DNSSEC
Transforming a protocol bug into an admin tool

Lutz Donnerhacke

db089309: 1c1c 6311 ef09 d819 e029 65be bfb6 c9cb
A protocol from better times

- An ancient protocol
- People were friendly and trustworthy
- Internet was a warm and fuzzy place
- *DNS is a protocol from admins for admins*
- Main assumption: Computers do not lie
- Idea: A hierarchical distributed database
- Store locally, read globally
Playground to extend

- DNS works, so use is as a container
  - http://tools.ietf.org/wg/dnsext/
- DNS scales, so push a lot of data in
  - in-addr.arpa
- DNS can be misused as a catchword repository: www.catchword.com
- DNS may have multiple roots, so introduce private name spaces
Playground to manipulate

- Push all initial requests to a payment site
- Prevent requests to bad sites
- Offer own search engine for NXDOMAIN
- Geolocation for efficient content delivery
- Geolocation for lawful content selection
- Provide different software updates
- Prevent worm updates
trustroute +trace

- Modelling real world data as DNS records
- Transferring data into DNS primary server
- Transferring data into DNS secondaries
- Updating meta data in parent zone
- Delivering data to recursive servers
- Processing by resolver code
- Providing structures to applications
- Interpreting data by users
Securing the data flow

• Two possible design goals:
  – Detect manipulation
  – Prevent wire-tapping

• Facing typical problems
  – The compatibility hydra
  – Partial roll-out
  – Satellite networks

• Still designed by admins: NSEC(3)
DNS SECurity

• Trust the primary name server data
  – Signed by the zone-c

• A framework to verify integrity
  – Signature chains up to a trust anchor

• In band key management
  – DS records in parent zone (but glue!)

• Supports caching as well as offloading

• Provides peer authentication
Trust anchor management

• In an ideal world the root is signed
• Many roots: Trust Anchor Repositories
• In band key roll-overs: RFC 5011
• Manual trust anchors: Edit files on disk
• Automatic trust anchors: Look aside zones
• Open question: Precedence of sources
The last mile

- In an ideal world, apps use a new API
  - Error messages might become helpful
  - Validation errors are SERVFAIL

- Resolver offloading
  - Provide validated data with AD
  - Allow validator chaining with CD
  - Question: Provide bogus data at all?

- Attacks on the last mile even for LEAs
Finally gain benefits

- **DNSSEC adds trust to DNS**
- Use DNS as a hierarchical distributed DB
- Manage your SSHFPs centrally
- Manage your CERTs distributed
- Manage your OpenPGP keys distributed
- Do not deliver poisoned data to clients
- Validate late, validate centrally
Did you sign your zones?

Why not?