5V-07

SDN に基づく Moving Target Defense のセキュリティ機能の高度化に関する一考察

千葉 翔也 †1　小野 大地 †1　ギリエ ルイス †2　和泉 諭 †3　阿部 亨 †1,†4　菅沼 拓夫 †1,†4

†1 東北大学大学院情報科学研究科　†2 東北大学電気通信研究所
†3 仙台高等専門学校　†4 東北大学サイバーサイエンスセンター

1　はじめに

多くのサイバー攻撃では標的を調査するためのネットワークスキャンが行われる．そのスキャンで得た情報を元に攻撃が行われるため，ネットワークスキャン対策は重要である．しかし，ネットワーク型侵入検知システムなどの既存のスキャン検知手法では，長い時間をかけて少しずつネットワークをスキャンする低速スキャンの検知が課題となる．その解決策として，標的のホストアドレスを頻繁に変化させて資産を防御する Moving Target Defense（MTD）が提案されているが，MTD のみでは短時間に多くのホストをスキャンする高速スキャンへの対応が難しい．

本稿では，低速・高速スキャンの両方への対応を目指し，既存のスキャン対策と MTD の併用について検討する．特に，ネットワークの MTD ではアドレス変更をパケットヘッダの書き換えで実現するため，Software Defined Network（SDN）が実装に用いられることが多い．そこで本研究では，SDN に基づく MTD を基盤として，高速スキャンを検知するためのトラフィックモニタを導入し，スキャン元ホストの識別と遮断を行う仕組みを SDN の機能を活用し実装する手法を検討する．

2　関連研究

MTD は既存の製品やスキャン検知手法では対応が難しい低速スキャンなどの脅威に対処するために登場した．低速スキャンは，短期的な通信の増加といった特徴を示すことは少なく，その検知の難しさが課題となる．そのため，ネットワークの分野では，IP アドレスを定期的に変更することで標的の移動を実現し，スキャンを妨害するネットワークの MTD [1, 2] が多く提案されている．これらは定期的にアドレスを変更することで低速スキャンを妨害できるが，アドレスが変更されるまでの間に高速スキャンを行い標的に接続することで，新たな標的ホストへの攻撃が可能となる．

A Study on Improvement of Security Features for Moving Target Defense Based on SDN
Shoya CHIBA†1, Daichi ONO†1, Luis GUILLEN†2, Satoru IZUMI†3, Toru ABE†1,†4, and Takuo SUGANUMA†1,†4
†1Graduate School of Information Sciences, Tohoku University
†2Research Institute of Electrical Communication ,Tohoku university
†3National Institute of Technology, Sendai College
†4Cyberscience Center, Tohoku University

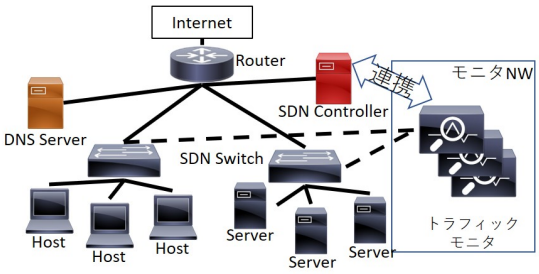

図 1: MTD 環境におけるモニタ NW の概要

また MTD の実装には SDN を用いることが多い．SDN の特徴として，ネットワークの構成を柔軟かつ動的に変更できる点がある．その特徴に着目し，MTD の実装に SDN を用いることで転送制御が容易になる．

高速スキャンに SDN に基づく MTD で対応する場合，アドレス変更間隔の短縮で実現できるが，アドレスの書き換えなどの処理をネットワーク機器が担うため，ネットワーク機器の負荷や通信遅延の増加が懸念される．そこで実際の運用では Intrusion Detection System（IDS）などの既存の製品やスキャン検知手法を用いた対策との併用が考えられる．先行研究として IDS との連携を考慮した MTD [2] があるが，そちらはポートスキャン検知を MTD のアドレス変更のトリガとして使うもので，不正な通信の遮断は検討されていない．

3　トラフィックモニタを導入した MTD システムの検討

3.1　概要

本章では，2 章であげた課題を解決するために，スキャン検知との併用を前提とした SDN に基づく MTD システムを検討する．本提案では，図 1 に示すように SDN に基づく MTD に，スキャン対策に用いるトラフィックモニタ用のネットワーク（以下モニタ NW）を構築する．

MTD が有効なネットワーク内の高速スキャンを検知するため，SDN スイッチは，モニタがスキャン検知に利用するトラフィックを収集しモニタ NW 上のモニタに転送する．モニタが高速スキャンを検知した場合は，SDN コントローラと連携し SDN スイッチを介して通信の遮断が行われる．また，MTD のアドレスランダム化が有効であるため，低

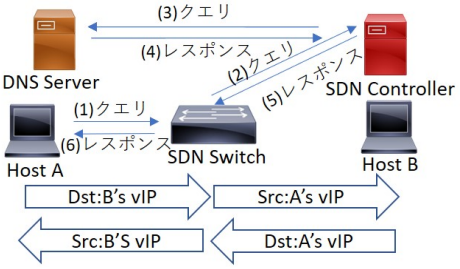

図 2: DNS を利用した vIP の取得と通信

速スキャンに対しての妨害効果が期待できる．

また，本提案ではモニタによる高速スキャン検知と SDN を利用した通信の遮断が可能なため，高速スキャンに対応するためにアドレス変更間隔を短くする必要がなく，ネットワーク機器の負荷や遅延の低減が期待できる．

3.2 DNS を用いた SDN に基づく MTD

本研究においては，実装の容易さと各ホストに対する透過性から，DNS を用いた MTD [1] を基盤として，システムの構築を行う．この手法では，各ホストに設定した実際の IP アドレス rIP とそのホストの rIP を隠蔽するために用いる仮想のアドレス vIP の 2 種類のアドレスを用いて定期的にアドレスを変化させるアドレスランダム化を行う．

図 2 に，ホスト間の通信開始時の vIP の取得とそれ以後の通信の流れを示す．MTD が有効なネットワークでは，セキュリティのために rIP によるアクセスがスイッチによってブロックされるため，各ホストは vIP を宛先として通信を行う．しかしネットワーク内のユーザが vIP の変化を常に把握し直接 vIP を宛先としてホストに接続することは難しく，ユーザは vIP ではなくホスト名でホストを指定し接続を試みる．その際，以下の手順でコントローラが名前解決に割り込み，DNS クエリ（以下クエリ）と DNS レスポンス（以下レスポンス）を書き換える．それによりユーザはその時点での vIP を取得し，通信できるようになる．

(1) ホスト A がホスト B に対するクエリを送信
(2) スイッチがコントローラにクエリを転送
(3) コントローラがクエリを DNS サーバに転送
(4) DNS サーバがレスポンスをコントローラに送信
(5) コントローラがスイッチにレスポンスの転送を指示
(6) スイッチがレスポンスをホスト A に転送

vIP 宛の通信は対応する rIP をもつホストへ転送されるため，ホスト A（以下 A）がホスト B（以下 B）の vIP に宛てた通信は B へと転送される．その際 A が送信するパケットの送信元アドレスは A の vIP に，宛先アドレスは B の rIP にスイッチが書き換えるため，各ホストに対して透過的である．また B が A にパケットを送信する場合も同様の操作を行い，A は B の vIP，B は A の vIP のみを知ることができ，この vIP は変更間隔を T として T 秒毎にランダムに変化するため，低速スキャンへの妨害ができる．

しかし，この手法は攻撃者が vIP のアドレス体系を推測・調査し vIP での直接接続を試みた場合，正規のユーザと同様に他のホストに接続できる．そのため本提案では，名前解決を経ない vIP への接続を検知して遮断する機能を追加することで，攻撃者への妨害能力の低下を抑える．

3.3 モニタ NW の構築と利用

本研究では高速スキャンを検知可能な既存のスキャン対策手法を利用できるネットワークを，モニタ NW として SDN を用いて構築する．また，MTD の実装には OpenFlow を用いることを想定しており，モニタ NW の構築にも同様に OpenFlow を利用する．このモニタ NW にトラフィックモニタを配置しスキャン対策を利用することで，高速スキャンを行うホストの識別を行い，SDN の機能を利用した通信の遮断が可能となる．

ネットワーク内の全トラフィックを利用するスキャン検知は，装置の帯域幅などの観点から難しい．そこで，本研究ではスキャン発生時に急増するといった特徴をもつことからスキャン検知に利用される事が多いフロー情報とブロードキャストパケットのみを転送して利用する．また，モニタ NW に転送する情報に含まれる IP アドレスはすべて rIP で表されるように実装することで，スキャン検知手法にアドレスの変化を解釈する仕組みが不要となり，既存のスキャン検知手法に対して透過的となる．トラフィックモニタがスキャンを検知し，スキャン元ホストを特定した場合は，コントローラにそのホストの情報を通知する．通知を受け取ったコントローラは，そのホストの通信を遮断するフローエントリをスイッチに書き込むため，MTD のみでは対応が難しい高速スキャンに対応できる．

4 おわりに

本稿では，高速・低速スキャン対策として，スキャン検知手法と MTD を併用するためのモニタ NW の構築を検討した．今後は，SDN に基づいた MTD を実装し，モニタ NW を構築することで生じる負荷の増加や通信遅延などの評価，通信遮断処理の実装などを行う．

参考文献

[1] J. H. Jafarian et al., “OpenFlow random host mutation: Transparent moving target defense using software defined networking,” HotSDN’12 - Proc. 1st ACM Int. Work. Hot Top. Softw. Defin. Networks, pp. 127–132, 2012, doi: 10.1145/2342441.2342467.

[2] Y. Shi et al., “CHAOS: An SDN-Based Moving Target Defense System,” Secur. Commun. Networks, vol. 2017, 2017, doi: 10.1155/2017/3659167.