

DNSSEC - NSEC oder NSEC3?

Patrick Koetter und Carsten Strotmann, sys4 AG

Agenda

- Authenticated Denial of Existence
- Der NSEC Record
- Das Problem des NSEC Records
- NSEC3 als mögliche Lösung
- Die Probleme des NSEC3 Records
- Aktuelle Empfehlungen

NSEC-Record

Authenticated Denial of existence

- Die RRSIG-Einträge in DNSSEC sichern die positiven DNS Antworten (Antworten auf Abfragen, bei denen DNS-Einträge existieren)
- Aber auch negative Antworten müssen geschützt werden
 - Ohne Schutz für negative Antworten könnten Angreifer negative Antworten fälschen, um z.B. Denial-of-Service-Angriffe zu starten. Der Angreifer kann DNS-Clients glauben machen, dass eine DNS-Ressource nicht existiert

Authenticated Denial of existence

- DNS kennt zwei Arten von negativen Antworten: NXDOMAIN und NODATA/NXRRSET
 - NXDOMAIN = der angeforderte Domänenname existiert nicht
 - NODATA/NXRRSET = der angeforderte Domain-Name existiert, aber der angeforderte Datensatztyp existiert nicht für diesen Namen
- DNS-Fehlermeldungen wie SERVFAIL, FORMERR oder REFUSED können nicht mit DNSSEC gesichert werden (diese Fehler weisen auf Fehler im Protokoll oder in der Infrastruktur des DNS-Servers hin). Wenn das Protokoll defekt ist, kann auch DNSSEC nicht funktionieren.

Authenticated Denial of existence

- Die Lösung: Die NSEC-Einträge in der DNSSEC-signierten Zone erstellen eine Liste aller vorhandenen Daten in der Zone (Domännennamen und Typen für die Domännennamen)
 - Bei einer negativen Antwort sendet der DNS-Server den SOA-Record sowie den NSEC-Datensatz (plus eine Signatur für den NSEC-Eintrag), die beweist, dass die angeforderten Daten nicht im DNS existieren

Authenticated Denial of existence

```
example.com.      IN SOA ns1 hostmaster 100 3h 1h 41d 1h
example.com.      IN NS  ns1
example.com.      IN NS  ns2
example.com.      IN MX  10 mail1
example.com.      IN MX  20 mail2
example.com.      IN NSEC acc.example.com. SOA NS MX NSEC
acc.example.com.  IN A  192.0.2.77
acc.example.com.  IN NSEC mx1.example.com. A NSEC
mx1.example.com.  IN A  192.0.2.25
mx1.example.com.  IN NSEC mx2.example.com. A NSEC
mx2.example.com.  IN A  192.0.2.50
mx2.example.com.  IN NSEC ns1.example.com. A NSEC
ns1.example.com.  IN A  192.0.2.10
ns1.example.com.  IN NSEC ns2.example.com. A NSEC
ns2.example.com.  IN A  192.0.2.20
ns2.example.com.  IN NSEC www.example.com. A NSEC
www.example.com.  IN A  192.0.2.80
www.example.com.  IN NSEC example.com. A NSEC
```

NSEC Sortierung der Zone

- Für NSEC müssen alle DNS-Einträge in der Zone eine bestimmte Reihenfolge haben
 - Alle Domännennamen (Besitzernamen) müssen voll qualifizierte Namen (FQDN) sein
 - DNS-Einträge mit einer geringen Anzahl von Bezeichnungen im Domännennamen werden an den Anfang der Zone sortiert, während Einträge mit mehr Bezeichnungen im Namen am Ende der Zonendatei sortiert werden
 - Alle Domännennamen mit der gleichen Anzahl von Bezeichnungen werden alphanumerisch sortiert

NSEC Sortierung der Zone

- Für NSEC müssen alle DNS-Einträge in der Zone eine bestimmte Reihenfolge haben
 - Bei jedem neuen Domännennamen in der Zone wird ein neuer NSEC-Eintrag eingefügt. Der NSEC-Eintrag trägt den Besitzernamen des aktuellen Domännennamens in der Zone und verweist auf den nächsten Domännennamen in der Zone
 - Der NSEC-Eintrag listet alle DNS-Eintragstypen (A, AAAA, NS, TXT ...) die für den Domännennamen des NSEC-Eintrags existieren
 - Ein NSEC-Eintrag, der hinter dem letzten Eintrag in der Zone eingefügt wird, verweist zurück auf den Anfang der Zone (den Domännennamen des SOA-Eintrags)

NSEC-Antworten (NXDOMAIN)

- Bei einer NXDOMAIN-Antwort gibt der DNS-Server den NSEC-Eintrag für den Domännennamen zurück, der direkt über dem angeforderten (aber nicht existierenden) Namen
 - Dies beweist die Nichtexistenz des angeforderten Namens, da der NSEC Eintrag den existierenden Namen (oberhalb des angeforderten Namens) und den nächsten existierenden Namen (unterhalb des angeforderten Namens)

NSEC-Antworten (NODATA)

- Bei einer NODATA/NXRRSET-Antwort gibt der DNS-Server den NSEC Datensatz für den angeforderten Domännennamen zurück
 - Der NSEC-Eintrag listet alle DNS-Eintragstypen auf, die für den angeforderten Domain-Namen existieren. Der angeforderte DNS-Eintragstyp ist nicht in der Liste dieser Eintragstypen. Dies beweist, dass der angeforderte DNS-Eintragstyp nicht existiert
- NSEC-Datensätze werden mit DNSSEC-Signaturen signiert. Die Gültigkeit des des NSEC-Eintrags kann wie bei jedem anderen DNS-Eintrag überprüft werden

Probleme mit NSEC

- Der NSEC-Eintrag ist eine elegante Lösung für das Problem, aber er hat Nachteile:
 - Es ist nun für Außenstehende möglich, den gesamten Zoneninhalt aufzulisten Inhalt aufzulisten, indem sie der NSEC-Eintragskette folgen. Dies wird als *Zonenwalking* bezeichnet
 - Für die meisten Zonen stellt dies kein großes Problem dar, da der Inhalt der DNS-Zone ohnehin öffentlich ist (SOA, NS-Einträge, WWW-A, MX-Einträge)

Probleme mit NSEC

- Zonewalking ...
 - Kann ein Problem für Zonen mit sensiblem Inhalt sein (E-Mail Adressen, Hostnamen kritischer Infrastrukturen, neue Produktnamen Namen, die noch nicht veröffentlicht werden sollten)
 - Betreiber von TLD-Zonen halten sich von DNSSEC mit NSEC fern, da es es Außenstehenden ermöglicht, alle Änderungen an der TLD-Zone aufzuzeichnen (neue Delegationen und Delegationsentfernungen)

Probleme mit NSEC

- Beispiel für Zonenwalking:

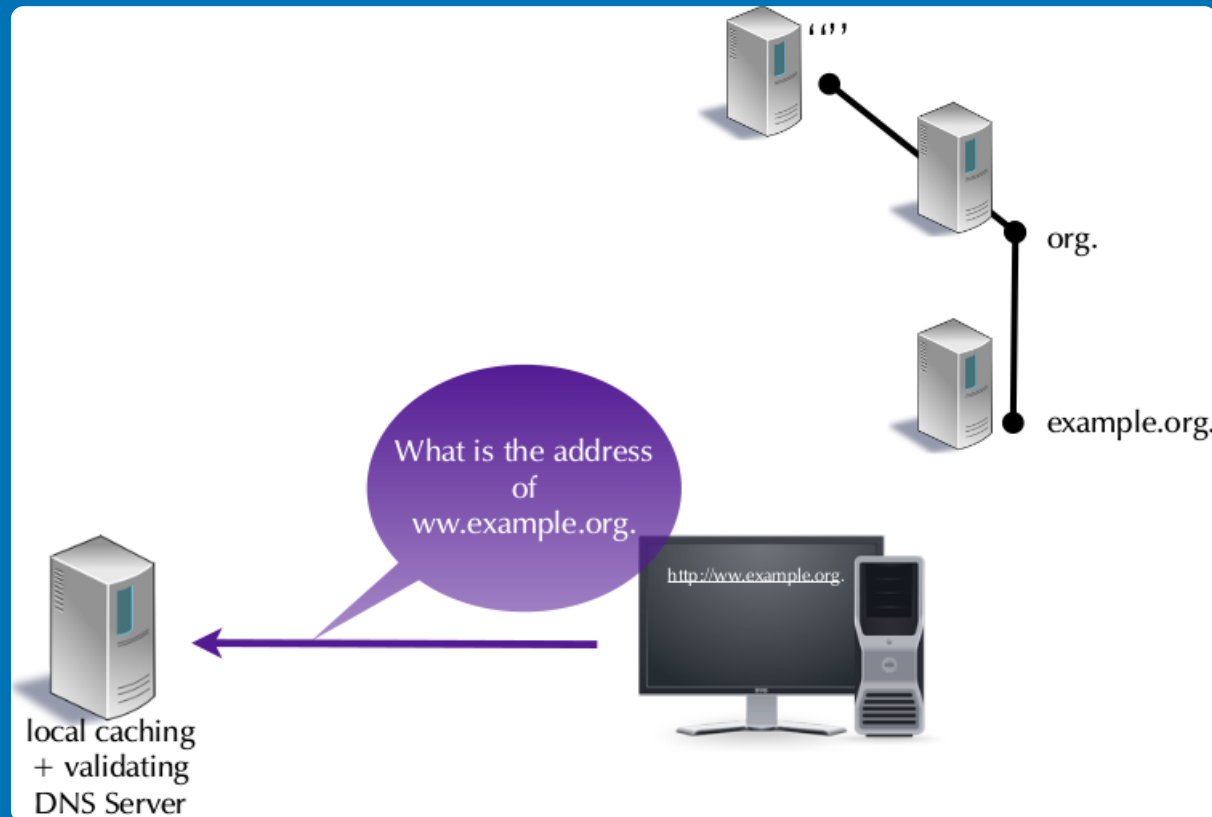
```
$ ldns-walk paypal.com
```

NSEC3

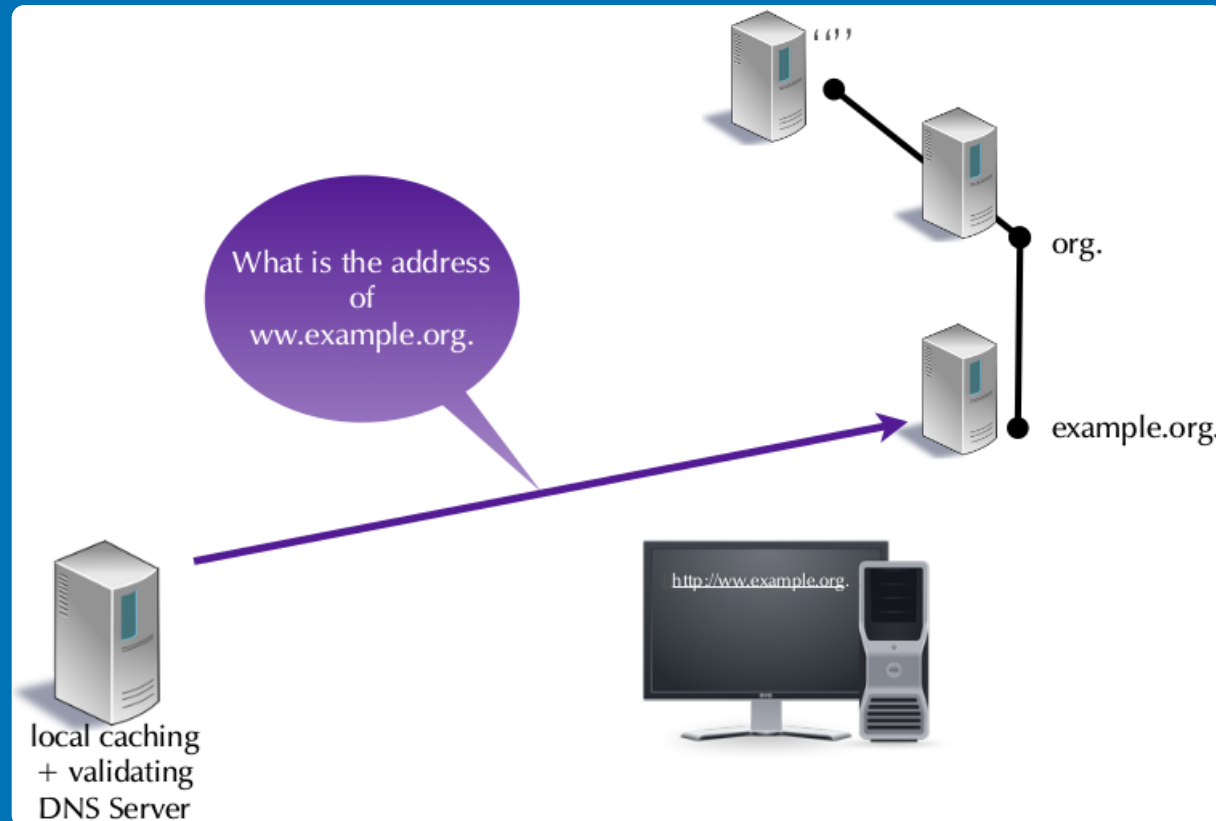
Der NSEC3-Record

- ↪ RFC 5155 (2008) definiert den NSEC3-Record als eine Alternative zu NSEC
 - Alle modernen DNS-Server unterstützen NSEC3
 - Der NSEC3-Eintrag funktioniert ähnlich wie NSEC, mit dem Unterschied, dass die Verbindung zwischen den Besitzernamen mit SHA1-Hashes der Domännennamen anstelle der Klartextnamen
 - NSEC3 macht es schwieriger, aber nicht unmöglich, den Zoneninhalt aufzulisten

NSEC 3 Validierung



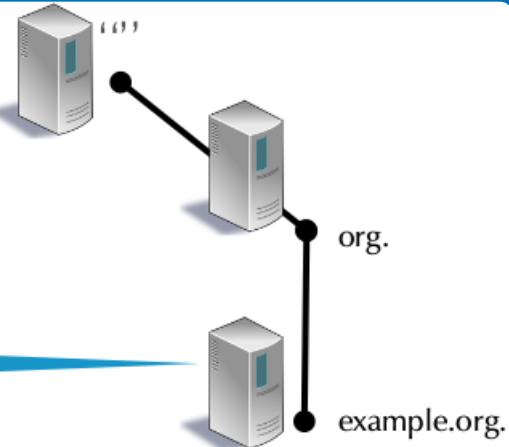
NSEC 3 Validierung



NSEC 3 Validierung

NXDOMAIN?

```
$TTL 300
@ IN SOA ns1. 1 2010010100 1 1 1
IN NS ns1
IN MX 10 mail
ns1 IN A 192.0.2.10
ns1 IN AAAA 2001:db8:100::53
www IN A 192.0.2.20
IN AAAA 2001:db8:100::80
mail IN A 192.0.2.25
```

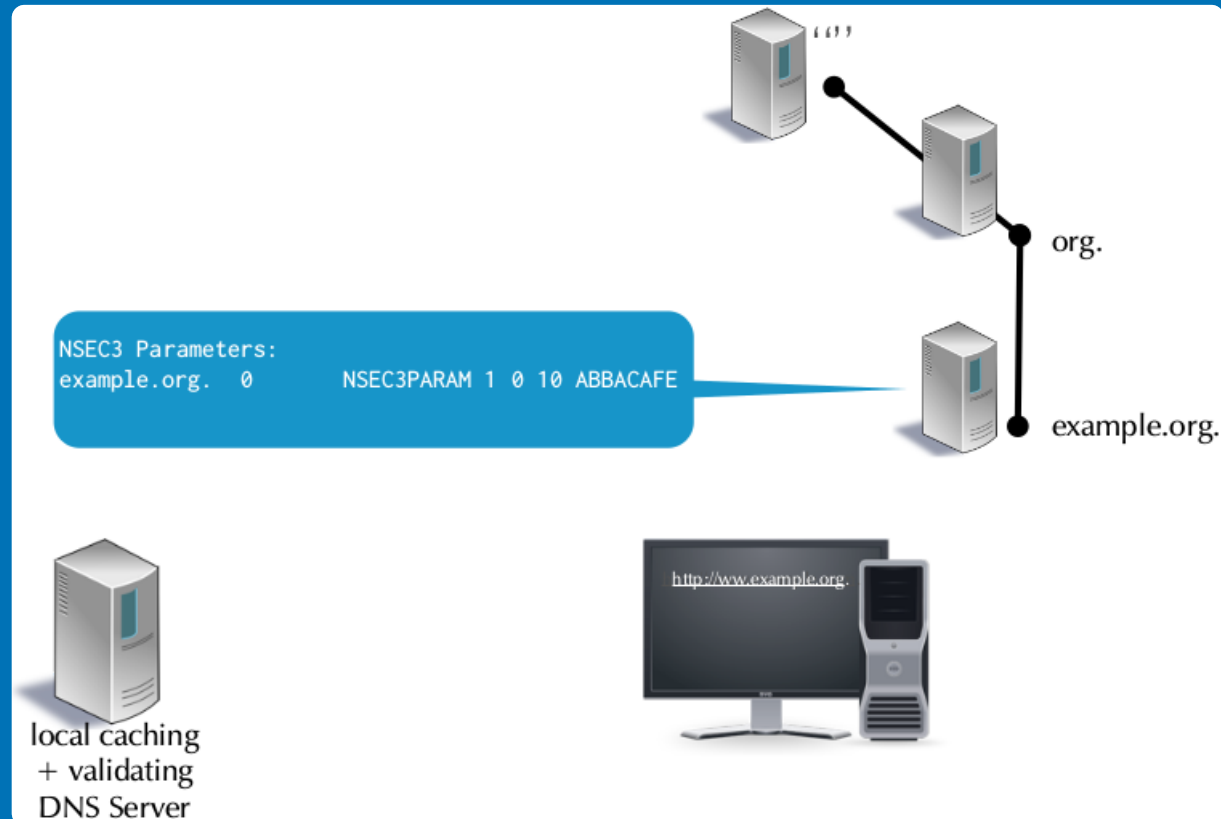


local caching
+ validating
DNS Server

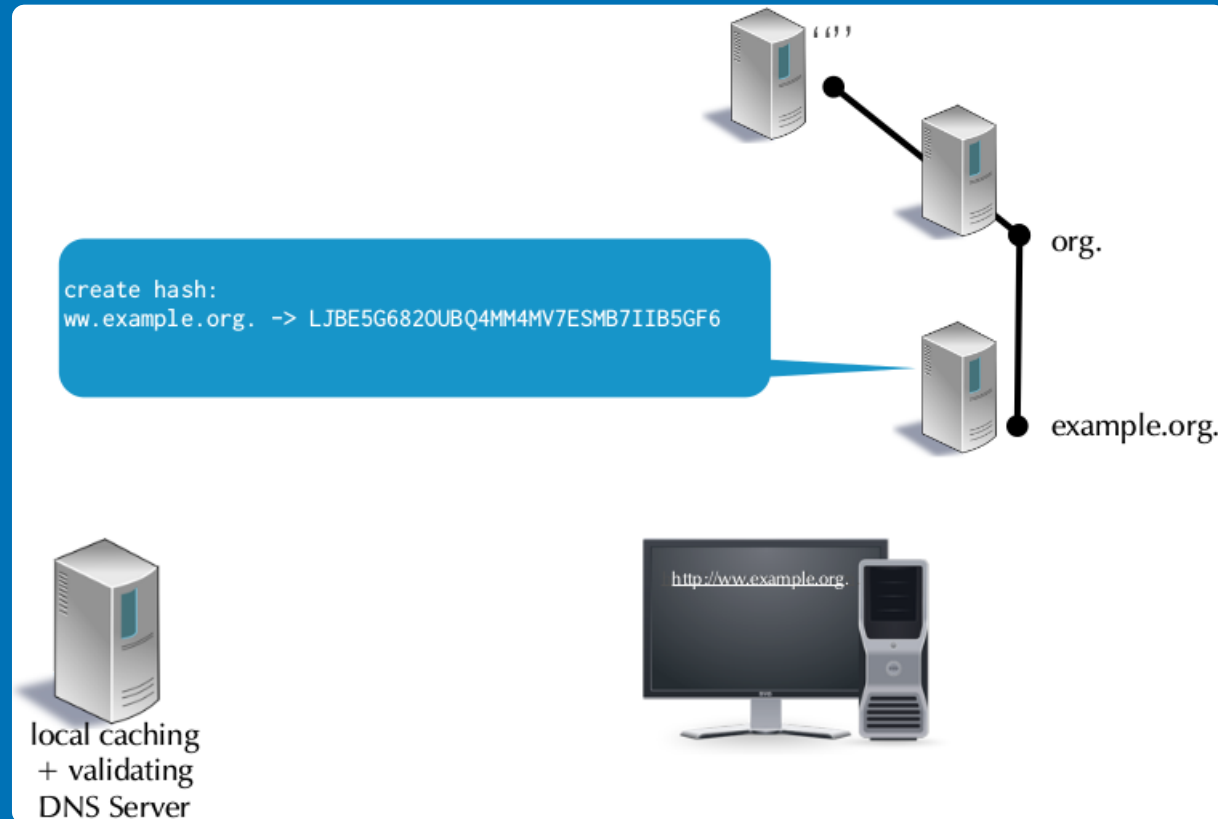


<http://www.example.org>

NSEC 3 Validierung

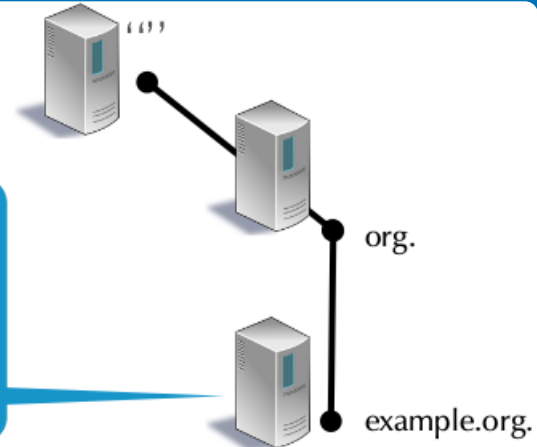


NSEC 3 Validierung



NSEC 3 Validierung

search for next matching hash in order:
J1MGP57A9UG79P76932PD4SE8SFIGIK0 3600 IN NSEC3 (1 0 10
ABBACAFE
LV5AGGD50HNDK501IR7J1LA4HQVRSG05
A RRSIG)

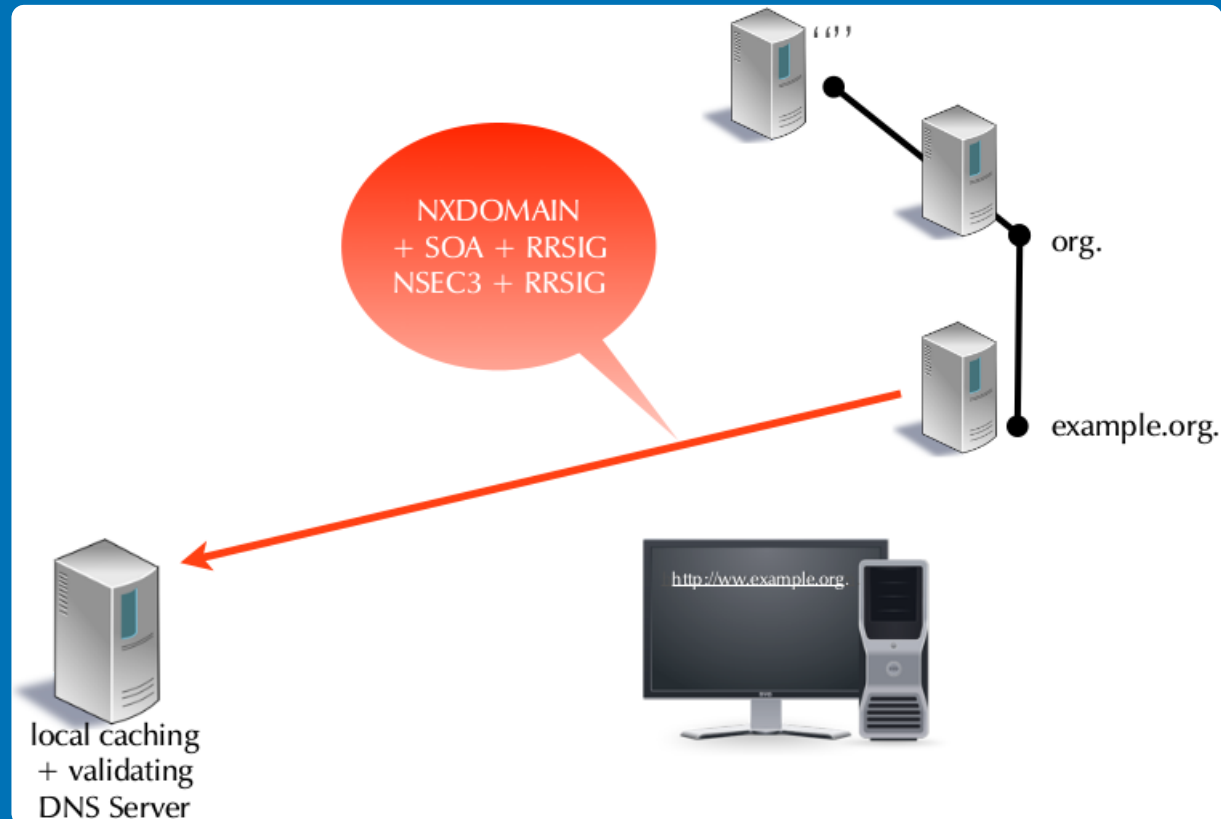


local caching
+ validating
DNS Server



<http://www.example.org>

NSEC3 Validierung



NSEC3 Validierung

create hash:

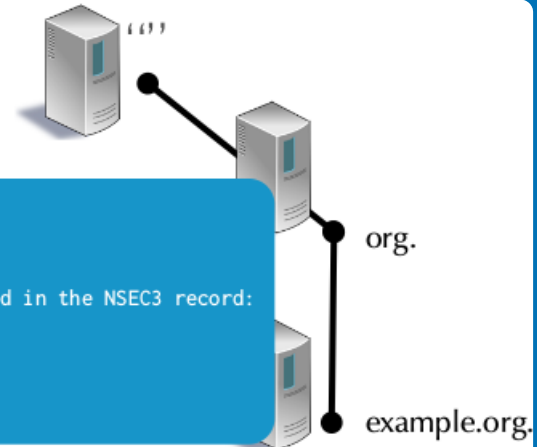
ww.example.org. -> LJBE5G682OUBQ4MM4MV7ESMB7IIB5GF6

and verify that hash is in-between the hashes contained in the NSEC3 record:

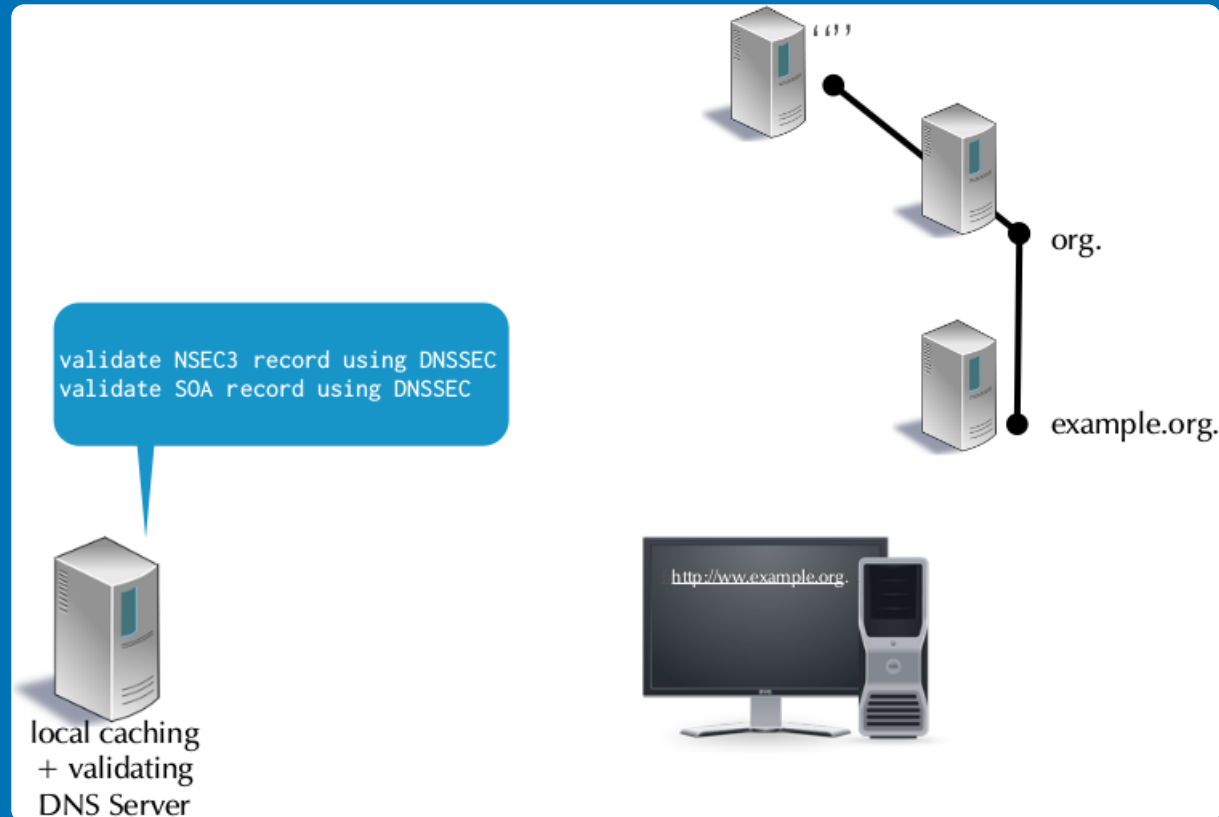
J1MGP57A9UG79P76932PD4SE8SFIGIK0 (owner of NSEC3)

<<< LJBE5G682OUBQ4MM4MV7ESMB7IIB5GF6 (calculated hash)

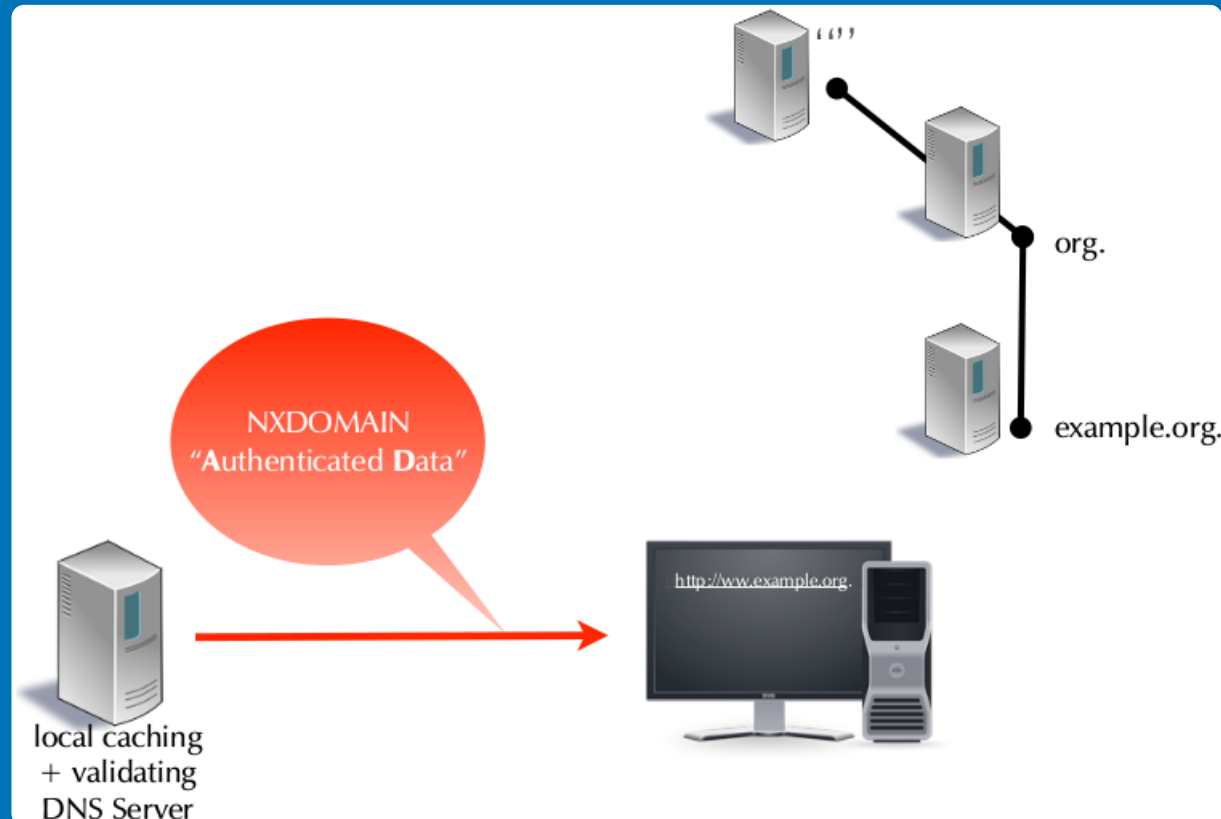
LV5AGGD50HNDK501IR7J1LA4HQVRSG05 (next name in zone)



NSEC3 Validierung



NSEC 3 Validierung



NSEC3-Parameter

- Der NSEC3-Datensatz enthält eine Reihe von Parametern für die Verarbeitung von NSEC3-Records
 - Der verwendete Hashing-Algorithmus (derzeit ist nur SHA1 definiert)
 - Flags: ermöglicht das DNSSEC-Opt-out in Delegationen. Dies ist für Top-Level-Domains wichtig, da NSEC3-Datensätze mit Signaturen nur für Zonen erstellt werden müssen, die DNSSEC signiert sind.
 - Anzahl der Hash-Iterationen
 - Ein Salt-Wert

NSEC3-Parameter

- Jede Zone mit NSEC3-Einträgen enthält einen NSEC3PARAM-Eintrag. Dieser Datensatz enthält Informationen, die von autoritativen DNS-Servern benötigt werden, um NSEC3-Einträge für negative Antworten zu generieren
- Beispiel: (SHA1, keine Flags, 20 Iterationen, Salt "ABBACAFE")

```
nsec3.dnslab.org.      0 IN NSEC3PARAM 1 0 20 ABBACAFE
```

NSEC3 Iterationen und Salz

- Mittels der Hash-Iterationen im NSEC3PARAM-Eintrag kann der Betreiber der Zone den Arbeitsaufwand für die Berechnung des Hashwerts anpassen
 - Eine höhere Anzahl von Iterationen macht es Angreifern (ein wenig) schwerer, einen NSEC3-Domännennamen mit roher Gewalt zu knacken
 - Eine höhere Anzahl von Iterationen führt jedoch zu einer höheren CPU-Last für DNS-Resolver, die die NSEC3-Datensätze validieren, wodurch die DNS-Namensauflösung langsamer wird
- Das Salz macht es für einen Angreifer unmöglich, per Vorberechnung eine ↪Rainbowtable für die Zone herzustellen

NSEC3 Iterationen und Salz

- Das Salt ist eine hexadezimale Zahl, jede Hex-Ziffer enthält 4 Bit an Information
 - Die empfohlene Größe des Salzes beträgt 32-64 Bit (8-16 Hexadezimalziffern)
 - RFC 5155 empfiehlt, das Salt bei jeder Änderung in der Zone zu ändern
 - Dies würde alle bestehenden NSEC3-Einträge ungültig machen, der DNS Server müsste neue NSEC3-Einträge erstellen und die NSEC3-Kette neu berechnen. die NSEC3-Kette neu berechnen. Dies wird inzwischen als überflüssig angesehen.
 - Die derzeitige Empfehlung lautet, das Salz bei jeder Änderung des des ZSK zu ändern (wenn sich der ZSK ändert, müssen alle Signaturen neu erstellt werden, so dass die Änderung der NSEC3-Kette keinen zusätzlichen viel zusätzliche Arbeit)

NSEC 3 Iterationen seit April 2021

- Eine Hash-Iteration ist ausreichend um (einfaches) Zone-Walking zu verhindern
 - Einen entschlossenen Angreifer werden auch mehrere Hash-Iterationen nicht abschrecken

When using NSEC3 to sign your domain, please make sure your extra iteration count is not needlessly large (i.e. above ~25, 0 is best).

- Die aktuelle Empfehlung für NSEC3PARAM ist 1 0 0 – (0 Iterationen, kein Salt)
- Seit April 2021 behandeln DNSSEC validierende Resolver DNS Zonen mit mehr als 150 NSEC3-Hash-Iterationen als "unsicher" (insecure)
 - d.h. es wird keine DNSSEC Validierung durchgeführt
- Referenzen:
 - ↪ <https://mail.sys4.de/pipermail/dane-users/2021-March/000594.html>
 - ↪ <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-nsec3-guidance>

NSEC3 Narrow-Mode

- ↪RFC 7129 (auch ↪RFC 4470 und ↪RFC 4471) beschreiben eine spezielle Variante der NSEC3-Nutzung, genannt *narrow mode*
 - Beim *narrow mode* werden die NSEC3-Records nicht beim signieren der Zone vorberechnet, sondern sie werden *on the fly* erstellt, wenn eine negative Antwort benötigt wird
 - Um die Signaturen für solche Antworten berechnen zu können, muss **jeder** autoritativer DNS-Server für die Zone Zugang zu den privaten DNSSEC-Schlüssel (zumindest den ZSK) haben! Dies ist ein zusätzliches Sicherheitsrisiko für die DNSSEC Schlüssel.

NSEC3 Narrow-Mode

- Bei NSEC3 *narrow mode* gibt der DNS-Server nicht eine NSEC3 Kette bestehender Einträge zurück, sondern einen synthetischen NSEC3-Eintrag, der beweist dass der angeforderte Name nicht existiert
 - Dies verhindert ein "Zone Walking", da die Anzahl der möglichen NSEC3 Datensätze zurückgegeben wird, nahezu unendlich ist. Dies erschöpft den Speicher des Angreifers, der versucht, diese NSEC3-Kette zu speichern.

NSEC3 Narrow-Mode

- Bekannte Implementierungen:
 - ↪ Phreebird (Dan Kaminski, Proof-of-Concept, nicht aktiv weiterentwickelt)
 - ↪ PowerDNS Authoritative
 - ↪ Cloudflare CDN NSEC3 Narrow-Mode (geschlossene Quellimplementierung)

Ende des Kapitels "NSEC oder NSEC3" - Fragen?
