Survey of DNSSEC

Lutz Donnerhacke

DNSSEC Meeting (2008-01-16)

DNSSEC related actions

- Run DNSSEC in productive enviroments (currently using a signed root)
- Gather as much signed domains as possible.
- Include all entry points into a DLV and keep this list up to date.

How to gather domains

- grep all zones listed at SecSpider
- grep the known web key repositories (like RIPE)
- retry all zones a came across in the last years
- try to fill all holes in the DNS hierarchy
- try AXFR on the known signed zones or - if this fails - collect a few hundred entries by zone walking (that's even true for DLVs, I came across)
- make reverse lookups of IPs near the IPs listed in signed zones
- try all zones of TLDs, I have access to: AT, FR, RU, COM, NET ... (preferably with written contract)

➢ All is run on a weekly or monthly basis

Running the signed root

- obtain the data from ICANN and RIPE
- check each modification personally
- collect the DNSKEY entries using validating resolvers and update the keysets if necessary
- modify them to point to my servers and sign them
- distribute it to a set of servers

Monthly statistics

- based on a website snapshot
- remove test hierarchies
- summarize in different categories
- Category „unreachable“ is NOT signed
- „unreachable“ times out, if no DNSKEY and no DS

Biyearly mailing

- send e-mail to the SOA mname
- each category has a special text
- defensive hints about misconfiguration (learned the hard way)
- weak keys category refined to <1024 bits