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	10675002	氏　名	飯田　貴大
論文題目	仮想マシンを用いて既存 IDS をオフロードするための実行環境		

1　はじめに

インターネットに接続されたサーバへの攻撃は年々増加しており、攻撃を検出するための侵入検知システム (IDS) の重要性が増している。近年、IDS を安全に実行できるようにするために、仮想マシンを用いて IDS をオフロードするという手法が提案されている。この手法では監視対象のシステムをサーバ VM と呼ばれる仮想マシンを用いて動作させ、IDS だけを IDS-VM と呼ばれる別の仮想マシンで動作させる。これにより、侵入を検知する前に攻撃者によって IDS が無力化されてしまう事態を防ぐことができる。しかし、IDS をオフロードして動作させられるようにするにはプログラムの大幅な変更などの多大な労力が必要とされることが多く、既存の IDS を使うことができなかった。

本研究では IDS に修正を加えることなくオフロードできるようにする実行環境である VM Shadow を提案する。

2　VM Shadow

VM Shadow は図 1 のように IDS-VM 上のプロセスがサーバ VM を透過的に監視するための実行環境である。VM Shadow は監視の点でサーバ VM にリモートログインしたかのような実行環境を提供し、既存の IDS を VM Shadow の中で動作させることでサーバ VM の情報へのアクセスを可能とする。そのために、VM Shadow はシステムコールとファイルシステムのエミュレーションを行う。

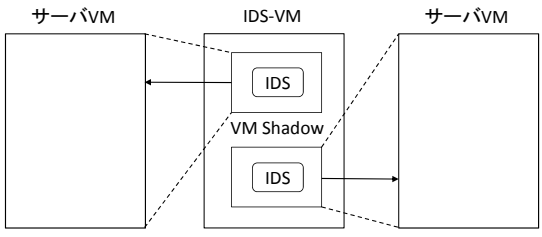

図 1: VM Shadow を用いた監視システム

VM Shadow はその中で動くプロセスがサーバ VM の OS の情報を取得できるようにするために、いくつかのシステムコールをエミュレートする。例えば、IDS が uname システムコールを発行した際にはサーバ VM の OS のバージョン等を返す。それ以外のシステムコールについては IDS-VM の機能を利用する。

また、VM Shadow は Shadow ファイルシステムを提供し、サーバ VM のファイルシステムにアクセスできるようにする。ただし、IDS の実行のために読み込まれるファイルについては、安全のために IDS-VM のファイルにアクセスさせる。プロセスなどの OS カーネル内部の情報を参照するために使われる proc ファイルシステムにもアクセスできるように Shadow proc ファイルシステムを提供する。Shadow proc ファイルシステムはサーバ VM の OS カーネルを解析することで必要な情報を取得する。

3　実験

VM Shadow を提供するシステム Transcall を Xen 上に実装し、いくつかの IDS の動作確認を行った。まず、不正にインストールされたルートキットを検出する chkrootkit を動作させた。その結果、ファイル、プロセス情報、ネットワーク情報などに基づく検出を正しく行えることが確認できた。エミュレーションのオーバヘッドのため、chkrootkit の実行時間はサーバ VM で動作させる場合の約 1.5 倍となった。

次に、ディスクの整合性チェックを行う Tripwire を動作させた。実験の結果、Tripwire のポリシファイルに変更を加えることなく、サーバ VM のファイルの改ざんを検出できることが確認できた。ディスク仮想化のオーバヘッドが軽減されるため、Tripwire の実行時間は約 20 %高速になった。

最後に、ネットワークの監視を行う Snort を動作させた。サーバ VM に攻撃パケットを送信したところ、その攻撃を正しく検出することができた。ネットワーク仮想化のオーバヘッドがなくなるため、Snort の CPU 使用率が約 40 %低下した。

4　おわりに

本研究では、既存の IDS に修正を加えることなくオフロードすることを可能にする実行環境である VM Shadow を提案した。既存の IDS を VM Shadow の中で動作させることで透過的にサーバ VM の監視を行うことができる。今後の課題は、より多くの IDS を動作させられるようにすることである。