Accepted Manuscript

Title: Saving energy in aggressive intrusion detection through dynamic latency sensitivity recognition

Author: Sherenaz Al-Haj Baddar, Alessio Merlo, Mauro Migliardi, Francesco Palmieri

PII: S0167-4048(17)30263-8
DOI: https://doi.org/10.1016/j.cose.2017.12.003
Reference: COSE 1251

To appear in: *Computers & Security*

Please cite this article as: Sherenaz Al-Haj Baddar, Alessio Merlo, Mauro Migliardi, Francesco Palmieri, Saving energy in aggressive intrusion detection through dynamic latency sensitivity recognition, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.12.003.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Saving Energy in Aggressive Intrusion Detection Through Dynamic Latency Sensitivity Recognition

Sherenaz Al-Haj Baddar[a], Alessio Merlo[b], Mauro Migliardi[c], Francesco Palmieri[d]

[a]*The University of Jordan, Amman, Jordan.*

s.baddar@ju.edu.jo

[b]*DIBRIS, Università degli Studi di Genova, Italy*

alessio@dibris.unige.it

[c]*DEI, University of Padova, Italy*

mauro.migliardi@unipd.it

[d]*Department of Computer Science, University of Salerno, Italy.*

fpalmieri@unisa.it

Highlights

- Selective distributed routing and intrusion detection based on dynamic statistical analysis
- Adaptively organizes the intrusion detection activities
- Suppresses at the network ingress the undesired components of latency-insensitive traffic
- Distributes over multiple nodes the security check for latency sensitive flows
- Saves energy without affecting latency-sensitive traffic by introducing processing delays

Abstract

In an always connected world, cyber-attacks and computer security breaches can produce significant financial damages as well as introduce new risks and menaces in everyday's life. As a consequence, more and more sophisticated packet screening/filtering solutions are deployed everywhere, typically on network border devices, in order to sanitize Internet traffic. Despite the obvious benefits associated to the proactive detection of security threats, these devices, by performing deep packet inspection and inline analysis, may both affect latency-sensitive traffic introducing non-negligible delays, and increase the energy demand at the network element level. Starting from these considerations, we present a selective routing and intrusion detection technique based on dynamic statistical analysis. Our technique separates latency-sensitive traffic from latency-insensitive one and adaptively organizes the intrusion detection activities over multiple nodes. This allows suppressing directly at the network ingress, when possible, all the undesired components of latency-insensitive traffic and distributing on the innermost nodes the

Accepted Manuscript

Download English Version:

https://daneshyari.com/en/article/6883943

Download Persian Version:

https://daneshyari.com/article/6883943

Daneshyari.com