Accepted Manuscript

Measuring the efficiency of SDN mitigations against attacks on computer infrastructures

R. Koning, B. de Graaff, G. Polevoy, R. Meijer, C. de Laat, P. Grosso

PII: S0167-739X(18)30225-5
DOI: https://doi.org/10.1016/j.future.2018.08.011
Reference: FUTURE 4395

To appear in: *Future Generation Computer Systems*

Received date : 30 January 2018
Revised date : 13 June 2018
Accepted date : 7 August 2018

Please cite this article as: R. Koning, et al., Measuring the efficiency of SDN mitigations against attacks on computer infrastructures, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.08.011

Measuring the Efficiency of SDN Mitigations Against Attacks on Computer Infrastructures

R. Koning[a], B. de Graaff[a], G. Polevoy[a], R. Meijer[a], C. de Laat[a], P. Grosso[a]

[a] System and Network Engineering group (SNE) University of Amsterdam, The Netherlands

Abstract

Software Defined Networks (SDN) and Network Function Virtualisation (NFV) provide the basis for autonomous response and mitigation against attacks on networked computer infrastructures. We propose a new framework that uses SDNs and NFV to achieve this goal: Secure Autonomous Response Network (SARNET). In a SARNET, an agent running a control loop constantly assesses the security state of the network by means of observables. The agent reacts to and resolves security problems, while learning from its previous decisions. Two main metrics govern the decision process in a SARNET: *impact* and *efficiency*; these metrics can be used to compare and evaluate countermeasures and are the building blocks for self-learning SARNETs that exhibit autonomous response. In this paper we present the software implementation of the SARNET framework, evaluate it in a real-life network and discuss the tradeoffs between parameters used by the SARNET agent and the efficiency of its actions.

Keywords: Software Defined Networks, Network Function Virtualization, cyber attacks, cyber security, defense efficiency, overlay networks

1. Introduction

Crime directed to network infrastructures and network protocols is increasing [1]. The economic and societal consequences of such attacks are reaching front pages in the news leading society to question their trust in the Internet [2, 3, 4]. Not surprisingly, an entire industry emerged to create an ecosystem of tools and devices that are marketed to prevent, stop, or to mitigate the negative effects of such malicious behaviour. We can install off the shelf Intrusion Detection Systems (IDS) to identify the existence of attacks and we can deploy specialised firewalls to prevent malicious traffic from entering a specific network domain.

A major development in the networking landscape of the past years is the emergence of Software Defined Networks (SDNs). SDNs allow computer networks to be controlled from one or more software controllers using a common interface. These controllers have the ability to monitor and dynamically reconfigure the network, redirect traffic flows and adapt the network to the situation on demand. The question that then arises naturally is whether SDNs can provide novel methods to counteract attacks.

Email addresses: r.koning@uva.nl (R. Koning), b.degraaff@uva.nl (B. de Graaff), g.polevoy@uva.nl (G. Polevoy), r.j.meijer@uva.nl (R. Meijer), delaat@uva.nl (C. de Laat), p.grosso@uva.nl (P. Grosso)