九州工業大学 情報工学部 情報・通信工学科 2023 年度 卒業論文 概要

コース	情報通信ネットワーク	指導教員	光來 健一
学生番号	22222201	氏　　名	岩井 正輝

論文題目	VM 内情報を利用可能な仮想 P4 スイッチの安全な実行

1　はじめに

近年，ネットワークスイッチにおいて P4 言語を用いてパケットの転送処理をプログラミングできるようになってきている．例えば，高度なパケットフィルタリングを行ったり，パケットのデータ書き換えを行ったりすることができる．クラウドにおいて仮想マシン (VM) をネットワークに接続する際には仮想スイッチが用いられ，P4 に対応した仮想スイッチも開発されている．VM のユーザが仮想スイッチに P4 プログラムをロードできるようになれば，VM 内の情報を用いたよりきめ細かいパケット処理が実現可能となる．しかし，クラウドによって提供されている仮想スイッチは信頼できるとは限らない．ユーザがロードした P4 プログラムを改ざんされたり，P4 プログラムが利用する VM 内の情報を盗聴されたりするリスクがある．

本研究では，VM 内情報を利用できるように拡張した P4 プログラムをユーザごとに用意される保護された P4 VM で安全に実行する P4 Shield を提案する．

2　P4 Shield

P4 Shield は図 1 のように，ユーザごとに P4 プログラムを実行するための VM (P4 VM) を用意し，AMD SEV で VM のメモリを暗号化することにより保護する．これにより，クラウドによる P4 VM への攻撃の多くを防ぐことができる．クラウドは P4 プログラムを改ざんすることはできず，P4 プログラムが取得した VM 内情報を盗聴することもできない．仮想スイッチはユーザの VM が送信元または宛先になっているパケットを対応する P4 VM に転送して P4 プログラムを安全に実行し，その実行結果を受け取る．そして，実行結果に基づいてパケットを破棄したり，パケットのデータを更新したりする．

P4 VM はユーザが用意した P4 プログラムから生成された uBPF バイトコードを実行する．uBPF は OS カーネル内で動作する eBPF よりも制約が少ないユーザ空間 BPF である．uBPF を用いることにより，ユーザが複数の P4 プログラムをロードした場合でも安全に実行することができる．

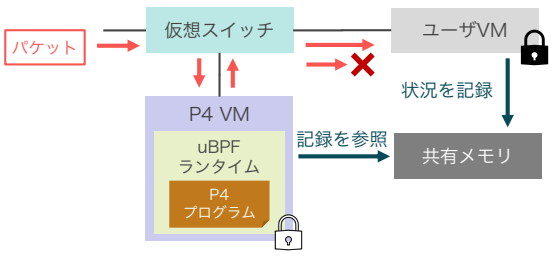

図 1. P4 Shield のシステム構成

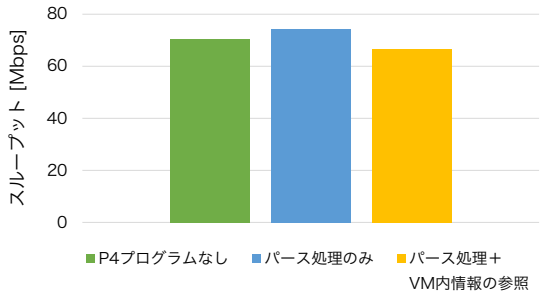

図 2. P4 VM 内での P4 プログラム実行の影響

uBPF バイトコードは JIT コンパイルすることにより高速に実行される．P4 VM が仮想スイッチからパケットを受け取ると P4 プログラムを実行し，そのパケットの転送の可否や必要に応じて書き換え後のパケットを仮想スイッチに返す．

P4 プログラムからユーザ VM 内の情報を利用できるようにするために，P4 VM とユーザ VM はメモリの一部を共有する．ユーザ VM は内部情報を VM 間で共有する鍵を用いて暗号化して共有メモリに格納する．これにより，クラウドは VM 内情報を盗聴することはできない．従来の P4 プログラムはこの共有メモリにアクセスできないため，C 言語で記述した外部関数経由で uBPF ランタイムのヘルパー関数を呼び出すことによって VM 内情報を取得する．

3　実験

P4 Shield を用いて，P4 VM 内の P4 プログラムがユーザ VM 内の情報を活用してパケットを破棄できることを確認する実験を行った．この実験では，ユーザ VM が送信したことを想定した UDP パケットの情報を共有メモリに書き込んでおいた．この VM 内情報を用いて，ユーザ VM が送信していない UDP パケットの不着を示す ICMP パケットを受信した場合に，不正なパケットとして破棄できることを確認した．

また，P4 Shield を用いた場合の ICMP スループットを図 2 に示す．この結果より，P4 プログラムによるパケットヘッダのパース処理や VM 内情報の参照の性能への影響は小さいことが分かる．P4 Shield を用いない場合の 538Mbps から大幅に低下しているが，これは P4 VM へのパケットの転送にソケット通信を用いていることが原因である．

4　まとめ

本研究では，VM 内情報を利用できるように拡張した P4 プログラムをユーザごとに用意される SEV で保護された P4 VM で安全に実行する P4 Shield を提案した．今後の課題は，共有メモリへの VM 内情報の格納や性能の向上などである．