Sicherheitserweiterungen im DNS nach RFC 2535

Referentin: Ursula Loch

Gliederung

1) Einordnung des DNS in das OSI-Schichtenmodell
2) Überblick Erweiterungen
3) SIG RR – Signature Resource Record
4) KEY RR – KEY Resource Record
5) Zonenstatus
6) NXT RR – Next Resource Record
7) TTL, CNAMEs und Delegationspunkte
8) Sichere Namensauflösung
9) Server und Resolver Konformität
10) Probleme von DNSSec

1) Einordnung des DNS in das OSI-Schichtenmodell

2) Überblick Erweiterungen

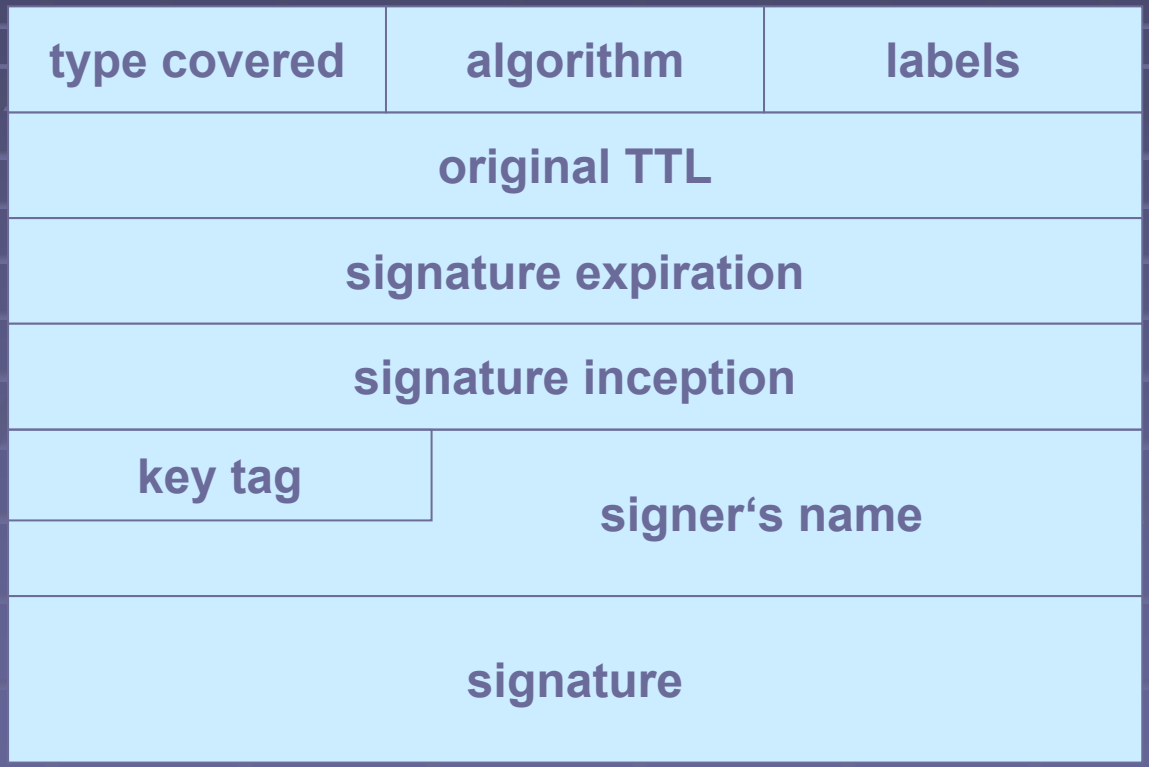
- DNSSec Erweiterungen unterstützen drei Dienste:
  - Verteilung der Schlüssel
  - Authentifizierung der Herkunft der Daten
  - Authentifizierung von Transaktionen und Anfragen
- Besondere Berücksichtigung von TTL, CNAMEs und Delegationspunkten

3) SIG RR – Signature Resource Record

- SIG RR
  - sichert Integrität der Daten
  - authentisiert RR-Set
- digitale Signatur enthält:
  - kryptographischen Hashwert
  - Daten über den Ersteller der Signatur
  - angewendetes Verfahren
  - Gültigkeitintervall der Signatur
- Signatur wird an eine Antwort auf eine DNS-Anfrage als zusätzliche Information angehängt

3) SIG RR – Signature Resource Record

- RDATA eines SIG RRs:



3) SIG RR – Signature Resource Record

- Authentifizierung einer Transaktion:
  - Einfügen einer spezieller SIG RR ans Ende einer Antwort
  - Transaktions SIG RR wird mittels Server Host Key und nicht mittels Zone Key signiert
  - Verifikation des Transaktions SIG RR durch Resolver zeigt, dass
    - Anfrage und Antwort bei der Übermittlung nicht verändert wurden
    - die Antwort der Anfrage entspricht
    - die Antwort wirklich von dem Server stammt, an den die Anfrage ging

3) SIG RR – Signature Resource Record

- Signierung von Anfragen mittels SIG RR
  - spezielle SIG RRs werden am Ende einer Anfrage eingebunden
  - nur für UPDATE-Anfragen sinnvoll
  - bei älteren DNS Servern können Fehler auftreten
  - evtl. für zukünftig mögliche Anfragen notwendig

- für jeden authentifizierten RR Set, den die Anfrage zurückliefert, soll ebenfalls authentifizierender SIG RR gesendet werden (soweit dies möglich ist)

3) SIG RR – Signature Resource Record

- Erstellung einer Signatur:
  - zu RR Set Hashwert durch Hashfunktion berechnen
  - Empfehlung: Verwendung des DSA-Verfahrens
  - Verschlüsselung des Hashwerts mit Private Key der Domain
    → digitale Signatur
- Prüfung der Integrität einer Nachricht:
  - Hashwert der Nachricht (ohne Signatur) berechnen
  - Entschlüsseln der digitalen Signatur mit Public Key
  - beide Werte gleich → Nachricht wurde nicht verändert
- Erhalt des Public Keys durch DNS Anfrage
  → Zweck des KEY RR

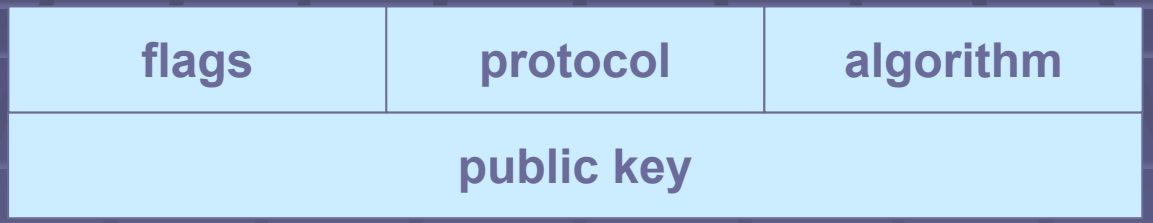
4) KEY RR – KEY Resource Record

- KEY RR:
  - enthält Public Key, welcher mit einem DNS-Namen verknüpft ist
  - befindet sich entweder in der Zone, deren Signatur mit dem zugehörigen Private Key erstellt wurde oder in deren Superzone
- mindestens ein Schlüssel pro Zone (mehrere erlaubt!)

  → sicherheitsbewusste DNS Implementierungen müssen mind. zwei gleichzeitig gültige Schlüssel des selben Typs, welche mit dem selben Namen verbunden sind, handhaben können
- sicherheitsbewusste DNS Server fügen KEY RR (falls vorhanden) an das Ende von Antworten hinzu

4) KEY RR – KEY Resource Record

- RDATA eines KEY RRs:



5) Zonenstatus

- für jeden Algorithmus können Zonen
  - **sicher** sein
    - jeder abgerufene RR wird durch einen SIG RR authentifiziert
  - **experimentell sicher** sein
    - SIG RR können vorhanden sein
    - wenn sie vorhanden sind, müssen sie überprüft werden
  - **unsicher** sein
    - SIG RRs werden nicht benötigt, um RR von einer Zone abzufragen

5) Zonenstatus

- Bestimmung des Zonenstatus
  - jeder glaubwürdige KEY RR der Zone behauptet, es gibt keinen Schlüssel

    → Zone ist für diesem Algorithmus **unsicher**
  - ein KEY RR der Zone mit Schlüssel und einer ohne Schlüssel vorhanden

    → Zone ist **experimentell sicher**
  - jeder vertrauenswürdige KEY RR der Zone spezifiziert einen Schlüssel

    → Zone ist für diesem Algorithmus **sicher**

    → es werden nur authentifizierte RR der Zone akzeptiert

5) Zonenstatus

- Beispiel:
  - Resolver vertraut der Superzone von Z und einer dritten Partei X
  - Daten der Zone Z können von keinem, von einem oder von beiden signiert werden
  - abhängig von den signierten KEY RR der Zone Z wird nun der Status bestimmt:

Superzone

X	k.A.	NoKey	gemischt	Schlüssel
k.A.	illegal	unsicher	experim.	sicher
NoKey	unsicher	unsicher	experim.	sicher
gemischt	experim.	experim.	experim.	sicher
Schlüssel	sicher	sicher	sicher	sicher

6) NXT RR – Next Resource Record

- NXT RRs ermöglichen authentifizierbare Antwort auf
  - Anfragen nach nicht existierenden Rechnernamen
  - Anfragen nach nicht existierenden DNS Einträgen

  d.h. es kann z.B. versichert werden, dass in einer Zone kein RR mit einem bestimmten Besitzernamen existiert
- zeigen an, welche RR Typen für einen existierenden Namen vorliegen

6) NXT RR – Next Resource Record

- RDATA eines NXT RR

- NXT RRs erstellen eine Kette aller Besitzernamen in einer Zone
- Existenz eines NXT RR deutet darauf hin, dass
  - kein Name zwischen Besitzernamen des NXT RR und dem Namen in seinen RDATA existiert
  - kein anderer Typ unter diesem Besitzernamen existiert

6) NXT RR – Next Resource Record

- Problem
  - kein Name für RDATA des letzten NXT RRs vorhanden
- Lösung
  - ringförmige Anordnung
  - letzter NXT RR enthält in den RDATA den Zonennamen
- Antworten bzgl. der Nicht-Existenz eines Namens benötigen u. U. mehrere NXT RRs
  - Beweis, dass kein Wildcard existiert, deren Erweiterung zurückgegeben werden müsste
  - Beweis, dass nicht mehr Namen (oder Wildcards) existieren, die bei der Antwort hätten berücksichtigt werden müssen

7) TTL, CNAMEs und Delegationspunkte

TTL (time to live)

- Widerspruch
  - keine Änderung der Daten zwischen ihrer Signierung und Verifizierung der Signatur erlaubt
  - TTL soll beim Zwischenspeichern der Daten verringert werden
- Idee
  - TTL außerhalb der digitalen Signatur halten
  - ABER: Server können unentdeckt willkürlich lange TTL-Werte setzen
- Lösung
  - Einbindung des ursprünglichen TTL-Werts in die Signatur
  - Übertragung der Daten mit dem aktuellen TTL-Wert

7) TTL, CNAMEs und Delegationspunkte

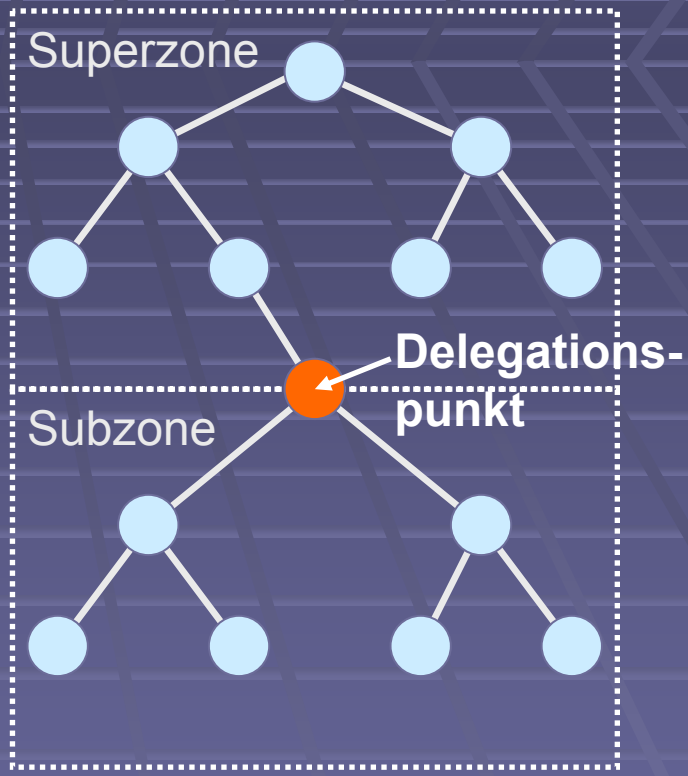
CNAMEs (canonical names)

- Problem bei Abfrage von gesicherten RRs mit gleichem Besitzernamen wie CNAME RR durch einen ungesicherten Server
- Anforderungen an sicherheitsbewusste Server bzgl. sicherer CNAMEs im DNS
  - KEY, SIG und NXT RRs zusammen mit CNAMEs erlauben
  - Verarbeitung von CNAMEs bei Abfrage von KEY, SIG und NXT RRs und CNAMEs unterdrücken
  - automatisch SIG RR zurückgeben, die CNAME(s) authentifizieren
- Änderung zu RFC 1034/1035: in Knoten in denen ein CNAME RR vorkommt waren andere RR-Typen verboten

7) TTL, CNAMEs und Delegationspunkte

Delegationspunkte

- gehören zu beiden Zonen
- können von beiden Zonen signiert sein
- Anfragen können RRs und SIG RRs von beiden Zonen erhalten



- Superzone sicher:
  - jede Subzone enthält von Superzone signierten Zone KEY RR
- Subzone unsicher:
  - Subzone muss durch einen Schlüssel als unsicher deklariert sein
  - Schlüssel wird von Superzone signiert und ist auch in dieser enthalten

8) Sichere Namensauflösung

- Start mit statisch im Resolver konfigurierten Public Key
- Kategorisierung der Daten auf einem sicherheitsbewussten Server:
  - authentifizierte Daten
    - gültige Signatur aufgrund Schlüssel vorhanden
    - Schlüssel ist rückverfolgbar zu statisch konfiguriertem Schlüssel mittels Kette von SIG und KEY RRs
    - KEY und SIG RRs sind durch Resolverrichtlinien zugelassen
  - unbearbeitete Daten
    - besitzen keine gültige Signatur
    - mindestens eine gültige Signatur, die der Resolver noch versucht zu authentifizieren

8) Sichere Namensauflösung

- unsichere Daten
  - Daten die sicher niemals authentifiziert werden
  - Daten die in der Zone aus der sie stammen als ‚bad' kategorisiert werden
  - Daten die sich in einer unsicheren Zone befinden
  - Daten die durch eine unsichere Zone angekommen sind
  - Daten die eine unsignierte glue address haben
  - Name Service Daten eines Delegationspunktes

- ‚bad' Daten
  - Daten bei denen alle Signatur-Tests fehlgeschlagen sind
  - Daten werden vom Server gelöscht

8) Sichere Namensauflösung

- AD und CD Header Bits
  - werden außerhalb des DNS Anfrage/Antwort Headers zugewiesen
  - **AD** (authentic data) **Bit** (Antwort)
    - alle Daten in der Antwort und im Authentifizierungsbereich der Antwort sind vom Server nach dessen Richtlinien authentifiziert
  - **CD** (checking disabled) **Bit** (Abfrage)
    - unbearbeitete, (noch) nicht authentifizierte Daten sind für den Resolver, der die Abfrage sendet akzeptabel

8) Sichere Namensauflösung

- sicherheitsbewusste Resolver dürfen AD Bit nur vertrauen, wenn
  - sie dem Server vertrauen
  - sie einen sicheren Kanal zu dem Server haben oder
  - sie sichere DNS Transaktionen benutzen

- sicherheitsbewusste Resolver, die Verschlüsselung nutzen wollen, sollten auf das CD Bit in der Abfrage bestehen, um
  - der Abfrage eigene Richtlinien aufzwingen zu können
  - die Latenzzeit zu verringern, indem sie dem Server erlauben, mit unbearbeiteten Daten zu antworten

8) Sichere Namensauflösung

- Verkettung durch Schlüssel:
  - i.A. sind **RR Sets** von einem oder mehreren **SIG RRs** signiert
  - jeder **SIG RR** hat einen Signierer, unter dessen Name der **Public Key** gespeichert ist, der bei der Authentifizierung des SIG RR verwendet wird
  - jeder dieser **Public Keys** wird wieder von einem **SIG RR** signiert
  - diese **SIG RRs** haben wiederum Signierernamen, die auf einen **Schlüssel** verweisen u.s.w.

  → Authentifizierung führt zu einer Kette mit abwechselnden SIG und KEY RR

8) Sichere Namensauflösung

- Validierung jedes SIG RRs mit Bezug zu einem Schlüssel muss objektiven Verschlüsselungstest bestehen
- Verschlüsselungstest wird von Verschlüsselungs-algorithmus beinhaltet
- letztlich entscheiden Resolverrichtlinien, ob ein bestimmter SIG RR bestimmte Daten authentifizieren kann
- empfohlene Richtlinien:
  - A < B: A ist indirekt oder direkt eine Superdomäne von B
  - A = B: A und B sind die selben Domänennamen
  - A > B: A ist indirekte oder direkte Subdomäne von B

  (A bzw. B wird durch Weglassen oder Hinzufügen von Labels zu B bzw. A erzeugt)

8) Sichere Namensauflösung

- STATIC: Besitzername eines Satzes von statisch konfigurierten, vertrauenswürdigen Schlüsseln auf einem Resolver
- OWNER: RR Set mit Besitzername OWNER
- SIGNER: ist dann gültiger Name eines SIG RRs, der OWNER authentifiziert, wenn folgende drei Regeln gelten:

8) Sichere Namensauflösung

- (1) **OWNER > oder = SIGNER**
  - OWNER ist in der selben Domäne oder in einer Subdomäne von B
  - wenn SIGNER = root ist, muss OWNER = root oder ein Domänenname höchster Ebene sein
- (2) **(OWNER < SIGNER) und (SIGNER > oder = static)**
  - OWNER ist Superdomäne von SIGNER und
  - SIGNER ist statisch konfiguriert oder eine Subdomäne eines statisch konfigurierten Schlüssels
- (3) **SIGNER = static**
  - SIGNER ist genau ein statisch konfigurierter Schlüssel

8) Sichere Namensauflösung

- Regel (1)
  - Regel zum **Absteigen** innerhalb des DNS Baums
  - beinhaltet spezielles Verbot für root Zone, aufgrund deren Beschränkung auf eine Tiefe von einer Ebene
  - wichtigste Regel
- Regel (2)
  - Regel zum **Aufsteigen** von einem oder mehreren statisch konfigurierten Schlüsseln innerhalb des DNS Baums
  - bewirkt nichts, wenn nur die root Zone statisch konfigurierte Schlüssel besitzt
- Regel (3)
  - erlaubt unmittelbare **quer-Zertifizierung**
  - bewirkt nichts, wenn nur die root Zone statisch konfigurierte Schlüssel besitzt

9) Server und Resolver Konformität

Server Konformität

- BASIC:
  - speichert SIG, KEY und NXT RRs und fragt sie ab
  - Mindestanforderung für untergeordnete Server und Caching-Server
  - u.a. können sichere CNAMEs nicht unterstützt werden

9) Server und Resolver Konformität

- FULL (umfasst grundlegende und zusätzliche Fertigkeiten):
  - liest SIG, KEY und NXT RRs in Zonendaten
  - fügt, mit gegebener Zonendatei und Private Key, geeignete SIG und NXT RRs hinzu
  - bindet ordnungsgemäß und automatisch SIG, KEY und NXT RRs in Antworten ein
  - unterdrückt bei der Abfrage der RRs des Sicherheitstyps, die Zurücklieferung von CNAMEs
  - erkennt CD Abfrage Header Bit und setzt AD Abfrage Header Bits
  - behandelt an Delegationspunkten die beiden NXT RRs richtig
  - Mindestanforderung für übergeordnete Server für sichere Zonen
  - Mindestanforderung für alle Server für vollkommen sicheren Betrieb

9) Server und Resolver Konformität

Resolver Konformität

- BASIC:
  - bearbeitet SIG, KEY, NXT RR, wenn sie explizit abgefragt werden
- FULL (umfasst grundlegende und zusätzliche Fertigkeiten):
  - versteht KEY, SIG und NXT RR einschl. der Verifizierung der Signaturen für vorgeschriebenen Algorithmus
  - speichert Informationen im Cache und in der Datenbank, welche RRs für welche Erweiterung authentifiziert wurden
  - führt zusätzliche Abfragen durch, falls diese gebraucht werden um SIG, KEY oder NXT RRs zu erhalten
  - setzt gewöhnlich das CD Abfrage Header Bit bei seinen Abfragen

10) Probleme von DNSSec

- beeinflusst die Effizienz des DNS negativ
  - Datenbankgröße steigt sehr stark
  - Signieren von Zonen und Entschlüsseln von Signaturen verlangsamt die Namensauflösung erheblich
- Fehler in der Verteilung der Root-Keys haben verheerende Folgen
  - macht ganzes DNSSec nutzlos
  - Resolver die DNSSec benutzen, könnten dann keine Namensauflösung mehr durchführen
  - Problem noch nicht gelöst

Vielen Dank für die Aufmerksamkeit!