DNSSEC Deployment: Big Steps Forward; Several Steps to Go

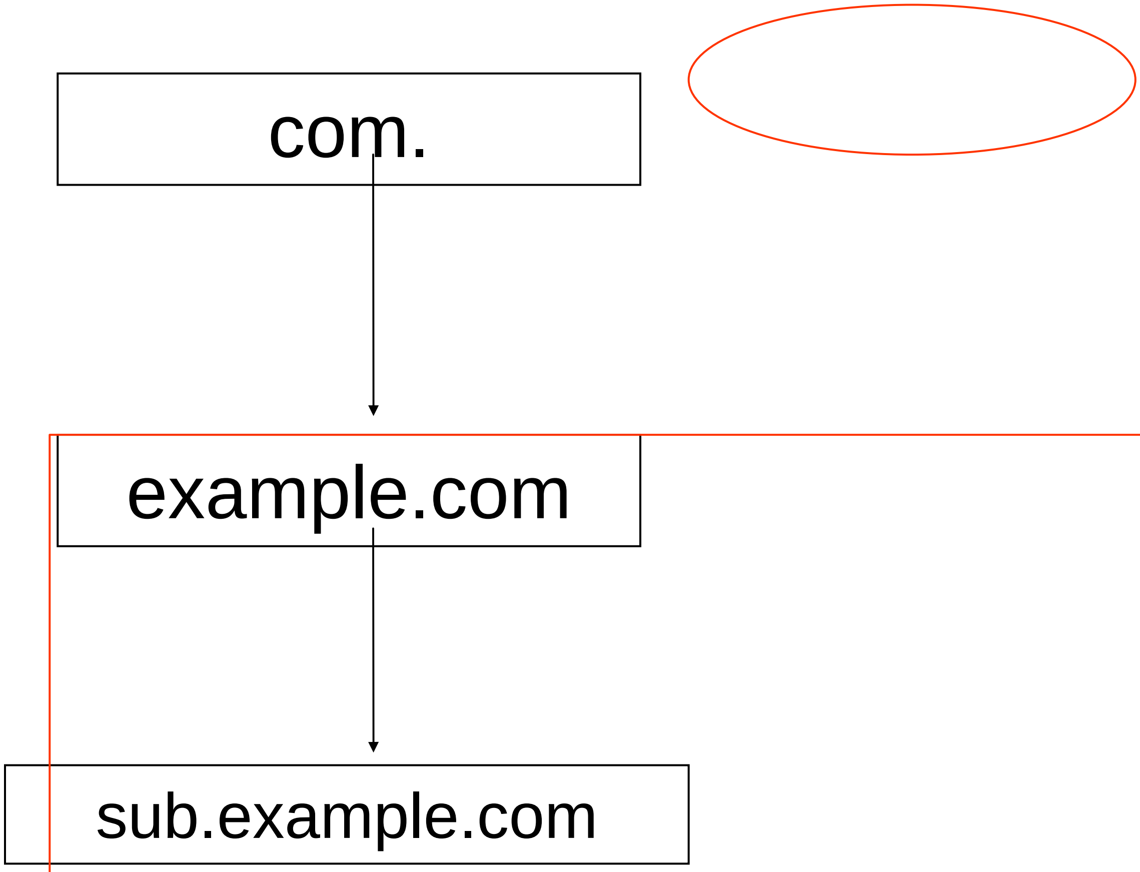
NANOG 32

REAL threats

- One-way SSL authentication tunnel
  - How do you know if you are communicatinommuni-•aa

End-to-End protection

Trustedcom.



com.

example.com

sub.example.com

signs this

Registrant-Registrar-Registry Setup

Registr

Registrant (Enterprise) view – What is different?

- Key gen and Key mgmt
- Zone signing operations
- Nameserver provisioning
- Need to securely transmit DNSSEC-related info to registrar
- Security from validating resolvers to non-validating stubs
- Incident handling

Registrar view – What is different?

- Need to securely receive DNSSEC-related information from the registrant
- Need to securely transmit DNSSEC-related info to registry
- Incident handling

Registry view – What is different?

- Need to securely receive DNSSEC-related information from the registrar
- Need to create the secure delegation in the parent zone
- Key generation and Key management operations
- Zone signing operations
- Nameserver provisioning
  - Size of zone data increases because of signatures
  - More computational power needed (crypto operations can take time)
  - Synchronized time (signatures have temporal dependency)
- Incident handling

Tools – present and missing

Registrant

Registry

Enterprise-wide Experiments

- “Shadow” deployment efforts are ongoing
  - Mirrn502 DNSSEC oxpeations in a non-g

Registry-level Experiments

- NLnet (.nl) – Netherlands
  - http://www.nlnetlabs.nl/dnssec/
- NIC-SE (.se) – Sweden
  - http://dnssec.nic-se.se/
- JPRS (.jp) – Japan
  - DNSSEC field test in conjunction with ENUM trial (http://jprs.jp/en/)
- Verisign (.net DNSSEC pilot) – U.S.
  - http://www.dnssec-net.verisignlabs.com/
- Verisign DLV (.com/.net) – U.S.
  - http://www.dlv.verisignlabs.com/

Application-level Experiments

- SSH

Hard(er) Problems

- Privacy – Not originally a goal
- Root key – Politically charged

DNSSEC Resources

- The DNSSEC deployment Working Group home page
  - http://www.dnssec-deployment.org
- Comprehensive DNSSEC resource page
  - http://www.dnssec.org
- Software
  - BIND 9.3.0 (http://www.isc.org)
  - NSD (http://www.nlnetlabs.nl/nsd/)
  - Net::DNS::Sec (http://www.ripe.net/disi/)