SDNコントローラに対する攻撃検知

Attack Detection against SDN Controller

杉本久美・ネットワーク分科会・情報セキュリティ大学院大学

Abstract: SDN is increasingly being deployed in data centers and is attracting attention as a security measure. However, because of its architecture, if the control of the controller is lost, the control of the entire network is lost, and serious incidents may occur. To propose a detection method against SDN controller attacks, in this poster, we will discuss the attacks and countermeasures. There are various attack paths to the SDN controller. It is important to establish trust with applications and switches to determine whether they are legitimate or not.

1. 研究背景と目的

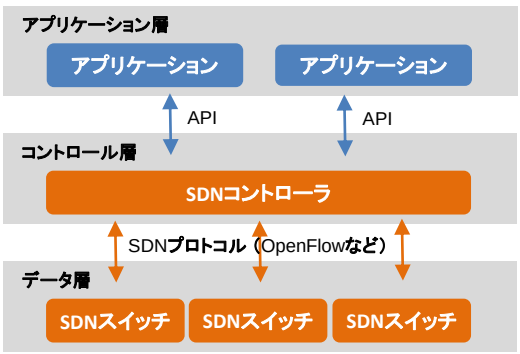
サーバ仮想化技術の発展により、仮想マシンを必要に応じて生成・消去することが出来るようになった。しかし従来のネットワークではその都度個別に設定する必要があり、動的な仮想マシンに対応出来なかった。そこで動的なネットワークのニーズが生まれ、柔軟性・迅速性を兼ね備えたSDNが登場した。

SDNはデータセンターを中心に導入が進んでいる。SDNの主な導入理由の1つに、マルウェアやDDoS攻撃などへのセキュリティ対策が挙げられる。SDNによるセキュリティ対策の研究は近年盛んに行われているが、SDNへの攻撃やその対策の研究はまだ少ない。本研究ではSDNのセキュリティ向上を目的とし、SDNのセキュリティ課題について考察する。コントローラへの攻撃に対する検知手法の提案を目標とする。

2. SDNのセキュリティの弱点

SDN（Software Defined Network）

- ソフトウェアでネットワークを制御する概念
- 主な技術として OpenFlow がある



SDNアーキテクチャ

- コントローラ：データ転送処理のためのルール作成など転送制御を行う
- スイッチ：コントローラの指示に従ってデータ転送を行う

- **SDNコントローラはネットワークを集中制御しているため、攻撃者から見れば狙う価値が高い**（コントローラの制御を奪えばネットワーク全体を制御できる）。

3. コントローラへの攻撃と対策

- SDNのセキュリティを確保する手段の1つとして、**コントローラに対する攻撃検知**の機能が求められる。
- SDNコントローラへの攻撃は、第三者によるコントローラへの不正なアクセスや、コントローラへのなりすまし、DDoS攻撃などが考えられる。
- 不正なアプリケーションやスイッチ、プログラマブルであることで生まれるソフトウェアの脆弱性、従来のネットワーク機器が混在していることによる脆弱性など、攻撃経路は様々。
- 攻撃への対策として、アプリケーションとコントローラ、スイッチとコントローラ間の**信頼を確立**することが必要である。

4. 今後の方針

- SDNのセキュリティ課題に関する論文やSDNの詳細を調査することで、具体的な攻撃手法を検討する。
- 既存の検知手法などから目的の攻撃に対する検知手法の検討を進め、実装の準備をする。
- クラウドセキュリティについても調査する。