

|      |                                                 |      |       |
|------|-------------------------------------------------|------|-------|
| コース  | コンピュータ工学                                        | 指導教員 | 光来 健一 |
| 学生番号 | 212C1156                                        | 氏 名  | 村上 和馬 |
| 論文題目 | AMD SEV-SNP の VMPL によって隔離されるエージェントを用いた機密 VM の監視 |      |       |

## 1 はじめに

IaaS 型クラウドの普及に伴い、仮想マシン (VM) の中で機密情報を扱うことが増えている。そのため、クラウドの内部犯による VM 内の機密情報の盗聴が問題となっている。このような情報漏洩を防ぐために、最近のクラウドは AMD SEV 等の CPU 機構を用いてメモリが暗号化された機密 VM を提供している。一方、機密 VM であっても侵入されると機密情報の盗聴を防ぐことはできないため、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。IDS を VM 内で実行すると侵入者に無効化される恐れがあるため、IDS を VM の外で動作させる手法が用いられている。この手法は VM のメモリ上の OS データを監視するため、メモリが暗号化されている機密 VM に対しては適用することができない。そこで、VM 内で動作するエージェントを経由してメモリデータを取得するシステム [1] が提案されている。しかし、エージェントの配置方法には安全性とシステム性能のトレードオフがある。

本研究では、AMD SEV-SNP で導入された VM 特権レベル (VMPL) を用いてエージェントを安全に隔離しつつ、監視対象 VM の性能低下を最小限に抑えるシステム SNPmonitor を提案する。

## 2 SNPmonitor

SNPmonitor は図 1 のように、SEV-SNP で保護された機密 VM において低い特権レベル (VMPL2) で監視対象システムを動作させ、高い特権レベル (VMPL0) でエージェントを動作させることによりエージェントを隔離する。VMPL は VM 内のメモリを 4 つの特権レベルに分割することができる SEV-SNP の機能である。VMPL を用いることにより、監視対象システムはエージェントを攻撃することができないが、エージェントからは監視対象システムのメモリにアクセスすることができる。また、エージェントの実行中に一つの仮想 CPU が使えなくなるだけである。

SNPmonitor は監視対象システム内にプロキシを配置し、IDS が監視対象システムのメモリデータを取得する際には仮想ネットワーク経由でプロキシに要求を送る。取得するメ

モリデータのアドレスは IDS とエージェントの間に確立した共有メモリに格納する。プロキシは VM の下で動作するハイパーバイザを呼び出し、VMPL2 から VMPL0 に切り替えることによってエージェントを呼び出す。エージェントは共有メモリに格納されたアドレスを取得し、対応するメモリデータを共有メモリに格納する。IDS はプロキシからの応答を受け取ると、共有メモリに格納されたメモリデータを取り出す。

IDS が共有メモリに格納するのはメモリデータの仮想アドレスであるため、エージェントは監視対象システムのメモリにアクセスするためにそれを物理アドレスに変換する。VMPL2 から VMPL0 に切り替える際に監視対象システムの CPU レジスタの値が VMSA と呼ばれる領域に保存されるため、エージェントは VMSA 中の CR3 レジスタの値から OS のページテーブルを特定する。そして、ページテーブルをたどることによってアドレス変換を行い、得られた物理アドレスに対応するメモリデータを取得する。

## 3 実験

SNPmonitor を用いて監視対象 VM の OS バージョンを取得する時間を測定した。比較のために、監視対象 VM の OS 内でエージェントを動作させる先行研究についても測定を行った。実験結果は図 2 に示すようになり、SNPmonitor における取得時間は先行研究の 31 倍となった。これは仮想ネットワークとプロキシを用いているためと考えられる。ただし、SNPmonitor の方がエージェントをより安全に実行できる。

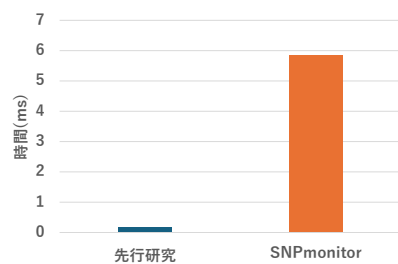


図 2. OS バージョンの取得時間

## 4 まとめ

本研究では、SEV-SNP の VMPL によって隔離されたエージェントを用いて安全性とシステム性能を両立させることのできる VM 監視システム SNPmonitor を提案した。今後の課題は、IDS がエージェントを直接呼び出せるようにすることである。

## 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.

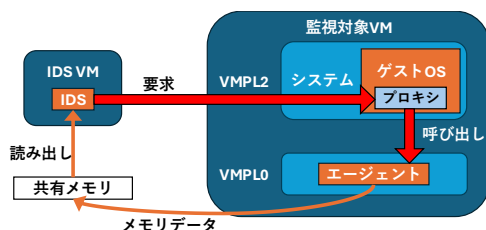


図 1. SNPmonitor のシステム構成