リファレンスモニタの多重化に関する研究

川崎 仁嗣 † 鈴木 勝博 † 阿部 洋丈 ‡ 加藤 和彦 †

1. はじめに

近年、セキュリティの問題についてニュースなどで取り上げられるようになってきた。例えば、Web サーバにバグがあり、悪意のあるユーザが特殊なリクエストを送るとサーバプログラムが誤動作し、サーバの権限で何でもできる状態にしてしまう攻撃（サーバを乗っ取る攻撃）などがある。このような脅威に対し、サンドボックスと呼ばれる一部の環境を全体の環境から隔離するシステムや、IDS (Intrusion Detection System) と呼ばれる攻撃を検知して処置を行うシステムなど（以降、防御用システム）を用いる事でほとんどの場合防ぐことができる。防御用システムにはホストの外部で動作するものと内部で動作するものがある。

防御用システムを多段にすることは普通に行われている。ホストの外側で動作する防御用システムはチェーン状につなげる事で容易に多段にすることができる。それに対し、リファレンスモニタを用いたホスト内のシステムは一般的に多重化可能なようには設計されていない。監視対象となるプロセスの動きを見張り、動作の許可や棄却を行う部分をリファレンスモニタと呼ぶ。先に述べたサンドボックスや IDS はリファレンスモニタの技術を利用して実装可能である。

また、多重化の実装（提案手法の項で詳細を述べる）には大きなオーバヘッドを伴うという問題がある。本研究では多重化できるリファレンスモニタを設計すると共に、オーバヘッドをなるべく増やさずに、多重化が可能なシステムの構築を目指す。

2. 基本事項

2.1. 侵入検知システム(IDS)

侵入検知システムは悪意のある攻撃によってシステムが乗っ取られたり、誤動作させられたりすることを防ぐ機構である。IDS はネットワーク型とホスト型の 2 種類に大別できる。

2.1.1. ネットワーク型 IDS

ネットワーク型 IDS とは、ホストに送られるネットワークのパケットを監視し、異常なパケットの流れを検知すると通信を遮断し管理者に報告するなどの処置を行うシステムである。

監視にかかるコストの制約から、ネットワーク型 IDS の多くはサービスを提供するホストの外に設置されるため本研究の対象とならない場合が多い。

2.1.2. ホスト型 IDS

ホスト型 IDS とはホスト内で動作し、ファイルの状態や、動作しているプログラムを監視し、プログラムの異常な動作を検知するとプログラムを停止させるなどの処置を行うシステムである。

2 つの IDS の違いを簡単に述べる。例えば Web サーバに悪質なリクエストを送って誤動作させ、シェルプログラムを起動させるような攻撃を考える。ネットワーク型 IDS では攻撃者が送信した「悪質なリクエスト」を検知し処置を行う。それに対しホスト型 IDS ではシェルを起動させるという「本来 Web サーバが行わない動作」を検知し処置を行うという違いがある。

本研究ではホスト型 IDS の実装に当研究室で開

† 筑波大学システム情報工学研究科
University of Tsukuba, Graduate School of Systems and Information Engineering.
‡ 科学技術振興機構
Japan Science and Technology Agency

発された IDS [1] を用いる。

2.2. サンドボックス

ホスト内の一部の環境のみを隔離し、内部で起こる事象による影響を外に及ぼさないようにするシステムである。主に信頼できないプログラムなどを隔離して実行するときに用いる（図 1）。

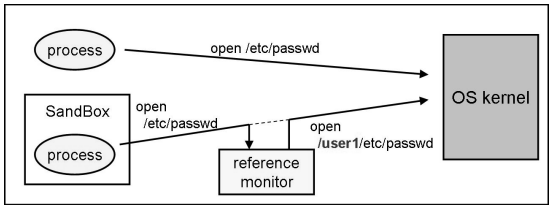

図 1　サンドボックス

先と同様に Web サーバに悪質なリクエストを送って乗っ取る例を考える。サンドボックスを利用すると、Web サーバへの攻撃が成功し乗っ取られても、攻撃者はサンドボックスの外へ出られない。Web サーバを閉じ込めているサンドボックス内に重要なデータを置かないようにすることで、攻撃者からデータを守ることができる。

本研究では、サンドボックスの実装に当研究室で開発している SoftwarePot [2] を用いる。

3.　提案手法

リファレンスモニタの実装手法としては、プロセス状態監視用のシステムコール（ptrace）や LSM（Linux Security Module） の利用、またはシステムコールテーブルの書き換えなどが挙げられる。本研究では、プロセス状態監視用のシステムコールを利用してリファレンスモニタを実装した。その理由として、ユーザモードで実行可能なこと、UNIX 系 OS に広く採用されていることが挙げられる。

ptrace を用いたリファレンスモニタの場合、監視している空間内で ptrace は使えない。つまり、監視する側と監視される側の関係が 1 対 n である。例えば、サンドボックスが監視を行っているプロセスに対して、IDS は監視を行うことが出来ない。

多重化を行うためのアイデアとして ptrace をエミュレーションする実装が考えられる。これにより、監視する側と監視される側の関係が n 対 1（または n 対 n）であっても正常に動作させることが可能である。エミュレーションによるリファレンスモニタを用い、サンドボックス内でホスト型 IDS を動作させたときを考えると、図 2 のような状態になる。

図 2 ではあるプロセスを監視している IDS のプロセスを、さらにサンドボックスのプロセスが監視する。

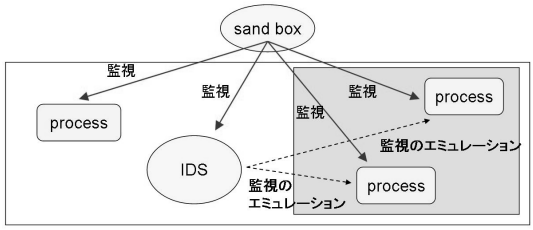

図 2　プロセス監視のエミュレーションによる多重化

参　考　文　献

[1] 阿部 洋丈, 大山 恵弘, 岡 瑞起, 加藤 和彦, “静的解析に基づく侵入検知システムの最適化”, 情報処理学会論文誌 第 45 巻 SIG 3 (ACS 5), pp. 11-20, March 2004.

[2] 大山 恵弘, 神田 勝規, 加藤 和彦, “安全なソフトウェア実行システム SoftwarePot の設計と実装”, コンピュータソフトウェア, 日本ソフトウェア科学会, Vol. 16, No. 6, pp.2-12, November 2002.