家庭内無線 LAN における「無線 LAN ただ乗りおよび不正アクセスポイント」 対策システムの開発

桧室 和馬†

神屋 郁子‡

下川 俊彦‡

†九州産業大学大学院

‡九州産業大学

1 はじめに

近年、様々な場所でインターネットを利用できるようになった。それを可能にしている技術の1つに無線 LAN が存在する。無線 LAN を用いることで、電波が受信できる範囲であれば場所を選ばずインターネットを利用することが可能である。現在利用されている無線 LAN として、駅やカフェに存在する公衆無線 LAN、学校内にあるキャンパス内無線 LAN、そして各家庭に存在する家庭内無線 LAN などが存在する。しかし家庭内無線 LAN は公衆無線 LAN やキャンパス内無線 LAN と比べ、IT やセキュリティに詳しい人間が管理しているとは限らないため攻撃対象になりやすい。現在の対策は事前防御のみ存在しており、攻撃された場合それを知るのは困難である。また、攻撃に対する明確な対策も存在していない。

そのため本研究では、脅威に晒されやすい家庭内無線 LAN を対象とした攻撃対策を目的としている。家庭内無線 LAN への脅威として主に無線 LAN ただ乗りと不正アクセスポイントの2つが挙げられる。このうち本研究では無線 LAN ただ乗りを扱う。

2 無線 LAN ただ乗り

無線 LAN ただ乗りとは、無断で第三者の無線 LAN を利用することである。これによる影響として、通信の盗聴や改ざん、ただ乗り無線 LAN 経由でのウイルス送信や外部への攻撃・違法ダウンロードなど不正行為の身元詐称が行われてしまう可能性がある。

無線 LAN ただ乗り方法自体はシンプルである。ただ乗り対象である無線 LAN に接続することで完了する。無線 LAN が暗号化されていなかった場合、接続を試みるだけでただ乗りできる場合が多い。

これに対する既存の対策としては暗号化、SSID ステルス、MAC アドレスフィルタリングの3つがある。しかし、これらの対策は効果的でない点が多い。

暗号化は暗号解析により解読されネットワークが利用される可能性がある。SSID ステルスは SSID の通知

を行わないだけで、そのネットワークを利用することは可能である。MAC アドレスフィルタリングは攻撃者端末の MAC アドレスを変更することで回避可能である。アクセスポイントに接続している端末の MAC アドレスは傍受することが可能である。

3 家庭内無線 LAN ただ乗り対策システム DeFRer

本研究で開発したシステム“DeFRer”(Defend from FreeRider)の設計を記す。DeFRer は家庭内ネットワークを監視し、ただ乗り端末を遮断するシステムである。監視および遮断手法については3.1、3.2で説明する。

3.1 無線 LAN ただ乗り監視手法

現在、無線 LAN ただ乗りがいつ行われているかを知るには困難である。ユーザが家を離れている間にもただ乗りが行われる可能性がある。つまり、家庭内無線 LAN を常に監視し、検知・通知そしてただ乗り端末を遮断する必要がある。

本研究では無線 LAN ただ乗り検知手法としてブラックリスト、ホワイトリストの2つを用いる。接続を許可する端末の MAC アドレスをホワイトリストに、許可しない端末の MAC アドレスをブラックリストに登録する。ホワイトリストに登録された端末は通常通り利用することができる。しかしブラックリストに登録された端末の接続が検知された場合は、自動的に該当端末に対して遮断処理が行われる。どちらのリストにも存在しない MAC アドレスを持つ端末が接続された場合、ユーザへ通知する。通知を受けたユーザはその後、検知された端末を遮断するかどうかを選択する。

3.2 無線 LAN ただ乗り端末遮断手法

遮断手法として本研究では ARP Spoofing とパケットフィルタリングを用いる。

ARP Spoofing は ARP cache poisoning と呼ばれる。対象機器がネットワーク接続の際に送られる ARP リクエストに対する ARP リプライを、別の機器が正規のルータよりも先に出すことで対象のアクセス先を自身

†Kazuma HIMURO ‡Yuko KAMIYA ‡Toshihiko SHIMOKAWA
†Kyushu Sangyo University Graduate School
‡Kyushu Sangyo University

へ誘導する。これにより正規のルータになりすまし、自身を介してネットワークを利用させる技法である。

パケットフィルタリングとは、指定したパケットが送られてきた場合に遮断し、ネットワーク利用に制限をかける技法である。

本研究ではこの2つの技法を合わせ、対象の端末を ARP Spoofing によって DeFRer に誘導しパケットフィルタリングを行い遮断することで、無線 LAN ただ乗り対策を行う。

3.3 DeFRer の設計

設計したシステムの構成とホワイトリスト自動登録機能、監視デーモン、遮断プロセス、通知機能について説明する。

3.3.1 システム構成

本システムは検知・通知を行う監視デーモン、ユーザが操作を行う WebUI の2つで構成される。守りたい家庭内無線 LAN と同一セグメント上に監視デーモンを配置する。WebUI を提供する Web アプリケーションはどこに配置してもいい。ただし、この Web アプリケーションと監視デーモンは共通のデータベースを参照する。

3.3.2 ホワイトリスト自動登録機能

監視デーモンを起動した際に同一セグメントに接続している端末を自動的にホワイトリストに登録する機能である。これによりユーザによるホワイトリストへの端末登録の負担が減ると考えた。

3.3.3 監視デーモン

監視デーモンは一定周期でネットワーク上に存在する端末とブラックリスト、ホワイトリストに登録されている端末情報とを比較する。この際ブラックリストに登録されている端末がネットワーク上に存在する場合、遮断プロセスを起動する。ネットワーク上に存在する端末情報が、どちらのリストにも存在しない場合、登録されているメールアドレスに対しメールを送信し、未登録端末の存在を通知する。

遮断されている端末がネットワーク上から存在しなくなった場合、またはブラックリストから削除された場合、自動的に遮断プロセスを停止させる。

3.3.4 遮断プロセス

監視デーモンにより自動的に起動するプロセスである。ARP テーブルを確認しブラックリストに登録されている MAC アドレスと比較することで、該当端末の

IP アドレスを特定する。その IP アドレスに対して ARP Spoofing を行いパケットを DeFRer へ誘導する。また、パケットフィルタリングを同時に行うことで該当端末へ遮断を行う。

3.3.5 通知機能

本システムによるユーザへの通知はメールにより行う。通知先メールアドレスは WebUI から登録する。監視デーモンにより未登録端末が検出されると、登録しているメールアドレスに対して未登録端末検知の通知メールを送信する。

3.3.6 未登録端末登録機能

これは WebUI の機能である。監視デーモンにより検出された未登録端末の MAC アドレスとベンダー名を表示する。ユーザは表示されている未登録端末を選択し、ホワイトリストまたはブラックリストに登録する。これによりユーザは MAC アドレスを入力することなく登録することができる。このブラックリストは 3.3.3、3.3.4 で述べた監視デーモンと遮断プロセスで利用される。

4 DeFRer の実装

実装環境として OS は KaliLinux を用いた。KaliLinux とは、ペネトレーションテストで使用するツールをまとめた Debian ベースの Linux ディストリビューションである。遮断手法である ARP Spoofing を行うためのパッケージである dsniff がデフォルトで導入されているため、これを用いた。

また、本システムを搭載する端末として Raspberry Pi 2 MODEL B を用いた。これは小型で本システムによるネットワーク監視が可能であり、Web サーバとしても機能するためである。

開発言語としては Ruby 2.1.5、Web フレームワークに Ruby on Rails 4.2.4、データベースには SQLite3 を用いた。

5 まとめ

本研究では家庭内無線 LAN ただ乗り対策システムとして “DeFRer” を開発した。

現在の問題は、本システムに対する攻撃対策が不十分な点である。そのため今後の課題として本システムに対する攻撃対策を行う必要がある。