Chapter 2
IP Layer Client Puzzles: A Cryptographic Defense against DDoS Attack

Genti Daci
Polytechnic University of Tirana, Albania

Rezarta Jaupi
Polytechnic University of Tirana, Albania

ABSTRACT

It is very common today that many business models are based on offering on-line services. Profitability and efficiency of this business model relies on a secure and undisturbed Internet infrastructure. Unfortunately, services offered on Internet infrastructure, being an Open and yet untrusted network, are very often targets of Denial-of-Service and Distributed Denial-of-Service attacks. These attacks are today a serious problem for on-line services offered by many business models. Preventing or minimizing DoS and DDoS is a difficult task which could serve to many on-line service offering business models to provide quality services to their clients. The main objective of this chapter is to present the Client Puzzle mechanism as a new method designed to defend business networks and their on-line services from these attacks. By using a client puzzle protocol on the IP level, the client is forced to solve a cryptographic puzzle before it can request any operation from a server, thus creating computational efforts and delays to illegitimate attackers and minimizing their attack effects on services. In this chapter, the authors show that chained puzzle protocol reduces the network and insfrastructure overhead because the servers do not have to generate puzzles on a per-packet basis. In addition, the chapter analyzes the effectiveness and some limitations of chained puzzles method with regards to minimizing DDoS attacks and outlines a general approach for addressing the identified limitations. At the last part, the authors propose a solution based on the general principle that under attack legitimate clients should be willing to experience some degradation in their performance in order to obtain the requested service.

DOI: 10.4018/978-1-4666-3946-1.ch002

1. INTRODUCTION

To the present day, in every business model, the Internet technology and structure is used successfully to increase communication efficiency, lower the costs of work processes, and bring new revenue streams. Internet, being an open and untrusted network, brings to business more complex operations including consequences and concerns in areas such as privacy, identity and security. In recent years, many on-line offering services business models suffered from Denial-of-Service (DoS) attacks and Distributed DoS (DDoS) attacks, which have become a serious problem for every business model which uses Internet to provide on-line services. In recent years, several online companies such as eBay, Amazon.com, CNN.com, and Yahoo were all affected by large-scale DDoS attacks. During this type of attack, their Websites were unreachable to many Internet users, resulting in severe financial losses, in addition to the many unsatisfied customers. Also, several root Domain Name System (DNS) servers which provide vital services to Internet community were not able to function properly for some time because have been targeted by DDoS type attacks.

The DoS/DDoS resource depletion attacks are as difficult to prevent, as they are easy to mount. One method of minimizing DDoS attacks effects is to implement a client puzzle protocol. The principle of this protocol is that a client, requesting a given service, should first solve puzzle before the server's resources are compromised (Aura, Nikander, & Leiwo, 2000). A number of practical implementations of client puzzle protocols reported positive results in preventing and minimizing DoS attacks (Dean & Stubblefield, 2001; Wang & Reiter, 2003).

In our experiments, we choose to implement the protocol in the IP layer as it is the lowest layer on which an Internet DDoS attack can be mounted. The IP layer mechanism will protect against flooding attacks at the IP layer, and it will provide protection against attacks at higher layers because all traffic must pass through the IP layer. The disadvantage of an IP-layer mechanism is that reduces the routing capacity of a network due to an increase in the per-packet processing time at the router. Instead of using per-packet operations, we propose to use IP-Streams, which are composed by same source/destination packet flowing like a stream on a router.

The following sections of the paper outlines as follow: section 2 describes the client puzzles protocol. Section 3 describes the design of chained puzzle, including the modification of IP layer, while section 4 analyses the protocol effectiveness and limitations. Section 5 presents conclusions and section 6 recommends the future work.

2. CLIENT PUZZLE PROTOCOL

A cryptographic puzzle is a cryptogram that is encrypted with a strong encryption function and a part of the solution is revealed to the solver. Thus, a puzzle would consist of a plaintext, a ciphertext, and a part of the key. The remaining unknown bits of the key would be the solution to the puzzle. In order for the solver to find the solution to the puzzle, a brute-force approach must be applied that tries random values for the remaining bits of the key and then checks the value of the ciphertext to determine if the correct key has been found.

The properties of client puzzle (Aura, Nikander, & Leiwo, 2000) are:

1. Creating a puzzle and verifying the solution is inexpensive for the server.
2. The cost of solving the puzzle is easy to adjust from zero to impossible.
3. The puzzle can be solved on most types of client hardware.
4. While the client is solving the puzzle, the server does not need to store the solution or other client specific data.
5. The puzzle should be solved in a predetermined amount of time.
6. Puzzle solution must be unique.