Die Dinge „beim Namen“ nennen ...

D N S

G r u n d l a g e n , M ö g l i c h k e i t e n u n d A t t a c k e n

Über mich

- Stefan Neufeind
- Aus Neuss
- Tätig für SpeedPartner GmbH (Consulting, Entwicklung, Administration)
  - Hosting, Housing, Managed Services
  - XDSL, IP-Upstream, IPv6
  - Domains / Domain-Services

Agenda

- Grundlagen
- Einsatzszenarien
- Attacken (Auswahl) und mögliche Absicherungen
  - Zonetransfers
  - Offene Recursor
  - Injection
- Offene Diskussion

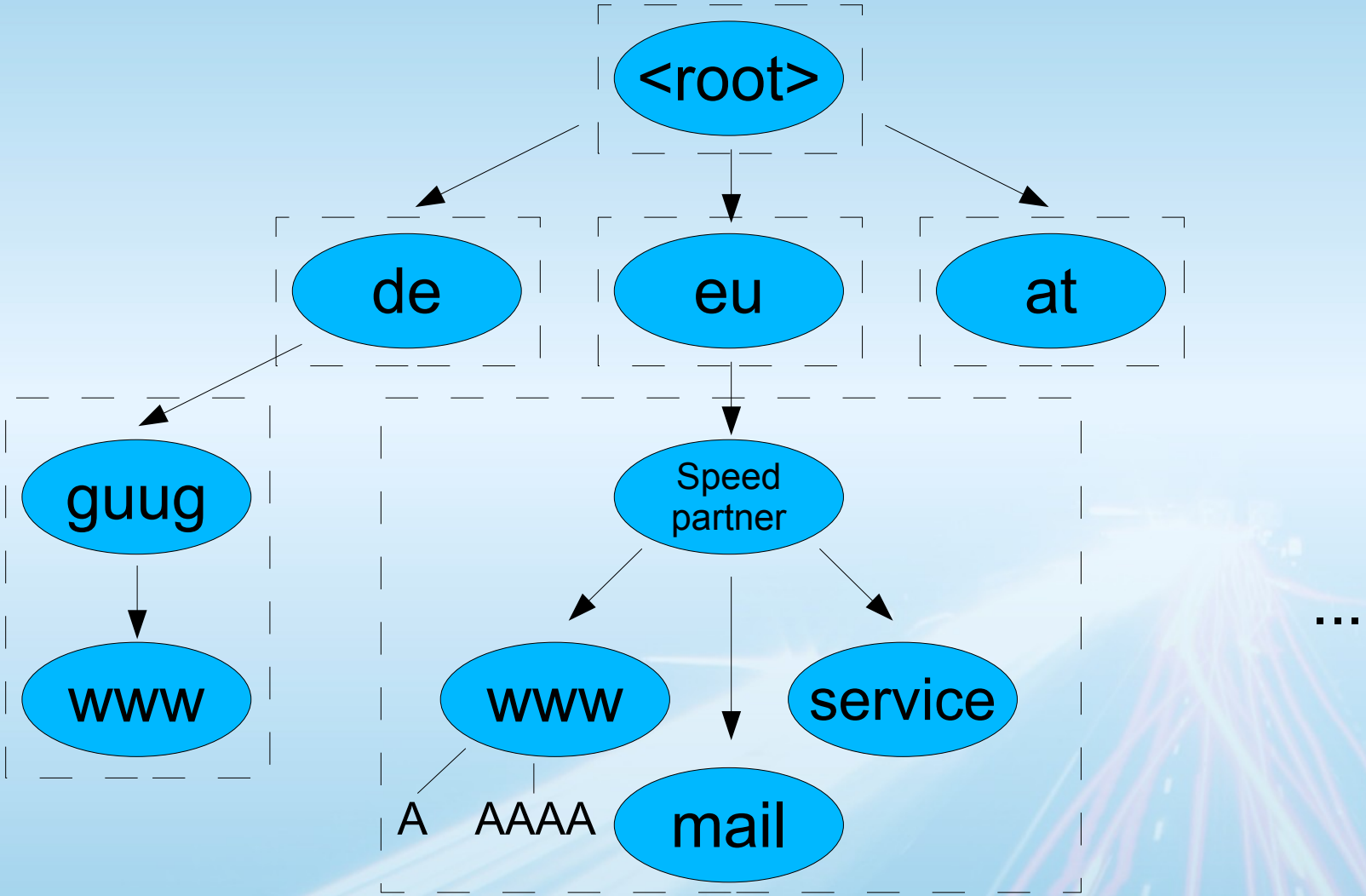
Grundlagen

- DNS = Domain Name System
- „Telefonbuch“ für Netzwerke
- Verbindung Domain-Namen mit Informationen
  - „menschen-lesbare“ Hostnamen
  - Verknüpfung mit verschiedenen Informationen/Diensten

Grundlagen

- Hierarchisch strukturiert (Baum)
  - Pro Knoten/Blatt: 0 bis n Resourcen mit Informationen
- Aufgeteilt in Zonen
  - Enthalten Sammlung zusammenhänger Knoten
  - Mehrere Zonen pro Nameserver möglich
  - Bereitgestellt durch authoritative Nameserver

Grundlagen



Grundlagen

- DNS-Client: Resolver
  - Nicht-rekursive Anfrage: Schritt für Schritt entlang Baum
    - z.B. lokalen caching-nameserver installieren
  - Rekursive Anfrage: Recursor übernimmt Auflösung
    - Einfachere Realisierung
    - Spart Resourcen
    - Erlaubt Caching
    - z.B. über DNS-Server des Internet-Zugangsanbieters

Grundlagen

- Anfragen per
  - UDP: einfache Anfragen, für Antworten bis 512 Bytes
    - Mit Erweiterung auch größere Antworten möglich (EDNS, siehe RFC2671)
  - TCP: für komplexe Anfragen, Zonetransfers, ...

Einsatzszenarien: Beispiel-Anfragen

- Hostname zu IP:
  www.guug.de A → 212.227.83.207
  www.linuxtag.org AAAA → 2a01:198:12::13
- IP zu Hostname (Reverse):
  207.83.227.212.in-addr.arpa. PTR → p15193709.pureserver.info.
  (an der shell: dig -x 212.227.83.207)
- Abfrage von Diensten (Beispiel: Jabber-Server):
  _xmpp-server._tcp.speedpartner.de SRV →
  10 0 5269 collab.speedpartner.de

  (Angabe über Verfügbarkeit von Dienst, ggf. mehrere Server mit Priorität/Gewichtung, Port und Server für Verbindung)

Einsatzszenarien: Beispiel-Anfragen

- Abfrage von Zusatzinfos:
  qupps.biz TXT → zone transfers for this zone have been [...]

  _domainkey.example.com TXT → o=~\; r=hostmaster@example.com
  mail._domainkey.example.com TXT → k=rsa\; t=y\; p=MHwwDQYJ[...]

- Blacklist-Abfragen (dnsbl, z.B. für Spam-Vermeidung):
  14.33.110.85.ix.dnsbl.manitu.net A → 127.0.0.2
  14.33.110.85.ix.dnsbl.manitu.net TXT
  → A message sent to the mailhost [...] was detected as spam by NiX Spam at Tue, 12 Aug 2008 15:54:54 +0200

- Tunneln von beliebigem Traffic über DNS
  ... falls man gerade mal nur DNS zur freien Verfügung hat :-)

Attacken (Auswahl)

- Zonetransfers
  - Massentransfer aller Inhalte einer Zone
  - „verrät“ auch versteckte Einträge

www.example.com.	86400	IN	A	10.0.0.1
ftp.example.com.	86400	IN	A	10.0.0.2
[...]				
vpn.example.com.	86400	IN	A	10.210.9.8
db.example.com.	86400	IN	A	10.212.37.11
backup.example.com.	86400	IN	A	10.244.51.45
secret-project.example.com.	86400	IN	A	10.251.73.91

Attacken (Auswahl)

- Zonetransfers
  - Abhilfe: Unnötige Zonetransfers verbieten

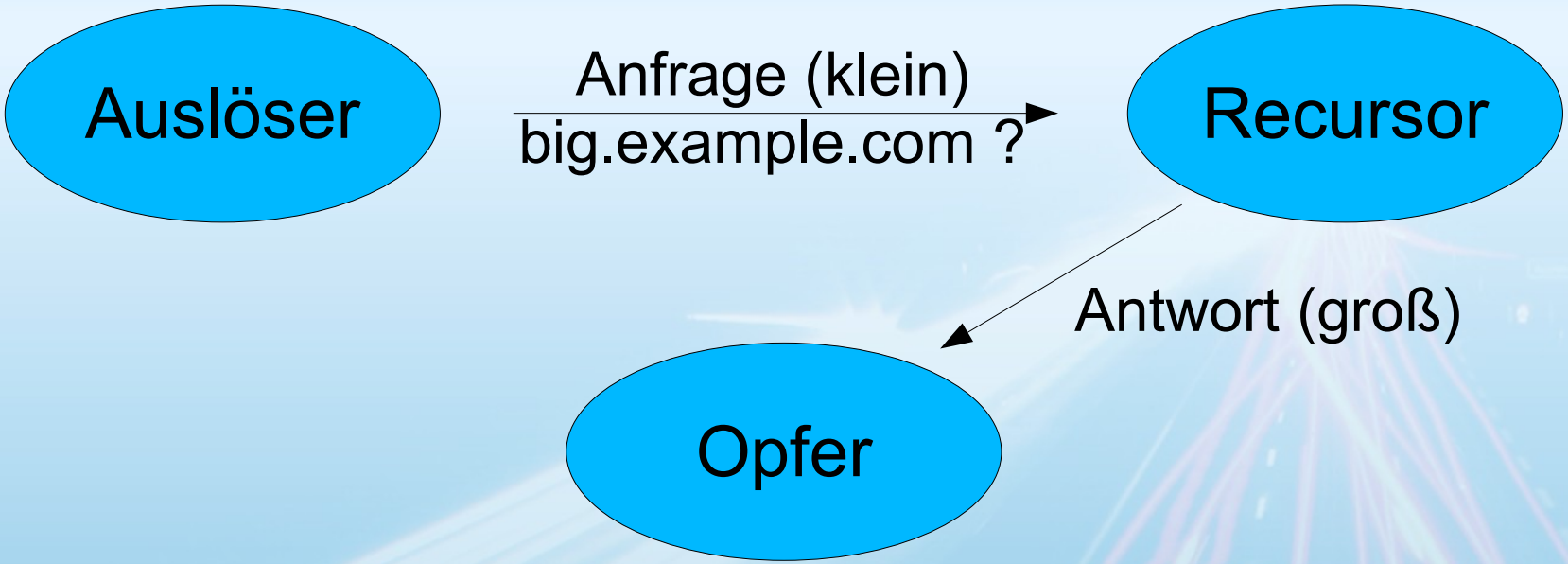
Bind: /etc/named.conf

```
acl slave-dns {
        192.168.7.33;
        192.168.99.8;
};
options {
  allow-transfer { slave-dns; };

[...]
```

Attacken (Auswahl)

- Offene Recursor
  - Anfrage per UDP: Fälschung Absender möglich
  - Beliebige Abfrage, da offener Recursor:
    Abfrage mit großer Antwort stellen



Attacken (Auswahl)

- Offene Recursor
  - Effekt: Denial of Service (DoS) im Eigenbau
    - Kleine Abfragen = geringe Bandbreite notwendig
    - Große Antworten = große Wirkung
    - Fälschung Absender =
      Antworten an beliebiges „Opfer“, Auslöser unerkannt
    - Nutzung Recursor als „Angreifer“ =
      ggf. hohe Bandbreite, Auslöser unerkannt

Attacken (Auswahl)

- Offene Recursor
  - Abhilfe:
    Nur Antworten für eigene Domains,
    Recursor nur für notwendige Clients

Bind: /etc/named.conf

```
acl our-clients {
        192.168.7.0/24;
};
options {
  allow-recursion { our-clients; };
  allow-query { our-clients; };
[...]
```

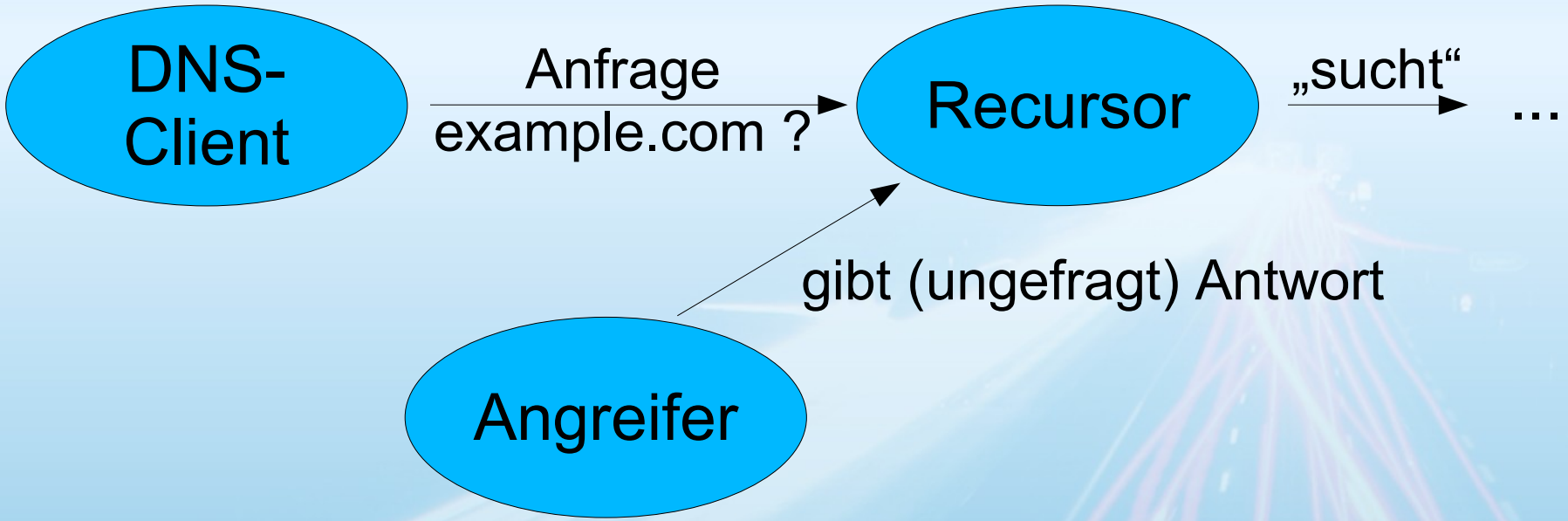
Bind: /var/named/named.primary

```
zone "example.com" IN {
    type master;
    file "zone.example.com";
    allow-query { any; };
};

[...]
```

Attacken (Auswahl)

- Injection
  - Unterschieben einer gefälschten Antwort



Attacken (Auswahl)

- Injection
  - Thema aktuell (erneut) heiss diskutiert
    - Dan Kaminsky plante Vortrag zur Black-Hat-Konferenz
    - Details vorab veröffentlicht (z.B. Full-Disclosure-Mailingliste)
    - Einige Newsmeldungen zum Thema
      - Heise 22.7.: Hinweis auf Sicherheitsproblem
      - Heise 28.7.: Nameserver DTAG und Kabeldeutschland bisher ungepatched; betrifft auch andere (z.B. Teilweise 1&1)
      - Heise 31.7.: Patches Bind 9.5.0-P1 bremsen Server aus
      - ...

Attacken (Auswahl)

- Injection
  - Denkbare Gründe:
    - Stören von Zugriffen
    - Man-in-the-middle-Attacken
  - Effektivität:
    - Erfolgreiche Störungen werden gecached
    - Injection auf Recursor mit Auswirkung auf viele Clients
    - Auch Angriffe auf „vernachlässigte“ Clients möglich

Attacken (Auswahl)

- Injection
  - Warum/wann/wie:
    - Bei ausgehender Anfrage speziell hierfür Injection?
      - Zeitpunkt muss abgepasst werden
      - Anfragen werden gecached
    - Bei beliebiger Anfrage ungefragt Antwort senden?
      - Denkbar, wird aber über Prüfung meist abgefangen (Bailwick-Checking, out-of-bailwick-Attacke)

Attacken (Auswahl)

- Injection
  - Warum/wann/wie:
    - Antwort „passend“ zur Anfrage
      - „in-bailwick“, also bailwick-Prüfung erfolgreich
      - Provozieren von Anfragen für z.B. aaa.example.com, bbb.example.com, ... und Lieferung passender „Additional Resource Records“ (z.B. für www.example.com)

Attacken (Auswahl)

- Injection
  - DNS-Antwort muss zu Anfrage passen:
    - Quelle der Antwort (DNS-Server)
    - Quell-Port DNS-Client (<16 Bit)
    - Transaktions-ID (16 Bit)
  - Problem:
    - Quell-Port DNS-Client ggf. vorhersagbar, da häufig wiederverwendet oder geringe Anzahl Variationen
    - Transaktions-ID erratbar oder gar vorhersagbar (BIND v4 und v8 verwendeten sequentiellen IDs)

Attacken (Auswahl)

- Injection
  - Aussicht auf Erfolg
    - Oft keine Filterung nach Source-IP von Traffic (siehe BCP38)
      - Viele ISPs noch nicht
      - Oft keine Filterung im LAN zum Recursor ob gespoofte Adressen externer, authoritativer Server genutzt
    - Anzahl Versuche „überschaubar“: worst-case <16 Bit, best-case <32 Bit

Attacken (Auswahl)

- Injection
  - Angriff per „man-in-the-middle“ falls Injection erfolgreich?
    - Falls keine Verschlüsselung verwendet
    - Falls keine andere Form der Authentifizierung (SSL mit Prüfung) verwendet wird oder
    - Falls Authentifizierung falsch verwendet wird (Klick auf "Zertifikat trotzdem akzeptieren")

Attacken (Auswahl)

- Injection
  - Probleme bei Filterung
    - Gefälschte Antworten kommen mit IP der echten, authoritativen Server
      (können also nicht einfach "geblockt" werden)
    - rate-limits o.ä. ggf. problematisch für legitime Nutzer
      (keine Auflösungen mehr möglich)
    - Auch Clients „verwundbar“, nicht nur Recursor
      - Angreifer direkt im LAN? Infizierte Hosts? ...

Attacken (Auswahl)

- Injection
  - „Lösung“ über Monitoring?
    - Monitoring Recursor auf massenhafte Anfragen
    - Monitoring Recursor auf massenhaft falsche Query-IDs in Antworten (Counter bei Bind z.B. ab 9.5 verfügbar)
    - Monitoring LAN auf lokale Attacken (sflow, ...)
    - Jedoch nur Indizien, keine Problemlösung

Attacken (Auswahl)

- Injection
  - „Lösung“ über TCP-Fallback? (bereits 2006 erwähnt)
    - wenn gefälschte IDs erkannt,
      weitere Anfragen per TCP statt UDP
    - Performance/Skalierung? ...
  - „Lösung“ über DNSSEC?
    - Alle DNS-Zonen ab Root müssten signiert sein
    - Client (oder mind. vertrauenswürdiger Resolver)
      müssten Prüfung der Kette vornehmen
    - Performance?

Attacken (Auswahl)

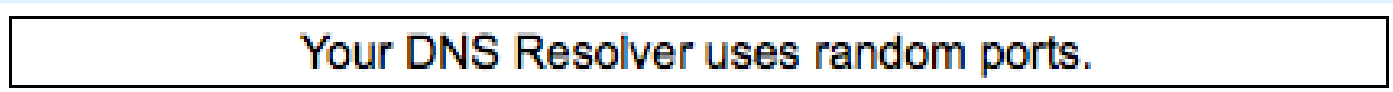
- Injection
  - „Abhilfe“
    - Patches einspielen
    - Filtern wo möglich
    - Monitoring
    - DNSSEC?

Attacken (Auswahl)

- Injection
  - Stolperfallen
    - NAT für DNS
      kann ggf. zufällige Source-Ports o.ä. verwässern
    - Auch Clients oder z.B. kleine Router anfällig
    - Tests „mit Vorsicht“ zu genießen

Attacken (Auswahl)

- Injection
  - Testmöglichkeiten
    - Automatisches DNS-Testbild
      http://porttest.honeyd.org/-s-_dns.png



    - Per DNS-Abfrage auf TXT-Record

```
# dig +short porttest.dns-oarc.net TXT
  z.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
  "217.237.150.202 is POOR: 27 queries in 4.8 seconds from 26 ports with std dev 160.37"

# dig +short @my.nameserver.net porttest.dns-oarc.net TXT
  porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
  "80.69.100.142 is GREAT: 26 queries in 4.2 seconds from 26 ports with std dev 16735"
```

Weitere Links

- Injection-Attacken

http://seclists.org/fulldisclosure/2008/Jul/0375.html

http://www.heise.de/security/Details-zum-DNS-Sicherheitsproblem-veroeffentlicht--/news/meldung/113133

http://www.net-security.org/dl/articles/Attacking_the_DNS_Protocol.pdf

http://www.nytimes.com/2008/08/09/technology/09flaw.html

http://tservice.net.ru/~s0mbre/blog/devel/networking/dns/2008_08_08.html

http://de.wikipedia.org/wiki/DNSSEC

Danke fürs Zuhören!

Folien verfügbar unter:

http://talks.speedpartner.de/

Fragen?
neufeind (at) speedpartner.de