

Research Article

A Client Bootstrapping Protocol for DoS Attack Mitigation on Entry Point Services in the Cloud

Hussain M. J. Almohri¹, Mohammad Almutawa¹, Mahmoud Alawadh¹, and Karim Elish²

¹Department of Computer Science, Kuwait University, Kuwait City, Kuwait

²Department of Computer Science, Florida Polytechnic University, Lakeland, USA

Correspondence should be addressed to Hussain M. J. Almohri; almohri@cs.ku.edu.kw

DOI: 10.1155/2020/1234567

Academic Editor: Mamoun Alazab

Copyright © 2020 Hussain M. J. Almohri et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper presents a client bootstrapping protocol for proxy-based moving target defense system for the cloud. The protocol establishes the identity of prospective clients who intend to connect to web services behind obscure proxy servers in a cloud-based network. In client bootstrapping, a set of initial line of defense services receive new client requests, execute an algorithm to assign them to a proxy server, and reply back with the address of the chosen proxy server. The bootstrapping protocol only reveals one proxy address to each client, maintaining the obscurity of the addresses for other proxy servers. Hiding the addresses of proxy servers aims to lower the likelihood that a proxy server becomes the victim of a denial-of-service (DoS) attack. Existing works address this problem by requiring the solution of computationally intensive puzzles from prospective clients. This solution slows the progression of attacks as well as new clients. This paper presents an alternative idea by observing that limited capacity of handling initial network requests is the primary cause of denial-of-service attacks. Thus, the suggested alternative is to utilize cost-effective high-capacity networks to handle client bootstrapping, thus thwarting attacks on the initial line of defense. The prototype implementation of the protocol using Google's Firebase demonstrates the proof of concept for web services that receive network requests from clients on mobile devices.

1. Introduction

Denial-of-service (DoS) attacks on web services in cloud-based virtual networks continue to threaten small or medium-sized networks by exhausting the available memory and computation power of the hosting machines. Small or medium-sized networks are particularly vulnerable because of the budget limitation, severely restricting the computation capacity of the machines that serve external clients. Thus, attackers can win the resource race against the target network by using simple denial-of-service vulnerabilities such as the ones in prominent web server software. A growing interest is in the use of moving target defense (MTD) strategy against DoS attacks on vulnerable networks. In this case, target services dynamically change IP addresses and introduce diversity in the hosting machines to gain the advantage of time. The moving target defense model benefits

from the elasticity of the cloud, which allows for swift and dynamic responses to attacks, using programmable firewall rules and network interfaces applied to elastic computing resources.

Moving target defense provides a strong defense strategy against DoS attacks without focusing on the details of specific network service vulnerabilities that attackers exploit.

The central idea is to increase the DoS attacker's effort in finding and attacking large services in the network. Formally, suppose that a function search (S, N) is used by the denial-of-service attacker, given a possible search space S to find the target addresses in a network N . With no moving target defense, assume that search (S, N) terminates with the complexity $O(f(n))$, for a typically linear $f(n)$ number of possible addresses (usually requiring a Nmap scan [1]).

The key to maximizing the attacker's search effort is in randomizing the network address search space. Thus,

