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	24222201	氏　　名	伊藤 大輝
論文題目	RISC-V PMP を用いた静的パーティショニング型 VM の保護		

1　はじめに

近年，自動車や産業制御分野でも仮想マシン (VM) を用いて複数のサブシステムを一つのハードウェア上に統合する動きがある．このような組み込みシステムがインターネットに接続されると，まず最も脆弱な VM が攻撃を受ける．その VM の下で動作するハイパーバイザにも脆弱性があると，ハイパーバイザ経由で他のすべての VM が攻撃を受ける．その結果，VM 内の AI モデルや制御ロジックなど，企業の知的財産を盗まれる可能性がある．そこで，最近のプロセッサは隔離実行環境を提供し，ハイパーバイザや他の VM から保護された機密 VM を作成できるようになっている．組み込みシステムでの導入が進んでいる RISC-V においても，機密 VM 拡張 (CoVE) [1] が提供されている．しかし，VM 間のメモリ隔離を実現するために必要な機能が実装された RISC-V プロセッサはまだ存在しない．

本研究では，RISC-V の標準ハードウェアのみを用いて VM のメモリをハイパーバイザおよび他の VM から隔離する PRICEE を提案する．

2　PRICEE

PRICEE は図 1 のように，ハイパーバイザの下で動作するセキュリティモニタが RISC-V の標準ハードウェアの PMP を用いることにより，VM のメモリをハイパーバイザや他の VM から隔離する．セキュリティモニタは最も権限の高い M モードで動作するため，ハイパーバイザは PMP の設定を変更することはできない．PMP は物理メモリ領域ごとにアクセス権限を設定できるが，設定可能な領域数が限られるため，メモリ領域が連続していない一般的な VM には適用できない．一方，組み込みシステムでは，ハードウェアリソースを分割して VM に割り当てる静的パーティショニング・ハイパーバイザがよく用いられる．この VM のメモリ領域は連続しているため，PMP の利用が可能である．

PRICEE は実行中のコンテキストに応じて PMP の設定を切り替えることで，VM やハイパーバイザが自身のメモリのみにアクセスできるようにする．PMP の設定の変更は VM とハイパーバイザ間でコンテキストが切り替わる際に行う．VM の実行中に例外や割り込みが発生するとハイパーバイザに遷移するが，その前にセキュリティモニタが PMP の設定を変更し，ハイパーバイザが VM のメモリにアクセスできないようにする．ハイパーバイザでの処理が終了すると VM に遷移するが，その前にセキュリティモニタが PMP の設定を変更し，VM が自身のメモリにアクセスできるようにする．

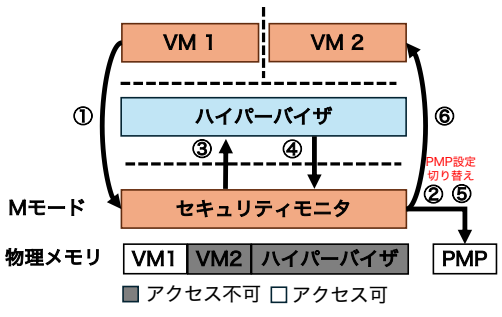

図 1. PRICEE のシステム構成

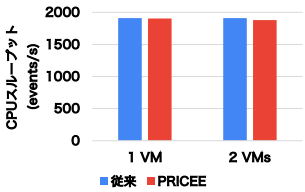

図 2. CPU 性能

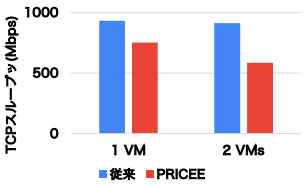

図 3. TCP スループット

このようにハイパーバイザは VM のメモリにアクセスすることができなくなるが，VM を実行するために必要なメモリアクセスだけは可能にする．VM の起動時には OS 等の初期イメージを VM のメモリに書き込む必要があるため，VM への最初の遷移時までは VM のメモリへのアクセス制限を行わないようにする．また，VM の I/O 命令をエミュレートする際にも VM のメモリを読み書きする必要があるため，セキュリティモニタから共有メモリ経由でハイパーバイザに必要な情報を渡せるようにする．

3　実験

PRICEE を用いて，ハイパーバイザから VM のメモリに不正にアクセスする実験を行った．ハイパーバイザの例外ハンドラの中で VM のメモリにアクセスしたところ，メモリアクセスに失敗することが確認できた．

また，VM 内のシステム性能を sysbench と iperf3 を用いて測定し，PRICEE と従来システムの性能を比較した．測定結果は図 2 と図 3 のようになり，CPU 性能は PRICEE の方が低下しているものの，性能低下率は 2.5〜3%程度であった．一方で，TCP スループットは割り込みが多発し，性能が 20〜36%と大きく低下した．

4　まとめ

本研究では，RISC-V の PMP を用いてそれぞれの VM のメモリを隔離する PRICEE を提案した．今後の課題は，VM での例外発生時にハイパーバイザに必要最小限のレジスタのみを見せられるようにすることである．

参考文献

[1] RISC-V International: Confidential VM Extension (CoVE) for Confidential Computing Version 0.7. 2024.