平成 29 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	14237058	学生氏名	中野 智晴
論文題目	Intel SGX を用いた仮想マシンの安全な監視機構		

1　はじめに

近年，ユーザにネットワーク経由で仮想マシン（VM）を提供する IaaS 型クラウドの普及が進んでいる．その一方で，クラウド内の VM はインターネット経由で様々な攻撃を受けやすいという問題がある．そのため，侵入検知システム（IDS）を用いて VM を監視し，VM の安全性を確保することがますます重要となっている．IDS は監視対象の VM 内で動作させるのが一般的であるが，VM に侵入されると無効化される危険性がある．そこで，IDS を監視対象 VM の外側で実行する IDS オフロードと呼ばれる手法が提案されている．IDS オフロードを用いることにより，攻撃者が監視対象 VM に侵入したとしても IDS を無効化することはできなくなる．しかし，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，IDS オフロードを用いても管理者による IDS への攻撃を防ぐことはできない．また，オフロードした IDS に対してクラウド外部から攻撃が行われる可能性もある．その結果，オフロードした IDS が取得した VM 内の機密情報を管理者や攻撃者に盗まれる恐れがある．

本研究では，Intel SGX を用いて IDS を安全に実行し，正しい IDS だけが VM 内の情報を取得できるシステム SGmonitor を提案する．

2　クラウドにおける IDS オフロード

IDS オフロードは図 1 のように，IDS を監視対象 VM の外部で動作させて，VM 内部のシステムの監視を行う手法である．IDS オフロードを用いることにより，監視対象 VM に侵入されたとしても VM 内で IDS は動作していないため，無効化される危険はない．オフロードした IDS は監視対象 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ことで，監視対象 VM 内で動作させた場合と同様にシステムの監視を行い，攻撃を検知することができる．例えば，VM 内で実行されているプロセスの一覧を取得することにより，不正なプログラムが実行されていないかをチェックすることができる．

しかし，IDS オフロードを行ったとしても，まだ 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おかれるが，クラウドの管理者は必ずしも信頼

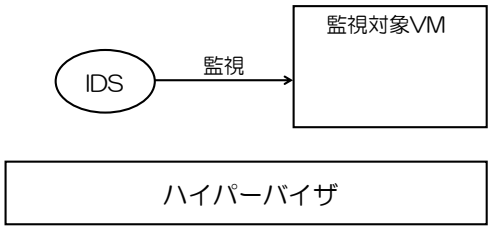

図 1　IDS オフロード

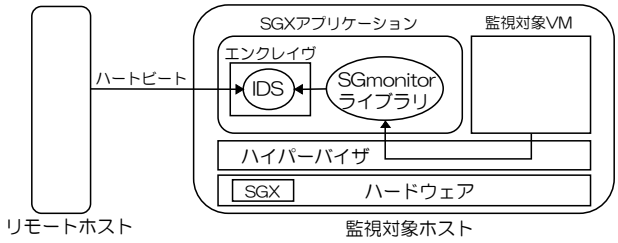

図 2　SGmonitor のシステム構成

できるとは限らない．そのため，クラウドの管理者によってオフロードした IDS が攻撃される危険性がある．また，外部の攻撃者によってオフロードした IDS への攻撃が行われる危険性もある．その結果，オフロードした IDS が取得した VM 内の機密情報を盗まれる恐れがある．

これらの問題を解決するために，VM の下で動作するハイパーバイザを信頼して，オフロードした IDS を安全に実行する手法が提案されてきた．しかし，いずれの手法も管理やセキュリティ，性能の面で問題があり，実用的に利用するのが難しい．例えば，ハイパーバイザ内で IDS を動作させる手法が提案されているが，ハイパーバイザ内で動作する複雑な IDS を開発するのは難しく，IDS を更新する際には再起動が必要になる．また，ユーザが管理する別の VM に IDS をオフロードする手法もあるが，その VM が攻撃を受ける危険性がある．

3　SGmonitor

本研究では，Intel SGX を用いて IDS を保護することにより，VM を安全に監視できるようにするシステム SGmonitor を提案する．Intel SGX は，エンクレイヴと呼ばれる保護領域を用いてプログラムの安全な実行を保証する CPU の機構である．エンクレイヴで IDS の実行を開始する際には SGX によってプログラムの電子署名が検査されるため，攻撃者が改ざんした IDS を実行することはできない．また，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，実行中に IDS を改ざんすることもできない．それに加えて，エンクレイヴのメモリは暗号化されるため，IDS が取得した監視対象 VM 内の情報が漏洩することもない．ただし，攻撃者が IDS の実行を停止することは防げないため，クラウド外部のホストからハートビートを送ることで IDS の正常な動作を確認する．

図 2 に SGmonitor のシステム構成を示す．IDS は SGX アプリケーションとして作成され，従来の IDS オフロードと同様に監視対象 VM が動作しているハイパーバイザ上で実行される．SGX アプリケーションはエンクレイヴと SGmonitor ライブラリで構成され，エンクレイヴ内の IDS はライブラリを介してハイパーバイザとの通信を行う．SGmonitor では，監視対象ホストのハイパーバイザとハードウェアおよび，ハー

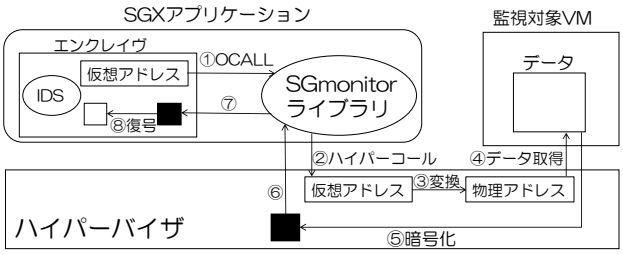

図 3　VM 内の OS データ取得

トビートを行うリモートホストを信頼する．一方で，IDS を動作させる OS などの実行環境や SGX アプリケーション内のライブラリは信頼しない．

3.1　VM 内の OS データの取得

エンクレイヴ内の IDS は監視対象 VM のメモリ上の OS データを取得するために，図 3 のように，まず OCALL と呼ばれる機構を用いてエンクレイヴ外部の SGmonitor ライブラリを呼び出す．これはエンクレイヴが直接ハイパーバイザを呼び出すことができないためである．そして，SGmonitor ライブラリ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．ハイパーバイザは監視対象 VM 内のページテーブルを参照して，取得したいデータの仮想アドレスを対応する物理アドレスに変換する．その物理アドレスを用いて監視対象 VM から OS データを取得し，信頼できない SGmonitor ライブラリなどでの情報漏洩を防ぐために暗号化する．暗号化された OS データが SGmonitor ライブラリを介してエンクレイヴに返されると，IDS は OS データを復号して監視に用いる．データの暗号化・復号化を行うために，エンクレイヴとハイパーバイザに wolfSSL の AES を移植した．

SGmonitor では，エンクレイヴ内の IDS は明示的に OCALL を呼び出すことなく，透過的に VM 内の OS データを取得することができる．この機能を実現するために，SGmonitor は LLView[1] を用いて IDS のコンパイルを行う．LLView はプログラムが OS データを取得しようとした時に VM 内のメモリにアクセスするようにプログラムを変換するツールである．SGmonitor ではその際に OCALL を呼び出す処理を実行するように IDS を変換する．これにより，監視対象 OS 内で動作するように IDS を作成することで，エンクレイヴ内で動作する IDS を得ることができる．

3.2　暗号鍵の管理

エンクレイヴ内の IDS だけが監視対象 VM の OS データを安全に取得できるようにするために，エンクレイヴとハイパーバイザ間で OS データを暗号化・復号化するための暗号鍵を公開鍵暗号を用いて共有する．まず，エンクレイヴ内の IDS が暗号鍵を生成し，それをハイパーバイザの公開鍵で暗号化する．ハイパーバイザの公開鍵はあらかじめ，IDS に埋め込んでおく．IDS は SGmonitor ライブラリを介して暗号鍵をハイパーバイザに渡し，ハイパーバイザは自身の秘密鍵を用いて暗号鍵を復号する．秘密鍵はハイパーバイザだけが知っているため，ハイパーバイザ以外は暗号鍵を復号することができない．同時に，IDS はクラウド外部の第三者機関と通信して暗号鍵の電子署名を取得し，それをハイパーバイザが検証する．正しい IDS に対してのみ電子署名を行うようにすることにより，正しい IDS だけが暗号鍵を登録することができる．

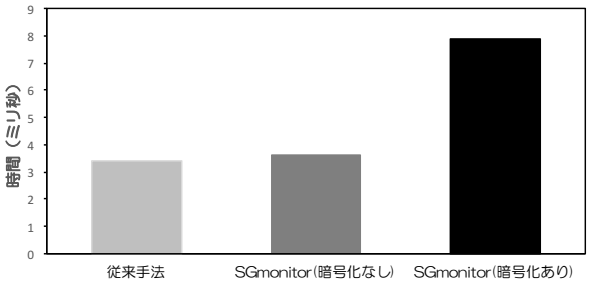

図 4　プロセス情報の取得時間

3.3　ハートビートによる動作確認

IDS が正常に動作していることをリモートホストから確認するために，チャレンジ・レスポンスを利用する．まず，チャレンジと呼ばれる乱数をリモートホストから SGmonitor ライブラリに送信し，ECALL と呼ばれる機構を用いてその乱数をエンクレイヴ内の IDS に渡す．IDS はリモートホストと共有している暗号鍵と受信した乱数からハッシュ値を計算した後，それをレスポンスとしてリモートホストに返す．リモートホスト内でも同様に暗号鍵と乱数からハッシュ値を計算し，それがレスポンスと一致すれば IDS の正常な動作を確認できる．ハッシュ値計算に暗号鍵を含めることにより，正しい IDS 以外は正しいレスポンスを返すことができない．

4　実験

SGmonitor を用いて VM 内のプロセス情報を取得する IDS を実行し，取得時間を測定した．本実験では，OS データの暗号化を行う場合と行わない場合についてそれぞれ測定を行った．比較として，従来手法でオフロードした IDS を実行した場合の取得時間も測定した．実験には，Intel Xeon E3-1225 v5 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 をサポートした Xen 4.7 を使用した．

VM 内のプロセス情報の取得にかかる時間を 10 回測定した時の平均値を図 4 に示す．データの暗号化を行わない場合，SGmonitor における取得時間は従来手法と比較して 8% 増加した．これは OCALL によるオーバヘッドが原因と考えられる．一方，データの暗号化を行う場合，暗号化を行わない場合と比べて 2 倍以上の時間がかかった．このオーバヘッドは AES-NI と呼ばれる CPU の AES 支援機構を用いることによって削減できると考えられる．

5　まとめ

本研究では，Intel SGX を用いて IDS を保護し，正しい IDS だけが VM 内の情報を取得できるシステム SGmonitor を提案した．SGmonitor はエンクレイヴ内で IDS を動作させることにより IDS の改ざんを防ぎ，監視対象 VM から取得した機密情報の漏洩を防ぐことを可能にする．今後の課題は，リモートホストからのハートビートを実装することや，安全な鍵管理を実現することである．

参考文献

[1] 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．九州工業大学情報工学部機械情報工学科卒業論文．2015 年．