L-033

ネットワーク動的構成による高セキュリティLANの試作
Prototyping Highly-Secured LAN using Dynamic Network Reconfiguration

十場 裕 † 黄 宏軒 † 川越 恭二 †
Yutaka Juba Hung-Hsuan Huang Kyoji Kawagoe

1. はじめに

近年, ネットワーク接続可能な電子機器が増加している. プリンターや NAS(Network Attached Storage), テレビ, レコーダーに加えて, 最近では, 炊飯器や玄関ドアカメラ等の家電でもネットワーク接続可能である. これらの電子機器はネットワーク接続可能であるため, 利用者は遠隔で電子機器を使用できる. ネットワーク接続可能な電子機器のソフトウェアは, Linux などの OS やオープンソースソフトウェアをベースにして構築されていることが多い. また, 電子機器のソフトウェアバグの修正や機能の追加, さらに, OS 等のソフトウェアに関連するアップデートは, ネットワーク経由でのアップデートにより行うことができる.

しかし, サポートやサービス提供期間終了後でアップデートが提供されない場合や, 利用者によるソフトウェアアップデートが実行されていない場合等では, 電子機器が利用する OS やオープンソースソフトウェアに由来する脆弱性によって, 電子機器およびそれが接続しているネットワークが危険に晒される可能性がある. ネットワークの外からの攻撃はファイアウォールや侵入検知システムなどにより防ぐことが可能であるが, ネットワークの内部からの攻撃を防ぐことはできない.

そこで, 本論文ではこの問題を解決するために OpenFlow と侵入検知システムを用いて LAN 内のセキュリティを向上させるシステムを提案する. ソフトウェアでネットワーク構成を制御する OpenFlow を用いることで, LAN 内の通信をプログラマブルに制御することができる. これにより, 通信が必要な端末間のみの通信を許可することや, 不適切なプロトコルによるアクセスなどを遮断することが可能である. また, OpenFlow 単体では適切な端末間における許可されたプロトコル上での攻撃を防ぐことはできない問題も, 侵入検知システムと組み合わせることで対処することができる.

2.OpenFlow [1]

OpenFlow は, ネットワーク構成をソフトウェアで制御可能なネットワークスイッチである. OpenFlow ではパケットの転送を行う OpenFlow スイッチと転送先の決定や転送の可否を決定する OpenFlow コントローラで構成される. 従来のルータやスイッチでは個別に行った機器設定に従ってパケットの転送を行なっていた. 一方, OpenFlow では, そのコントローラがプログラムとして実装されるため, ネットワークトラフィックの流れをプログラムで制御することが可能になる. OpenFlow の主たるターゲットは, ネットワーク構成の制御を大規模に行う必要のあるデータセンター等での大規模ネットワークである [2]. 特に, データセンターでの運用自動化を目的に, サーバやストレージ等の仮想化技術との組みわせで利用されることが多い. また, OpenFlow を使用することで, ネットワーク構成を OpenFlow コントローラで一元管理できるため, ネットワークの管理コスト削減が可能である. 本研究では, 大規模ネットワークの構成制御で利用されている OpenFlow を, ネットワーク構成を動的に制御できるその特徴を小規模 LAN に適用することで, 高セキュリティLAN の実現を目指す.

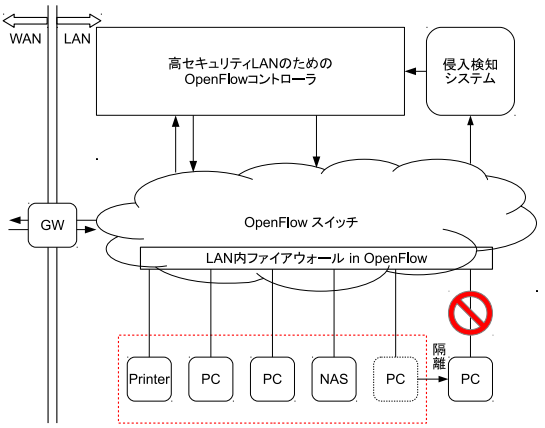

図 1: ネットワーク動的構成による高セキュリティLAN

3. ネットワーク動的構成による高セキュリティLAN システム

3.1. 目的

本セキュリティLAN システムは, LAN(Local Area Network) 内で利用されるネットワークプリンタや NAS などのネットワーク機器 (LAN 機器) が, 必要なアップデートが提供されない事で抱えている脆弱性に対して, LAN 内からの攻撃を防ぐためのシステムである. 具体的には, LAN 内での侵入検知機能と端末隔離機能により, LAN 内での通信内容から検知された侵入アラートによって当該端末を LAN からの隔離をリアルタイムに行うことを可能とする.

3.2.LAN システムの構成

図 1 に本 LAN システムの構成を示す.

図 1 に示すように, 本システムは, 主に OpenFlow スイッチ, それを制御する OpenFlow コントローラと通信内容を監視するための侵入検知システム (IDS) から構成されているいる. OpenFlow スイッチには, OpenFlow コントローラが生成した LAN 内ファイアウォールを実現する制御データが保持されている.

図 2 に, OpenFlow コントローラの内部構成を示す.

図 2 に示すように, OpenFlow コントローラは, 以下の 3 つのコンポーネントから構成されている.

- 転送判定部 : パケットを受け取り, その転送の可否を決定する.

† 立命館大学

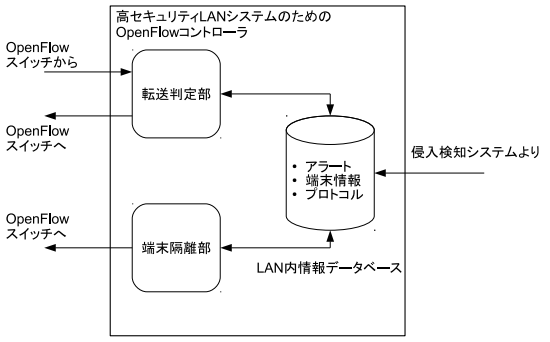

図 2: コントローラ内部構成

- 端末隔離部：侵入検知システムから送られる通信内容に関するアラートによって端末の隔離を行う.
- LAN 内情報データーベース : 転送判定部および端末隔離部の両者から参照される情報を管理する. 具体的には, 本データベースには転送判定部で利用する端末間の通信の可否に関する情報と利用可能なプロトコルに関する情報（以降, LAN 内端末情報）と, 端末隔離部で利用する侵入検知システムから送られてきたアラートに関する情報（以降, アラート情報）が格納されている.

3.3. 転送判定部

転送判定部は, OpenFlow スイッチから送られてくるパケットの送信元・送信先に関する情報 (MAC アドレス, IP アドレス, TCP/UDP ポート番号など) を LAN 内情報データベースに格納されている情報と逐次照合して転送の可否を判定する. これによって, OpenFlow スイッチでファイアウォールとしての機能を実現すると同時に, LAN を論理的なグループに分割し, 異なるポリシーで運用される端末をひとつの LAN に混在させることを可能にしている.

3.4. 端末隔離部

端末隔離部は, LAN 内情報データベースに格納された侵入検知システムからのアラートの内容を基に, 必要に応じて問題のある端末の LAN からの隔離を行う. 転送判定部では, 許可されている端末間やプロトコル上における攻撃を防ぐことはできない. このため, 侵入検知システムを利用し, 問題のある通信を行った端末を LAN から隔離することで転送判定部に不足している機能を補い LAN 内のセキュリティの向上を図る.

3.5.LAN 内情報データベース

LAN 内情報データベースには, アラート情報と LAN 内端末情報を格納する. 表 1 に, これらの情報を示す.

表 1 に示すように, アラート情報には, アラートを発生させた通信に関する情報と発生した問題に関する情報, その危険度などが含まれている. これらの情報は, 侵入検知システムから送られてくる. また, LAN 内端末情報には, その端末を識別するための MAC アドレスや端末間の通信の可否, 利用が許可されているプロトコルに関する情報などが含まれている. これらの情報は, LAN 管理者によって設定される. 端末の追加や変更が発生した場合に, 随時, LAN 内端末情報を変更可能である.

表 1: LAN 内情報データベースの格納情報

アラート情報	攻撃した端末に関する情報 (アラート情報)
	攻撃した状況に関する情報・危険度
LAN 内端末情報	端末識別用の MAC アドレス
	端末間の通信の可否
	利用可能なプロトコル

4. 高セキュリティLAN システムによる研究室 LAN 再構築

本システムは, OpenFlow スイッチに Open vSwitch [*1]を, IDS には Snort[*2]を用いて Linux 上に実装を行った. 実装に使用した計算機の構成は, OS:Debian GNU/Linux 6.0, CPU:Xeon E31220 3.10GHz, メモリ:8G である.

本システムを導入した後, 研究室 LAN において異常な通信を意図的に発生させ, 適切に端末が LAN から隔離されることを確認した. また, 本システムの導入によって正常な通信が妨げられることや, スループットに影響が無いことを確認した.

5. おわりに

本論文では, OpenFlow と侵入検知システムを用いて, LAN 内のセキュリティを向上させるための高セキュリティLAN システムを提案した. 本システムにより, ネットワーク機器が抱えている脆弱性に対する LAN 内からの攻撃を防ぐことができる. 通常のパーソナルコンピュータと異なりファイアウォールなどの自衛手段を持たないネットワーク機器のセキュリティを向上することが可能となる. 提案する高セキュリティLAN システムを試作し, 小規模な研究室 LAN に適用した.

現在, 攻撃の検知を侵入検知システムからのアラートのみに頼っているが, 今後は, マルウェアなどに対応できるよう他の攻撃検知方法の利用を検討する. また攻撃検知の際, 攻撃を行った LAN 内端末を LAN から隔離するが, LAN 内セキュリティを維持できる範囲内で隔離端末を利用可能とする機能の実現を行う.

参考文献

[1] OpenFlow Switch Specification Version 1.0.0, Dec 2009. http://www.openflow.org/documents/openflow-spec-v1.0.0.pdf.

[2] R. Sherwood et al. Flowvisor: A network virtualization layer, OPENFLOW-TR-2009-1, Stanford Univ. (2009).

[3] R.Braga et al. Lightweight DDoS flooding attack detection using NOX/OpenFlow, IEEE LCN'10(2010).

[*1] http://openvswitch.org/
[*2] http://www.snort.org/