

IoT デバイスの通信セキュリティ向上のための ホームネットワーク仮想化フレームワークの提案

Proposal of Home Network Virtualization Framework to Improve Communication Security of IoT Devices

塚崎 拓真 / Takuma Tsukasaki

1 はじめに

近年, IoT(Internet of Things) の可能性が注目され, 今後あらゆるモノがネットワークに接続, 利用されることが予想される. しかし, 従来ネットワークに接続されていなかったモノが接続されることにより, セキュリティ上のリスクも高まっている [1]. IoT デバイスは, 最低限の性能を発揮する CPU やメモリしか保持しておらず, 適用できる機能が限られるという問題がある. そのため, ログ出力や暗号化などのセキュリティ対策の適用は困難となる. また, 今後はホームネットワーク内で閉じたデバイス間の通信によって連携を行う形になることが想定され [3], 各デバイスにおいてアクセス制御等の更なるセキュリティ対策を行う必要がある.

そこで本研究では, コンテナ上にセキュリティ対策を施した Proxy を作成し, IoT デバイスに対して, 仮想的にセキュリティ対策を適用するシステムを提案する. また, OpenFlow を用いて, ホームネットワーク内の通信を監視するフレームワークの構築も検討する.

2 提案システム

2.1 システム構成

提案システムの構成を図 1 に示し, 詳細を以下に示す. 本提案システムは, IoT デバイス, Proxy, ルータ, OpenFlow コントローラから構成される.

- IoT デバイス

CPU やメモリなどのリソースを十分に保持しておらず, 直接セキュリティ対策を適用できないデバイスと定義する.

- Proxy

IoT デバイ스에要求されるセキュリティ対策を, コンテナ上で実現したものである. そして, IoT デバイスからの通信を中継し, セキュリティ対策を適用する.

- ルータ

IoT デバイス間通信の中継機器として用いる. ルータ上に Proxy の実行環境を生成する. 必要とされるリソースを提供することが可能である.

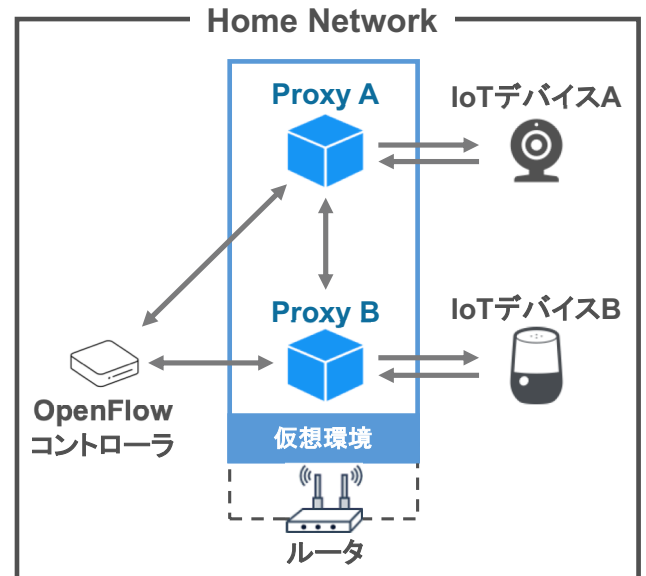


図 1: 提案システムの構成

- OpenFlow コントローラ

Proxy 内に作成された OpenFlow スイッチと通信を行い, ホームネットワーク内の通信を監視する. ホームネットワーク内部に設置する.

2.2 Proxy のセキュリティ対策

本研究におけるセキュリティ対策は, Proxy ごとに異なるセキュリティ対策を適用可能である. これにより, リソース制限が原因で IoT デバイスに直接適用できないセキュリティ対策を柔軟に適用できる.

コンテナ上で作成されるセキュリティ対策は, 各セキュリティ対策に対応したコンテナの image ファイルで定義される. IoT デバイスに適用したいセキュリティ対策が複数ある場合においても, 対象デバイスの規格に対応したセキュリティ対策をそれぞれ作成し, 組み合わせて定義することで, image ファイルを作成することが可能となる.

2.3 OpenFlow によるフローチェック

本研究におけるネットワーク監視を OpenFlow を用いて行う. 一つの IoT デバイスに対し, コンテナ上に OpenFlow スイッチの機能を生成する. IoT デバイスは, この OpenFlow スイッチを中継し, デバイス間通信を行う. OpenFlow

```

*** s3 -----
cookie=0x0, duration=41.578s, table=0, n_packets=11, n_bytes=1022, priority=1, in_port="s3-eth1", dl_dst=86:49:46:a5:a8:74 actions=output:"s3-eth2"
cookie=0x0, duration=12.852s, table=0, n_packets=10, n_bytes=924, priority=1, in_port="s3-eth2", dl_dst=4e:98:97:5f:fc:6e actions=output:"s3-eth1"
cookie=0x0, duration=89.081s, table=0, n_packets=73, n_bytes=9112, priority=0 actions=CONTROLLER:65535

*** s3 -----
cookie=0x0, duration=6.029s, table=0, n_packets=0, n_bytes=0, priority=1, in_port="s3-eth1", dl_dst=86:49:46:a5:a8:74 actions=output:"s3-eth2"
cookie=0x0, duration=6.020s, table=0, n_packets=3, n_bytes=294, priority=10, in_port="s3-eth2", dl_dst=4e:98:97:5f:fc:6e actions=drop
cookie=0x0, duration=53.532s, table=0, n_packets=65, n_bytes=8258, priority=0 actions=CONTROLLER:65535

*** s3 -----
cookie=0x0, duration=11.782s, table=0, n_packets=0, n_bytes=0, priority=1, in_port="s3-eth1", dl_dst=86:49:46:a5:a8:74 actions=output:"s3-eth2"
cookie=0x0, duration=59.285s, table=0, n_packets=65, n_bytes=8258, priority=0 actions=CONTROLLER:65535

```

図 2: 登録済みのホストのフローテーブル (上), 異常時のパケットを Drop 処理するフローテーブル (中), その後のアクションが削除されたフローテーブル (下)

コントローラは事前に IoT デバイスの情報を保持しており, OpenFlow スイッチとの通信が確立でき次第, デバイス間通信のフローテーブルを作成する. ホームネットワークの特性である各 IoT デバイスのトラフィック情報は既知であることや, 変化が大きいことを考慮し, IP アドレスや通信頻度の確認を行い, フローレベルにおける異常の検知を行う.

3 シミュレーション実験

3.1 評価内容

本研究の評価として, まずセキュリティ対策が適用されているかを検証した. 今回の異常通信としては, 未登録の IoT デバイスから通信があった場合と, 通信頻度が通常と異なる場合を想定した. その状況において, コンテナ上で作成した OpenFlow によるフローチェックが行われているかを検証した.

また, 提案システムの有効性を示すため, 提案システムを適用した上で, IoT デバイス間通信を 20 回行なった際のラウンドトリップタイムを計測した. 比較対象として, セキュリティ対策を適用せず, デバイス間通信を行う場合についても計測を行った.

3.2 評価環境

今回のシミュレーション実験においては, IoT デバイスや通信に関するログの収集・出力機能を実装し, セキュリティ対策として適用した. また, OpenFlow によるフローチェックも行った. 事前に 2 台のホストを設置した環境に, 新たに 1 台ホストを追加し, そのホストが通信要求を行う環境を作成した.

3.3 評価結果

登録済みの IoT デバイスから通信要求が来た場合, 登録していない IoT デバイスや, 通常の通信頻度と異なる等の異常の通信がなされている場合のフローテーブルの結果を図 2 に示す. 通常時は他のデバイスに対し, 通信を許可するフローテーブルが作成されている. 一方で, 異常時はパケットを Drop 処理するフローテーブルが作成されており, その後, そのフローテーブルが削除されていることが

わかる.

また, 提案システムは, セキュリティ対策を施していないシステムにおける通信より, ラウンドトリップタイムの平均値が約 1.06ms, 最大値が約 10.62ms 大きくなった.

4 考察

IoT デバイス情報を基に, フローレベルで制御できることを示した. 追加のフロー制御を行うことで, 更にセキュリティを高めることが可能である. また, 本提案システムは, セキュリティ対策なしの場合と比較し, 遅延が発生した. これは, Docker によって適用されたセキュリティ対策や OpenFlow によるフローチェックを行った際の負荷によるものである. しかし, Machine to Machine 接続におけるデバイス遠隔操作の遅延要件は約 100 ミリ秒とされているため, 許容範囲内である.

5 まとめ

本研究では, IoT のセキュリティ上のリスクにおいて, 今後, ホームネットワーク内で閉じたデバイス間通信が多くなり, 各 IoT デバイスにおいてアクセス制御等の更なるセキュリティ対策を行う必要があることに注目した. そこで, コンテナを用いた IoT デバイスへのセキュリティ対策の適用と, OpenFlow を用いたホームネットワーク監視を行うフレームワークの構築を提案した. そして, IoT デバイス間で閉じた通信を行うシミュレーション評価の比較を行い, 提案システムはホームネットワークにおいてセキュリティ要件を保つことと, 通信性能も許容範囲であることを示した.

参考文献

- [1] 総務省: IoT・5G セキュリティ総合対策 2020, 総務省 (オンライン), https://www.soumu.go.jp/main_content/000698567.pdf (参照 2022-03-28).
- [2] Ferrara, P., Mandal, A.K., Cortesi, A. and Spoto, F.: Static analysis for discovering IoT vulnerabilities, International Journal on Software Tools for Technology Transfer, Vol.23, No.1, pp.71-88(2021).
- [3] Pawar, P. and Trivedi, A.: Device-to-Device Communication Based IoT System: Benefits and Challenges, IETE Technical Review, Vol.36, No.4, pp.362-374(2019).