平成 30 年度 卒業論文概要			
所　　属	機械情報工学科	指導教員	光來 健一
学生番号	15237032	学生氏名	篠原 悠介
論文題目	Intel SGX とライブラリ OS を用いた IDS オフロード		

1　はじめに

近年，ネットワーク経由でユーザに仮想マシン (VM) を提供する IaaS 型クラウドの普及が進んでいる．VM の安全性を確保するために侵入検知システム (IDS) による監視が行われているが，VM に侵入されると IDS が無効化される恐れがある．IDS に対するこのような攻撃を防ぐために，IDS を監視対象 VM の外側で実行する手法である IDS オフロードが用いられている．一方，IDS オフロードを用いてもクラウド管理者やクラウド外部からの IDS への攻撃は防ぐことができない．そこで，CPU のセキュリティ機構である Intel SGX を用いた SGmonitor[1] と呼ばれるシステムが提案されている．SGmonitor は SGX によって作成される保護領域 (エンクレイヴ) 内で IDS を実行することにより IDS への攻撃を防ぐ．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であり，既存の IDS を動かすのは難しい．

本研究では，エンクレイヴ内でライブラリ OS を用いることにより既存の IDS を安全にオフロードすることのできる GLvisor を提案する．

2　クラウドにおける安全な IDS オフロード

VM を用いた IDS オフロードは，図 1 のように IDS を監視対象 VM の外で動作させて VM の監視を行う手法である．IDS をオフロードすることにより，攻撃者が監視対象 VM に侵入したとしても IDS を無効化される恐れはない．IDS は監視対象 VM 内で動作させる場合とは異なり，VM のメモリを解析して OS が管理しているデータを取得する．例えば VM 内のネットワーク情報を取得することにより，不正な通信が行われていないかを検知することができる．しかし，IDS オフロードを行ってもまだオフロードした IDS が攻撃を受ける可能性がある．オフロードした IDS はクラウド管理者の管理下に置かれるが，クラウドの管理者は必ずしも信頼できるとは限らないためである．また，クラウド外部の攻撃者によって IDS が直接攻撃されてしまう恐れもある．IDS が攻撃を受けると IDS が取得した VM 内の機密情報を盗まれる可能性がある．

そこで，Intel SGX を用いて IDS を保護することにより，VM を安全に監視するシステム SGmonitor が提案されている．

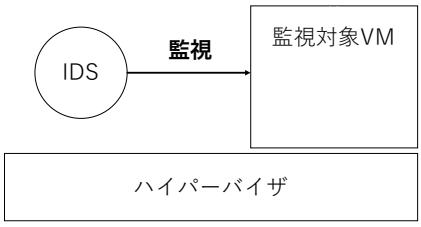

図 1　IDS オフロード

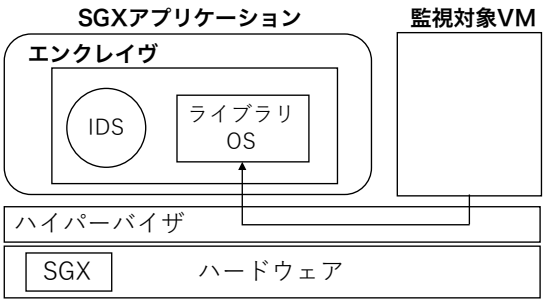

図 2　GLvisor のシステム構成

る．SGX はエンクレイヴと呼ばれる保護領域の中でプログラムの安全な実行を可能にする CPU 機構である．SGmonitor は IDS を SGX アプリケーションとして作成し，エンクレイヴ内で IDS を実行する．SGX によってエンクレイヴのメモリの整合性が保証されるため，IDS の改ざんを防ぐことができる．また，エンクレイブのメモリは暗号化されるため，IDS が取得した VM 内の機密情報の漏洩も防ぐことができる．

しかし，SGmonitor で動作する IDS を開発するのは容易ではない．OS カーネル内のデータ構造を用いて OS カーネルレベルのプログラミングを行う必要があるためである．これはアプリケーションレベルのプログラミングに比べて難しく，OS カーネルのバージョンにも大きな影響を受ける．OS の提供するインタフェースを利用できないため，既存の IDS を動作させることはできない．これまでに既存の IDS をオフロードするためのシステムも提案されてきたが，エンクレイヴの中では利用することができない．

3　GLvisor

本研究では，Intel SGX とライブラリ OS を用いて既存の IDS を安全にオフロードすることを可能にするシステム GLvisor を提案する．GLvisor は，エンクレイヴ内でライブラリ OS と呼ばれる軽量な OS を動作させ，IDS に対して OS インタフェースを提供する．ライブラリ OS は通常の OS とは異なり，アプリケーションごとにリンクされるライブラリである．ライブラリ OS を用いることにより，アプリケーションレベルのプログラミングで IDS を開発することができる．シェルを動作させることもできるため，IDS をシェルスクリプトで記述することもできる．そのため，多くの既存の IDS を動作させることが可能となる．

図 2 に GLvisor のシステム構成を示す．エンクレイヴ内で IDS とライブラリ OS が動作し，IDS は VM の監視に必要な情報をライブラリ OS 経由で取得する．ライブラリ OS は SGX の機構を用いてエンクレイヴの外部のプログラムを安全に呼び出し，ハイパーバイザと通信を行うことで監視対象 VM

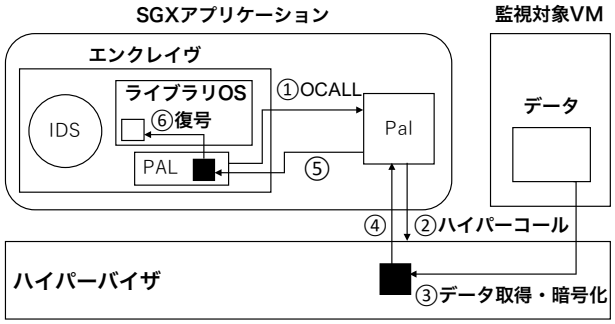

図 3　VM 内の OS データの取得

の情報を取得する．

3.1　VM 内のシステム情報を提供するライブラリ OS

GLvisor は，Graphene-SGX[2] をベースに開発したライブラリ OS を提供する．Graphene-SGX は SGX に対応した Linux 互換のライブラリ OS である．ライブラリ OS の下には Platform Adaptation Layer (PAL) と呼ばれる層があり，エンクレイブ外部にある PAL と通信することで，OS の機能を実現する．ライブラリ OS は IDS に対してシステムコールのインタフェースおよび proc ファイルシステムと呼ばれる特殊なファイルシステムを提供する．proc ファイルシステムは疑似的なファイルを介してシステムの情報を返す．従来の Graphene-SGX は SGX アプリケーションが動作しているシステムの情報を返していたが，GLvisor ではその代わりに監視対象 VM の情報を返す．

3.2　VM 内の OS データの取得

IDS に監視対象 VM 内のシステム情報を提供するために，GLvisor は図 3 のように VM から OS データを取得する．まず，ライブラリ OS がエンクレイヴ内の PAL を呼び出し，PAL は OCALL と呼ばれる SGX の機構を用いてエンクレイヴ外部の PAL を呼び出す．次に，外部 PAL はハイパーコールと呼ばれる機構を用いてハイパーバイザを呼び出す．ハイパーバイザは指定された OS データの仮想アドレスを対応する物理アドレスに変換し，VM のメモリ上の OS データを取得する．情報漏洩を防ぐために，データはハイパーバイザ内で暗号化する．暗号化されたデータは PAL に渡され，エンクレイヴ内のライブラリ OS で復号される．

GLvisor では，LLView[3] を用いてライブラリ OS の中で VM 内の OS データを扱うプログラムのコンパイルを行う．これは VM 内の OS データを必要とするたびに明示的に PAL を呼び出すプログラムを記述することなく，透過的に監視対象 VM の情報を取得させるためである．LLView はプログラムがメモリからデータを読み込む際に，必要に応じて監視対象 VM のメモリからデータを取得するようにプログラムを変換する．これにより，監視対象 VM 内の OS のソースコードを利用してライブラリ OS の機能を開発することができる．

3.3　提供するシステム情報

GLvisor の proc ファイルシステムは CPU 情報を返す cpuinfo ファイルと，TCP や UDP の情報を返す net/tcp, net/udp ファイルを提供している．CPU 情報としては，CPU 番号，種類，モデル番号などの情報を返す．これらの情報は Linux の cpuinfo_x86 構造体から取得することができる．CPU 情報は Meltdown などの CPU 固有の脆弱性を調べるために利用される．また，TCP の情報としては，接続元と接続先の IP アドレス，ポート番号の情報などを返す．この情報は Linux の sockaddr_in 構造体から取得することができる．UDP も TCP と同様に sockaddr_in 構造体から情報を取得する．ネットワーク情報はネットワーク経由での攻撃を調べるために利用される．

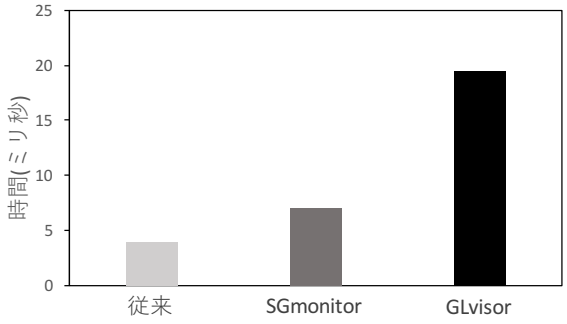

図 4　CPU 情報の取得時間

4　実験

GLvisor を用いて監視対象 VM 内の CPU の情報を取得する IDS を実行し，取得時間を測定した．比較として SGmonitor を用いた場合と，従来手法を用いた場合の取得時間をそれぞれ測定した．実験には Intel Xeon E3-1225v5 の CPU，8GB のメモリを搭載したマシンを使用し，仮想化ソフトウェアには SGX をサポートしている Xen-SGX 4.7 を使用した．

VM 内の CPU の情報の表示にかかった時間を 10 回測定した時の平均を図 4 に示す．GLvisor を用いてデータを取得した場合，SGmonitor での取得時間と比較すると 2.8 倍の時間がかかった．これはエンクレイヴ内でライブラリ OS を動かすオーバヘッドが原因だと考えられる．このオーバヘッドは一度のハイパーコールでより多くのデータを取得し，ハイパーコールの回数を減らすことで削減できると考えられる．一方，従来手法と比べると 4.9 倍の取得時間となり，データの暗号化・復号化のオーバヘッドも大きかった．

5　まとめ

本研究では，Intel SGX とライブラリ OS を用いて IDS を安全にオフロードすることを可能にする GLvisor を提案した．GLvisor では，ライブラリ OS が IDS に OS インタフェースを提供し，proc ファイルシステム経由で監視対象 VM 内のシステム情報を返す．今後の課題は，シェルスクリプトで記述された IDS を含めて，既存の IDS を実際に実行できるようにすることである．

参考文献

[1] 中野智晴, 光来健一. クラウドにおける Intel SGX を用いた VM の安全な監視機構. 第 142 回 OS 研究会, 2018.

[2] C. Tsai, et al. Cooperation and Security Isolation of Library OSes for Multi-Process Applications. EuroSys 2014.

[3] 植木あずさ. LLVM の中間表現を用いた IDS オフロードの開発支援. 九州工業大学卒業論文, 2015.