Accepted Manuscript

Title: *ArOMA*: an SDN based autonomic DDoS mitigation framework

Author: Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, Hervé Debar

PII: S0167-4048(17)30149-9
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.07.008
Reference: COSE 1174

To appear in: *Computers & Security*

Received date: 15-11-2016
Revised date: 7-6-2017
Accepted date: 9-7-2017

Please cite this article as: Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, Hervé Debar, *ArOMA*: an SDN based autonomic DDoS mitigation framework, *Computers & Security* (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.07.008.

ArOMA: an SDN based Autonomic DDoS Mitigation Framework

Rishikesh Sahay[a,c], Gregory Blanc[a,c], Zonghua Zhang[b,c], Hervé Debar[a,c]

[a]*Télécom SudParis, Institut Mines-Télécom, France*

[b]*IMT Lille Douai, Institut Mines-Télécom, France*

[c]*CNRS UMR 5157 SAMOVAR, France*

Abstract

Distributed Denial of Service (DDoS) attacks have been the plague of the Internet for more than two decades, despite the tremendous and continuous efforts from both academia and industry to counter them. The lessons learned from the past DDoS mitigation designs indicate that the heavy reliance on additional software modules and dedicated hardware devices seriously impede their widespread deployment. This paper proposes an autonomic DDoS defense framework, called *ArOMA*, that leverages the programmability and centralized manageability features of Software Defined Networking (SDN) paradigm. Specifically, *ArOMA* can systematically bridge the gaps between different security functions, ranging from traffic monitoring to anomaly detection to mitigation, while sparing human operators from non-trivial interventions. It also facilitates the collaborations between ISPs and their customers on DDoS mitigation by logically distributing the essential security functions, allowing the ISP to handle DDoS traffic based on the requests of its customers. Our experimental results demonstrate that, in the face of DDoS flooding attacks, *ArOMA* can effectively maintain the performance of video streams at a satisfactory level.

Keywords: DDoS attacks, DDoS mitigation, Software Defined Networking, Anomaly detection, Security policy

1. Introduction

Distributed Denial of Service (DDoS) attacks have continuously occurred on the Internet for most of the past three decades, attracting tremendous research efforts from both academia and industry. In particular, flooding-based attacks, such as the ones manipulating UDP, TCP SYN or ICMP packets, are the most prevalent attack variants on the Internet [3]. As a matter of

Email addresses: rishikesh.sahay@telecom-sudparis.eu (Rishikesh Sahay), gregory.blanc@telecom-sudparis.eu (Gregory Blanc), zonghua.zhang@imt-lille-douai.fr (Zonghua Zhang), herve.debar@telecom-sudparis.eu (Hervé Debar)