The Domain Name System (DNS) Explained

- Structure, Usage, and Involved Parties -

Peter Koch, DENIC eG
<koch@denic.de>

European Commission, Brussels, 23 February 2012
Domain Name System
Registries & Registrars
DNSSEC
The Domain Name System

- Names are much more user friendly than numbers (addresses)
  - 2001:67c:2e8:22::c100:68b
- Hierarchy offers logical context
- DNS is also called the *Phone Book for the Internet*
- Maps names to numbers (IPv4 or IPv6 addresses)
  - ... or other elements of Internet technical infrastructure
  - like mail servers
- Unlike the phone book, you can map a name to *any* number
- Computers continue to talk numbers (addresses), not names
- Names are spelled left-to-right with dots as separators
  - bbc.co.uk
  - ec.europa.eu
The Domain Name System

- Lookup System
  - No search
  - No fuzzy matching
  - Need to know exactly what to ask for

- DNS is service agnostic
  - No idea what a requested IP address will be used for
  - e.g., web server names may or may not start with www (see ec.europa.eu)
  - ... and there is much more than the web!
The Domain Name System – Key Features and Components

- Distributed, redundant and resilient
- Responsibility for name space can be delegated
- Multiple name servers per DNS zone

- Provisioning
  - Creation and maintenance of domain data in a database

- Publication
  - Conversion of technical domain information into collection called zone file
  - Name servers respond with information from zone file

- Resolution
  - Active fetching DNS information, following hierarchy
Domain Name System
Registries & Registrars
DNSSEC
The Domain Name System – Cooperating Parties

- Registry – maintains TLD database
  - Publishes DNS zone file
- Registrant – registers domain name
  - Operates (or initiates operation of) servers and services
- Registrar – agent
  - Maintains individual domain name registrations
The Top Level Domains

ccTLDs
- Country codes per ISO 3166
- Role defined in RFC 1591
- mostly not-for-profit
- Policy setting within local community
- Diverse in the details

gTLDs
- Generic Top Level Domains
- Policy setting within ICANN
The Role of the Registrar (backup slide)

- Registrar maintains domain registration of behalf customer (registrant)
- Multiple Registrars per TLD
- Increases competition
- Easy access to multiple TLDs for the customer
- Increased efficiency and security
- Registrant can transfer a domain form one registrar to another
Domain Name System
Registries & Registrars
DNSSEC
Secure DNS (DNSSEC)

- The DNS is intentionally very lightweight
- Initially designed without authentication of the response data
- Various attacks described as exercises and demonstrated in the wild
  - Attacker needs resources and chance

- Digital signatures to authenticate DNS responses
  - Make sure the data originates from the correct source (zone file)
DNS Resolution – Cache Poisoning Attack – without DNSSEC

Resolver

Nameserver

Query vvv.insecure.example

DNS Answer 1.2.3.4

DNS Answer 6.7.8.9

Redirecting e-mail or web traffic or more

Query vvv.insecure.example
Cache Poisoning – Mitigation with DNSSEC

Diagram showing the interaction between a resolver and a nameserver, with queries and responses indicated. The diagram includes the following labels:

- Resolver
- Nameserver
- Query vvv.secure.example
- DNS Answer 1.2.3.4
- Shielded by authenticated responses
- DNS Answer 6.7.8.9

The diagram illustrates how DNSSEC can protect against cache poisoning by shielding responses with authenticated data.
Domain Name System
Registries & Registrars
DNSSEC
Thank You!

koch@denic.de

<http://www.denic.de>

<http://www.centr.org>