九州工業大学 情報工学部 情報・通信工学科 2022 年度 卒業論文 概要

コース	ソフトウェアデザイン	指導教員	光來 健一
学生番号	192C1025	氏　　名	上杉 貫太

論文題目	eBPF を用いた OS データの一括取得による高速なリモート VM 監視

1　はじめに

クラウド上の仮想マシン (VM) を利用するユーザが増えるにつれ，VM 内の機密情報がクラウドの内部犯によって盗聴されるリスクが問題となっている．そのため，AMD 製の CPU は VM のメモリを暗号化することで VM 外からの盗聴を防ぐ SEV と呼ばれる機能を提供している．SEV は VM 内の侵入者に対しては無力であるため侵入検知システム (IDS) と併用する必要があるが，VM が SEV で保護されていると VM の外で動作する IDS は VM のメモリ上の OS データを監視できなくなる．そこで，SEVmonitor [1] は VM 内で安全に動作するエージェントと通信することでメモリデータを取得し，OS データの監視を可能にしている．しかし，メモリデータは IDS が必要とした時に取得されるため，ポインタを用いる OS データの場合はポインタをたどる度に通信が必要となり，監視性能が低下する．

本研究では，SEV で保護された VM に eBPF プログラムを送り込み，OS データを先読みして一括で取得することにより VM の監視を高速化する eBPFmonitor を提案する．

2　eBPFmonitor

eBPFmonitor は図 1 のように，監視対象 VM 内で動作するエージェントが IDS からの要求に応じて，ポインタを用いる OS データ全体を先読みする．対象となる OS データの例としては，プロセスやカーネルモジュールのリスト，ネットワークソケットを管理するハッシュ表などがある．IDS からの 1 回の要求で OS データを一括で返送することにより，通信のオーバヘッドを減らすことができる．

先読みする OS データは IDS ごとに異なるため，eBPFmonitor は IDS ごとに作成した eBPF プログラムを監視対象 VM 内の OS に動的に送り込んで実行する．eBPF は性能等を監視するために用いられている Linux の機構である．カーネルモジュールを同様の目的で利用することも考えられるが，eBPF プログラムは OS へのロード時に検査器によって安全性が保証される．そのため，OS に影響を与えることなく実行することができる．

eBPFmonitor では，IDS がエージェントを介して監視対象 VM に eBPF プログラムをロードし，eBPF プログラムを

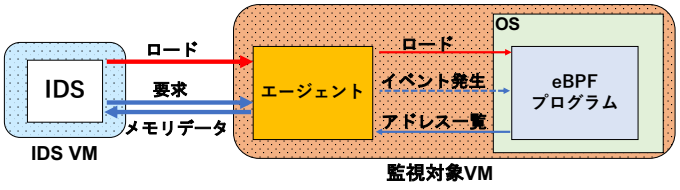

図 1. eBPFmonitor のシステム構成

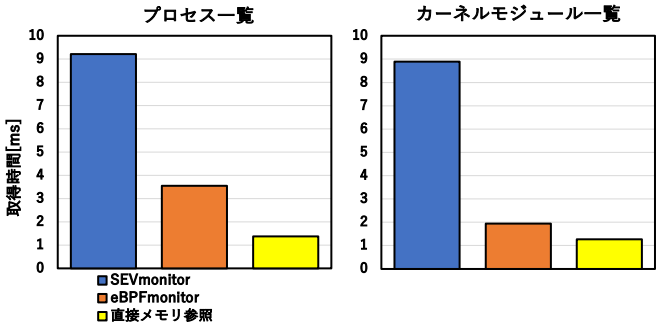

図 2. ポインタを用いた OS データの取得時間

呼び出すためのイベントを OS に設定する．エージェントが IDS から OS データの一括取得要求を受信すると，要求に対応するイベントを発生させて eBPF プログラムを呼び出す．eBPF プログラムは終了しない可能性のあるループを実行できないため，有限ループを用いて OS データのポインタをたどり, アドレス一覧を収集する．その後，エージェントは収集したアドレスに対応するメモリデータを OS から取得し，順次 IDS に返送する．IDS は受信したメモリデータをキャッシュに保存し，先読みした OS データにアクセスする場合には通信を行わない．

3　実験

eBPFmonitor により VM の監視が高速化できるかどうかを調べるために，IDS がプロセスおよびカーネルモジュールの一覧を取得するのにかかる時間を測定した．監視対象 VM にはプロセスリストとカーネルモジュールリスト全体を取得する 2 つの eBPF プログラムをロードした．比較として，ポインタをたどる度に通信を行う SEVmonitor と監視対象 VM のメモリを直接参照する従来手法でも実験を行った．図 2 に示すように，eBPFmonitor は SEVmonitor よりプロセス一覧を 2.6 倍, カーネルモジュール一覧を 4.6 倍高速に取得できた．直接メモリ参照と比べると，プロセス一覧が 2.6 倍, カーネルモジュール一覧が 1.5 倍の取得時間となった．

4　まとめ

本研究では，SEV で保護された VM に送り込んだ eBPF プログラムを用いて OS データを先読みして一括で取得し，VM の監視を高速化する eBPFmonitor を提案した．今後の課題は，IDS が必要とするデータのみを一括取得し，通信データ量の削減によるさらなる高速化を行うことである．

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*.