SMMエージェントとuBPFによる機密VMの安全かつ効率的な監視方式

山口 紘輝[1]　末永 道正[1]　光来 健一[1]

1. はじめに

近年，クラウド上の仮想マシン（VM）を用いて機密情報を扱う機会が増えている．これに伴い，クラウド内部での不正アクセスによる情報漏洩が問題となり，CPU の隔離実行環境を活用した機密 VM が利用が進んでいる．しかし，機密 VM 内に侵入されると情報漏洩を防げないため，侵入検知システム（IDS）による監視が不可欠である．IDS を VM 内に設置すると侵入時に無効化されるリスクがあるため，VM の外部で IDS を動作させる IDS オフロードが行われている．しかし，機密 VM はメモリが暗号化されており，IDS が VM のメモリ上の OS データを直接解析することはできない．この課題に対して，先行研究 [1] では機密 VM 内にエージェントを配置し，そのエージェントを介して IDS がメモリデータを取得する手法を提案している．ただし，エージェントの配置方法により，安全性とシステム性能の間にトレードオフが生じる．

本研究では，エージェントを機密 VM の BIOS 内に配置し，uBPF を用いて OS データを一括取得することにより安全性と性能の両立を可能にする uBPF-SV を提案する．

2. uBPF-SV

uBPF-SV では，図 1 のように機密 VM の BIOS 内でシステムマネジメントモード（SMM）を用いてエージェントを安全に動作させる．SMM は BIOS のみが使用可能な CPU の動作モードであり，独立した実行環境を提供する．そのため，この SMM エージェントを攻撃者が無効化するのは難しい．SMM エージェントは SMI インジェクションと呼ぶ手法を用いて呼び出す．この手法は VM 外部からシステムマネジメント割り込み（SMI）を注入し，BIOS 内部の割り込みハンドラを実行させる．エージェントを保護するためにシステムを隔離実行する必要がなく，SMM エージェントの実行中以外はシステム性能が低下しない．

VM 内の OS データを一つ取得するたびに SMI インジェクションを行うのはオーバヘッドが大きいため，uBPF を用いて VM のメモリ上の OS データを解析することで必要なデータを一括取得する．OS データの解析を柔軟に行えるようにするために，uBPF-SV は BIOS 内に uBPF プログラムを送り込んで実行する．uBPF は Linux カーネルで用いられている eBPF のユーザ空間実装であり，プログラムを安全に実行することができる．そのために，ロード時に uBPF プログラムの検証を行うことで，任意のメモリ領域への不正アクセスなどの危険な動作を防止する．uBPF プログラムは JIT コンパイルを用いてネイティブコードに変換することで，高速な実行が可能である．

uBPF プログラムは，監視対象システムのメモリ上に存在する OS データを共有メモリへコピーすることで IDS に返送する．uBPF プログラム自身はシステムメモリや共有メモリに直接アクセスできないため，uBPF ランタイムが提供するヘルパー関数を利用する．このヘルパー関数は，システムメモリ上の OS データの仮想アドレスを物理アドレスに変換し，対応するメモリデータを共有メモリにコピーする．アドレス変換に失敗した場合にはシステムメモリへのアクセスを行わないため，不正な仮想アドレスへのアクセスは防止される．また，共有メモリの範囲外アドレスが指定された場合も検出可能であり，安全なメモリアクセスが保証される．

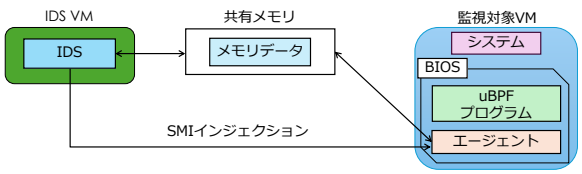
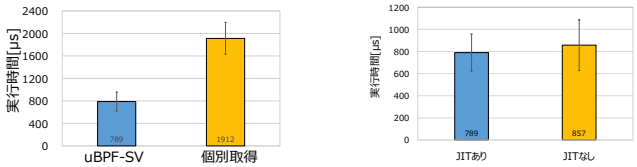


図 1: uBPF-SV のシステム構成

[1] 九州工業大学
Kyushu Institute of Technology



(a) OS データの一括取得　　(b) JIT による実行

図 2: uBPF-SV の監視性能

3. 実験

uBPF-SV を用いて，2 種類の OS バージョン文字列を一括取得するのにかかる時間を調べた．IDS が SMI インジェクションを用いて要求を送信してから，uBPF プログラムが共有メモリに格納したメモリデータを受信して表示するまでの時間を測定した．比較として，uBPF プログラムを用いずに 2 つの OS データを 1 つずつ取得した場合についても測定を行った．図 2(a) の結果より，uBPF-SV は一括取得により監視性能を 58%向上させられることがわかった．また，わずかではあるが，図 2(b) のように JIT による高速化も確認することができた．

4. まとめ

本研究では，SMM エージェントと uBPF を用いて機密 VM からメモリデータを取得して監視を行う uBPF-SV を提案した．今後の課題は，uBPF プログラムを用いて複雑な OS のデータ構造を解析しながらメモリデータを取得できるようにすることである．

謝辞　本研究の一部は，JST，CREST，JPMJCR21M4 の支援を受けたものである．

参考文献

[1] T. Nono, K. Kourai: Secure Monitoring of Confidential VMs with Isolated Agents, *In Proceedings of the 18th IEEE/ACM International Conference on Utility and Cloud Computing* (2025).