九州工業大学 情報工学部 情報・通信工学科 2025 年度 卒業論文 概要

コース	ソフトウェアデザイン	指導教員	光來 健一
学生番号	222C3055	氏　　名	新矢 将宗

論文題目	Intel TDX と機密 VM を用いた通信の安全かつ軽量な追跡

1　はじめに

近年，多様な IT サービスがクラウド上で稼働し，顧客情報などの機密データもクラウド上に集約されるようになっている．一方，マイクロサービス化などによりサービス間通信が増加し，データフローは複雑化している．その結果，機密データが様々なサービスに転送され，クラウドからの情報漏洩を増加させる要因になっている．そのため，ユーザが自身のデータの流れを追跡できることが求められているが，クラウドが提供する追跡機構は信頼できるとは限らない．そこで，仮想マシン (VM) とネストした仮想化を用いて通信を安全に追跡するシステム [1] が提案されている．このシステムは，クラウドから保護された機密 VM にユーザのハイパーバイザを送り込み，その上に作られた VM 内で動作するサービスの通信を監視する．しかし，機密 VM 内で VM を動かし，すべてのパケットをキャプチャするオーバヘッドが大きい．

本研究では，Intel TDX の機能を用いて機密 VM 内で追跡機構を安全に動作させることで，より軽量に通信の追跡を行う TDX-Tracker を提案する．

2　TDX-Tracker

TDX-Tracker は図 1 のように，Intel TDX を用いて保護された機密 VM 内で，TD パーティショニング機能を用いて隔離された SVSM [2] を動作させて通信の追跡を行う．TD パーティショニングは機密 VM 内でハイパーバイザを動作させ，その上に軽量な VM を作成することを可能にする．TDX-Tracker は機密 VM 内で通常のハイパーバイザの代わりに，最小限の機能のみを持つ SVSM を動作させることで，ネストした仮想化のオーバヘッドを削減する．

機密 VM 内の SVSM において軽量 VM の通信を追跡するために，TDX-Tracker は軽量 VM 内の OS が保持している TCP 接続情報を定期的に参照する．これにより，軽量 VM が送受信する全パケットをハイパーバイザがキャプチャするオーバヘッドを削減し，通信の追跡に必要な TCP 接続情報のみを効率よく取得する．そのために，軽量 VM のメモリ上にある TCP ソケットを管理するためのハッシュ表を特定し，そのデータ構造を解析して送信元と宛先の IP アドレスとポート番号の組を取得する．使用中の TCP 接続に加えて，切断後一定時間以内の TCP 接続の情報も取得することにより，定期的な監視による見逃しを減らす．

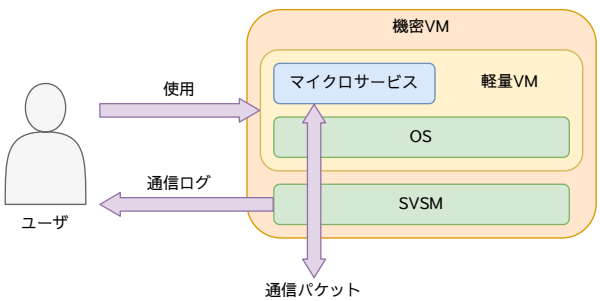

図 1. TDX-Tracker のシステム構成

SVSM ではタイマを用いることができないため，TDX-Tracker は CPU のタイムスタンプカウンタを利用して SVSM 内の追跡機構を定期的に呼び出す．軽量 VM は内部でイベントが発生するたびに SVSM に遷移してイベントの処理を行う．その際に，タイムスタンプカウンタを参照し，前回の追跡機構の実行から一定時間が経過していれば追跡機構を呼び出す．SVSM への遷移はクラウドの信頼できないハイパーバイザを経由しないため，クラウドから干渉されることなく追跡機構を実行することができる．

3　実験

TDX-Tracker を用いてローカルホストおよび外部ホストへの TCP 接続が追跡可能かどうかを確認する実験を行った．それぞれ 1000 回の HTTP リクエストを送信した結果，ローカルホストへの通信ではほぼ 100%，外部ホストへの通信では 98〜100%の TCP 接続情報を取得することができた．

また，TDX-Tracker のオーバヘッドを調べるために，様々な VM を用いて HTTP 通信性能を測定した．測定結果は図 2 に示すようになり，SVSM を動作させた機密 VM と比較して，スループットでは 10〜20%，レイテンシでは 10〜15%の性能低下がみられた．

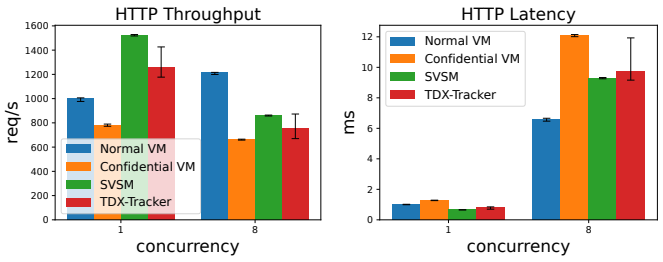

図 2. HTTP 通信性能

4　まとめ

本研究では，Intel TDX を用いて機密 VM 内で追跡機構を安全かつ軽量に動作させて通信の追跡を行う TDX-Tracker を提案した．今後の課題は，より軽量にすべての通信を追跡できるようにすることである．

参考文献

[1] N. Ando et al.: Secure Privacy Control inside Clouds with AMD SEV and Nested Virtualization. COMPSAC 2025.

[2] P. Fang et al.: Intel TD Partitioning and vTPM on COCONUT-SVSM. LPC 2024.