

コース	コンピュータ工学	指導教員	光来 健一
学生番号	182C1096	氏 名	末永 道正
論文題目	AMD SEV で保護された VM の SMI インジェクションを用いた監視		

1 はじめに

クラウドによって提供される仮想マシン (VM) の利用が増加するにつれて、クラウド内部の悪意ある管理者等による VM からの機密情報の盗聴が問題になっている。VM のメモリの盗聴を防ぐために AMD 製 CPU は SEV と呼ばれる透過的なメモリ暗号化を提供しているが、VM 内に侵入されると SEV では盗聴を防ぐことができない。そこで、侵入検知システム (IDS) を用いて VM の監視を行う必要があるが、侵入者によって IDS が無効化されないようにするために、IDS を VM 外で動作させる IDS オフロードが用いられる。VM が SEV で保護されている場合、VM 外からメモリの監視を行えないため、SEVmonitor [1] では VM 内で動作するエージェント経由でメモリデータを取得する。しかし、エージェントの配置方法によって安全性とシステム性能にトレードオフが生じる。

本研究では、VM の BIOS 内に配置したエージェントを直接呼び出し、共有メモリを用いてメモリデータを取得する SMMmonitor を提案する。

2 SMMmonitor

SMMmonitor は図 1 のようにエージェントを監視対象 VM の BIOS 内に配置し、システムマネジメントモード (SMM) で動作させる。SMM は BIOS のみが使用可能な CPU モードで、独立した実行環境を提供する。エージェントが配置されるメモリは SMM 以外の CPU モードの時には VM に割り当てられていないため、VM 内の OS が攻撃を受けたとしてもエージェントを無効化することはできない。また、システムをエージェントから隔離するためのオーバーヘッドがないため、エージェントの実行中以外はシステム性能がまったく低下しない。

SEV で保護された IDS VM で動作する IDS は監視対象 VM の外からシステムマネジメント割込み (SMI) を挿入することで、BIOS 内のエージェントを直接呼び出す。この SMI インジェクションを実行するために、IDS は VM のデバイスエミュレータと通信して SMI 挿入コマンドを送信する。デバイスエミュレータはハイパーバイザを呼び出し、対象 VM

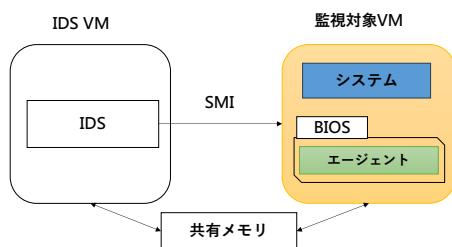


図 1. SMMmonitor の構成

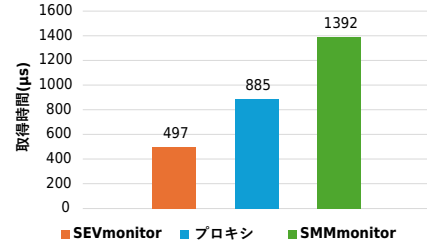


図 2. メモリデータの取得時間

に対して SMI を発生させる。すると、BIOS 内で登録された SMI ハンドラが実行される。

SMI ハンドラは IDS VM と監視対象 VM の間に確立された共有メモリに IDS からの要求が格納されていればエージェントを呼び出す。エージェントは OS のページテーブルを用いて要求されたメモリの仮想アドレスを物理アドレスに変換し、メモリデータと応答を共有メモリに格納する。IDS VM と監視対象 VM は共有メモリに仮想 PCI デバイス経由でアクセスする。しかし、アクセスに必要なデバイスドライバは BIOS 用には提供されていないため、BIOS がこの仮想 PCI デバイスにアクセスするのは容易ではない。そこで、OS が起動時に仮想 PCI デバイスから取得した共有メモリのアドレスを SMI を用いて BIOS に登録することで、BIOS が共有メモリにアクセスできるようにする。

3 実験

SMMmonitor の性能を調べるために、VM のメモリ上にある OS のバージョン情報を取得するのに要する時間を測定した。比較として、監視対象システムの OS 内にエージェントを配置する SEVmonitor と、プロキシ経由で BIOS 内のエージェントを呼び出す先行研究 [2] でも測定を行った。実験の結果、図 2 に示すように、SMMmonitor は SEVmonitor と比較して 2.8 倍、プロキシを用いる先行研究と比較して 1.6 倍の時間となった。これはデバイスエミュレータと通信して SMI を挿入するオーバーヘッドのためだと考えられる。

4 まとめ

本研究では、SEV で保護された VM に対して SMI インジェクションを用いて BIOS 内のエージェントを直接呼び出し、共有メモリを用いてメモリデータを取得するシステムを提案した。今後の課題は、監視対象 VM の様々な情報を取得する IDS を動作させることである。

参考文献

- [1] 能野, 光来. AMD SEV で保護された VM の隔離エージェントを用いた安全な監視. CSS 2022.
- [2] 武田. SEV で保護された VM を監視可能にするエージェントの SMM による隔離. 九州工業大学 卒業論文, 2023.