AMD SEV-SNP の VMPL による P4 プログラムの安全かつ軽量な実行

村上 和馬[1,a)]　光来 健一[1,b)]

1. はじめに

近年，P4 言語により動作をプログラム可能なネットワークスイッチが登場している．仮想マシン (VM) においても，P4 プログラムを実行可能な仮想 P4 スイッチが開発されている．しかし，信頼できないクラウドにおいては，ユーザが仮想 P4 スイッチにロードした P4 プログラムを改ざんされたり，P4 プログラムで利用する VM 内のシステム情報を盗聴される可能性がある．逆に，ユーザにより不正な P4 プログラムがロードされた場合，仮想スイッチ全体に影響を及ぼし，正常なパケット転送が行われなくなる可能性もある．そこで，AMD SEV によりメモリが保護された P4 VM をユーザごとに用意し，その中で安全に P4 プログラムを実行するシステム [1] が提案されている．しかし，P4 VM をユーザごとに用意するとクラウドのリソースを余分に使ってしまう．

本研究では，AMD SEV-SNP の VM 特権レベル (VMPL) を用いてユーザの VM 内に隔離環境を作成し，P4 プログラムを安全かつ軽量に実行する Parasite-P4 を提案する．

2. Parasite-P4

Parasite-P4 では，図 1 のようにユーザ VM 内の高い VM 特権レベルで P4 プログラムを実行し，低い VM 特権レベルで OS やサービスなどからなるシステムを動作させる．

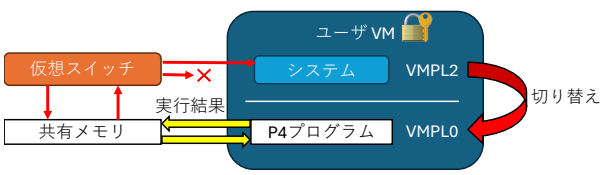

図 1. Parasite-P4 の構成

これにより，P4 プログラムをシステムから保護しながら VM 内で安全に実行することができる．また，ユーザ VM は AMD SEV-SNP によりメモリが保護されるため，P4 プログラムは VM 外にある仮想スイッチからも保護される．

同時に，不正な P4 プログラムがロードされたとしても，P4 プログラムは VM のリソースのみを用いるため仮想スイッチの動作に影響を及ぼすことはない．しかし，VM 内のシステムには影響を及ぼす可能性があるため，eBPF を用いて P4 プログラムを実行する．これにより，ロード時に eBPF の検証器を用いて不正な P4 プログラムを排除し，実行時に P4 プログラムのメモリアクセスを制限することができる．

P4 プログラムはシステムと同じユーザ VM 内で実行され，より高い権限で動作するため，システムのメモリ上にある OS データを解析することで VM 内情報を利用することができる．しかし，eBPF のメモリアクセス制限のために P4 プログラムはシステムのメモリにはアクセスできないため，eBPF ランタイムが提供するヘルパー関数を用いる．このヘルパー関数は要求された OS データの仮想アドレスを OS のページテーブルを用いて物理アドレスに変換し，対応するメモリデータを P4 プログラムに返す．

仮想スイッチと P4 プログラムは共有メモリを用いて通信を行う．VM 内のシステムが共有メモリをポーリングし，仮想スイッチによる要求の書き込みを検知すると VM 特権レベルを切り替えることで P4 プログラムを実行する．P4 プログラムは共有メモリに書き込まれているパケット情報を基に，転送・破棄の判断を共有メモリに書き込む．仮想スイッチはこの結果を基にパケットの転送・破棄の処理を行う．

3. 実験

Parasite-P4 を用いてパケットの転送・破棄の判断が正しく行えることを確認した．この実験では，システムの TCP

[1] 九州工業大学
[a)] murakami@ksl.ci.kyutech.ac.jp
[b)] kourai@csn.kyutech.ac.jp

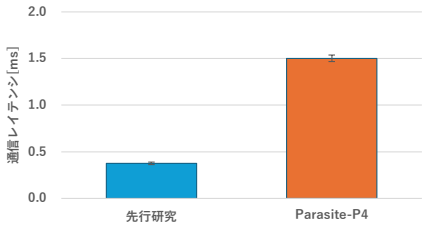

図 2. 通信レイテンシの増加

通信でのメモリ使用量に応じてパケットの転送・破棄の判断を行う P4 プログラムを用いた．実験の結果，システムが TCP 通信をしている時には P4 プログラムはパケット破棄の判断を返し，TCP 通信を行っていない時にはパケット転送の判断を返すことを確認した．

また，P4 プログラムの実行による通信レイテンシの増加を測定した．その結果は図 2 のようになり，Parasite-P4 におけるレイテンシの増加は先行研究の 3.9 倍となった．この原因としては，OS データを取得する際のシステムメモリのマッピングのオーバヘッドが考えられる．

4. まとめ

本研究では，安全かつ軽量に P4 プログラムの実行を行う Parasite-P4 を提案した．今後の課題は，システムのメモリを事前にマッピングできるようにすることや，より複雑な OS データを用いられるようにすることである．

謝辞 本研究は，JST 経済安全保障重要技術育成プログラム【JPMJKP24U4】の支援を受けたものである．

参考文献

[1] 岩井，光来：VM 内情報を利用する仮想 P4 スイッチの安全な実行，セキュリティサマーサミット 2024.