Using a Control Theoretic Load Balancer for Efficient Attack Traffic Analysis and Defense on Virtualized Infrastructure

Nabeel Akhtar* Marzieh Babaieanjelodar* Ibrahim Matta* Yaqoing Liu*
*Boston University, Clarkson University

Abstract

- Resources are elastically managed using Software Defined Networking (SDN), Network Function Virtualization (NFV) and Control theory
- Control theory (Pl controller), along with SDN, is used to balance load across different VNF instances running Snort-IDS
- RINA [1] management architecture is used to monitor VNF instances over the GENI testbed
- A generalized framework using Attack Analyzer is used to analyze different types of attacks
- Attacks are detected faster with load balancer

What is RINA? [1]

- RINA: Recursive InterNetwork Architecture
- A clean-slate network architecture
- Based on the fundamental principle that networking is Inter-Process Communication (IPC) and only IPC
- Distributed IPC Facility (DIF): a collection of distributed IPC processes with shared states
- Distributed Application Facility (DAF): a set of application processes cooperating to perform a certain function
- Two design principles: (i) divide and conquer (recursion), and (ii) separation of mechanisms and policies

Experiment over GENI

- Experimental setup (Fig. 2):
  - two VNF instances running Snort IDS (VNF1 and VNF2)
  - one OVS switch and one open-flow controller
  - two sources (S1 and S2) and one destination (destination)
- Traffic is sent to Snort-IDS running on VNF1 or VNF2
- RINA management architecture is used to send load and Snort-IDS alerts of VNF instances to Controller
- Load Balancer determines the fraction of traffic to divert from VNF1 to VNF2 and updates the OVS controller
- Attack Analyzer processes Snort-IDS alerts and updates the attacker list for the OVS controller
- OVS controller updates OpenFlow rules on the OVS switch based on Load Balancer and Attack Analyzer input

Control Theoretic Load Balancer

- Pl controller (Fig. 3):
  \[ x(t) = \max\{0, \min[1, x(t - 1) + K \frac{L(t)}{T} - 1]\} \]
  \(x(t)\): ratio of traffic diverted to VNF2 at time \(t\)
  \(L(t)\): load on VNF1
  \(T\): target load on VNF1

Results

- On average, attacks are stopped significantly faster under load balancer
- Attacks sometimes go undetected without load balancer

Fig. 4: Port Scanning Attack (a) 2.6 seconds with load-balancer (b) 5.4 seconds without load-balancer

References