様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月３日現在

機関番号：１２６１２
研究種目：若手研究(B)
研究期間：２００７年度～２０１０年度
課題番号：１９７００００２４
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)　Study on Security Enhancement Techniques for Virtual Machine Monitors

研究代表者
大山 恵弘（YOSHIHIRO OYAMA）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：１０３６１５３６

研究成果の概要（和文）：
仮想マシンモニタのための安全性向上技術について研究を行った．まず，仮想マシンモニタのソフトウェアを高級言語で開発する技術について研究を行った．具体的には，本研究では純粋関数型言語 Haskell にて仮想マシンモニタを開発し，プログラムの読みやすさや性能を，実験を通じて評価した．また，仮想マシンモニタを用いてセキュリティを向上させるシステムについても研究を行った．本研究では実際にバッファオーバフロー攻撃を防止するための仮想マシンモニタを実装し，実験により確かに攻撃が防止できることを確認した．

研究成果の概要（英文）：
We developed security enhancement techniques for virtual machine monitors. First, we investigated a technique for developing software of virtual machine monitors in a high-level programming language. Specifically, we developed a virtual machine monitor in a purely functional programming language Haskell, and evaluated its readability and performance through experiments. Next, we also investigated the systems that enhance the security by using a virtual machine monitor. We implemented a security system for preventing buffer overflow attacks, and confirmed through experiments that the system could actually prevent attacks.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	800,000	0	800,000
2008 年度	800,000	240,000	1,040,000
2009 年度	800,000	240,000	1,040,000
2010 年度	800,000	240,000	1,040,000
総　計	3,200,000	720,000	3,920,000

研究分野：ソフトウェア
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，システムソフトウェア，マルウェア

１．研究開始当初の背景

近年、仮想マシンモニタと呼ばれるソフトウェアが普及しつつある。仮想マシンモニタは計算機ハードウェアを仮想的に実現するソフトウェアであり、ある OS の上で別の OS を動かすことを可能にする（以降では、仮想マシンモニタの上で動く OS をゲスト OS と呼ぶ）。仮想マシンモニタは有用であり、多くの応用を持つ。現在、VMware、Xen などのソフトウェアが世界中で用いられている。
仮想マシンモニタの安全性は極めて重要で

ある。コンピュータウィルスや攻撃者が仮想マシンモニタを乗っ取ると、ゲスト OS の全制御権が奪われる。仮想マシンモニタの脆弱性は、任意の種類の OS の乗っ取りを許す点で、OS の脆弱性と同等またはそれ以上に深刻である。しかし、残念ながら、仮想マシンモニタからは脆弱性が発見され続けている。

仮想マシンモニタの分野では、長い間、性能が最大の関心事であったが、近年、性能以外にも注目が向き出している。仮想マシンモニタの安全性を高めるための研究にも注目が向かいつつあるが、どの研究グループも、まだ着手し始めた段階である。

現在、ほぼすべての仮想マシンモニタは、C 言語で記述されている。C 言語のプログラムは実行が高速という利点がある一方、脆弱性（特にバッファオーバフロー脆弱性）が入りやすいという致命的な欠点がある。たとえば広く利用されているオープンソース仮想マシンモニタの Xen は、数十万行の C 言語で記述されているため、開発者のミスによりバッファオーバフロー脆弱性が入りうる。この規模のソフトウェアでは、人間が注意深く開発を行うという方法だけでは、脆弱性の排除は難しい。体系的に安全性を高める技術を構築することが現実的かつ急務である。

２．研究の目的

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。

これまで、システムソフトウェアの安全性は国内外において主に OS を対象に研究されてきた。90 年代では高級言語の Java で OS を記述する JavaOS の研究が著名である。近年では Microsoft 社が、安全性を保証する言語で OS を記述する Singularity プロジェクトを始めている。しかし、仮想マシンモニタを安全な高級言語で記述する試みは、申請者の知る限り存在しない。OS を対象とした安全性向上技術が、仮想マシンモニタの分野でどの程度有効であるかは、未知のままとなっている。

３．研究の方法

(1) 現在の主流である C/C++言語とアセンブリ言語の組み合わせではない方法で仮想マシンモニタを開発する技術を開発する．高級言語のうちから一つを選択して，その言語により仮想マシンモニタを実際に構築する．結果的には純粋関数型言語である Haskell を用いることとなった．C 言語によっても同様の仮想マシンモニタを構築する．2 つの仮想マシンモニタの間で，プログラムの開発のしやすさ，プログラムの読みやすさやメンテナンスのしやすさ，性能について比較する．

(2) 安全性向上のための処理を組み込んだ仮想マシンモニタを開発する．開発にあたっては，仮想マシンモニタの分野における新しい技術である CPU 内仮想化支援機構を用いる．その仮想マシンモニタは OS を再起動や停止させることなく，OS を実計算機上で実行させたり仮想マシン上で実行させたりできるという便利な機能を提供する．同時に，最も深刻な被害をもたらす攻撃の一つであるバッファオーバフロー攻撃を防止する機能を提供する．

４．研究成果

(1) 純粋関数型言語 Haskell により仮想マシンモニタを実際に開発し，高級言語で仮想マシンモニタが実装可能であることを示した．その仮想マシンモニタ上では，世界で広く利用されている OS である Linux を起動させることができている．Haskell で書かれた仮想マシンモニタと C 言語で書かれた仮想マシンモニタを比較し，強い型システム，高階関数，ガベージコレクション，遅延評価などが，記性や性能にどう影響するかをまとめた．

(2) 必要に応じて OS に組み込んだり取り外したりすることが可能な，セキュリティ向上のための仮想マシンモニタを実装した．カーネルレベルデバイスドライバの脆弱性を突く攻撃コードを作り，それを用いて攻撃実験を行った．その結果，本研究の仮想マシンモニタがその攻撃を防

止したことを確認した．また，その仮想マシンモニタが性能に与える影響をベンチマークによって測定したところ，ある程度現実的な範囲に収まっていることを確認した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

① Tomohiro Shioya, Yoshihiro Oyama, Hideya Iwasaki, “A Sandbox with Dynamic Policy Based on Execution Contexts of Applications”, Proceedings of the 12th Annual Asian Computing Science Conference, volume 4846 of Lecture Notes in Computer Science, pp. 297-311, 2007, 査読あり.

〔学会発表〕（計 16 件）

① Yoshihiro Oyama, Youhei Hoshi, “A Hypervisor for Injecting Scenario-Based Attack Effects”, Proceedings of the 35th Annual IEEE Computer Software and Applications Conference (COMPSAC 2011), July 21,2011(予定), 査読あり.
② 大山 恵弘, 岩崎 英哉, “Haskell で記述した仮想マシンモニタの評価”, 第13回プログラミングおよびプログラミング言語ワークショップ (PPL2011), 北海道札幌市, 2011 年 3 月 10 日.
③ 岡村 圭祐, 大山 恵弘, “仮想マシンモニタを用いたマルウェア実行抑止機構”, 第 22 回 コンピュータシステム・シンポジウム (ComSys 2010), 大阪大学中之島センター, 2010 年 11 月 29 日.
④ Tsutomu Nomoto, Yoshihiro Oyama, Hideki Eiraku, Takahiro Shinagawa, Kazuhiko Kato, “Using a Hypervisor to Migrate Running Operating Systems to Secure Virtual Machines”, Proceedings of the 34th Annual IEEE Computer Software and Applications Conference (COMPSAC 2010), pp. 37-46, Seoul, Korea, July 20, 2010, 査読あり.
⑤ Keisuke Okamura, Yoshihiro Oyama, “Load-based Covert Channels between Xen Virtual Machines”, Proceedings of the 25th ACM Symposium on Applied Computing, pp. 173-180, Sierre, Switzerland, March 24, 2010, 査読あり.
⑥ 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, 札幌コンベンションセンター, 2010 年 1 月 27 日.
⑦ 星 洋平, 大山 恵弘, “仮想マシンモニタを用いたSoftware Fault Injection”, 2009 年並列／分散／協調処理に関する『仙台』サマー・ワークショップ, 宮城県仙台市, 2009 年 8 月 6 日.
⑧ Yu Adachi, Yoshihiro Oyama, “Malware Analysis System using Process-level Virtualization”, Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC 2009), pp. 550-556, Sousse, Tunisia, July 7, 2009, 査読あり.
⑨ 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, 広島国際会議場, 2009 年 5 月 29 日, 査読あり.
⑩ 岡村 圭祐, 大山 恵弘, “仮想マシン間における covert timing channel の評価”, 情報処理学会 第 111 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, 沖縄県青年会館, 2009 年 4 月 22 日.
⑪ Yoshihiro Oyama, Yoshiki Kaneko, Hideya Iwasaki, “Kenro: A Virtual Machine Monitor Mostly Described in Haskell”, Proceedings of the 24th ACM Symposium on Applied Computing (SAC 2009), pp. 1940-1941, Hawaii, USA, March 10, 2009, 査読あり.
⑫ 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”, 電子情報通信学会コンピュータシステム研究会 2008 年 10 月研究会, 広島市立大学, 2008 年 10 月 31 日.
⑬ 安達 悠, 大山 恵弘, “プロセスレベルの仮想化を用いたマルウェアの挙動解析システム”, コンピュータセキュリティシンポジウム 2008 (CSS 2008), 沖縄コンベンションセンター, 2008 年 10 月 9 日.
⑭ Koichi Onoue, Yoshihiro Oyama, Akinori Yonezawa, “Control of System Calls from Outside of Virtual Machines”, Proceedings of the 23rd Annual ACM Symposium on Applied Computing (SAC 2008), pp. 2120-2125, March 20, 2008, 査読あり.
⑮ 金子 佳樹, 大山 恵弘, 岩崎 英哉, “純関数型言語による仮想マシンモニタの実現”, 第 10 回プログラミングおよ

びプログラミング言語ワークショップ(PPL2008), 宮城県仙台市, 2007年3月5日.
⑯ 尾上 浩一, 大山 恵弘, 米澤 明憲, “仮想マシンモニタによる仮想マシン内プロセスの制御”, 2007年並列／分散／協調処理に関する『旭川』サマー・ワークショップ（SWoPP旭川2007）, 北海道旭川市, 2007年8月3日.
⑰ 塩谷 知宏, 大山 恵弘, 岩崎 英哉, “実行コンテキストに応じて振る舞いが変わるサンドボックス”, 情報処理学会第105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, 沖縄県那覇市, 2007年4月5日.

〔その他〕
ホームページ等

http://www.ol.inf.uec.ac.jp/

６．研究組織
(1)研究代表者
大山 恵弘（YOSHIHIRO OYAMA）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：10361536

(2)研究分担者
なし

(3)連携研究者
なし