

Smartphone Firewall

OpenFlow 対応 Wireless AP を用いた
柔軟なサイバー防御の研究開発

OpenFlow

SDN 技術の一つであり、複数のベンダが OpenFlow に対応したスイッチを提供しています。コントロールプレーンに相当するコントローラ機能も、複数のオープンソースプロジェクトにて開発されています。OpenFlow は Open Networking Foundation (ONF) により標準化が行われています。

OpenWrt

ネットワーク制御装置、とりわけ無線アクセスポイントなどに向けて開発されている、組み込みシステム用の Linux ディストリビューションです。OpenWrt プロジェクトによってオープンソースにて開発されています。

NECOMA の研究活動ならびに成果についての詳細は、Web サイト www.necoma-project.jp をご覧ください。

サイバー防御機能の設計

スマートフォンを狙ったマルウェアが増加しており、感染した端末を利用したサイバー脅威が予想される場所です。しかし、スマートフォンは計算性能やバッテリーの問題があり、複雑な防御を行うには適さないという制約があります。

NECOMA プロジェクトでは、SDN 技術をコアネットワークにおいてサイバー防御に応用する研究を推進し、PIX-IE に代表されるサービスが生まれました。その一方で、リーフネットワークにもサイバー防御を波及させることを目的とし、OpenFlow に対応した Wireless Access Point (AP) を用いるサービスも実現しました。

コントローラの実装と評価

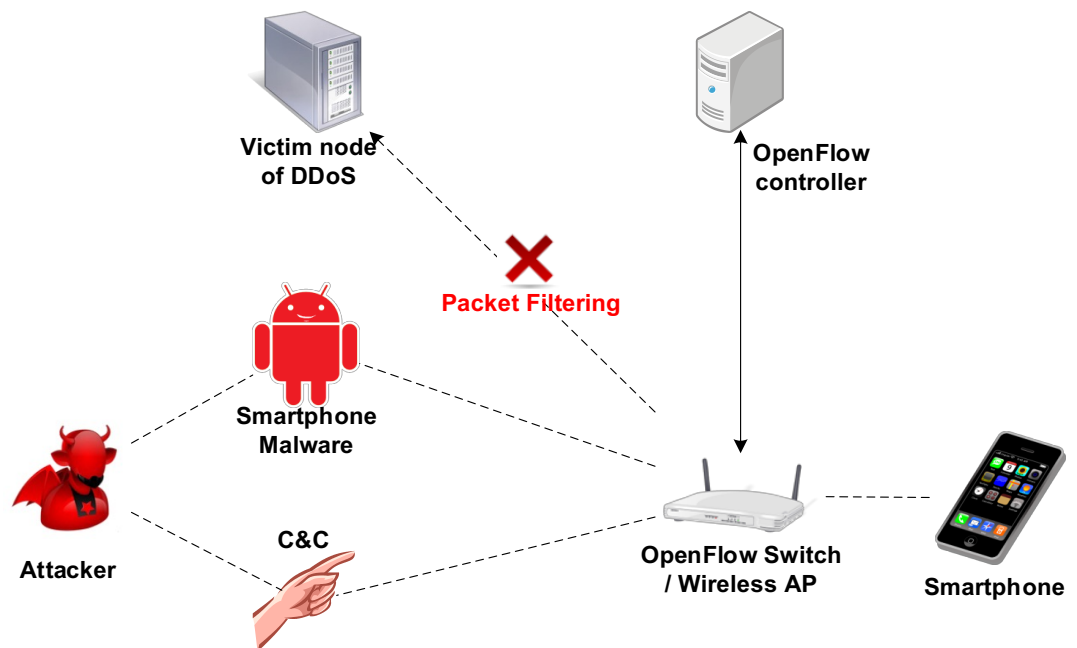
サイバー防御に必要なものは

- 1) 活用可能なサイバー脅威情報
- 2) サイバー防御を行うポリシー実施点
- 3) 柔軟にポリシーを制御できる機能

です。脅威情報は NECOMatter システムにて共有されている情報を、ポリシー実施点には OpenFlow 対応 Wireless AP を用います。これらに加えて、柔軟にポリシーを制御する機能が必要となります。

NECOMA プロジェクトでは、OpenFlow コントローラの機能として柔軟なポリシー制御が可能な RESTful API を実装し、オープンソースで提供しています。

※提供元 <https://github.com/necoma>



市販のプロードバンドルータ製品にファームウェアとして OpenWrt を導入し、SDN 拡張を行うだけで、OpenFlow に対応した Wireless AP が利用できます。NECOMA プロジェクトではこの AP を活用したサイバー防御に取り組みました。

【お問い合わせ先】

奈良先端科学技術大学院大学 情報科学研究科

インターネット工学研究室内

NECOMA プロジェクト事務局

Mail: fp7-necoma-pr@is.naist.jp

Web: <http://www.necoma-project.jp>