DNSSEC IN THE MODERN WORLD

Ólafur Guðumundsson
Shinkuro, Inc.
Ogud@shinkuro.com

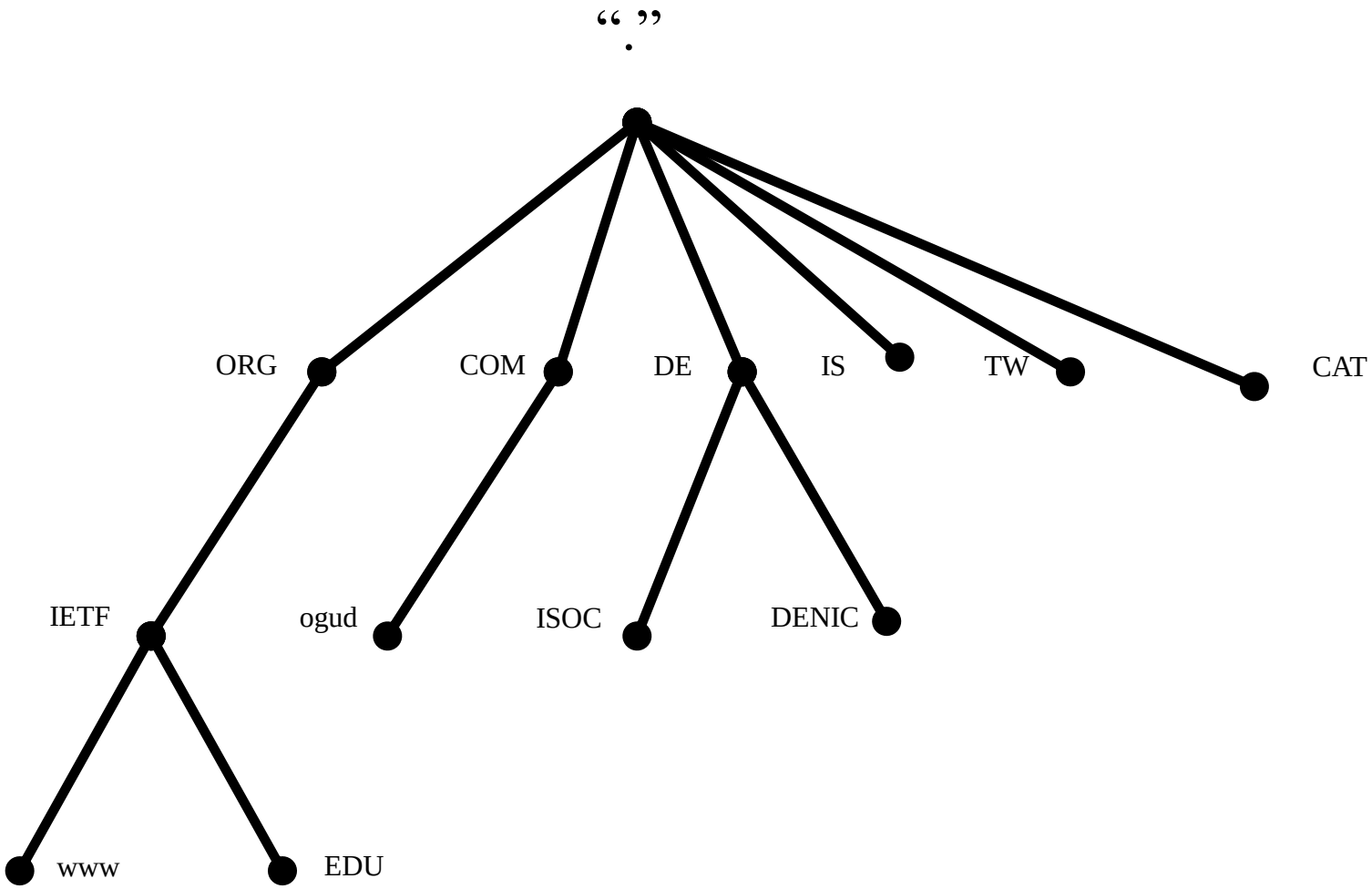
OUTLINE

- DNS and DNSSEC intro
- Status of DNSSEC deployment
- IPv6 and DNSSEC
- Deployment

BASICS OF DNS

- DNS is a hierarchical distributed database
  - Not a general purpose DB only simple lookup no search
- Lookup is by name and type
  - Name broken into parts called labels, labels are separated by a dot “.” in presentation format.
    - www.twnic.net.tw
  - The names form a tree
  - Each label can represent a simple ascii string or a Unicode encoding of non English characters.
    - Xn--<blob>.com.tw
- Answer consists of one or more Resource Record sets (RRset).

DNS TREE

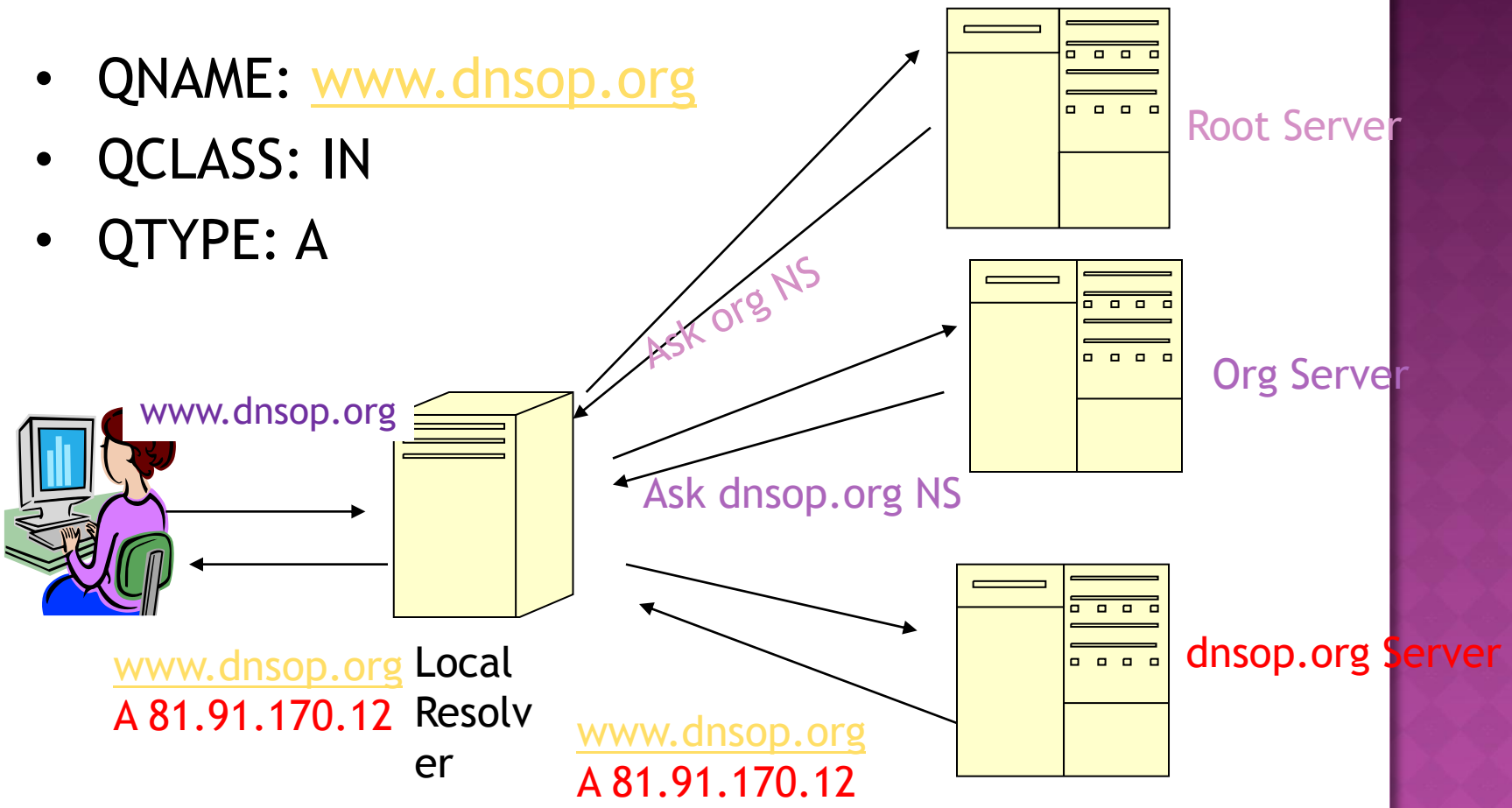


DNS FUNCTIONAL COMPONENTS

- Resolver
  - *stub*: simple, only asks questions
  - *recursive*: takes simple query and makes all necessary steps to assemble the full answer,
  - *caching*: A recursive resolver that stores prior results and reuses them
- Server
  - *authoritative*: the servers that contain the zone file for a zone, one Primary, one or more Secondaries,
- Some implementations perform resolver and server roles.

TRAVERSING THE DNS TREE

- QNAME: www.dnsop.org
- QCLASS: IN
- QTYPE: A



DNSSEC INTRO

- DNSSEC is a recent addition to the protocol to provide integrity to DNS answers.
- Role: Protect DNS
  - How done: view from 10 km.
    - A DNS RRSet is signed by the zone it belongs to.
    - DS RRSet is vouched for by parent zone.
      - Chain of trust DS→ DNSKEY → DS →DNSKEY
- What DNSSEC does not do:
  - Make data in DNS any more correct
- Single Trust Anchor: DNS Root is signed
  - IANA Root

DNSSEC: MORE DETAILS

- Data integrity protection
  - Each DNS RRSet is signed by a digital signature
    - RRSIG containing a signature by the zone private key, for a certain time period
- Existence proof:
  - Chain of NSEC or NSEC3 records lists all names in a zone and their RR types. (authentic proof/denial of existence)
- Parent signs a fingerprint of child's Key Signing DNSKEY (DS RR)
  - allows transition from a secure parent zone to a secure child zone.

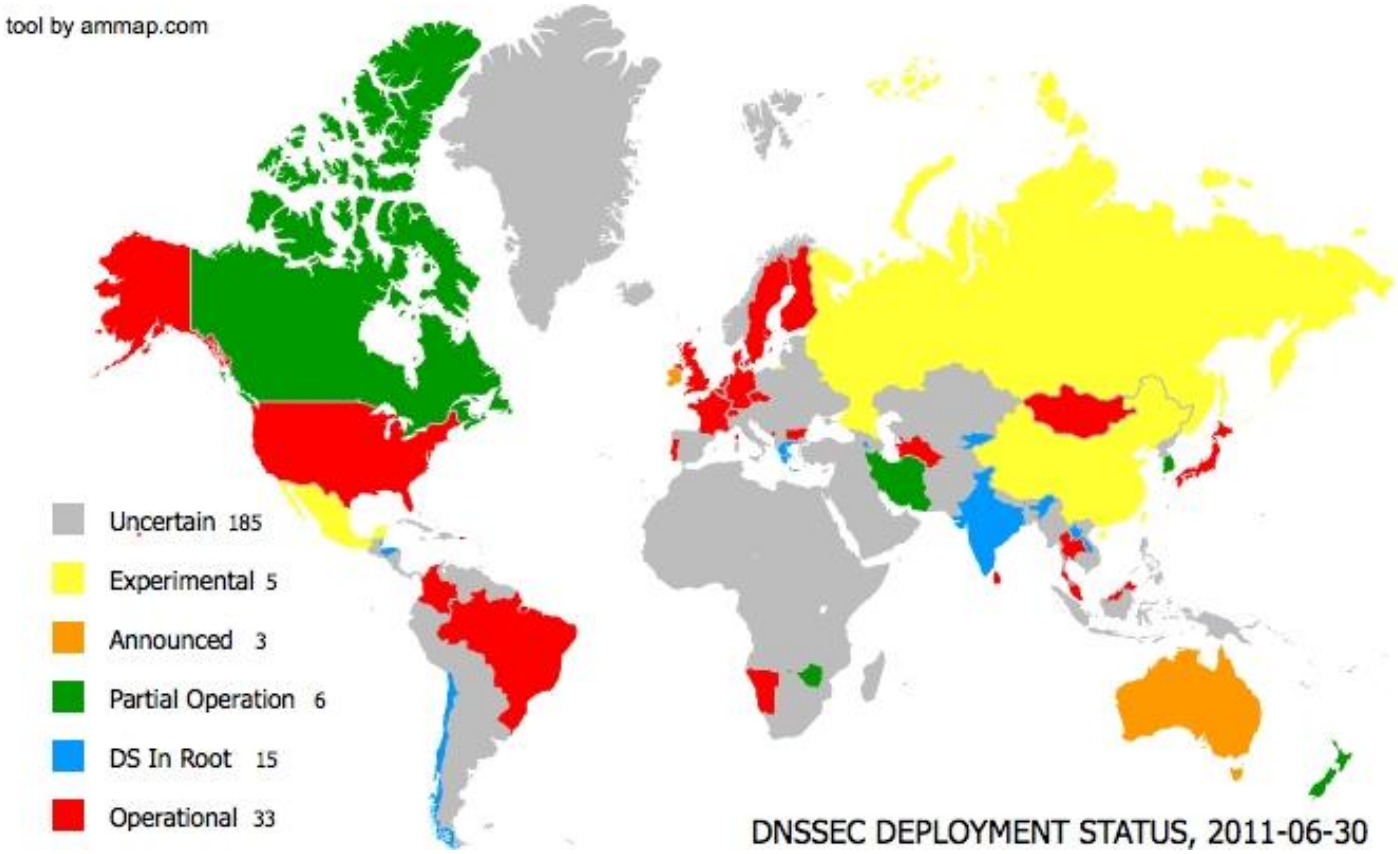
DNSSEC IMPACT ON OPERATIONS

- More things can go wrong
  - "Fire and forget until next change" operation not possible any more
    - DNS zones need to be resigned periodically
      - Really should be handled by tools not humans
  - Key rollovers
    - Timing is important
  - Trust anchor maintenance
    - Order and timing constraints must be respected
      - ➔ domains can become invisible for a while
- Keep up with vendor updates

DNSSEC IN TLD'S 2011/11/16

12 Nov 2011	Total	Signed	DS in Root
ccTLD	247	56	53
IDN ccTLD	30	4	2
gTLD	22	12	11
IDN gTLD	0	0	0
Test IDN	11	11	11
Total	310	81	77

CCTLD'S DNSSEC STATUS



DNSSEC AS ENABLING TECHNOLOGY

- DNSSEC provides allows the insertion of higher value data in the DNS
  - Keys
  - Identites
  - Policies
- This has the potential to become a disruptive force for new applications

DNSSEC ENABLED: DANE

- DNS-based Authentication of Named Entities: is to place TLS keys and CERT's in DNS
  - Augment Certification Authorities
  - Express what CA's are used by a domain
- Goal:
  - Stop TLS MiM attacks
  - Avoid the use of fake Certs
    - Replace CA's for most uses but EV certs
- Later: other protocols in addition to HTTPS/TLS

DNSSEC ENABLED: DKIM

- Domain Keying Internet Mail
  - Mail servers sign outgoing emails
  - Recipients can check signatures that mail came from servers in that domain
    - Prevents spammers from impersonating your mail servers

DNSSEC AND IPV6

- Reverse IPv6 lookup
  - Provision: hard
  - Maintenance: hard
  - Signing: Hard and expensive
- Solutions:
  - Sign on the fly (JPRS demo)
  - Signed wild cards
  - No reverse map

How to deploy DNSSEC

- Slow and steady in phases
  - Update tools and servers
    - You may need to replace firewalls, routers
    - Revisit procedures
  - Sign Zone's
    - Not important ones first
  - Test and Test some more
    - Create a test plan and walk through it
  - Monitor
  - Add Trust anchors to parent zone
- Start adding new services
- Keep up with vendor Updates

DNSSEC TOOLS

- There are all kinds of tools at various levels of maturity: Use them
- DNSSEC is not a simple technology

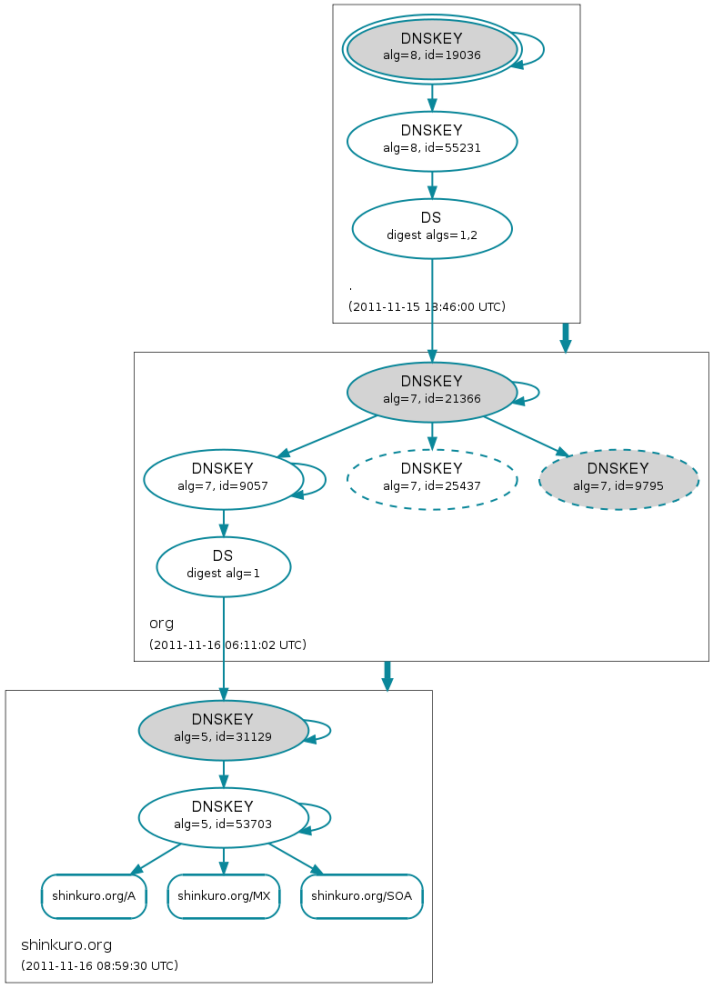
DNSSEC TOOLS: NAME SERVER

- Software:
  - NSD/Unbound full support
  - Bind-9.7,9.8 full support
  - Nominum: full support
  - Microsoft 2008 server: partial Support
  - PowerDNS: full support
- Appliances:
  - Xelerance
  - InfoBlox
  - Secure64
  - InfoWeapons

MORE TOOLS

- Signing and maintainance tools
  - Dnssec-tools.org
  - OpenDNSSEC
- Monitoring tools:
  - DnsViz
  - Dnssecmonitor
  - ZoneCheck v3.0

DNSVIZ: SHINKURO.ORG



DNSSEC IN THE NEAR FUTURE

- Most TLD's will be signed
- Many enterprises will adopt DNSSEC in particular ecommerce
- Many web services will adopt to avoid issues with Rouge Certificates
  - No more Iranian certs for gmail.com

DNSSEC and Embedded Systems

- Any product that has DNS component and does not support DNSSEC has the potential to become a barrier for DNSSEC deployment
  - Firewalls
  - Smart Routers
  - Application Gateways
- DNSSEC support is a market opportunity

QUESTIONS

- Thank you