様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月　４日現在

研究種目：若手研究（Ｂ）
研究期間：2008～2009
課題番号：20700020
研究課題名（和文）　仮想マシンによる動的情報流追跡の実現

研究課題名（英文）　Dynamic Information-flow Tracking via Virtual Machines

研究代表者
品川　高廣（SHINAGAWA TAKAHIRO）
筑波大学・大学院システム情報工学研究科・講師
研究者番号：40361745

研究成果の概要（和文）：

本研究では，仮想マシンの技術を利用した動的情報流追跡などにより，オペレーティングシステムが扱う情報の流れを監視・管理して，強固なセキュリティを実現する手法に関する研究を行った．仮想マシンモニタのレイヤでオペレーティングシステムからの入出力を監視・変更する技術を確立することにより，仮想マシンモニタのレイヤでオペレーティングシステムからファイルへのアクセスを把握して強力な保護が実現できるようになった．

研究成果の概要（英文）：

We have carried out the research on virtual machine technologies for enforcing the security of operating systems by monitoring the flow of information. We have developed a virtual machine monitor technology for monitoring I/O access to devices, allowing the virtual machine monitor to mediate and protect file access from the operating systems.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,800,000	540,000	2,340,000
２００９年度	1,500,000	450,000	1,950,000
年度			
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：オペレーティングシステム
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

１．研究開始当初の背景

近年のインターネットでは，ウィルスの感染による不正アクセスや情報漏洩などのセキュリティ問題への対策が重要な課題となっている．これらの問題が生じる原因の多くはソフトウェアのバグであるが，近年の OS やアプリケーションは高機能化によりプログラムの規模が極めて膨大になっており，バグが全く発生しないように正しく実装する

ことは極めて困難になっている．従って，上記のようなセキュリティ問題に対処するためには，低レイヤのシステムソフトウェアによって強固な保護機構を実現し，仮にソフトウェアにバグがあったとしてもその被害を最小限に抑えられる仕組みが必要とされている．

不正アクセスや情報漏洩を防ぐための手法としては，近年 Dynamic Information Flow Tracking（動的情報流追跡）という手法が着目されつつある．これは，プログラムの実行時に情報の流れを追跡することにより，ウィルスなどを含む不正なデータをプログラムとして実行してしまうことや，機密情報が意図せず外部に流出してしまうことを検出して防止する手法である．動的情報流追跡の特徴は，プログラムの動作という主体側の挙動を監視するのではなく，プログラムによって扱われるデータという客体側の挙動を監視する点にある．これにより，外部から送り込まれたデータを内部で実行してしまうことによる不正アクセスや，内部にとどめておくべきデータを外部に送ってしまう情報漏洩といった，ユーザが防止したいセキュリティ問題を直接的かつ確実に防止することができるという利点を持っている．

動的情報流追跡を仮想マシンモニタのような低レイヤのシステムで実現しようとする場合，データを管理する単位の細かさ（粒度）やデータが持つ意味とのギャップ（セマンティックギャップ）が問題となる．例えば，オペレーティングシステムはファイルをストレージに格納する際にはファイルシステムを用いて管理をしているが，その管理のためのデータ構造はワードやバイトなどの細かい単位で区分けされているほか，それぞれの値には意味が持たされている．一方，仮想マシンモニタのようにハードウェアに近い低レイヤでは，512 バイト単位のセクタなどまとまった単位で入出力がなされるほか，それらは意味を持たない透明なバイト列として扱われるため，オペレーティングシステムがそれらのデータに与えている意味に関する情報は失われてしまっている．一方，オペレーティングシステムやアプリケーションなどのソフトウェアのレベルで動的情報流追跡を実現した場合には，バイト単位で確実に情報流を追跡することができるが，既存のソフトウェアへの改変が必要になってしまう．

２．研究の目的

本研究では，既存の OS やアプリケーションを改変することなく，確実なセキュリティを実現する手法として，仮想マシンを用いた動的情報流追跡などによりセキュリティを強化する手法に関する研究をおこなう．仮想マシンにより，プロセッサによるメモリアクセスだけではなく，ストレージやネットワークなどの周辺機器も含むシステム全体における全ての情報の流れをソフトウェアによって把握して，仮想マシン内で動作するプログラムに一切依存することなく強固なセキュリティを実現する．これにより，Windows や Office など既存の OS やアプリケーションがそのまま動作しつつも，不正アクセスや情報漏洩を確実に防止できるシステムの確立を目指す．

３．研究の方法

本研究では，仮想マシンモニタにおいて，メモリやプロセッサ，ストレージ，ネットワークのそれぞれのハードウェア・デバイスにおいて，情報の流れを監視・変換機能を実装することで，セキュリティ機能を実現する．また，それらの機能を用いて実際にセキュリティを実施するためのポリシーの実現方法についても研究を行う．

(1) 仮想マシンモニタ

仮想マシンモニタによる情報の流れの監視・変換を可能にするために，メモリ及びプロセッサに対して部分的な仮想化を行い，オペレーティングシステムからは透過な形で仮想マシンモニタがシステム内に存在できるようにする．メモリに関しては，仮想マシンモニタが使用する領域へのアクセスを監視して不正アクセスを防止するほか，オペレーティングシステムが入出力時に使用するメモリ領域を特定することで，情報の流れを確実に把握する．プロセッサに関しては，オペレーティングシステムからシステムレジスタへのアクセスを監視することで，不正アクセスを防止する．

ストレージやネットワークにおける情報の流れを監視・変換する機能に関しては，研究代表者が考案した準パススルー・アーキテクチャをベースとして，入出力情報を監視・変換する機能を追加するほか，後述のセキュリティポリシーに応じて，入出力を禁止するなどのアクセス制御機能を導入する

(2) セキュリティポリシー

セキュリティポリシーについては，情報の入出力を監視することで，読み込み及び書き込みアクセスに対するアクセス制御を実現し，それによって情報漏洩の防止や不正な書き込みの防止を実現できるようなポリシー記述方式を考案する．

オペレーティングシステムと仮想マシンモニタとの間のデータの粒度やセマンティックギャップの問題を解決するために，仮想マシンモニタのレイヤでありながらオペレーティングシステムの意味情報を抽出できる仮想マシンイントロスペクションの技術を応用して，セキュリティポリシーで記述する高レベルのポリシー情報を仮想マシンモニタがエンフォースできる低レベルの情報にマッピングして，粒度が細かい詳細なポリシー記述を可能にしつつ，仮想マシンモニタのレイヤで強力なセキュリティを実現可能にする．

４．研究成果

本研究では，仮想マシンモニタのレイヤで情報の監視・変換を行うフレームワークとして，研究代表者が考案した準パススルー型アーキテクチャに基づく仮想マシンモニタ[2]を基盤とした研究をおこない，実際に情報の流れを監視することでセキュリティを実現する例として，仮想マシンモニタによるファイル保護に関する研究をおこなった．

(1) 準パススルー型仮想マシンモニタ

本研究で用いる仮想マシンモニタでは，情報の流れを監視することにより強力なセキュリティを実現することを目的としている．従って，仮想マシンモニタ自体にセキュリティ上の脆弱性が存在してしまうと，システム全体のセキュリティを保つことが難しくなってしまう．

ソフトウェアの脆弱性を減らすためには，ソフトウェアをシンプルかつ小さく保つことが有効とされている．しかし従来の仮想マシンモニタでは，仮想マシンモニタ本体のほかにホストとなるオペレーティングシステムが必要なアーキテクチャが多く，そのサイズを小さく保つことが難しくなっていた．

そこで本研究では，準パススルー型という新しいアーキテクチャに基づくことで，仮想マシンモニタ自体のサイズを非常に小さく保つ仕組みを導入した．このアーキテクチャでは，オペレーティングシステムにおける情報を監視・変換することに特化して，セキュリティに関係ないデバイスの仮想化をやめてパススルーによる直接アクセスを許可することにより，仮想マシンモニタのサイズを小さく保っている．また，入出力デバイスの監視においても，デバイスに対するアクセスを制御 I/O とデータ I/O とその他の I/O に分けて考え，制御 I/O により入出力の状況を把握し，データ I/O を必要に応じて捉えることにより，仮想マシンモニタによる確実な監視・変換を可能にしつつ，この操作に関係ないその他の I/O に関してはパススルーすることにより，必要最小限度のコードによってセキュリティを実現することが可能になっている．

本研究では，準パススルー型アーキテクチャをベースとしてさらに改良を加え，情報漏洩防止など機密性を保つ目的だけでなく，アクセス制御など更に柔軟なセキュリティ機能を実現できるようにするための機能追加を行っている．その成果は，国際会議において発表した文献[2]の一部として反映されているほか，文献[1][3]の一部においてもその内容を記述している．

(2) 仮想マシンモニタによるファイル保護

準パススルー型仮想マシンモニタに関する研究の成果を踏まえて，具体的に情報の流れを監視してセキュリティを強化する仕組みとして，仮想マシンモニタによりファイル保護を実現する仕組みに関して研究を行った．

近年のマルウェアの中には，カーネルルートキットなどオペレーティングシステムのカーネル権限を乗っ取って感染するタイプのソフトウェアが増えている．この場合，オペレーティングシステムレベルでのセキュリティ機能は原理的に無効にされてしまう可能性があるため，より高い特権をもった仮想マシンモニタによる保護が有効となる．

しかし，この場合，オペレーティングシステムと仮想マシンモニタとのセマンティックギャップが問題となる．オペレーティングシステムではファイルの単位で情報を管理するのに対し，仮想マシンモニタではセクタなど固定長のバイト列を単位として情報の入出力をおこなうため，仮想マシンモニタからファイルに関する情報を取得することは容易ではない．更に，準パススルー型アーキテクチャでは，仮想マシンモニタをシンプル化するために，基本的にアクセスのチェックはオペレーティングシステムが行ったものに対して受動的に行うことしかできないため，仮想マシンモニタが能動的にストレージにアクセスしに行くことによりファイル情報を再構成するという手法は取ることが出来ない．

そこで本研究では，事前にファイルシステムとストレージ内の領域とのマッピングを作成する方式により，仮想マシンモニタの大きさを肥大させることなく仮想マシンモニタによるファイルレベルの保護を実現できるようになった．また，データの粒度の問題に対しても，セクタ内のデータに対してバイト単位でアクセス制御を行う技術により，オペレーティングシステムのアクセスに対して受動的かつ透過的にアクセス制御を実現

することが可能になった．本研究の成果は，無査読の国内会議において文献[3]として報告したのち，査読付き国際会議において文献[1]として採択されて発表を行った．

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）

〔学会発表〕（計３件）

[1] Yosuke Chubachi, Takahiro Shinagawa, Kazuhiko Kato. Hypervisor-based Prevention of Persistent Rootkits. 25th ACM Symposium On Applied Computing (ACM SAC 2010), Sierre, Switzerland, Mar 24, 2010.

[2] Takahiro Shinagawa, Hideki Eiraku, Kouichi Tanimoto, Kazumasa Omote, Shoichi Hasegawa, Takashi Horie, Manabu Hirano, Kenichi Kourai, Yoshihiro Oyama, Eiji Kawai, Kenji Kono, Shigeru Chiba, Yasushi Shinjo and Kazuhiko Kato. BitVisor: A Thin Hypervisor for Enforcing I/O Device Security. 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE 2009), Washington, DC, USA, Mar 13, 2009.

[3] 忠鉢 洋輔, 品川 高廣, 加藤 和彦. 仮想マシンモニタによるゲスト OS のファイル保護．情報処理学会研究報告(2009-OS-111), 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, 情報処理学会, 沖縄, 2009 年 4 月 24 日.

６．研究組織
(1)研究代表者
品川　高廣（SHINAGAWA TAKAHIRO）
筑波大学・大学院システム情報工学研究科・講師
研究者番号：40361745