KVMにおける仮想マシンを用いたIDSオフロードの実現

中村 孝介† 光来 健一 †,††

1. はじめに

インターネットに接続されたホストへの攻撃を検知するために侵入検知システム（IDS）が用いられている。IDSは攻撃の兆候を検知して管理者に通知する。一方、攻撃者はIDSに検知されるのを防ぐために、ホストへの侵入後にIDSの無効化や改竄を試みることが増えてきた。このようなIDS自身への攻撃に対処するために、仮想マシン(VM)を用いてIDSをオフロードするという手法が提案されている。IDSのオフロードを行うことにより、監視対象VMに侵入した攻撃者によってIDSが無効化されることを防ぐことができ、セキュリティを向上させることができる。これまで、IDSオフロードの研究は主にXenを用いて行われてきた。一方で、最近普及してきたKVMにおいてIDSオフロードはまだほとんど研究されていない。

本研究ではKVMを用いてIDSのオフロードを実現するKVMonitorを提案する。

2. KVMonitor

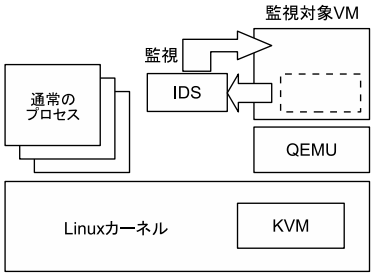

図 1 KVMonitor の構成

KVMonitorはIDSをホストOS上にオフロードし、VMの監視を行うことを可能にする。

2.1 ディスクの監視

ディスクの監視を行うために監視対象VMのディスクをホストOS上にマウントする。KVMでは主にqcow2というファイル形式が使用されるが、qcow2形式のファイルは直接マウントすることができない。そこでネットワークブロックデバイス（NBD）を用いてホストOSに仮想的なブロックデバイスとして見せる。IDSはこのブロックデバイスを監視することでディスクの監視を行う。

2.2 メモリの監視

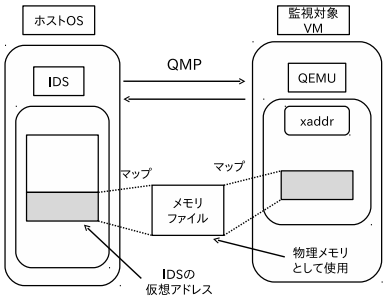

図 2 メモリファイルのマップ

メモリを監視できるようにするために、KVMonitorはVMの物理メモリをファイルとしてIDSに提供する。IDSはこのファイルを mmap システムコールを用いてメモリマップすることで、VMのメモリにアクセスする。ただし、従来のQEMUはこのファイルをオープンした後で削除していたため、IDSからアクセスできるようにQEMUに修正を加えた。

仮想アドレスを使ってVMのメモリ上のデータにアクセスするために、IDSはQEMUと通信して仮想アドレスを物理アドレスに変換する。VM内部のOSカーネルの変数の仮想アドレスは分かっているが、VMのメモリには物理アドレスでアクセスする必要がある。そこでQEMU外部から仮想アドレスを物理アドレスに変換を行えるようにする xaddr コマンドをQEMUに追加した。IDSは得られた物理アドレスをオフセットとして、メモリ用ファイルにアクセスする。

IDSからQEMUの xaddr コマンドを呼び出すには、QEMU Monitor Protocol（QMP）を使ってQEMUと通信を行う。QMPはJSON[1)]を用いてアプリケー

† 九州工業大学
†† 独立行政法人科学技術振興機構、CREST

ションと QEMU の間で通信を行うプロトコルである。IDS は QEMU の QMP 用ポートに接続した後、xaddr コマンドの実行を要求する。QEMU はこのコマンドを実行して、変換した物理アドレスを返す。

2.3 資源管理

IDS とオフロード元 VM をひとまとまりとして柔軟な資源管理を行えるようにするために、KVMonitor は Linux カーネルが提供している Cgroups 機能を用いる。Cgroups は複数のプロセスをグループ化して、そのグループ単位での資源管理を可能にする。Cgroups を用いて、ホスト OS 上で IDS と監視対象 VM の 2 つのプロセスをグループ化する。KVM では VM が 1 プロセスとして作成されるため、このようなグループ化を容易に行うことができる。このグループに対して CPU やメモリに対する制約を設定する。

3. 実験

オフロードした IDS から VM のディスクとメモリの監視および性能分離に関する実験を行った。実験には CPU に Intel Xeon 2.53GHz の CPU、6GB のメモリを搭載したマシンを使用した。VM には 30GB のディスクと、512MB のメモリを割り当てた。

3.1 Tripwire を用いた監視

Tripwire を用いて監視対象 VM のディスクの整合性を検査する実験を行った。Tripwire をホスト OS 上にオフロードした場合でも、VM のディスクの検査を行うことができ、追加・削除・変更されたファイルを検出できることが確認できた。

表 1 Tripwire の実行時間

	実行時間（分）
オフロードなし	9.2
オフロードあり	9.9

3.2 CPU に関する性能分離

ディスクを監視する IDS である Tripwire をオフロードし、この Tripwire と監視対象 VM のグループに対して CPU 使用率の下限が設定できることを確かめる実験を行った。Tripwire と VM のプロセスを Group1、ホスト OS 上で無限ループするプロセスを Group2 とし、Group1 と Group2 に割り当てる CPU の割合を 40:60 とした。図 2 に Group1 と Group2 の CPU 使用率と Group1 中の Tripwire と VM のそれぞれの CPU 使用率を示す。Group1 の CPU 使用率は 40%でほぼ一定していることがわかる。

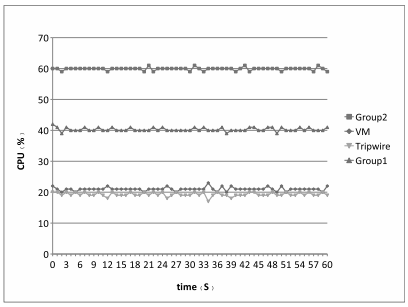

図 3 VM と Tripwire の CPU 使用率

4. まとめ

本研究では KVM における IDS オフロードを実現するシステム KVMonitor を提案した。KVMonitor では、NBD を用いることで IDS によるディスクの監視を可能にし、QEMU を改造することで IDS によるメモリの監視を可能にした。さらに、Linux の Cgroups 機能を用いることで、IDS オフロード時の柔軟な資源管理を実現した。今後の課題は、ネットワーク IDS のオフロードに対応することである。

参考文献

1) D.Crockford. The application/json Media Type for JavaScript Object Notation (JSON) RFC4627, 2006.