DNSSEC Support by Home Routers in Germany

Thorsten Dietrich

Federal Office for Information Security

RIPE-60 / 06. May 2010

Content

- Motivation / BSI activities
- Previous Tests
- Objectives
- Test Methodology / Testbed
- Reviewed Devices
- Results
- Conclusions

Motivation / BSI-Activities

- DNS is crucial part of Internet-infrastructure
- Vulnerable by design
- DNSSEC helps to improve the security of the internet
- Adoption of DNSSEC strongly required from BSI point of view
- Launch of DNSSEC-Initiative by DENIC, eco (german provider association) and BSI to evaluate the introduction of DNSSEC for .de domains
    - DENIC: Provision of test environment for collecting and reviewing operational and technical experiences
- Raising awareness, discussions with public and private sector, universities
- German government domain “.bund.de” was signed a few weeks ago
- Home router study

Previous Tests

- Origin in 2007:

  DNSSEC-signed zones were suddenly unreachable for some users in Sweden

  → Reason: Some Home Routers couldn't handle DNSSEC-Flags
- Tests of Home Router capabilities in Sweden (Feb. 2008) and GB (Sept. 2008) followed
  - Findings:
    - Only few devices could **proxy** DNSSEC queries without limitations
    - Most devices could **route** DNSSEC queries to upstream resolvers
  - Tested devices mostly relevant for Swedish / British market
  - Further development / technical progress since 2008 ?
  - Specification of IETF RFC 5625 „DNS Proxy Implementation Guidelines“
- → Necessity to examine the situation in Germany

Objectives of BSI-Study

- Assess router support for DNS queries relating to DNSSEC-signed domains
  - Is the router able to **proxy** DNSSEC requests ?
  - Is the router able to **route** DNSSEC requests ? (Bypassing the integrated DNS-Proxy)
- In detail:
  - Handling of Signaling-Flags (D0, AD, CD), introduced with DNSSEC
  - Handling of UDP-Packets > 512 Byte (EDNS0 Support)
  - TCP-Fallback
- Other security issues, i.e. factory security settings for Wireless-LAN

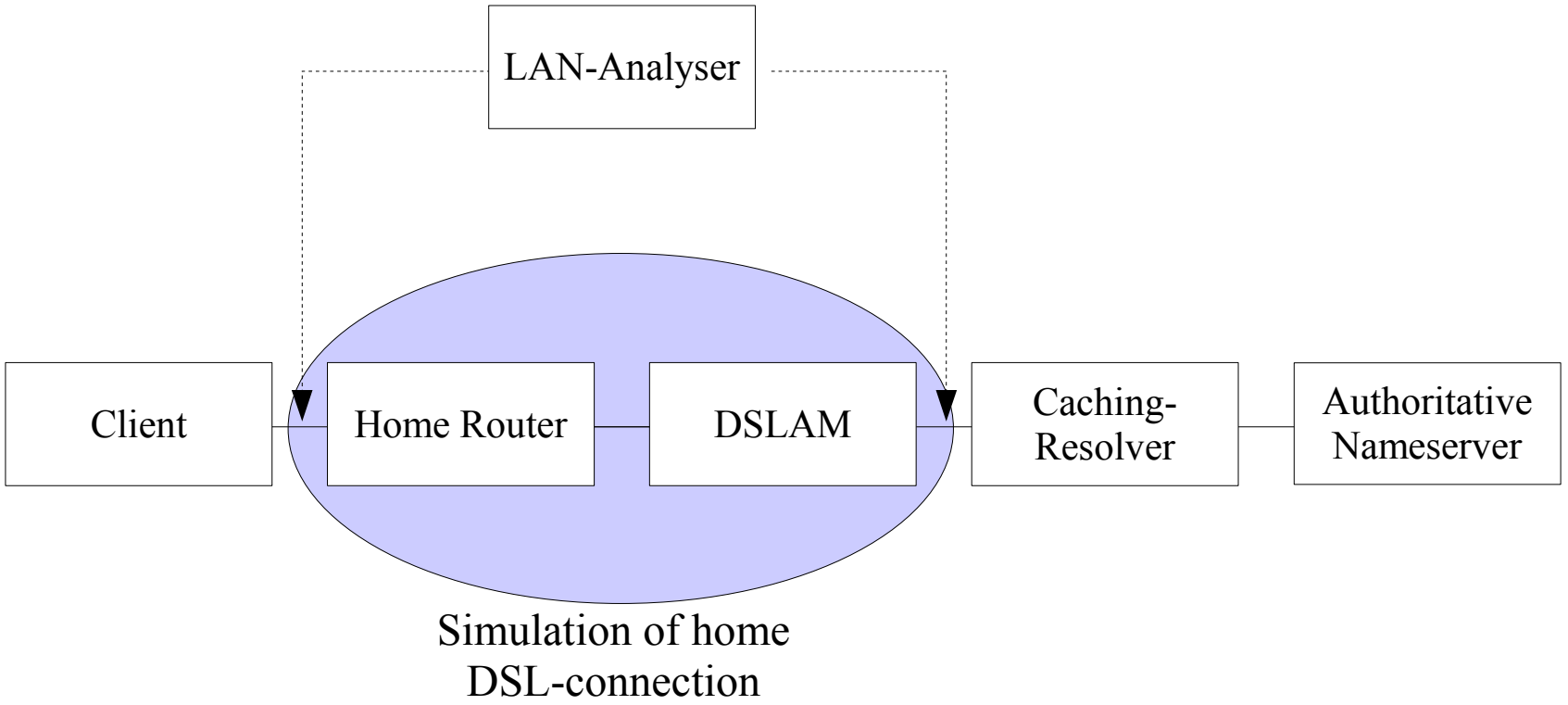
- Study published under
  https://www.bsi.bund.de/cae/servlet/contentblob/995592/publicationFile/63661/DNSSEC_pdf.pdf

Test Methodology

- Several DNS queries of various Resource Records to examine capabilities
  - UDP and TCP-based queries
  - EDNS0 queries with various buffer sizes
  - Resource Records with various length
  - Signed and unsigned Resource Records
  - Use of DNSSEC-related flags
- Using and bypassing of internal DNS-proxy

Testbed

- DNS-client
- DNSSEC-aware caching-resolver
- DSLAM
- Authoritative nameserver



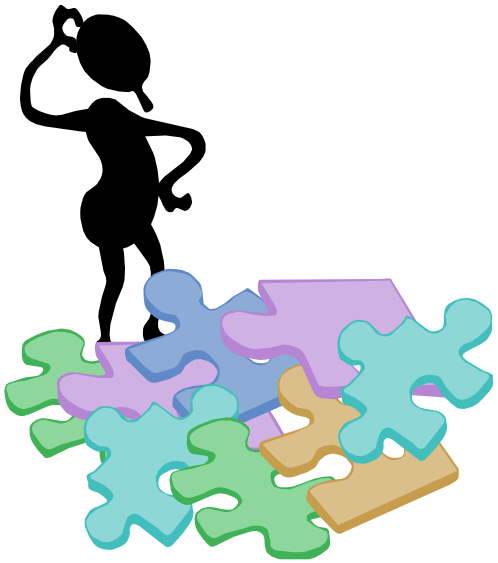
- N.B.: Internet-based tests not reliable, i.e. due to lack of configuration parameter for queried caching-resolver

Reviewed Devices

- 36 devices tested
- Thereof 23 with integrated DSL-modem
- Study considers about 90% of home routers supplied by broadband providers
- BUT: No representative study
- Support by different ISPs (20 devices) and manufacturers (no hidden study)
- Additionally: Tests of some devices from German “free market”
- Each router was tested in supplied condition with factory defaults

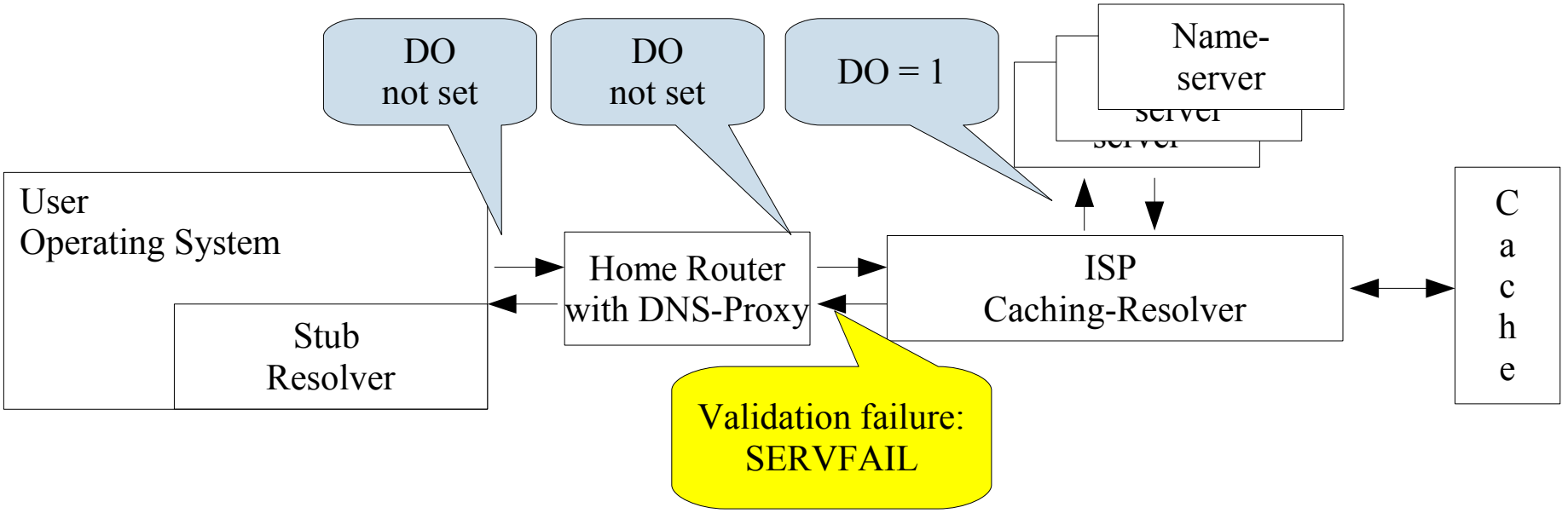
Content

- Motivation / BSI activities
- Previous Tests
- Objectives
- Test Methodology / Testbed
- Reviewed Devices
- Results
- Conclusions



Test scenarios
1. Proxy DNS queries

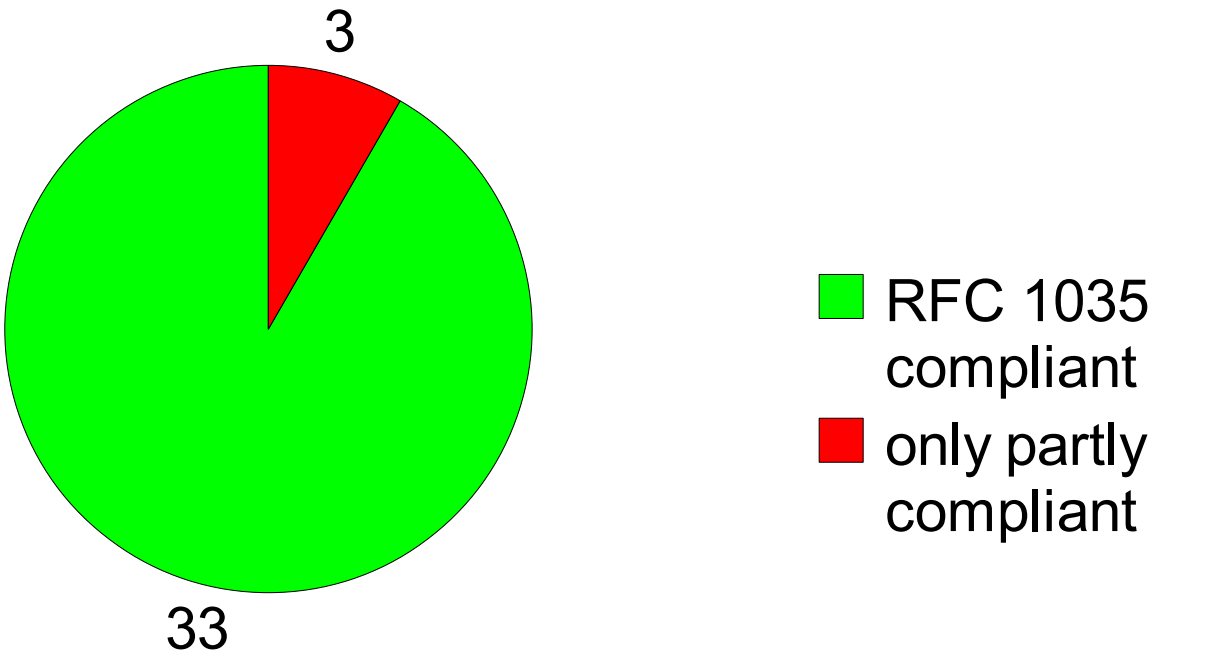
- DNSSEC-validation by caching-resolver of ISP
  - → Client queries DNS-proxy of home router without setting of DNSSEC-bits
  - → DNS-caching-resolver answers with SERVFAIL or NXDOMAIN if validation fails
  - → No modification of hard- and software from user needed



Federal Office
for Information Security

Test Results
DNS-proxy: RFC-1035 Compliance

Can the router proxy standard DNS queries over UDP ?



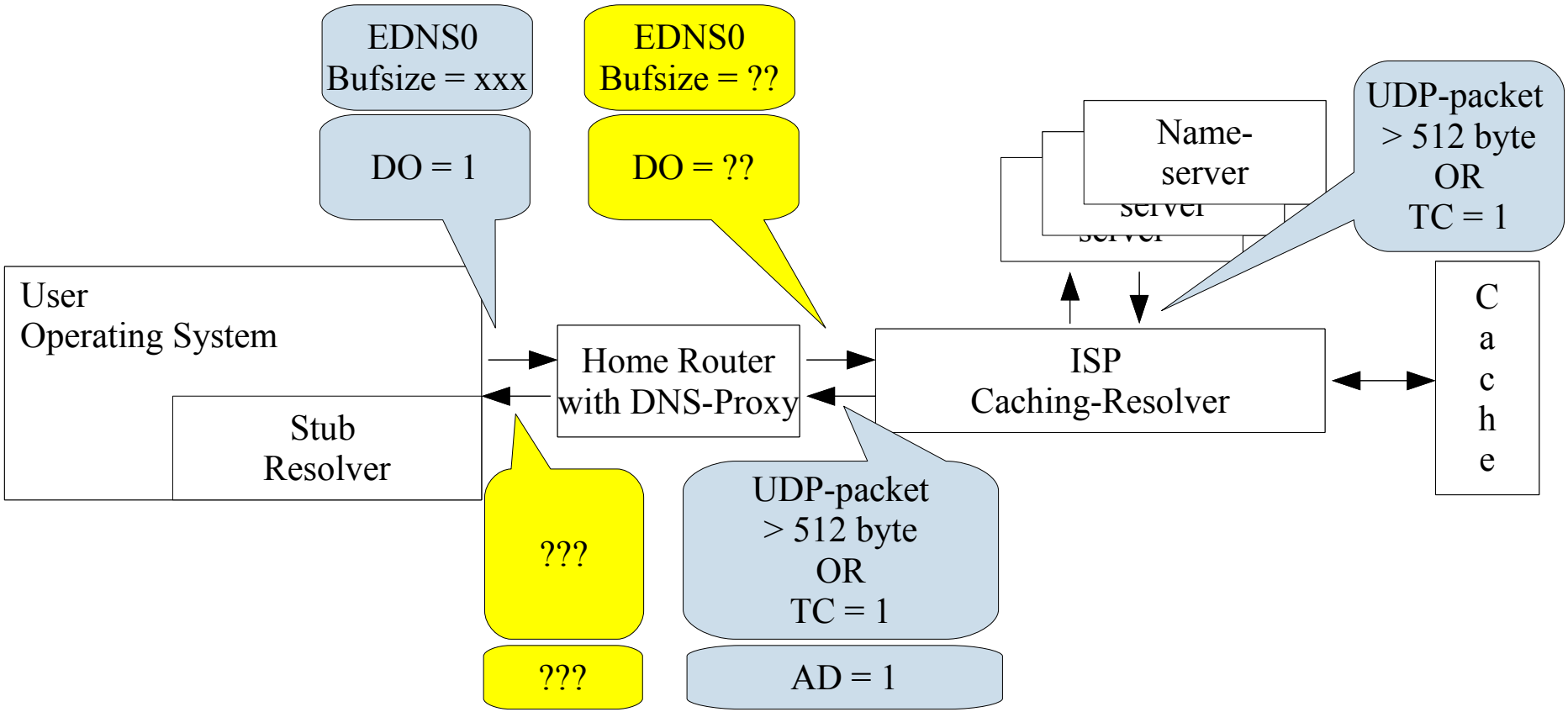
- 3 devices could not handle all Resource Records (RR) types
- Excluded from further proxy-tests

Test scenarios
2. Proxy DNSSEC queries

- DNSSEC-validation by caching-resolver of ISP

  → Client is DNSSEC-aware and sets DO

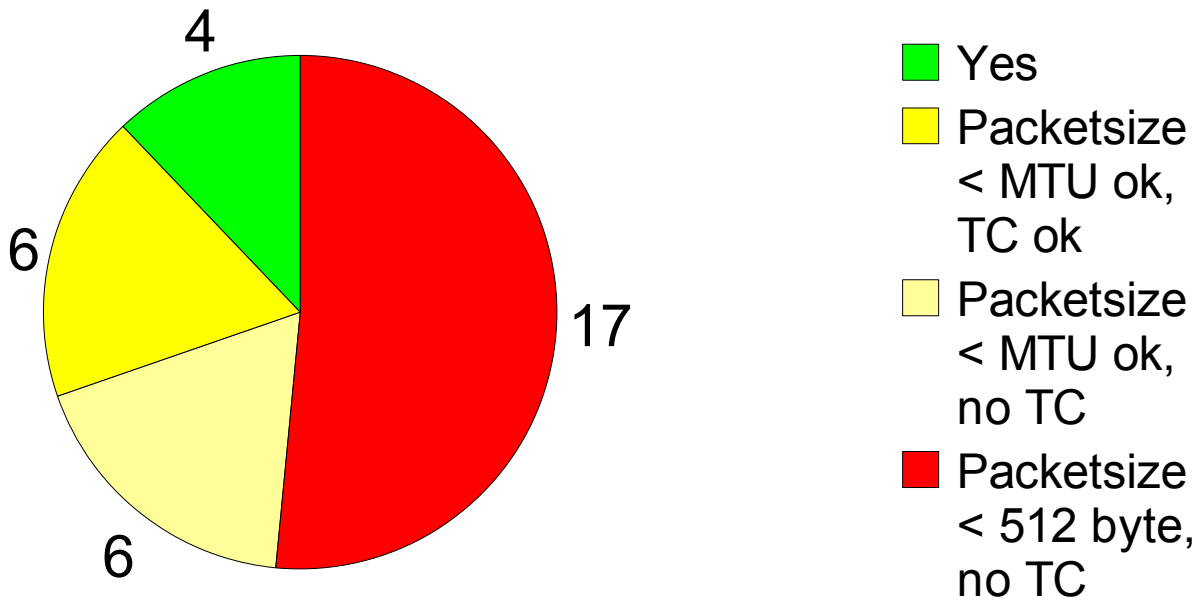
  → DNS-caching-resolver delivers signatures and sets AD in case of successfully validated domain



Federal Office
for Information Security

Test Results
EDNS0-Support

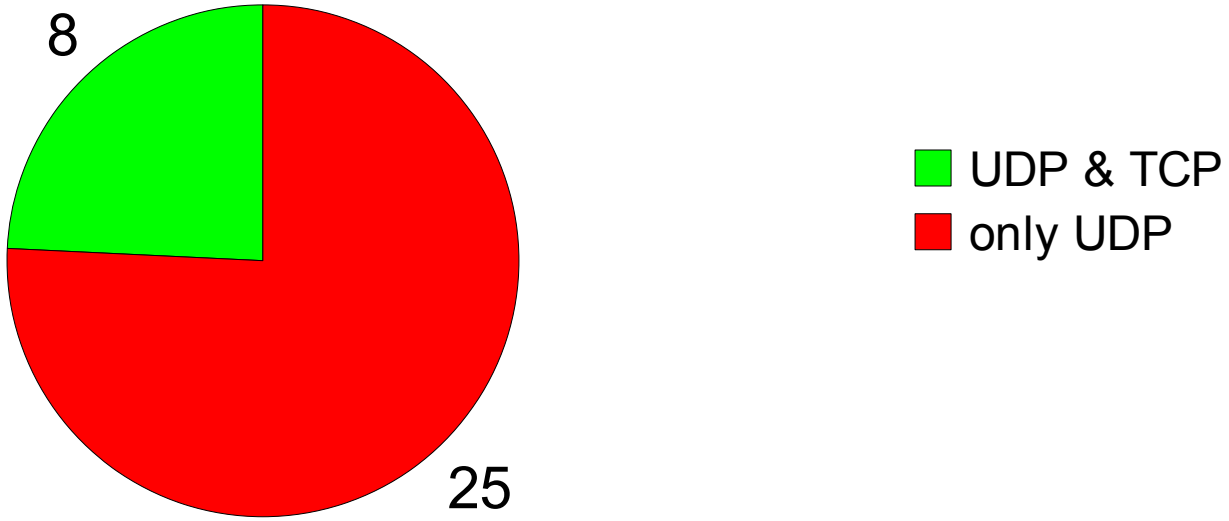
Can the router proxy DNS queries over UDP using EDNS0 ?



- Main problems:
  - Packets were discarded
  - TC was not set or passed through

Test Results
TCP-Support

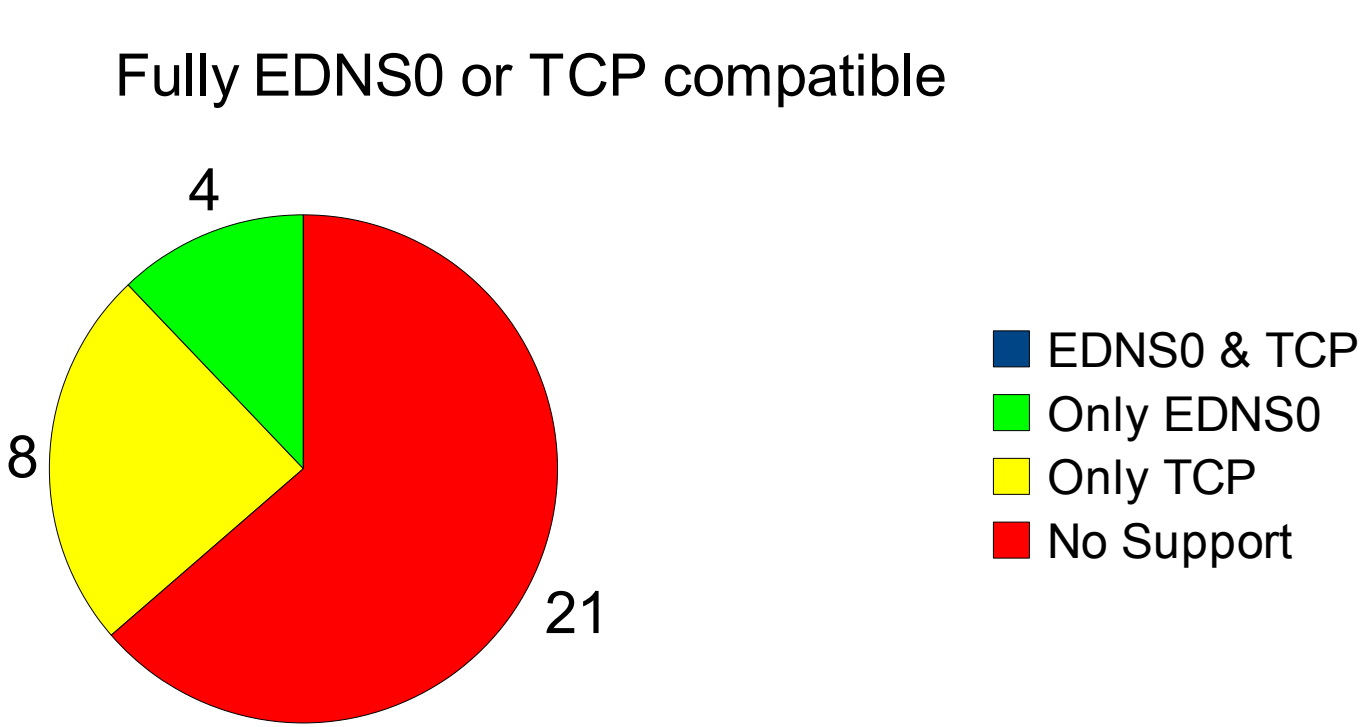
Does the router accept DNS queries over TCP?



- Only 8 DNS-proxies accept DNS queries over TCP

Federal Office
for Information Security

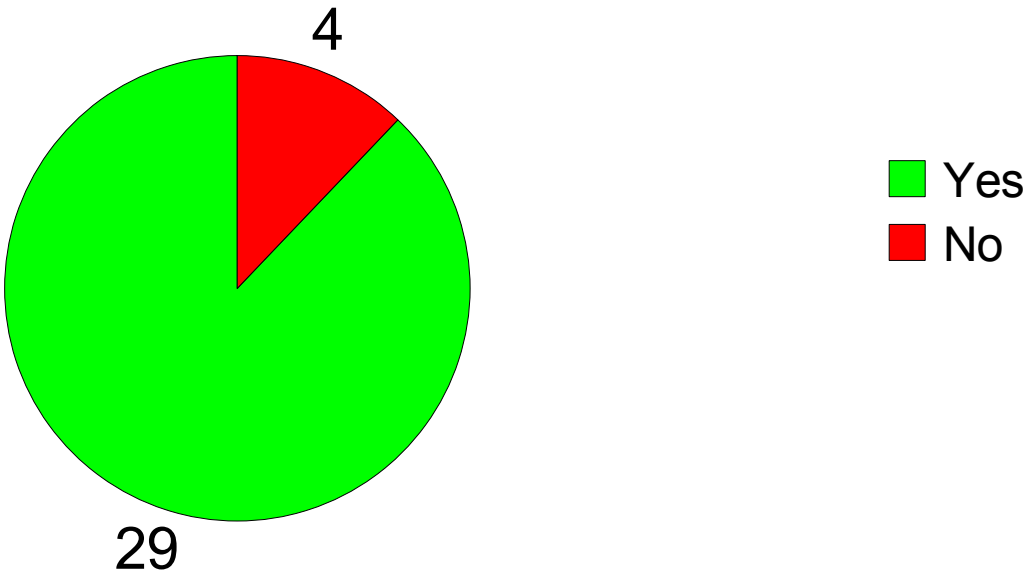
Test Results
EDNS0 or TCP Compatibility



- No integrated DNS-proxy supported both EDNS0 and TCP

Test Results
DNSSEC-Flags Compatibility

Can the router proxy DNS(SEC) queries
that set DNSSEC-related flags ?

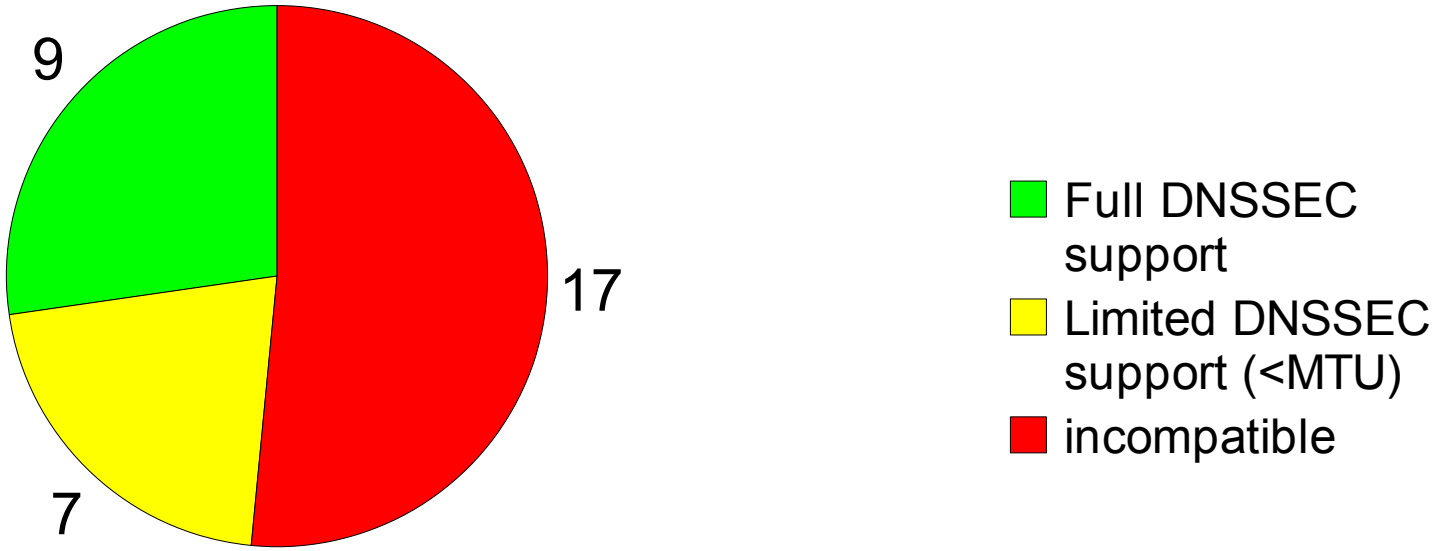


- Most devices can handle DNSSEC-flags
- 3 devices modify DNSSEC-flags
- 1 device returns „Connection Timeout“ with AD or CD set

Federal Office
for Information Security

Test Results
DNS-Proxy DNSSEC Support

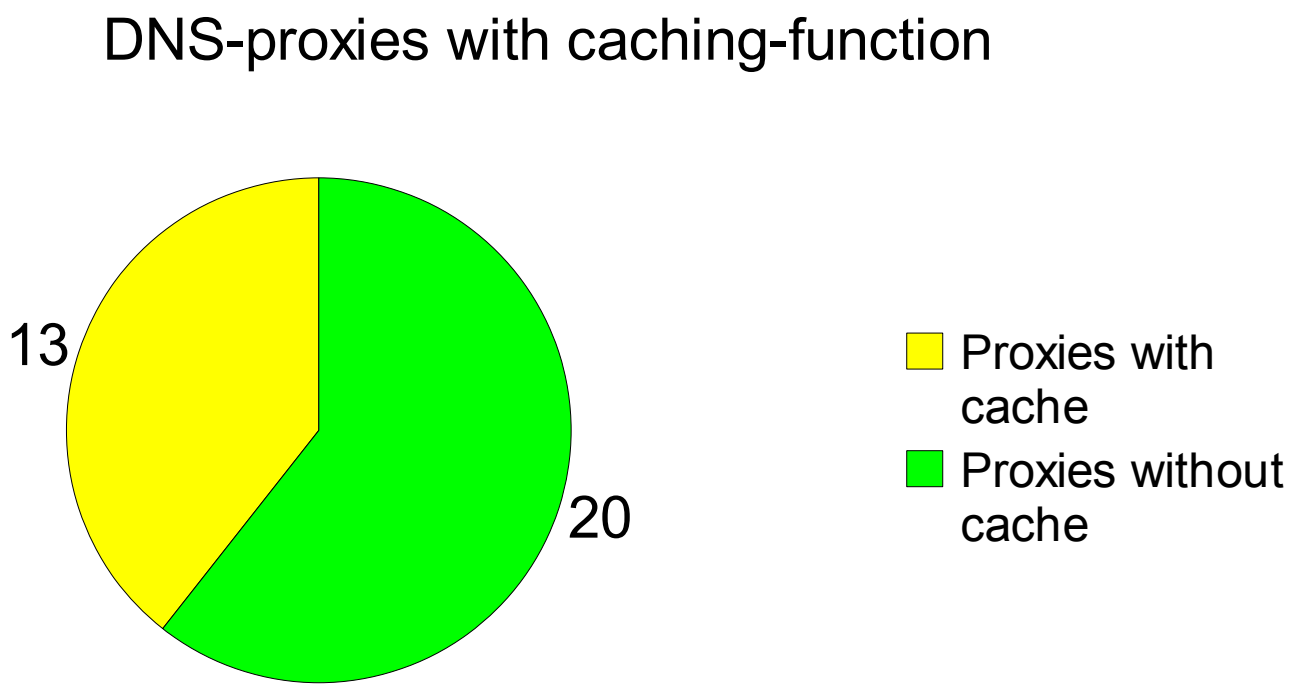
Overall DNSSEC-compatibility of DNS-proxy



- Only 9 of 33 tested DNS-proxy implementations fully support DNSSEC
- Additionally, 7 devices have limited support (Answering packet size < MTU-size)

Federal Office
for Information Security

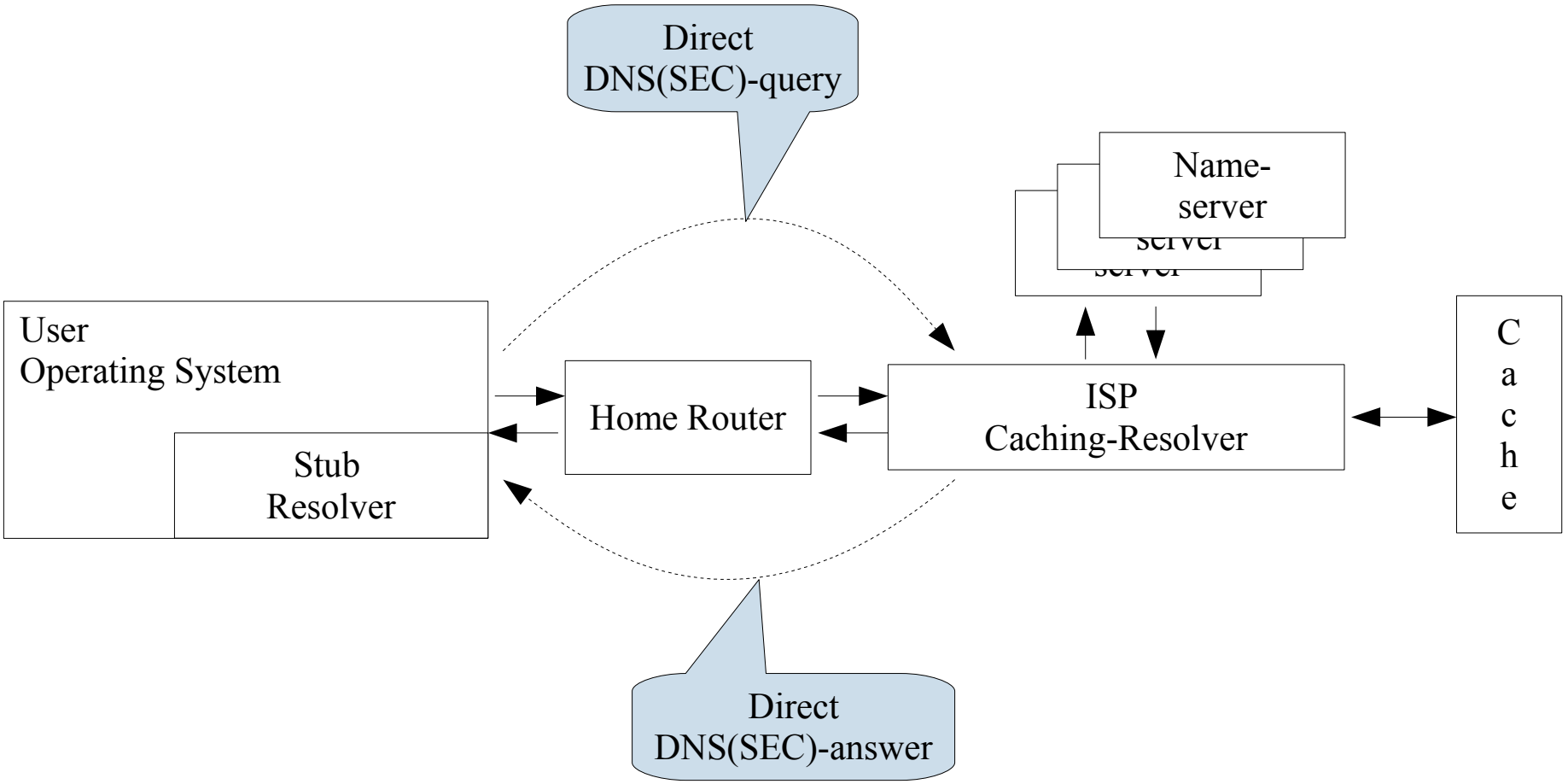
Test Results
Proxy & Caching



- All proxies with caching-function had problems to distinguish between DNSSEC and non-DNSSEC queries. That leads to problems in mixed environments.

Test scenarios
3. Route DNS(SEC)-Queries

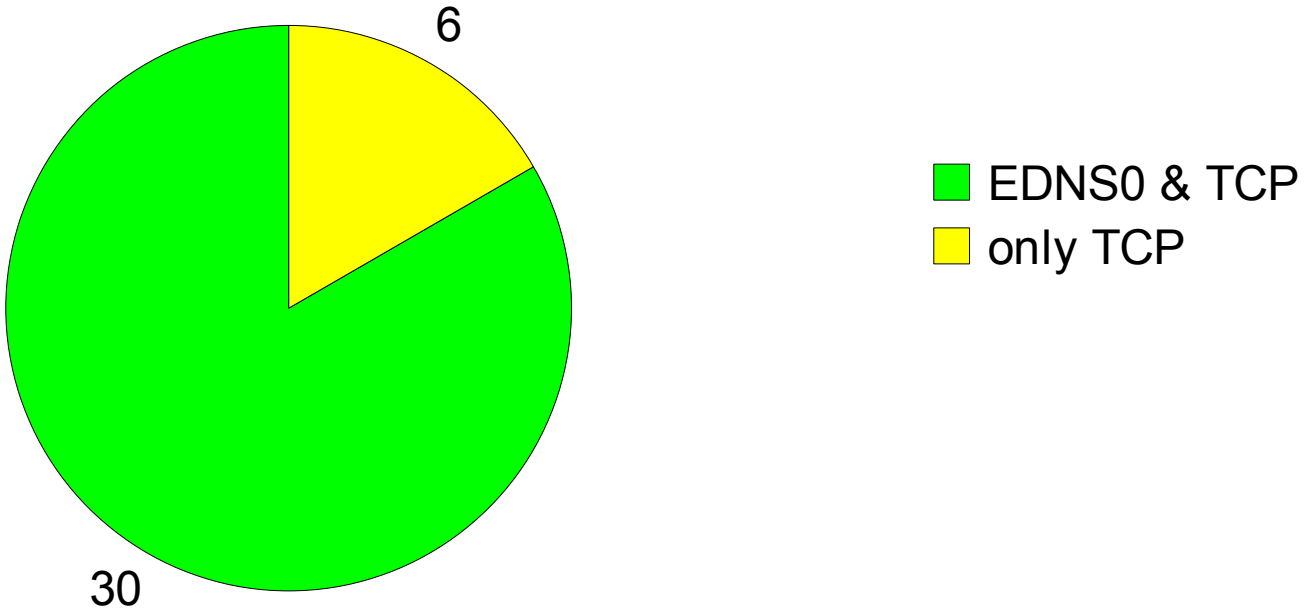
- Direct DNSSEC-queries to ISP caching-resolver



Federal Office
for Information Security

Test Results
Bypass of DNS Proxy

Can the router route DNS(SEC) queries
with set of DNSEC-related flags and use of EDNS0?



- All tested devices fully support DNSSEC when the implemented DNS-proxy is bypassed
- 6 of the tested devices only via TCP-fallback, due to routing limitations with fragmented packets

Federal Office
for Information Security

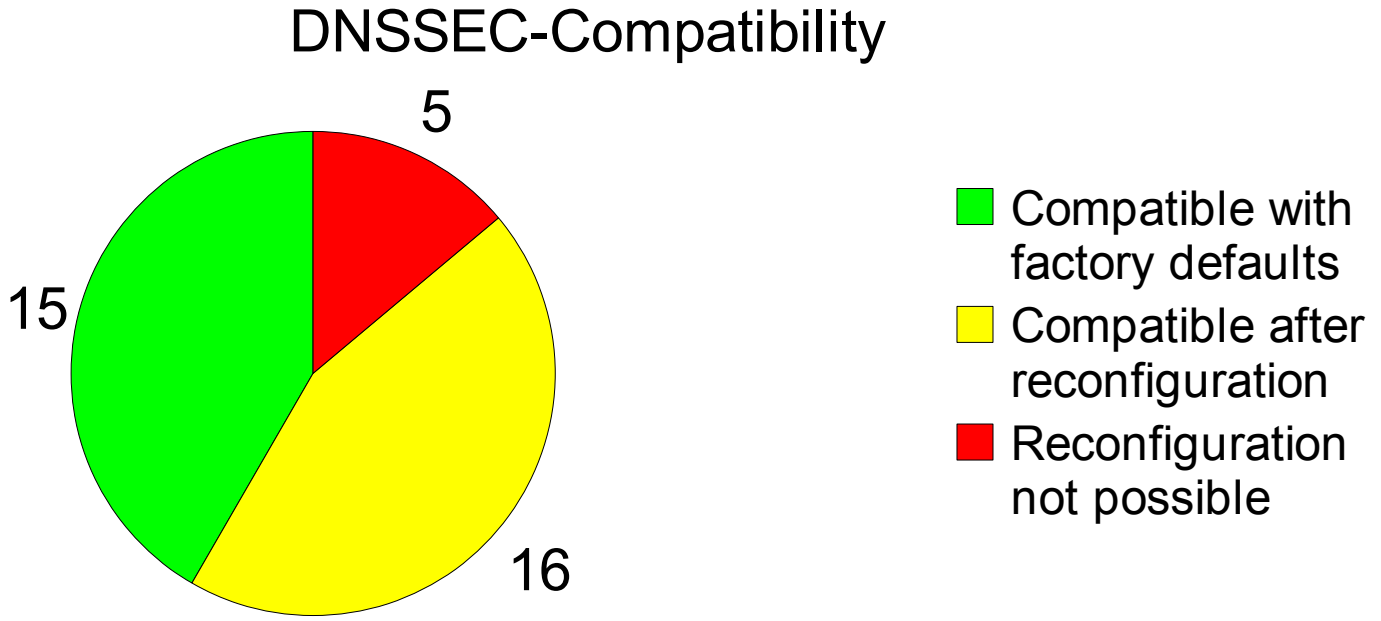
Test Results
Configuration of DHCP DNS parameters

- With LAN DHCP defaults many (30) devices supply themselves as the local DNS
- Some (5) devices supply the ISP's DNS address, inherited from WAN link
- Unfortunately 6 devices with a DNSSEC incompatible DNS-Proxy have no DHCP configuration option

	Manual configuration of DHCP DNS parameters possible	Manual configuration of DHCP DNS parametes **not** possible
Integrated DNS-proxy DNSSEC-capable	9 (Default proxy: 9) (Default ISP: 0)	0
Integrated DNS-proxy with limited DNSSEC-support	7 (Default proxy: 5) (Default ISP: 2)	0
No DNSSEC-support by integrated DNS-proxy	11 (Default proxy:10) (Default ISP: 1)	6 (Default proxy: 5) (Default ISP: 1)
Incomplete DNS-proxy implementation	2 (Default proxy:1) (Default ISP: 1)	1 (no DHCP)

Federal Office
for Information Security

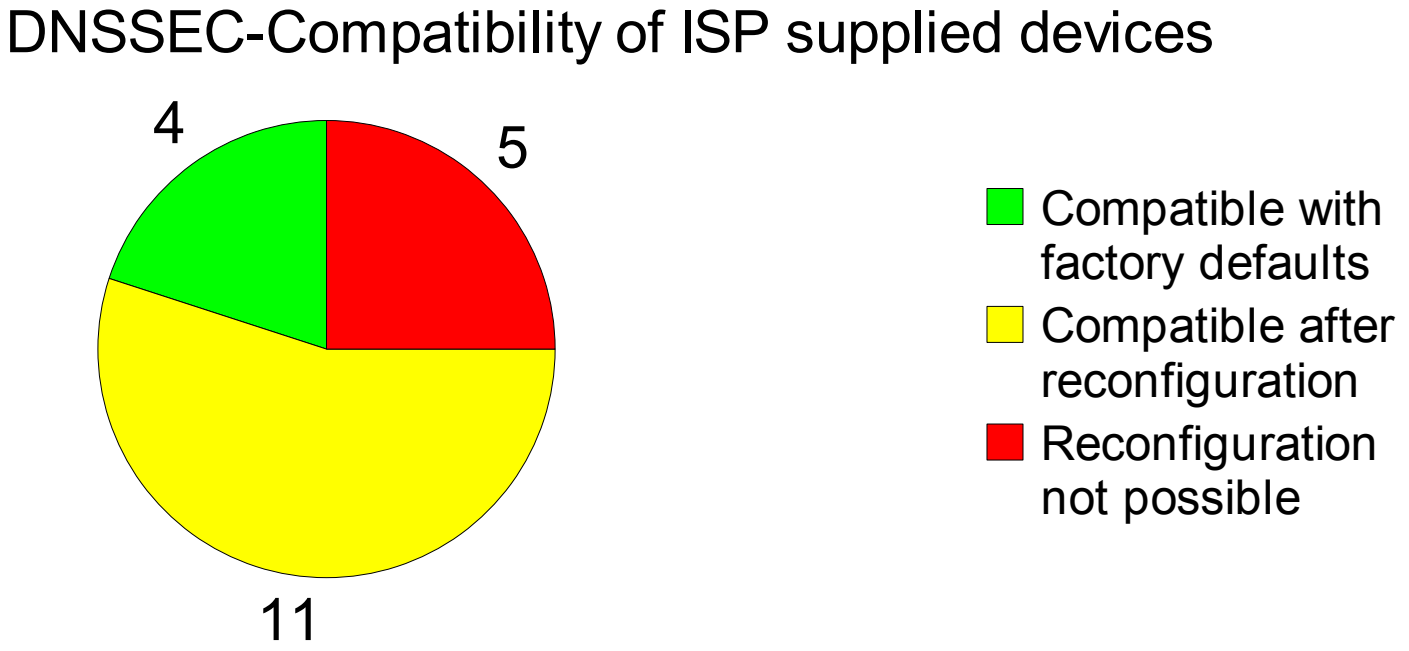
Test Results
DNSSEC-Compatibility



- 15 devices are DNSSEC-compatible with factory defaults, due to the fact that either the implemented DNS-proxy fully supports DNSSEC or they provide the ISP's DNS-server settings via DHCP
- 16 devices can be reconfigured to provide the ISP's DNS-server settings via DHCP
- 5 devices lack reconfigurable DHCP DNS parameters

Federal Office
for Information Security

Test Results
DNSSEC-Compatibility (ISP devices only)



- 4 devices are DNSSEC-compatible with factory defaults, due to the fact that either the implemented DNS-proxy fully supports DNSSEC or they provide the ISP's DNS-server settings via DHCP
- 11 devices can be reconfigured to provide the ISP's DNS-server settings via DHCP
- 5 devices lack reconfigurable DHCP DNS parameters

Conclusions

- Non DNSSEC-aware client operating system:
  - No compatibility issues
- DNSSEC-aware client operating system:
  - 15 devices can be used out of the box
  - 16 devices can be reconfigured to be DNSSEC compatible
  - 5 devices lack reconfigurable DHCP DNS parameters
    → individual reconfiguration of DNS settings on each client
- Compatibility issues mostly due to missing EDNS0- and TCP-support of built-in DNS-proxy
  - Only 9 of 36 devices have full DNSSEC proxy support
  - 7 devices have limited DNSSEC proxy support
    (packet size < MTU)

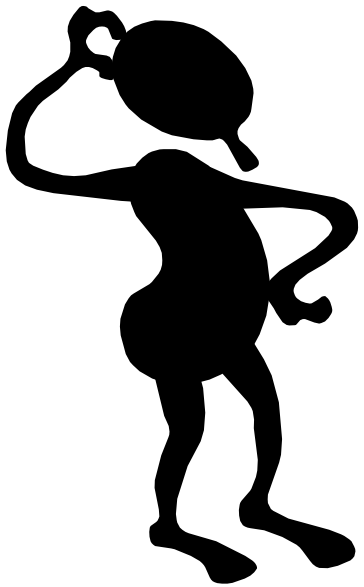
Comparison with .se und .uk studies

	.se	.uk	.de
EDNS0 compatible	3/10	4/22	4/33
TCP-support	3/10	1/22	8/33
DNSSEC-flag support	7/10	16/22	29/33
DNSSEC compatible as router	-	24/24	36/36
DNSSEC compatible with factory settings	3/12 (25%)	6/24 (25%)	15/36 (42%)
DNSSEC compatible after reconfiguration	-	9/24 (38%)	16/36 (44%)

Perspective

- Results were communicated to Manufacturer's and ISP's
- Positive feedback
- One manufacturer already released beta-firmware with improvements
- Others want to adopt recommendations at least in future products

Thanks for your attention!



Questions?

Federal Office
for Information Security

Contact

Federal Office for
Information Security (BSI)

Thorsten Dietrich
Godesberger Allee 185 - 189
53175 Bonn
Germany

thorsten.dietrich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de