Intel SGXとSCONEを用いた既存IDSの安全なオフロード

河村 拓実[1]　光来 健一[1]

1. はじめに

近年，仮想マシン（VM）を提供するIaaS型クラウドが普及しているが，VMはインターネット経由で攻撃を受けやすい．そのため，侵入検知システム（IDS）を用いてVMの監視を行う必要がある．IDSをVM内で動かした場合，攻撃者に侵入されてしまうとIDSが無効化される恐れがあるため，IDSをVMの外で実行するIDSオフロードという手法が用いられている．これにより，攻撃者はVMに侵入してもIDSを攻撃できなくなるが，まだIDSがクラウド外部の攻撃者やクラウドの内部犯から攻撃を受ける恐れがあるため，オフロードしたIDSを保護する必要がある．そこで，CPUのセキュリティ機構であるIntel SGXを用いてオフロードしたIDSを保護し，安全にVMを監視可能にするシステム[1]が提案されてきた．しかし，IDSの開発にはOSカーネルレベルのプログラミングが必要となる上に，エンクレイヴ内ではSGX向けに用意されたライブラリを使わなければならないという問題点がある．

本稿では，Intel SGX向け実行環境SCONE[2]を用いて既存のIDSをエンクレイヴ内にオフロード可能にするシステムSCwatcherを提案する．

2. クラウドにおける安全なIDSオフロード

IDSオフロードを行う場合，オフロードしたIDSは監視対象VMのメモリを解析し，OSが管理しているデータを取得することで監視を行う．例えば，監視対象VMのネットワーク接続状況を取得することで不正な通信を検知することができる．しかし，IDSオフロードを用いてもなお，クラウド外部の攻撃者からオフロードしたIDSが攻撃を受ける恐れがある．また，オフロードしたIDSを実行するクラウド内に内部犯がいる可能性もある．IDSが攻撃を受けた場合，IDSが取得した監視対象VMの機密情報が盗まれる危険性がある．

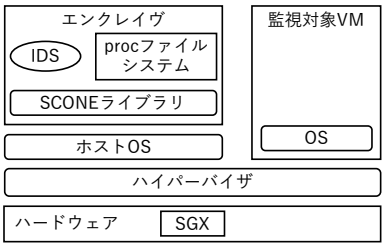

図 1　SCwatcherのシステム構成

この問題を解決するために，Intel SGXを用いてオフロードしたIDSを安全に実行可能にするシステムSGmonitor[1]が提案されている．SGXは，Intel製CPUに搭載されているセキュリティ機構である．SGXを用いることでメインメモリ上にエンクレイヴと呼ばれる保護領域を作成し，この中で安全にアプリケーションを実行することができる．SGmonitorでは，オフロードしたIDSをエンクレイヴ内で実行することで，IDSの改竄や監視対象VMから取得した情報の漏洩を防ぐ．

しかし，SGmonitor上で動作するIDSの開発は一般の開発者には難しい．オフロードしたIDSは標準的なOSインタフェースを用いることができないため，OSカーネルレベルのプログラミングが必要になるからである．そのため，アプリケーションレベルで開発された既存のIDSを動かすこともできない．また，エンクレイヴ内で動作するIDSの開発には，SGX向けに提供されているSDKを用いる必要があるため，標準的に用いられているライブラリを利用することができない．

3. SCwatcher

SCwatcherは，SGX向け実行環境であるSCONE[2]を用いてエンクレイヴ内にオフロードしたIDSに標準的なOSインタフェースを提供する．**図 1**にSCwatcherのシステ

[1] 九州工業大学
Kyushu Institute of Technology

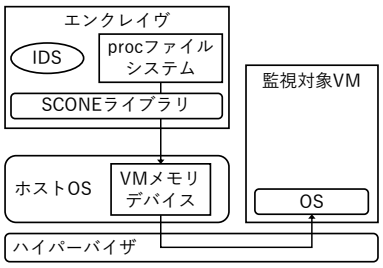

図 2 OS データの取得

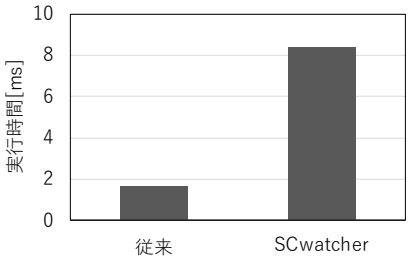

図 3 netstat の実行時間

ム構成を示す．SCONE は既存のアプリケーションを SGX を用いて安全に実行するための実行環境である．SCONE のライブラリがエンクレイヴ内のアプリケーションに標準 C ライブラリのインタフェースを提供する．SCwatcher は，IDS の多くがシステム情報を取得するために利用している proc ファイルシステムをエンクレイヴ内で動かす．この proc ファイルシステムは信頼できるハイパーバイザを経由して監視対象 VM のメモリにアクセスし，OS データを取得して IDS へ提供する．これにより，IDS は標準的な OS インタフェースを用いて監視対象 VM のシステム情報を得ることができる．

エンクレイヴ内の proc ファイルシステムは，SGX の機能を用いてエンクレイヴ外のハイパーバイザを呼び出すことで監視対象 VM の OS データを取得する．しかし，ソースコードが公開されていない SCONE にこのような機能を追加するのは難しい．そこで，**図 2** に示すようにエンクレイヴが動作しているホスト OS 内に，監視対象 VM のメモリへのインタフェースを提供する VM メモリデバイスを用意する．proc ファイルシステムが OS データを取得する際には，SCONE の非同期システムコール機能を利用してこの VM メモリデバイスにアクセスするようにする．VM メモリデバイスは，ハイパーバイザを呼び出して監視対象 VM の OS データを取得し，エンクレイヴ内の proc ファイルシステムへ返す．この時，取得した OS データは信頼できない VM メモリデバイスに渡される前にハイパーバイザ内で暗号化し，エンクレイヴ内で復号する．

IDS がホスト OS の proc ファイルシステムではなく，エンクレイヴ内の proc ファイルシステムにアクセスするように，SCwatcher はコンパイル時に IDS をプログラム変換する．fread などの標準ファイル関数を SCwatcher 用の関数に置き換えることで，必要に応じてエンクレイヴ内の proc ファイルシステムを呼び出すようにする．

4. 実験

SGX 仮想化をサポートした Xen-SGX に SCwatcher を実装し，既存の netstat コマンドを実行してその実行時間を測定した．netstat は，proc ファイルシステムから取得した情報を基にネットワークの接続状況を表示するコマンドであり，IDS から呼び出して使われることが多い．比較のために，エンクレイヴを用いない従来の手法でも同様に実行時間を測定した．実験の結果，SCwatcher を用いた netstat で監視対象 VM のネットワーク接続状況を正しく取得できていることが分かった．実行時間は，**図 3** に示すように SCwatcher が従来の手法の 5.0 倍となった．

SCONE のオーバヘッドを詳細に分析するために，エンクレイヴ内の proc ファイルシステムが VM メモリデバイスにアクセスする際に用いる pread システムコールの実行時間を測定した。SCONE を用いない場合の実行時間は約 2μs となり、SCONE を用いた場合は 3μs から 300μs の値をとった。同様の実験を VM を用いずに行ったところ、SCONE を用いた場合は 3μs から 300μs の値をとったが、VM 内で実行した場合と比べて 4μs 以上の値が出る頻度は極めて低かった。このことから，仮想化の影響により SCONE のオーバヘッドが大きくなってしまっている可能性があることが分かった．

5. まとめ

本稿では，オフロードした IDS を Intel SGX 向け実行環境である SCONE を用いて安全に実行可能にするシステム SCwatcher を提案した．監視対象 VM のシステム情報を取得可能にする proc ファイルシステムを IDS に提供することにより，IDS が標準的な OS インタフェースを用いて VM を監視することができる．

今後の課題は，SCONE を用いて pread システムコールを実行するオーバヘッドを削減することである．仮想化システムを Xen-SGX から KVM-SGX に変更すると改善する可能性がある．また，実際に様々な既存 IDS を実行できるようにすることも今後の課題である．

参考文献

[1] 中野智晴，光来健一：Intel SGX を用いた VM のメモリとディスクを安全な監視，コンピュータセキュリティシンポジウム 2019 (2019)

[2] Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., Lind,J., Muthukumaran, D., O'Keeffe, D., Stillwell, M., Goltzsche, D., Eyers, D., Kapitza, R., Pietzuch, P., Fetzer, C.: Secure Linux Containers with Intel SGX, *Proceedings of the 12th USENIX Symposium on Operating System Design and Implementation*, pp. 689-703 (2016).