連載

5分で分かる!? 有名論文ナナメ読み

佐藤将也（岡山大学）

Garfinkel, T. and Rosenblum, M. :
A Virtual Machine Introspection Based Architecture for Intrusion Detection

NDSS (2003)

侵入検知システム

本稿で紹介する論文では，従来の侵入検知システムが持つ問題点に対処している．そこでまず，侵入検知システムについて簡単に説明する．侵入検知システム（Intrusion Detection System，IDS）とは，その名のとおり，計算機システムへの侵入を検知するためのシステムである．本稿では，IDS は専用の機器ではなく，計算機上のプログラムとして実現されているものとして説明する．皆様もセキュリティソフトウェアを計算機にインストールして利用しているかもしれないが，侵入検知の機能を持つものが多いだろう．IDS は，さまざまな情報をもとに侵入の有無を検知する．これらの情報には，特定のメモリ領域に格納されたデータ，ファイルシステム，および入出力などを含む．IDS は，これらの情報を定期的またはイベント発生を契機に検査し，異常を検知するシステムである．

侵入検知システムの保護

システム管理者は IDS を利用して計算機の安全性を保ち，侵入を検知した際は一部の機能を止めるなどして被害の拡大を防止したり，より詳細な情報を取得して侵入された原因を調査したりする．しかし，侵入された際に IDS が無効化または妨害された場合には，管理者は侵入を検知できず，被害が拡大し顕在化するまで対策できない．そこで，IDS が侵入の被害を受けないことが重要になる．

従来の IDS では，取得できる情報と保護のしやすさがトレードオフの関係にあった．ホストベース IDS（HIDS）では，計算機システム内のプログラムとして IDS を実現しているため，プログラムの動作やイベント発生など詳細な情報を侵入検知に利用できる．しかし，侵入検知システムが攻撃や妨害により無効化される可能性が高く保護が難しい．一方，ネットワークベース IDS（NIDS）は検査対象の計算機とは異なる計算機で実現されており，侵入検知には検査対象のシステムが送受信するパケットなどのネットワーク経由で取得できる情報を利用する．このため，取得できる情報が HIDS よりも限定的である．しかし，検査対象のシステムから隔離されているため，検査対象のシステムが侵入の被害を受けても NIDS が被害を受ける可能性が低い．

本稿で紹介する論文では，HIDS のように詳細な情報が取得可能かつ NIDS のように侵入の被害を受けにくい手法として，仮想計算機モニタを用いた検査手法として Virtual Machine Introspection（VMI）を提案している．本稿では仮想計算機モニタを簡単に説明した後に，VMI を解説する．

仮想計算機モニタ

仮想計算機モニタ（Virtual Machine Monitor（VMM））は，仮想計算機（Virtual Machine（VM））を提供するための基盤ソフトウェアである．VMM は計算機のハードウェアを抽象化して VM に提供する．これにより，たとえば 1 台の計算機で複数の VM を走行させることもできる．VMM はこの機能を提供するために，VM で実行される特定のイベントを検知

して，ほかのVMやプログラムへ影響が及ばないように介入し制御する．たとえばVMMは，2つのVMが利用するメモリがお互いに重複しないように，ページテーブルに関する操作を検知する．また，VMごとに異なるディスク領域を利用するように，ハードウェアに対する要求を検知する．このように，VMMはVM上で発生するさまざまなイベントを検知できる．また，計算機を抽象化してVMに提供するため，VMMはVMよりも高い権限で動作する．さらに，VMMからはVM内部の情報を取得したり，場合によってはVMを一時的に停止させたりできる．以上のことから，VMMは，VMに対してHIDSを実現するために必要な情報の取得に利用できる．一方で，VM-VMM間やVM-VM間は隔離されている．

仮想計算機モニタを用いた侵入検知

VMIは，VMMが持つ「隔離」，「検査」，および「介入」の特性を利用することで，詳細な情報が取得可能かつ検査対象へ侵入されても，IDS自体へ被害が及ぶ可能性を低減した検査手法である．本稿で紹介する論文では，図-1に示すように，検査対象のVM，VMM，およびIDSが動作する環境を想定している．VMIを実現するためにVMMを一部改変し，IDSと連携するための機能が追加されている．IDSは，VMMへコマンドを送信し，VMMはコマンドに応じてVMを検査する．IDSから検査対象のVMを監視する際の問題として，セマンティックギャップがある．VMMが観測できるのは検査対象のハードウェアをもとにした情報であるため，その内部をどのように解釈すればよいかは分からない．たとえば，IDSがVMMを介して，検査対象のVM上の特定のプログラムの情報を取得しようとしても，どのメモリ領域を参照すれば目的のデータを取得できるか分からない．このため，IDSは検査対象のVMで動作するOSのメタデータを保持しておき，レジスタなどの実行状態の情報をもとに参照する領域を決定し検査する．

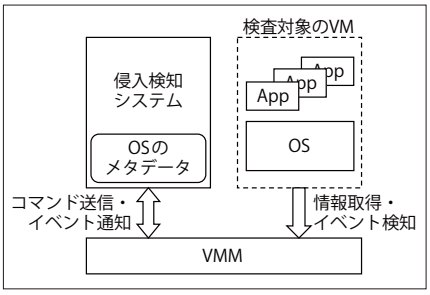

図-1　仮想計算機モニタを用いた侵入検知

本稿で紹介したようなVMMを利用したセキュリティ機能が数多く提案されている理由の1つは，VMMがセキュリティ機能を実現するうえで非常に強力であるためである．これは，VMMはVMをさまざまなタイミングで検査でき，さらに一時的にVMの動作を止めたり特定の処理をスキップさせたり，さまざまな操作が可能だからである．一方で，VMMによるセキュリティ機能を想定した攻撃もあり，攻撃と防御の双方が複雑化している．

VMはさまざまな場所で利用されており，近年ではCPUによる仮想化支援機能の発達により多くの計算機で気軽に利用できる．また，VMを前提としたセキュリティ機能が多く研究されており，実用化されている．セキュリティ機能は利用者の利便性を損なわず，かつ，安全性を向上する必要があり，日々改良が重ねられている．本稿で紹介した論文は基礎的だが強力な手法を提案したものである．近年ではVMを前提として，より強力かつ利便性を損なわない手法が多く提案されており，ソフトウェアだけでなくハードウェアの機能を駆使したものも多く，非常に興味深い．本稿をきっかけにVMを利用したセキュリティに興味を持っていただければ幸いである．

(2020年9月1日受付)

佐藤将也（正会員） sato@cs.okayama-u.ac.jp

2014年岡山大学大学院自然科学研究科博士後期課程修了．2013年日本学術振興会特別研究員（DC2）．現在，岡山大学大学院自然科学研究科助教．博士（工学）．コンピュータセキュリティ，仮想化技術に興味を持つ．