DNS is a simple game?

Musing about a protocol

Jaap Akkerhuis
In the beginning

- HOSTS.TXT (RFC 952)
- Maintained by SRI (Stanford)
  - Later by ISI
- A look up table
- Didn’t scale well

EXAMPLE OF HOST TABLE FORMAT

NET: 10.0.0.0: ARPANET:
NET: 128.10.0.0: PURDUE-CS-NET:
GATEWAY: 10.0.0.77, 18.10.0.4: MIT-GW.ARPA, MIT-GATEWAY: PDP-11:
MOS: IP/GW, EGP:
HOST: 26.0.0.73, 10.0.0.51: SRI-NIC.ARPA, SRI-NIC, NIC: DEC-2060:
TOPS20: TCP/TELNET, TCP/SMTP, TCP/TIME, TCP/FTP, TCP/ECHO, ICMP:
HOST: 10.2.0.11: SU-TAC.ARPA, SU-TAC: C/30: TAC: TCP:
Three Pillars make the Internet

• Naming — how we call things
  – Domain names
• Numbers — how address things uniquely
  – IP Number assignment (IANA, RIR’s)
• Routing — how to get to the address
  – Autonomous systems and BGP
Domain Name Service

- Hierarchical name space
- Notion of delegation
- Best effort
  - a-synchronous updates
  - a loosely coherent database
- Still: lookup of information
  - not a search engine!
- RFC 103[345]
DNS name space
Delegated Authority

- Fully Qualified Domain Name

jaap.do.nlnetlabs.nl

Digital Ocean  NLnet Labs  SIDN  PTI/IANA

authorities
jaap.do.nlnetlabs.nl. ???

- Ask the root-servers, refer to
- nl. name servers, refer to
- nlnetlab.nl. name servers, refer to
- digital.ocean.com. servers answers
  with IP-address (A record) 167.172.34.102
Name Server Types

• **Stub resolver, talks to**

• **Recursive resolver**
  – can caching answers
  – can talks to other resolvers
    • actually iterative
  – can follow referrals

• **Authoritative server**
  – gives the final answer
Not just IP addresses

- **MX**: mail address
- **CNAME**: alias to other name
- **SOA**: Start of authority
- **AAAA**: IPv6 address
- **NS**: name servers

- location, mothers name etc....
Scales well

- Started with thousands of names
- Now billions of names
- Thanks to lots of caching
- Loosely coherent system
What goes wrong?

- Sloppy implementations
- Desire to always try to give an answer
- Sloppy configuration
  - 90% of name servers are wrong, DNS works by accident
- Easy for monkey in the middle attacks (MITM)
  - data is public
- It is a cost center
Implementation

- Install and forget
- Often done on the cheap
  - old hardware
  - junior sysadmin is made responsible
- Importance often overlooked
Naming Complications

• Private name spaces
  – Company Intranet
  – NAT boxes
  – “split horizons”
  – leaking information

• Name collisions
  – fritz, corp, home,
  – corp.com
  – Certificates for non-FQDN’s
Security extensions

• Authenticates the answer
  – Note, the authority might still be lying
  – Allow for auditing
  – Substrate for other security methods
    • DANE etc.

• Changes paradigm
  – needs maintenance
  – make the systems brittle
    • punishes badly configured DNS servers

• Data is still public
Games with DNS

• Make answer dependent on question
  – CDN can route to topological closest data
    • best effort
      – Defer some kinds of DOS attacks
• Rewrite (negative) answers to insert adds etc.
  – DNSSEC can prevent that
• Forwarding
  – Central caching, avoiding ISP etc.
Privacy extensions

• **Data is public**
  - easy to listen to
  - post Snowdon people started to worry about “Meta Data”

• **Hop by hop**
  - DNS cookies

• **End to end**
  - VPN style
DOT: DNS over TLS

- TLS protection
- Per system same namespace
- Known port, easy to block
DOH: DNS Over HTTPS

- Bypasses the local stub resolver
  - application picks the resolver
  - trust that that resolver doesn’t lie
  - impossible to scan
    - malware?
  - possible to control the name space for that application
  - difficult for “parent controls”
    - my net, my rules
  - “Balkanisation” of the net for different apps
    - IETF Working Group: ADD
Who controls the root?

- **ICANN**: International Corporations for Assignment of Names and Numbers
  - Protocol parameters, mostly via IETF
    - Internet Engineering Task Force
  - IP numbers, policies by ASO, but really NRO
    - Address Support Organization
    - Number Resource Organisations (RIRs)
  - Names via SO’s (GNSO, CNSO) and AC’s
    - Generic Name SO, Country Name SO
    - Government Advisory Committee
IANA — PTI

- Registry for Protocol Parameters
- Registry for IP numbers
- Root Registry allocates TLDs
  - legacy (com, org, net, edu …)
  - country codes (nl, us, ss …)
  - sponsored (aero, jobs, gov …)
  - generic (club, xyz, politie, study …)
  - brand domains (sony, canon …)
Root Zone Maintenance

- IANA/PTI decides (confirmed by ICANN)
- Verisign for technical checks and database operator
- 12 Root Zone operators, see root-servers.org
  - 9 root zone operators in Amsterdam
  - Zone current refreshed twice daily
  - More than 1000 instances
    - by means of anycasting
Wat can you do?

• Fix your DNS, add DNSSEC
  – Check with internet.nl for advice
• Help with open standards
  – ietf.org
• Become a politician
  – ICANN
  – IGF