様式 C-7-2

自己評価報告書

平成２２年４月１２日現在

研究種目：若手研究(B)
研究期間：2007 年度～2010 年度
課題番号：19700024
研究課題名（和文）
仮想マシンモニタのための安全性向上技術に関する研究
研究課題名（英文）
Security enhancement technology for virtual machine monitors
研究代表者
大山 恵弘（電気通信大学電気通信学部・准教授）

研究者番号：10361536

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：仮想マシンモニタ、セキュリティ、オペレーティングシステム

１．研究計画の概要

本研究は安全な仮想マシンを開発するためのソフトウェア構築技術の確立を目的とする。仮想マシンによってサーバなどの安全性を高める技術の研究とは異なり、本研究は仮想マシン自身のセキュリティを高める技術の深化を目指す。本研究では特に仮想マシンモニタと呼ばれる種類の仮想マシンを扱う。本研究で開発する要素技術の柱は、安全な高級言語による仮想マシンモニタの開発手法と、仮想マシンモニタを監視するセキュリティシステムの 2 つである。前者の要素技術の研究では、プログラムに脆弱性を含ませやすいという欠点にもかかわらず現在開発言語の主流となっている C 言語以外の高級言語で仮想マシンモニタを開発する方式を構築する。必要に応じて、システムソフトウェアの実装を支援するための高級プログラミング言語の独自拡張を設計する作業も行う。後者の要素技術の研究では、仮想マシンモニタの外で攻撃や異常を検知するための方式を提案する。仮想マシンモニタの挙動を外部から監視して攻撃や異常を検知するセキュリティシステムを構築し、その有効性を評価する。

２．研究の進捗状況

本研究では今までに以下の成果が得られている。まず、安全な高級言語 Haskell により小さい仮想マシンモニタを実装し、その上で世界で広く用いられているオペレーティングシステムである Linux を稼働させることに成功している。そのオペレーティングシステム上でいくつかのアプリケーションプログラムの性能測定を行い、結果を国際会議で報告した。高級言語の独自拡張については、上記の仮想マシンモニタの開発では、拡張しなくとも十分であることがわかったため、独自拡張に関する作業は行っていない。

本研究課題では、Haskell 以外にも、関数型言語 OCaml による開発を行うことも検討した。実際に OCaml によって低レベルシステムソフトウェアを開発し、OCaml が仮想マシンモニタの開発において有用かどうかを調査した。

他の成果としては、ルートキットの技術を応用した仮想マシンモニタを用いた防御システムの構築がある。本システムは動作中の OS に対して動的な挿入と削除が可能である仮想マシンモニタであり、利便性が極めて高い。具体的には、本システムはカーネルレベルバッファオーバフロー攻撃を防止することができる。本システムの設計、実装、性能評価について述べた論文は国際会議で採択されている。

また、セキュリティシステムをテストするための、仮想マシンモニタを利用したシステムを構築した。このシステムはアプリケーションプログラムやカーネルに対して、マルウェアなどによる攻撃の効果を外部から注入するものである。攻撃の効果はユーザが記述したシナリオに従って注入される。注入された攻撃への反応を調べることにより、セキュリティシステムをテストすることができる。

さらに、仮想マシンモニタ間に隠しチャネルを構築する手法の構築と評価を行った。具体的には本手法は、異なる仮想マシン内のプログラムが CPU 負荷を通じて通信を行うこ

とを可能にする。隠しチャネルの精度とバンド幅を計測する実験を行い、論文にまとめた。その論文は国際会議ですでに発表ずみである。

３．現在までの達成度

達成度は
2. おおむね順調に進展している。
であると考える。
高級言語による仮想マシンモニタの開発手法を構築、提案、評価するという目標は達成している。仮想マシンモニタに関するセキュリティシステムに関しても、国内外の会議に複数の論文が出ており、一定の成果をあげていると考える。

４．今後の研究の推進方策

今後は、現在までに遂行してきた研究の方向は維持し、研究のまとめを主に行いたいと考えている。新たな実験や開発を行うよりは、これまでの成果を論文にまとめたり、ウェブなどを通じて世界に伝える作業に取り組みたい。

５． 代表的な研究成果
（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計 14 件）

(1) Keisuke Okamura, Yoshihiro Oyama. Load-based Covert Channels between Xen Virtual Machines. In Proceedings of the 25th Symposium on Applied Computing (SAC 2010), pages 173-180, Sierre, Switzerland, March 24th, 2010. 査読あり.
(2) 井上 翔大, 大山 恵弘. OCaml による OS の実装. 情報処理学会第 113 回システムソフトウェアとオペレーティング・システム研究会, 札幌, 2010 年 1 月 27 日. 査読なし.
(3) Yu Adachi, Yoshihiro Oyama. Malware Analysis System using Process-level Virtualization. In Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC '09), pages 550-556, Sousse, Tunisia, July 7th, 2009. 査読あり.
(4) 野元 励, 大山 恵弘. HyperShield: 動作中の OS を安全な仮想マシン上に移行するための仮想マシンモニタ. 第 7 回先進的計算基盤システムシンポジウム（SACSIS 2009）, pages 179-187, 広島国際会議場, 2009 年 5 月 29 日. 査読あり.
(5) Yoshihiro Oyama, Yoshiki Kaneko, Hideya Iwasaki. Kenro: A Virtual Machine Monitor Mostly Described in Haskell. In the 24th ACM Symposium on Applied Computing (SAC 2009), poster session, pages 1940-1941, Hawaii, USA, March 10th, 2009. 査読あり.