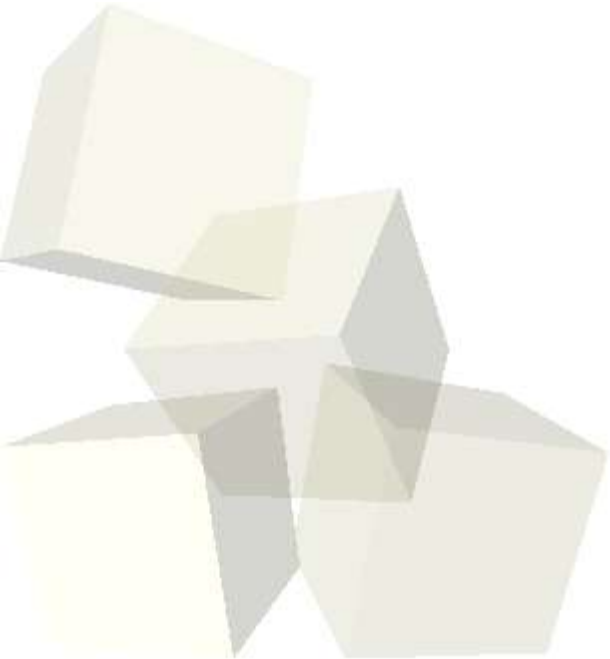
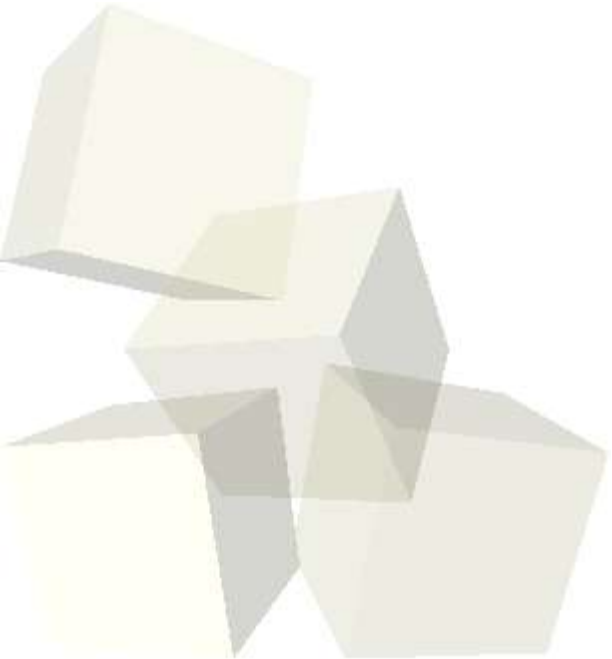


Programm für heute

- Einführung in DNS
- Wie man's kaputt kriegt
- Mögliche Auswege



Warum DNS?

- Problem:
  - IP-Protokoll will 67.72.100.173
  - Mensch mag lieber www.ogrish.com
- Intuitiver Ansatz: Liste machen und an alle verteilen

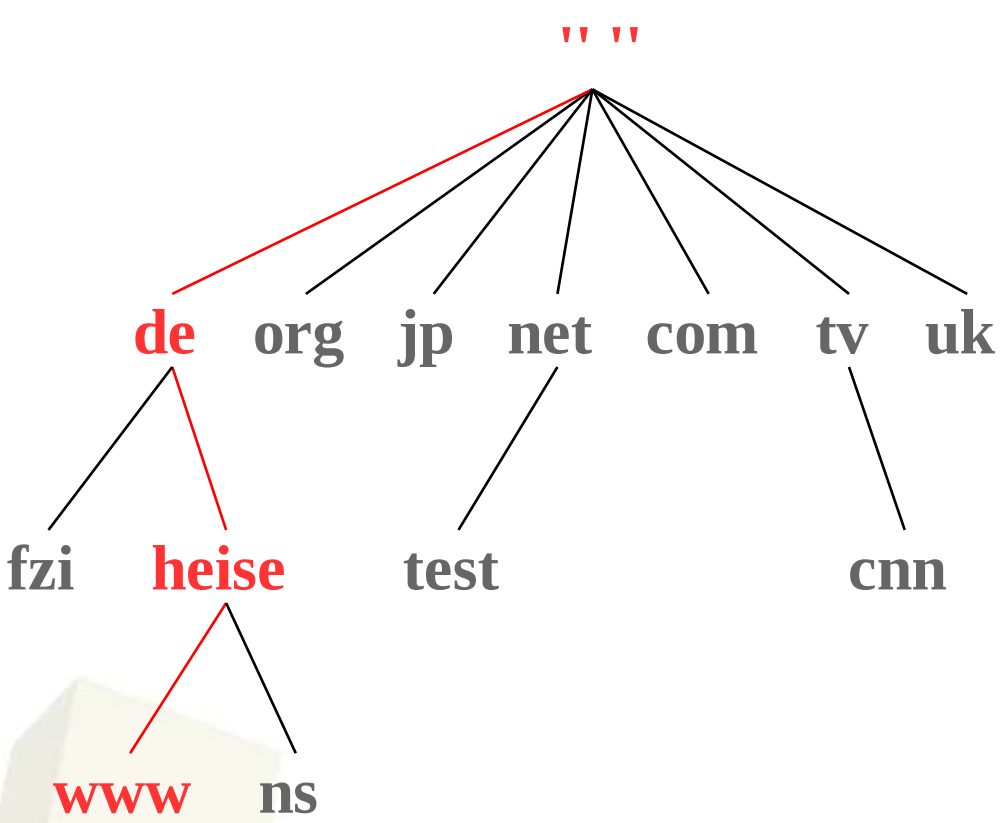
Historisches

- ARPAnet der 70er und 80er:
  - Ein paar hundert Rechner
  - Nur nette Menschen
- NIC verwaltet zentral eine HOSTS.TXT und verteilt diese per FTP, UUCP und eMail
- Problem: skaliert nicht
  - Starkes Wachstum der kompletten Netzes
  - HOSTS.TXT zu gross zum Verwalten und Verteilen
  - Inkonsistenz und Kollisionen
- Lösung: Einfach DNS erfinden (Anfang 1983)

Anforderungen an DNS

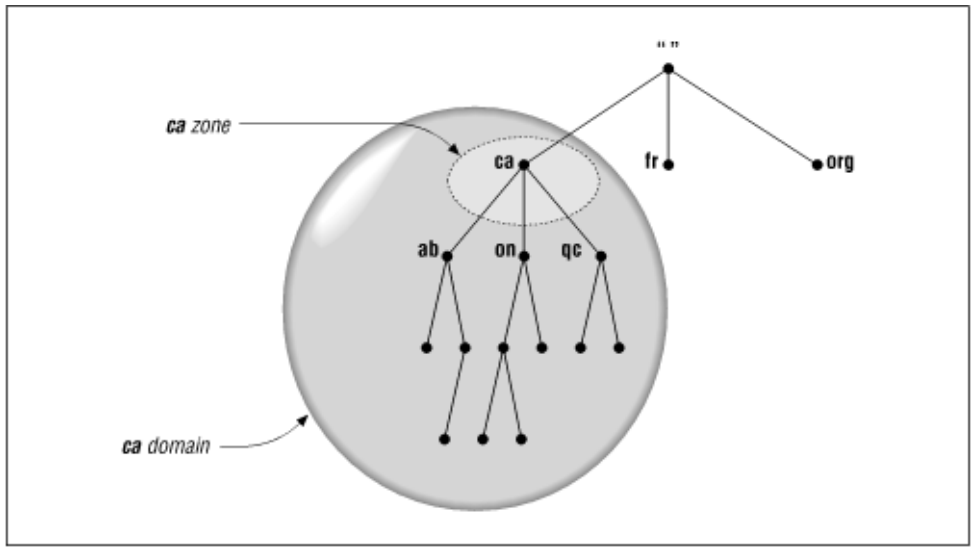
- Ausfallsicher
- Leicht delegierbar
- Konsistent
- Geordnet, kein Chaos/Anarchie
- Kann gleich noch beim Verschicken von eMails mithelfen

Organisation des Namensraumes

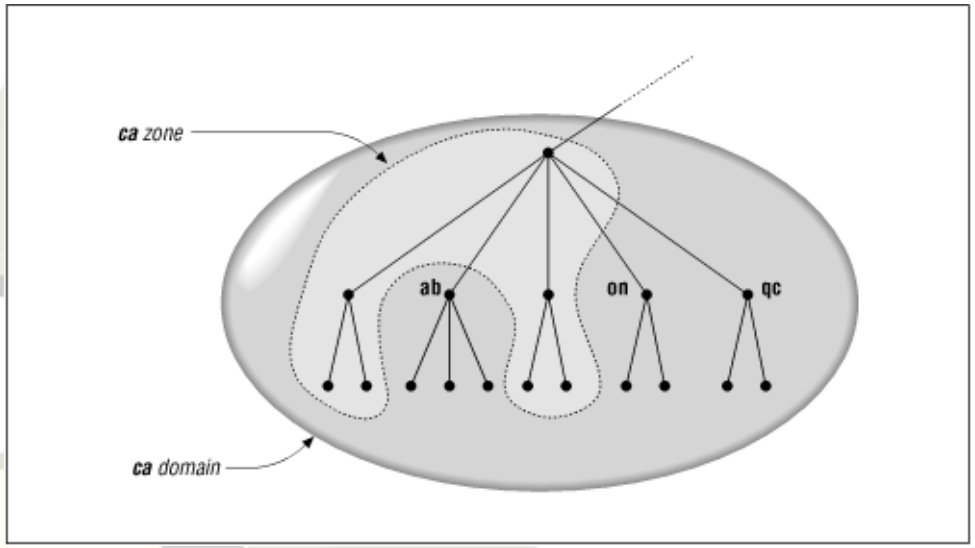


- Hierarchischer Namensraum
- Für die Wurzel ("Root") sind dreizehn Server zuständig
- Teilbäume können an Dritte delegiert werden

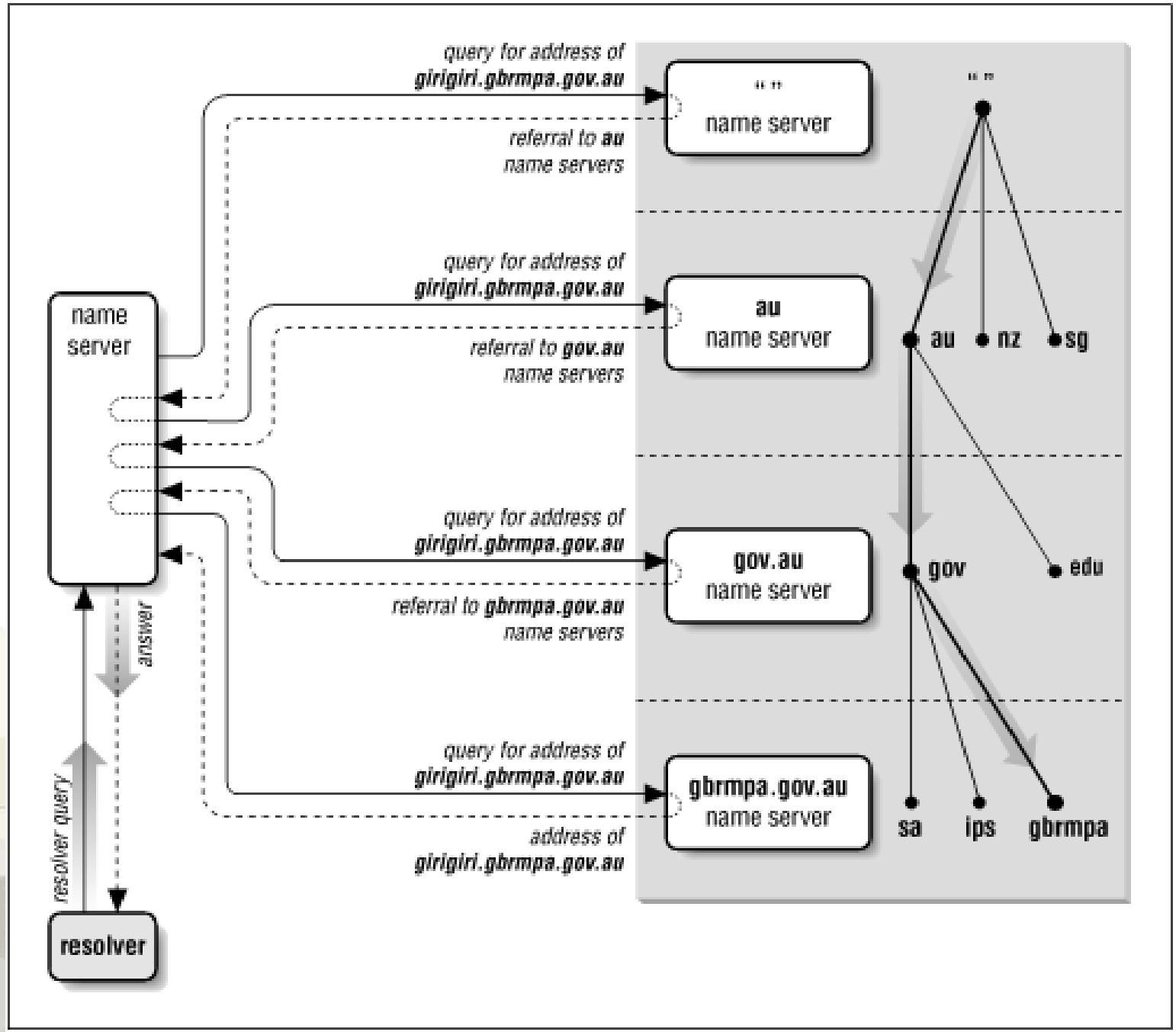
Domains vs. Zonen



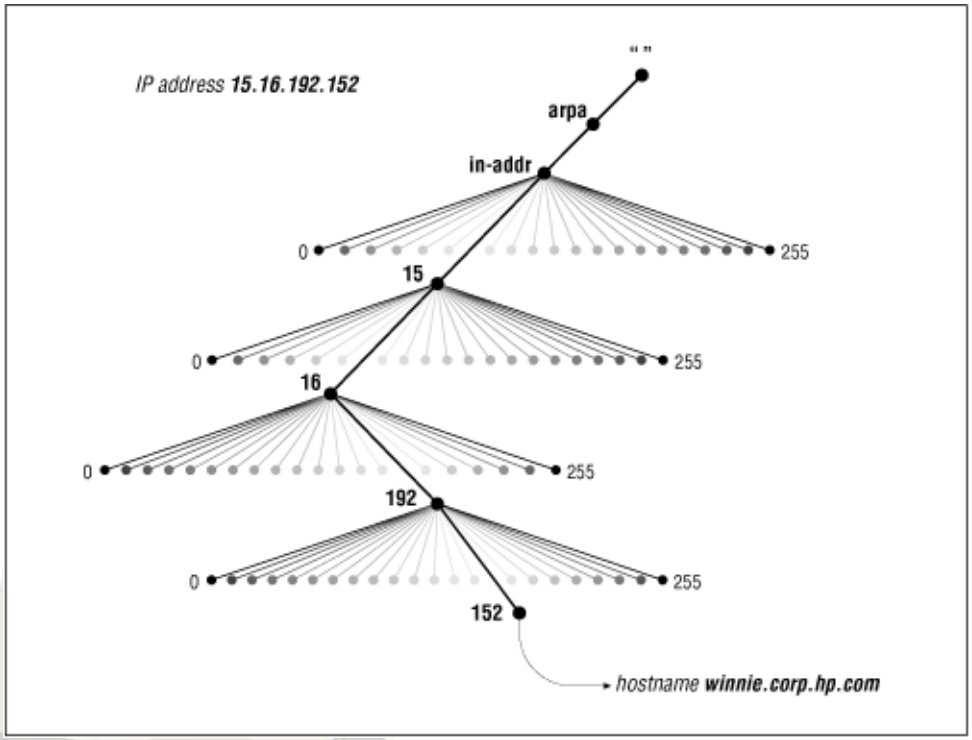
- Domain: Teilbaum des Namensraumes
- Zone: Zuständigkeitsbereich eines Nameservers



Suchen von Namen



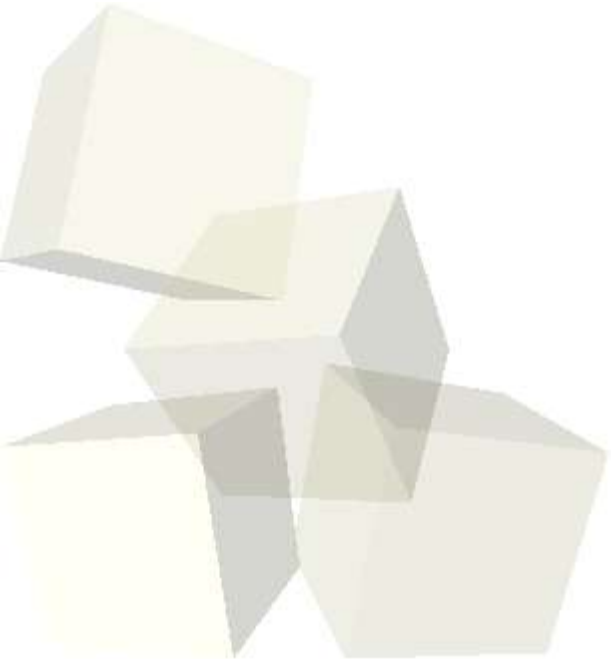
in-addr.arpa ?



- Problem: wie finde ich den Namen zu 212.227.3.124?
- Einbetten das IPv4-Namesraumes im DNS-Namespace mittels PRT-Records
  - 124.3.227.212.in-addr.arpa.
- Optional (weil scheisse?)

Was man so alles im DNS finden kann

- Verschiedene Typen von Informationen für jeden Namen: A, CNAME, MX, NS, PRT, TXT, SOA und noch viel mehr (RFC1035)



Warum ist DNS eine kritische Infrastruktur?

- Was passiert, wenn DNS nicht mehr funktioniert:
  - Die meisten Server sind nicht mehr (sinnvoll) erreichbar
  - eMail funktioniert nicht mehr
- Folgen für Verkehr und Wirtschaft?
  - Das wird teuer ...

Bedrohungszenario 1: Denial of Service

- Bei einem DoS bricht ein Server unter einer Flut von Anfragen zusammen
- Folge: Ausweichen auf sekundären Server
- Wenn der auch nicht mehr geht, dann ist die betroffene Zone "erstmal weg"
- Dauer: bis der Angreifer aufhört oder abgeklemmt wird

Bedrohungszenario 2: DNS Spoofing (MiM)

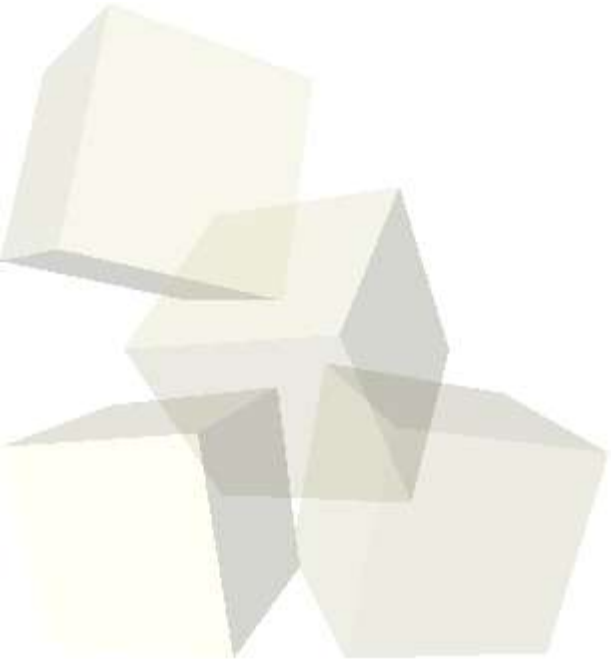
- Angreifer versucht, im Namen des echten DNS-Server falsche Informationen zu verbreiten
- Folge: Angreifer hat Zugang zum kompletten Mailverkehr und auf alle Anfragen an die betroffenen Server.
- Dauer: kurz und punktuell
- (Birthday Attack)

Bedrohungszenario 3: Cache Poisoning

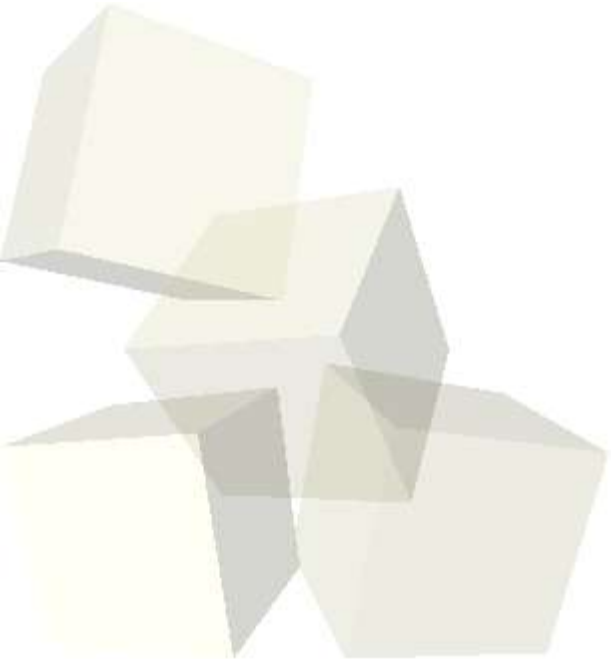
- Angreifer schleust falsche Informationen in die Caches von DNS-Servern und Resolvern ein
- Folge: alle Anfragen an eine bestimmte Domain werden umgeleitet
- Dauer: kann der Angreifer selbst bestimmen

Weitere Szenarien

- Social Engineering
- DNS-Server "regulär" hacken
- BIND benutzt...



- Gegenmassnahmen:
  - Integrität der Zonendaten sicherstellen
  - DNS-Server muss sich gegenüber dem Anfragenden ausweisen



Neue RRs

- KEY
  - Öffentlicher Schlüssel
- SIG
  - Signatur eines RR
- NXT
  - Wie kann ich sicherstellen, das mir niemand existente Hosts als nichtexistent markiert?

Vorteile von DNSSEC

- Viele der genannten Angriffsformen nicht mehr möglich

Nachteile von DNSSEC

- Funktioniert erst, wenn alle mitmachen
- Datenbankgrösse steigt um ca. Faktor 7-8
  - Belastung für Netz und Hardware steigt stark an
- Benötigt eine komplette Public-Key-Infrastruktur
  - was tun, wenn der Root-Schlüssel kompromitiert ist?
- DNSSEC ermöglicht einen kompletten Zonentransfer -> Informationsleck

Alternativen?

- DJB: NYM-based Security
  - http://cr.yp.to/djbdns/forgery.html
- Zurück zur HOSTS.TXT ?