DNS Cache Poisoning
Looking at CERT VU#800113

Nadhem J. AlFardan
Consulting Systems Engineer

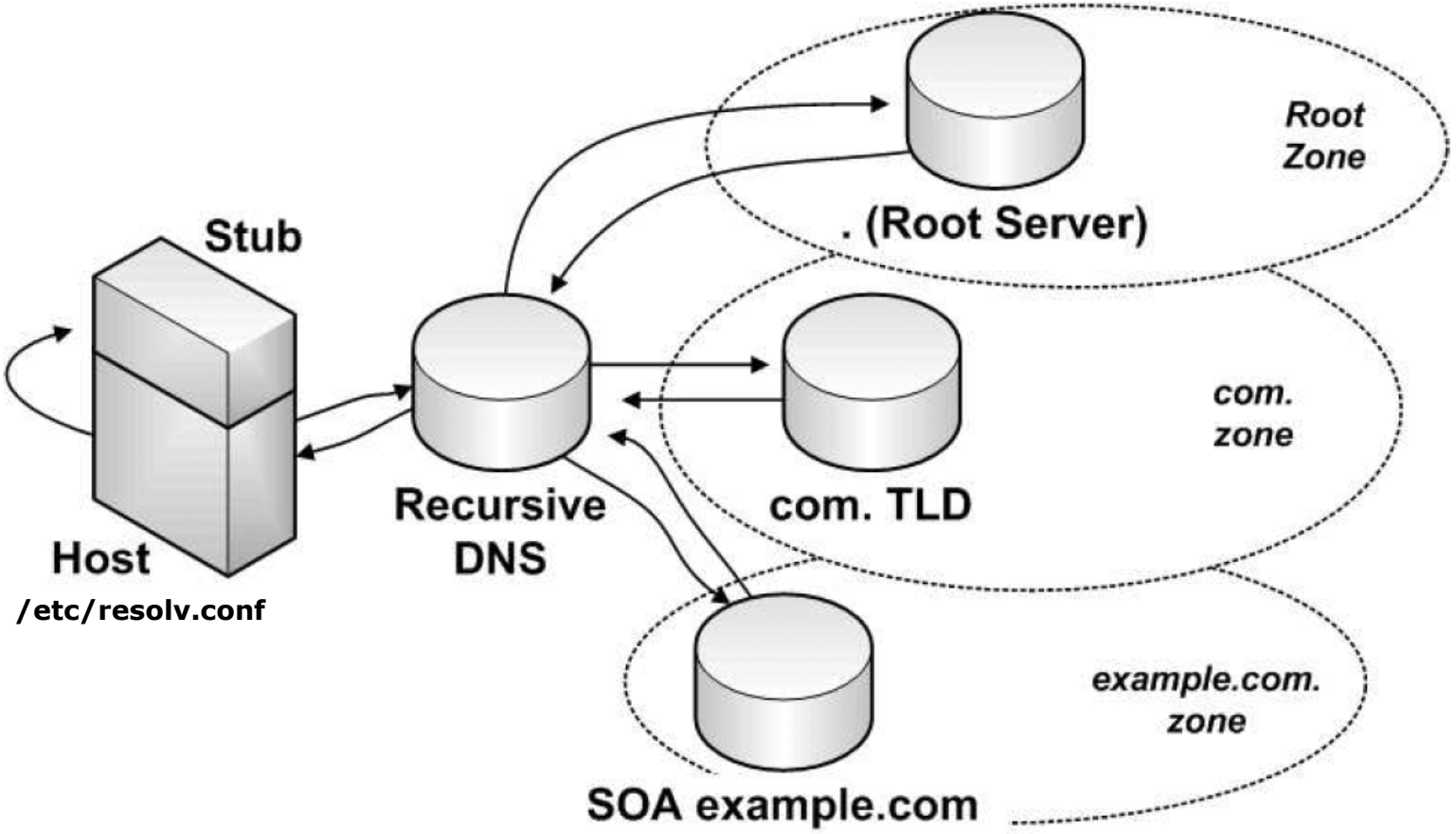
Cisco Systems

ANOTHER BORING DNS ISSUE

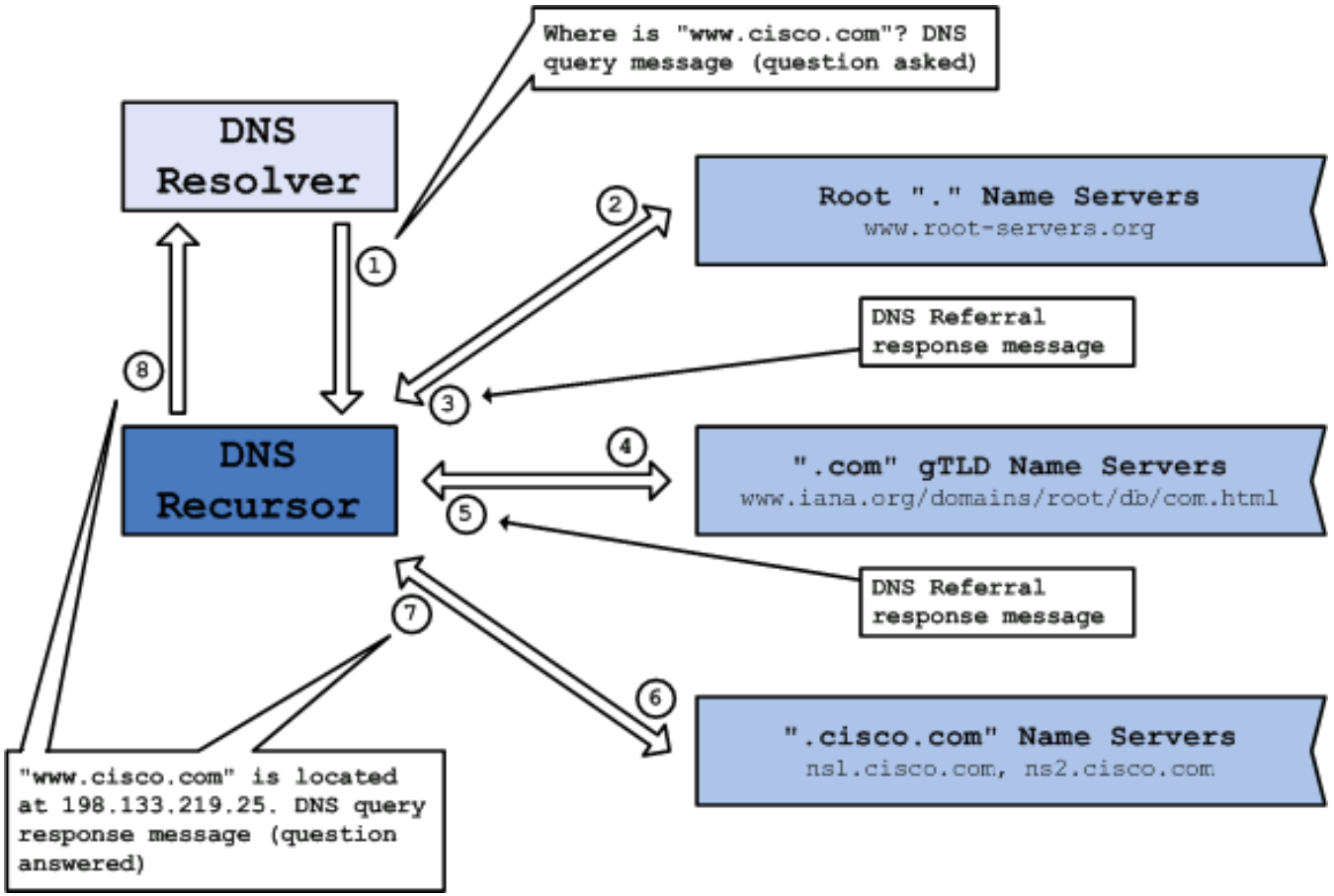
Agenda

- DNS Poisoning - Introduction
- Looking at “DNS Insufficient Socket Entropy Vulnerability”
- Mitigation Methods

DNS - Basic Background



DNS - Basic Background



DNS Poisoning - Introduction

In a nutshell its injecting bogus data into a recursive nameserver's cache

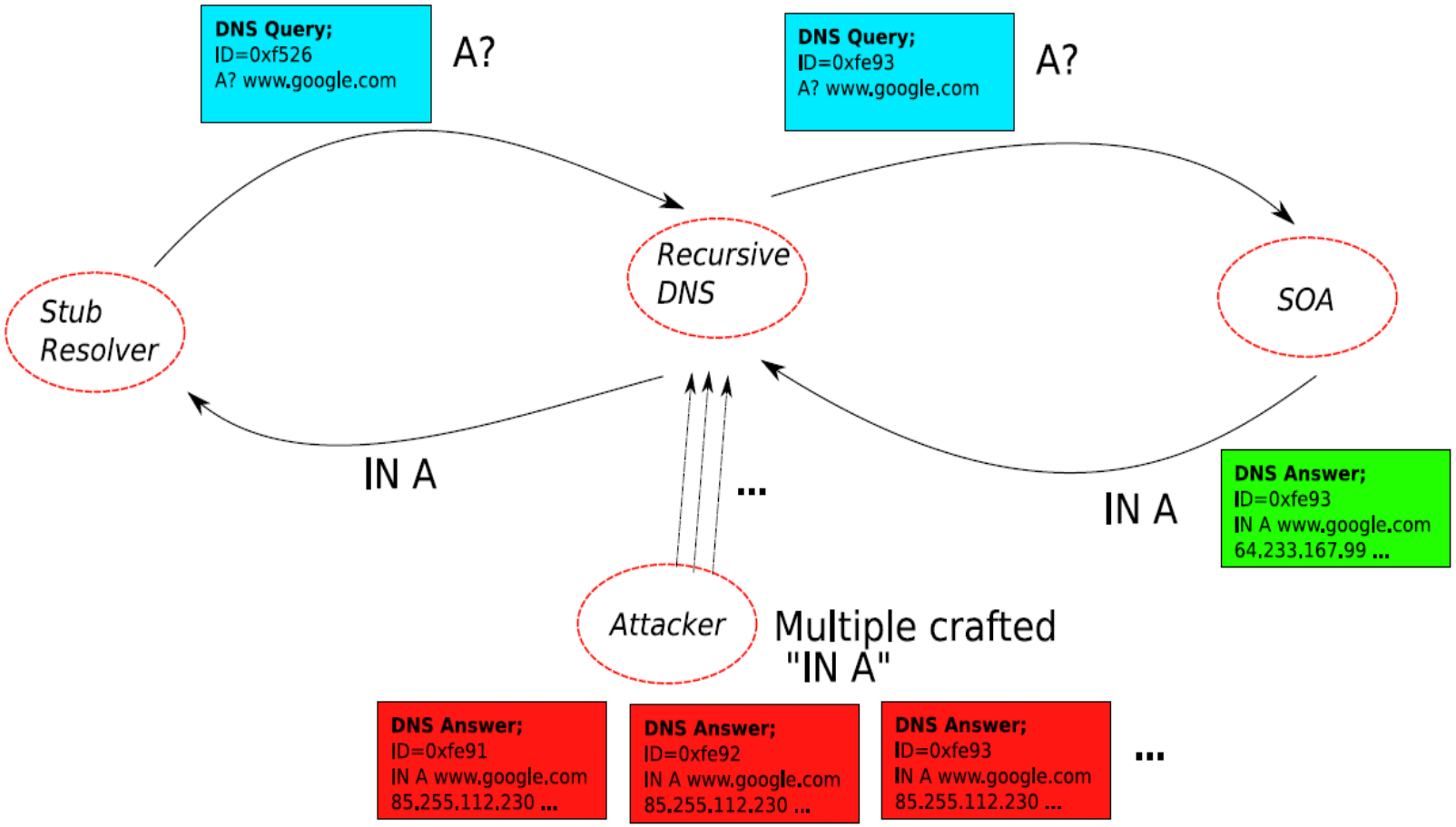
It's not so simple as just sending random DNS packets to a nameserver !

IT'S A RACE !

Protection is provided using:

- Source IP
- Destination IP
- Source Port
- Destination Port (UDP 53)
- Transaction ID (Query ID) (16 bits)

DNS Poisoning - Introduction



DNS Poisoning - Introduction

- The underlying feature in the major threat associated with DNS query/ response is the integrity of DNS data returned in the response.

- Hence, the security objective is to verify the integrity of each response received. An integral part of integrity verification is to ensure that valid data has originated from the right source.

- Establishing trust in the source is called data origin authentication.

Dan's Bug

- Dan Kaminsky found an approach that's dramatically more effective than standard DNS poisoning !

- There was a "*secret*" meeting at Microsoft, Mar 2008.

- Most vendors are vulnerable:
http://www.kb.cert.org/vuls/id/800113
Examples include ISC BIND and MS.
Ones that were not vulnerable included djbdns and PowerDNS

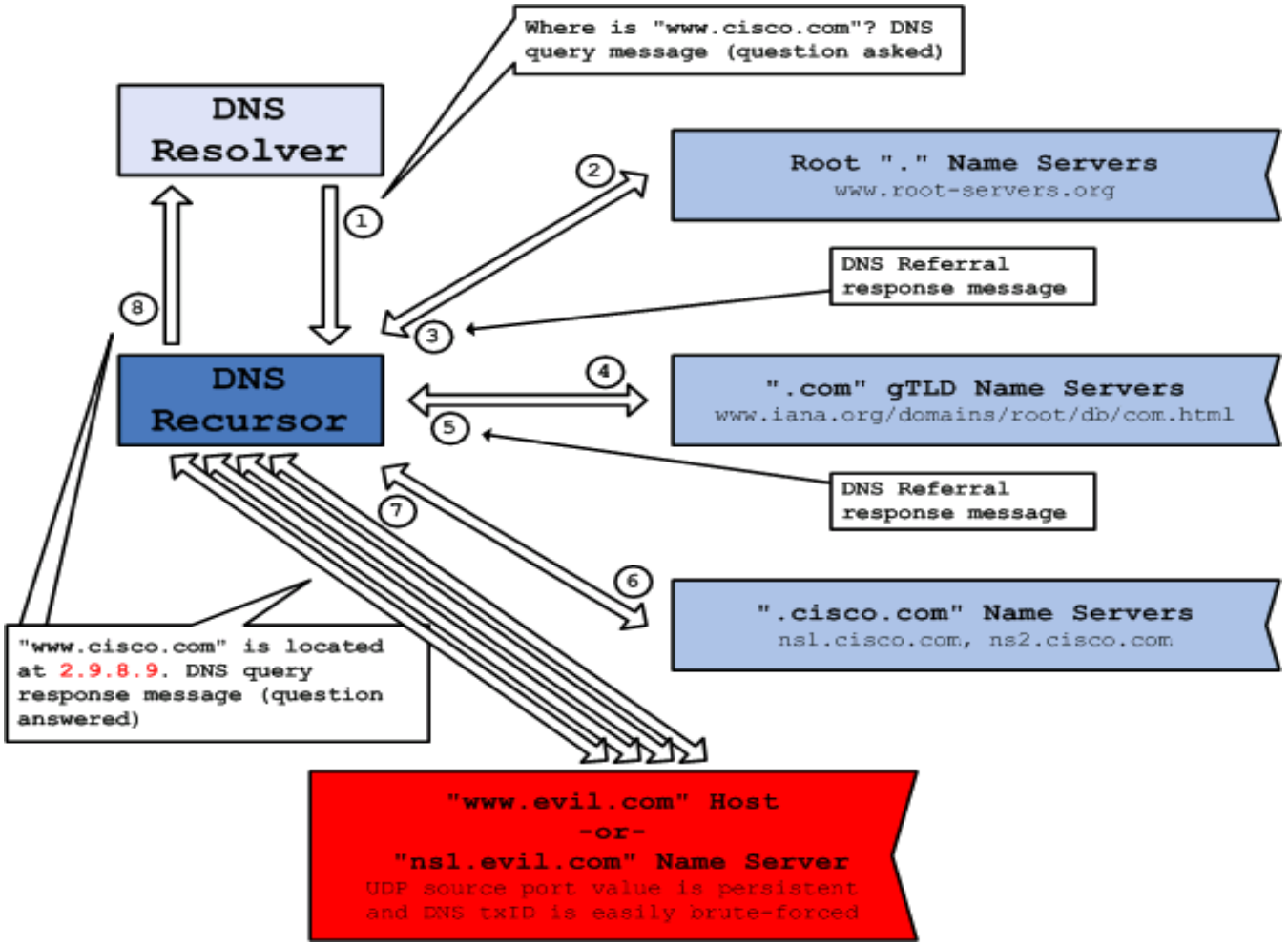
- Coordinated patch release from most vendors on July 8th, 2008.

- The general approach is the same as the simple approach, but the key difference is the nature of the forged payload !

- Dan discovered is that we can go up one level and **hijack the authority records** instead.

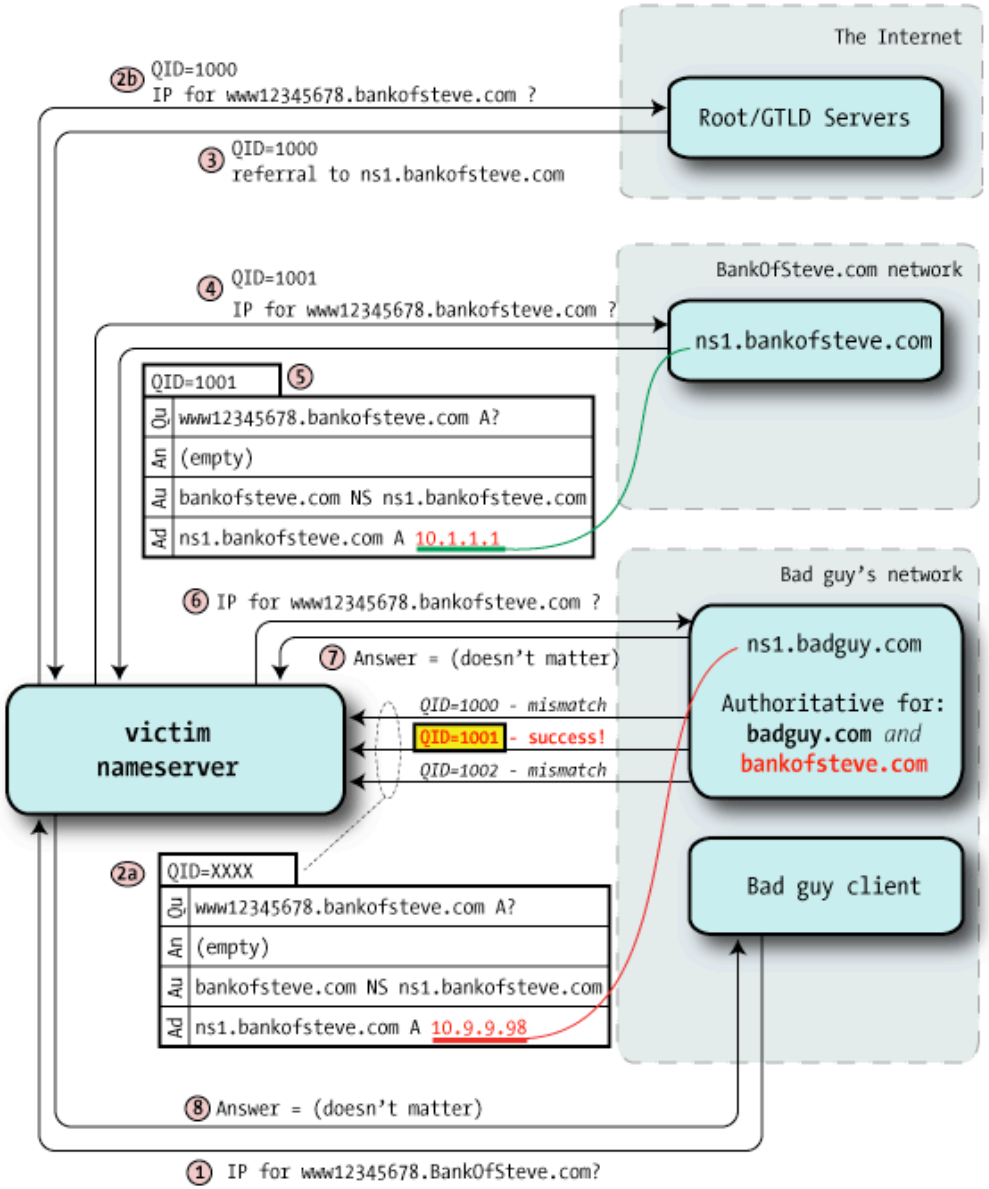
- Available tools include Metasploit exploit:
http://www.caughq.org/exploits/CAU-EX-2008-0003.txt

Dan's Bug


Where is "www.cisco.com"? DNS query message (question asked)
DNS Resolver
Root "." Name Servers
www.root-servers.org
DNS Referral response message
DNS Recursor
".com" gTLD Name Servers
www.iana.org/domains/root/db/com.html
DNS Referral response message
".cisco.com" Name Servers
ns1.cisco.com, ns2.cisco.com
"www.cisco.com" is located at 2.9.8.9. DNS query response message (question answered)
"www.evil.com" Host
-or-
"ns1.evil.com" Name Server
UDP source port value is persistent and DNS txID is easily brute-forced
1
2
3
4
5
6
7
8

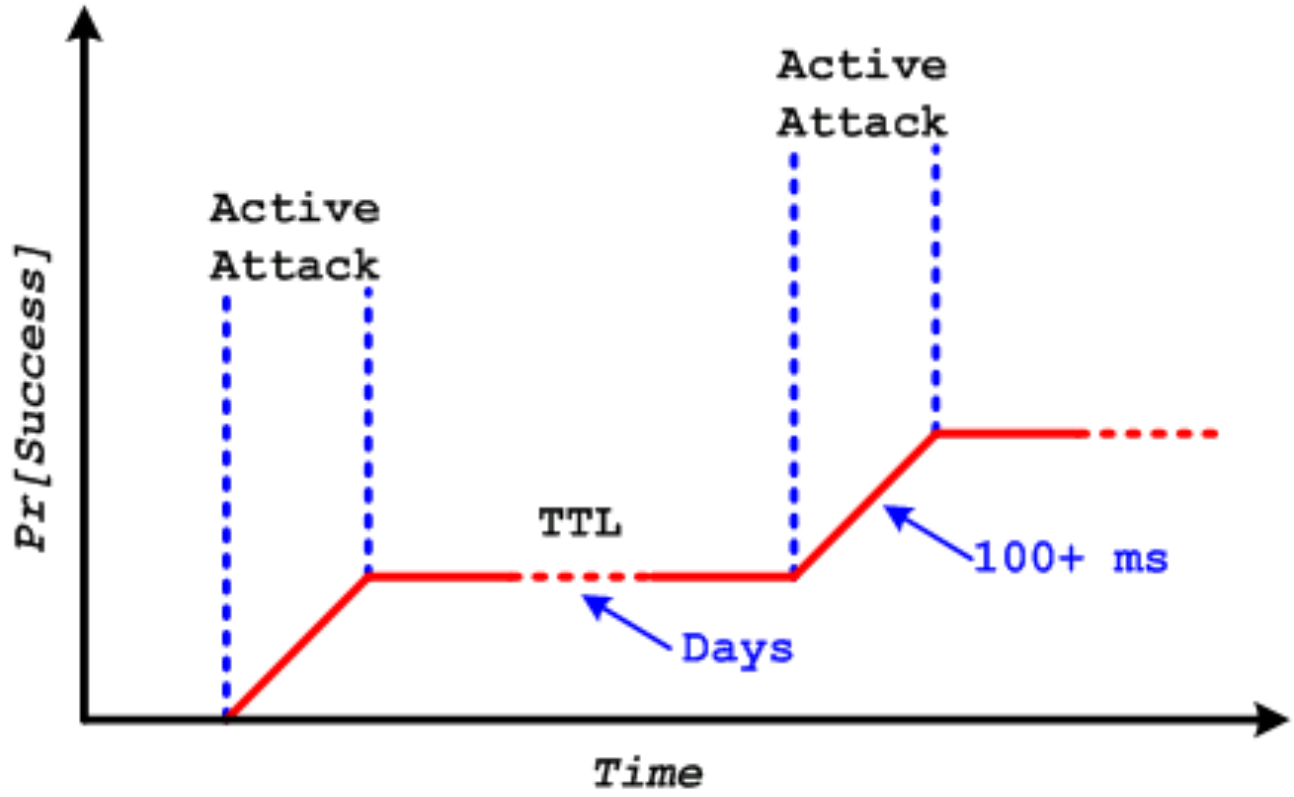
Dan's Bug

- The attacker will send a request to a random name under the attacked domain (nadhem.cisco.com)
- Attacker sends forged replies with malicious authority data.
- The attacker will still need to guess the Transaction ID !!
- BUT in this case the attacker CAN send a large number of requests to random names using an automated tool
- This increases his/her chance to hit a correct Transaction ID and hence modify the existing authority record cache
- What is next? I will leave it to your imagination ....

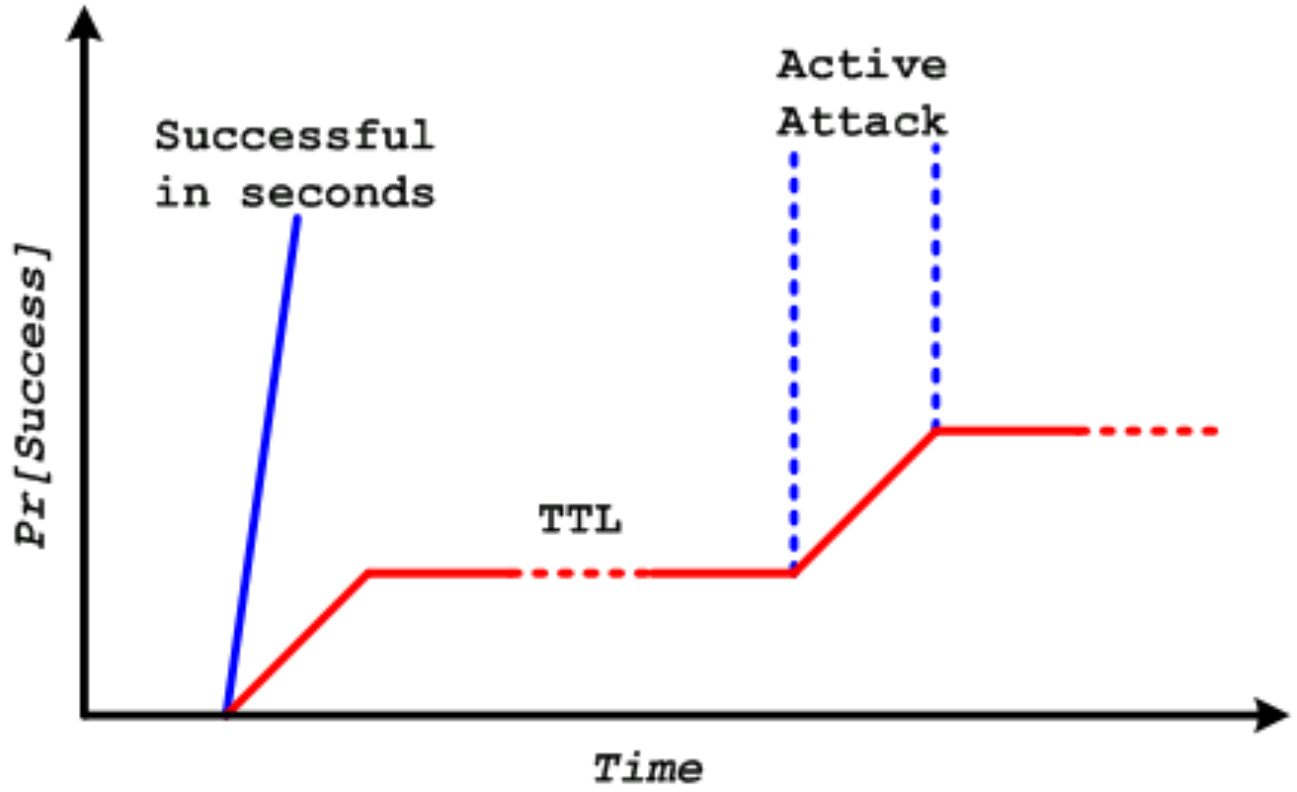


The diagram above is taken from
http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Time to success - old poisoning attacks



Time to success - with Dan's bug

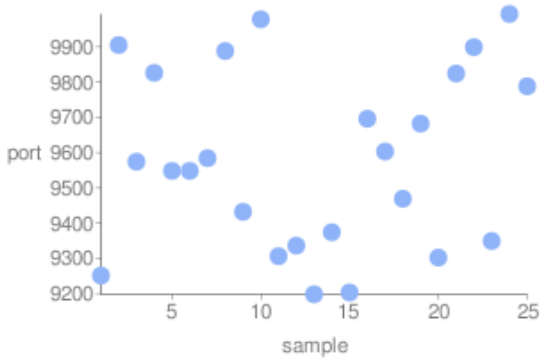


- Reported an average time of around 10sec is needed to get a successful attack !!

So you think that by now ppl patched !
Lets have a look ..This is done 3.5 hours ago !

80.88[redacted] Source Port Randomness: GREAT

193.188.[redacted] Source Port Randomness: POOR



Num

Modified Stanc

Bits c

Number of samples: 25

Unique port[redacted]: 24

Rang[redacted]: 9198 - 9993

Modified Standard Deviation: 244

Bits of Randomness: 10

Values Seen: 9251 9905 9574 9826 9548 9548 9584 9888 9432 9978 9306 9336 9198 9374 9203 9696 9603 9469 9682 9302 9824 9899 9349 9993 9788

Mitigation Methods

- Patch and/or upgrade to fixed code
  Patches specifically added randomized UDP source port values for queries.

  Configure and verify RANDOMIZATION!
  - query-source address <ip.address> port *; (ISC BIND)
  - dig @<dns.server> +short porttest.dns-oarc.net TXT
  - dig @<dns.server> +short txidtest.dns-oarc.net TXT
  - http://entropy.dns-oarc.net/test
  - http://www.doxpara.com

- Disable "recursion" if it is not needed !

Mitigation Methods

- DNSSEC is the only long-term solution
  Deployment is NOT realistic in the short-term

  ✓ The underlying feature in the major threat associated with DNS query/response is the integrity of DNS data returned in the response.

  ✓ Hence, the security objective is to verify the integrity of each response received. An integral part of integrity verification is to ensure that valid data has originated from the right source.

  ✓ Establishing trust in the source is called data origin authentication.

  ✓ Answers are digitally signed using public-key cryptography

- Don't forget to secure your system from other threats:
  - ✓ DNS amplification and reflection attacks
  - ✓ Resource utilization attacks
  - ✓ Attacks against the network infrastructure
  - ✓ Attacks against the OS
  - ✓ Attacks against service

- Some links:

http://www.cisco.com/web/about/security/intelligence/dns-bcp.html
http://www.doxpara.com/DMK_BO2K8.ppt
http://www.kb.cert.org/vuls/id/800113

Other Stuff

- DNS poisoning Malware !!
  A good example is DNSChanger.
  New variants are seen on the Internet

http://news.softpedia.com/news/DNS-Poisoning-Malware-Gets-Upgrade-106953.shtml

DMG on (on your own risk)
http://gamecodec.com/download/gamecodec1000.dmg

Deep thoughts by "Dan Kaminsky"

There are four possibilities [regarding how you view the criticality of the alert]:

DNS does NOT matter. Do NOT patch. :(
It is bad, but old. Do NOT patch. :(
It is bad, but old. Patch. :)
It is bad, and new. Patch. :)

I [Kaminsky] argue #4. I do not care about #3 and the less time people spend trying to find out what is new, the better. I am terrified about #1 and #2.