九州工業大学 情報工学部 情報・通信工学科 2022 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	21222008	氏　　名	瀧口 和樹

論文題目	VM 内で動作する VM の AMD SEV を用いた保護

1　はじめに

機密性の高い情報をクラウドで扱うようになるにつれて，クラウドの内部犯などから仮想マシン (VM) 内の機密情報を盗まれる危険性が増している．AMD のプロセッサでは VM のメモリを VM ごとの鍵で透過的に暗号化する SEV と呼ばれる機能が提供されており，VM のメモリ上にある機密情報の VM 外からの盗聴を防ぐことができる．SEV-ES と呼ばれる拡張ではメモリに加えてレジスタの状態も暗号化することができる．VM のすべてのメモリを暗号化すると I/O に使用するメモリをハイパーバイザと共有できなくなるため，SEV によるメモリ暗号化を制御するための対応が VM 内の OS に必要である．一方，VM の中で VM を動作させるネストした仮想化と呼ばれる技術を用いた様々なシステムが提案されているが，現状ではハイパーバイザが SEV に対応していないため，SEV を適用することができない．

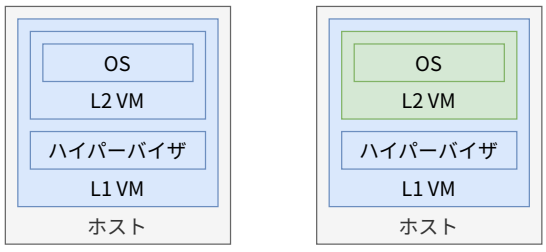
本研究では，VM 内で動作する VM の SEV による保護を可能にする Nested SEV を提案する．

2　Nested SEV

Nested SEV は図 1 のように，SEV で保護されたクラウドの VM (L1 VM) の中でハイパーバイザを動作させ，その上で動作する VM (L2 VM) に SEV を適用することができる．その際に，L1 VM と L2 VM のメモリ暗号化に同一の鍵を用いる構成と異なる鍵を用いる構成が考えられる．同一のメモリ暗号化を行うと，L1 VM 内のハイパーバイザに L2 VM へのアクセスを許可することができる．この構成は安全な仮想プライベートクラウドの構築などに利用できる．一方，異なるメモリ暗号化を行うと，L1 VM 内のハイパーバイザから L2 VM を保護することができる．この構成は安全な仮想パブリッククラウドの構築などに利用できる．

L2 VM に SEV を適用するために，Nested SEV は透過的 SEV，SEV パススルー，SEV 仮想化の 3 種類の方式を提供する．透過的 SEV は VTE と呼ばれる SEV の機能を用いることにより，L2 VM 内の OS を SEV に対応させることなく，L2 VM に SEV を透過的に適用することができる．VTE を用いると L2 VM のすべてのメモリが L1 VM に適用されている SEV と同一の鍵を使って無条件に暗号化される．ただし，L2 VM から L1 VM の仮想デバイスに直接アクセスするパススルーアクセスを行うことはできず，VTE をサポートしていない SEV-ES には適用することができない．

それに対して，SEV パススルーは L1 VM に適用されている SEV をそのまま L2 VM にも適用する．透過的 SEV とは異なり，L2 VM 内の OS がどのメモリ領域を暗号化するかを制御することができる．そのため，L1 VM の仮想デバイスにもパススルーアクセスを行うことができ，SEV-ES にも適用することができる．一方，SEV 仮想化は SEV を仮想化し，仮想 SEV を L2 VM に適用する．透過的 SEV や SEV パススルーとは異なり，L1 VM に適用されている SEV とは異なる鍵を用いて L2 VM のメモリを暗号化する．



(a) 鍵が同一の構成　　(b) 鍵が異なる構成

図 1. Nested SEV を用いたシステム構成

3　実験

L1 VM と L2 VM に SEV および SEV-ES を適用した場合の性能を調べる実験を行った．この実験では，KVM 上の L1 VM 内でハイパーバイザとして KVM，BitVisor，Xen を動作させ，L2 VM 内で Linux を動作させた．Apache HTTP Server に 1000 並列でリクエストを送信した際の性能を図 2 に示す．SEV を適用すると Xen 以外では性能が低下した．KVM では方式にかかわらず 95〜97 %に，BitVisor では SEV パススルーの適用時に 92 %の性能になった．SEV-ES を適用するとさらに性能が低下し，KVM に SEV パススルーを適用したときに 83 %の性能となった．

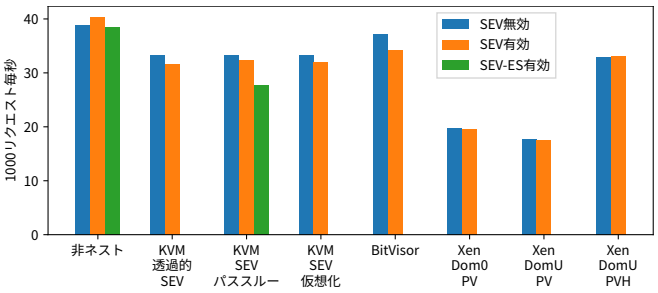


図 2. SEV によるウェブサーバの性能低下

4　まとめ

本研究では，ネストした仮想化に SEV を適用することを可能にする Nested SEV を提案した．今後の課題は，それぞれのハイパーバイザに未実装の方式を実装することや，よりセキュリティを高めた拡張である SEV-SNP に対応することである．