DNSSEC bei Netzzugangsgeräten

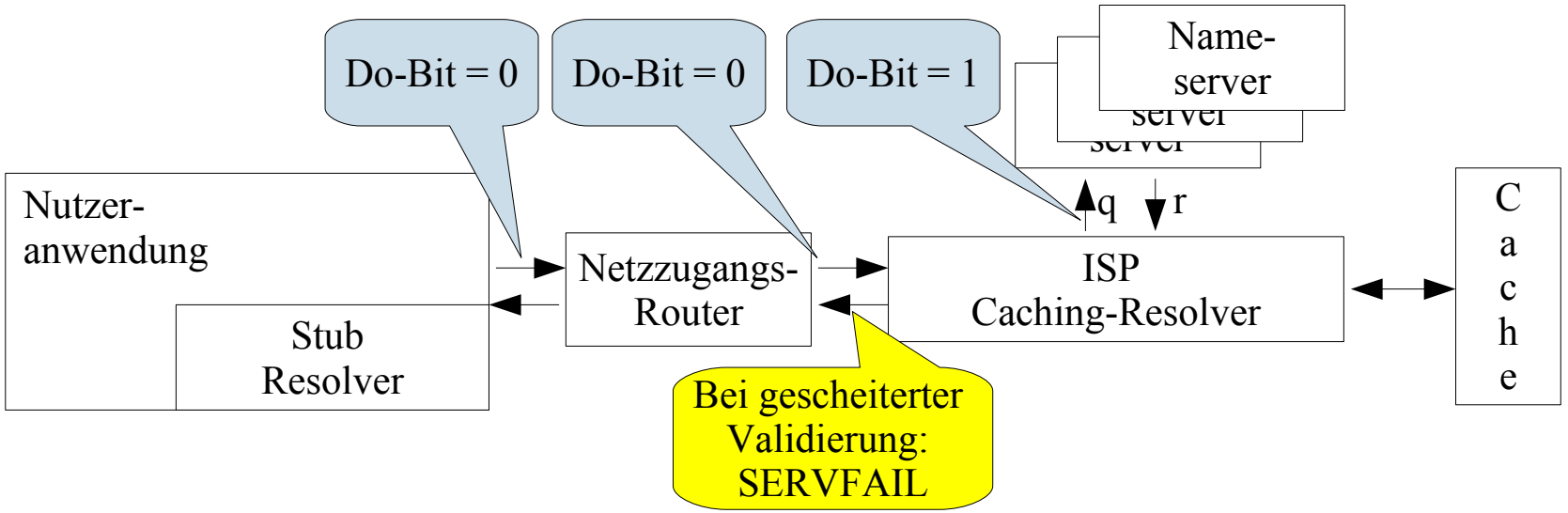
Thorsten Dietrich

Bundesamt für Sicherheit in der Informationstechnik

DNSSEC-Testbed für Deutschland / 02. Juli 2009

Motivation / Anforderungen

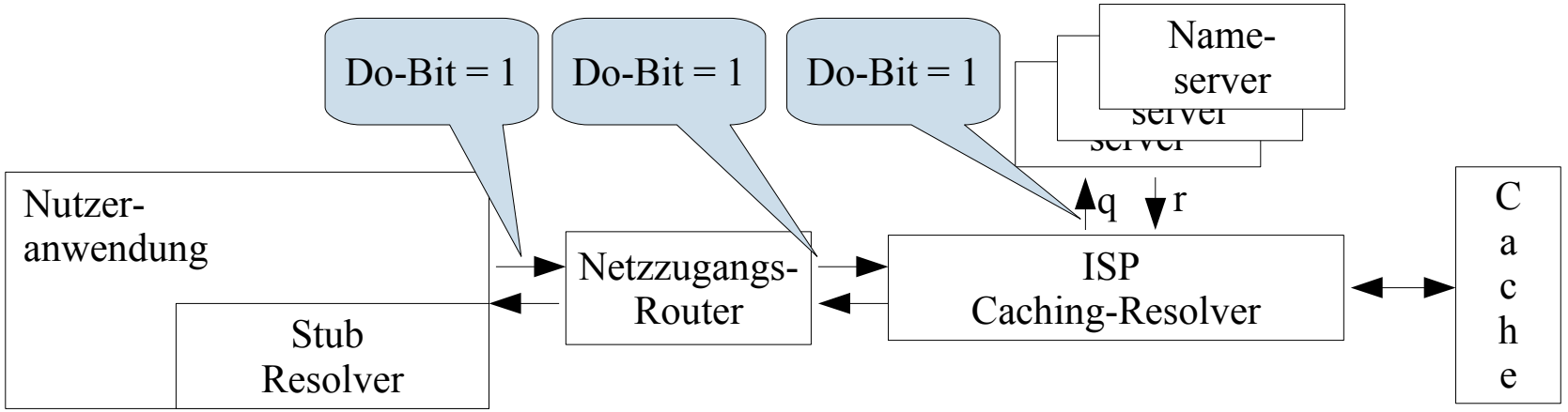
- Zunächst: DNSSEC-Validierung durch Caching-Resolver des ISPs
  - → Client stellt unverändert DNS-Abfragen
  - → DNS-Caching-Resolver liefert bei fehlgeschlagener Validierung SERVFAIL oder NXDOMAIN zurück
  - → Keine Veränderung an Hard- und Software des Kunden notwendig



Motivation / Anforderungen (cont.)

ABER:

- DNSSEC-Validierungskette sollte im Idealfall durchgängig bis zur Client-Applikation bestehen



→ Unterstützung durch Hard- und Software des Endanwenders erforderlich

DNSSEC-Unterstützung auf Clientseite (Betriebssystem / Software)

- Unterstützung durch Betriebssysteme wächst

Betriebssystem		DNSSEC-Support
Microsoft	Microsoft ≤ Vista	Nein
	Windows 7 / Server 2008	Ja („Non Validating Security-Aware Stub-Resolver“)
Linux, BSD, Solaris, Mac OS X	Standard-Distributionen	Nein
	DNSSEC validation libraries	Ja
	Firefox / Thunderbird patches	Ja
	FTP-Client patches	Ja
	IPSec client patches	Ja
	Open SSH patches	Ja

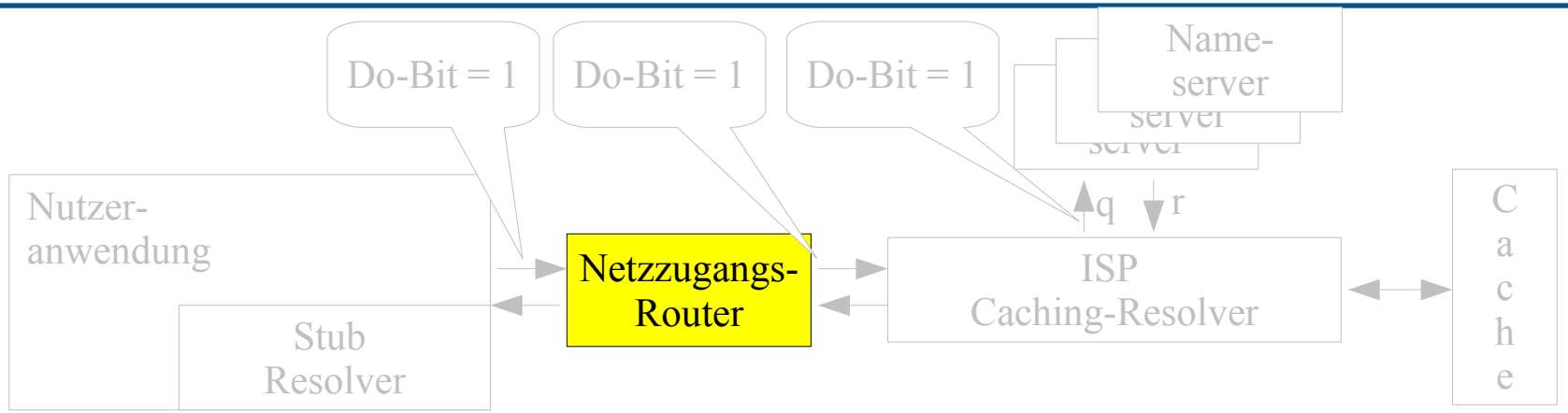
DNSSEC und Windows 7

Security -Aware	DNSEC-OK (DO)	Validating	Checking-Disabled (CD)	Authentic-Data Bit (AD)
-	-	-	-	Wird nicht ausgewertet
√	√	-	-	Wird ausgewertet
√	√	√	-	Validiert selbst
√	√	√	√	Validiert selbst

Windows 7, „Non-Validating, Security-Aware Stub Resolver“

- In Windows 7 kann zonenabhängig die Validierung durch einen externen Resolver aktiviert werden.
- Die Kommunikation mit dem externen Resolver kann über IPSec abgesichert werden

DNSSEC-Unterstützung auf Clientseite (Hardware)



- Router häufig mit DNS-Proxy Funktionalität

  → Router muss zukünftig DNSSEC-Anfragen der Endgeräte unterstützen

  → Wunsch: Optionale Validierung durch Router

- Untersuchungen durch .SE (Feb. 2008) sowie durch Nominet / CORE competence (Sep. 2008) haben gezeigt, dass hier Probleme vorhanden sind

DNSSEC-Unterstützung durch Router
Ergebnisse bisheriger Untersuchungen

nominet®

CORE competence

Test Report:
DNSSEC Impact on Broadband Routers and Firewalls
September, 2008

Ray Bellis
Nominet UK
ray.bellis@nominet.org.uk

Lisa Phifer
Core Competence
lisa@corecom.com

Executive Summary

To assess potential impact of DNSSEC on broadband consumers, we tested two dozen residential Internet router and SOHO firewall devices commonly used with broadband services. In summary, we found that:

- All 24 units could **route** DNSSEC queries addressed to upstream resolvers (referred to herein as route mode) without size limitations.
- 22 units could **proxy** DNS queries addressed directly to them (referred to herein as proxy mode), with varying degrees of success.
- 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses that effectively prevented DNSSEC use in proxy mode.
- 16 of 22 DNS proxies could successfully pass DNSSEC queries and return validated responses of some size.
- 18 DNS proxies limited responses over UDP to either 512 bytes or a size constrained by the MTU. Only 4 could return responses over UDP up to 4096 bytes, while just 1 could proxy DNS over TCP (no size limit). Such limits can interfere with returning longer DNSSEC responses.
- When deployed with factory defaults, 15 units are likely to be used as DNS proxies, while 3 always route DNS queries. The rest (6) vary over time, preferring to route DNS after being connected to a WAN.

DNSSEC-Unterstützung durch Router Ergebnisse bisheriger Untersuchungen (cont.)

- Verschiedenartige Probleme vorhanden
- Nur 6 der 24 getesteten Geräte funktionierten „out-of-the-box“
- Hersteller wurden auf Ergebnis hingewiesen
- Als Folge des Studienergebnisses wurde der Internet-Draft „DNS Proxy Implementation Guidelines“ erstellt
- Daher Studien heute ggf. „veraltet“
- Getestete Produkte mehrheitlich für den schwedischen bzw. britischen Markt relevant

  → Untersuchung der Situation in Deutschland erforderlich

DNSSEC-Unterstützung durch Router
Zielsetzung der geplanten Studie

- Identifizierung der marktüblichen Netzzugangsrouter
- Untersuchung auf erforderliche DNSSEC-Eigenschaften

<u>Weiterhin:</u>

- Lebensdauer der Router
- Remote-Update Möglichkeiten
- Gespräche mit Herstellern
  - Studienergebnisse
  - Implementierung validierender Caching-Resolver
- IPv6

Bitte um Unterstützung

- Welche Router werden den Kunden angeboten?
- Gibt es Erfahrungen bzgl. des Lebenszyklus der Geräte?
- Können evtl. Testgeräte zur Verfügung gestellt werden?

Fragen ?

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Thorsten Dietrich
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-9582-5947
Fax: +49 (0)22899-10-9582-5947

Thorsten.Dietrich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de