Secure DNS
Stand und Perspektiven

Dipl.-Inform. Peter Koch
Technische Fakultät
Universität Bielefeld
pk@TechFak.Uni-Bielefeld.DE

Was Sie erwartet . . .

- Einleitung und Begriffsklärung
- Übersicht DNSSEC
- Operationelle Gegenwart
- Ausblick & Diskussion

Ein wenig Formalia

- DNS: hierarchisch, verteilt, repliziert
- Domain vs. Zone
- Verschiedene *Resource Record*-Typen (`A`, `SOA`, ...)
- *Resource Record* vs. *Resource Record Set* (RRSet)
- Die Beteiligten: Server, Resolver (*stub* und *full*), Caches
- Weitgehend ausgereifte Technik

Gift für den Cache

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr aa rd ra; Ques: 1, Ans: 2, Auth: 1, Addit: 3
;; QUESTIONS:
;;      malicio.us, type = MX, class = IN

;; ANSWERS:
malicio.us.         172800  MX      100 mail.malicio.us.
malicio.us.         172800  MX      200 www.opfer.xy.

;; AUTHORITY RECORDS:
malicio.us.         172800  NS      dns.malicio.us.

;; ADDITIONAL RECORDS:
mail.malicio.us.    21600   A       192.168.42.17
www.opfer.xy.       172800  A       192.168.42.18
dns.malicio.us.     21600   A       192.168.42.22
```

Anforderungen an ein sicheres DNS

- Quellenauthentisierung – *data origin authentication*
- Datenintegrität
- In Ausnahmefällen: Authentisierung der Kommunikationspartner
- *Keine* Vertraulichkeit der Anfragen und Antworten

Bekannte Lösungsansätze . . .

- IPSec
- TLS
- . . . scheiden aus

Erweiterter Anforderungskatalog

- Skalierbarkeit
- Weltweite Einsatzmöglichkeit
- „Leichtgewicht“

Secure DNS mit Public Key-Technologie

- DNS-Zonen sind die Datenquellen
- Schlüssel(paare) für diese Quellen (Zonen)
- *Public Key Infrastructure* im DNS selbst
- $\rightsquigarrow$ „neue“ *Resource Record*-Typen (`KEY`, `SIG`, `NXT`)

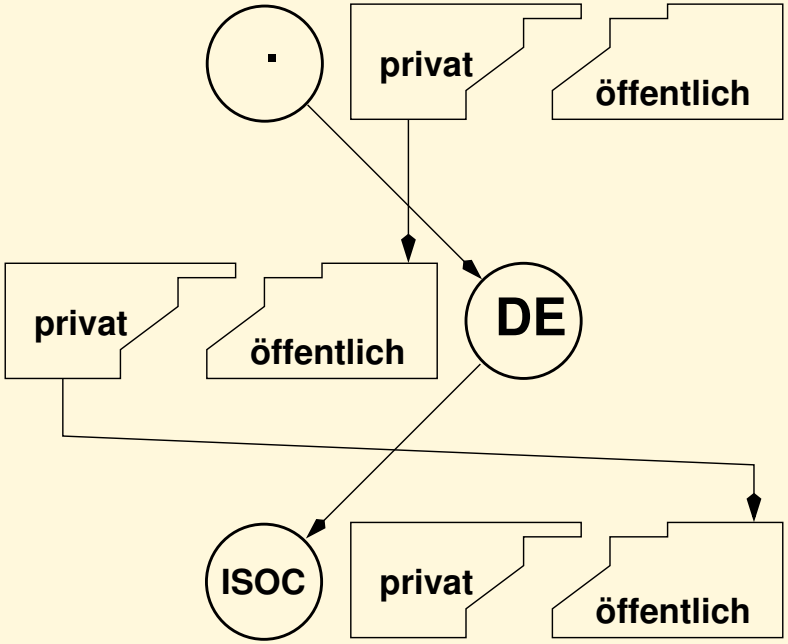
Der Schlüssel zu Secure DNS: KEY-RR

```
ISOC.DE.   172800  IN   KEY     256 (  ; A+C, zone key
                                3      ; DNSSEC
                                1      ; RSA/MD5
                                AQOq1567hKcaj2vy/rex6uAQx/bF9ssipzW7
                                [...]
                                TVBFVtcN0LSlunccFP8Dq9RlOk0teC3xr3mQ
                                IlmK/uuvXboMc6qH5GtV ) ; key id = 58475
```

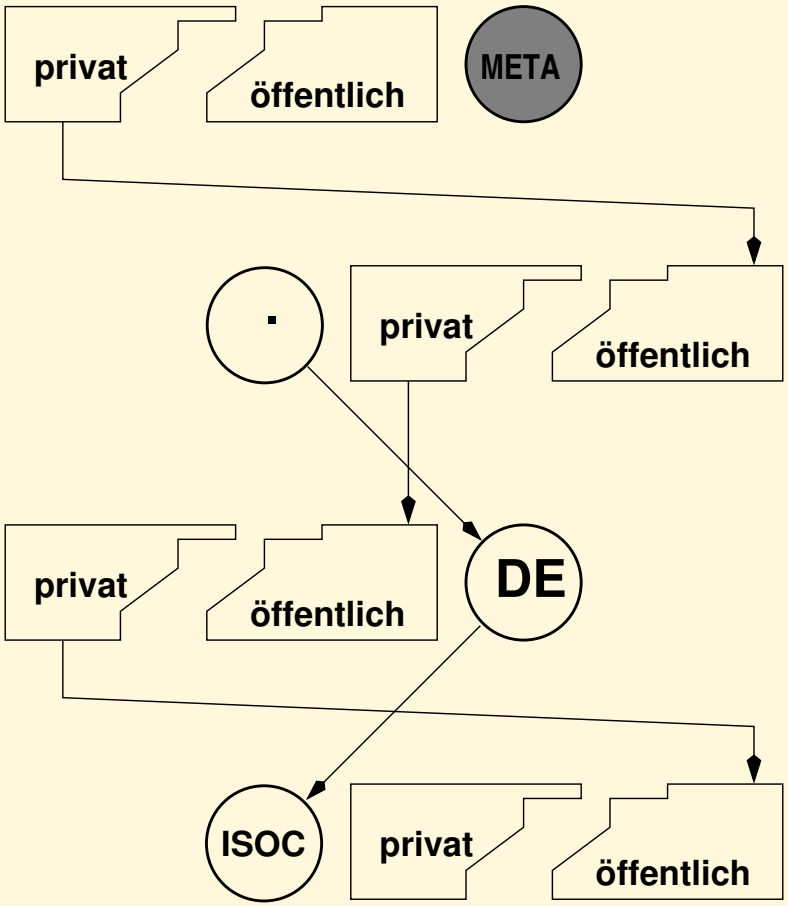
SIG-RR bürgt

```
www.ISOC.DE. 172800 IN A    193.98.9.108
             172800 IN SIG  A 1 (          ; A-RR, RSA/MD5
                            3             ; labels
                            172800        ; original TTL
                            20010501152545 ; sig expiration
                            20010401152545 ; sig inception
                            58475         ; key id
                            ISOC.DE.      ; signer's name
                            mlpZnSYR1syNphbLnhLlCZBHNs6wDAG1+X1W
                            [...]
                            fcZaKYkhN0mVlZLtW+0pdNvxdSiBt4DUhRdh
                            X3by/78pZFXyZfqRtw== )
```

Zertifizierungskette



. . . mit Wurzelbehandlung



Arbeit für die Resolver

- Verifikation der `SIG`naturen
- Ermittlung der Schlüssel
- Verfolgung der Delegations- und Zertifizierungskette
- Verifikation auch für *additional data*
- $\leadsto$ Last, Cache-Größe, Latenz

Kanonische Sortierreihenfolge


```
SOA, NS,        TXT, SIG, NXT        A, SIG, NXT
MX,RP,
KEY, SIG, NXT
```

Von der Kunst, „Nein“ zu sagen: NXT-RR

- Negative Antworten
  - RRSet existiert nicht
  - Domainname existiert nicht (NXDOMAIN)
- `www.ISOC.DE.  3600  IN NXT  ISOC.DE. A SIG NXT`
- Ein NXT-RR pro Name (*owner*) in der Zone
- Begleitet von je einer SIGnatur

Zwischenbilanz

- Secure DNS ist seit einiger Zeit spezifiziert
- Architektur ist überschaubar
- Erste Produkte sind verfügbar (BIND 9.1.2)

Wo muß ich unterschreiben?

- Politische und administrative Probleme
- Protokollbezogene Unklarheiten
- Operationelle Herausforderungen

Spitzen-Probleme

- Vorsicht bei Änderungen an der Root-Zone
- Behandlung des *Root*- oder *Meta-Root*-Schlüssels
- Volumenprobleme einiger TLDs
- Policies der Registries
- Neue Monopole?
- Bedeutung der `SIG`naturen

So viele Standards . . .

- DNSSEC offen hinsichtlich der kryptographischen Verfahren
- IETF: *unencumbered technology*
- RFC 2535: DSA *muß*, RSA/MD5 *soll*
- Demnächst: RSA/SHA-1 *muß*, RSA/MD5 *soll nicht*
- Weitere Verfahren sind bzw. werden spezifiziert (ECC)

NXT, NO or neither?

- NXT-RRs und SIGnaturen vergrößern die Zone
- NXT ermöglicht Traversierung der Zone
- NO ist aufwendiger und bisher nicht implementiert
- Zwei Lösungen im Feld erhöhen die Komplexität zusätzlich
- *Wird authentisiertes Dementi überhaupt benötigt?*

Paketwachstum

- UDP-DNS-Paket trägt höchstens 512 Byte Nutzdaten
- Satz der Root-Nameserver in Zahl und Namen optimiert
- Kein Platz für `SIG`-RRs für „.“
- $\rightsquigarrow$ EDNS mit größeren UDP-Datenpaketen

Bremsende Dynamik

- DNS *Dynamic Update* ändert Zoneninhalte
- Authentisierung/Autorisierung der Updates selbst
- Absicherung der eingefügten *RRSet*s
- Aktualisierung der `NXT`-RRs
- $\leadsto$ Zonen trennen

Die Letzte Meile

- Resolver sind nicht intelligent genug (`libresolv`)
- $\rightsquigarrow$ Zentraler DNSSEC-fähiger Resolver
- Bedarfsgesteuerte Verifikation
- Nachfrage durch Applikationen?
- API?

Opt-In

- Verständnis „alter “ Software für die neuen RR-Typen
  - rein syntaktisch
  - in ihrer Bedeutung in der Nachricht
- Probleme mit der Nachrichtengröße
- Entwurf: `DNSSEC OK` Bit im EDNS0-`OPT`-RR
- Problem: Zwischenstationen

Schlüssel in Kinderhände?

- Wo $\texttt{SIG}_{parent}(\texttt{KEY}_{child})$ speichern?
- Namensraum $\rightsquigarrow$ delegierte Zone
- Problem mit *Key-Rollover*
- Entwurf: `SIG`natur in der delegierenden Zone
- Registry-Policies, Lebensdauern
- Kein *NULL-Key*

Beteiligte Organisationen

- RSSAC $\rightsquigarrow$ ICANN
- CENTR
- RIPE, RIPE NCC
- Registries: `SE`, `NL`, `DE`, ...
- Neue gTLDs?
- IETF *dnsext*, *dnsop*

Zusammenfassung

- Secure DNS ist ein Lösungsansatz für ein ernstes Problem
- Implementierungen sind verfügbar
- Leider noch kaum praktische Erfahrungen
- *Henne und Ei*-Problem
- Secure DNS erhöht die Komplexität
  - für die Infrastruktur
  - für die Zonenverwalter
  - für die Registries
- Produktionsreife nicht vor 2002
- $\leadsto$ Überarbeitung der Spezifikation

Wunschzettel

- Werkzeuge
- Dokumentation
  - der Technik
  - der Policies
- Flächendeckende Testbeds
- Nachfrage durch Applikationen
- Koordination und Weitsicht (IPv6, IDN, . . .)