A Measurement Method of Threat for Co-Residency Detection Based On Cloud Model

Rui-xiang DU¹, Hong RONG¹, Ming XIAN¹, Jun GU¹ and Wen WANG²

¹State Key Laboratory of Complex Electromagnetic Environment Effects on Electronic and Information System, National University of Defense Technology, Changsha, China
²Ordnance Engineering College, Shijiazhuang, China

Keywords: Cloud model; Virtual machine; Co-residency detection; Threat measurement.

Abstract. Ideally, each VM should be deployed independently and isolated form one another while multiple virtual machines share the same physical resource. Unfortunately, the absence of physical isolation inevitably give opportunities to number of security threats. In this paper, A cloud model-based method for measuring potential threat of virtual machine co-residency detection is proposed to solve the problem, which is caused by co-residency malicious VM, that malicious users steal private message and slow down others' performance. Based on the analysis of co-residency detection behavior characteristics, we utilized the method’s advantage in the uncertain conversion of multi-attribute decision and the evaluation of fuzziness and randomness. The method comprehensively considers the threat attributes of co-residency detecting, and gives full play to the advantages of the cloud model, which provides an important basis for the research and application of the detection and defense of the virtual machine in the cloud environment.

Introduction

At present, cloud security is the inevitable focus when cloud business and academia talking about the development and application of cloud computing. According to the actual operation required, multiple virtual resources may be bound to the same physical resource in the mainstream of cloud computing service platform, which rent physical resource to multi tenants in the model of virtual resources [1]. Theoretically, any two virtual machine are and completely separate independent, but because of the physical dependencies between virtual machines, these virtual machines are not completely independent[5], that is physical basis condition for virtual machine co-resident potential threats. Along with the development of cloud computing technology and commercial applications, public cloud resources has been low-priced, malicious users can attack co-resident virtual machine or others in cloud platform in low cost. Malicious users can attack the virtual machine and application of other users through the same physical resource sharing of physical resources that result in potential security threats, destruction of data confidentiality and resource availability in the cloud platform [2]. The virtual machine with such threat as shown in Figure 1.

![Co-Residency Threat of Virtual Machine](image)

Figure 1. Co-Residency Threat of Virtual Machine.

In cloud platform, Physical resources, which mainly include CPU, memory, disk resources, network card and I/O interface[6], have been shared and mutual interfered by co-resident virtual
machine. In different virtualization technology, resources allocation mechanisms are different. But it always exists mutual interference between co-resident virtual machines because resources competition, and that of course influence the performance of virtual machine. In the Amazon WC2, through the study conducted by Ristenpart et al., found that a malicious user can achieve 40% of VM co-residency rate at a lower price [3], and successfully to steal private letter from other virtual users through physical machine with ambassador. In article [4], Bedi et al. in University of Memphis, used the mechanism of virtual machine sharing network resources, put forward a program of denial of service attacks by blocking network transmission queue. Varadarajan et al. put forward resource attack, which changes the victim's use of the virtual machine resources, on the basis of analyzing the physical competition for resources, that attackers got hold of resources from co-resident virtual machine [7]. Hence, these co-residency security issues (CRSI) are become great security challenges in cloud computing.

The Main Technology of Virtual Machine Co-Resident Detection and Defense

Virtual Machine Co-resident Detection

In cloud environment, co-residency detection refers to the attacker to confirm their virtual machines and objective virtual machines on the same physical platform through the known detection methods. There are mainly four kinds of method for co-residency detection. The first bases on the network information [3], analysis network parameters to determine whether virtual machines are co-resident or not; the second bases on I/O resource competition [8], analysis the mutation of throughput load; the third bases on Co-Residency Watermarking [9], analysis time interval distribution of received network packet which are watermarked or non-watermarked; the fourth is use of L2 Cache Home Alone [10], analysis of the use of Cache.

The Defense of Co-Residency Detection

For the possible damage ,which has become a great threat to the safety of cloud environment, caused by malicious co-resident virtual machine, scientist also have brought numbers of corresponding defense technology. We sorted them in the following four categories: the first utilizes cloud security mechanism [2] to defense cloud platform LLC side-channel attacks; the second utilize the intermittent work scheduling strategy to enhance the isolation between virtual machines; the third draw lessons from multi-core processor chip system (CMPs) to achieve the anti-interference process scheduling algorithm; the fourth is hardware cooperative defense technology. But this defense technology will destroy the advantages of cloud computing and virtualization technology, resulting in waste of CPU resources, memory resources, network card resources, I/O resources, reduce the performance of virtual machines. Therefore, the effect of these co-residency defense methods are not obvious.

Virtual machine co-residency detection is a necessary precondition steps to deployment malicious co-resident virtual machine to implement covert information stealing and resource destruction, if we can measure the potentially threat during the stage of co-resident detection, according to the measurement results, taking advance corresponding resource scheduling policy or security strategy with purpose, such as limiting or isolating malicious users, protecting virtual machine which may be attacked and other measures, then we can avoid influencing cloud computing system performance caused by defense technology ,and also reduce harm caused by co-resident attackers.

Evaluation Attribute

Xiao-lin Gui does a lot of co-residency attack experiments on CPU Cache in the actual cloud computing system, found that the rate of a malicious user successfully implementing virtual machine co-resident attack has correlation with the number of controlled VMs[13]. The vast majority of malicious users will conduct co-residency detection before the side-channel attacks. To decreasing the cost of attack, attackers will also revoke VMs after completion co-residency detection. Through analysis detecting behavior conducted by Xiaolin Gui et al. in actual cloud environment, combining articles[3,8,9,10,13], we preliminary got eight possible attributes in co-residency detection threats, as shown in Figure 2. The measurement object is the virtual machine co-residency detection threats, set measurement attribute set $S_t$, and
\( S_t = \{S_{t1}, S_{t2}, S_{t3}, S_{t4}, S_{t5}, S_{t6}, S_{t7}, S_{t8}\} \). (This metric is based on literature analysis and it can be adjusted according to actual situation).

Figure 2. Attribute of Virtual Machine Co-residency Detection \( S_t \).

Determine the weight of each attribute: set the weight value as \( \omega \) (\( S_{t1} \) corresponds to \( \omega_1 \)), and meet \( \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5 + \omega_6 + \omega_7 + \omega_8 = 1 \). We considered the distribution of weight value based on weight determination method, and do not analyze it in detail here.

The Method of Virtual Machine Co-Residency Detection Based on Cloud Model

Cloud Model And Its Numerical Characteristics. Cloud model is one of the best excellent measurement for evaluation[11]. It combines the characteristics of fuzzy and random, and provides an effective evaluation method for qualitative and quantitative information decision process.

Cloud Model Definition. Set \( U \) to an exact value representation of the quantitative domain, \( C \) is the qualitative concept on \( U \), if the quantitative value \( x \in U \) is a random realization of the qualitative concept of \( C \), the degree of certainty \( \mu(x) \in [0,1] \) is a random number with a stable tendency, that is, the:

\[
U \rightarrow [0,1], \quad \forall x \in U, \quad x \rightarrow \mu(x)
\]

The distribution \( x \) in \( U = \{x\} \) is called cloud, each \( (x, \mu(x)) \) called a cloud droplet [11].

Numerical characteristics of cloud model. 3 tuple \( (E_x, E_n, H_e) \) represents the number of cloud features, expectation \( (E_x) \), entropy \( (E_n) \), super entropy \( (H_e) \).

a) Expectations: represent the expectation value of cloud drops distributed in the domain, is the most representative point of qualitative concept, is the value which corresponding to cloud gravity center, apparently it marked the position of model object, and this position is in the domain space.

b) Entropy: it reflects the range size of droplet that can be accepted by natural language value \( B \), while entropy also reveals its relevance, namely randomness and fuzziness, it is uncertain measurement of the concept of qualitative.

c) The super entropy: it reflects the discrete degree of cloud, condensation degree of cloud droplet, its size is in the \((0-0.02)\), change from quantitative to qualitative, data size for quantitative should be more than 200, the error will become smaller with more data.
The Method Of Virtual Machine Co-residency Detection Based on Cloud Model

The threat measurement of virtual machine co-residency detection is a problem of multiple attribute decision, and the cloud model can integrate the fuzziness and randomness of the qualitative concept, have good performance in conversion between quantitative evaluation and qualitative evaluation, make the evaluation results more credible [14].

The Specific Process. Based on analysis the attribute of virtual machine co-residency detection, utilize the advantage of cloud model, we proposed a measurement method of virtual machine co-resident detecting threat based on cloud model. The specific process as shown in Figure 3.

Figure 3. The process flow of cloud model-based method for measuring virtual machine co-residency detection threat.

**Ascertain the Evaluation Cloud of Assessment Level.**

We divided the metric assessment for virtual machine co-residency detection into 5 levels and comprise a set of qualitative measurement concept T, T = {T₁, T₂, T₃, T₄, T₅, T₆, T₇}. From Equation (1), we can know that the mapping reign is [0,1], through dividing the interval to reflect the evaluation level, mapping quantitative data to the reign.

By using forward cloud model, we used the bilateral constraint method to determine the variables of the quantitative attributes, as x ∈ (a, b). The calculate equation for numerical characteristics of the cloud model is:

\[
\begin{align*}
E_x &= \frac{(a + b)}{2} \\
E_n &= \frac{(b - a)}{6} \\
H_e &= K \\
\end{align*}
\]

In the equation, K is a constant, can be adjusted in the region of (0-0.02) according to the size of the attribute variable of the fuzzy threshold, be generally valued 0.02.

The concept of each level of qualitative metrics is divided into the measurement range shown in Table 1, and the parameters of each evaluation cloud are given according to the Equation 2. The forward cloud generator algorithm is used to generate the cloud image with 7 levels that represent virtual machine co-residency detection threat level, as shown in Figure 4.

Table 1. Table for evaluation cloud of each level.

<table>
<thead>
<tr>
<th>COMMENT</th>
<th>METRIC REGION</th>
<th>Eₓ</th>
<th>Eₙ</th>
<th>Hₑ</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₁</td>
<td>[0.0,0.1]</td>
<td>0.05</td>
<td>0.01667</td>
<td>0.02</td>
</tr>
<tr>
<td>V₂</td>
<td>[0.1,0.2]</td>
<td>0.15</td>
<td>0.01667</td>
<td>0.02</td>
</tr>
<tr>
<td>V₃</td>
<td>[0.2,0.4]</td>
<td>0.30</td>
<td>0.03333</td>
<td>0.02</td>
</tr>
<tr>
<td>V₄</td>
<td>[0.4,0.6]</td>
<td>0.50</td>
<td>0.03333</td>
<td>0.02</td>
</tr>
<tr>
<td>V₅</td>
<td>[0.6,0.8]</td>
<td>0.70</td>
<td>0.03333</td>
<td>0.02</td>
</tr>
<tr>
<td>V₆</td>
<td>[0.8,0.9]</td>
<td>0.85</td>
<td>0.01667</td>
<td>0.02</td>
</tr>
<tr>
<td>V₇</td>
<td>[0.9,1.0]</td>
<td>0.95</td>
<td>0.01667</td>
<td>0.02</td>
</tr>
</tbody>
</table>
Determine the Interval Mapping. In [15], Qing et al. discussed level mapping range of each attribute in detail, and reflects the threat level measurement, through reverse cloud algorithm simulate, has a good effect in the evaluation of cloud model measurement. The user has more than half of instances of VM on a physical machine, then the user is evaluated as high threat, i.e., $T_1 \geq 50\%$ mapped to $[0.9,1]$ extremely high threat; $30\% \leq T_1 < 50\%$ mapped to $[0.8,0.9]$ high threat; $15\% \leq T_1 < 30\%$ mapped to $[0.6,0.8]$ relative high threat; $10\% \leq T_1 < 15\%$ mapped to $[0.4,0.6]$ moderate threat; $5\% \leq T_1 < 10\%$ mapped to $[0.2,0.4]$ relative low threat; $2\% \leq T_1 < 5\%$ mapped to $[0.1,0.2]$ low threat; $T_1 < 2\%$ or $T_1 = 100\%$ mapped to $[0,0.1]$ excellent low threat.

We set $N$, that represent times of user cancels virtual machine in a short time, as the threat threshold, then the specific mapping interval is: $(T_3 \geq 2N)\sim[0.9,1.0]; (1.5N \leq T_3 < 2N)\sim[0.8,0.9]; (1N \leq T_3 < 1.5N)\sim[0.6,0.8]; (0.5N \leq T_3 < 1N)\sim[0.4,0.6]; (0.3N \leq T_3 < 0.5N)\sim[0.2,0.4]; (0.1N \leq T_3 < 0.3N)\sim[0.1,0.2]; (T_3 \leq 0.1N)\sim[0,0.1]$. The evaluation method of the attribute $T_2$, $T_5$, $T_6$, $T_8$ similar to that of $T_1$; the evaluation method of the attribute $T_3$, $T_4$, $T_7$ similar to that of $T_3$.

Ascertain Generation Algorithm of Integrated Cloud Parameter. We give 8 measurement attributes for the threat of virtual machine co-residency detection. We get the parameters of threat cloud by forward cloud generator based on the data of 8 attributes.

\[
\begin{align*}
E_{x_i} &= \bar{X} \\
E_{n_i} &= (\pi/2)^{1/2} \times \frac{1}{n} \sum_{i=1}^{n} |x_i - \bar{X}| \\
H_{e_i} &= (S^2 - E_{n_i}^2)^{1/2}
\end{align*}
\]

(3)

In the equation, $n$ is the number of samples; is the sample average of group; is the sample variance; is the center distance of the sample.

According to the digital features and the corresponding weights of each attribute, the weighted synthetic calculation of the 8 indicators of the virtual machine with the detection threat is as follows:

\[
\begin{align*}
E_{x_T} &= \sum_{j=1}^{m} \left( E_{x_j} \times \omega_j \right) \\
E_{n_T} &= \left( \sum_{j=1}^{m} \left( E_{n_j}^2 \times \omega_j \right) \right)^{1/2} \\
H_{e_T} &= \sum_{j=1}^{m} \left( H_{e_j} \times \omega_j \right)
\end{align*}
\]

(4)

In the equation, $m = 8$, $T(E_{x_T}, E_{n_T}, H_{e_T})$ is a set of integrated cloud parameters which expresses a virtual machine co-residency detection threats.

Determine the Threat Level Through Similarity Algorithm. By using the weighted Euclidean distance method[17], we compare the threat evaluation cloud to the integrated cloud of each $T_i$ level,

Figure 4. Evaluation cloud figure of measurement for virtual machine co-residency detection.
which we got in last section. Then we evaluated threat level of user as $T_i$, if the evaluation cloud was the most similar with cloud of $T_i$ level.

The integrated cloud parameters of threat measures $T(E_{x_1}, E_{n_1}, H_{e_1})$ and the cloud parameters of each level $T_i$ ($E_{x_i}, E_{n_i}, H_{e_i}$) are the determined weight values of the 3 parameters. Specific algorithms are as follows:

- Step 1 $D_1 = \left( \omega_{E_{x}}(E_{x} - E_{x_1})^2 + \omega_{E_{n}}(E_{n} - E_{n_1})^2 + \omega_{H_{e}}(H_{e} - H_{e_1})^2 \right)^{1/2}$;
- Step 2 $\delta_1 = 1/D_1$, $\delta_i$ is the weighted Euclidean distance;
- Step 3 $O_1 = (\delta_1/\sum_{i=1}^{n} \delta_i)$, $O_i$ is similarity;
- Step 4 repeat step 1 to step 3, work out all the $O_i$;
- Step 5 $\max(O_i)$ corresponds to $T_i$ is the user threat level.

**Experimental Results and Analysis**

To verify the feasibility of the method for detecting threats in the ideal case, we design 4 users $U_1$, $U_2$, $U_3$, $U_4$, which respectively represent the moderate threat, the low threat, the high threat, a little higher threat, belong to four threat levels, simulate attribute collection number of each user by random number generator (10 groups data for each attribute), utilize the method of grade evaluation, which has been talked about in third section, to measure evaluate the threat level.

We generated the stochastic experimental data according to the threat level of each user by using random generating, then calculate the data through the reverse cloud algorithm (equation (3)) to get threat cloud parameters of each attribute, then we calculate the comprehensive threat cloud parameters according to the weight of each index (Equation 4) [15]. As shown in table 2.

<table>
<thead>
<tr>
<th>USER ATTRIBUTES</th>
<th>$E_x$</th>
<th>$E_n$</th>
<th>$H_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_1$</td>
<td>0.42354</td>
<td>0.08426</td>
<td>0.03206</td>
</tr>
<tr>
<td>$U_2$</td>
<td>0.15806</td>
<td>0.07965</td>
<td>0.01421</td>
</tr>
<tr>
<td>$U_3$</td>
<td>0.80703</td>
<td>0.06531</td>
<td>0.00398</td>
</tr>
<tr>
<td>$U_4$</td>
<td>0.60408</td>
<td>0.05632</td>
<td>0.01151</td>
</tr>
</tbody>
</table>

According to the fifth step in the section 3.2, we use the cloud similarity algorithm to calculate the similarity of each users compare to each grade cloud, then we can determine the maximum similarity level as the user's threat level. When we using the method of similarity measurement in the cloud are respectively determined as 0.7, 0.2, 0.1. The similarity of each user cloud feature parameters and the evaluation parameters is shown in Table 3. The comparison of simulating cloud of each user with rating cloud is shown in Figure 5.

<table>
<thead>
<tr>
<th>SIMILARITY OF USER</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMENT</td>
</tr>
<tr>
<td>$V_1$</td>
</tr>
<tr>
<td>$V_2$</td>
</tr>
<tr>
<td>$V_3$</td>
</tr>
<tr>
<td>$V_4$</td>
</tr>
<tr>
<td>$V_5$</td>
</tr>
<tr>
<td>$V_6$</td>
</tr>
<tr>
<td>$V_7$</td>
</tr>
</tbody>
</table>
Figure 5. Comparison of level evaluation and 4 user's simulation cloud.

According to Table 3, simulation user U1 maximum similarity is 36.58%, close to the region of moderate threat; simulation user U2 maximum similarity is 58.56%, close to the region of low threat; simulation user U3 maximum similarity is 49.87%, close to the region of high threat; simulation user U4 maximum similarity is 33.96% and 32.96%, result in we can’t judge threat level of U4 directly. From Figure 5 can also be more intuitive to see the threat of 4 simulation users respectively. The results verify that the proposed method is feasible and has reference value in the cloud computing security and virtualization security.

Conclusion

In this paper, we briefly introduced the potential threat of virtual machine co-residency detection, analyze the technology of virtual machine co-residency detection and the technology of co-resident attack and defense, and then put forward attributes of co-residency attack threats, proposed by Gui et al., as framework, sum-up a more comprehensive threat attribute set, which is combined with the advantages of cloud model in multi-attributes decision metrics, present a measurement for threat of virtual machine co-residency detection based on cloud model. The method comprehensively evaluates the threat in multi attributes in cloud platform. Experiment results show that the proposed method can comprehensively consider the influence of various attributes, realize the comprehensive measurement of threat level. This research is a new exploration of cloud model application, and has important reference value to virtual machine security in cloud platform. Especially in virtual machine co-residency attack and defense, this research has significant sense. Then we can bring forward defense of co-residency attack to the phase of co-residency detection, further reduce the potential threat of co-resident virtual machine in cloud platform.

References


