審 査 の 結 果 の 要 旨

氏　　名　　尾上　浩一

サンドボックスシステムや侵入検知システムのようなセキュリティシステムはアプリケーションの不正な振る舞いやデータの改竄を検出・防止することができる。しかし、セキュリティシステムは信頼できないプログラムと同一のOS上で稼働するため、攻撃者はOSカーネルや特権レベルで稼働するプログラムを乗っ取ることができれば、セキュリティシステムそのものを乗っ取ることが出来てしまう。このようなセキュリティシステムへの攻撃を防ぐためには仮想マシンモニタ（VMM）が有用である。制御対象であるOSおよびアプリケーションを動作させるVMとセキュリティシステムを動作させるVMを動作させることにより上記脅威を守ることが可能となる。しかし、制御対象プログラムをVMの外側から制御するためには2つの課題がある。ひとつは、VMMが取得可能なレジスタやメモリの値のようなハードウェアレベルの実行状態からプロセス等のOSレベルの実行状態を復元することである。もうひとつは、セキュリティシステムが制御のために必要な、VMM が検出できないイベントを捕捉できるようにすることである。

本論文では、OSとしてLinuxカーネルを想定すると共にカーネルソースプログラムが提供されている環境において、Linuxカーネルが想定しているハードウェアレジスタの使い方に注目してVMMからVM上のOS実行状況を捕捉し、OS上のプロセスを制御可能とする手法であるShadowVoxを提案している。ShadowVoxを用いることにより、セキュリティシステムと制御対象プログラムをそれぞれ別のVM上で効率良く動作させることが可能となる。ShadowVoxを異なるプロセッサアーキテクチャに実装し、サーバプログラムやセキュリティシステムに適用している。さらに、ShadowVoxがセキュリティシステム自体に対する攻撃から保護できることを確認するとともにシステムコール捕捉に伴うオーバーヘッドを測定している。

さらに、本論文では、上記提案手法を用いて、2つのセキュリティシステム、Shadowall, ShadowXeckを提案、実装し、評価している。Shadowallは、保護対象プログラムのデータの漏洩や改竄を同一OS上で稼働するOSカーネルを含む信頼できないプログラムから防ぐことができる。Shadowallの評価では、保護対象のメモリ・ディスク上のデータに関する漏洩と改竄が防げることを確認し、Shadowallにより生じる実行時のオーバーヘッドを計測した。

ShadowXeckは、VM内で稼働するOSカーネルの振舞いを制御するセキュリティシステムであり、読込み専用領域の書き換え防止および関数ポインター変数の書き換え防止に焦点を当てている。本手法により、VMMを用いた既存のアンチカーネルレベルマルウェアシステムにおける、保守的すぎる手法や適用時の実行時の性能低下に関する課題を解決している。ShadowXeckの評価では、既存のカーネルレベルマルウェアを用いたShadowXeckによるOSカーネルの振舞い制御確認や実行時オーバーヘッドの計測を行った。

本論文では、このように、従来実現されていなかったセキュリティシステムと制御対象プログラムを異なるVM上で効率良く動作させる手法を確立し、セキュリティシステムの安全性を向上させることに成功している。本手法はLinuxカーネルを想定しているが、OSカーネルソースが公開されているシステムであれば適用可能であり一般性のある手法であり、セキュリティシステム構成法の研究に顕著な貢献をしたといえる。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。