論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻

学生番号	11675025	氏　名	中村　孝介
論文題目	KVM における IDS オフロードのための仮想マシン監視機構		

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。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 の無効化や改ざん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、IDS を仮想マシン（VM）の外にオフロードするという手法が提案されている。IDS オフロードは VM に侵入した攻撃者が IDS を無効化することを防ぐ。しかし、最近、普及してきた仮想化ソフトウェアの KVM においては IDS オフロードはまだあまり研究されていない。

本研究では KVM において IDS オフロードを実現するシステム KVMonitor を提案する。

2　KVMonitor

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。Xen と異なり、KVM では図 1 のようにホスト OS 上で VM が動作するため、オフロードした IDS をホスト OS 上のプロセスとして動作させることができる。KVMonitor は VM のメモリとディスク、ネットワークの監視に対応している。

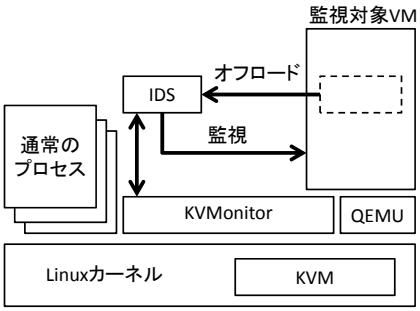

図 1: KVMonitor の構成

オフロードした IDS が VM のメモリを監視できるようにするために、KVMonitor は VM に割り当てる物理メモリをファイルとして作成し、そのファイルを VM と IDS の両方にメモリマップする。これにより、VM に対して従来通りの直接メモリアクセスを可能にしつつ、外部の IDS もそのメモリを参照することができる。

IDS は仮想アドレスを用いて VM のメモリ上のデータにアクセスするため、KVMonitor が仮想アドレスを物理アドレスに変換する。メモリマップされる VM のメモリは物理メモリであり、物理アドレスでアクセスする必要があるためである。KVMonitor はメモリアドレスを変換するために必要な CR3 レジスタの値を QEMU と通信して取得し、アドレス変換を行う。

KVMonitor は VM のディスクの監視を可能にするためにネットワークブロックデバイス（NBD）の機能を用いる。KVM で標準的に用いられるディスク形式はホスト OS 上で直接マウントできない。KVMonitor は NBD を通して VM のディスクを仮想的なブロックデバイスとしてマウントする。また、KVMonitor は VM 毎に tap デバイスを生成してホスト OS にブリッジ接続することで、IDS がネットワークの監視を行えるようにする。

3　実験

KVMonitor を用いた場合の監視性能を調べるために、Xen 用に開発された Transcall[1] を KVM 用に移植した。Transcall は VM のメモリ、ディスク、ネットワークへのアクセスを隠蔽し、既存の IDS を修正なしでオフロードすることを可能にする。ルートキットを検出する chkrootkit をオフロードして実行した場合の実行時間は、オフロードしない場合の約 2 倍となった。Xen ではオフロードしない場合の約 2.6 倍になるため、KVMonitor における IDS オフロードによる性能低下は Xen を用いる場合より小さいことが分かった。

4　おわりに

本研究では KVM において IDS オフロードを実現するシステム KVMonitor を提案した。KVMonitor を用いることにより、KVM でもオフロードした IDS が VM を監視することができるようになる。

参考文献

[1] 飯田貴大, 光来健一, VM Shadow:既存 IDS をオフロードするための実行環境, 第 119 回 OS 研究会, 2011 年.