DNSSec - Intro

Wolfgang Jung (post@wolfgang-jung.net)

whoami

- einer der Micromata Gründer
- arbeite derzeit bei Polyas
- Schwerpunkte: Security, Infrastruktur, Linux, Scala

DNS-Intro 1

- Hierarchisches System
- „Liefere IP zu symbolischem Namen”
- UDP-basiert
- RFC-1034 - Nov.1987
- Zone file:

```
m451.de. 86400  SOA  ns.inwx.de.          # Start Of Authority
                     hostmaster.m451.de.  # Mail-Addresse
                     2018090901           # Serialnumber
                     10800                # refresh
                     3600                 # retry
                     604800               # expire
                     3600                 # TTL
m451.de. 86400  NS   ns.inwx.de.          # Nameserver
m451.de. 86400  NS   ns2.inwx.de.         # Nameserver
m451.de. 3600   IN A 185.11.138.5
m451.de. 3600   MX   100 mail.ideas-in-logic.de.
```

DNS-Intro 2

- Abfrage: www.m451.de (ohne qname-minimisation):

```
NS für www.m451.de -> x.root-server.net?: ".de -> NS a.nic.de"
NS für www.m451.de -> a.nic.de?: "m451.de -> NS ns.inwx.de"
A für www.m451.de -> ns.inwx.de?: "www.m451.de -> IN A 185.11.138.5"
```

- Nachteile: UDP basiert, nicht signiert
- Antwort kann von jedem geliefert werden
- Antwort muss nichts mit der Frage zu tun haben (MitM)

DNS-Intro 3

- Ursprüngliche RRs: SOA, NS, MX, A, PTR, HINFO?
- Referenzimplementierung BIND
- später Erweiterungen wie SPF, TXT, RRSIG, CDS, DNSKEY, TLSA... Siehe RRTypes
- RFCs liefern die Spec auf 2781 Seiten, siehe auch dieser Rant:

RFC 1034, Domain Names - Concepts and Facilities
RFC 1035, Domain Names - Implementation and Specification
RFC 1123, Requirements for Internet Hosts—Application and Support
RFC 1995, Incremental Zone Transfer in DNS
RFC 1996, A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
RFC 2136, Dynamic Updates in the domain name system (DNS UPDATE)
RFC 2181, Clarifications to the DNS Specification
RFC 2308, Negative Caching of DNS Queries (DNS NCACHE)
RFC 2672, Non-Terminal DNS Name Redirection
RFC 2845, Secret Key Transaction Authentication for DNS (TSIG)
RFC 3225, Indicating Resolver Support of DNSSEC
RFC 3226, DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 3596, DNS Extensions to Support IP Version 6
RFC 3597, Handling of Unknown DNS Resource Record (RR) Types
RFC 4343, Domain Name System (DNS) Case Insensitivity Clarification
RFC 4592, The Role of Wildcards in the Domain Name System
RFC 4635, HMAC SHA TSIG Algorithm Identifiers
RFC 5001, DNS Name Server Identifier (NSID) Option
RFC 5452, Measures for Making DNS More Resilient against Forged Answers
RFC 5890, Internationalized Domain Names for Applications (IDNA):Definitions and Document Framework
RFC 5891, Internationalized Domain Names in Applications (IDNA): Protocol
RFC 5892, The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)
RFC 5893, Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)
RFC 6891, Extension Mechanisms for DNS (EDNS0)
RFC 7766, DNS Transport over TCP - Implementation Requirements
Security
RFC 4033, DNS Security Introduction and Requirements
RFC 4034, Resource Records for the DNS Security Extensions
RFC 4035, Protocol Modifications for the DNS Security Extensions
RFC 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records
RFC 4470, Minimally Covering NSEC Records and DNSSEC On-line Signing
RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors
RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
RFC 5910, Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
RFC 5933, Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
RFC 7858, Specification for DNS over Transport Layer Security (TLS)
Experimental
RFC 1183, New DNS RR Definitions
Best Current Practices
RFC 2182, Selection and Operation of Secondary DNS Servers (BCP 16)
RFC 2317, Classless IN-ADDR.ARPA delegation (BCP 20)
RFC 5625, DNS Proxy Implementation Guidelines (BCP 152)
RFC 6895, Domain Name System (DNS) IANA Considerations (BCP 42)
RFC 7720, DNS Root Name Service Protocol and Deployment Requirements (BCP 40)
Informational
RFC 1178, Choosing a Name for Your Computer (FYI 5)
RFC 1591, Domain Name System Structure and Delegation
RFC 1912, Common DNS Operational and Configuration Errors
RFC 2100, The Naming of Hosts
RFC 3696, Application Techniques for Checking and Transformation of Names
RFC 4892, Requirements for a Mechanism Identifying a Name Server Instance
RFC 5894, Internationalized Domain Names for Applications (IDNA):Background, Explanation, and Rationale
RFC 5895, Mapping Characters for Internationalized Domain Names in Applications (IDNA) 2008
RFC 7626, DNS Privacy Considerations
RFC 7706, Decreasing Access Time to Root Servers by Running One on Loopback

DNSSec - RFC 4033

- Jeder Nameserver signiert seine Antworten
- Jeder Nameserver kennt die Public Keys der untergeordneten Zone
- Neue RRs: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM
- Zwei Schlüssel pro Zone:
  ZSK (volatil, 14d Lebensdauer) &
  KSK (wird dem Parent mitgeteilt)
- KSK signiert sich selbst und ZSK. ZSK signiert alle Records (RRSIG)
- Vorteil: ZSK Key-Rollover kann ohne Mitarbeit der übergeordneten Zone erfolgen
- Vorteil: ZSK kann kurz sein (wichtig für schnelle Antworten)
- Nachteil: An der Root-Zone hängt alles

DNSSec - Rootzone/Trustanchor des Internets

The DNSSEC Root Signing Ceremony

Hier gibt es das 3h15m(!) Video der Zeremonie.

DNSSec - Abfrage

```
> delv +vtrace +mtrace A www.m451.de
;; fetch: www.m451.de/A
;; received packet from 192.168.1.4#53
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:  10286
;; flags: qr rd ra ad; QUESTION: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1252
;; QUESTION SECTION:
;www.m451.de.                   IN      A

;; ANSWER SECTION:
;www.m451.de.           2796    IN      A       185.11.138.5
;www.m451.de.           2796    IN      RRSIG   A 13 3 3600 (
;                                               20180922125042 20180908112042 13461 m451.de.
;                                               FwYUGXWl6ThYkFBWH4z3fSyMO3yv
;                                               O0HGRhb/tWYmCqxMsLQKVLAqfLX+
;                                               r1DTmueRHs+WCvmA0UCN15CfySmf
;                                               Wg== )


;; validating www.m451.de/A: starting
;; validating www.m451.de/A: attempting positive response validation
;; fetch: m451.de/DNSKEY
;; received packet from 192.168.1.4#53
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:  26443
;; flags: qr rd ra ad; QUESTION: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1252
;; QUESTION SECTION:
;m451.de.                       IN      DNSKEY
```

DNSSec - Antwort

```
www.m451.de. 3297 IN A     185.11.138.5
www.m451.de. 3297 IN RRSIG A   # Signatur zum A-Record
                13             # Signaturverfahren -> ECDSAP256SHA256
                3              # Name besteht aus 3 Komponenten
                3600           # TTL der Antwort
                20180922125042 # not valid before
                20180908112042 # not valid after
                13461          # Schlüssel ID
                m451.de.       # Name des Signierers
                FwYUGXWl6ThYk...SmfWg== # base64 signatur
```

DNSSec - Was bringt es denn nun?

- DNS Betreiber kann signierte Informationen zu seiner Domain liefern.
- IP-Adressauflösung als Standard
- Falls signiert, dann auch ok
- Beim MitM fehlt die Signatur oder löst nicht zum Root-Schlüssel auf
- MX Records zur Domain
- Aber auch: welche Namenseinträge gibt es nicht (NSEC3)
- Bester Anwendungsfall: DANE

DANE - Domain-authenticated named entities

- DNSSec stellt sicher, dass die Antwort von dem Inhaber des DNS der Domain kommt
- Publizieren des Fingerprints von Zertifikaten!
- Via TLSA Record:

```
_25._tcp.mail.ideas-in-logic.de. 3600 IN TLSA   3 1 1 AD1...28
_25._tcp.mail.ideas-in-logic.de. 3600 IN TLSA   2 1 1 60B...18
```

- Liefert den Fingerprint des Zertifikats des TLS Servers auf Port 25
- Domain-Validated Zertifikat ohne CA!
- Funktioniert nur mit DNSSec (ansonsten ist ja ein MitM möglich), Pflicht für EmiG.
- Lösung für Postfix: https://www.cs-ware.de/blog/archives/175

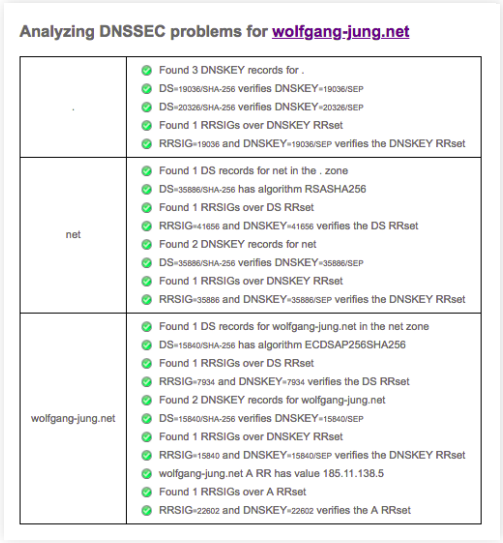
DNSSec - Ok, aber wie?

- Durch den DNS-Dienstleister (Private-Key liegt dann aber auch bei dem)
- Betrieb eigener DNS-Server, oder als hidden-primary
- BIND, powerdns oder knotdns
- knot:

```
policy:
  - id: "default"
    algorithm: "ecdsap256sha256"
    nsec3: "on"
    nsec3-iterations: "100"
template:
  - id: "default"
    storage: "/var/lib/knot/zones"
    notify: "slave"
    acl: [ "acl_slave", "deny_all" ]
    dnssec-signing: "on"
    dnssec-policy: "default"
    serial-policy: "dateserial"
```

Debugging

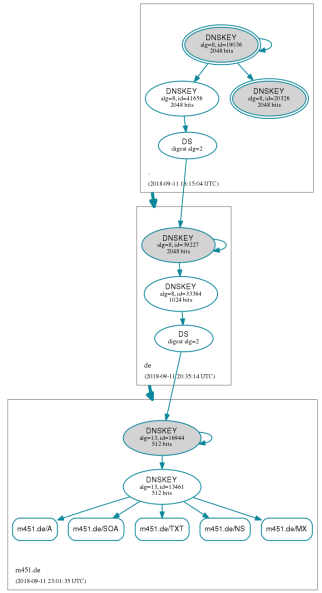
dnssec-debugger.verisignlabs.com



Analyzing DNSSEC problems for wolfgang-jung.net

.	Found 3 DNSKEY records for . DS=19036/SHA-256 verifies DNSKEY=19036/SEP DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
net	Found 1 DS records for net in the . zone DS=35886/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=41656 and DNSKEY=41656 verifies the DS RRset Found 2 DNSKEY records for net DS=35886/SHA-256 verifies DNSKEY=35886/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=35886 and DNSKEY=35886/SEP verifies the DNSKEY RRset
wolfgang-jung.net	Found 1 DS records for wolfgang-jung.net in the net zone DS=15840/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=7934 and DNSKEY=7934 verifies the DS RRset Found 2 DNSKEY records for wolfgang-jung.net DS=15840/SHA-256 verifies DNSKEY=15840/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=15840 and DNSKEY=15840/SEP verifies the DNSKEY RRset wolfgang-jung.net A RR has value 185.11.138.5 Found 1 RRSIGs over A RRset RRSIG=22602 and DNSKEY=22602 verifies the A RRset

dnsviz.net



delv (aus BIND9)

```
delv +vtrace +mtrace m451.de
```

Fragen?