Improving DNS Security and Resiliency

PacNOG 8 - Pohnpei, Micronesia
Carlos Vicente
NSRC-University of Oregon
Why?

• When your DNS servers are down:
  – Your customers can’t resolve other domains
  – The world can’t resolve your own domains
  – Might as well not be connected to the Internet!

• When the data in your DNS servers becomes compromised
  – Users will inadvertently direct their traffic to illegitimate servers
Threats to DNS

- Server crashes
- Server compromise
- Denial of service attacks
- Amplification attacks
- Cache poisoning
- Targeted host attacks using zone information
- More
  - http://www.dnssec.net/dns-threats
DoS attacks

• Saturating the target machine with external requests, such that it cannot respond to legitimate traffic
Amplification Attacks

- Also known as “Reflection Attacks”
- DNS servers being used as tools in the attack
  - Sending responses to queries whose source addresses have been spoofed
- The actual node that owns the spoofed address is the victim
Amplification Attacks

The Attack

ATACKER

Zombies

Send Queries SPOOFED from Victim

Victim Receives Large DNS Answers

Army of 30,000 to 500,000 open recursive DNS Servers

Query Once, Then Cache

Break In! Publish BIG TXT Record

Innocent DNS Server

Source: http://www.nanog.org/meetings/nanog37/presentations/frank-scalzo.pdf
Amplification Attacks

• Difficult to protect our users against
  – Impossible to filter thousands of servers

• What we can do is avoid taking part
  – Egress filtering (IETF BCP 38)
  – Restrict access to recursive DNS servers
    • However, authoritatives can still be used in attacks

• What we should NOT do
  – Limit the size of DNS packets (breaks DNSSEC)
Burma hit by massive net attack ahead of election

An ongoing computer attack has knocked Burma off the internet, just days ahead of its first election in 20 years.

The attack started in late October but has grown in the last few days to overwhelm the nation’s link to the net, said security firm Arbor Networks.

Reports from Burma say the disruption is ongoing.

The attack, which is believed to have started on 25 October, comes ahead of closely-watched national elections on 7 November.

International observers and foreign journalists are not being allowed into the country to cover the polls.

It will raise suspicions that Burma’s military authorities could be trying to restrict the flow of information over the election period.
Cache Poisoning

• Attacker tricks a caching server to store a wrong answer
  – www.mybank.com -> 1.2.3.4
    • 1.2.3.4 is the attacker’s web server, disguised as your bank!
  – One successful attack affects many (if not all) users
Cache Poisoning

Master DNS Server

Query:
www.mybank.com?
Source: s.s.s.s:x
Destination: d.d.d.d:y
ID: 123456

Reply:
www.mybank.com=1.2.3.4
Source: d.d.d.d:y
Destination: s.s.s.s:x
ID: 123456

Open Resolver

www.mybank.com=1.2.3.4

Attacker
Cache-poisoning attack snares top Brazilian bank

Google Adsense spoofed

By Dan Goodin in San Francisco • Get more from this author

Posted in Crime, 22nd April 2009 00:32 GMT

Free whitepaper – The 10 myths of safe web browsing

One of Brazil’s biggest banks has suffered an attack that redirected its customers to fraudulent websites that attempted to steal passwords and install malware, according to an unconfirmed report.

According to this Google translation of an article penned in Portuguese, the redirection of Bradesco was the result of what’s known as a cache poisoning attack on Brazilian internet service provider NET Virtua.
Cross-Pollination Check

The discovery of a highly-effective cache poisoning attack that can affect name servers providing recursive name service has made it important that such servers be patched to mitigate against the problem. Furthermore, the risk of cache poisoning for servers that share recursive and authoritative functions can cross-pollinate the authoritative function with incorrect data. This tool is designed to assess the authorities for a given domain and determine whether they provide vulnerable recursive service.

Provide a domain name to analyse: uoregon.edu

---

Safe.
The servers tested for UOREGON.EDU appear not to be vulnerable to cache poisoning.

Note that not all authoritative name servers could be reached, so there may be additional issues that were not discovered.

<table>
<thead>
<tr>
<th>Name server</th>
<th>IP Address</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARIZONA.EDU</td>
<td>128.196.128.233</td>
<td>Not recursive</td>
</tr>
<tr>
<td>BIGDOG.LSU.EDU</td>
<td>192.16.176.1</td>
<td>Not recursive</td>
</tr>
<tr>
<td></td>
<td>2620:9:8:0000::1</td>
<td></td>
</tr>
<tr>
<td>DNS.CS.UOREGON.EDU</td>
<td>128.223.6.9</td>
<td>Not recursive</td>
</tr>
<tr>
<td>PHILOEM.UOREGON.EDU</td>
<td>2001:486:0:1:6::80df609</td>
<td>Not recursive</td>
</tr>
<tr>
<td>RUMINANT.UOREGON.EDU</td>
<td>128.223.32.35</td>
<td>Not recursive</td>
</tr>
<tr>
<td></td>
<td>2001:486:0:1:20::80df2023</td>
<td>Not recursive</td>
</tr>
<tr>
<td>SNS-PBI.ORG</td>
<td>192.5.4.1</td>
<td>Not recursive</td>
</tr>
<tr>
<td></td>
<td>2001:900:2e::1</td>
<td></td>
</tr>
</tbody>
</table>
Dangers of zone transfers

• Zone transfers meant to be used to distribute zones among authoritative servers
• Transfers are expensive operations in terms of resources
  – Could be used for DoS attack
• Having your whole zone makes hacker’s life easier:
  – No need to scan your address space
  – Better understanding of your network
# Authoritative vs. Recursive

<table>
<thead>
<tr>
<th>Server Function</th>
<th>Information</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authoritative</td>
<td>Your domains</td>
<td>The Internet</td>
</tr>
<tr>
<td>Recursive</td>
<td>All other domains</td>
<td>Your users</td>
</tr>
</tbody>
</table>
Separation of Duties

• Physically separating authoritative and recursive servers gives you:
  – Easier control
    • Apply restrictions to what the servers can be used for, and by whom
  – Easier troubleshooting
    • Consider what happens when a DNS-hosted customer moves their domain to another provider without telling you
Authoritative – BIND options

options {
    version "9999.9.9";
    allow-transfer { peers; };
    blackhole { attackers; };
    recursion no;
    allow-query { any; };
    ...
};
Authoritative – IP filters

• Can’t really filter much here
  – Ports udp/53 and tcp/53 should be open to the world.

• Just don’t run any other services
  – No web server, mail server, etc.
  – Keep it really simple
  – The goal is to minimize the potential for a server compromise
Authoritative - Location

- Locate your servers topologically and geographically dispersed
  - Establish a relationship with another operator, or
  - There are companies that provide secondary service
    - Ask for anycast, DNSSEC and IPv6 support!
  - See RFC 2182
Recursive – BIND options

options {
    version "9999.9.9";
    recursive-clients 5000;
    allow-transfer { none; };
    blackhole { attackers; };
    allow-recursion { customers; };
    allow-query { customers; };
    dnssec-enable yes;
    dnssec-validation yes;
    ...
};
Recursive – IP filters

- udp/53 and tcp/53 open only to customers
  - Drop the packets early, don’t bother the DNS daemon
  - Remember to filter IPv6 as well if you have v6 connectivity
  - Can be done simply with iptables on Linux.
DNSSEC Validation

• The root is now signed!
• Only true way to avoid cache poisoning
• Started with universities and research organizations, now large ISPs are joining:
  – http://www.dnssec.comcast.net/
Source: dnsviz.net
DNSSEC Validation

options {
    dnssec-enable yes;
    dnssec-validation yes;
}

managed-keys {
    "." initial-key 257 3 8 "AwEAAagAIKlVZrpC6la7gEzahOR +9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUf6v58fLjwBd0YI0Ezr AcQqBGCzh/
    RStIoO8g0NfifL2MTJRkxoXbfDaUeVPQuYEHg37NZWAJQ9VnMV
    DxP/VHL496M/QZxkjif5/
    Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJ
    BBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzugul0sGlcG
    OYI7OyQdXfZ57relSQageu
    +ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
    QxA+Uk1ihz0=";
};
DNSSEC packet size implications

• Responses can easily exceed previous max. of 512 bytes over UDP
• Two solutions:
  – Use EDNS0: The client signals that it can support larger UDP packets
  – Use TCP
• In both cases, need to make sure that the path between your customers and your name servers is capable
  – Especially, check out firewalls
Client failover behavior

• Clients of authoritative servers (other recursive servers)
  – Fail over well using different NS records

• Clients of recursive servers (stub resolvers)
  – Do a very poor job at failing over
  – Users complain immediately
  – Other services break due to timeouts
Anycast

- Routing trick in which the same IP address is announced by multiple routers so that a particular sender reaches the topologically nearest node that responds to that address
- Excellent solution to enhance DNS:
  - Load-balancing
  - Failover
  - DoS attack isolation
  - Cache poisoning isolation
Anycast DNS

• Two approaches
  – Running a routing daemon on the DNS server
    • Zebra, Quagga, etc.
    • Must tie the prefix announcements to DNS service start/stop and… daemon crashes
  – Using IP SLA with Cisco routers
    • Check that the service is operational before injecting prefix in the routing domain
    • No need to trust your sysadmins injecting routes into your routing domain ;-)  
    • Server configuration much simpler
Anycast Topology
Anycast Topology

![Diagram of Anycast Topology]
Anycast DNS – Cisco IP SLA

ip sla 1
dns www.mydomain.com name-server 192.0.2.202
timeout 500
frequency 10
ip sla schedule 1 life forever start-time now

track 1 ip sla 1
ip route 192.0.2.100 255.255.255.255 192.0.2.200 track 1 tag 999

route-map V4-STATIC permit 10
match tag 999

router isis mynet
redistribute static ip metric 100 route-map V4-STATIC level-1
Anycast – Server Interfaces

eth0 Link encap:Ethernet  HWaddr F0:4D:A2:01:65:42
inet addr:192.0.2.2  Bcast:192.0.2.3  Mask:255.255.255.252

lo Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0

lo:1 Link encap:Local Loopback
inet addr:192.0.2.202  Mask:255.255.255.255
Configuration Management

• Keep configurations and zone files under revision control
  – SVN, Git, CVS

• Generate, don’t edit, zone files
  – http://netdot.uoregon.edu
  – http://www.nictool.com/info/

• Use CM tool to distribute these files, reload services, etc.
  – Puppet, CFEngine, etc.
  – Run a syntax check before loading
    named-checkzone mydomain.com zonefile
Diversify OS and DNS software

- Consider running different DNS software (Bind, Unbound, NSD, etc.) on different OSs
  - Saves you from total disaster when you hit a bug, but…
  - Makes configuration management a lot more challenging
Periodic zone checks

• Periodically run checks for
  – Consistent, missing or bad data
  – Catching common misconfigurations
  – RFC 1912

• Check out dnscheck
  – https://github.com/dotse/dnscheck
Watch those logs

• Use a tool to analyze your DNS logs and alarm on important messages
  – Swatch, Tenshi, etc.
Monitoring Availability – Nagios

• Use the check_dns to make sure that the server is actually resolving
  – Don’t just ping the server

• You can also use this to make sure that very important A records are there:
  – www, smtp, imap,…

• Make sure that your alarms will work despite DNS being down!
Monitoring Availability - Nagios

Service 'DNS' On Host 'ns1'

01-01-2010 00:00:00 to 11-07-2010 21:08:40
Duration: 310d 21h 8m 40s

[ Availability report completed in 0 min 16 sec ]

Service State Breakdowns:

<table>
<thead>
<tr>
<th>State</th>
<th>Type / Reason</th>
<th>Time</th>
<th>% Total Time</th>
<th>% Known Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Unscheduled</td>
<td>00d 22h 8m 40s</td>
<td>29.247%</td>
<td>100.000%</td>
</tr>
<tr>
<td></td>
<td>Scheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>00d 22h 8m 40s</td>
<td>29.247%</td>
<td>100.000%</td>
</tr>
<tr>
<td>WARNING</td>
<td>Unscheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Scheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>Unscheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Scheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Unscheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Scheduled</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
<tr>
<td></td>
<td>Nagios Not Running</td>
<td>0d 0h 0m 0s</td>
<td>0.000%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insufficient Data</td>
<td>213d 23h 0m 0s</td>
<td>70.753%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>213d 23h 0m 0s</td>
<td>70.753%</td>
<td></td>
</tr>
<tr>
<td>All</td>
<td>Total</td>
<td>310d 21h 8m 40s</td>
<td>100.000%</td>
<td>100.000%</td>
</tr>
</tbody>
</table>
Monitoring Delay

• Important to look at both
  – Network delay
  – DNS service delay
Monitoring Delay - Smokeping

Recursive

ns1 (DNS)

---

ns1 (ICMP)

---

ns2 (DNS)

---

ns2 (ICMP)
DNS Statistics - DSC

Queries by QType

Query Rate (q/s)

Time, PST

23:00  0:00  1:00  2:00  3:00  4:00  5:00  6:00  7:00  8:00  9:00  10:00  11:00  12:00  13:00  14:00  15:00  16:00  17:00  18:00  19:00  20:00  21:00  22:00

Nov6
Checklist

- Separate authoritative and recursive servers
- Locate authoritative servers in different networks
- Turn off recursive queries in authoritative servers
- Restrict zone transfers
- Limit recursive queries to your customers only
- Restrict forged traffic (IETF BCP 38)
- Start doing DNSSEC validation
- Keep configurations and zone files under revision control
- Perform zone checks periodically
- Monitor availability, delay, logs, traffic
Questions?

• Thank you