Frequency-Minimal Moving Target Defense using Software-Defined Networking

[1]Saptarshi Debroy , [1]Prasad Calyam, [1]Minh Nguyen, [2]Allen Stage, [3]Vladimir Georgiev
[1] Department of Computer Science, University of Missouri, MO
[2] Humboldt State University, CA
[3] Southeast Missouri State University, MO
Point-of-contact: calyamp@missouri.edu
July 2015

Overview

- Cyber attacks such as DDoS are on the rise

- Need for intelligent counter-strategies to protect critical cloud-hosted applications

- Challenge is to minimize cloud resource overhead and loss of availability to thwart attackers

- Lack of adequate protection against attacks can impact reputation and cause millions of $$ in damages to applications in healthcare and finance

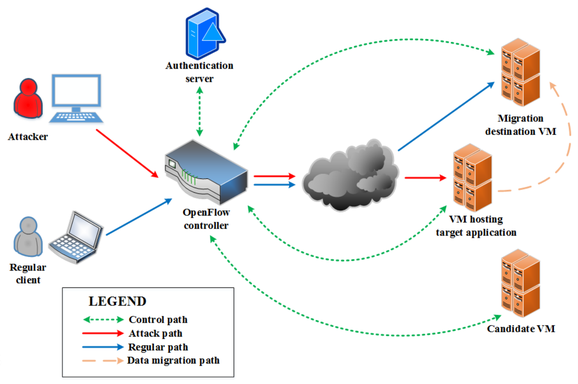

Figure 1 : System and Attack Model

Novel MTD Architecture within a Cloud Platform

- We propose an intelligent MTD based VM migration technique that can proactively and reactively migrate VMs using SDN to defend against DDoS attacks

- Novelty of our technique

- Our SDN-enabled migration sheme performs dynamic VM migration, whereas existing works resorts to IP address shuffling

- Our scheme is both proactive and reactive unlike most existing works which are purely reactive

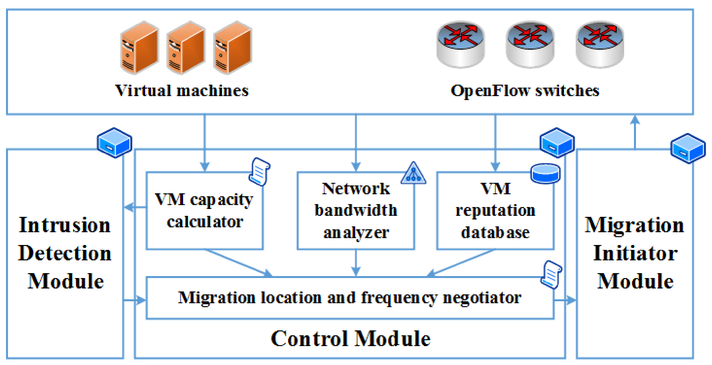

Figure 2: Software Architecture of our proposed MTD Controller

- Our scheme is adaptive to attack probability and attack budget, whereas existing schemes use a migration frequency which is static

- Our scheme considers heterogeneous VM pool, whereas existing works assume a homogeneous VM pool

- There are two fundamental questions that we address with our technique:
  - What is the optimal *frequency* of proactive migration that protects the VM without consuming excessive resources or causing management overhead?
  - What is the preferred VM *location* for migration using SDN that does not affect application performance?

MTD Optimization based on Attack Probability

Objective I*:* Finding optimal frequency of migration that is frequent enough to avoid vulnerability, yet not too often to waste cloud resources

$$minimize\left(\text{Prob}\{z \leq T_m\}\right)$$

where $\text{Prob}\{z \leq T_m\} = \begin{cases} \frac{\mu_i(e^{-\lambda_a T_m}-1)+\lambda_a(1-e^{-\mu_i T_m})}{\lambda_a-\mu_i} & \forall\ \lambda_a \neq \mu_i \\ 1-e^{-\lambda_a T_m}(\lambda_a T_m+1) & \text{otherwise} \end{cases}$

Objective II*:* Finding ideal location for migration based on:
(a) candidate destination VM capacity, (b) network bandwidth between candidate destination VM and VM hosting target application, and (c) VM reputation in terms of history for previous cyber attacks

$$maximize(\mathcal{S}_p^v)$$

where $\mathcal{S}_p^v = w_c \times C_p + w_b \times B_p^v + w_r \times R_p^j$

and $R_p^j = 1 - \frac{\alpha_p^j + \frac{\beta_p^j}{\beta_p^j+\gamma_p^j}}{\alpha_p^j+\beta_p^j+\gamma_p^j} \quad \forall\ p \in V$

Experimental Testbed Setup

- Target Application: Just-in-time news feeds

- Application users are a prime target for cyber attacks, and their loss of service availability is loss of $$

- NSF GENI Cloud Testbed

- VM file migration module that is based on RSync and implements MTD controller decisions

- Our GENI experiment involved testing the optimal frequency of migration with our scheme (FM-MTD), in comparison with a static migration scheme that assumes homogeneous VM pool (SH-MTD)

- We considered attack budgets of 1/10 and 1/100, and attack pattern following exponential distribution

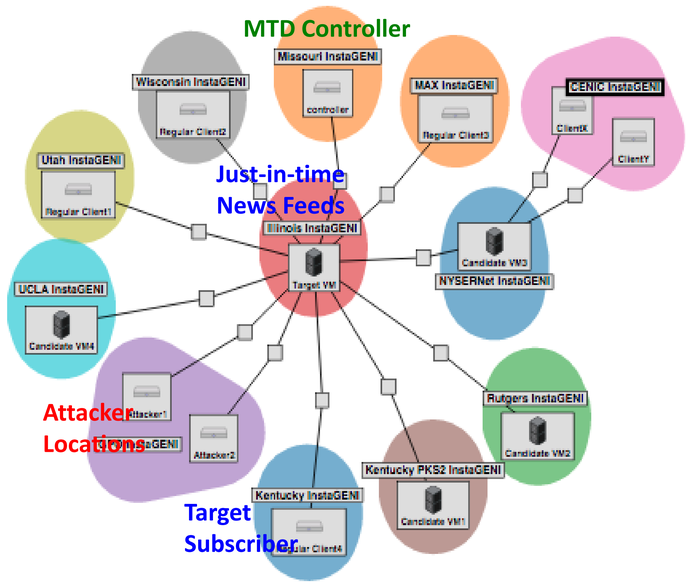

Figure 3: GENI Cloud Testbed for MTD protection of just-in-time news feeds application

Experiment Results

- Location Selection Comparison:
  - Ideal destination selection with FM-MTD resulted in up to 4X faster application response time compared to SH-MTD

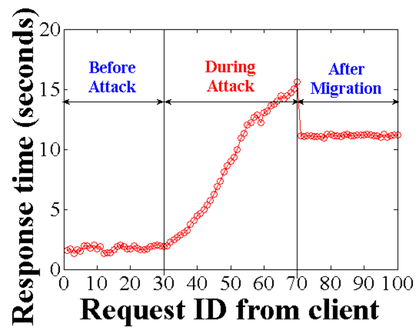

Figure 4: Location Selection Comparison Results: Response time with SH-MTD

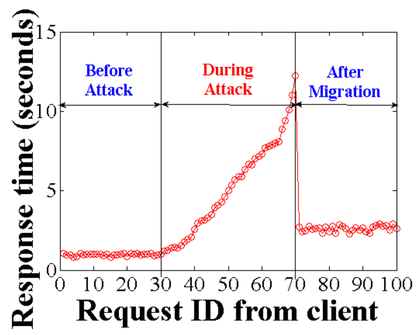

Figure 5: Location Selection Comparison Results: Response time with FM-MTD

- Optimal Frequency Comparison:
  - Optimal migration frequency with FM-MTD showed up to 50% lower attack probability compared to SH-MTD

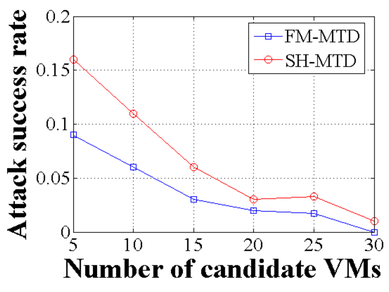

Figure 6: Frequency Setting Comparison Results: 1/10 attack budget

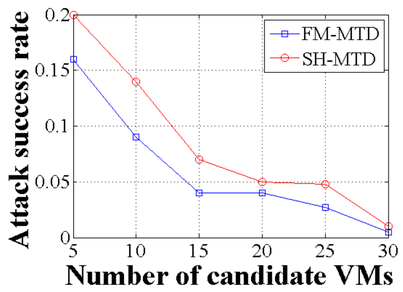

Figure 7: Frequency Setting Comparison Results: 1/100 attack budget

Our system of moving target defense will allow critical applications to be protected without a significant disruption for the user and proactively defends cloud providers against cyber attacks!

Acknowledgements

This material is based upon work supported by the National Science Foundation under Award No. CNS-1359125, Thomson Reuters and University of Missouri. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or Thomson Reuters.