DNSSEC in Fedora

Red Hat, Inc.

Adam Tkáč

September 10, 2009

Recursive servers

- easy targets, large impact of successfull attack
- complex maintenance of trust anchors
- automatic update of trust anchors requires support from domain maintainer (RFC 5011)
- accurate time required
- limited performance of DLV registers

Distribution can help

- automatic update of trust anchors
- centralized administration of DNSSEC configuration
- problems
    - installation of distribution with old keys
    - recovery when trust anchors are outdated

Intergration in Fedora 11

- /etc/pki/dnssec-keys/ directory includes keys for signed TLDs
- centralized DNSSEC configuration in /etc/sysconfig/dnssec
- BIND and unbound servers are integrated
- DNSSEC validation and DLV on by default
- all in dnssec-conf package

dnssec-conf
utility

DNSSEC
configuration

DLV
configuration

DNSSEC keys

unbound
daemon

named
daemon
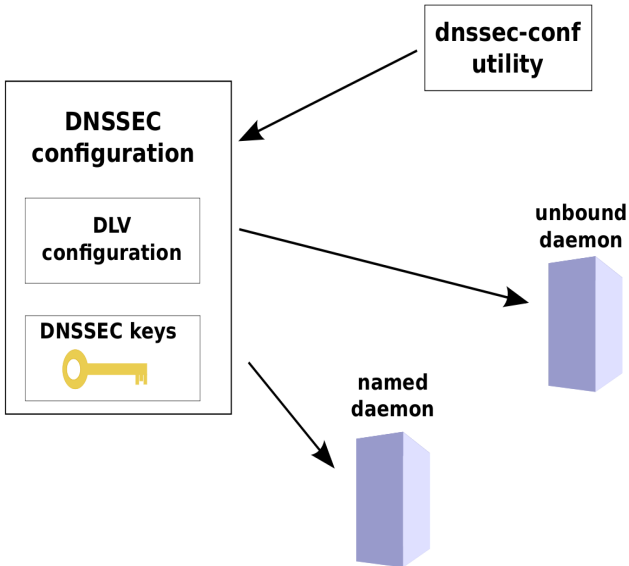
Clients

- DNSSEC integration to stub resolver is contraproductive
- clients are recursive servers
- send queries to ISP servers only
- fully automated administration of trust anchors

DNSSEC and NetworkManager

- dynamically reacts to network changes
- exposes all information needed by local DNSSEC server
- current servers (BIND, unbound) are not capable to obtain information from NM

User problems

- broken middleware
  - DNS doesn't work? Buy a new router!
- keys become outdated
- resolving needs more time
- more services have to run

fedora

Advandates

- after more than 10 years DNSSEC will become widely used
- crucial network service becomes secure
- client-side caching

Questions?

The end.

Thanks for listening.