Protecting against DNS Reflection
Attacks with Bloom Filters

Sebastiano Di Paola and Dario Lombardo
Telecom Italia S.p.A., Via Reiss Romoli 274, 10148 Torino, Italy
{sebastiano.dipaola,dario.lombardo}@telecomitalia.it

Abstract. Nowadays the DNS protocol is under the attention of the security community for its lack of security and for the flaws found in the last few years. In the Internet scenario, the reflection/amplification is the most common and nasty attack that requires very powerful and expensive hardware to be protected from. In this paper we propose a robust countermeasure against this type of threats based on Bloom filters. The proposed method is fast and not too eager of resources, and has a very low error rate, blocking 99.9% of attack packets. The mechanism has been implemented within a project by Telecom Italia S.p.A., named jdshape, based on Juniper Networks® SDK.

1 Introduction

The DNS protocol is one of the most important protocol of the TCP/IP suite. It is used to convert names into numeric addresses and is the base of any high-level service. Due to its early birth it lacks the basic security features that a modern protocol has. Many attacks have been documented against this protocol: in this paper one will be analyzed in deep, the DNS reflection attack. It is a DoS attack where the victim is flooded with DNS responses. The paper will describe a defense approach based on Bloom filters: they are used to store the observed DNS queries, and checked against a response. This method allows to couple a query and a response that belong to the same DNS transaction. All the responses that don’t have a coupled query are part of the attack. The Bloom filter approach is fast and effective despite of an error rate due to its statistic origin. The filter is a trade-off between the desired precision (error rate and packet rate) and the memory consumption. We used two filters of about 8.22 MB that can store 3 seconds of traffic at a 800000 pkts/s each. The two filters are needed to have a lock-free implementation that runs on an expansion card of a Juniper router (MS-PIC) and are swapped every predefined time-slot. The proposal has been developed and tested in a simulated environment to verify its behavior. It has been also tested running on the router in lab with both test and real traffic. It has been demonstrated to be effective with respect to the preset error rate (0.1%).

The remainder of the paper is organized as follows. Section 2 describes major DNS protocol security concerns. In section 3 reflection attack are outlined.
Section 4 provides an high level overview of Bloom Filter data structure. In section 5 an exhaustive approach to solve the problem is analyzed and in section 6 our solution is proposed. In section 7 real world implementation design parameters are evaluated and chosen. In section 8 performances and experimental result are reported and finally in section 9 conclusions and possible improvements end the paper.

2 Security Concerns in the Domain Name System

DNS (Domain Name System) is the protocol used to convert symbolic names (such as www.google.com) into IP addresses (such as 72.14.255.104). It is an ancient protocol, ancient as the Internet itself, and it was developed when protocols were designed without security concerns.

It is the prototype of the insecure protocol:

- it’s based on IP than is connection-less and not authenticated
- the most common transport for DNS is UDP, that is connection-less (while TCP is connection-oriented), so easier to attack
- it is unauthenticated itself, allowing easy information forging.

Despite its insecurity, this protocol, as IP and the others belonging to the TCP/IP suite, is commonly used in modern networks. In the plethora of the network protocols, IP has the role of the “center of the hourglass”. This means that there are many layer-2 protocols, and many layer 4-7 protocols, but IP is the only layer-3 used, so it is a sort of bottleneck (as in the hourglass). The DNS has a similar role in the services context. If a public service is stopped, others can continue to work (e.g. if the Web is stopped for some reason, the email service still works). If the DNS is stopped all the other services are stopped too, because they depend on it: web addresses cannot be resolved, e-mails cannot be delivered, generally speaking servers can’t be reached. This is due to the wide use of the symbolic names instead of IP addresses. It is not forbidden to use IP addresses instead of names, but it’s not done because of the possibility of dynamic changes in that association. Moreover non-technical users have no idea of what an IP address is, so they use just symbolic names.

In summary our proposal is an application of the Bloom filters [6] to mitigate DNS DoS attacks, and has been implemented on a Juniper router using Juniper SDK [16]. The solution was designed taking into account both development platform functionalities and real networks measures (as packet rate, packet sizes, latency, and so on).

3 DNS Reflection Attacks

Due to its lack of security, attacks based on IP spoofing are widely used against DNS infrastructures. The most common one is called the reflection attack (see [1],

1 DNSSEC digital signature should solve the problem.