様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １８ 日現在

機関番号：１７２０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１３２

研究課題名（和文）SDNの統合セキュリティ確保に関する研究

研究課題名（英文）Integrated Security of SDN

研究代表者
堀　良彰（Hori, Yoshiaki）

佐賀大学・全学教育機構・教授

研究者番号：９０２６４１２６

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：OpenFlow ネットワークシステムのセキュリティ脅威を整理し、いくつかの重要なリスク項目を追加してセキュリティの脅威リストを作成した。その上で、各々のセキュリティリスクに対するリスク評価とリスクへの対策手法について整理し、SDNネットワークシステムのためのセキュリティチェックシートを作成した。
新たなサイバー攻撃傾向の変化を検出する手法として、サイバー攻撃の初期段階として行われるポートスキャンなどの不特定多数を対象とした攻撃に着目し、攻撃の急激な変化を Change Finderによるスコア算出と、ボリンジャーバンドによる異常発見手法を考案した。

研究成果の学術的意義や社会的意義
SDN を各構成要素からなるシステムであることに着目し、システムという観点から全体および構成要素を分析し、SDN システムのセキュリティ確保ための分析と検討を行い、チェックシートとしてまとめた。

研究成果の概要（英文）：We organize security threats in the OpenFlow network system and create a security threat list. After that, we organize the risk assessment for each security risk and the measures for the risk. We create the security check sheet for the SDN network system.
As a method to detect changes in new cyber attack tendency, focusing on attacks targeting an unspecified number such as port scan performed as an initial stage of cyber attack, we propose an anomaly detection by using of time series of Change Finder with Bollinger band.

研究分野：情報工学

キーワード：セキュア・ネットワーク　Software Defined Network　SDN　セキュリティ評価

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

ネットワークの動的構成を可能にする SDN (Software Defined Networking) 技術は、OpenFlow 等関連プロトコルの標準化や、OpenFlow 対応スイッチの発売等、現実のネットワーク構築技術として取り入れられつつある。しかしながら、SDN 自体のセキュリティ確保のための研究開発や、SDN を前提として新たなセキュリティ機構の研究開発は開始されたばかりである。

SDN 技術は、現在のネットワーク基盤の限界を打破することが期待される新たなネットワーク技術である。従来ハードウェア機器で実現していた制御をソフトウェアによって実現することにより、通信資源の更なる最適化、より厳密なポリシに基づくネットワーク運用やセキュリティ対策の実現が期待される。既に、トラヒック制御の面では多くの研究がなされているが、セキュリティ面での課題は未解決である。

２．研究の目的

SDN におけるセキュリティ研究は、SDN により構成される新たなアーキテクチャに基づくネットワークを守る面と、SDN 技術によりセキュアネットワークを実現する面に大別される。現在、SDN 技術として OpenFlow をはじめ Cisco 社の onePK 等さまざまな技術が登場している。本研究では、設計や評価にあたっては OpenFlow を例として検討する。しかしながら、OpenFlow の仕様に限定せず、SDN の本質部分に着目した研究開発を実施する。

SDN は、ソフトウェアによって動的に構成されるネットワークサービス基盤を実現しようとするものであることから、ソフトウェアにおける動的構成がもたらす利点だけでなく、欠点を吟味する必要がある。特に、その欠点に起因する脅威については十分な対策を行うことが SDN システムの実用面での大きな課題である。

SDN システムは、コントロールプレーン、データプレーン等の各層に分けて議論を行うことができ、それぞれに対して、認証認可の機構、それに基づくアクセス制御の機構等に分けて議論できる。現実の SDN システムのセキュリティ対策を議論する場合には、それらの全てにおいて高度なセキュリティ対策を行う必要がない場合が多い。そのことが、適切なセキュリティ対策の導出を複雑にしているという課題がある。

３．研究の方法

前項の目的を達成するために次の２つの副課題に関して研究を取組む。

［副課題１］SDN システムのセキュリティ評価手法の確立

SDN は、コントローラ、ソフトウェア制御可能なスイッチ等複数の構成要素が接続されて全体のシステムとして機能する。そのため、SDN システムを構成する構成要素のセキュリティ評価と、構成要素間が接続され一体として機能する部分のセキュリティ評価を行う。それらを合わせ全体のセキュリティ評価を行うことで、システムとしてのセキュリティ評価を行う。

［副課題２］SDN システムの異常検知手法の確立

本副課題では、SDN システムを構成する構成要素およびそれらの接続点における挙動に着目し、システムセキュリティを向上させる異常検知技術の研究開発を行う。動的に構成される SDN システムでは、動的に構成され構成要素の組み合わせの数も増大する。したがって、異常挙動の検知ルールを直接形式化することが困難であるので、定常挙動に基づく異常検知技術を活用する。

４．研究成果

［副課題１］の成果として次の成果を得た。

OpenFlow ネットワークのセキュリティ上の脅威を分類し、そのセキュリティ上のリスクを明確にした。そのために、Kreutz らによる脅威ベクトルと SDNSecurity.org の攻撃リストを比較し、OpenFlow ネットワークシステムのセキュリティの脅威を整理し、いくつかの重要なリスク項目を追加してセキュリティの脅威リストを作成した。

その上で、各々のセキュリティリスクに対するリスク評価とリスクへの対策手法について整理した。これらを基にして、SDN システムセキュリティのためのセキュリティチェックシートを作成した。この SDN セキュリティチェックシートは、安全な SDN ネットワークを設計するのに寄与する。

さらに、一般的な商用 OpenFlow スイッチとオープンソースの OpenFlow コントローラを実装した実際の OpenFlow ネットワークテストベッドで、PACKET_IN フラッディング攻撃およびフロールールフラッディング攻撃の 2 つの DoS リスクシナリオを評価し、性能低下の様子を定量的に確認した。

［副課題２］の成果として次の成果を得た。

新たなサイバー攻撃傾向の変化を検出する手法として、サイバー攻撃の初期段階として行われるポートスキャンなどの不特定多数を対象とした攻撃に着目し、攻撃の急激な変化を Change Finder によるスコア算出と、ボリンジャーバンドによる異常発見手法を考案した。

Change Finder は，時系列データの変化の度合いをスコアとして算出することができる手法であるが、パケット観測によって得られる時系列データの変化に敏感であった。

そこで、本研究では、Change Finder が算出したスコアに対して、統計的性質を用いた異常検知を行い、新たな攻撃出現をより正確に検出できる手法を考案した。さらに、本手法を、佐賀大学で観測したダークネットデータに適用し、その有効性を確認した。

５．主な発表論文等

〔雑誌論文〕（計２件）

① Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai,
Detection System for Distributed DoS Attacks Based on Automatic Extraction of Normal Mode and Its Performance Evaluation
Proceedings of the 10th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2017), 査読有, Lecture Notes in Computer Science (LNCS), Springer, Volume 10656, 461-473, 2017
DOI: 10.1007/978-3-319-72389-1

② Yoshiaki Hori, Seiichiro Mizoguchi, Ryosuke Miyazaki, Akira Yamada, Yaokai Feng, Ayumu Kubota, Kouichi Sakurai
A Comprehensive Security Analysis Checksheet for OpenFlow Networks
Proceedings of the 11th International Conference on Broadband and Wireless Computing , Communication and Applications (BWCCA 2016), 査読有, Lecture Notes on Data Engineering and Communications Technologies (LNDECT), Springer, Volume 2, 234-242, 2017
DOI: 10.1007/978-3-319-49106-6_22

〔学会発表〕（計２件）

① 今永 大遥，大谷 誠，堀 良彰，田中 久治
ダークネットを用いた新たなサイバー攻撃傾向の変化検出
火の国情報シンポジウム 2019，情報処理学会九州支部，2019，熊本市

② 溝口 誠一郎，宮崎 亮輔，山田 明，山本 幸二，窪田 歩，フォン ヤオカイ，堀 良彰，櫻井 幸一
端末ローミングを例としたマルチドメイン SDN アプリケーションのセキュリティ評価に関する考察
2017 年暗号と情報セキュリティシンポジウム（SCIS2017），2017，那覇市

６．研究組織

研究代表者単独で実施

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。