DNSSEC

Stand der Einführung, Probleme und Entwicklungen

Datum:
25.3.2009

Otmar Lendl
Michael Braunöder

Programm

- Warum DNSSEC?
- Wie funktioniert DNSSEC?
- Alternativen?
- Was heißt es, DNSSEC einzuführen?

Fragen sind willkommen!

Danke an Olaf Kolkman, Phil Regnauld, … für die Erlaubnis, aus ihren Slides zu zitieren.

Warum überhaupt DNSSEC?

- Was macht das DNS so wichtig?
- Was sind die Angriffsszenarien auf das DNS?
- Der Kaminsky Attack.

DNS: Was ist das?

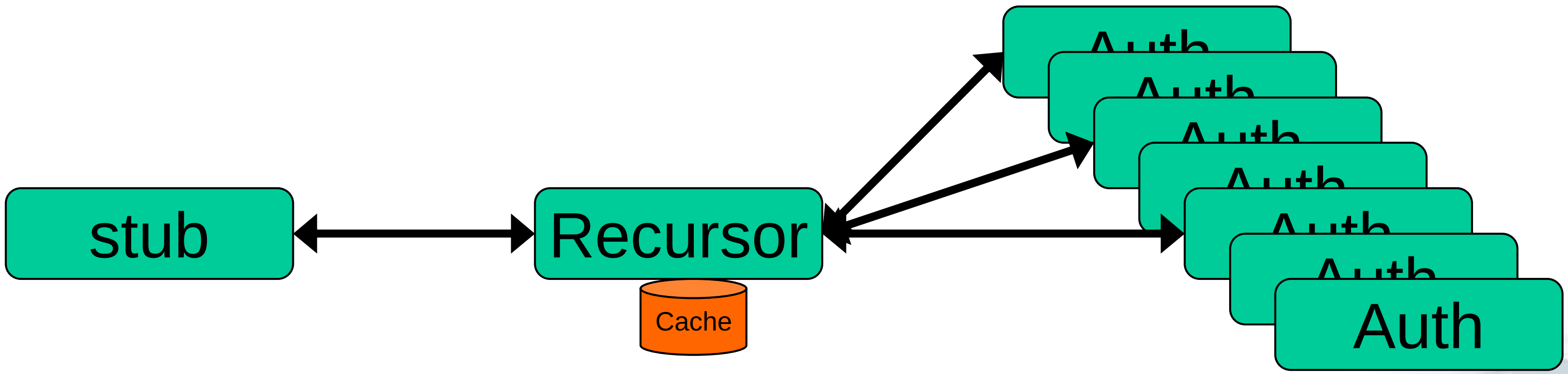
- Global, distributed Database
- Input: Domain name
- Output: Resource Record **Sets**
  - A, AAA — IP addresses
  - MX — Mail routing
  - CNAME — Aliasing
  - NS — Delegation
  - PTR, NAPTR, SRV,
  - RRSIG, DS, NSEC, NSEC3
- Transport: mainly UDP
- Lots of caching

DNS: Warum ist es wichtig?

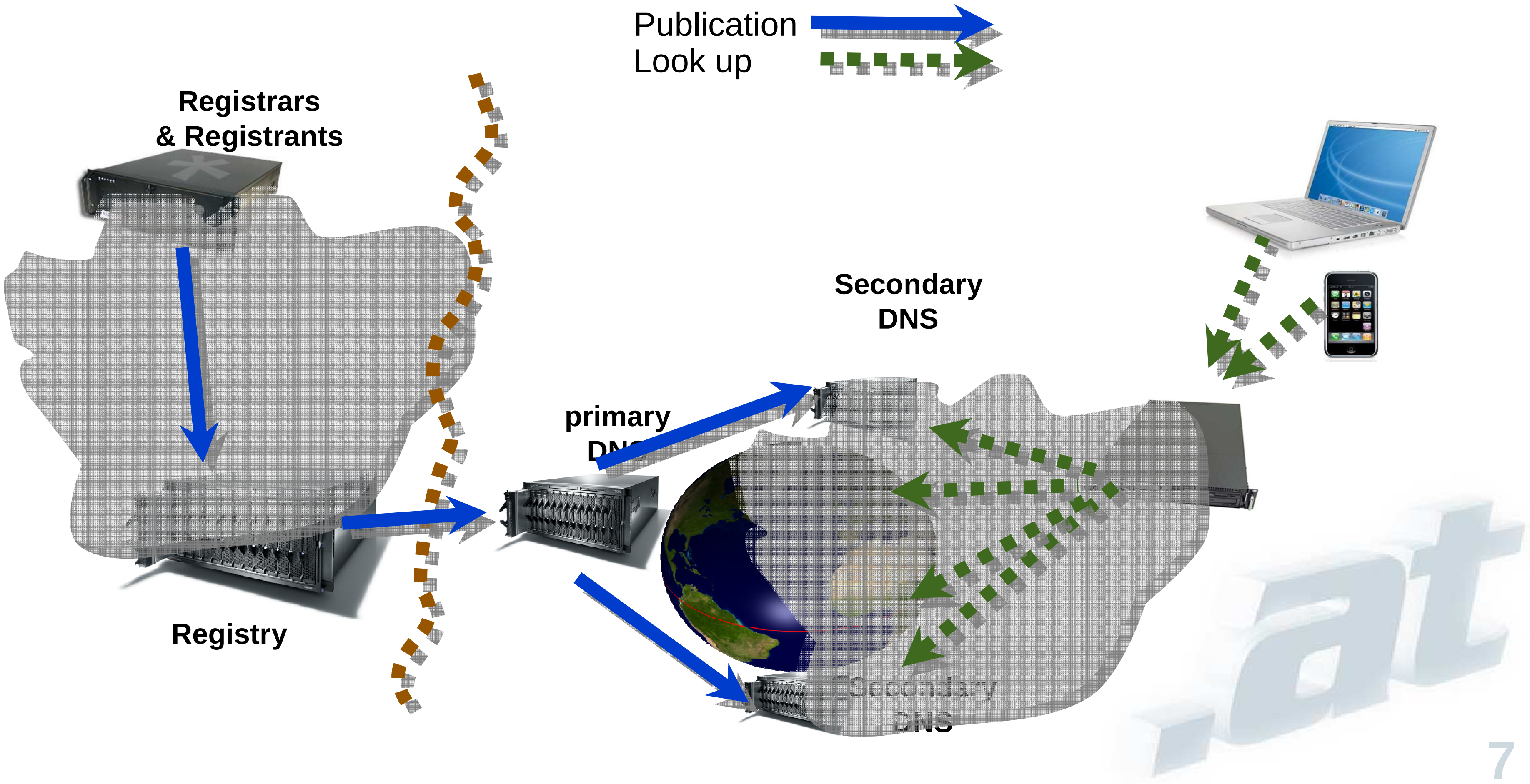
- DoS
- Man-in-the-middle almost *everything*
  - Phishing
  - Email hijacking
- Password reset emails
- Software Updates
- SSL and PKI for the rescue?
  - How do users react to X.509 errors?
  - CA email-loop
  - CA whois lookup
- Für den Enduser ist „DNS Kaputt“ nicht von „Internet ist kaputt“ unterscheidbar

Die Mitspieler

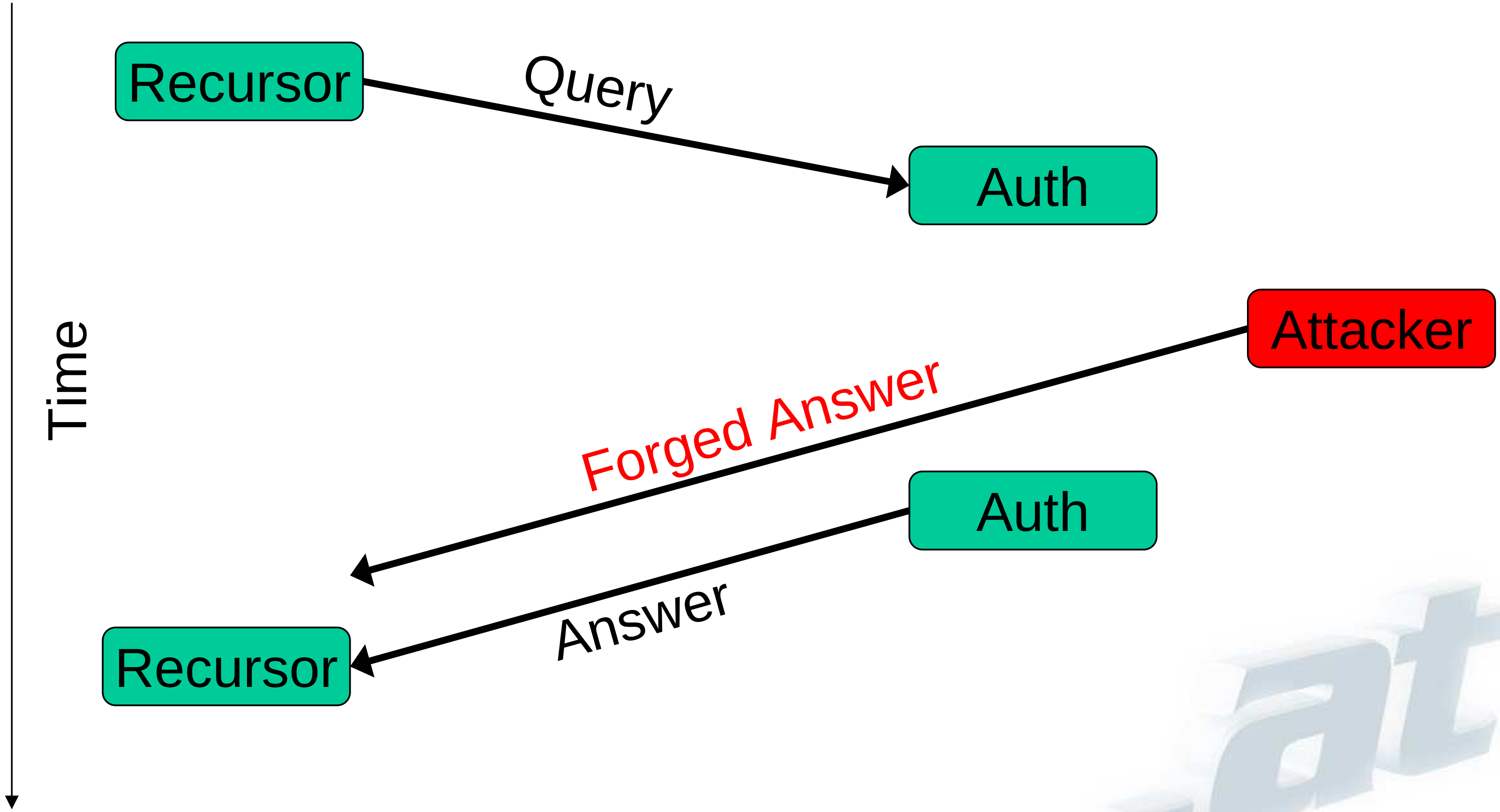
- Stub Resolvers
- Recursive Nameservers
- Authoritative Nameservers



Data flow through the DNS



DNS Spoofing



Gefahrenanalyse

- Cache poisoning
  - Off-path attacks
  - On-path attacks
- Name chaining
- Falsche Antwort durch den Recursor
  - Sitefinder
  - NXdomain monetizing

- Siehe auch RFC 3833

Cache Poisoning (off-path)

- Das ist nichts neues.
  - Kashpureff
  - Triviale Query-ID
  - Parallele Anfragen
- Berechnungen zur Erfolgswahrscheinlichkeit in RFC 5452

Pre-Kaminsky

- An attack needs to match
  - Question section
  - The ID field
  - IP address of the nameserver queried
  - IP address / port from which the query was sent
- How often can an attack take place?
  - Each query from a recursor starts a race.
  - Forcing a query helps the attacker
  - The cache limits attacks to once per Time-To-Live for the same query

Attacking www.example.org

```
;; QUESTION SECTION:
;345678.example.org.            IN      A

;; ANSWER SECTION:
345678.example.org.   3600      IN      A       192.0.2.1

;; AUTHORITY SECTION:
example.org.        100000      IN      NS      ns1.evil.net.
example.org.        100000      IN      NS      ns2.evil.net.
```

Source: IETF namedroppers list. (P. Koch, T. Finch)

Oder ...

```
;; QUESTION SECTION:
;345678.www.example.org.                A

;; AUTHORITY SECTION:
www.example.org.     NS ns1.evil.net.
www.example.org.     NS ns2.evil.net.
```

... oder ...

```
;; QUESTION SECTION:
;345678.example.org.           IN    A

;; ANSWER SECTION:
345678.example.org.      CNAME www.example.org.
www.example.org.         A     192.0.2.80   ; evil
```

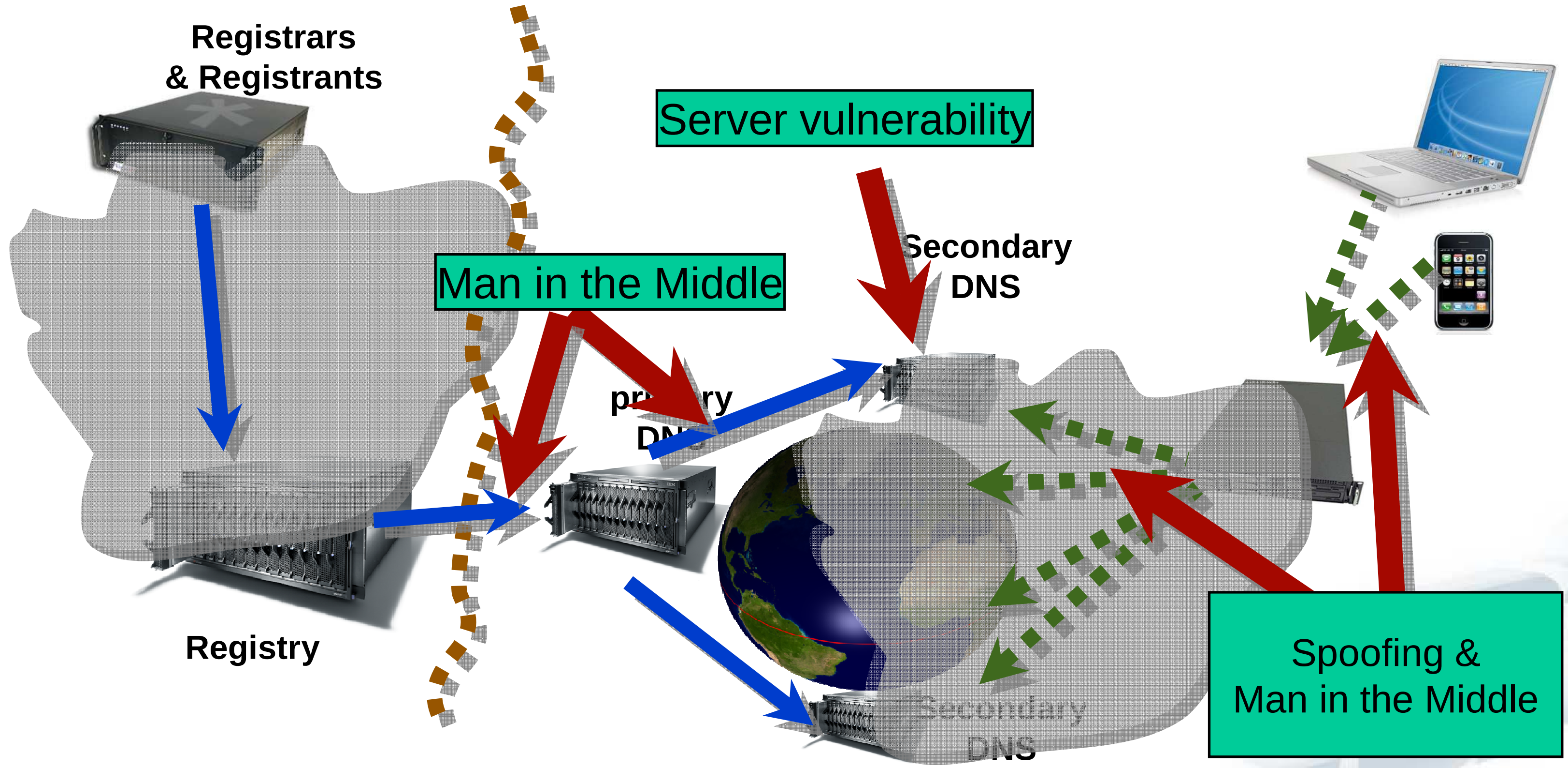
Wie funktioniert DNSSEC?

- Was soll DNSSEC leisten
- Die neuen Resource records
- Secure Delegations
- Key Management / Key Rollover
- NSEC3

DNSSEC Specs

- Details zum Nachlesen:
  - RFC4033, “DNS Security Introduction and Requirements”
  - RFC4034, “Resource Records for the DNS Security Extensions”
  - RFC4035, “Protocol Modifications for the DNS Security Extensions”
  - RFC5011, “Automated Updates of DNS Security (DNSSEC) Trust Anchors“
  - RFC5155, “DNS Security (DNSSEC) Hashed Authenticated Denial of Existence”

Where are the vulnerable points?



Welche Security?

- Confidentiality
  - Kann wer mitlesen?
- Integrity
  - Stimmt das, was ich bekommen habe?
- Availability
  - Bekomme ich überhaupt eine Antwort?

DNSSEC betrifft ausschließlich „Integrity“!

Grundidee

- Kompatible Erweiterung des DNS
- Public Key Kryptografie Signaturen innerhalb der DNS Antworten
- Schutz der Daten, nicht Schutz des Transports
- Delegationshierarchie des DNS wird auch zur Trust-Hierarchie

New Resource Records

- Three Public key crypto related RRs
  - RRSIG Signature over RRset made using private key
  - DNSKEY Public key, needed for verifying a RRSIG
  - DS Delegation Signer; ‘Pointer’ for building chains of authentication
- Two RR for internal consistency
  - NSEC Indicates which name is the next one in the zone and which typecodes are available for the current name.
  - NSEC3 NSEC++

RRSIG – Signature

- 16 bits - type covered
- 8 bits - algorithm
- 8 bits - nr. labels covered
- 32 bits - original TTL
- 32 bit - signature expiration
- 32 bit - signature inception
- 16 bit - key tag
- signer's name

RRSIGs gelten nicht ewig!

```
nlnetlabs.nl.  3600 IN  RRSIG   A 5  2 3600  (
            20050611144523 20050511144523  3112 nlnetlabs.nl.
            VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
            vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
            66DJubZPmNSYXw== )
```

DNSKEY – Public Key

- 16 bits: FLAGS
- 8 bits: protocol
- 8 bits: algorithm
- N*32 bits: public key

```
nlnetlabs.nl. 3600 IN DNSKEY  256 3 5 (
          AQOvhvXXU61Pr8sCwELcqqq1g4JJ
          CALG4C9EtraBKVd+vGIF/unwigfLOA
          O3nHp/cgGrG6gJYe8OWKYNgq3kDChN)
```

Delegation Signer (DS)

- Delegation Signer (DS) RR indicates that:
  - delegated zone is digitally signed
  - indicated key is used for the delegated zone
- Parent is authorative for the DS of the child's zone
  - Not for the NS record delegating the child's zone!
  - DS **should not** be in the child's zone

DS – Key of Subdomain

- 16 bits: key tag
- 8 bits: algorithm
- 8 bits: digest type
- 20 bytes: SHA-1 Digest

```
$ORIGIN nlnetlabs.nl.
lab.nlnetlabs.nl.   3600 IN   NS  ns.lab.nlnetlabs.nl
lab.nlnetlabs.nl.   3600 IN   DS  3112   5  1 (
                                   239af98b923c023371b52
                                   1g23b92da12f42162b1a9
                                 )
```

NSEC – Proof of non-existance

- FQDN: Next Name in Zone
- N*32 bit map: RRTypes present

```
www.nlnetlabs.nl. 3600 IN   NSEC z.nlnetlabs.nl. A RRSIG NSEC
```

NSEC Records

- NSEC RR provides proof of non-existence
- If the servers response is Name Error (NXDOMAIN):
  - One or more NSEC RRs indicate that the name or a wildcard expansion does not exist
- If the servers response is NOERROR:
  - And empty answer section
  - The NSEC proves that the QTYPE did not exist
- More than one NSEC may be required in response
  - Wildcards
- NSEC records are generated by tools
  - Tools also order the zone

NSEC Walk

- NSEC records allow for zone enumeration
- Providing privacy was not a requirement at the time
- Zone enumeration is a deployment barrier

- Solution is developed: NSEC3
  - RFC 5155
  - Complicated piece of protocol work
  - Hard to troubleshoot
  - Only to be used over Delegation Centric Zones

DNSSEC Queries

- DO
  - DNSSEC OK (EDNS0 OPT header) to indicate client support for DNSSEC options
  - EDNS0 is required for DNSSEC
- CD
  - “Don’t check signatures for me, just give me the raw DNSSEC records”

DNSSEC Answers

- SECURE Validated with key
  - AD – bit set in Packet
- INSECURE Validated but no key
- BOGUS Validation failed
- UNKNOWN ServFail etc

Key management

- To allow for key updates (“rollovers”), generate two keys:
  - Key Signing Key (KSK)
    - pointed to by parent zone (Secure Entry Point), in the form of DS (Delegation Signer)
    - used to sign the Zone Signing Key (ZSK)
  - Zone Signing Key (ZSK)
    - signed by the Key Signing Key
    - used to sign the zone data RRsets
- This decoupling allows for independent updating of the ZSK without having to update the KSK, and involve the parent.

Deployment Server-side

- Key management
  - Generate keys
  - Add DNSKEY records
- Sign zone
  - Signing & serving need not be performed on same machine
  - Signing system can be offline
- Make sure authoritative nameservers handle DNSSEC
- Communicate your keys to parent zone

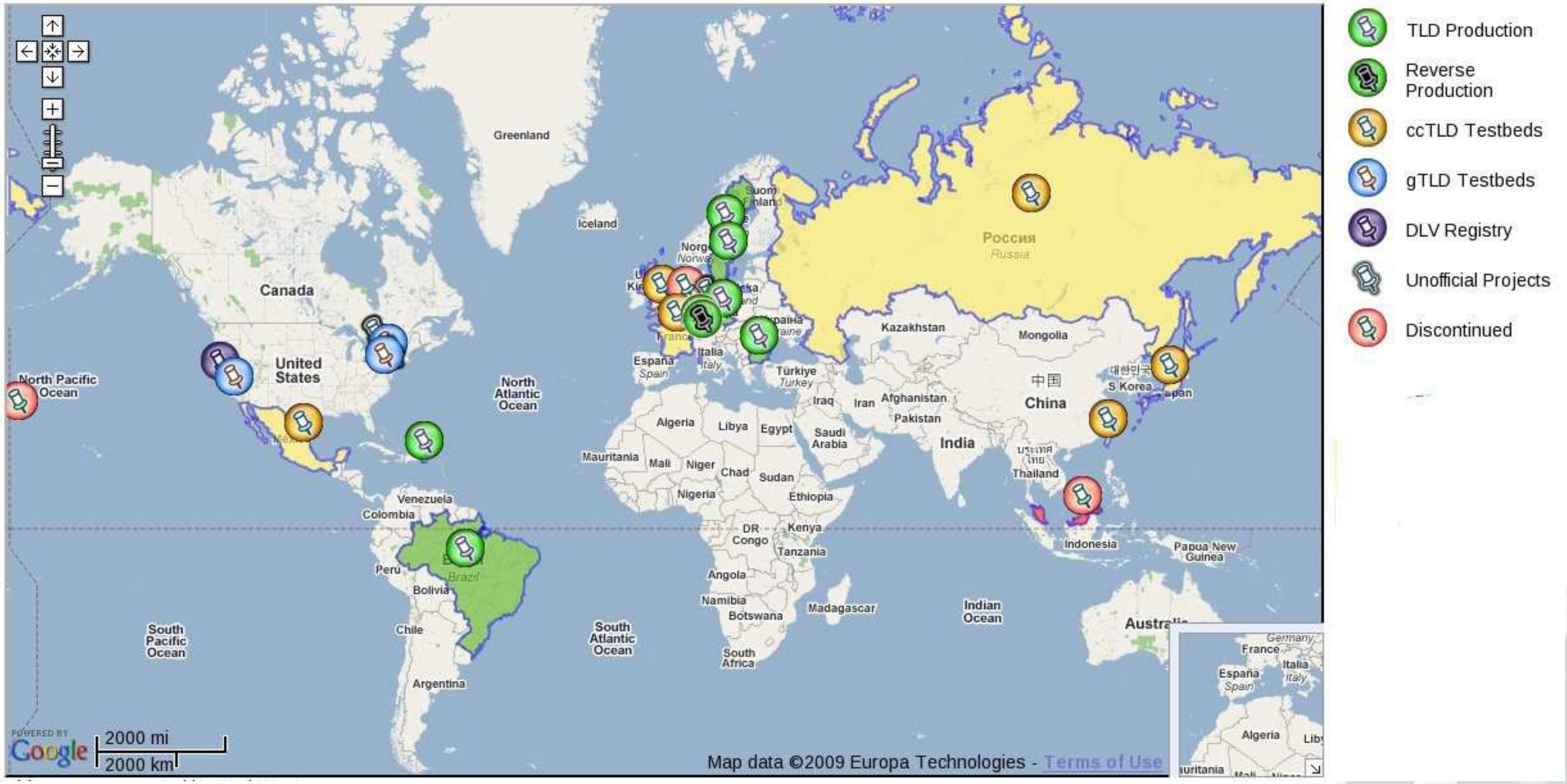
Deployment Client-side

- Stub-Resolver speaks DNSSEC
  - Inefficient
  - Slow rollout
  - Upsides in User-Interface
- Recursor does DNSSEC Validation
  - Need a way to secure last hop
  - Huge multiplier possibilities
- Secure Entry Points?

Trust Anchors

- Irgendwem muss der Client vertrauen
  - Hardcoded (domain, DNSKEY) Paare in der resolver-config
  - Analog zu dem „root.hints“ File
- Optimal:
  - Root ist signiert, alle TLDs, ….
- Realität:
  - Es gibt signierte Inseln:

Status 2009



Source: http://www.xelerance.com/dnssec/

Zwischenlösungen

- Selber Trust Anchors zusammensuchen
- DNSSEC Lookaside Validation (DLV)
  - <fqdn>.dlv.isc.org
- Trust Anchor Registries:
  - IANA Interim Trust Anchor Repository
    - https://itar.iana.org/
  - RIPE NCC?
    - http://www.ripe.net/ripe/tf/dnssec-key/
- Private, signed roots

Alternativen?

- On-path attacker?
  - Keine chance.
- Off-path attacker:
  - Mehr Entropie
    - 0x20
    - EDNS-PING
  - Skepsis bzgl. Zusatzinfos in DNS Anwort
    - Never cache data from auth and additional section.
    - Explicitly query for NS and A records.
    - Be careful when overwriting the cache.
  - Dynamisches reagieren:
    - Fallback to TCP
    - Multiple Queries