九州工業大学 情報工学部 情報・通信工学科 2024 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	23222206	氏　　名	田中 隆樹

論文題目	機密コンテナと Nested SEV を用いた通信の安全な追跡

1　はじめに

クラウドの普及に伴い，クラウドサービスを用いてプライバシデータが扱われるようになっている．特に，多数のマイクロサービスを連携させるクラウドサービスの場合，設定ミスや攻撃により大規模な情報漏洩が発生しやすい．このようなプライバシデータの流出リスクを低減するには，クラウド内のデータ流をユーザが正確に把握できる仕組みが必要となる．そこで，クラウドの仮想マシン (VM) 内でユーザのハイパーバイザを実行し，クラウドサービスの通信を追跡するシステム [1] が提案されている．このシステムでは，CPU の隔離実行環境を用いることで，ユーザ・ハイパーバイザとクラウドサービス双方の保護を両立させている．しかし，コンテナを用いて構築されることの多いマイクロサービスを実行するのは難しい．また，軽量化のためにクラウドサービスは Unikernel として作成する必要がある．

本研究では，VM の代わりに機密コンテナを用い，Nested SEV[2] と組み合わせることでマイクロサービスの通信を安全に追跡するシステム CoCo-Tracker を提案する．

2　CoCo-Tracker

CoCo-Tracker は図 1 のように機密コンテナを用いてマイクロサービスを動作させ，ユーザ・ハイパーバイザを用いてその通信を安全に追跡する．機密コンテナは AMD SEV で保護された VM を利用して作成されたコンテナである．機密コンテナの中では軽量 Linux が動作し，従来のコンテナイメージをマウントしてアクセスする．CoCo-Tracker は機密コンテナの中でユーザ・ハイパーバイザを安全に動作させ，その上に作成したユーザ VM 内で軽量 Linux とマイクロサービスを実行する．ユーザ VM に Nested SEV を適用することにより，マイクロサービスをユーザ・ハイパーバイザから保護しつつ，ユーザ VM の通信の監視を可能にする．

CoCo-Tracker の機密コンテナは従来，内部で直接動作していた軽量 Linux を新たに作成したユーザ VM の中で動作させるが，従来の機密コンテナと同様に扱うことができる．これは，ユーザ・ハイパーバイザとして BitVisor を用いることで，軽量 Linux が機密コンテナの仮想デバイスに透過的にアクセスすることができるためである．この互換性により，Kubernetes を用いた既存のマイクロサービス・フレームワークをそのまま利用することができる．また，Linux 上で動作する既存のマイクロサービスを実行することができる．

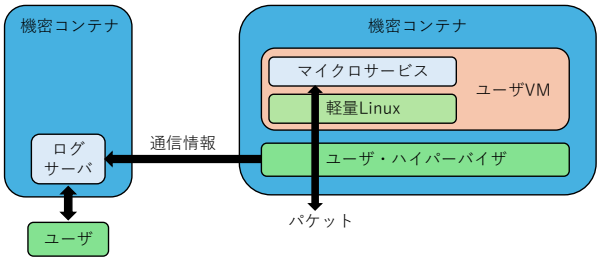

図 1. CoCo-Tracker のシステム構成

BitVisor を用いて機密コンテナを起動できるようにするために，CoCo-Tracker は BitVisor と軽量 Linux，UEFI シェルスクリプト等からなるディスクイメージを用いる．UEFI BIOS がスクリプトを実行して BitVisor を起動し，BitVisor は作成したユーザ VM 内で軽量 Linux を起動する．BitVisor はネットワークデバイスのみを仮想化し，ユーザ VM が送受信するパケットを横取りして通信ログを記録する．そのログはユーザのログサーバに転送され，ユーザはそれを基にクラウド内のデータ流を把握する．

3　実験

CoCo-Tracker を用いて 2 個のマイクロサービスに対して負荷試験を実施し，クラウドサービスの応答時間を計測した．比較として，通信ログを記録しない場合と BitVisor を用いない場合についても負荷試験を行った．実験の結果，図 2 に示すように，BitVisor を用いることで応答速度が 1.2〜1.4 倍になることが分かった．すべての通信を記録するとさらに 1.6〜2.9 倍になることが分かった．記録する通信を減らすことで性能が改善できると考えられる．

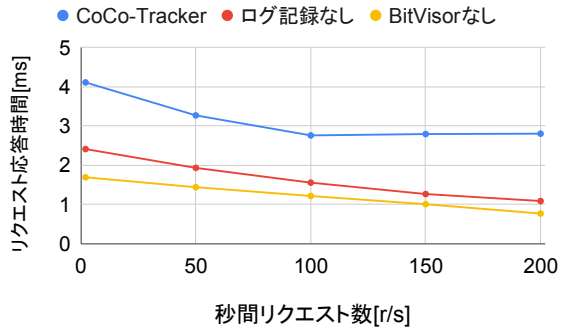

図 2. 負荷試験の結果

4　おわりに

本研究では，機密コンテナと Nested SEV を組み合わせることでクラウドにおけるマイクロサービスの通信を安全に追跡するシステム CoCo-Tracker を提案した．今後の課題は，より大規模なマイクロサービスを対象にした評価を行うことである．

参考文献

[1] 安東ら: AMD SEV とネストした仮想化を用いた安全な通信の追跡・制御, CSEC 研究会, 2024.

[2] 瀧口ら: Nested SEV: ネストした仮想化への AMD SEV の適用, ComSys 2022.