ハイパーバイザによるルートキットの永続化防止

忠鉢洋輔† 品川高廣† 加藤和彦†

1. はじめに

オペレーティングシステム（OS）を乗っ取り，不正なプログラムを実行しユーザに損害を与える手法としてルートキットがある．ルートキットの悪意のある振る舞いとして，OS に対する攻撃に成功した後，OS が再起動されても悪用できるように自身の永続化することが挙げられる．永続化はシステムプログラムや設定ファイルなどを改ざんすることによって行われ，その結果，OS を再起動しても永続化したルートキットが起動する．

このような永続化を行うルートキットに対してハイパーバイザを用いて振る舞いを検知する手法[1] や，ストレージレベルでルートキットの永続化を阻止する手法[2] が提案されているが，OS の保護まで踏み込んでいない，オーバーヘッドが大きいなどの問題がある．本研究では，ハイパーバイザによるファイル保護[3] を用いてルートキットの永続化を防止する手法を提案する．本手法では，OS ファイルとセクタをあらかじめ関連付けることにより，ハイパーバイザによるファイル単位のアクセス制御を可能にする．これにより，OS が攻撃されてルートキットが OS を掌握した場合でも，ハイパーバイザがシステムプログラムや設定ファイルを改ざんから保護することでルートキットの永続化を防止する．

2. システム設計

我々は，準パススルー型ハイパーバイザを用いてストレージ上のファイルを保護する手法を提案する．この手法では OS を仮想マシン上で実行させ，OS のシステムファイルなど重要なファイルに書き込みを試みた際にそれをブロックして，ルートキットの永続化を防ぐ．このシステムによって，ルートキットが OS に侵入しても再起動によりその脅威を取り除くことが可能になる．提案システムの概要を**図 1** に示す．

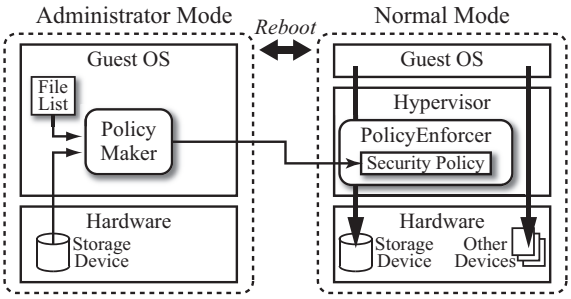

図 1 Administrator Mode と Normal Mode

提案システムは，管理者によって運用され保護に必要な情報の収集や OS の更新等を行う *Administrator Mode* と，ハイパーバイザによる保護が行われる *Normal Mode* の 2 つのモードを切り替えて運用する．*Administrator Mode* では，保護に必要なセキュリティポリシをポリシメーカーで生成する．ポリシメーカーは保護の対象となるシステムファイルのリストを用い，ファイルの属性情報やデータが格納されているセクタ情報と対応させたセキュリティポリシを生成する．*Normal Mode* では，生成したセキュリティポリシを用いてハイパーバイザがストレージデバイスへの I/O をフックし，保護の対象となるファイル領域への書き込みを禁止する．

3. 実　　装

我々は，ポリシメーカーと，ハイパーバイザによるファイル保護の実装を行った．ポリシメーカーは FAT32 を対象として実装を行った．また，ハイパーバイザにはベースに BitVisor[4] を用い，その ATA デバイスドライバを拡張することでファイル保護を実現した．

3.1 ポリシメーカー

ポリシメーカーは FAT32 でフォーマットされたストレージを探索し，与えられたファイル名を元にそのファイルの配置情報と属性情報を列挙するプログラムである．このマッピングにより，ハイパーバイザは

† 筑波大学大学院 システム情報工学研究科 コンピュータサイエンス専攻
Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba

ファイルシステムを理解することなくファイル単位のアクセス制御を行うことができる．FAT32 は，ストレージをクラスタという単位に分割し，File Allocation Table(FAT) というデータテーブルを用いて管理する．また，ファイルのメタ情報をディレクトリエントリと呼ばれる 32byte のデータセットに格納し，同階層のディレクトリエントリをまとめて一つのクラスタに保存している．

ポリシメーカーは，ファイル名を用いて保護対象であるファイルのディレクトリエントリ（32bit）を探索し，ディレクトリエントリが保存されているクラスタ番号と同時に保存する．次に，ディレクトリエントリに存在するデータ領域の先頭クラスタ情報と，File Allocation Table を参照して連鎖しているクラスタ番号を保存する．収集したクラスタをそれぞれセクタの集合に変換したものと，ディレクトリエントリの内容がハイパーバイザのアクセス制御に用いるセキュリティポリシとなる．

3.2 ハイパーバイザによるストレージの改ざん防止

本研究ではハイパーバイザのベースとして BitVisor を用い，その ATA デバイス仮想化機能にストレージ上のファイルの改ざんを防止する機能を実装した．これは，ATA ドライバが ATA コマンドを発行する前に書き込み先のセクタがシステムファイルかどうかをチェックし，システムファイルの改ざんを行う内容の場合，このコマンドを発行せずにエラーを返すことで実現する．また，書き込み先がディレクトリエントリである場合，書き込もうとしているデータをチェックし，保護の対象となるディレクトリエントリが変更されていなければ書き込みを許可する．

4. 実　　験

実装したシステムを用いて，Windows XP SP2 のシステムファイルを保護するためのセキュリティポリシを生成し，その実際のポリシを用いてベンチマークを行った．実験には，OS に Windows XP SP2， BitVisor 0．7 ベースにしたハイパーバイザ，ハードウェアとして Intel Core2 Duo E6850(3．0GHz)， 3GB memory，MTON MSP-SATA7035 SSD によって構成された PC を用いた． CrystalDiskMark 2.2.0 を用いて性能評価を行った結果を**表 1** に示す．このベンチマークでは，保護の対象となっていないフォルダに対してファイルを生成しているため，ディレクトリエントリのチェックのみ行われている．しかし，ディレクトリエントリに関するポリシが非常に少ないため，このオーバーヘッドは BitVisor とその ATA 仮想化によるものと考えられる．

表 1 ディスクベンチマーク

	Windows	+ Hypervisor
Sequential Read	84.2 MB/s	76.6 MB/s
Sequential Write	80.0 MB/s	68.8 MB/s
Random Read (512K)	84.0 MB/s	75.3 MB/s
Random Write (512K)	42．7 MB/s	42.1 MB/s

5. おわりに

本研究で対象とするルートキットの永続化について述べ，また，ハイパーバイザによりそれを防ぐシステムの設計とポリシメーカーとハイパーバイザの実装，その性能の評価を示した．今後は実装の改善や，実際の Rootkit について保護実験を行う予定である．

参 考 文 献

1) Zhang, Y., Gu, Y., Wang, H. and Wang, D.: Virtual-Machine-based Intrusion Detection on File-aware Block Level Storage, *Computer Architecture and High Performance Computing, Symposium on*, Vol. 0, pp. 185–192 (2006).
2) Butler, K. R. B., Mclaughlin, S. and Mcdaniel, P. D.: Rootkit-resistant disks, *ACM Conference on Computer and Communications Security* (Ning, P., Syverson, P. F., Jha, S., Ning, P., Syverson, P. F. and Jha, S.(eds.)), ACM, pp. 403–416 (2008).
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), 情報処理学会, pp. 1–8 (2009).
4) Shinagawa, T., Eiraku, H., Tanimoto, K., Omote, K., Hasegawa, S., Horie, T., Hirano, M., Kourai, K., Oyama, Y., Kawai, E., Kono, K., Chiba, S., Shinjo, Y. and Kato, K.: BitVisor: a thin hypervisor for enforcing i/o device security, *VEE '09: Proceedings of the 2009 ACM SIGPLAN/SIGOPS international conference on Virtual execution environments*, New York, NY, USA, ACM, pp. 121–130 (2009).