論 文 内 容 の 要 旨

博士論文題目　A Dynamic Analysis with Static Source Code Instrumentation for the Guest Monitoring Problem in Virtualization Environments

氏　　名　Ady Wahyudi Paundu

（論文内容の要旨）

Even though the cloud technology shows the trend of rapid development and decreasing cost, it still has not been fully embraced by organizations and industries around the world. This reluctance mostly stems from the cloud system security issues. One of the main potential attack vectors in a cloud system is the guest Virtual Machine (VM). Therefore, it is necessary to provide a system to monitor the guest VM operations. In the public cloud model, there are several operational requirements for the monitoring program. First, the monitoring system must work separately outside of the guest VM. Separating the monitoring process and the monitored system can deny any malicious processes in the monitored system from compromising the monitoring agent. However, this separation requirement could lead to the semantic gap problem. A good monitoring system is expected to choose the observation data that preserve the semantic information as much as it can. Second, the monitoring system must be able to work without any cooperation from the guest VM. The guest VM should not even realise the existence of the monitoring program. Therefore, for the third requirement, the monitoring program should cost, in term of computation resources usage, as efficient as possible.

In this thesis, we investigate a guest VM monitoring method that can work independently outside the monitored guest VM, without losing much of the semantic information and without high computation cost for either the host and the guest VM. We propose a method that embeds multiple tracepoints inside the source code of the hypervisor (Static Instrumentation). During the hypervisor operation we collect the tracepoints execution data to dynamically monitor the operational flow of a guest VM (Dynamic Source Code Analysis). Since the instrumentation was carried out within the underlying process of the instances of guest VM, we believe that the dynamic pattern of the tracepoints sequences can indirectly describe the operations of the VM.

We first applied this dynamic source code analysis with static instrumentation method to the user space of Qemu-KVM hypervisor. We captured the tracepoints from the Qemu operation and used it for an Anomaly Detection System. We emulated a web server VM and multiple attack scenario, such as DDoS for network-based attack and Flush-Reload attack for virtualization-based attack. We factored in the mimicry attack scenario. We compared several

machine learning algorithms for monitoring data analysis process. Finally, we compared our detection result with system-call data analysis. Our evaluation showed that monitoring guest VM using dynamic source code analysis with static instrumentation method gave better detection results compared to the system-call data, with minimum computation cost. However, we had subpar results when trying to detect malicious activities that work upon host CPU. That is because on Qemu-KVM combination, CPU operations are performed natively through the KVM kernel module.

We investigated further this dynamic source code analysis with static instrumentation method at the kernel layer by instrumenting the KVM module. We used this method to implement a signature-based intrusion detection system and try to detect multiple variants of Cache-based Side Channel Attack (CSCA) including a new stealthier variant called Flush- Flush attack. In our evaluation phase, we showed that our proposed approach is the first successful attempt to detect this Flush-Flush attack in the virtualization environment.

氏　名	Ady Wahyudi Paundu

（論文審査結果の要旨）

近年、クラウドコンピューティングが従来の計算機利用モデルに比べて多くの利点をもつものとして期待を集めているが、その一方で、セキュリティへの懸念が全面的な利活用を阻んでいる。本論文では、クラウド環境において今日でも残存するセキュリティ脅威を対象とし、これを検知するために、ハイパーバイザにおいて静的計装と機械学習を用いた方式を提案している。本論文の主な成果は、以下に要約される。

1. 脆弱性などにより隣接テナントおよびハイパーバイザへ悪影響を及ぼす場合を脅威モデルとして想定し、そのような異常を検知するために、ハイパーバイザへの静的計装と機械学習を用いた動的解析を組み合わせた方式を提案している。これにより、ゲスト環境によらずに高い精度で異常検知を行えることを実証している。

2. 異常検知方式として、３種の機械学習アルゴリズムを用いて比較評価し、サイドチャネル攻撃およびファジングを脅威モデルとして想定し、正常なワークロードが多い状況においても、低いオーバーヘッドと低い誤検知率で異常検知が可能であることを実証している。

3. 従来方式では検知が難しいキャッシュベースのサイドチャネル攻撃を対象として、ハイパーバイザへの静的計装と機械学習を用いた動的解析を適用し、正常なワークロードが多い状況や正常なワークロードを模擬した検知回避攻撃に対しても高い検知精度が実現できたことを報告している。

以上のように、本論文はクラウドコンピューティングのセキュリティ向上に資する異常検知方式を提案し、テストベッドでの比較実験と性能評価によってその有効性を検証している。それぞれの成果は１編の学術論文と２編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。