Netzsicherheit – Architekturen und Protokolle
DNS Security

1. Einführung DNS
2. DNSsec

Netzsicherheit – Architekturen und Protokolle
DNS Security

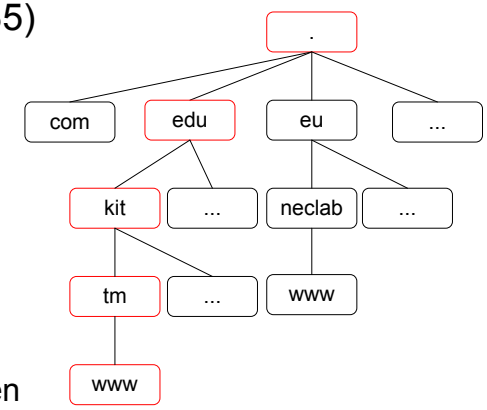
1. Einführung DNS
2. DNSsec

DNS Überblick

- Domain Name System (DNS) (RFC 1034 / 1035)
  - Namensauflösung von Domainnamen nach IP Adresse
  - Verteilter hierarchischer Verzeichnisdienst
  - Standard UDP Port 53 – Backup TCP Port 53
  - Maximale Paketgröße: 512 Byte
    - Einführung von EDNS (RFC 2671)
    - Variable UDP-Größe
    - Erweiterung um 16 neue Flags
    - DNSsec erfordert zwingend EDNS wegen neuem Flag und Größe der DNS Antwort
  - Modi:
    - Rekursive Namensauflösung
    - Iterative Namensauflösung

DNS Namensraum

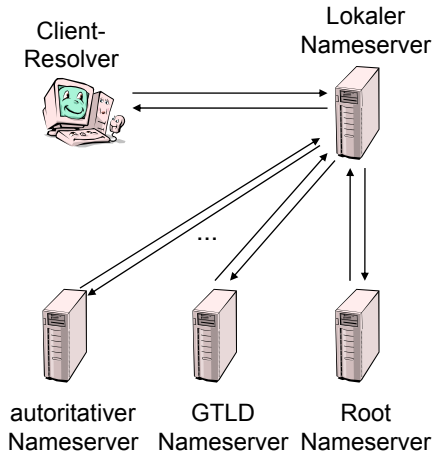
- Domain Names (RFC1035)
  - Max. Länge: 255 Zeichen
  - Delegation von rechts nach links
- Hirarchischer Aufbau in Form eines Baums
  - Erste Ebene: Top-Level-Domains (TLD)
  - Blätterbezeichner zwischen 1 und 63 Zeichen



Beispiel FQDN: www.tm.kit.edu

DNS Infrastruktur

- Rekursive Namensauflösung
  1. Resolver (Client) stellt Anfrage an lokalen NS (z.B. des ISP)
     - NS Kennt die Abbildung Name → IP nicht
  2. Wählt einen Root-NS und leitet die Anfrage weiter
     - Dieser kennt die Antwort nicht und delegiert an GTLD (global TLD)
  3. Wählt einen GTLD-NS und wiederholt die Anfrage
     - Kennt die Antwort auch nicht und delegiert
  4. Wiederholung der Anfrage bis zum zuständigen (autoritativen) NS
     - Sendet die Abbildung als Antwort
  5. Lokaler NS sendet Antwort an Client
     - Antwort ist nicht autoritativ!



„Dig +trace <*name*>" zeigt alle Anfragen and Antworten an

Pharming

- Namensauflösung gesteuert durch Konfiguration des Resolvers
  - *Hosts*-Datei statisch konfiguriert
  - Standard Auflösungsreihenfolge: hosts, dns
- Pharming manipuliert die *hosts*-Datei
  - Eintragen von statischen Abbildungen
  - Meist durch Virus oder Trojaner
  - Umleiten von Verkehr auf gefälschte Seite um
    - Login-Daten abzugreifen
    - Personen-bezogene Daten zu stehlen

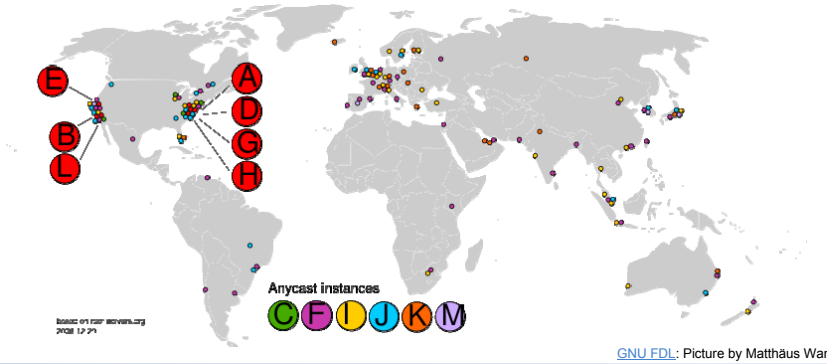
→ Für den Benutzer absolut nicht erkennbar

DNS Terminologie

- Resolver
  - Client Software des DNS, das Anfragen stellt und Antworten entgegennimmt
  - Besitze eigene minimal Konfiguration
- Zone
  - Administrative Domäne eines Netzanbieters
- Resource Record
  - DB-Typ der Abbildung
  - Z.B. Name → IPv4
  - IPv6, MX, NS, SOA
- Nameserver (NS)
  - Server software
- Autoritativer NS
  - Löst die angefragte Abbildung auf
- Delegation
  - Verweis auf einen anderen NS, um die angefragte Abbildung aufzulösen
- Rekursiver NS
  - Ein NS, der alle Delegation bis zum autoritativen NS folgt

DNS Root-Server

- 13 Root-Server weltweit verteilt
  - 7 zentralistisch
  - 6 verteilt auf Anycast-Basis
- Verteilung



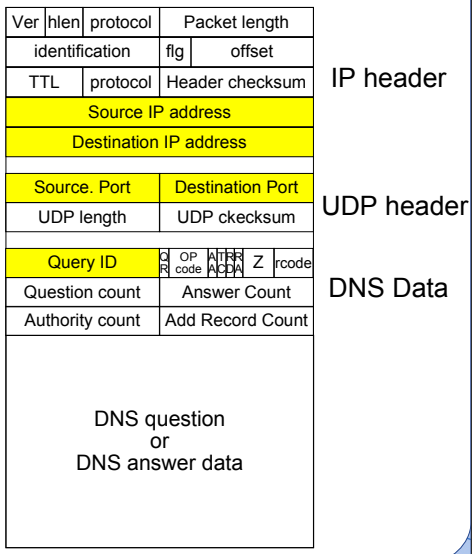
GNU FDL: Picture by Matthäus Wander

DNS Updates

- Neue Daten
  - Aufspielen neuer Abbildungen
- NS-Replizierung
  - Master-Slave Ansatz in einer Zone
  - Lastverteilung und Ausfallsicherheit
- Dynamische Updates
  - Änderungen per DNS-Request
- TSIG Resource Record
  - Meta-RR
  - Integritätssicherung der DNS Daten mittles MD5
  - Vorverteiltes Geheimnis
  - Keine Verschlüsselung
- Nachteil
  - Schlechte Skalierbarkeit
  - Nur in kleinen isolierten Netzen sinnvoll einsetzbar

DNS Paketformat

- IP Adressen
  - Fälschen der Quell IP-Adresse einfach
- UDP Port Nummer
  - Server: 53/udp
  - Client: 53/udp, fixed config, fixed on random init
- Query ID
  - Eindeutige ID, um Anfrage und Antwort zuzuordnen
  - Häufig: 1-er Inkrement für jede Anfrage



QR: 0 zeigt Anfrage (Query) an, 1 Antwort (Response)

AA (Authorative Answer): 1 bei Antwort von authorativen NS, sonst 0

TC (Truncated): 1, wenn Antwort größer als 512 Byte; Client kann Anfrage über TCP wiederholen

RD (Recursion Desired): Client setzt 1, wenn rekursive Namensauflösung durch lokalen NS gewünscht;
0, wenn Resolver selbst iterative den Namen auflöst

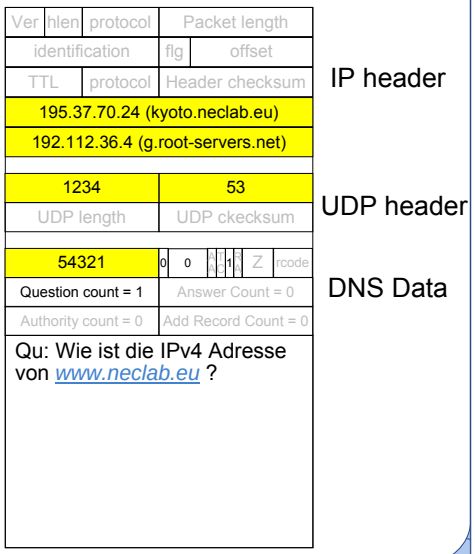
RA (Recursion Available): Server unterstützt rekursive Namensauflösung (1) oder nicht (0)

Z – reserved: muss auf 0 gesetzt sein

Rcode (response code): Server zeigt Erfolg oder Misserfolg der Namensauflösung an

DNS Paketformat – Beispiel I

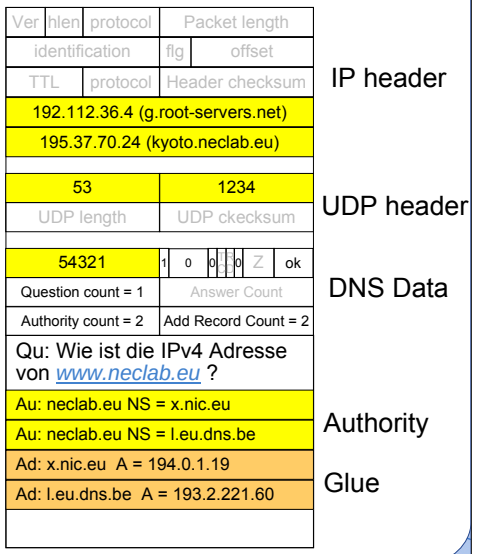
- Anfrage nach www.neclab.eu
  - Lokaler NS: kyoto.neclab.eu
  - Gesucht IPv4 Adresse
- Beispiel: Nachricht von Kyoto an TLD NS
  - Query Count = 1 zeigt an, dass im Datenfeld ein Anfrage enthalten ist
  - QR = 0: Anfrage
  - OP = 0: Standardanfrage
  - RD = 1: Rekursive Auflösung gewünscht



„dig +trace www.neclab.eu any +multiline +all +answer"

DNS Paketformat – Beispiel II

- Antwort des TLD
  - QR = 1: Antwort
  - AA = 0: nicht authorativ
  - RA = 0: Rekursion nicht unterstützt
- Delegierung
  - Liste von NS für nächsten Rekursionsschritt (Authority Count = 2)
  - List von A-Records für diese NS (Add Record Count = 2)
- Anfrage-Antwort Verknüpfung
  - NS hält Liste von ausstehenden Anfragen (Query-ID)
  - Ignorieren von Antworten ohne Query-ID in Liste



„dig +trace www.neclab.eu any +multiline +all +answer"

DNS Paketformat – Beispiel III

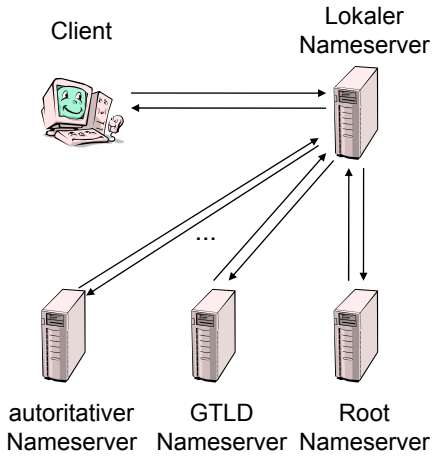
- Antwort von kyoto.neclab.eu
  - QR = 1: Antwort
  - AA = 1: autoritativ
  - RA = 0: Rekursion nicht unterstützt
- Canonical Name
  - Alias oder alternativer Name
  - Antwort enthält keine Abbildung zu IPv4 Adresse
  - Weitere Namensauflösung notwendig

Ver	hlen	protocol	Packet length	IP header
identification		flg	offset	
TTL	protocol	Header checksum		
192.112.36.4 (g.root-servers.net)				
195.37.70.24 (kyoto.neclab.eu)				
53		1234		UDP header
UDP length		UDP ckecksum		
54322	1	0 1 - - 0 Z ok		DNS Data
Question count = 1		Answer Count = 1		
Authority count = 2		Add Record Count = 2		
Qu: Wie ist die IPv4 Adresse von *www.neclab.eu* ?				
An: www.neclab.eu CNAME = www.netlab.nec.de				Answer
Au: nec.de NS = a.nic.de				Authority
Au: nec.de NS = l.de.net				
Ad: a.nic.de A = 194.0.0.53				Glue
Ad: l.de.net A = 77.67.63.105				

„dig +trace www.neclab.eu any +multiline +all +answer"

Team-Diskussion

- Was muss man tun, damit der lokale NS eine gefälscht/gespoofte DNS-Antwort annimt?

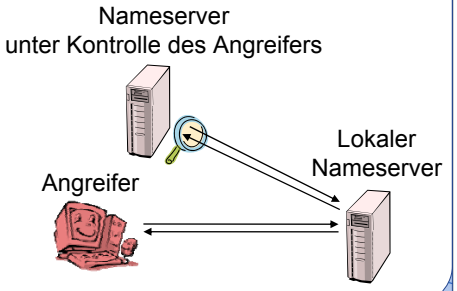


„Dig +trace <*name*>" zeigt alle Anfragen and Antworten an

DNS cache poisoning

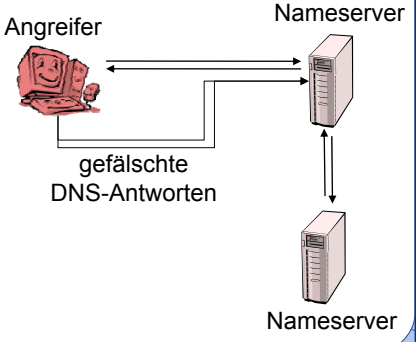
- DNS cache poisoning Angriff
  - Eintrag gefälschter Abbildungen in den DNS Cache
  - Übernahme von Zonen möglich
- Kein Phishing!
  - Resultat ähnlich
  - Phishing kann von Benutzer erkannt werden

- Vorbereitung
  - DNS Anfrage eines Namens, für den ein kontrollierter NS autoritativ ist
  - ➔ Auslesen, des UDP Source Ports und des aktuellen Query-ID-Werts



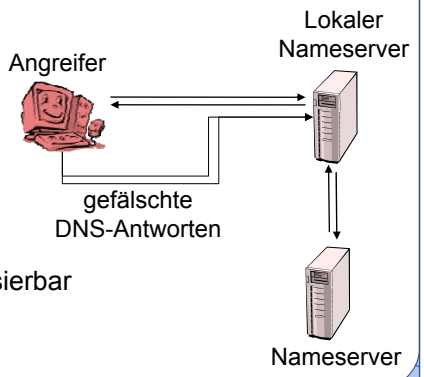
DNS cache poisoning – II

- Annahme
  - UDP source port statisch
  - Query-ID wird für jede Anfrage inkrementiert
  - Abbildung nicht im DNS-cache
- Angriff auf lokalen NS
  - DNS-Anfrage nach www.trustedbank.com
  - Senden von DNS-Antworten mittels IP-Spoofing und verschiedenen Query-Ids
    - Enthalten gefälschte Abbildung
  - Angriff erfolgreich, wenn
    - die richtige Query-ID erraten wird
    - Antwort den lokalen NS vor der richtigen DNS Antwort erreicht



The Dan Kaminsky Threat

- Erweiterung des einfachen Angriffs
  - Setup eines NS für trustedbank.com
  - DNS-Anfrage für einen Namen, der nicht im Cache ist
    - Vorschläge?
  - Fälschen der Root- oder GTLD-Antwort
    - Gefälschte Glue-Einträge
  - Übernahme der geasmten Zone
  - Erfolgswahrscheinlichkeit pro Zone gering, aber einfach automatisierbar



DNS Fixes

- Keine echte Lösung des Problems, aber schnell ausrollbar
  - Zufällige Query-ID
    - Beschränkt auf 16-bit wegen Kompatibilität
  - Zufällige UDP-Portnummer
    - Speichern der verwendeten Portnummer mit DNS-Anfrage
    - Beispiel: Microsoft DNS Server reserviert 2500 Portnummern
- Echte Lösung: DNSsec
  - Problem: Umstellen der Infrastruktur erst begonnen

Netzsicherheit – Architekturen und Protokolle
DNS Security

1. Einführung DNS
2. DNSsec

- Formulieren Sie Designkriterien für eine sicheres Namensauflösungssystem
- Wie können diese technisch umgesetzt werden?
- Welche Vorteile bzw. Nachteile haben die unterschiedlichen Ansätze?

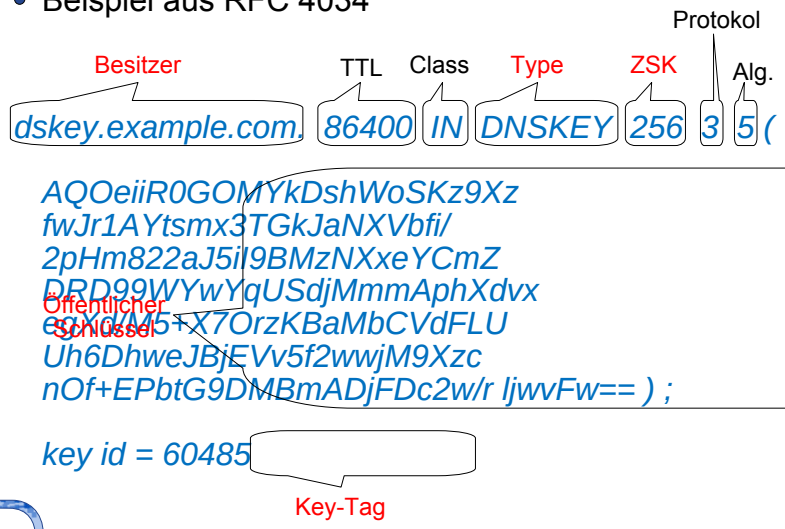
DNSsec Geschichte

- Schwachstellen des DNS bekannt seit 90er
  - Steven Bellovin: *Using the Domain Name System for System Break-ins*, veröffentlicht 1995
- IETF WG: DNS Security
  - 1997: RFC 2065 veröffentlicht
  - 1999: Überarbeitung als RFC 2535 standardisiert
  - 2001: Skalierungsprobleme entdeckt
    - Schlüsselerneuerung erfordert 6 Nachrichten zwischen Zone und Vaterzone
    - Schlüsselerneuerung einer TLD-Zone hätte Millionen Update-Nachrichten zu allen Kindzonen erfordert
  - 2005: RFCs 4033 – 4035 veröffentlicht
  - 25.01.2010: L-Rootserver signiert (DURZ)
  - Mai 2010: Alle Rootserver DNSSec fähig
  - 01.07.2010: Umstellung auf echten Schlüssel

Deliberately Unvalidatable Root Zone (DURZ)

DNS KEY (DNSKEY) RR

- Beispiel aus RFC 4034

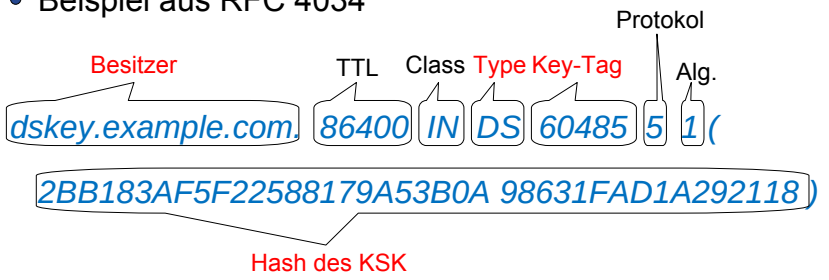


Delgation der Signierung

- Zone Signing Key (ZSK)
  - Öffentlicher Schlüssel abgelegt in Zonendatei
  - Signierung der RRs der Zone
  - Signiert durch KSK der Zone
  - Flag: 256
- Key Signing Key (KSK)
  - Öffentlicher Schlüssel abgelegt in Zonendatei
  - Signierung des ZSK der Zone
  - Signiert durch den ZSK der Vaterzone
  - Flag: 257
- Trennung in zwei Schlüssel erleichter Schlüsselerneuerung

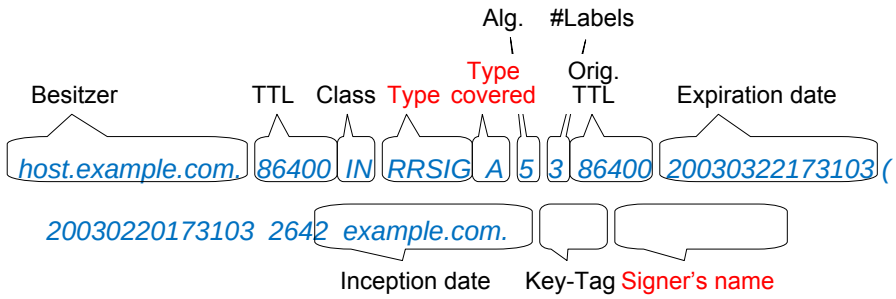
Delegation Signer (DS) RR

- Beispiel aus RFC 4034



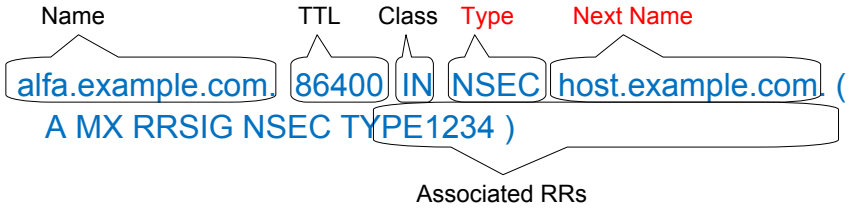
RR Signature (RRSIG)

- Beispiel aus RFC 4034



Next SECure (NSEC) RR

- Beispiel aus RFC 4034



- Authentizität bestätigt durch RRSIG

Aufzählung der Zoneneinträge

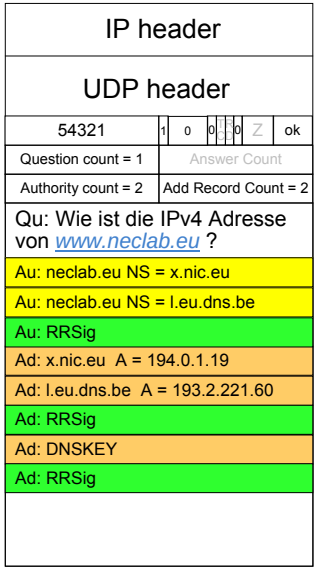
- DNS Daten sind als öffentlich anzusehen
  - Gefahr: Information für neue Angriffe
- *“It's the difference between letting random folks call your company's switchboard and ask for John Q. Cubicle's phone number [versus] sending them a copy of your corporate phone directory”*
- DNSSec mit NSEC kann möglicherweise nicht legal in allen Ländern eingesetzt werden

NSEC3 RR

- Zusicherung, dass ein Name nicht exisitiert ohne Namen der Zone offenzulegen
  - NSEC3 RR enthalten Hashwerte an Stelle von Name
- Anfrage vergleicht Hash des angefragten Namens mit den Hashwerten der Antwort
  - Hash ungleich der beiden Hashwerte ➔ Name exisitert nicht in der Zone

DNSSec Paketformat

- Antwort des TLD
  - QR = 1: Antwort
  - AA = 0: nicht authorativ
  - RA = 0: Rekursion nicht unterstützt
- Delegierung
  - Liste von NS für nächsten Rekursionsschritt (Authority Count = 2)
  - List von A-Records für diese NS (Add Record Count = 2)
- Anfrage-Antwort Verknüpfung
  - NS hält Liste von ausstehenden Anfragen (Query-ID)
  - Ignorieren von Antworten ohne Query-ID in Liste



„dig +trace www.neclab.eu any +multiline +all +answer"

Offene Punkte

- Größere DNS-Pakete
  - Firewalls filtern DNS-Pakete größer als 512Byte
- Höhere Last auf Nameservern
  - Krypto-Operationen führen zu langsamern Auflösung
  - DDoS-Angriffe
- Anwednungsverhalten bei DNSSec Problem unklar
  - Definition von Fehlerverhalten
- Zeitsynchronisation der DNS-Server

- Erfahrung
  - Konfiguration
  - Betrieb

Literatur

- [2.1] “**Off-the-record communication, or, why not to use PGP”**, Nikita Borisov, Ian Goldberg, Eric Brewer; Workshop On Privacy In The Electronic Society, Pages: 77 – 84, 2004; http://doi.acm.org/10.1145/1029179.1029200