Secure Domain Name System

DNSSEC

Einführung und Überblick in die Funktionsweise

Secure Linux Administration Conference
Berlin
2. Dezember 2011

Holger.Zuleger@hznet.de

Agenda

- DNS / DNSSEC
  - Bedeutung DNS
  - Historie und Verbreitung
- Überblick
  - Angriffszenarien
  - DNSSEC Arbeitsweise
- DNSSEC en détail
  - Signaturen
  - Schlüssel Erzeugung und Austausch
  - DS Records
- Operative Herausforderungen
- Werkzeuge
- Anwendungen
- Referenzen

Bedeutung DNS

- DNS ist das grundlegende Protokoll im Internet
- Nahezu alle anderen Protokolle bedienen sich dem DNS
  - Web
    `http://www.example.net`
  - Mail
    `Max.Muster@example.net`
  - VoIP / ENUM
    `mm@sip.example.net`, `1.5.6.7.4.1.5.3.e164.arpa`
- DNS ist dabei für den Anwender nicht sichtbar
- Über 25 Jahre alt
  Grundlegende Sicherheitsprobleme bereits 1990 bekannt
- Problem:
  Ist DNS angreifbar sind auch andere Protokolle angreifbar

DNSSEC Historie

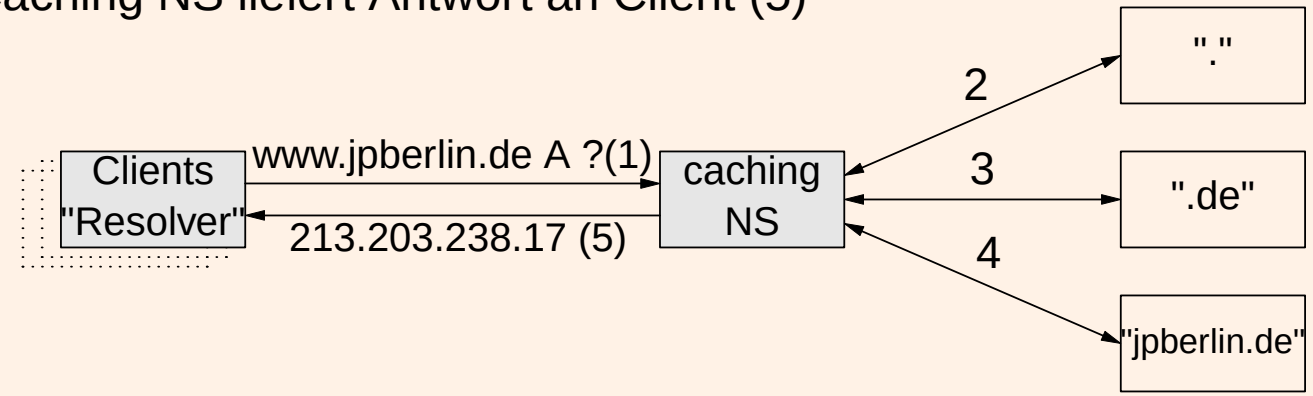
- DNS kommt aus dem Jahr 1987
  Grundlegende Sicherheitsprobleme bereits 1990 bekannt
- Arbeit an DNSSEC beginnt 1995 und endet (vorläufig) 1999
  RFC2535
- Neuausrichtung im März 2005
  RFC4033, RFC4034, RFC4035
- Weitere Ergänzungen notwendig
  - Operational Practices (RFC4641) September 2006
  - Automatisierte Trust Anchor Updates (RFC5011) September 2007
  - NSEC3 (RFC5155) November 2008
  - Neue Key Algorithmen und Signaturen ...
- „Rollout“ seit 2005
  Erste signierte TLD ist `.se`

DNSSEC Verbreitung

- Erste signierte TLD war `.se` im Jahre 2005
- Root Zone ist seit Mitte 2010 signiert
- Insgesamt sind aktuell ca. 84 (78 mit DS Records) TLD signiert
  http://stats.research.icann.org/dns/tld_report/
- Beispiele
  - Die drei wichtigsten TLDs: `.com` `.net` `.org`
  - Deutschland (`.de`) seit 31. Mai 2011
  - Reverse Tree
    `in-addr.arpa`, `ip6.arpa`
  - ENUM root Zone `e164.arpa`
- SecSpider zählt ca. 36.000 DNSSEC Domains weltweit
  http://secspider.cs.ucla.edu/

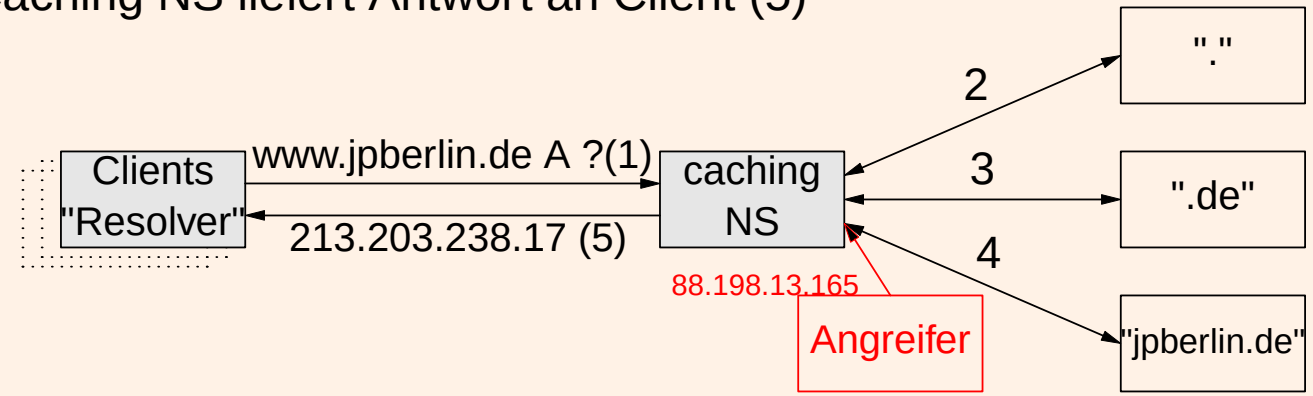
Angriffszenarien DNS

- Clients (Resolver) senden DNS Anfragen an Caching Nameserver (1)
- Caching NS ermittelt Antwort von authoritativen Nameserver (2,3,4)
- Caching NS liefert Antwort an Client (5)



Angriffszenarien DNS

- Clients (Resolver) senden DNS Anfragen an Caching Nameserver (1)
- Caching NS ermittelt Antwort von authoritativen Nameserver (2,3,4)
- Caching NS liefert Antwort an Client (5)



- DNS verwendet (meist) UDP
  - Einfaches Frage/Antwort Protokoll (2 Datenpakete)
  - Angreifer sendet Antwortpaket bevor es von authoritativem NS kommt
  - Cache poisoning
  - Alle Clients dieses Caching Nameservers bekommen falsche Antworten

- Cache Poisoning erlaubt Umleitung des Datenverkehrs
  Pharming Attacke

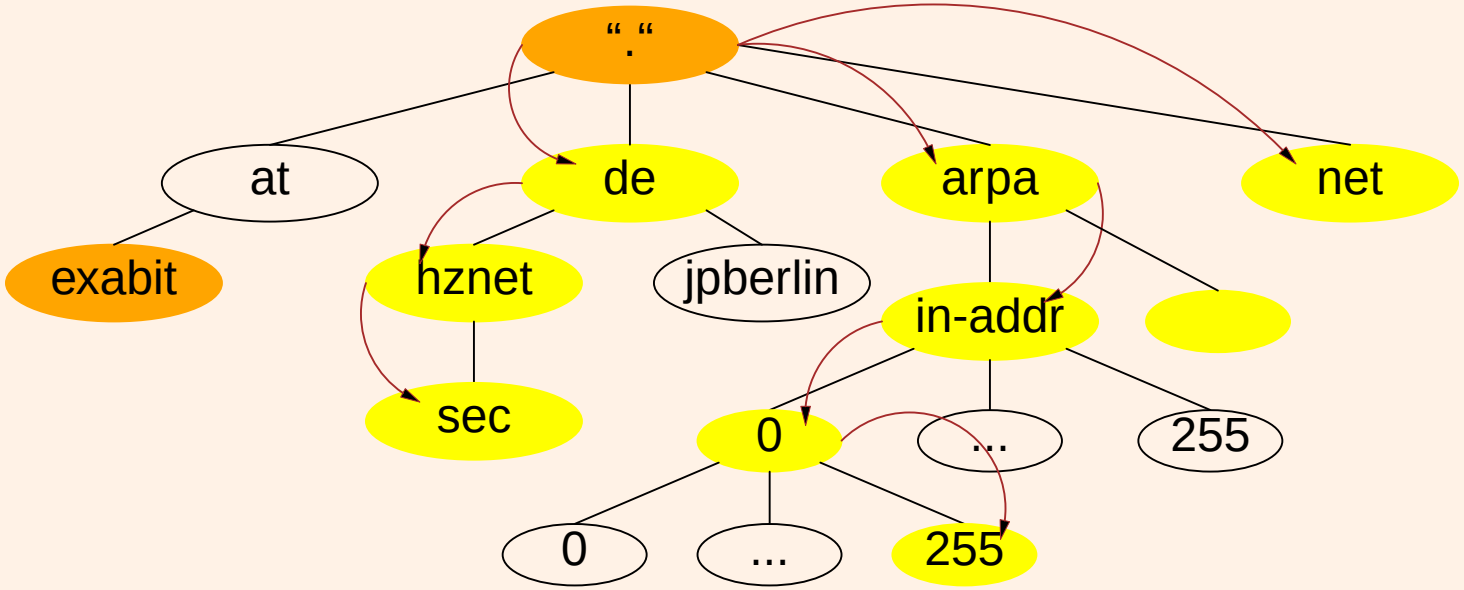
DNSSEC in a nutshell

- Domainverwalter signiert die „Domain“
  - Alle Datensätze der Domain (RR) erhalten eine Signatur (RRSIG)

```
www.jpberlin.de. 3600 A     213.203.238.17
                 3600 RRSIG A 5 3 3600 20111125061804 20111225061804 \
                              30377 jpberlin.de. R6zAmblKm4GJc+2FI9Y/0...
```

  - Für die Erzeugung der Signaturen benötigt man Schlüssel (DNSKEY)
- DNSSEC fähige (Caching) Resolver setzen DO-Bit in der Anfrage
  - Antwortpaket enthält zusätzlich die RRSIG Information
  - Resolver kann Antwort überprüfen (validieren)
  - Zur Validierung wird ein Trust Anchor benötigt (Schlüssel der Root Zone)
- Caching Resolver setzt AD-Bit in der Antwort zum Client
  - Client sieht ob Domain validiert wurde
  - Wird heute bereits von ssh genutzt
- „Chain of Trust“ bis zur Root vorteilhaft
  Verkettung über DS Records

Chain of Trust



- Chain of Trust wird durch DS Records gebildet
  Eltern Zone beinhaltet (signierten) Zeiger auf DNSKEY der Kindzone
- Der (validierende) Resolver bekommt „Trust Anchor“ konfiguriert
  Idealerweise nur den TA der Root Zone

Secure Resolving Nameserver

- „Resolving“ oder „rekursive“ Nameserver lösen Namen auf
  Bisher war immer auch von Caching Nameserver die Rede

- DNSSEC fähige resolving NS nennt man Validator
  Validator benötig (mindestens) Trust Anchor der Root Zone

```
options {
    recursion yes;
    dnssec-enable yes;
    dnssec-validation yes;
    managed-keys {
    "."   initial-key  257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJ
                    FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2
                     ...
                    Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N
                    QxA+Uk1ihz0=" ;
    };
};
```

- BIND und unbound verfolgen Rollover des Root Keys vollautomatisch
  RFC5011

DNSSEC Details: Signaturen

- Jeder Recordset (Datensatz) bekommt eine Signatur (RRSIG)

```
$ORIGIN example.net.
@     MX     10 mail.example.net.
      RRSIG  MX 5 2 10800 20111225190145 20111125190145 45222 example.net. o5X1P9aj...
mail  A      1.3.2.5
      RRSIG  A 5 3 10800 20111225190145 20111125190145 45222 example.net.  YRx7FvFQ...
mail  AAAA   2001:db8:1::25
      RRSIG AAAA 5 3 10800 20111225190145 20111125190145 45222 example.net. AmFsdl4...
```

- Signatur hat Gültigkeitsdauer (Start- und Endezeitpunkt)
  Vor Ablauf der Signatur neu signieren
- Per Zone Signing
  - Alle RRSIG haben gleiche Gültigkeitsdauer
  - Gut für „kleine“ Domains oder bei geringer Änderungshäufigkeit
- Per Record Signing
  - RRSIG haben unterschiedliche Gültigkeitsdauer
  - Nötig bei dynamischen Domains (hohe Änderungshäufigkeit)

DNSSEC Details: Schlüsselmaterial

- Für die Signaturen werden asymetrische Schlüssel benötigt
  Öffentlicher Teil des Schlüssel wird in der Domain veröffentlicht (DNSKEY)
- Zwei Arten von Schlüssel
  - Key Signing Key (KSK)
    Nur zum Signieren des Schlüsselmaterials (DNSKEY Records)
  - Zone Signing Key (ZSK)
    Zum Signieren aller anderen Datensätze (ausser delegierte NS Records)
- Gründe für mehrere Schlüssel
  a. Einfacheres Keyrollover
     - ZSK Rollover kann autark durchgeführt werden
     - KSK Rollover bedeutet Schlüsseltauch mit Parent
  b. Unterschiedliche Schlüsselspeicherung
     - KSK offline / Hardware Security Modul
     - ZSK online

DNSSEC Details: Schlüsseltausch

- Keyrollover ist operative Herausforderung
  - Caching der Antworten erfordert genaues Timing beim Rollover
  - Bei KSK Rollover kommt Kommunikation und Timing beim Parent dazu
  - Ohne geeignete Werkzeuge schwierig zu managen
- 6 verschiedene Rollover Varianten (3 pro Schlüsseltyp)
  Schnelligkeit, Zonengröße, Kommunikationsaufwand, Komplexität
- Klassiker (RFC4641)
  - Double Signature (KSK)
  - Pre-Publish (ZSK) (Für ZSK rollover am besten geeignet)
- Notfall Rollover
  Ein Standby Key vereinfacht (beschleunigt) i.A. einen Notfall Rollover
- Algorithm Rollover
  - Bei gutmütiger Auslegung von RFC4035 über Double Signature
  - Bei konservativer Auslegung ist spez. Mechanismus nötig (RFC4641bis)

DNSSEC Details: DS Records

- Parent benötigt „Zeiger“ auf den DNSKEY (KSK) in der Child Domain
  Delegation Signer Record (DS)
- DS findet sich ausschließlich in der Parent Domain

```
$ORIGIN net.
example  DS 31589 8 1 628FCA4806B2E475DA9FD97A1FB57B7E26F8494C
example  DS 31589 8 2 5A9EAEFC7CC7D6946E1D106418427D272D406B835BA9EA0219DFBD39...
```

- Parent signiert Child DS mit seinem Key
  ☞ Chain of Trust
- Parentkommunikation für Informationsaustausch ist nicht standardisiert
  - Übergabe des DS oder des DNSKEY?
  - EPP kennt DS Erweiterung (RFC5910)
  - Übergabe des DNSKEY ist optional
  - Nicht alle TLDs verwenden EPP (z.B. .de)

Operative Herausforderungen

- Zeitsynchronisation notwendig
  - Für TSIG im Bereich von Minuten
  - Für Resolver im Bereich von Stunden
- Regelmäßiges Signieren
  - Wann? (z.B. alle 7 Tage)
  - Gültigkeitsdauer? (z.B. 10 Tage)
  - TTL Werte beachten (z.B. 2 Tage)
  - Backup der Zone allein reicht nicht
- Fehler beim Signieren (z.B. falscher Key) sind nicht „rückholbar“
- Monitoring (nagios-plugin)
  Erreichbarkeit reicht nicht mehr aus
- Häufigere Kommunikation mit Parent (registry/registrar) nötig
  Bei jedem KSK Rollover

DNSSEC Werkzeuge

- BIND (bis 9.7)
  - Zwei Kommandos zur Schlüsselerzeugung und zum Signieren
  - Nicht ausreichend für produktiven Betrieb
  - Mindestens Skripte für autom. Resigning notwendig
- Zone Key Tool (http://www.zonekeytool.de)
  - Wrapper um die BIND Kommandos
  - Automatisches Resigning (Per Zone signing) inkl. SOA serial Erhöhung
  - Automatischer ZSK und KSK rollover
  - Zonendatei unverändert / „Human readable“
- OpenDNSSEC (http://www.opendnssec.org)
  - Profitool / Wird von vielen TLDs verwendet
- BIND ab 9.7 (http://www.isc.org)
  - Automatisches Resigning (dynamische Zonen)
  - Vereinfachte Schlüsselverwaltung
  - Kein automatischer Key Rollover
  - Inline signing (ab BIND 9.9)

DNSSEC Anwendungen

- Sichere Namensauflösung
  Findet im Hintergrund statt
- Firefox Plugin macht DNSSEC sichtbar
  `http://www.dnssec-validator.cz/`

DNSSEC Anwendungen (2)

- SPAM Schutz
  - DKIM / SPF Records im DNS
  - Unterschiedliche Kategorisierung abhängig von DNSSEC Validierung
- SSH
  - SSH Fingerprints werden im DNS hinterlegt (SSHFP)
  - Validierung beim Zugriff auf den SSH Server
- DNS als authentische Quelle von Schlüsselmaterial
  - Opportunistic IPSEC
  - PGP Keys im DNS
- Ersatz für Zertifikate (DANE)
  - Kein Binding Firma $\Rightarrow$ Domain
    Aber dies ist auch bei Zertifikaten häufig nicht gegeben
  - Ausschließlich Binding NAME bzw. IP $\Rightarrow$ Schlüssel
  - Noch nicht sehr verbreitet

References

RFCs
- 1035 (Domain Names - Implementation and Specification)
- 3833 (Threat Analysis of the Domain Name System)
- 3658 (Delegation Signer (DS) Resource Record (RR))
- 4033 (DNS Security Introduction and Requirements)
- 4034 (Resource Records for the DNS Security Extentions)
- 4035 (Protocol Modifications for the DNS Security Extensions)
- 4641 (DNSSEC Operational Practices)

Drafts
- DNSSEC Operational Practices, Version 2
  draft-ietf-dnsop-rfc4641bis-08
- DNSSEC Key Timing Considerations
  draft-ietf-dnsop-dnssec-key-timing-02.txt
  draft-mekking-dnsop-dnssec-key-timing-bis-02.txt
- Using Secure DNS to Associate Certificates with Domain Names For TLS
  draft-ietf-dane-protocol-12

Links
- http://www.dnssec.net
- http://tools.ietf.org/wg/dnsop/
- http://tools.ietf.org/wg/dnssext/

Fragen ?

DNSsec, VoIPsec, IPsec, XMPPsec, SMTPsec, WLANsec ...

... DKIM, Kerberos, IMAP, LDAP, ENUM, SIP, ...

... NTP, DNS, DHCP, IPv6, Routing, Switching

Holger.Zuleger@hznet.de

CONTENTS