DNSPD: Entrap Botnets Through DNS Cache Poisoning Detection

p1t1r

HITCON 2010

自介

- Hi, this is p1t1r
- 資安背景
  - Rootkit
  - Web
  - Network
    - DNS spoofing

DNS攻擊

- DNS Cache Poisoning攻擊
  - 很危險的東西，迄今尚未被解決
  - 你上的任何網站都有可能是攻擊者的網站
- 防禦機制
  - 一大堆
  - 不過預設的DNS環境是未受保護的

DNSPD

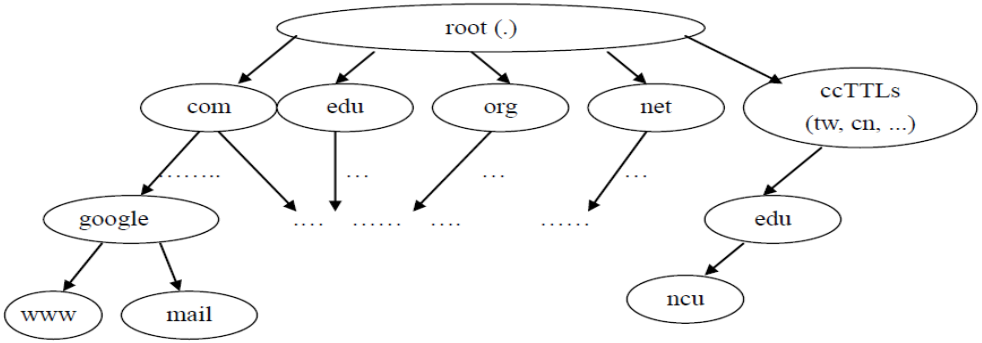
- 防禦，順便抓 Botnet
  - Botnet 正夯 !!!
- 問題：
  - 這個防禦機制夠穩當嗎?
    - 要看攻擊者的人品
  - 其他機制也可以抓，要你何用?
    - 好像可以快一點、準一點
  - 應該還有不少問題...
    - ……!!

DNS 簡介

- 功用
  - 將domain name 對應至 IP Address(es)
  - www.google.com <-> 74.125.153.103, …, etc.
- 特點
  - 大多採用UDP連線
    - 快
  - 先到的答案，就是正確的答案
    - (?)

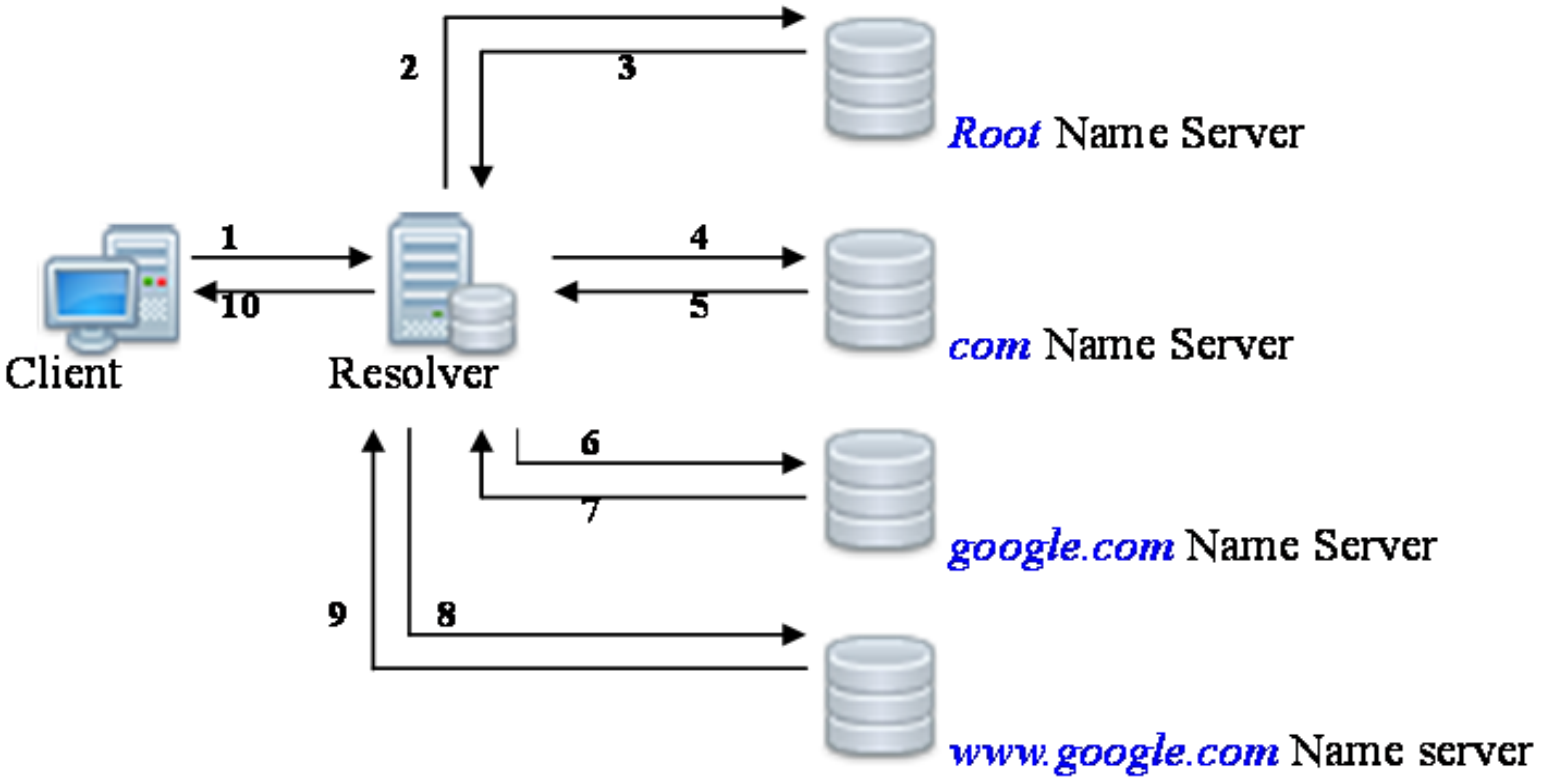
DNS 結構

- Domain Name Space



- Name Server
  - 儲存/管理 特定的domain name
- Resolver (cache server)
  - 暫存之前查詢過的資料(domain name & IPs)，方便快速回應
  - 保存資料，直到 TTL 過期
  - 攻擊者的主要目標!!!

DNS 運行方式


2
3
Root Name Server
1
10
4
5
com Name Server
Client
Resolver
6
7
google.com Name Server
9
8
www.google.com Name server

DNS Resolver 面對的威脅

- UDP封包可以偽造來源IP
  - 難以認證資料的可信度
- Resolver 如何驗證資料正確性?
  - 答案必須對應之前提出的問題
  - 來源IP 要符合
  - Port Number 要符合
  - Transaction ID 要符合

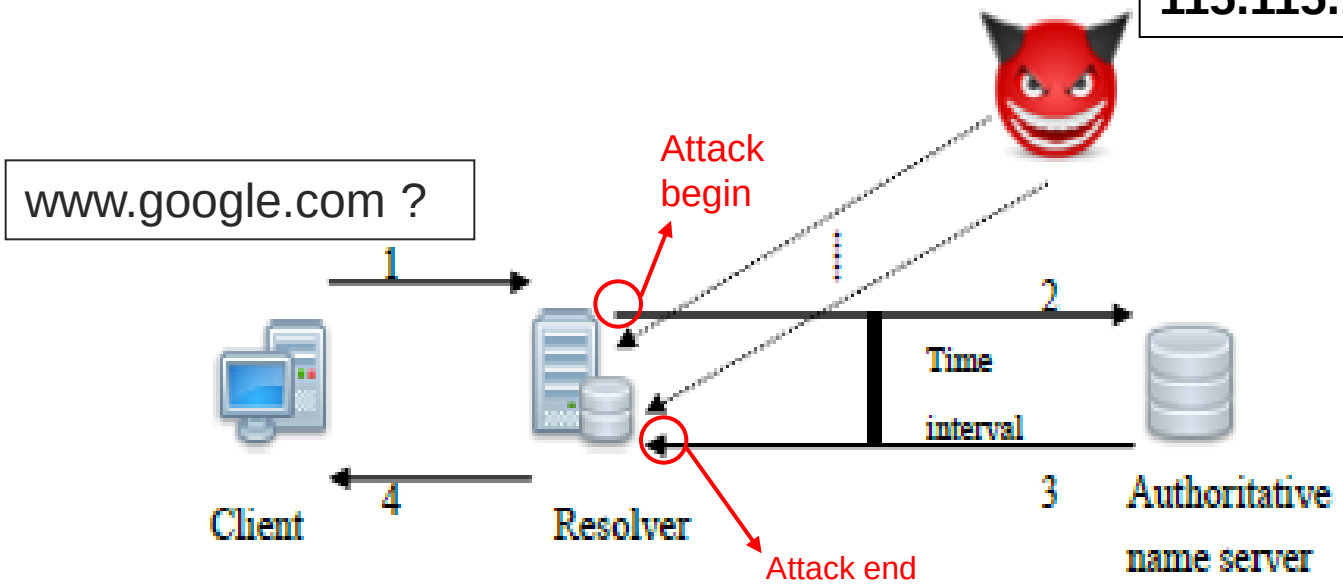
DNS Cache Poisoning 攻擊

- 攻擊目標
  1. 先選 DNS Cache主機 (Resolver)
     - Google Public DNS - 8.8.8.8
  2. 再選 特定domain
     - 例如: 將 blog.hitcon.org 的IP改成 攻擊者的IP

- 攻擊發起時機
  - 目標domain的資料，不存在Resolver的cache中
  - Resolver向外部name server發出詢問，而且尚未收到答案前

傳統 DNS Cache Poisoning 攻擊

相信我….
你要的答案是
115.115.115.115



實際上
www.google.com:

64.233.183.99
64.233.183.103
64.233.183.104
64.233.183.105
……

傳統攻擊之缺點

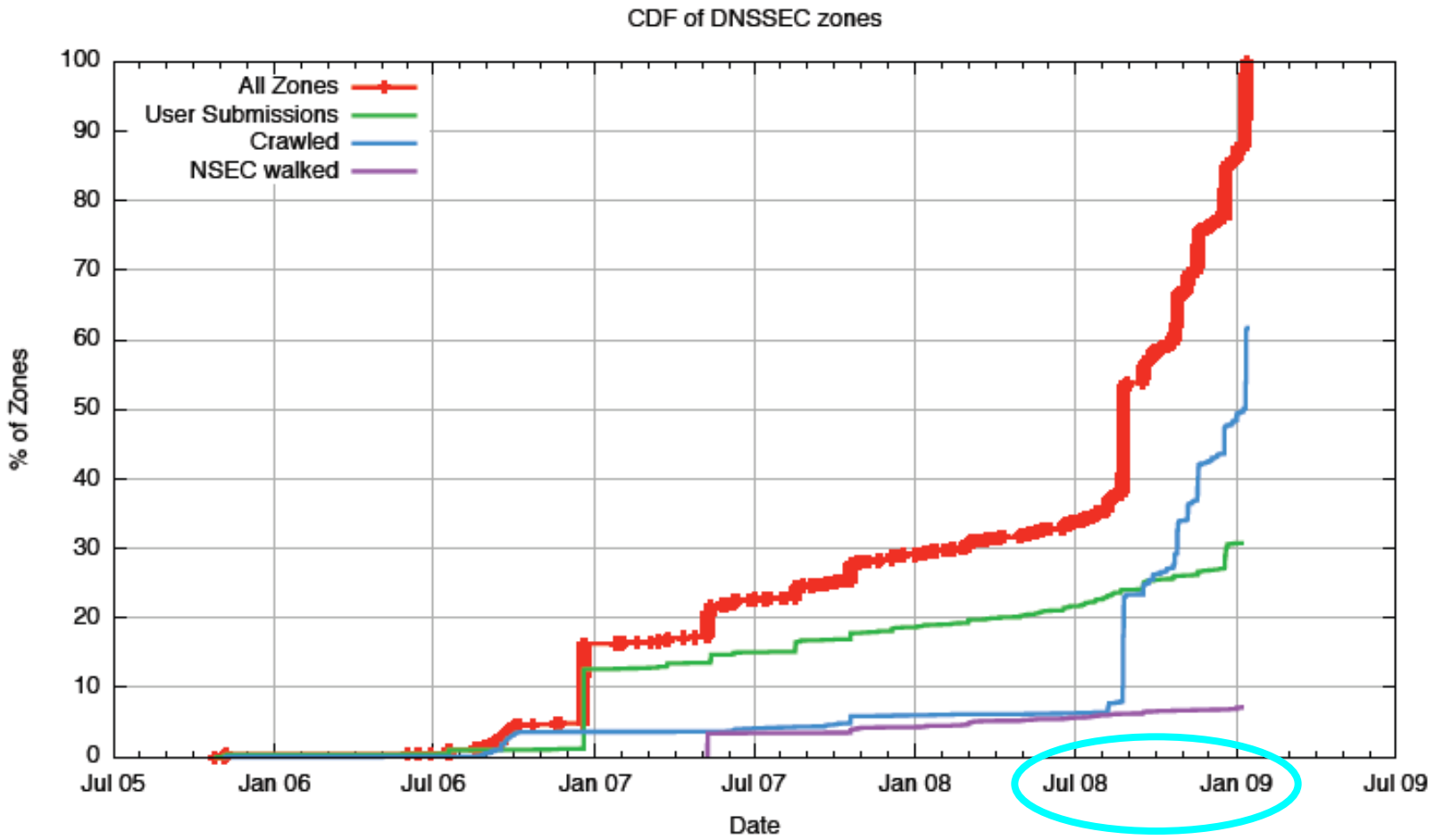
- 每次失敗都要等! 等! 等!
  - 等 TTL過期
- 若是TTL很長
  - 三秒捕魚，兩天曬網

Dan Kaminsky

- Black Hat USA 2008
- DNS Cache Poisoning Attack
  - 不用再爲TTL煩惱了！
  - 隨時可以發起攻擊
  - 想打多久也隨便你
- 適用BIND9任何版本
  - 不過，難度不同
  - v9.4.2之後，增加了random port

Kaminsky 效應：DNSSEC熱銷

From: "*Deploying and Monitoring DNS Security (DNSSEC)*"

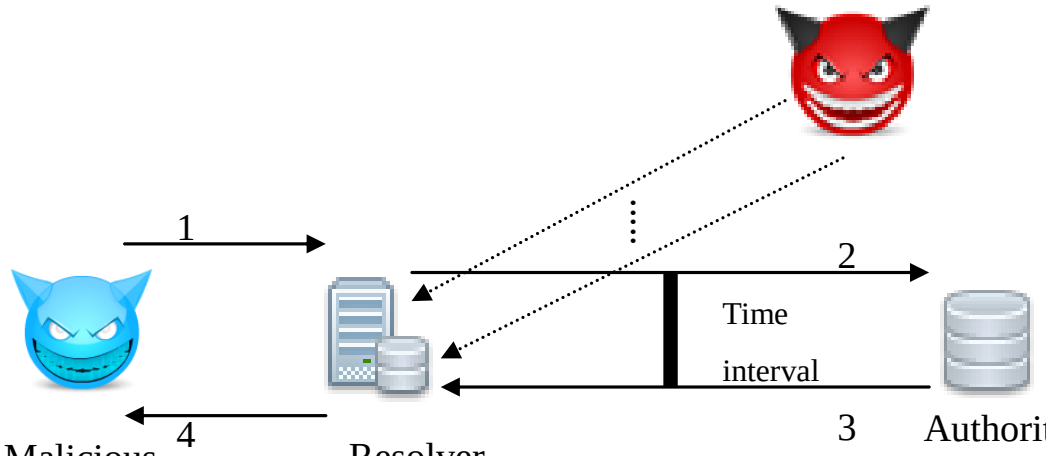


Kaminsky's Poisoning Attack

我是 **www.google.com**，
我來自**115.115.115.115**
你要找的答案 **並不存在**
請相信我喔~

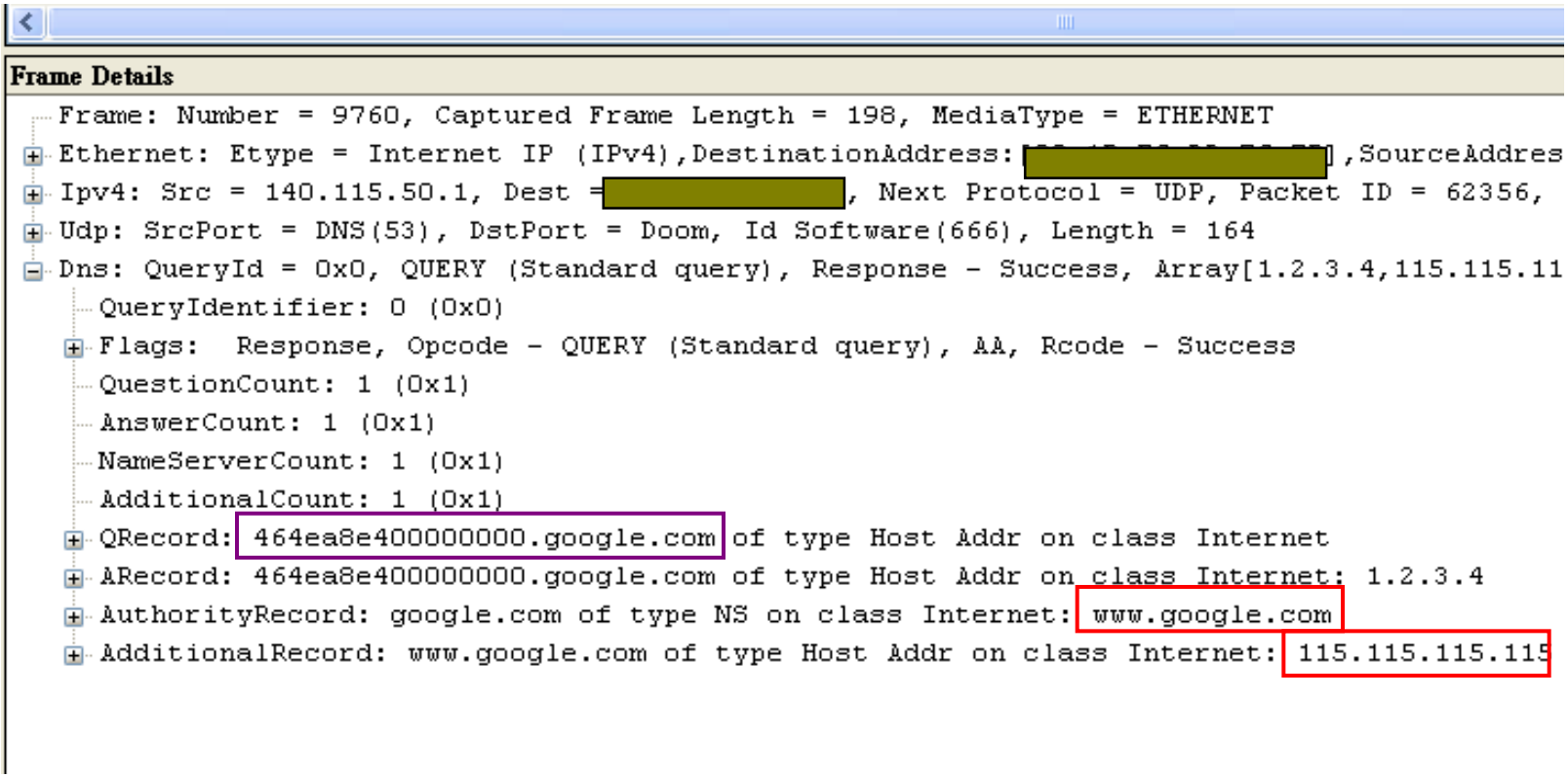
千萬別問
www.google.com

改問
123.google.com?
1234.google.com?
……
99999.google.com?
……



我是**ns1.google.com**
來自**216.239.32.10**
你要找的答案 **並不存在**

Kaminsky攻擊封包



數學公式 – 攻擊成功機率

- RFC 5452
  - Poisoning 成功機率

$$P_S = \frac{W * R}{N * P * I}$$

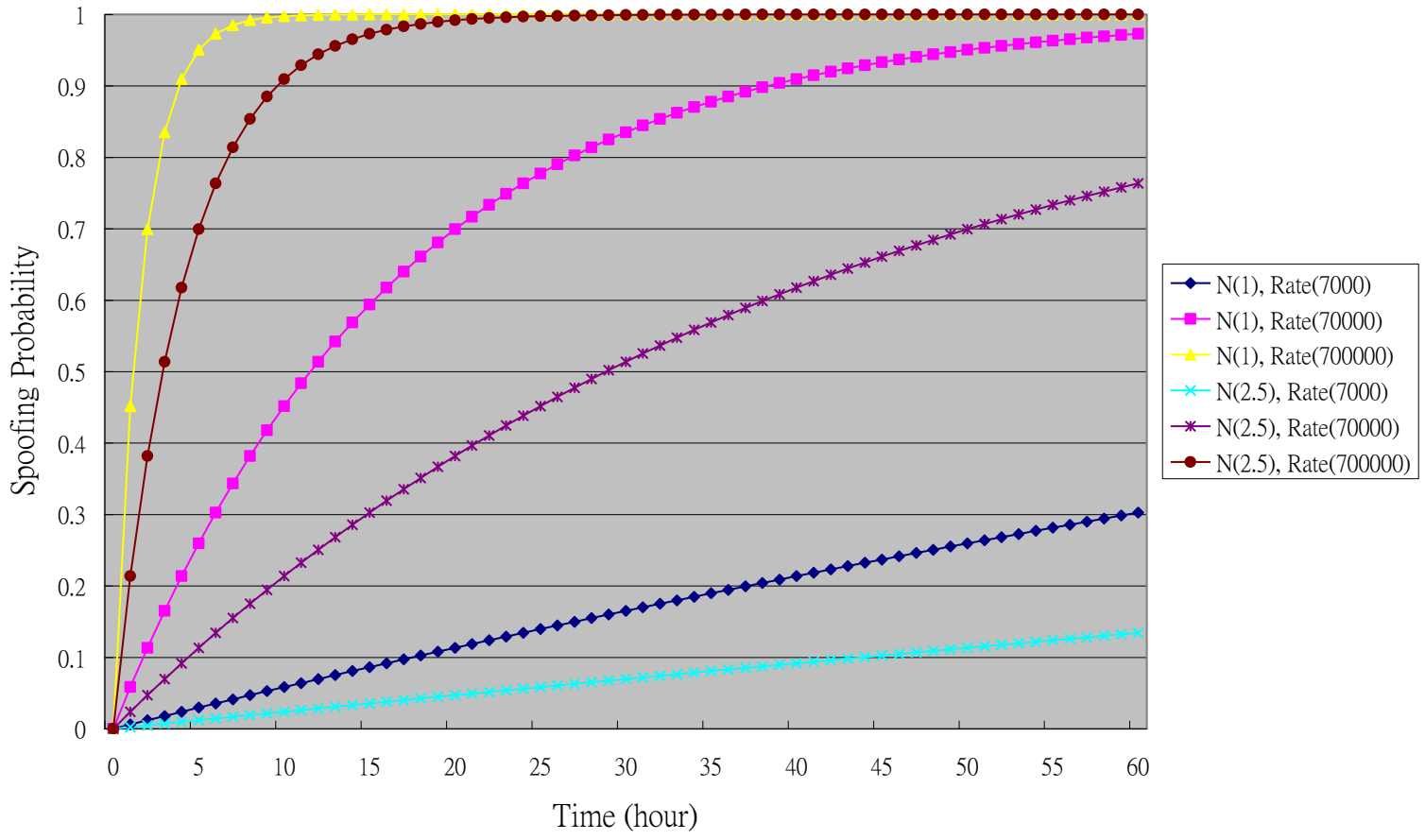
  - 打了很多回合，至少成功一次的機率

$$P_{CS} = 1 - (1 - P_S)^A = 1 - \left(1 - \frac{W * R}{N * P * I}\right)^{(T/W)}$$

  - 帶入參數

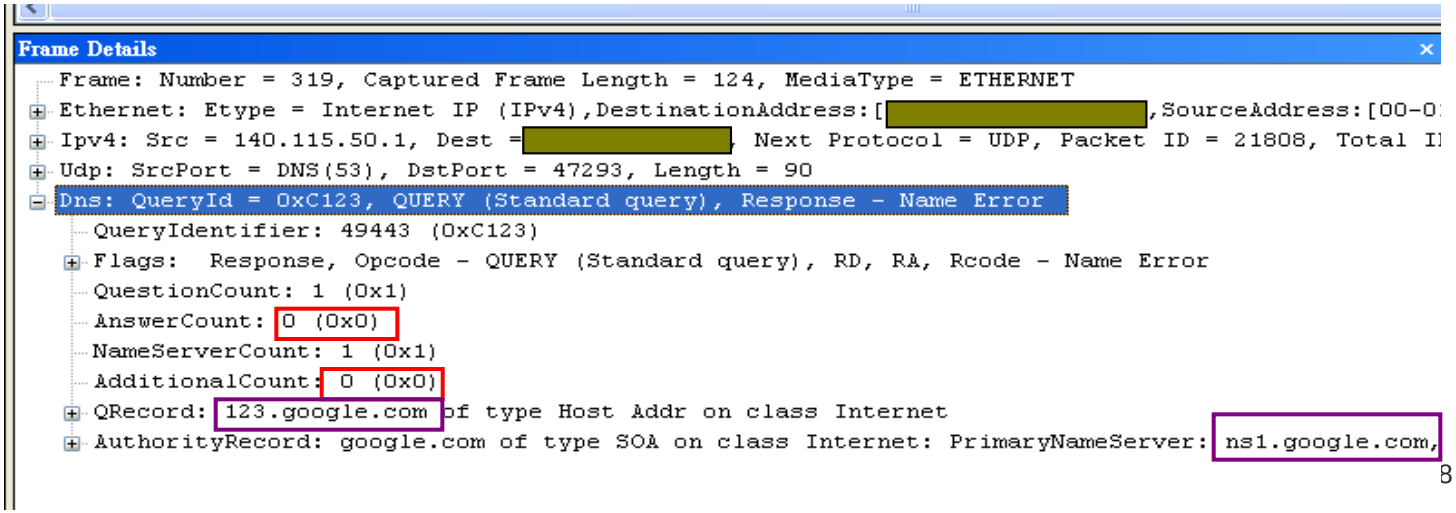
$$P_{CS} = 1 - \left(1 - \frac{0.1 * R}{2.5 * 64000 * 65536}\right)^{(T/W)}$$

攻擊模擬


Spoofing Probability
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
5
10
15
20
25
30
35
40
45
50
55
60
Time (hour)
N(1), Rate(7000)
N(1), Rate(70000)
N(1), Rate(700000)
N(2.5), Rate(7000)
N(2.5), Rate(70000)
N(2.5), Rate(700000)

一些防範措施

- DNSSEC
  - 非對稱式加密、電子簽章
- Google method
  - 沒有答案，就別多管閒事



Major Components of DNSPD

- DNS Resolver
- Router
- Analysis Crawler

DNSPD效應

- 如果攻擊者要躲避DNSPD的偵測
  - 攻擊頻率必須小於門檻值
    - 單一IP，非常難以成功
  - 使用 Botnet 成員
    - 投入多個IP
    - 攻擊低於門檻值的情況下，仍可提高成功機率
    - But …

結論

- DNSPD可以有效偵測Cache Poisoning攻擊，並避免其危害
- DNSPD可以迫使攻擊者使用Botnet
- DNSPD可能會間接保護其他Resolver

Q & A

- 謝謝大家