様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 5 月 23 日現在

機関番号：１２１０２
研究種目：挑戦的萌芽研究
研究期間：2010～2012
課題番号：２２６５０００５
研究課題名（和文）　仮想計算機と耐タンパーデバイス用いた競合プログラム実行環境の構築

研究課題名（英文）　Implementing execution environments of conflicting programs by using virtual machines and tamper-resistant devices

研究代表者
新城 靖（SHINJO, Yasushi）
筑波大学・システム情報系・准教授
研究者番号：００２５３９４８

研究成果の概要（和文）：PC で動作するプログラムと遠隔のサーバ上でプログラムは、競合関係にあり、利用者と競合するプログラムを利用者の PC で実行することは、一般的には不可能である。耐タンパー性を持つデバイスで利用者と競合するプログラムを動作させることはできるが、そのようなデバイスの処理能力は非常に低い。この研究では、仮想化技術と耐タンパー性を持つデバイスを用いて利用者が管理する PC で利用者と競合するプログラムを実行する環境を構築する。

研究成果の概要（英文）：Programs running on a PC and programs running on a server compete against each other, and it is generally impossible to run competitive programs on a PC. While it is safe to run competitive programs on a tamper-resistant device, such tamper-resistant devices have very limited computing power. In this research, we have implemented execution environments of competitive programs in a PC by using virtual machines and tamper-resistant devices.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,600,000	0	1,600,000
2011 年度	900,000	270,000	1,170,000
2012 年度	500,000	150,000	650,000
年度			
年度			
総　計	3,000,000	420,000	3,420,000

研究分野：計算機科学
科研費の分科・細目：ソフトウエア
キーワード：オペレーティングシステム、仮想計算機、耐タンパーデバイス、著作権管理、デジタル署名、Trusted Platform Module、Trusted Boot

１．研究開始当初の背景

IC カード等の耐タンパー性を持つデバイス(以下、耐タンパーデバイス)は、電子マネーや利用者認証を実現するために使われている。たとえば、PC にカードリーダを取り付け、Edy 等の電子マネーを使って Web 上で買い物をすることを考える。Web ブラウザは利用者のために動作するプログラムであり、これを協調プログラムと呼ぶことにする。この時、IC カード上で動作するプログラムと Web サーバで動作するプログラムは、通信を行い、カード内のデータとサーバ上のデータ

ベースを変更する。IC カード上で動作するプログラムと Web サーバで動作するプログラムは、利用者とは競合関係にある。このようなプログラムを競合プログラムと呼ぶことにする。

利用者が管理している PC で競合プログラムを実行することは一般的には不可能である。たとえば、もしも利用者の PC で電子マネー機能を持つプログラムを動作させたならば、利用者はデバッガ等を用いて電子マネー・プログラムのデータを覗き見たり改ざんすることができる。IC カード内で競合プログラムを動作させることはできるが、そのようなデバイスの処理能力は非常に低いため、複雑な処理は行えない。たとえば、現在 Web サーバで動作しているプログラムを IC カードで実行することはできない。

２．研究の目的

本研究の目的は、利用者が管理する PC において競合プログラムを実行する環境を構築することである。この目的を達成するために、本研究では仮想計算機と耐タンパーデバイスを組み合わせて用いる。

本研究では、次の 2 つの実行環境を構築する。

1. 協調環境: 従来通り PC の所有者と協調する OS、および、アプリケーションを実行する。耐タンパーデバイス以外の通常のデバイスをアクセスさせる。

2. 競合環境: 競合プログラムを実行する。耐タンパーデバイスのみをアクセスさせる。

PC において、競合プログラムは、競合環境と耐タンパーデバイスの２カ所で実行する。本研究では、まず耐タンパーデバイスから競合環境へオフローディングを実現する。耐タンパーデバイスは、競合環境の完全性と信頼性を確認する役目も持つ。競合環境のプログラムは、最近の高速な CPU で実行されるので、現在の耐タンパーデバイスの処理能力が実質的に数百倍に高速化されることになる。協調環境で動作する利用者用の OS は耐タンパーデバイスの代わりに競合環境で実行される高速なプログラムを利用する。さらに、Web サーバから競合環境へのオフローディングを実現する。これにより、Web サーバの負荷を下げ、高いスケーラビリティを実現しサーバの消費電力を削減する。

３．研究の方法

本研究では、PC 上で動作する中立的な仮想計算機モニタを開発し、それにより１台の PC(ハードウェア) に協調環境と競合環境の２つの実行環境を実現する。ここで中立とは、ハードウェアの CPU と同様に、期待された

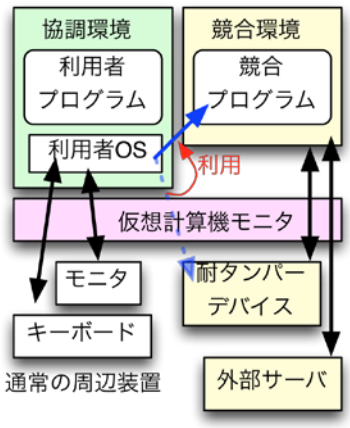

図 1　中立的仮想計算機モニタによる競合環境と競合環境の実現

動作だけを行い、協調環境と競合環境の双方に悪意がある行動をとらないことを意味する。仮想計算機モニタの中立性は、ソースコード公開とバイナリ作成手順の公開、または、信頼できる機関による検査により保証する。さらに、実行時には、協調環境と競合環境の双方からバイナリが改ざんされていないことを検証可能にする。これには、TPM (Trusted Platform Module) と呼ばれる耐タンパーデバイスを用いた Trusted boot の技術を用いる。

中立的仮想計算機は、２つの環境間で通信する機能を提供する。また、競合環境のプログラムは、IC カードや USB デバイス等の外付けの耐タンパーデバイスや外部のサーバと通信できるようにする。これにより、競合環境で利用者と競合するプログラムはこれらのデバイスやサーバと通信しながらサービスを提供することが可能となる。利用者は、この競合するプログラムが提供するサービスを中立的仮想計算機モニタが提供する環境間通信機能を通じて利用する。

４．研究成果

中立的仮想計算機モニタを実現するために、本研究では仮想計算機モニタ BitVisor を用いる。BitVisor は、筑波大学などが中心となって開発したハイパバイザ型の仮想計算機モニタである。BitVisor はハードディスクやネットワークの暗号化などセキュリティを保つために必要なデバイス以外はゲスト OS にそのままアクセスさせる。よって、デバイスドライバとデバイスのエミュレータを仮想計算機モニタ内に持つ必要がない。このため Xen などの他の仮想計算機モニタと比較するとソースコードが小規模で、TCB (Trusted Computing Base)が小さく検証しやすい。

中立的仮想計算機モニタは、協調環境と競合環境の２つの実行環境を生成しなければな

らない。一般の仮想計算機モニタでは、2 つの仮想計算機を生成し、それらを隔離することで、2 つの実行環境を容易に生成することができる。しかし本研究で用いる BitVisor は、1 つのゲスト OS にしか対応していない。そこで本研究では、協調環境を BitVisor 上のゲスト OS を実行するための仮想計算機として実装し、競合環境は BitVisor の拡張機能を用いて実装する。この拡張機能では、独立した ELF(Executable and Linkable Format) 形式のプログラムを保護されたメモリ内で実行することができる。そのプログラムはゲスト OS のメモリをアクセスできないように設定できる。また、BitVisor ではゲスト OS は仮想計算機モニタのメモリ領域にアクセスすることはできない。こうすることでユーザ環境と耐タンパー環境の間でメモリを完全に隔離することができる。

中立的仮想計算機モニタでは、競合環境からのみ特定の外付け耐タンパーデバイスへアクセス可能にする必要がある。BitVisor はデバイスをゲスト OS の環境から隠す機能がある。この機能を利用して耐タンパーデバイスをゲスト OS から隠す。また、BitVisor は USB デバイスやシリアルポート等の一部のデバイスを仮想計算機モニタ本体から利用できる機能がある。この機能を利用して、耐タンパー環境から耐タンパーデバイスへアクセスさせる。また、その他のデバイスについては、ユーザ環境からのみアクセスさせる。

BitVisor は、セキュリティを高めるためのハイパバイザとして開発されてきた。しかしながら、TPM を用いた Trusted Boot には対応していなかった。中立的仮想計算機モニタを実装するためには、TPM を用いた Trusted Boot の機能はどうしても必要である。そこで本研究では、BitVisor に対して TPM を用いた Trusted Boot の機能を付加した。具体的には、TPM を利用するために ROM に保存されているプログラムを呼び出す機能、および、BitVisor の実行後、計測 (measurement) を行い、信頼の連鎖 (chain of trust) を保持しながら次のプログラムに制御を移す機能を付加した。

BitVisor の拡張機能では、通常の TCP/IP による通信機能を利用することができない。BitVisor では、強制的にゲスト OS の通信を VPN (Virtual Private Network) への通信に変換する機能はある。しかし、この機能により拡張機能が外部のサーバと通信することはできない。また仮にそれを可能にしたとしても、利用者が拡張機能の通信先を検証できないという問題が生じる。

この問題を解決するために、本研究では、BitVisor の拡張機能のプログラムがゲスト OS の機能を利用しながら外部のサーバと通信する機能を実現する。この時、ゲスト OS 上で動くプログラムを、ソケットヘルパと呼ぶ。ソケットヘルパは、拡張機能のプログラムからの要求に従って、ゲスト OS の機能を利用して TCP/IP による通信を行なう。この通信の内容は、ゲスト OS のプログラムからも観測可能であり、利用者は、通信先を検証することができる。また、必要ならば、拡張機能のプログラムで SSL (Secure Sockets Layer) 等の機能を用いて暗号化することもできる。これにより、拡張機能のプログラムと外部サーバの間で機密のデータを送受信することもできる。

BitVisor は、仮想計算機モニタ内から USB デバイスをアクセスしたり、ゲスト OS からは隠す機能がある。しかしながら、一般に市販されている USB デバイスを扱うプログラムを BitVisor の拡張機能として動作させるためには、様々な機能が欠落している。それは、USB デバイスのプログラムを開発するためには、OS が標準的に持っている機能を利用するからである。

本研究では、耐タンパー性のある USB デバイスの例として、飛天ジャパン製 Rockey6 という USB デバイスを BitVisor 拡張機能から利用可能にした。Rockey6 は、C 言語のサブセットでプログラムを記述することができる USB デバイスである。Rockey6 には、RSA による暗号化と復号化を行なう機能や、秘密鍵を取り出せない状態で保持する機能がある。Rockey6 のアプリケーションは、Linux、および、Microsoft Windows 上で開発することが想定されている。本研究では、そのうち Linux 用の開発キットに対して BitVisor の拡張機能としてプログラムを記述するため関数を付加した。これにより、BitVisor 拡張機能で Rockey6 を利用するアプリケーションを記述することが可能になった。

本研究では、具体的なアプリケーションとして、次のものを開発した。

- ・デジタル署名
- ・ソフトウェアのコピー保護
- ・動画像配信

デジタル署名アプリケーションは、低速な USB デバイスによるデジタル署名処理を、競合環境で利用可能な高速な CPU と大量のメモリにより高速化するものである。このアプリケーションでは、まず、競合環境において動的に公開鍵と秘密鍵の組を生成する。その公開鍵を、低速な USB デバイスが持つデジタル署名で署名して取り出す。日常的な署名は、競合環境で動的に生成した秘密鍵で高速に行なう。実験の結果、Rockey6 と類似の USB デバイスである飛天ジャパン ePass3003 と比較して、30 倍の高速な署名を行なうことができた。ただし、通常のゲス

ト OS 上のプログラムと比較すると 20 分の 1 の性能しかなく、まだ高速化の余地があることがわかった。その原因は、シリアル通信のオーバヘッド、および、メモリ割り当てライブラリ関数のオーバヘッドが大きいことであると思われる。今後、これらの点を改善して、500 倍以上の高速化を目指す。

ソフトウェアのコピー保護では、特定の USB デバイスがコンピュータに接続されていることを確認し、その時だけ動作することで、不正なコピーを防ぐものである。この時、USB デバイスの中で保護したい重要なアルゴリズムを実行することができる。コピーされたソフトウェアは、USB デバイスが接続されていないので、重要なアルゴリズムが実行できないためにソフトウェアが動作しない。従来の方法では、保護したい重要なアルゴリズムを実行するには USB デバイスが低速であるため、十分な保護を行なうことができなかった。本研究の結果、競合環境で重要なアルゴリズムを実行することができるので、保護する範囲を拡大することが可能となった。

動画像配信アプリケーションは、動画配信サーバから暗号化された動画像データを受信し、それを復号してから画面デバイスに出力するものである。この時問題になるのは、ゲスト OS から画面デバイスをアクセスされると、復号化された後の動画像データが取られてしまうことである。PlayStation 3 では、著作権管理者側が提供した仮想計算機モニタにより DVD 等の著作物をゲスト OS からアクセスできないようにしていた。この手法では、著作物管理は可能であるが、利用者は安心してゲスト OS を利用することができない。それは、仮想計算機モニタという高い権限のプログラムにより、ゲスト OS 内の情報が全て把握されてしまうからである。この手法では、その仮想計算機モニタで利用者が望まないプログラムが動作することを防ぐ手段は存在しない。

本研究では、中立的仮想計算機モニタを用いて、利用者が安心して利用でき、かつ、動画像に対して強固な著作権保護を行なう仕組みを実現した。この仕組みでは、動画像再生プログラムを BitVisor の拡張機能で動作させる。拡張機能には、動画像再生中だけは、画面デバイスを専有させる。これにより、動画像データを保護する。また、拡張機能のプログラムからは、ゲスト OS のメモリへのアクセスを禁止する。これにより、利用者は安心してそのコンピュータを利用可能になる。

本研究では、中立的仮想計算機モニタと耐タンパーデバイスを用いることで、PC 上で利用者とは競合するプログラムを実行するための環境を構築することを提案した。提案手法に基づき、仮想計算機モニタ BitVisor を拡張して中立的仮想計算機モニタを実現した。実現した中立的仮想計算機モニタを用いて、デジタル署名、ソフトウェアのコピー保護、動画配信というアプリケーションを開発し、提案手法の有用性を確認した。また、本研究で開発した BitVisor の TPM を用いた Trusted Boot 機能、および、USB デバイス Rokey6 を利用可能にする関数群は、それら単体でも有用性がある。

今後は、利用者とは競合するプログラムを実行する環境の応用範囲をさらに広げていきたいと考えている。そのために、アプリケーション開発のためのツールキットを整備したいと考えている。また、メモリ管理のオーバヘッドを解消し、さらなる高速化を実現する。

５．主な発表論文等

〔雑誌論文〕（計 2 件）

[1] 小清水 滋, 新城 靖, 板野 肯三, 榮樂 英樹, 松原 克弥: "中立的 VMM による動画像を対象とした著作権保護", 情報処理学会研究会報告,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(OS),2012-OS-123(8), 8 pages (2012). 査読無.

[2] 松下 正吾, 新城 靖, 榮樂 英樹, 松原 克弥, 東 悠: "中立的仮想計算機モニタによる耐タンパーデバイスのアクセラレータの実装", 情報処理学会研究会報告,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 (OS),2011-OS-118(9), 8 pages (2011). 査読無.

〔学会発表〕（計 1 件）

[1] 小清水 滋, 新城 靖, 板野 肯三, 榮樂 英樹, 松原 克弥: "BitVisor による動画像を対象とした著作権保護", 情報処理学会 BitVisor Summit （2012 年 12 月 4 日 筑波大学東京キャンパス、東京都). 査読無.

〔その他〕
ホームページ等
http://www.softlab.cs.tsukuba.ac.jp/

６．研究組織
(1)研究代表者

新城 靖（SHINJO, Yasushi）
筑波大学・システム情報系・准教授
研究者番号：00253948