ARPテーブルスプーフィング攻撃のリスク評価

明治大学 北原 拓海，菊池浩明

背景：ホームセキュリティ

- ウイルスバスター for Home Network(VBHN)
- トレンドマイクロが発売しているセキュリティ対策機器
- ネットワーク内の端末の通信を監視するためにプロキシARPを行い，パケットがVBHNを経由するようにしている

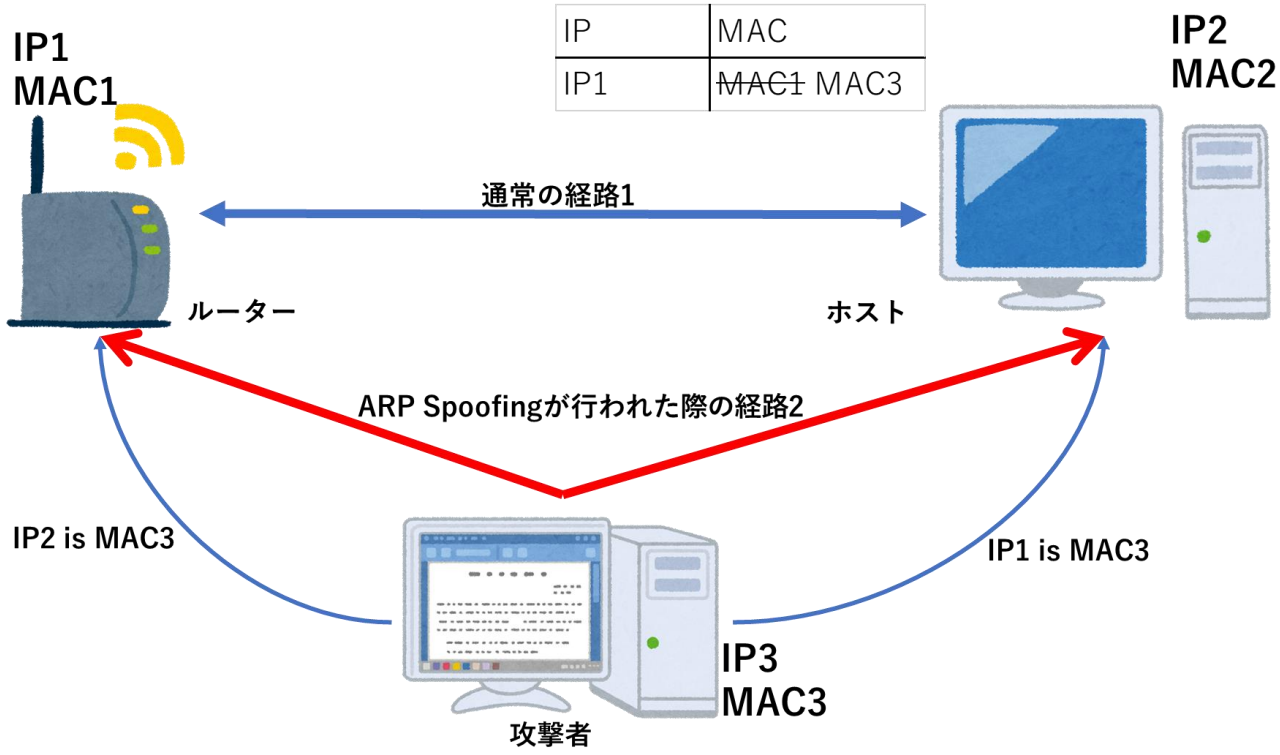
https://www.trendmicro.com/ja_jp/forHome/products/vbhn.html

ARPスプーフィングの脅威

- ARP(Address Resolution Protocol)で得られたIPアドレスとMACアドレスの関係の記録は**ARPテーブル**に保存される
- ARPにはパケットの内容が正しいか検証する方法が備わっていない

偽のパケットを送ることで経路を変えられてしまう

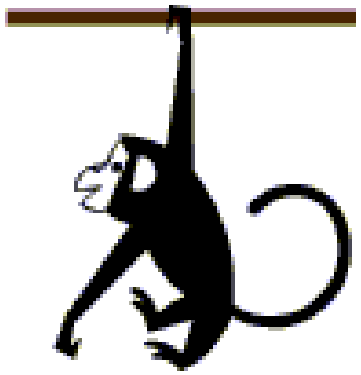
→**ARPスプーフィング**



ARPスプーフィングを行うツール

- 多くの攻撃ツールがあり容易に入手可能

- 今回使用したツールと本来の用途
  - Ettercap…ネットワーク及びホストの解析
  - Dsniff　…ネットワークの監査及びペネトレーションテスト
  - Scapy　…パケットの操作



Dsniff

問題点

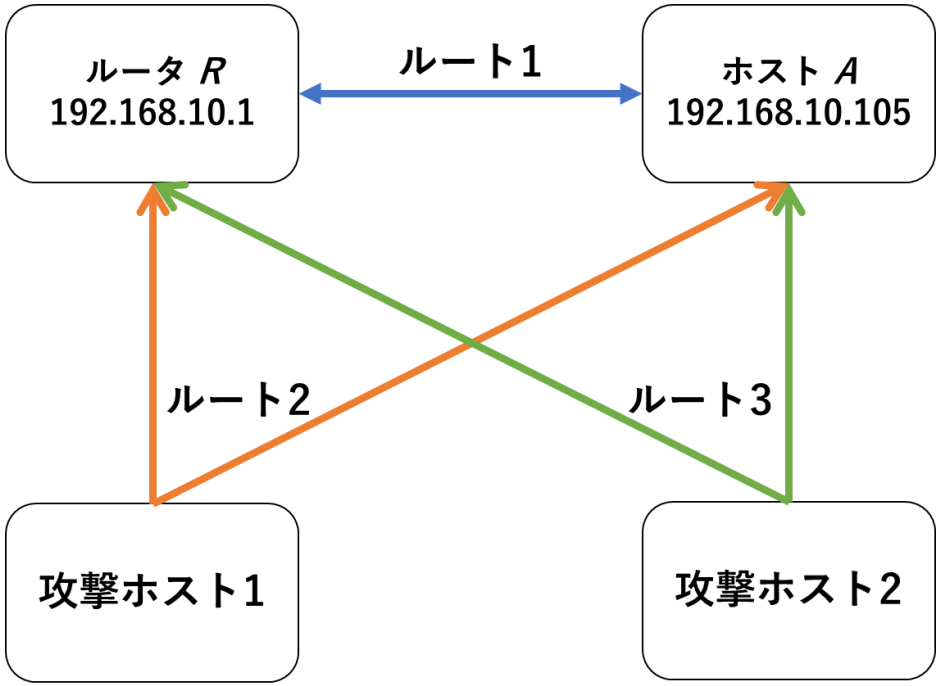
VBHNはARPスプーフィングに対して脆弱か？

- VBHNとARPスプーフィングのツールがやっていることは同じ
- ツール同士が競合するなかでVBHNは正常に動作できるのか？

研究目的

- VBHNのARPスプーフィングに対する耐性について不確定で評価が困難

- 解決策
  - ホストAのARPテーブルの変化を観測するPythonプログラムを作成
  - 得られたログをタイムチャートにする



使用ツール: scapy, dsniff, ettercap

プログラムの内容

1. ホストのARPテーブルを確認する
2. 調査対象 IP アドレスに対応しているMACアドレスの変化を記録する
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

出力されたログ(一部)

2021-11-14 21:54:36.228958: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:45.761540: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:46.181296: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:55.904047: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:56.178663: 192.168.10.1 changed to d0-c6-37-a5-24-63
router=0:00:00, b=0:00:07.279810, c=0:00:52.755185

実験内容

- 実験1
  - 4つのツールについて，**1つ**ずつARPスプーフィングを行った時のホストのARPテーブルの変化の仕方を調査する

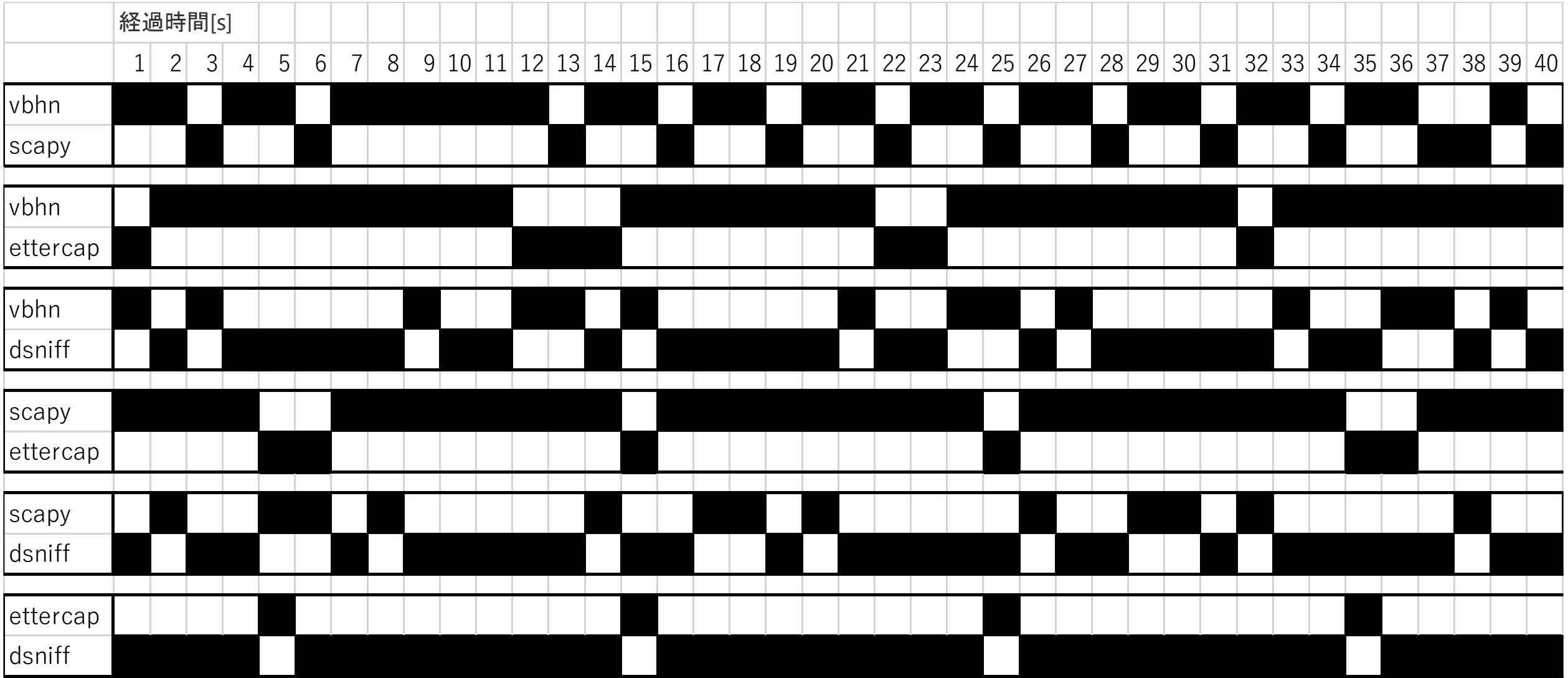
- 実験2
  - 4つのツールのうち**2つ**を選び，同時にARPスプーフィングを行った際のホストのARPテーブルの変化の違いを調査する

実験1 単独ツールでの結果

- VBHNとettercapは計測中は常にARPスプーフィングを行っていた
- 一方，scapyは1.15秒間，dsniffは1.95秒間ルータにARPテーブルを書き換えられていた

ツール	送信間隔[s]	計測時間[s]	テーブルを支配していた累積時間[s]	割合[%]
VBHN	3	60.24	60.24	100
scapy	3	60.51	59.36	97.93
ettercap	10	60.89	60.89	100
dsniff	2	59.29	57.34	98.71

実験2 タイムチャート(一部)



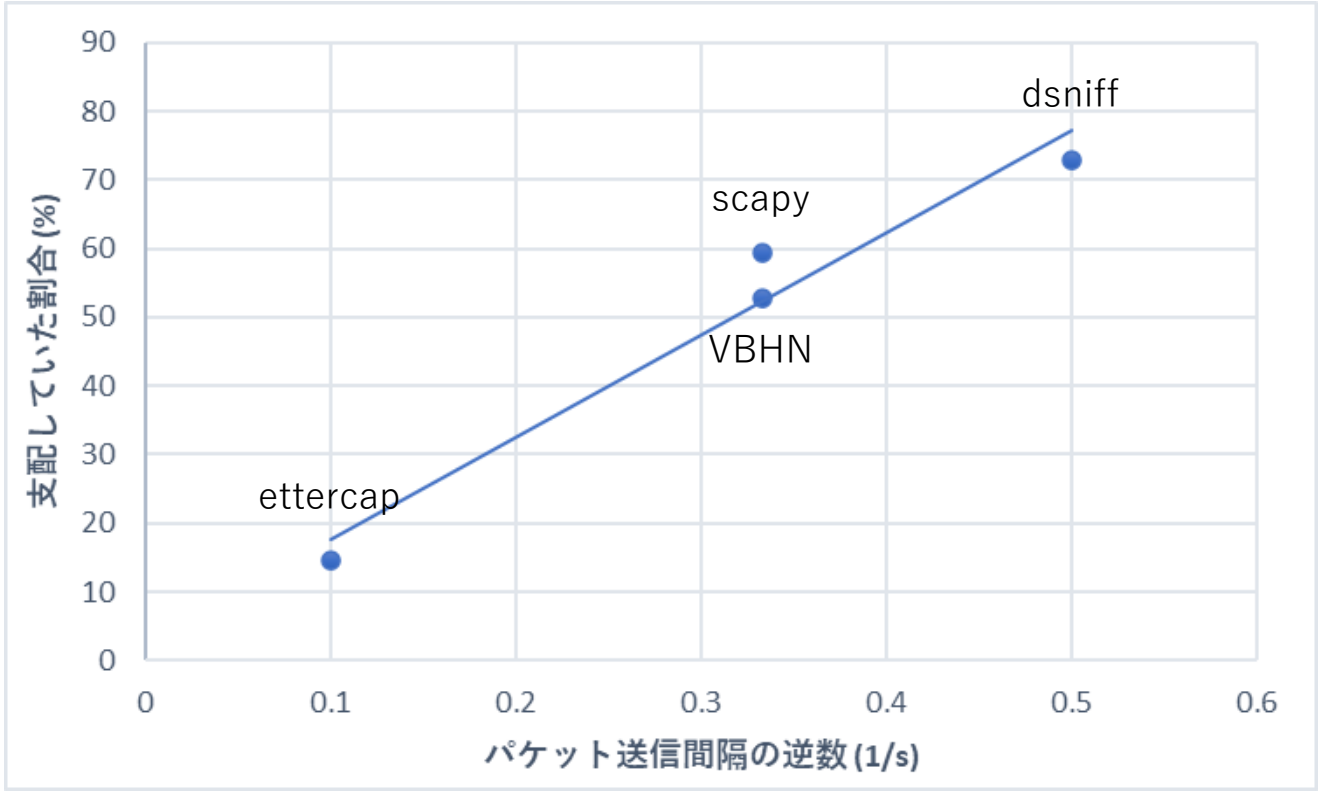
実験2 2つのツールでの結果

- ARPパケットの送信間隔が短いものの方がARPテーブルの支配時間が長かった
- 一方VBHNとscapyの様にパケット送信間隔が同じツールの実験は，結果が安定してなかった

	VBHN[s]	scapy[s]	ettercap[s]	dsniff[s]	平均[%]	送信間隔[s]
VBHN		25.55	46.83	18.19	52.32	3
scapy	34.26		50.85	21.69	59.26	3
ettercap	8.88	9.37		7.27	14.53	10
dsniff	39.61	37.59	52.75		72.93	2

考察

- 実験2より、パケットの送信間隔が安全性を左右する要因ということを実験的に検証し、明らかにした。



結論

- 実験2ではパケットの送信間隔が短いツールがホストのARPテーブルを平均74.11%の時間支配していた
- 4つのツールの中ではパケットの送信間隔が一番短いdsniffが最もテーブルの支配時間が長かった

- 今後の課題
  - ARPパケットの送信間隔を狭めすぎると動作しなくなる恐れがあるので調査したい