論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻

学生番号	20675010	氏　名	河村　拓実
論文題目	SGX 向け実行環境を用いた VM の安全な監視機構		

1　はじめに

利用者に仮想マシン（VM）を提供する IaaS 型クラウドはインターネット経由で攻撃を受けやすいため，侵入検知システム（IDS）を用いて VM を監視する必要がある．外部の攻撃者やクラウド内の内部犯から IDS が攻撃を受けるのを防ぐため，IDS を VM の外にオフロードし，Intel SGX を用いて作成した保護領域（エンクレイヴ）内で安全に実行する手法が提案されてきた．しかし，IDS の開発には OS レベルのプログラミングが必要となり，既存の IDS の多くを動かすことができていない．

本研究では，SGX 向け実行環境を用いることで既存の 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　SCwatcher

SCwatcher は図 1 のように，VM 内と同じ OS インタフェースを提供する SGX 向け実行環境を用いることで，既存 IDS をエンクレイヴ内で実行可能にする．さらに，VM 内のシステム情報を取得可能な proc ファイルシステムを提供し，VM の外にあるエンクレイヴから VM 内のシステムを監視可能にする。SGX 向け実行環境には様々なものがあるが，性能やセキュリティなどの面でトレードオフがある．そこで，本研究では SCONE [1] と Occlum [2] を用いて SCwatcher を実装した．

VM 監視用 proc ファイルシステムはハイパーバイザ経由で VM のメモリデータを暗号化して安全に取得する．SCONE を用いる場合はソースコードが公開されていないため，システムコールのインタフェースを利用してエンクレイヴ外の OS を呼び出し，そこからハイパーバイザを呼び出す．また，IDS をプログラム変換することで VM 監視用 proc ファイルシステムを呼び出させる．一方，Occlum を用いる場合は実行環境に proc ファイルシステムが含まれているため，その中から SGX のインタフェースを利用してエンクレイヴ外のプログラムを呼び出し，そこからハイパーバイザを呼び出す．

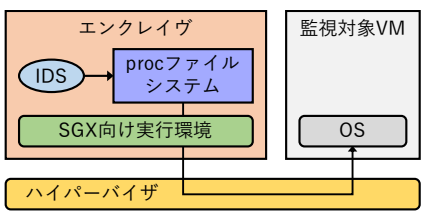

図 1: SCwatcher のシステム構成

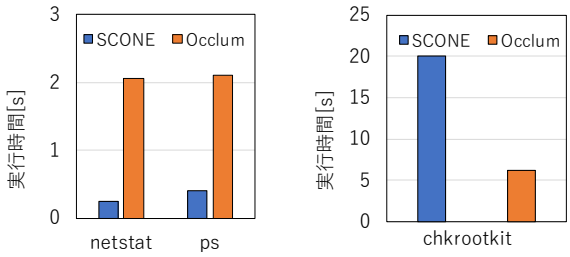

図 2: オフロードした IDS の実行時間の比較

3　実験

SCwatcher を用いて，IDS から呼び出して使われる外部コマンドの netstat と ps および，既存の IDS である chkrootkit の tcpd 検査機能をオフロード実行し，実行時間を測定した．実験結果を図 2 に示す．SCONE の方が実行環境の初期化にかかる時間が短いため，単一コマンドの実行は SCONE を用いる方が 5.3~8.4 倍高速であった．一方，Occlum は複数プロセスを 1 つのエンクレイヴで実行できるため，chkrootkit の実行時間は Occlum を用いる方が 3.2 倍高速であった．

4　まとめ

本研究では，SGX 向け実行環境を用いて既存 IDS を安全にオフロード可能にするシステム SCwatcher を提案した．今後の課題は，VM のメモリデータを取得する際のオーバヘッドを削減することである．

参考文献

[1] S. Arnautov et al. SCONE: Secure Linux Containers with Intel SGX. OSDI 2016.

[2] Y. Shen et al. Occlum: Secure and Efficient Multi-tasking Inside a Single Enclave of Intel SGX. ASPLOS 2020.