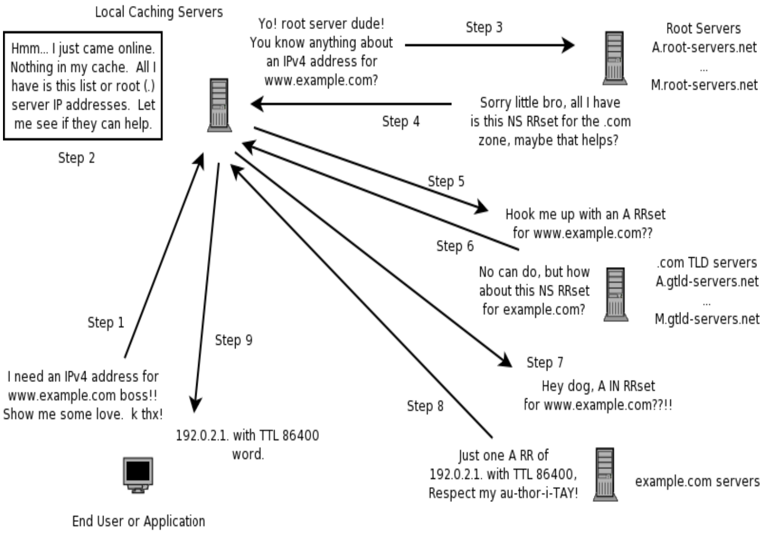
Open Resolvers and the Threat of Reflection Attacks

John Kristoff

jtk@depaul.edu

DPU CTI Networks Seminar

A Review of the DNS Lookup Process



Local Caching Servers

Root Servers
A.root-servers.net
...
M.root-servers.net

.com TLD servers
A.gtld-servers.net
...
M.gtld-servers.net

example.com servers

End User or Application

Step 1

I need an IPv4 address for
www.example.com boss!!
Show me some love. k thx!

Step 2

Hmm... I just came online. Nothing in my cache. All I have is this list or root (.) server IP addresses. Let me see if they can help.

Step 3

Yo! root server dude!
You know anything about
an IPv4 address for
www.example.com?

Step 4

Sorry little bro, all I have
is this NS RRset for the .com
zone, maybe that helps?

Step 5

Hook me up with an A RRset
for www.example.com??

Step 6

No can do, but how
about this NS RRset
for example.com?

Step 7

Hey dog, A IN RRset
for www.example.com??!!

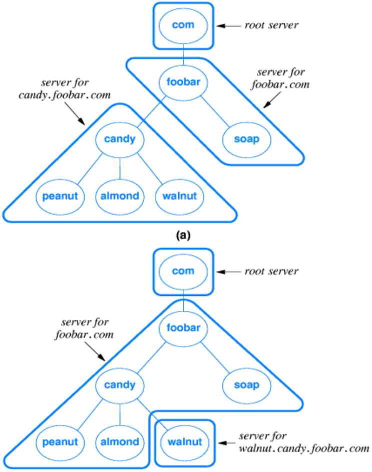
Step 8

Just one A RR of
192.0.2.1. with TTL 86400,
Respect my au-thor-i-TAY!

Step 9

192.0.2.1. with TTL 86400
word.

What Does Verisign Like About This Picture?



(a)

(b)

Resource Record (RR) format

```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                               |
/                                               /
/                      NAME                     /
|                                               |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      TYPE                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                     CLASS                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      TTL                      |
|                                               |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                   RDLENGTH                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--|
/                     RDATA                     /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

DNS Message Format

```
+---------------------+
|        Header       |
+---------------------+
|       Question      | the question for the name server
+---------------------+
|        Answer       | RRs answering the question
+---------------------+
|      Authority      | RRs pointing toward an authority
+---------------------+
|      Additional     | RRs holding additional information
+---------------------+
```

DNS Message Header Format

```
0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Open Resolver

- A DNS server that provides an answer or referral for anyone
- Full open recursive name servers can be particularly problematic
- It can be difficult to limit open recursion in practice
- There are **lots** of open resolvers

Amplification and Reflection Attacks Using Open Resolvers

- Imagine... lots of bots
- Imagine... lots of open recursive name servers
- Imagine... a 4 KB TXT resource record
- Imagine... source address spoofing
- Imagine... queries that are less than 100 bytes
- Imagine...

Resolver probing, not scanning

We could just send properly formatted DNS queries to TCP/UDP port 53 if all we cared about was finding name servers. However, we want to try to precisely identify resolver behavior, configuration and implementation.

Some Remote Open Resolver Probing Questions

- How do you *really* know if the server is recursing for you?
- Are there questions a server answers for in unexpected ways?
- Is the server you're asking the only server at that address?
- Are you getting a cached answer?
- Are wildcards being used?

Some Multifaceted Probing Techniques

- Query for whoareyou.ultradns.net
- Query for whoami.ultradns.net
- Query for unique, but bogus top-level domain (TLD)
- Fingerprint with fpdns
- Query for unique name in a zone we control
- Distribute query sources
- Disable recursion desired (rd) bit
- Query for popular names and NS RRsets
- Query for unique, but bogus name in popular zones and TLDs

Challenges to Remote Probing

- Recursion available (ra) is an unreliable indicator
- Non-exist name/TLD query doesn't always result in NXDOMAIN
- Adherence to TTL is inconsistent
- High-speed querying difficultly and timeout handling
- Various other unexpected answers due to config or implementation

Caching Weirdness

```
$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<>> DiG 9.2.2 <<>> @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options:  printcmd
whoareyou.ultradns.net. 0       IN      A       204.74.96.5

$ dig @61.46.219.237 whoareyou.ultradns.net +noall +answer

; <<>> DiG 9.2.2 <<>> @61.46.219.237 whoareyou.ultradns.net +noall +answer
;; global options:  printcmd
whoareyou.ultradns.net. 4294967292 IN   A       204.74.96.5
```

Alternate Root

```
$ dig @211.220.209.3 bogus-tld +noall +answer +authority

; <<>> DiG 9.2.2 <<>> @211.220.209.3 bogus-tld +noall +answer +authority
;; global options:  printcmd
realname.               86400   IN      A       211.106.67.200
realname.               86400   IN      NS      update-psi.netpia.com.
```

Wildcard

```
$ dig @213.30.189.132 nanug.org +noall +answer

; <<>> DiG 9.2.2 <<>> @213.30.189.132 nanug.org +noall +answer
;; global options:  printcmd
nanug.org.              10000   IN      A       62.210.183.75
nanug.org.              10000   IN      TXT     "toto"
```

Flags and Inconsistency

```
$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52909
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

$ dig @213.215.76.84 +noall +comments +answer www.nanog.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43523
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
www.nanog.org.          86392   IN      A       198.108.1.5
```

Query Amplification and Aggression?

```
Auth Server #1
client 209.63.146.65#37695: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
Auth Server #2
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -E
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
client 208.187.120.2#4444: query: researchprobe-3632192887.example.org IN A -
```

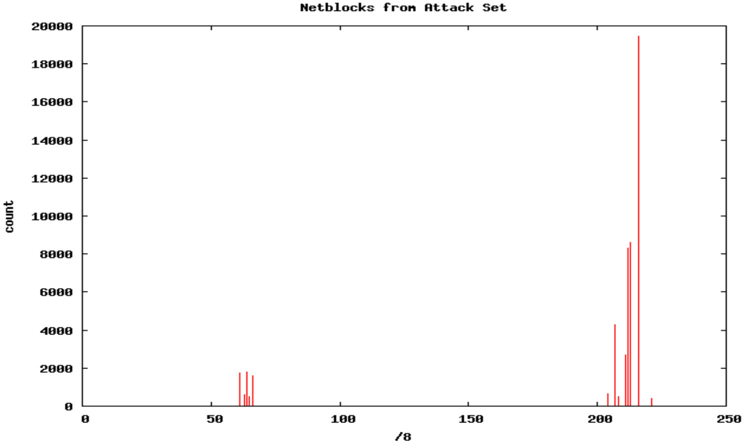
Bad Defaults

```
$ dig @202.146.225.194 bogus-tld +noall +comments +answer

; <<>> DiG 9.2.2 <<>> @202.146.225.194 bogus-tld +noall +comments +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30140
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
bogus-tld.              3600    IN      A       10.61.32.1
```

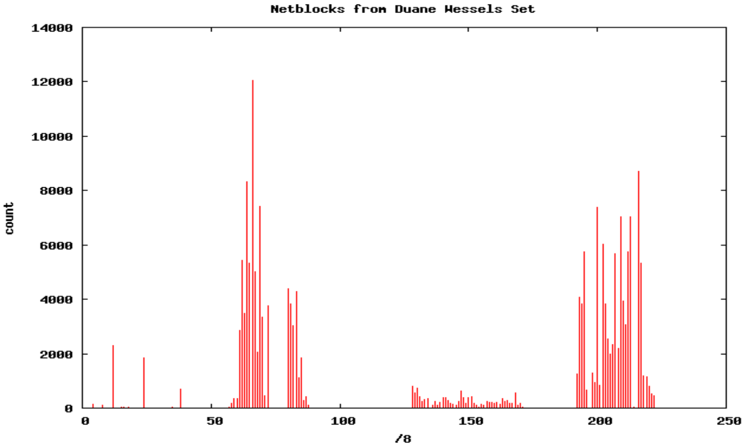
ORNS Candidate Data Sets

- 51,196 reflector attack, Feb. 2006
- 191,966 ORNS from Duane Wessels, March 2006
- 2,660,229 somethings querying us, March 2006

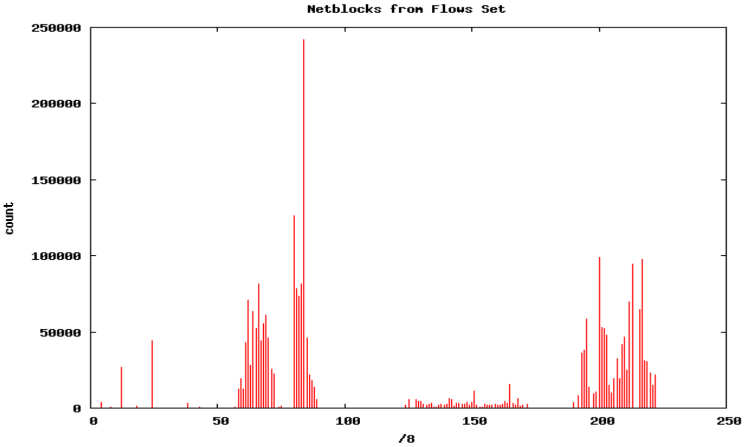
Netblocks - Attack Set



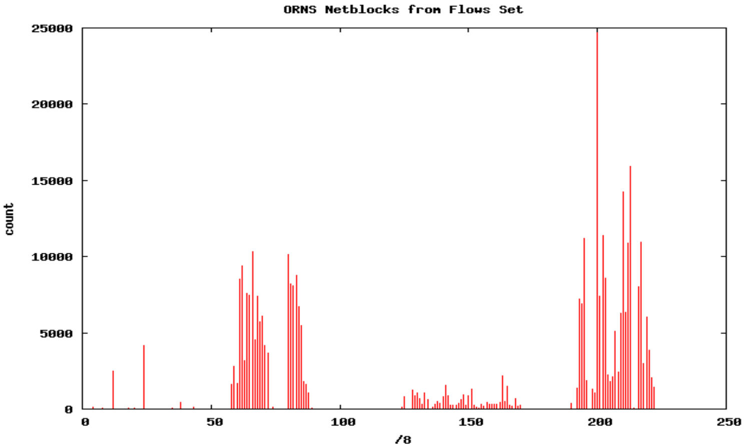
Netblocks - Duane's Set



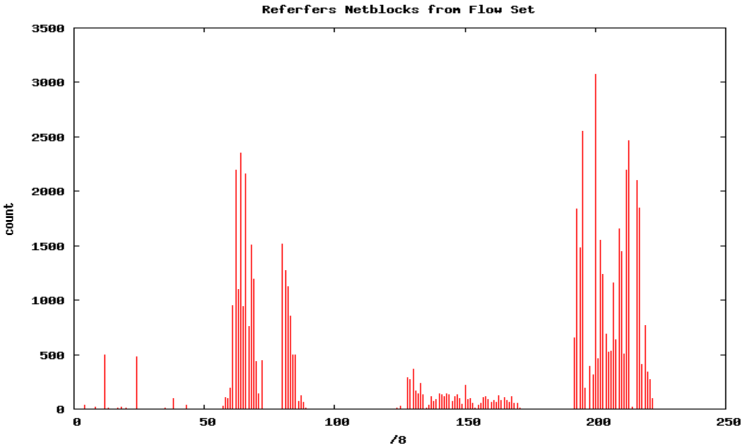
Netblocks - Our Flows



ORNS Netblocks - Our Flows (˜14%)



Referrer Netblocks - Our flows (~2%)



Building and Maintaining A Resolver Probing System

- Where do you get candidate probing addresses from?
- Where do you probe from? How fast? Will you get filtered?
- What queries do you send?
- Logs, packet captures or responses. What do you do with them?
- How do you re-test and maintain accuracy?
- How do you share the data and/or alert administrators?
- What else can you do with this data?

End - Work in Progress

- [dns-research01|dns-research02].cti.depaul.edu
- DNS prototype probing systems with web interface
- TLD zone monitoring and analysis