Delving into DNS

Sean Burford

Definition
Australia
Servers
Probing
Tools

Delving into DNS

- What is DNS
- DNS in Australia
- Architecture of Some Common Servers
- Fingerprinting DNS Servers
- Other DNS Tools
- Bibliography

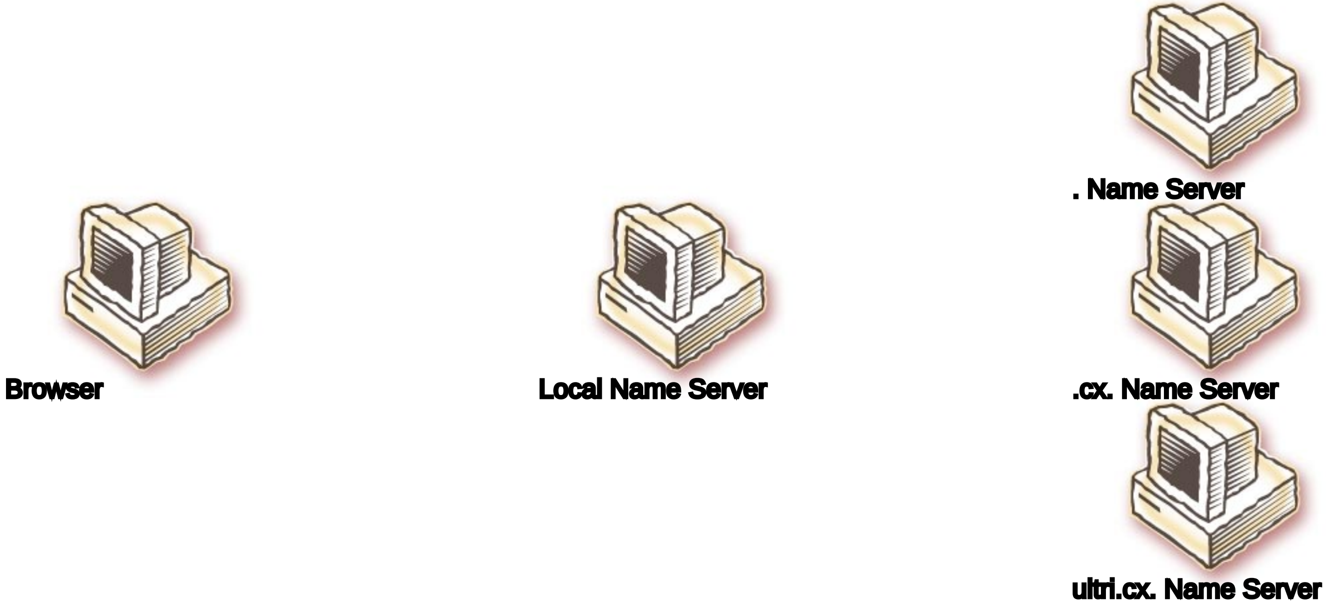
Updated 18/Aug/2003

What is DNS?

Definition
Australia
Servers
Probing
Tools

Definition

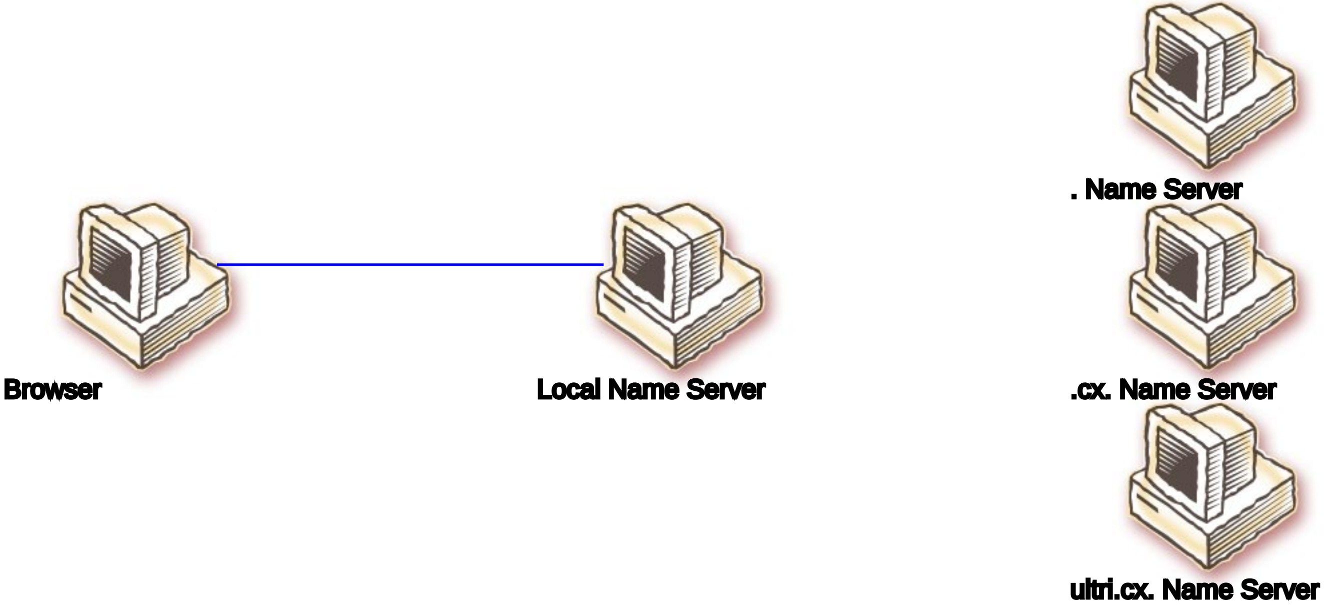
- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition
Australia
Servers
Probing
Tools

Definition

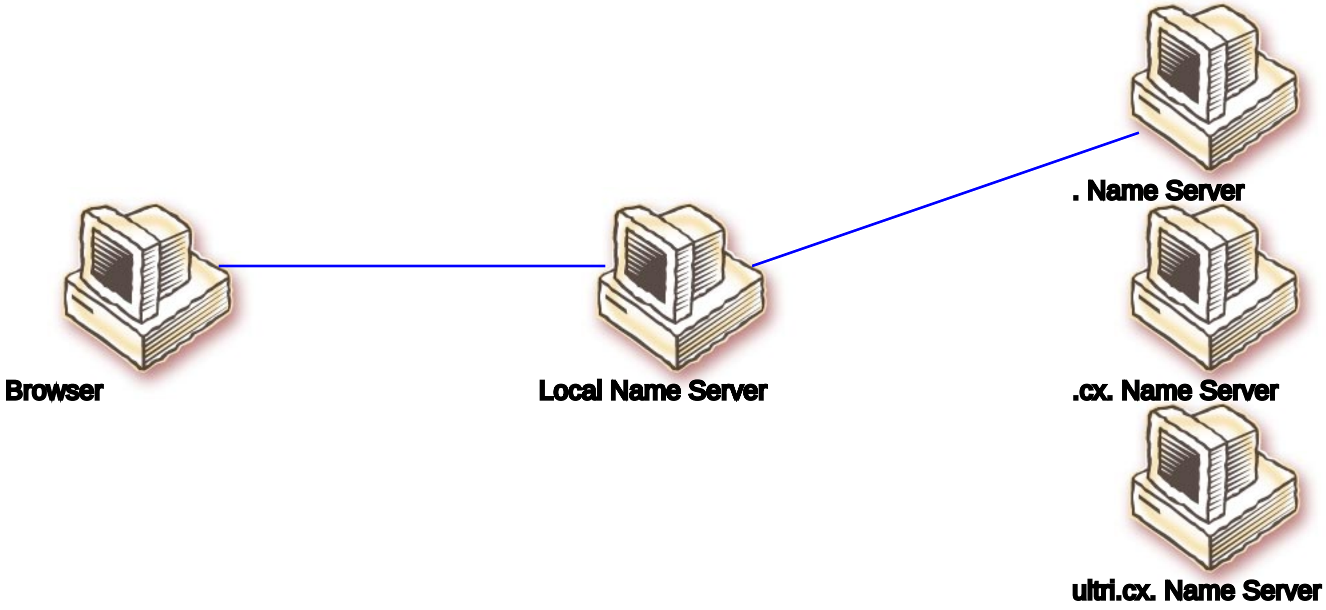
- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition
Australia
Servers
Probing
Tools

Definition

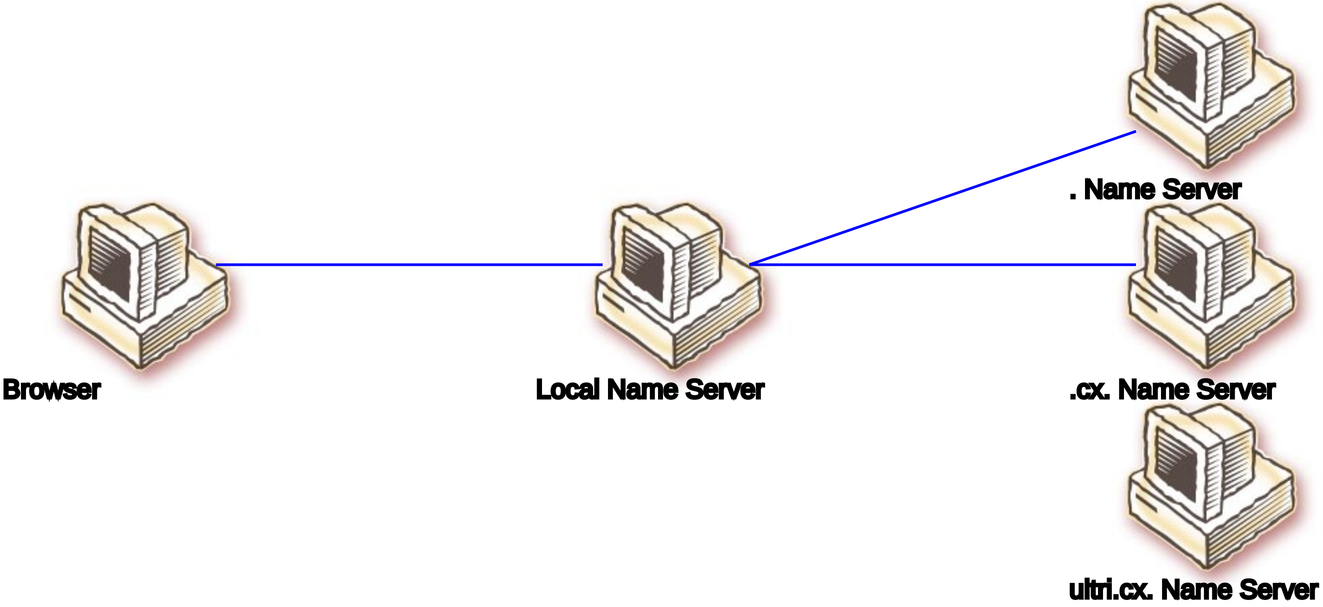
- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition
Australia
Servers
Probing
Tools

Definition

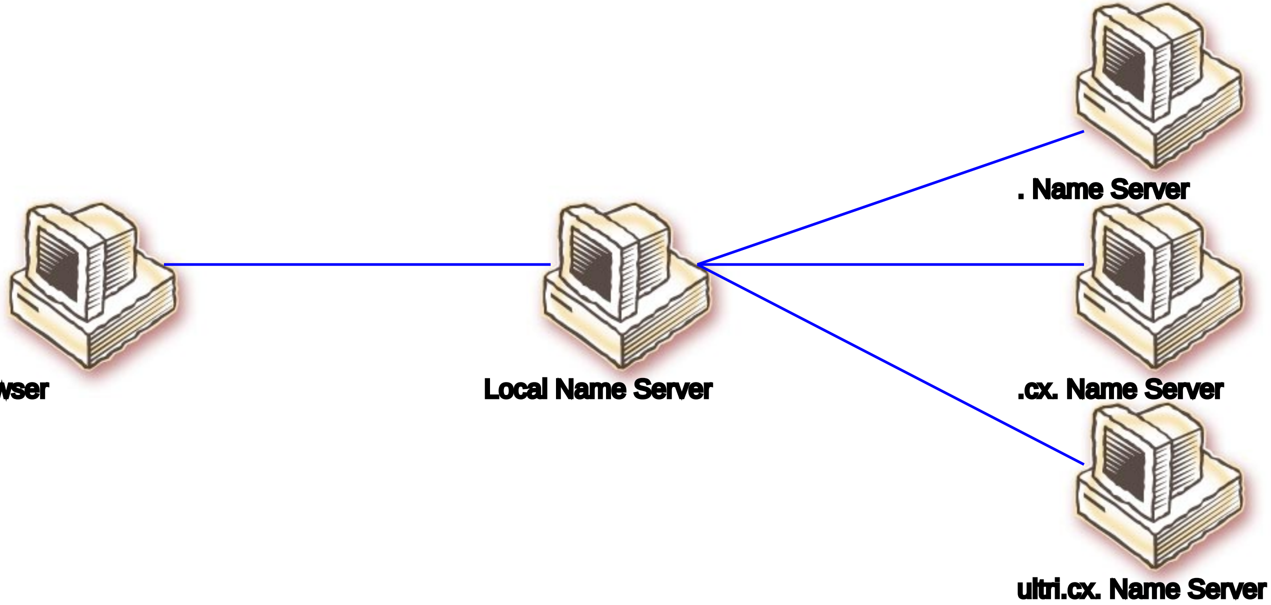
- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition
Australia
Servers
Probing
Tools

Definition

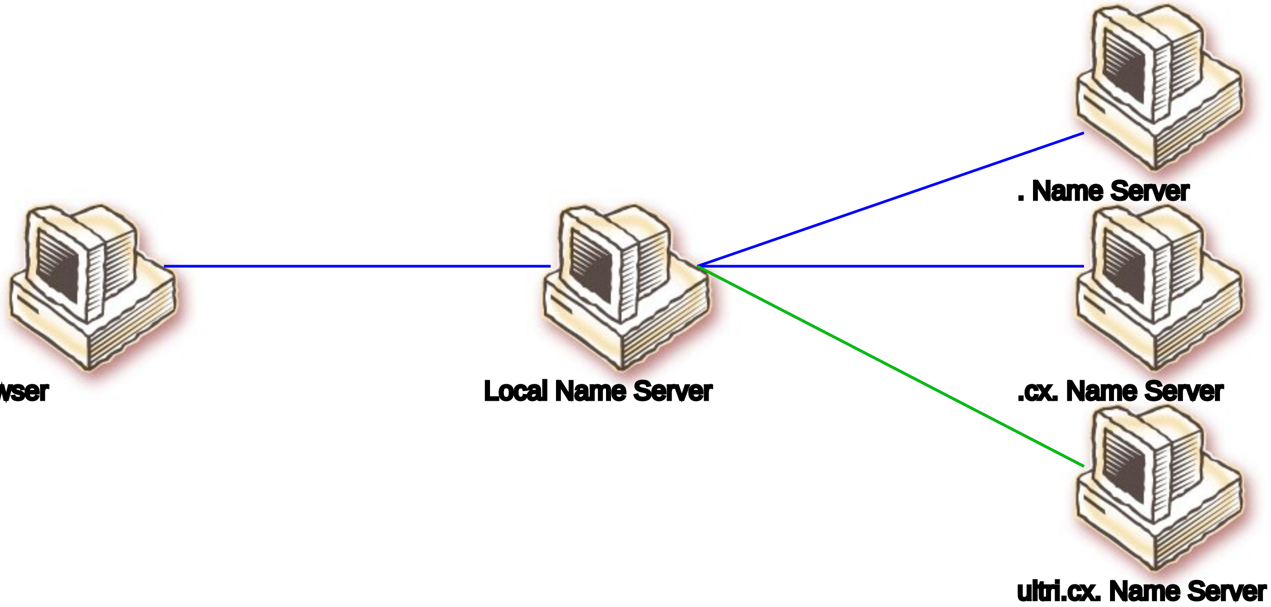
- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition
Australia
Servers
Probing
Tools

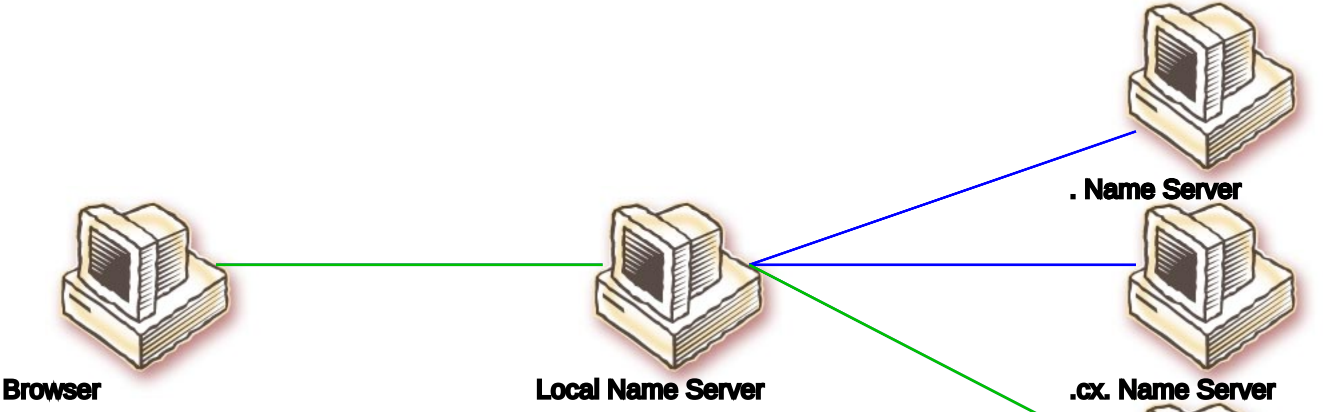
Definition

- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



Definition

- DNS stands for "Domain Name System" or "Domain Name Server"
- It provides a distributed database, commonly used for linking host names to Internet addresses



98% of traffic to the root servers is unnecessary

http://ucsdnews.ucsd.edu/newsrel/science/sdscRoot.htm

Definition
Australia
Servers
Probing
Tools

Commonly Used IN Record Types

- SOA: Metadata for a zone
- RP: The responsible people for a domain
- NS: The name server for a domain
- A: The IPv4 address for a name
- AAAA: The IPv6 address for a name
- CNAME: An alias for a name
- MX: A mail servers for a name or domain
- PTR: The name for an IPv4 address
- TXT: Text describing an object

Definition
Australia
Servers
Probing
Tools

Example zone file

```
@   IN  SOA  ns.adelaide.edu.au. hostmaster.adelaide.edu.au. (
    2003011503 ; Serial Number
    7200    ; Refresh Time
    1800    ; Retry Time
    2592000 ; Expire Time
    86400 ) ; Minimum Age
    IN  NS  ns.adelaide.edu.au.
    IN  NS  ns.saard.net.
$ORIGIN adelaide.edu.
    IN  A     129.127.41.6
    IN  MX    10  mx01.adelaide.edu.au.
    IN  MX    50  mx02.adelaide.edu.au.
    IN  RP    sb.adelaide.edu.au. sb.its.adelaide.edu.
    IN  RP    lc.adelaide.edu.au. lc.its.adelaide.edu.
www IN  CNAME web.services.adelaide.edu.au.
$ORIGIN its.adelaide.edu.
sb  IN  TXT   "Telephone - +61 8 303 3000"
    IN  TXT   "Facsimile - +61 8 303 4400"
lc  IN  TXT   "Telephone - +61 8 303 3000"
    IN  TXT   "Facsimile - +61 8 303 4400"
```

Definition
Australia
Servers
Probing
Tools

The Root Servers

- Serve ., the top most domain
- There are currently 13 root servers
    - Run by various organisations, situated around the world.
- Alternative roots exist, but do not enjoy a large installed base.
- Map!

Definition
Australia
Servers
Probing
Tools

Root Server Locations

A VeriSign GRS	Dulles VA
B Information Sciences Institute	Marina Del Rey CA
C Cogent Communications	Herndon VA, Los Angeles
D University of Maryland	College Park MD
E NASA Ames Research Center	Mountain View CA
F+Internet Software Consortium	Palo Alto CA, San Jose CA, New York City, San Francisco, Madrid, Hong Kong, Los Angeles, Rome, Auckland
G U.S. DOD NIC	Vienna VA
H+U.S. Army Research Lab	Aberdeen MD
I Autonomica	Stockholm
J VeriSign GRS	Dulles VA, Mountain View CA, Sterling VA (x2), Seattle WA, Amsterdam, Atlanta GA, Los Angeles CA
K Reseaux IP Europeens - NCC	London, Amsterdam
L IANA	Los Angeles
M WIDE Project	Tokyo

Definition
Australia
Servers
Probing
Tools

DNS in Australia

Definition
Australia
Servers
Probing
Tools

DNS in Australia - History

- 1984, the Top Level Domain (TLD) .au was delegated to Robert Elz (of ACSnet), at Melbourne University.
- May 1989, a 56Kbps satellite Internet link from the US to the University of Melbourne connects Australia to the Internet.
- May 1990, Geoff Huston becomes responsible for the second-level domains .edu.au and .gov.au.
- 1994, 1995, .net.au is delegated to Hugh Irvine of Connect.com.au (possibly Australias first ISP) and .asn.au to Michael Malone (Perths iiNet).

Definition
Australia
Servers
Probing
Tools

DNS in Australia - History (2)

- 1996, Robert Elz gives Melbourne-IT a non-exclusive 5-year licence to .com.au, in response to the workload. They start charging $125-$150 a year, so people start buying .net.au. Connect.com.au was flooded with name registrations and introduced a similar charge for .net.au.

- 1997, AARNet's commercial portion is broken off and sold to Telstra. AARNet2 is developed, which will later provide technology such as VoIP for AARNet2 members.

- 1999, Geoff Huston passes responsibility for .edu.au to auDA and .gov.au to OGO (now NOIE). Robert Elz passes responsibility for .com.au to Melbourne-IT.

- 2001, Robert Elz has administration of .au taken from him by auDA through ICANN.

Definition
Australia
Servers
Probing
Tools

DNS in Australia - Now

- Most high level Australian DNS servers are in Victoria and New South Wales, reflecting the adoption of the Internet in Australia
- munnari.oz.au is secondary for 26 gTLDs and 5 Australian 2lds
- Map!

Definition
Australia
Servers
Probing
Tools

Architecture of Some Common Name Servers

ISC Bind

- "BIND on Unix is regarded as the reference implementation of a DNS server and usually serves as the base for experimentation with DNS protocol extensions."
- Bind is nearly as old as DNS.
  - June, 1983 Jon Postel and Paul Mockapetris ran the first successful test of the automated domain name system. DNS is born.
  - Comments in Bind 4.8 indicate that version 1.1 was checked into SCCS on 30/April/86, 3 years later. The Bind pages seem to indicate that it is related to the original Jon Postel version?
  - Bind 4.8 was released 7/April/1988, contained about 9,000 lines of code, and included old SGI 68020 object files in the tarball.
  - Bind 9.3.0 is under development, the tarball currently contains about 286,000 lines of code, 132,000 of which are in bin/named/, lib/isc/ and lib/dns/.

Definition
Australia
Servers
Probing
Tools

ISC Bind - Versions

- There are three main versions of Bind
  - Bind 4: Was developed before 1985 at UCB as a graduate student project. Digital Equipment employees including Paul Vixie then took over maintenance of Bind 4. Security patches for it are currently maintained by ISC, however it is now deprecated in favour of Bind 8.
  - Bind 8: Bob Halley and Paul Vixie were co-architect/programmers for Bind 8, and released the first "production-ready" version of BIND version 8 in May 1997. Bind 8 was based heavily on Bind 4 code, and has had many security problems over the years.
  - Bind 9: A complete rewrite, attempting to improve security. It has stricter conformance to the RFCs.
- Bind 9 includes a name server, a resolver library, DNSSEC tools, Dynamic DNS tools, evaluation unicode domain name support and a set of client tools

INTERNET SOFTWARE CONSORTIUM

NLNetLabs NSD

- NSD is an authoritative only name server. It does no recursion, and knows every answer in advance.
  - As a result it is very fast, relatively simple and fairly robust.
- k.root-servers.net runs NSD.

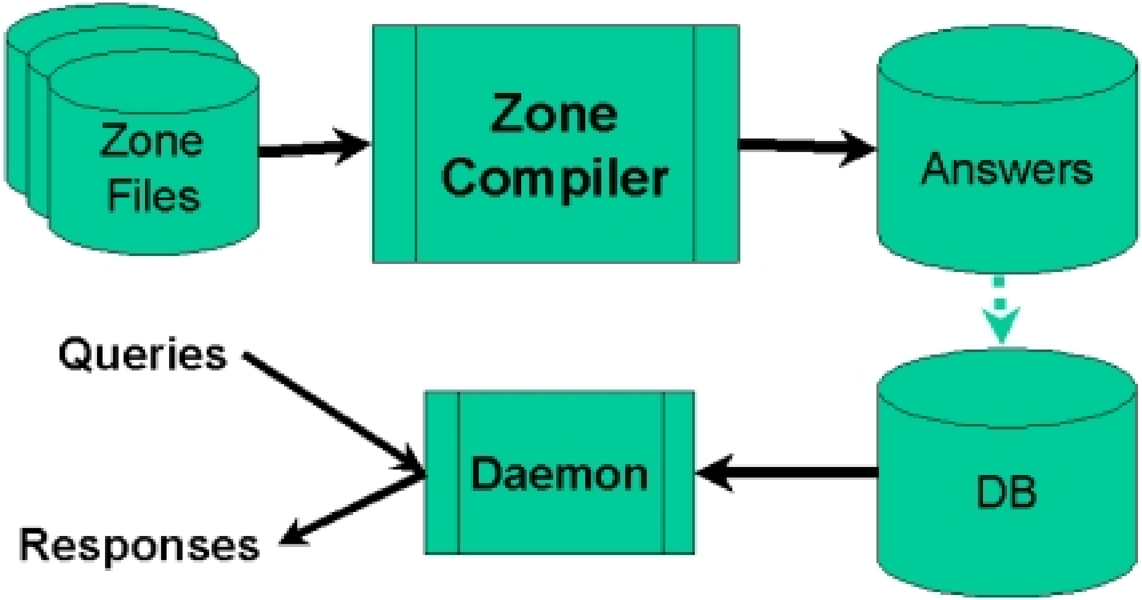


image from http://www.ripe.net/ripe/meetings/archive/ripe-42/presentations/ripe42-dns-aons/sld005.html

Dan Bernstein's DJBDNS

- DJBDNS is a collection of well designed Domain Name System tools. Security is one of the primary motivations for the development of djbdns.
- DJBDNS includes dnscache, tinydns (Authoritative only), axfrdns, axfr-get and some client programs. The server components are designed to by run under Dan's daemontools.
- Each component of DJBDNS has a conf tool, that is used for configuring it.
- Dan Bernstein is frequently misunderstood
  - Dan is well known for his ISC Bind and Sendmail critiques, which are well researched.
  - He has also identified problems with DNSSEC and other protocols, and specifically will not support DNSSEC until a key infrastructure is in place.

Definition
Australia
Servers
Probing
Tools

powered by djbdns

Fingerprinting DNS Servers

Definition
Australia
Servers
Probing
Tools

The Theory

- You can search for special values (version.bind, version.server)to determine which DNS server is running on a particular host
  - This response can be altered or refused

Definition
Australia
Servers
Probing
Tools

The Theory

- You can search for special values (version.bind, version.server)to determine which DNS server is running on a particular host
  - This response can be altered or refused
- DNS server behaviour largely follows the RFCs
  - Some behaviour is not clearly defined, or is altered to suit the implementation
  - Functionality specified by the RFCs has changed over time
- Identify the differences in implementations and versions, then craft queries that will indicate which server version is answering your query
  - For example, until version 1.0.1 NSD responded to Dynamic Update packets with "REFUSED", now it responds with "NOT IMPLEMENTED". You can send an update request to an NSD server to determine if it is version 1.0.1 or above.

Definition
Australia
Servers
Probing
Tools

Evolution of DNS

- DNS has changed over time:
  - Mailbox records have been phased out
  - Dynamic DNS has been introduced
  - DNSSEC is being engineered
  - IPv6 has been introduced
  - Authoritative only servers have emerged
  - Multilingual Support is being engineered
  - The OPT query field has been introduced
  - Additional query flags have been defined

Results of Some Fingerprinting

- Results!

Definition
Australia
Servers
Probing
Tools

Similar Studies

- Dan Bernstein has done some research into DNS fingerprinting.
  - http://cr.yp.to/surveys/dns1.html
    - 45% of .com name servers apparently run BIND 8
    - 23% of .com name servers apparently run BIND 9
    - 8% of .com name servers apparently run tinydns
    - 3% of .com name servers apparently run eNom DNS server
    - 2% of .com name servers apparently run BIND 4
- Brad Knowles ran a similar survey of gTLD servers
  - http://www.ripe.net/ripe/meetings/archive/ripe-44/
    - 56% of gTLD name servers apparently run BIND 4/8
    - 4.5% of gTLD name servers are unknown (SERVFAIL)
    - 2.7% of gTLD name servers apparently run UltraDNS
    - 79% of gTLD name servers allow recursion
    - During the "DNS wars", Eugene Kashpureff twice poisoned DNS and redirected InterNIC.net to AlterNIC in protest of NSI's monopoly on DNS name registrations. A Bind bug, in combination with recursion, made this possible.

Definition
Australia
Servers
Probing
Tools

Similar Studies (2)

- Men and Mice searched Fortune 1000 companies DNS for vulnerable versions of Bind
  - http://www.menandmice.com/6000/6200_bind_research.html
  - June 4th 2002, CERT announced a denial of service vulnerability in Bind 9.2.1. Men and Mice performed a survey to find how many Fortune 1000 companies were vulnerable
  - At least 69 were running vulnerable Bind 9 prior to 9.2.1
  - At least 139 were running versions of Bind with known vulnerabilities

Other DNS Tools

- Bind comes with tools such as dig, that can be used to perform queries and transfer zones.
- Whois can be used to query domain registries
  - http://www.samspade.org/
- Nmap can be used to resolve a block of IP addresses
  - http://www.insecure.org/nmap/
- DNSWalk Zone Integrity Checker
  - http://www.visi.com/~barr/dnswalk/
- Domtools DNS prober
  - http://www.domtools.com/dns/domtools.shtml
- On the web:
  - SamSpade.org has many tools
    - http://samspade.org/
  - Zonecheck is great for checking your domains settings
    - http://www.nic.fr/zonecheck/english.html

Definition
Australia
Servers
Probing
Tools

Other DNS Tools

- ding: DNS Ping. Measures the round trip time of DNS requests.
  - andrewc@internode.com.au

```
$ ./ding -c 3 -h www.google.com.au munnari.oz.au
DING munnari.oz.au (128.250.1.21):
        Hostname 'www.google.com.au', Type 'IN A'
251 bytes from 128.250.1.21: time=15.675 ms
246 bytes from 128.250.1.21: time=15.760 ms
246 bytes from 128.250.1.21: time=15.168 ms

--- munnari.oz.au ding statistics ---
3 queries sent, 3 responses received, 0% query loss
round-trip min/avg/max/stddev = 15.168/15.534/15.760/0.261 ms
```

Definition
Australia
Servers
Probing
Tools

Questions?

Definition
Australia
Servers
Probing
Tools

Special Thanks

- Thank you to the following people, who provided suggestions, historical and technical information, and in some cases proof reeding
  - Lachlan Cameron-Smith
  - Mark Prior
  - Rollo Ross
  - Dan Shearer
  - Seth Simons
  - Lindsay Whitbread
  - Clove Graphics

Definition
Australia
Servers
Probing
Tools

Bibliography

History of DNS
http://www.whmag.com/content/0601/dns/

History of the Internet in Australia
http://www.anu.edu.au/people/Roger.Clarke/II/OzIHist.html

Caught in a Bind
http://www.securityfocus.com/columnists/125

BIND History
http://www.isc.org/products/BIND/bind-history.html

Computer graphic in "What is DNS?:Definition" stolen from
www.parent.umn.edu/help.html

Dan Bernstein's DJBDNS
http://cr.yp.to/
http://homepages.tesco.net./~J.deBoynePollard/FGA/djbdns-myths-
http://www.lifewithdjbdns.com/

Fingerprinting DNS
http://cr.yp.to/surveys/dns1.html
http://www.ripe.net/ripe/meetings/archive/ripe-44/presentations/

- Slides rendered with AxPoint

Definition
Australia
Servers
Probing
Tools

AXKIT.COM
Open Source XML Web Publishing.