ISS-SP-233

PKI と連携する OpenFlow 制御による オフィスネットワーク向け標的型攻撃対策の提案

鈴木 亮平† 李 中淳†† 鈴木 裕之††† 大山 永昭††† 小尾 高史†††
†東京工業大学工学部電気電子工学科 ††東京工業大学社会情報流通基盤研究センター
†††東京工業大学像情報工学研究所

1. はじめに

近年，情報システムを利用する分野での標的型攻撃の被害が顕著になっている。標的型攻撃とは，特定の組織や団体をターゲットとし，様々な手法を用いてその内部ネットワークに対して行われるサイバー攻撃の一種である。攻撃に用いられるマルウェアが標的組織用に改造されていることや，メールなどを用いて組織構成員の操作による感染を狙う等の点からマルウェアの感染を完全に防ぐことは困難とされる。そのため、標的型攻撃対策では，マルウェアに感染した場合でもいかにして被害拡大を抑えるかが課題の一つとなっている。本研究では OpenFlow を用いて適切なネットワーク制御を行うことで組織内ユーザ端末が標的型攻撃によりマルウェアに感染した場合でも，被害拡大を抑える方法の提案を行う。

2. 標的型攻撃の特徴

標的型攻撃では，攻撃者はユーザ端末にマルウェアを感染させた後，その端末を起点に徐々に内部ネットワークを侵害するという特徴があり，多くの場合最初にマルウェアに感染した端末が外部のサーバと通信を行い内部攻撃用ツールのダウンロード等を行う。ツールの入手後は内部ネットワークの探索が行われ，近隣端末へ攻撃を実行することで侵害が拡大する。このように標的型攻撃では，マルウェアによる内外のネットワークへの通信が，ユーザの認識外で行われることが特徴である。本研究では，このようなマルウェアによる通信を防止することで標的型攻撃の進行を抑制し，被害の拡大防止を狙う。

3. 提案手法

本研究では，ユーザ認識外の通信を防止するために，マルウェアによる通信の可能性があるものに対しては明示的な利用者確認を行う方法を提案する。具体的には予め業務等で想定される通信フローをリスト化しておき，通信フローを切り替える際に必要に応じて本人確認を行う。例えば外部サーバ等への通信要求に対して本人確認を要求する。ユーザの認識外のタイミングで本人確認を要求された場合は異変を察知することが可能となる。また，このような場合は，端末のマルウェア感染が疑われるため，端末を遮断する設定を行うことも可能である。本研究では，本人確認に PKI 機能を有するICカード認証を用いており，この認証結果に基づく通信制御を行うために動的にネットワーク構成の変更が可能な OpenFlow を利用している。

本研究で提案するシステム構成を図 1 に示す。内部ネットワークには OpenFlow スイッチと OpenFlow コントローラが含まれる。利用者認証は内部ネットワーク内の認証サーバで行うこととする。

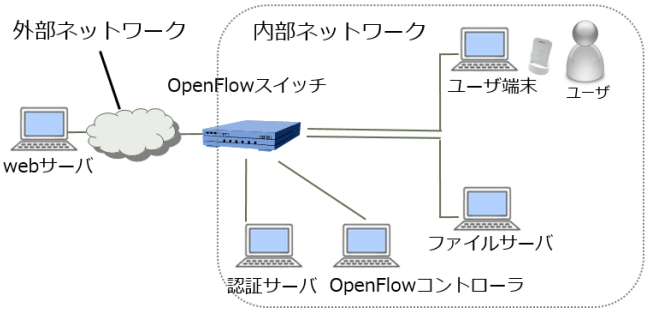

図 1. 提案システムの構成

4. 実験

試作システムを用いて動作確認を行い，マルウェアによる通信の疑いのある外部接続要求に対して利用者の認証要求が発生することを確認した。また，不審な通信が生じた場合にユーザ端末の接続を遮断できることを確認した。

5. 今後の課題

今後は試作したシステムを用いて通信速度等の評価を行い，その実用性を検証する予定である。

6. まとめ

標的型攻撃により端末がマルウェアに感染した場合に被害拡大を抑制するネットワーク制御手法を提案した。更に，実験システムにより基本性能の検証を行った。

参考文献

[1] 情報処理推進機構，”「高度標的型攻撃」対策に向けたシステム設計ガイド”,2014 年 9 月
[2] 情報処理推進機構，”標的型サイバー攻撃の事例分析と対策レポート”,2012 年 1 月
[3] 李 中淳ほか,信学技法 ICM2014-17,Nov.2014