様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　５　日現在

機関番号：　１５３０１
研究種目：　若手研究(B)
研究期間：　2016～2017
課題番号：　１６Ｋ１６０６７

研究課題名（和文）重要サービスに関するプロセスとファイル情報の不可視化による攻撃回避手法の研究

研究課題名（英文）Research on attack avoidance method for essential services by hiding process information and related files

研究代表者

佐藤　将也（Sato, Masaya）

岡山大学・自然科学研究科・助教

研究者番号：３０７５２４１４

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：計算機への攻撃防止や証拠保全のためのソフトウェアは、無効化された際に被害が拡大する可能性がある。攻撃者の攻撃手順では、予め攻撃対象の計算機で動作しているサービスを特定し、サービスに応じた攻撃が行われる。また、攻撃手段は、応用プログラムだけでなくオペレーティングシステムレベルの攻撃が観測されている。そこで、よりも高い権限を持つ仮想計算機モニタを利用して、重要サービスの特定を困難化する攻撃回避手法を提案した。特に、重要サービスの動作中の情報や関連するファイルへのアクセスを監視し、重要サービスからのみ参照可能とする機構を実現することで、既存の重要サービスの変更なしに、安全性を向上する手法を実現した。

研究成果の概要（英文）：Software for protecting computers or evidence preservation is critical to protecting computers. This software sometimes becomes an attack target because it is an obstacle to attackers. Attackers identify the service on a computer firstly. If the service is found, they disable it and achieve their goals. On the other hand, attackers utilize not only application programs but also an operating system to attack the computer. To address these problems, we propose an attack avoiding method to complicate identification of essential services by a virtual machine monitor. In particular, our method monitors access to running information or related files of essential services and controls the visibility of that information. Our method requires no modification to existing essential services and provides greater security for essential services.

研究分野：　コンピュータセキュリティ

キーワード：　情報セキュリティ　マルウェア対策　仮想化技術

１．研究開始当初の背景

サイバー攻撃の手法は複雑化し高度化しており、その対処の多くは応用プログラム（以降､AP)やオペレーティングシステム(以降、OS）の内部で実現されてきた。しかし、既存研究を適用した機構自体が攻撃され、無力化される可能性がある。このため、不正プログラム（以降、マルウェア）による攻撃を防止する手法を実現しても、各手法へ対処され、無力化される可能性がある。現在の OS の多くは、AP の動作モード（ユーザモード）と OS の動作する強い権限を持つ動作モード（カーネルモード）の 2 種類でしか動作レベルを分けていない。近年、カーネルモードで動作するマルウェア（カーネルモードマルウェア）が観測されていることから、たとえカーネルモードで動作するセキュリティソフトウェアであっても、既存の保護機構は攻撃により無効化される可能性がある。

カーネルモードマルウェアへの対策として、仮想計算機（Virtual Machine、以降、VM）を用いる手法が研究されている。VM は、1 台の計算機上で複数の OS を走行させる仮想化技術により実現されている。VM を提供する基盤ソフトウェアである仮想計算機モニタ（VM Monitor、以降、VMM）は、VM 上の OS よりも高い権限で動作し、VM から独立したソフトウェアである。VMM は、VM から独立したソフトウェアであることから、VMM をセキュリティ技術の実現に応用する研究が行われている。

既存研究の多くは、VM 内のセキュリティ機構を VM 外部に移行することで、セキュリティ機構の安全性を向上している。しかし、既存のセキュリティ機構を VMM に移植するには、VMM や既存のセキュリティ機構の大幅な改変が必要であり、そのコストは大きい。一方で、VM 内で動作する既存のセキュリティ機構を保護する研究は、調査した限りでは少ない。VM 内で動作する既存のセキュリティ機構の安全性を向上する手法を実現できれば、既存ソフトウェアを有効活用しつつ、VM の安全性を向上させることができる。

また、マルウェアによる攻撃に着目すると、攻撃の成功率を向上するために、セキュリティソフトウェアなどの重要サービスを停止する攻撃が存在する。これらの重要サービスの機能が停止すると、攻撃の検知や防止が遅れ、被害が拡大する可能性が高い。サイバー攻撃の手順に着目すると、攻撃者は、攻撃の前段階として攻撃対象の計算機の環境を調査する。調査段階において、重要サービスの存在や種類が特定されると、特定したサービスに応じた攻撃により重要サービスが停止される可能性がある。

以上より、VM 上の重要サービスの存在を攻撃者から不可視化する機構を実現できれば、重要サービスへの攻撃の可能性を低減し、安全性を向上できる。

２．研究の目的

本研究の目的は、VMM を利用して重要サービスの情報を攻撃者から不可視化することで、重要サービスへの攻撃を回避し、VM 上の重要サービスの安全性を向上させることにより、VM の安全性を向上させることである。重要サービスの特定に利用されうる情報には、プロセス情報、重要サービスの関連ファイル、および重要サービスの通信内容の 3 つが考えられる。プロセス情報とは、OS カーネル内でプロセスを管理するために用いられる情報である。関連ファイルは、重要サービスの設定ファイルや走行状態などを管理するファイルを想定している。通信内容は、重要サービスが計算機外部のサービスと連携するために行われる通信を想定している。このうち、本研究では、重要サービスを提供する AP（以降、重要プロセス）について、カーネルが管理する重要プロセスのプロセス情報と重要プロセスの関連ファイルを攻撃者から不可視化する。

具体的には、重要プロセスのプロセス情報へのアクセス制御と重要プロセスの関連ファイルの不可視化の実現を目的とする。これまでに、カーネルが管理する重要プロセスのプロセス情報を不可視化するために、重要プロセス以外が動作している間は偽の情報に置換する手法を提案し、実現してきた。本研究は、さらに安全性を向上させるために、プロセス情報へのアクセスを制限する手法を研究により実現する。具体的には、予め許可したプログラムテキスト以外からプロセス情報へアクセスされたときに、アクセスを検知し、偽の情報に置換する手法を実現する。関連ファイルの不可視化では、関連ファイルを重要プロセスからのみ参照可能とし、他の AP からは不可視のファイルを提供する手法を実現する。また、重要プロセスによる不可視のファイルへのアクセスを他の AP から検知されないアクセス手段を実現する。

３．研究の方法

重要サービスに関する情報の不可視化による攻撃回避手法の研究開発の実現のために、本研究では、以下の項目を研究する。

(1) 重要サービスのプロセス情報に関するアクセス制御の設計、実現、および評価
(2) 重要サービスの関連ファイル不可視化の設計、実現、および評価

以下では、それぞれの項目について、研究の方法および研究の計画を述べる。

(1) 重要サービスのプロセス情報に関するアクセス制御の設計、実現、および評価

重要サービスのプロセス情報へのアクセスを制御する方法を実現する。重要プロセスのプロセス情報を置換する手法をこれまでに実現したものの、攻撃者によりプロセス情報の置換を監視された場合に、重要プロセスを特定される問題があった。そこで、重要プロセスのプロセス情報へのアクセス制御を実

現し、カーネルモードマルウェアによる継続的なプロセス情報の監視からもプロセス情報を不可視化する。具体的には、Intel CPU の機能である Extended Page Table（以降、EPT）を用い、重要プロセスのプロセス情報が配置されるメモリページの読み込みを制御する機構の設計と実現を行う。ここで、アクセスを制御するのは、重要プロセスのプロセス情報が配置されたメモリページのみを対象とし、不要な制御が発生しないようにすることで、性能低下の抑制を目指す。この実現において、VMM として Xen を用い、VM 上の OS として Linux を想定する。これは、Linux のソースコードが公開されており、プロセス情報の管理方法を調査可能であるためである。また、実現において Xen の改修量を抑制する方法を検討する。これは、Xen の改修量が大きくなった際に Xen の改修部分にバグが混入する可能性を低減するためである。VMM のバグは、VMM 上で動作するすべての VM の動作に影響する可能性があるため、VMM へのバグ混入の可能性を低減するために改修量の抑制を目指す。

(2) 重要プロセスの関連ファイル不可視化の設計、実現、および評価

重要プロセスの関連ファイルを不可視化することで、関連ファイルをもとにした重要プロセスの特定を困難にする。重要プロセスの関連ファイルは、その内容を攻撃者に閲覧されることで、重要プロセスを特定される可能性がある。また、内容だけでなく、関連ファイルの存在が攻撃者に察知されるだけで重要プロセスを特定される可能性がある。このため、ファイルの内容だけでなく、ファイルの存在を攻撃者から不可視化する。具体的には、重要プロセスのプロセスから当該ファイルへのアクセス試行があった場合のみ、ファイルの本来の内容を返却し、重要プロセス以外のプロセスから当該ファイルへのアクセス試行があった場合は、ファイルが存在しないように見せかける。

本研究では、VM 上の AP から発行されるシステムコールを検知および制御することでファイルの不可視化を実現する。ファイルへのアクセスは、システムコールを用いて行われるため、システムコールの発行を検知し、VMM によりその実行を制御することで、関連ファイルの可視/不可視を制御する。例えば、重要プロセスが関連ファイルの内容を読みこもうとした場合のみ、関連ファイルの内容を返却し、重要プロセス以外の AP が関連ファイルの内容を読みこもうとした場合は、システムコールを失敗させる。

４．研究成果

(1) 重要プロセスのプロセス情報に関するアクセス制御の設計、実現、および評価

重要プロセスのプロセス情報のアクセスを制御する方法として、EPT を用いた制御方式を実現した。本方式では、重要プロセスが動作する VM を保護対象 VM とし、重要プロセスの制御やアクセス制御の方法を指定するための管理 AP が動作する VM を管理 VM とする。本方式では、まず、初期設定として、管理 AP が重要プロセスを指定する。VMM は、管理 AP による重要プロセスの指定を受け付け、重要プロセスのプロセス情報が配置されるメモリページに対応する EPT エントリの制御ビットを操作することで、重要プロセスのプロセス情報が配置されるメモリページの読み込みを禁止する。次に、保護対象 VM 上で当該ページへのアクセスが発生すると、EPT violation が発生する。この際、EPT violation を VMM が検知する。EPT violation が発生した EPT エントリが、初期設定で指定した EPT エントリであった場合は、本方式により指定したページとして処理し、それ以外の場合は既存の処理を行う。初期設定で指定した EPT エントリであった場合、走行中のプロセスを検査する。走行中のプロセスが重要プロセスであった場合、EPT エントリの制御ビットを操作し、読み込みを許可したうえで、保護対象 VM に処理を返却する。それ以外の場合は、当該ページに配置されたプロセス情報を管理 VM に退避し、偽のプロセス情報に置換したうえで、読み込みを許可し、保護対象 VM に処理を返却する。これにより、重要プロセスから参照した場合のみ、本来のプロセス情報を参照可能な機構を実現した。

本方式を実現するために VMM として Xen を用い保護対象 VM と管理 VM 上では Linux を用いた。本方式では、VMM と保護対象 VM 上の OS を改変した。また、管理 VM 上に管理 AP を実現し、VMM との連携、重要プロセスの指定、およびプロセス情報の退避と復元を行う機構を実現した。保護対象 VM で動作する OS は、一部改変し、プロセス情報がメモリページごとに配置されるようにした。プロセス情報の 1 つであるプロセス管理表のメモリ上への配置方法を図 1 に示す。これにより、ページ単位でのアクセス制御によりプロセス情報へ

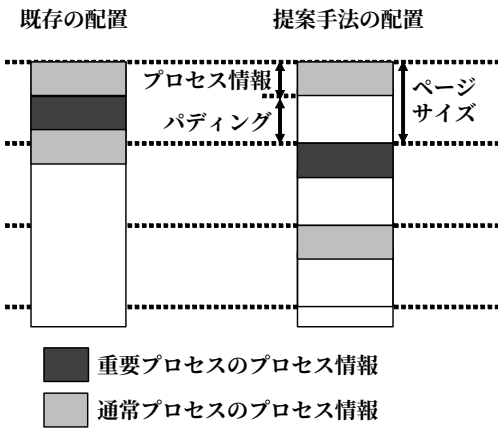

図 1 プロセス情報の配置方法

のアクセス制御を可能にした。ただし、本方式の目的は、保護対象 VM 上のソフトウェアの改変なしに、重要サービスの安全性を向上することである。このため、今後は、保護対象 VM 上のソフトウェアを改変することなく本方式を実現する方法を検討することで、より効果的な手法の実現を目指す。

評価では、重要プロセス以外からはそのプロセス情報を参照できないことを確認した。また、本方式を実現した際の実行性能への影響を明らかにした。

(2) 重要プロセスの関連ファイル不可視化の設計、実現、および評価

重要プロセスの関連ファイルを不可視化する手法を実現した。本手法では、ファイルの不可視化とファイル操作の不可視化を実現した。ファイルの不可視化では、関連ファイルを保護対象 VM とは異なる VM（以降、ファイル提供 VM）に配置する。これにより、保護対象 VM 内からは、仮想的に、計算機外部のファイルとすることで、関連ファイルを不可視化する方式を提案した。ここで、重要プロセスからは、関連ファイルは、保護対象 VM 内のファイルと同様に扱うことができ、他のプロセスからは扱えないようにする必要がある。

そこで、保護対象 VM におけるシステムコールを VMM により監視し、重要プロセスから関連ファイルへのアクセスを検知した際は、システムコールに関する情報をファイル提供 VM 上の代理プロセスに転送し、代理実行させる方式を設計し、実現した。本方式の全体像を図 2 に示す。代理プロセスは、VMM から、システムコールに関する情報（システムコールの引数）、およびファイルアクセスのために要する情報（パス情報など）、重要プロセスのプロセス ID、および保護対象 VM の VM 識別子を受け取る。これらの情報を用い、ファイル提供 VM 上でファイル操作を行う。

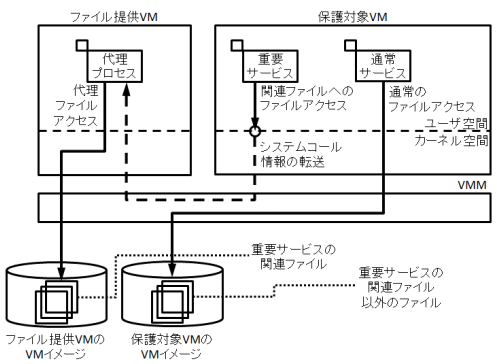

図 2　ファイル不可視化手法の全体像

また、ファイル操作の結果は、VMM を介して代理プロセスから重要プロセスに返却する。さらに、代理実行する際に重要プロセスや保護対象 VM が複数存在する場合を想定し、代理プロセスの割り当てと代理実行依頼の受け取りの周期について、各代理実行依頼を公平に処理するための方式を検討した。これにより、複数の保護対象 VM を走行させた場合でも、特定の保護対象 VM 上の重要プロセスからのファイル操作のみが優先して行われるのではなく、それぞれの操作を公平に実行する方式を実現した。以上より、保護対象 VM 上の重要プロセスから関連ファイルへのアクセスについて、保護対象 VM 上の OS を介さずに、ファイル提供 VM 上の関連ファイルを操作する手法を確立した。

以上より、保護対象 VM 上における重要サービスの関連ファイルをファイル提供 VM に配置することで不可視化し、かつ不可視化したファイルを保護対象 VM 上の重要プロセスから操作する手法を実現した。また、保護対象 VM 上の OS を介さずに関連ファイルを操作する方法を実現することで、保護対象 VM 上の OS からでさえ関連ファイルの操作を監視できない方式を実現した。さらに、ファイル提供 VM 上の代理プロセスへの代理実行依頼について、複数の保護対象 VM 上の重要プロセスからの代理実行依頼を公平に処理する方式を設計し、実現した。また、評価により、実現方式においてできるだけ公平に重要プロセスからの代理実行依頼を実行できることを確認した。

以上(1)と(2)の実現により、VM 上の重要サービスの安全性を重要サービスの改変なしに向上する手法を実現した。研究開始当初の背景で述べたように、既存研究は重要サービスを VM 外部に移行することで安全性を向上しているものの、本研究は既存の重要サービスを改変なしに安全性を向上できる。研究機関終了段階においても、調査した限りでは同様の観点で保護する手法は研究されておらず、新規性の高い方式であるといえる。

５．主な発表論文等

〔学会発表〕（計６件）

① 奥田勇喜、佐藤将也、谷口秀夫、重要サービスの特定を困難化する通信処理制御法、情報処理学会第 80 回全国大会、2018 年 3 月 15 日、東京都・新宿区大久保

② 佐藤将也、山内利宏、谷口秀夫、仮想計算機を用いた重要ファイル保護手法、コンピュータセキュリティシンポジウム 2017（CSS2017）2017 年 10 月 25 日、山形県・山形市

③ 佐藤将也、山内利宏、谷口秀夫、プロセス管理表へのアクセス制御機能の評価、第 78 回コンピュータセキュリティ第 24 回セキュリティ心理学とトラスト合同研究発表会、2017 年 7 月 14 日、東京都・中央区新川

④ Masaya Sato、Toshihiro Yamauchi、Hideo Taniguchi、Memory Access Monitoring and Disguising of Process Information to Avoid Attacks to Essential Services、

3rd International Workshop on Information and Communication Security (WICS2016)、2016 年 11 月 23 日、広島県・東広島市

⑤ 佐藤将也、山内利宏、谷口秀夫、攻撃回避のためのファイル不可視化手法の提案、コンピュータセキュリティシンポジウム 2016 (CSS2016) 2016 年 10 月 11 日、秋田県・秋田市

⑥ 佐藤将也、山内利宏、谷口秀夫、プロセス情報不可視化のための仮想計算機モニタによるメモリアクセス制御機能の評価、第 74 回コンピュータセキュリティ・第 19 回情報セキュリティ心理学とトラスト合同研究発表会、2016 年 7 月 15 日、山口県・山口市

６．研究組織

(1)研究代表者

佐藤　将也　　(SATO, Masaya)

岡山大学・大学院自然科学研究科・助教

研究者番号：30752414