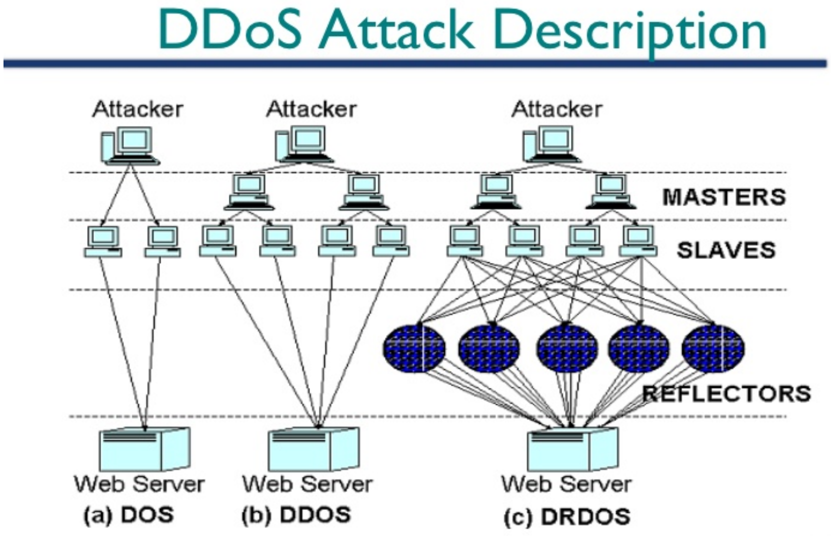

Figure 1: Distributed Denial-of-Service attack

By hindering the clients' access to a resource, these attacks can have the following negative effects on the company providing said resource:

1. Loss of financial income
2. Loss of customers
3. Reputation damage

The provided dataset contains information about different DDoS attacks that were detected by honeypot systems in different locations around the world over a period of two years (01-Jan-2014 to 31-Dec-2015). We decided to focus our selection of security metrics as well as our data exploration on the Amazon Web Services hosting platform. This is done because this business is a known high priority target for attackers and we can assume that the targeted servers had similar capabilities and levels of security.

2 What would be the ideal metrics for security decision makers ?

1. **Asset identification and evaluation** - the organization should identify and have a clear knowledge about their assets and clearly categorize them according to their type and value by estimating the importance of the asset for the organization's process.
2. **Asset capacity** - the capacity of the network resource after being attacked or compromised.
3. **Asset vulnerability** - the organization should have clear view of the weaknesses of an asset, which could potentially be exploited by attackers.
4. **Number of "killchains"** - the count of potential attack paths in a network an attacker can use, based on the analysis of previous attacks and self-assessment of the network.
5. **Average length of the "killchain"** - the average effort to penetrate a network or compromise a system/service.
6. **Attacked asset percentage** - the percentage of assets in a network affected by the attack.
7. **Network/service resilience** - the percentage of compromised systems /services that can be replaced or recovered after the attack by backup or alternative service.

3 What are the metrics that exist in practice ?

1. **Throughput** - the rate of sending and receiving data by a network and a way to measure the communication capacity of a system. It is measured by the number of bits passed per second.
2. **Response time** - the elapsed time between the end of an inquiry to a system and the beginning of the response.
3. **Number of active connections** - the amount of clients that have completed the three-way handshake and started sending data, i.e. the number of live connections interacting with the server.
4. **Request dropout** - the amount of requests being dropped out because of the attack
5. **Percentage link utilization** - the percentage of bandwidth being used for goodput, where goodput is defined as the number of bits per second of legitimate traffic being handled by the server.
6. **Normal packet survival ratio** - the ratio of legitimate packets to total packets received by the targeted server. This measures the impact of an attack as a percentage of legitimate packets received during the attack.

4 A definition of the metrics you can design from the dataset.

- **Number of attacks per location** - will give the priority of various targets.
- **The service used for the attack** - which services (chg, dns, ntp, snmp or ssdp) are preferred by the attackers.
- **Attack duration** - the time the target was under attack.
- **Number of attack packets** - the amount of malicious data used in the attack. It can be used to asses the magnitude of past attacks and allocate resources accordingly.
- **Rate of attack packets** - approximately equal to the the number of packets divided by the attack duration. This could be used to measure the throughput if the packet size and the machine bandwidth were known.
- **The country of the targeted IP** - some countries may present a higher incentive for the attackers, and will therefore require a higher security level.

5 An evaluation of the the metrics you have defined.

When analysing the data, we group the attacks by their respective services. As shown in figure 2, the **dns** and **chg** services are more prone to attacks than the others, while very few attacks target the **snmp** service. This way, the company can prioritize the purchase or implementation of service-specific security measures.

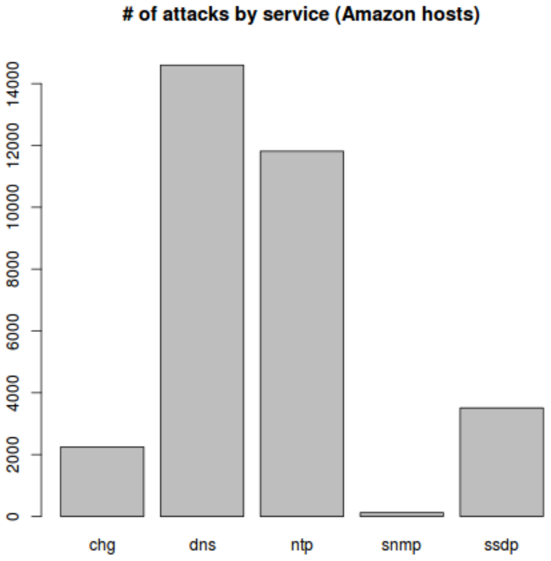

Figure 2: Number of attacks by service

The graphs in figures 3, 4, and 5, offer a statistical representation regarding the magnitude of the attacks in terms of number of packets, attack duration, and the frequency of attack packets. These statistics can be useful when measuring the security level of a service by assessing what attacks would be able to compromise it. The risk of the service being disrupted by a DDoS attack can therefore be determined b how common these attacks are. These graphs exclude outliers, which represent attacks of much higher magnitudes than the plotted ones. Taking them into account when allocating resources to protect the service against DDoS attacks would raise the level of security, but would also lead to inefficient spending since they are uncommon.

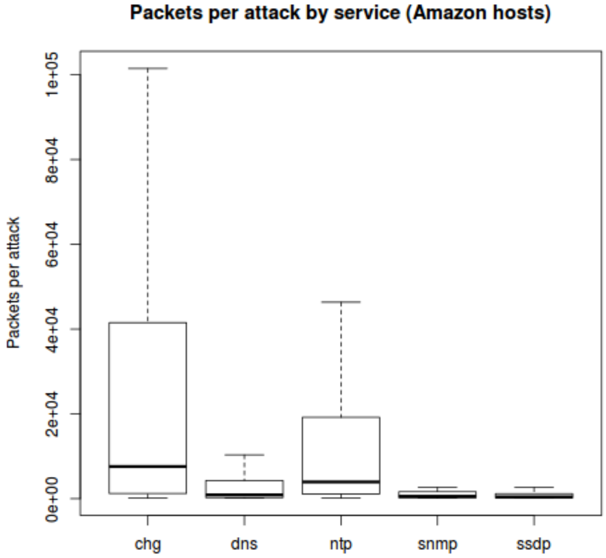

Figure 3: Number of packets per attack by service

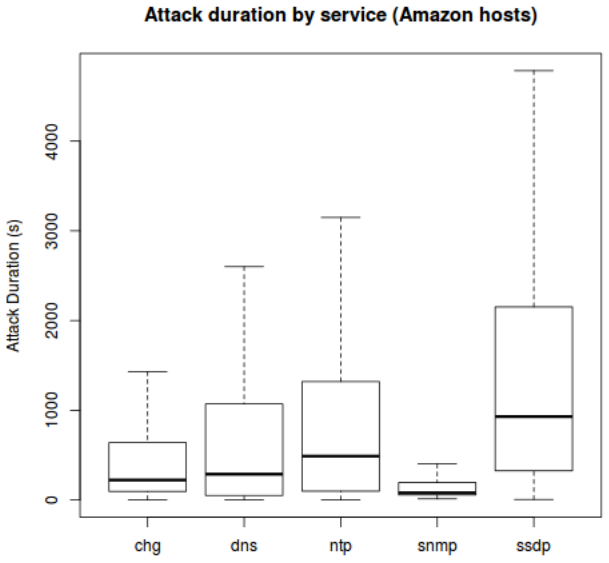

Figure 4: Attack duration by service

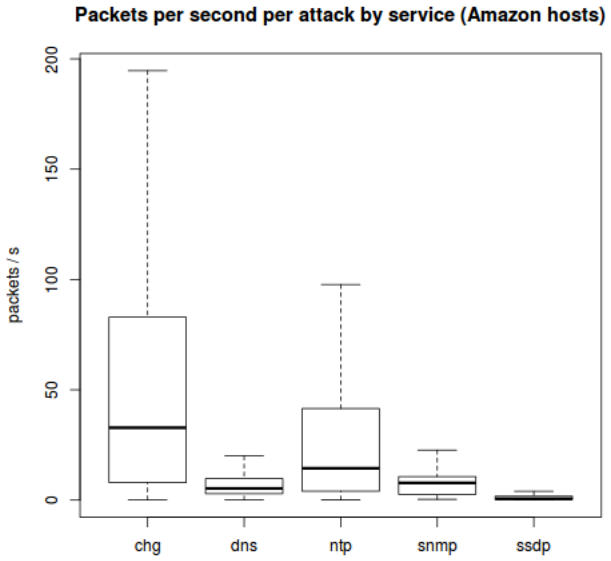

Figure 5: Rate of attack packets by service

Figures 6 and 7 show the disparity in the number of attacks between different countries. This could indicate which countries present a higher priority for the attackers, and therefore a higher risk for the service provider, but the data needs to normalized with the amount of services hosted in each country.

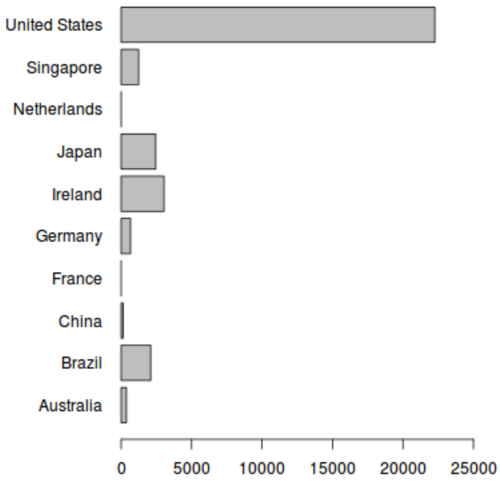

Figure 6: Number of attacks by country

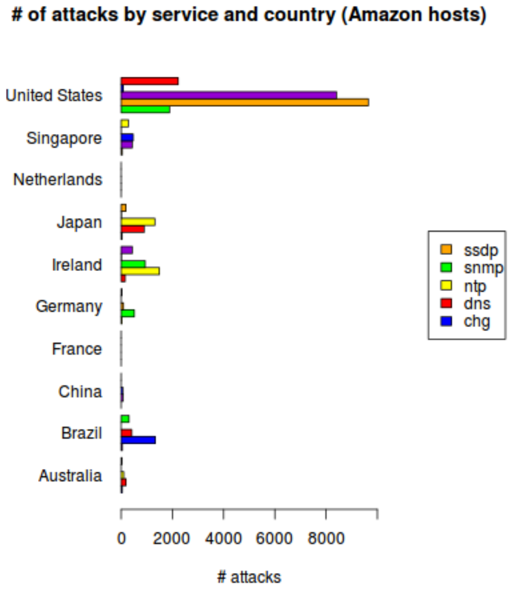

Figure 7: Number of attacks by country and service

References

[1] Monica Sachdeva, Gurvinder Singh, Krishan Kumar and Kuldip Singh: "Measuring impact of DDoS effects on Web Services". Journal of Information Assurance and Security 5 (2010), p.392-400.

[2] Wayne Boyer and Miles McQueen: "Ideal Based Cyber Security Technical Metrics for Control Systems". 2^{nd} International Workshop on Critical Information Infrastructures Security (October 2007).

[3] Y. Cheng, J. Deng, J. Li, S. DeLoach, A. Singhal, and X. Ou: "Metrics of security". In Cyber Defense and Situational Awareness. Vol. 62. (2014)