ハイパーバイザによる高セキュアなネットワーク監視・制御のためのSDNコントローラに関する研究

尾内 智哉[1,a)]　並木 美太郎[1,b)]

SDN Controler for High Secure Network Surveillance and Control Using Hypervisor

1. はじめに

OS は計算機が動作するために必要不可欠な大黒柱のようなソフトウェアである．新しい機能の実装や新しいハードウェアの対応のために OS のコードは日々増加し続けている．OS は非常に複雑なソフトウェアとなっており今までに多くのバグが見つかっている [1]．また, OS は一番高い特権レベルで動作するため OS が危殆化すると, その上で動作するすべてのアプリケーションに悪影響を及ぼすという問題がある．OS がカーネルパニックに陥ると, すべてのアプリケーションを再起動する必要があり処理途中の情報は失われる．悪意のある者が OS の脆弱性を利用することで OS の制御を奪うことも考えられる．これらの理由から, 安全にプログラムを実行できる計算環境が重要である．

2. 目標

ネットワーク経由での攻撃で攻撃対象の計算機に侵入するためにまず空いているポートを探す．ポートスキャンによる空きポートの特定や, OS を特定することで計算機の制御を奪うための準備を行う．

本研究ではこの攻撃を防ぐためにハイパーバイザでパケットをフィルタリングすることでポートスキャンを検出する．そしてハイパーバイザで動作する SDN コントローラでポートスキャンを行う計算機からの通信を遮断することで攻撃を防ぎ安全な計算環境を実現する．ハイパーバイザでのパケットフィルタリングではパケットの送信元での DDoS 攻撃の防止に応用されている [2]．この論文では eBPF により柔軟なパケットフィルタリングを行うが OS が動作する PC 外のネットワークの制御までは行わない．提案手法では, ハイパーバイザでのパケットフィルタリングに加えて SDN によるプログラマブルなネットワークの制御を行う．

[1] 東京農工大学
Tokyo University of Agriculture and Technology
[a)] s178565q@st.go.tuat.ac.jp
[b)] namiki@cc.tuat.ac.jp

3. 全体構成

本研究で提案するシステムの構成を次の**図 1** に示す．このシステムでは SDN スイッチに接続された複数の計算機が SDN による仮想ネットワークで通信する．これらの計算機はハイパーバイザ上では動作してもしなくても良いがハイパーバイザを使用することでセキュリティの向上が期待できる．このネットワークではハイパーバイザで動作する SDN コントローラが 1 つあり SDN スイッチを制御して, SDN スイッチに接続された計算機への攻撃から守る．攻撃を検出するとゲスト OS への通知を行い, SDN コントローラが SDN スイッチを制御して攻撃を行う計算機からの通信を遮断する．

SDN コントローラは VMX root モードの Ring 3 で動作する保護ドメインがプログラムによるネットワークの制御を行う．OS より高い特権レベルで OS に依存せずに動作することから OS の危殆化による影響を受けずにセキュリティを向上できる．

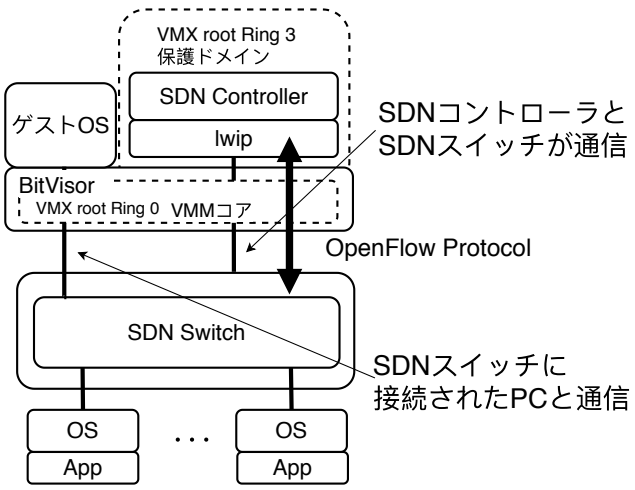

図 1　提案システムの構成

3.1 提案システムの特徴

提案システムの構成要素と特徴を次に示す.

- ハイパーバイザ
  BitVisor を使用する. ディスクやネットワーク I/O をゲスト OS から透過的に暗号化動作させることでゲスト OS のセキュリティを強化するためのハイパーバイザであり, 動作させることのできる OS を 1 つに制限することで仮想化によるオーバーヘッドを最小限にする.
- SDN
  ネットワークの制御には SDN を利用する. 従来 1 つのネットワーク機器で行われていたネットワークの制御と転送を, それぞれコントロールプレーンとデータプレーンに分けて行う. SDN によってコントロールプレーンでプログラムによるネットワークの制御ができるようになる. この SDN を OpenFlow プロトコルによって実現する.
  – コントロールプレーン
    コントロールプレーンの SDN コントローラは BitVisor に組み込まれた TCP/IP プロトコルスタックの lwip を使用して OpenFlow を扱うプログラムを実装する. BitVisor のプログラムの小ささから汎用的な OS と比較してもハイパーバイザに対する攻撃範囲も小さいことと, 動作する特権レベルの高さからより安全に動作すると言える.
  – データプレーン
    ソフトウェアスイッチの Open vSwitch を使用する. SDN コントローラから挿入されたパケットのヘッダにマッチする条件と, その条件にマッチしたときに行うアクションで構成されるフローエントリをもとにパケットの転送を行う.

3.2 実験

実験は**図 2** の環境で次の手順で行い, SDN スイッチに 2 つの計算機を接続して A からの攻撃から B を守ることができることを確認した. 将来的に lwip と SDN コントローラを保護ドメインで動作させたいが BitVisor のコアと lwip が密接に関係しているため, 保護ドメインで使えず今回は BitVisor のコアと同じ VMX root モードの Ring 0 で動作させている.

① A が BitVisor 上で動作する OS にポートスキャン
② SDN スイッチに入ってきたフローエントリにマッチしないパケットの処理方法を問い合わせる
③ SDN コントローラでポートスキャンを検出して通信を遮断するためのフローエントリを SDN スイッチに挿入する
④ ポートスキャンを行った A からの通信が遮断される

この実験によって A によるポートスキャンを SDN コントローラで検出して A からの通信を遮断するフローエントリを挿入することができた. これによって A からの攻撃を SDN スイッチで遮断し, B を守ることができた.

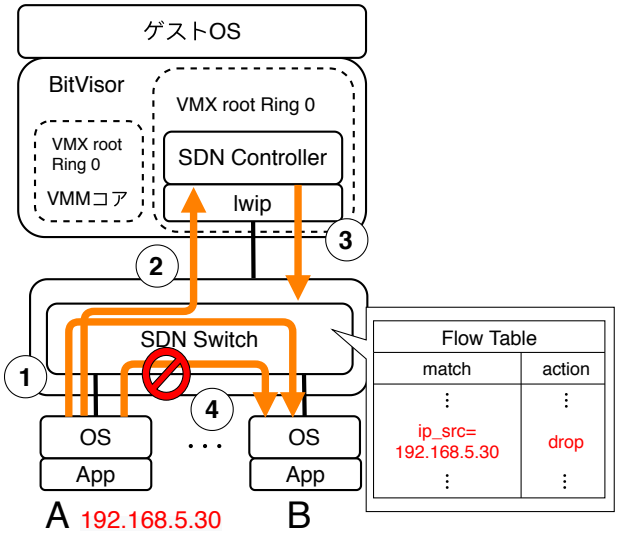

図 2 SDN でポートスキャンを防ぐ実験

3.3 現状

BitVisor で動作する SDN コントローラで OpenFlow を扱いとパケットのフィルタリング, そしてポートスキャンを検出して通信の遮断ができるようになった. しかし, ポートスキャンによって通信を遮断するまでに大量のパケットを処理することで通信が遮断されてしまうことがあり通信が不安定となっている.

4. おわりに

本研究では BitVisor で動作する SDN コントローラによって, その攻撃層の小ささから高セキュアに, また OS に依存せずに動作するネットワーク監視・制御を行うシステムを提案した.

今後は lwip と SDN コントローラを保護ドメインで動作させることやよりセキュアに動作させるために OpenFlow の通信の暗号化することが課題である.

参考文献

[1] Afifa Sajid, M Ali Shah, Muhammad Kamran, Qaisar Javaid, and Sijing Zhang. An analysis on host vulnerability evaluation of modern operating systems. International Journal of Advanced Computer Science and Applications (IJACSA),7(4):245254, 2016
[2] Masanori Misono, Kaito Yoshida, Juho Hwang and Takahiro Shinagawa, "Distributed Denial of Service Attack Prevention at Source Machines", The University of Tokyo 2018 IEEE 16th Int. Conf. on Dependable Autonomic & Secure Comp.