
Farhad Ahamed, Seyed Shahrestani and Bahman Javadi
School of Computing, Engineering and Mathematics
Western Sydney University, Australia
Security Concerns in Cloud Computing

- Confidentiality
- Availability
- Authentication
- Access control
- Integrity
- Scalability
- Side channels
- Virtualization leakage
- Fate sharing
- Malicious insider
- CSS
- Botnet
- Malware
- DDoS

Attack types – considering resource sharing issue
VM consolidation – What and why?

How do we ensure that our data in the Cloud is not living with a malicious neighbour?
Proposed Approaches

(a) The Compartment Isolation Approach of Secure Virtual Machine Consolidation
(b) Security Profiles for the Virtual Machines
Secure VM Consolidation

The Compartment Isolation Approach of Secure Virtual Machine Consolidation

Using the isolated compartment strategy; separation of VMs reduces the probability cross computer malware spreading.

\[ p(S) > p(S/r) \]
Secure VM Consolidation

Security Profiles for the Virtual Machines

- Internal vulnerability score
- Intrusion behaviour score
- Trust based score

Step 1. Compute and generate score of the VMs based on the relevant security parameters.
Secure VM Consolidation

Security Profiles for the Virtual Machines

Step 2. Weighted average of the multi-dimension security score

Step 3. Develop VM consolidation job integration security profile
Internal vulnerability

Internal vulnerability and Intrusion analysis score

<table>
<thead>
<tr>
<th>Plugin Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>18405</td>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness</td>
</tr>
<tr>
<td>57508</td>
<td>SMB Signing Disabled</td>
</tr>
<tr>
<td>57690</td>
<td>Terminal Services Encryption Level is Medium or Low</td>
</tr>
<tr>
<td>30218</td>
<td>Terminal Services Encryption Level is not FIPS-140 Compliant</td>
</tr>
<tr>
<td>10114</td>
<td>ICMP Timestamp Request Remote Date Disclosure</td>
</tr>
<tr>
<td>10287</td>
<td>Traceroute Information</td>
</tr>
<tr>
<td>10394</td>
<td>Microsoft Windows SMB Log In Possible</td>
</tr>
<tr>
<td>10397</td>
<td>Microsoft Windows SMB LanMan Pipe Server Listing Disclosure</td>
</tr>
<tr>
<td>10736</td>
<td>DCE Services Enumeration</td>
</tr>
<tr>
<td>10785</td>
<td>Microsoft Windows SMB NativeLanManager Remote System Information Disclosure</td>
</tr>
<tr>
<td>10340</td>
<td>Windows Terminal Services Enabled</td>
</tr>
</tbody>
</table>

Intrusion based score is being formed from n number of intrusion behavior inputs:

\[
BS(VM_i) = \frac{w_1 \times IB_1 + w_2 \times IB_2 + \ldots + w_n \times IB_n}{\sum_{j=1}^{n} w_j}
\]
Ranking of the security profiles of the VMs

- **IVS**
  - CVE, CVSS
  - Nessus, etc
  - $IVS(VM_i)$

- **IBS**
  - IPS, IDS, Snort
  - Palo-alto, etc
  - $IBS(VM_i)$

- **TBS**
  - Non-reputation
  - Reputation
  - $TBS(VM_i)$

$R_s(VM_i)$

**Ranking process**

**Weighted ranking of the security profile**
High level procedure of the VM migration

VM Migration Selection
1. Random Selection (RS)
2. Minimum Migration Time (MMT)
3. Maximum correlation (MC)
4. Minimum Utilization (MU)

VM Migration Placement
1. Local Regression (LR)
2. Local Regression Robust (LRR)
3. Median Absolute Deviation (MAD)
4. Static Threshold (THR)
Secure VM Selection Algorithm (SBS)

Algorithm 1: Secure VM selection to migrate
Input host : Output vmToMigrate

migratableVMs <- getMigratableVMs(host)
minMetric <- MAX
foreach vm in migratableVMs do
    if vm is not in migration then
        metric = vm.getRam()
        if metric < minMetric then
            if hostSecurityLevel != vmSecurityLevel
                vmToMigrate <- vm
        return vmToMigrate
Secure VM Placement Algorithm (SBP)

Algorithm 2: Secure VM placement
Input vmList, hostList Output

vmList.sortDecreasingUtilization()
foreach vm in vmList do
    minPower <- MAX
    allocatedHost <- NULL
    foreach host in hostList do
        if hostSecurityLevel Equals vmSecurityLevel then
            if host has enough resources for vm then
                power <- estimatedPower( vm, host )
                if (power < minPower) then
                    if ( VMsInPM < AllowedMaxVM )
                        allocatedHost <- host
                        minPower <- power
            If allocatedHost != NULL then
                allocation.add(allocatedHost, vm)
    return allocation
Simulation Setup

(a) CloudSim Simulator
(b) PlanetLab Workload
(c) Power Consumption Profile

<table>
<thead>
<tr>
<th>Server load</th>
<th>HP ProLiant G4(W)</th>
<th>HP ProLiant G5(W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>86</td>
<td>93.7</td>
</tr>
<tr>
<td>10%</td>
<td>89.4</td>
<td>97</td>
</tr>
<tr>
<td>20%</td>
<td>92.6</td>
<td>101</td>
</tr>
<tr>
<td>30%</td>
<td>96</td>
<td>105</td>
</tr>
<tr>
<td>40%</td>
<td>99.5</td>
<td>110</td>
</tr>
<tr>
<td>50%</td>
<td>102</td>
<td>116</td>
</tr>
<tr>
<td>60%</td>
<td>106</td>
<td>121</td>
</tr>
<tr>
<td>70%</td>
<td>108</td>
<td>125</td>
</tr>
<tr>
<td>80%</td>
<td>112</td>
<td>129</td>
</tr>
<tr>
<td>90%</td>
<td>114</td>
<td>133</td>
</tr>
<tr>
<td>100%</td>
<td>117</td>
<td>135</td>
</tr>
</tbody>
</table>
## VM and PM initial configuration for simulation

### Virtual Machine Details

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total MIPS of VM</td>
<td>2500</td>
</tr>
<tr>
<td>Total PES (Processor unit) of VM</td>
<td>1</td>
</tr>
<tr>
<td>Total RAM of VM</td>
<td>1024 MB</td>
</tr>
<tr>
<td>Network Bandwidth of VM</td>
<td>100 Mbit/s</td>
</tr>
<tr>
<td>Total Storage size of VM</td>
<td>2.5 GB</td>
</tr>
</tbody>
</table>

### Physical Machine Details

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total MIPS of PM</td>
<td>2660</td>
</tr>
<tr>
<td>Total PES (Processor unit) of PM</td>
<td>2</td>
</tr>
<tr>
<td>Total RAM of PM</td>
<td>8192 MB</td>
</tr>
<tr>
<td>Total Storage size of PM</td>
<td>80 GB</td>
</tr>
</tbody>
</table>
Security aware VM consolidation comparison for low-medium workload for 800 hosts

![Graph showing kWh vs Security level]
Energy consumption versus security graph when the number of PMs are 1000, 2000 and 3000
Security level vs. energy consumption in multiple security-aware algorithms

![Graph showing energy consumption vs. security level for different algorithms.](image-url)
Conclusions

Introduced the compartment isolation technique to achieve the security aware VM consolidation.

Different types of simulation setup and the subsequent result confirms that there are no abrupt changes in power consumption to achieve security aware VM consolidation.

The solution presents an added protection measure with the minimal impact on energy efficient algorithm.

This work could be extended to improve the VM reliability as well as security and energy consumption.