ARP テーブルスプーフィング攻撃のリスク評価

北原 拓海 † 菊池 浩明 †

明治大学 総合数理学部 †

1　はじめに

近年はテレワークの普及に伴い，家庭内 LAN におけるセキュリティ対策が問題になっている．通信内容の盗聴や，スプーフィングを利用してフィッシングサイトに誘導するといった脅威にさらされている．中でも，IP アドレス導出プロトコル ARP には認証機能がなく，容易に偽造される脅威が潜在しており，多くの攻撃ツールが入手容易な状態にある．

そこで，本研究ではルータへの通信を盗聴する中間者攻撃を実現する ARP スプーフィングを行うツールに対する，ARP を用いて家庭内ネットワークの構築を管理している商用セキュリティ機器ウィルスバスター for Home Network の耐性と，ARP 偽装の強度を明らかにすることを目的とする．ARP テーブルの時系列変化を観測する実験を行い，ARP パケットの送信間隔などの要因を調査する．

2　準備

2.1　ARP スプーフィング

ARP(Address Resolution Protocol) は LAN 内のホストの IP アドレスと MAC アドレスを紐付けるための 2 層のプロトコルである．ARP では ARP パケットの内容が正しいことを仮定し，正しさを検証する方法が備わっていない．悪意を持った攻撃者が偽りの ARP パケットを送信することで，本来のルータとホストの間の経路 1 を攻撃者 IP3 を経由する偽の経路 2 に変更する攻撃を ARP スプーフィングという．

2.2　ウイルスバスター for Home Network(VBHN)

VBHN はトレンドマイクロ株式会社が発売しているセキュリティ対策機器である，家庭内ネットワーク内の通信を監視してネットワーク内の端末に対しての攻撃のブロックやインターネットへのアクセス管理を行う．

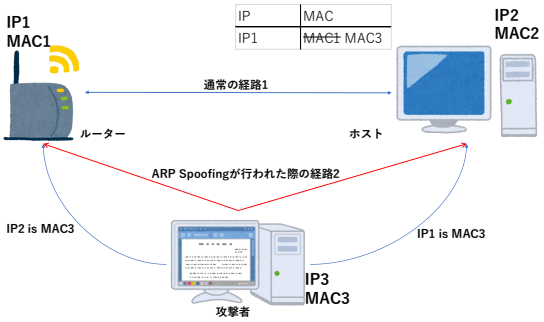

図 1　ARP スプーフィング

VBHN は通信を監視するためにネットワーク内の全端末にプロキシ ARP を行い，パケットが VBHN を経由するようにすることでこれらのセキュリティ対策を実現している．

3　実験

3.1　実験目的

ARP スプーフィングが行われるとホストの ARP テーブルでルータの IP アドレスに対応した MAC アドレスが変化する．しかし，複数のツールが混在する環境では，パケットの一部のみ中継されて，通信品質が不確定である．従って，ARP スプーフィングツールに対するネットワーク管理の安全性を正確に評価するためには，各ホストの ARP テーブルの変化をミクロに観測する必要がある．そこで，ARP テーブルの時系列変化を観測して，各種ツールのリスクを定量化することを本研究の目的とする．

3.2　観測ツールの開発

本ツールは ARP テーブルの変化の検知を行う．Python で作成した観測ツールのアルゴリズムを図 2 に示す．ではホストの ARP テーブルを 0.1 秒毎に観測し，ルータの IP アドレスに対応した MAC アドレスの変化を表示する．ホストが ARP テーブルを保有していた累積時間を集計し，計測終了後に表示する．

†Takumi Kitahara, Hiroaki Kikuchi, Risk Evaluation of ARP Table Spoofing Attacks, School of Interdisciplinary Mathematical Science, Meiji University.

表 1　2 台同時に ARP スプーフィングを行った際の ARP テーブルの保持期間

	VBHN[s]	scapy[s]	ettercap[s]	dsniff[s]	平均 [%]
VBHN		25.55(42.64%)	46.83(84.06%)	18.19(31.47%)	52.72
scapy	34.26(57.35%)		50.85(84.44%)	21.69(36.01%)	59.26
ettercap	8.88(15.93%)	9.37(15.55%)		7.27(12.11%)	14.53
dsniff	39.61(68.52%)	37.59(62.41%)	52.75(87.88%)		72.93

入力 調査対象 IP アドレス x, 競合する MAC アドレス m_1,m_2

1. ARP テーブルを確認する
2. x に対応している MAC アドレスが m_1 か m_2 か記録する
3. 1. から 2. を決められた時間繰り返す
4. ホスト別の ARP テーブル保有累積時間を求めて出力する

図 2　プログラムのアルゴリズム

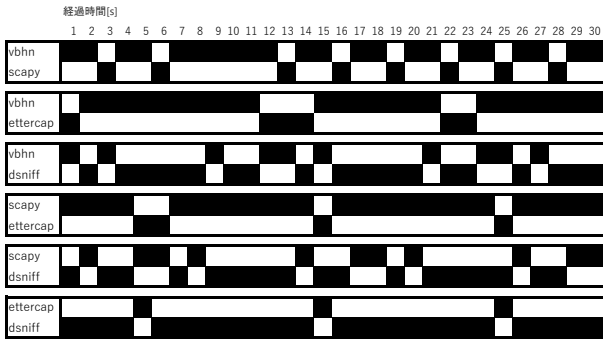

図 3　ARP テーブルを支配していたホストを示すタイムチャート

3.3　実験方法

本実験では複数の攻撃者が同時に一つのホストに ARP スプーフィング攻撃を行った際にその攻撃を受けたホストの ARP テーブルの変化の違いを観測することで ARP スプーフィング攻撃のリスクの調査を行う．実験環境は家庭内のネットワークである．ホスト A は Windows 10 である．本実験では VBHN とその他 3 つの ARP スプーフィングを行うツール，scapy，ettercap, dsniff について，このうち 2 つを選び同時に ARP スプーフィングを行った際の A の ARP テーブルの変化の違いを調査する．

開発したツールを用いて測定を行い，得られた 60 秒間の ARP テーブルの変化と，どの機器がどの期間 ARP テーブルを支配していたか記録する．

3.4　実験結果

2 台同時に ARP スプーフィング攻撃を行った際の結果を表 1 に示す．複数ツール同士の実験では，ARP パケットの送信間隔が短いものの方が ARP テーブルの保持期間が長かった．一方 VBHN と scapy の様にパケット送信間隔が同じ 3 秒のツール同士の実験については，実験の度に ARP テーブルの支配時間が変化して安定していなかった．ARP テーブルの支配している時間を図 3 のタイムテーブルに示す．

3.5　考察

2 台のツールを同時に動かした実験 2 では，パケットの送信間隔が同じである VBHN と scapy の組を除く 5 つの組み合わせにおいて ARP パケットの送信間隔が短いツールの方が平均 74.11% の期間ホストの ARP テーブルを支配していた．前述の VBHN と scapy で結果にばらつきが見られたことについては 2 つのツールを開始させるタイミングに依る要素が大きいものとる考える．

4　おわりに

本実験では ARP スプーフィングを行う 4 つのツールについて 2 つ同時に動作させた際の ARP テーブルの変化を観測した．ARP テーブルの保持期間には ARP パケットの送信間隔が関係しており，パケットの送信間隔の異なるツール同士が同時に ARP スプーフィングを行った場合にはパケットの送信間隔が短いツールのほうがより長い時間ホストの ARP テーブルを占有する．

参考文献

[1] 三宅猛ほか “ARP テーブルの集中管理による認証ネットワーク上の不正接続検出と排除方法の提案”，情報処理学会研究報告，2008-CSEC-40，2008.

[2] 住友 “ARP スプーフィング攻撃の調査”，2020 年度菊池研究室卒業論文，2020.