機密VM内の隔離環境でのOSメモリ解析による通信の安全かつ軽量な追跡

新矢 将宗[1,a)]　光来 健一[1]

1. はじめに

近年，クラウドの不適切な設定や脆弱性を狙った攻撃が増加しており，クラウドサービスからのユーザの機密情報の漏洩が問題になっている．そのため，クラウド内における通信の流れをユーザが安全に追跡できる機構が求められている．しかし，このような機構をクラウド側が提供する場合，ユーザがクラウドを無条件に信頼することが前提となっており，クラウドからの情報漏洩が発生していないことを保証することはできない．

そこで，クラウドから保護された仮想マシン (VM) である機密 VM を用いてクラウド内の通信を安全に追跡する SEV-tracker [1] が提案されている．しかし，機密 VM 内に VM を作成することでユーザの追跡機構を保護するため，オーバヘッドが大きい．また，クラウドサービスが送受信するすべてのパケットを捕捉して解析するため，通信量に比例してオーバヘッドが発生する．

本研究では，機密 VM 内に軽量な隔離環境を作成し，クラウドサービスが用いるゲスト OS のメモリを解析することで，通信をより軽量に追跡する SockTrawl を提案する．

2. SockTrawl

SockTrawl は図 1 のように，機密 VM 内に高い権限を持つ軽量な隔離環境を作成し，クラウドサービスの通信の追跡機構を動作させる．機密 VM によってユーザの追跡機構をクラウドから保護し，隔離環境によって追跡機構をクラウドサービスから保護することができる．追跡機構はクラウドサービスが用いるゲスト OS のメモリを解析することによって，小さなオーバヘッドで通信情報を取得する．隔離環境内では，ゲスト OS に対してセキュリティ機能やデバイス機能を提供する SVSM と呼ばれる特権モジュールを動作させ，通信の追跡機構は SVSM 内の一機能として実現する．

SockTrawl は Intel TDX と AMD SEV-SNP が提供するそれぞれの機構を用いて軽量な隔離環境を作成する．TDX を用いる機密 VM では，TD Partitioning と呼ばれる機構を用いて機密 VM 内を分割することによって VM を作成し，その VM の外側を隔離環境とする．機密 VM 内で VM を実行する点では先行研究と同様であるが，より軽量に動作させることができる．一方，SEV-SNP を用いる機密 VM では，VMPL と呼ばれる機構を用いて VM 内を新たな特権レベルに分け，最も高い特権レベルで追跡機構を動作させる．追跡機構が動作する時以外は通常の機密 VM と変わらないため，オーバヘッドが生じない．

SockTrawl は SVSM が呼び出されるたびに CPU のタイムスタンプカウンタの値をチェックすることにより，周期的に追跡機構を呼び出す．追跡機構はゲスト OS のメモリを解析して TCP ハッシュテーブルを取得し，登録されているすべての TCP ソケットを走査して TCP 接続情報を取得する．TCP ソケットは TCP 接続が切断されると解放されるため，TCP 接続の切断後も一定時間保持される TIME_WAIT 状態の TCP ソケットも追跡する．

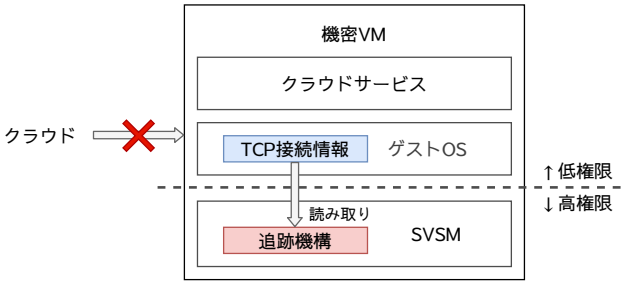


図 1　SockTrawl のシステム構成

[1] 九州工業大学
Kyushu Institute of Technology
[a)] sny430@ksl.ci.kyutech.ac.jp

© 1959 Information Processing Society of Japan

3. 実験

SockTrawl による TCP 接続の追跡能力を測定した．その結果，TDX 環境と SEV-SNP 環境の両方で，接続確立状態および TIME_WAIT 状態の TCP ソケットから接続情報を取得できることを確認した．また，機密 VM 内のクライアントから同じ VM 内のサーバおよび外部サーバに対して短時間に 1000 回の HTTP 通信を行った場合においても，TCP 接続を 100%追跡できることを確認した．

次に，隔離環境および追跡機構を導入することによるオーバヘッドを調べるため，機密 VM 内で nginx を動作させて 1KiB のファイルを配信し，外部ホストから wrk を用いて 30 秒間 HTTP リクエストを送信した．結果は図 2 のようになり，TDX 環境では隔離環境の導入により 19〜41%の性能低下が見られたが，SEV-SNP 環境では性能低下はほとんど見られなかった．いずれの環境でも，追跡機構の導入による性能低下はほとんど見られなかった．

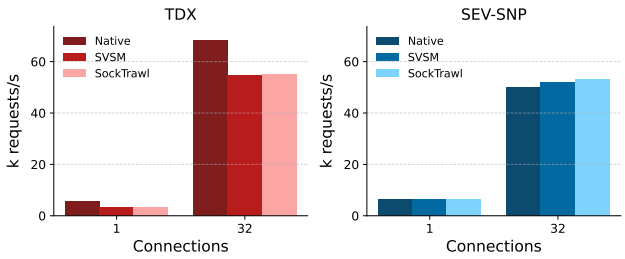


図 2 HTTP リクエスト処理性能

4. まとめ

本研究では，機密 VM 内の軽量な隔離環境においてゲスト OS のメモリを解析することにより，TCP 通信を安全かつ軽量に追跡する SockTrawl を提案した．今後の課題は，より安定かつ軽量な追跡を実現することと，取得した通信ログを安全にユーザに提供できるようにすることである．

謝辞 本研究の一部は，JST，CREST，JPMJCR21M4 の支援を受けたものである．

参考文献

[1] N. Ando et al., “Secure Privacy Control inside Clouds with AMD SEV and Nested Virtualization,” COMPSAC, pp. 83–88, 2025.

© 1959 Information Processing Society of Japan