Self Adaptation for Security Monitoring in IaaS clouds
Anna Giannakou, Louis Rilling, Christine Morin, Jean-Louis Pazat

To cite this version:
Self Adaptation for Security Monitoring in IaaS clouds
Anna Giannakou*, Louis Rilling∞, Christine Morin*, Jean-Louis Pazat*
* Inria, ∞DGA

Context: IaaS cloud environments. Frequent infrastructure-related changes:
- VM creation, migration, destruction
- Service addition or removal

Problem: Frequent changes make traditional security monitoring fail

Self adaptability: react to changes in virtual and physical infrastructures
Customization: allow tenants to request detection of specific types of attacks
Scalability: adapt to traffic load and changes in the size of the infrastructure
Cost minimization: for tenants and the provider

Adaptation probes: detect a change and reconfigure the components involved
Customized rules: include IDS rules targeting a tenant’s deployed services
New sensor deployment: rebalance traffic analysis when a local intrusion detection sensor is overloaded
Component sharing: tenants may share local IDS sensors

SAIDS architecture

1. Infrastructure monitoring probes notify the adaptation manager that a topology change occurs and relate the necessary information: VM id, VM IP, hostname of physical host
2. Adaptation manager decides which additional rules have to be activated in the local IDS (lIDS) responsible for the new host of the VM. Decision based on:
   - Deployed services (VM info)
   - Specific requests from tenants (SLA info)
3. The adaptation manager adapts the lIDS through remote execution of the adaptation driver

Goals
Evaluating the reconfiguration overhead & quality of detection

Technologies
- Cloud deployed with Openstack
- Inter VM communication through GRE tunnels on Open vSwitch

Scenario
- Load balanced setup representative of a production env.
- 3 interconnected VMs: web, mail, DNS services
- 2 lIDSs: one per virtual switch

Future Work
- Combine monitoring for provider and tenants
- Add other devices: collectors, aggregators
- Offer tenants partial control of the framework


Results

<table>
<thead>
<tr>
<th>Time in secs</th>
<th>Without adaptation</th>
<th>With adaptation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.7</td>
<td>2.3</td>
</tr>
<tr>
<td>1</td>
<td>2.1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Options