Über die Auswirkungen von DNSSEC auf das Internet[1]

Matthäus Wander[2]

Abstract: Im folgenden Beitrag werden die Sicherheitsdefizite des Domain Name Systems (DNS) untersucht und die Auswirkungen der DNSSEC-Sicherheitserweiterungen bewertet. Durch Messungen im Internet wird die systematische Durchführung von DNS-basierten Netzsperren belegt. In China und im Iran wird eine Technik eingesetzt, die vollumfänglich DNS-Anfragen im Netz untersucht und prinzipiell auch die Kommunikation Dritter in anderen Ländern beeinträchtigen kann.
Die Sicherheitsziele von DNSSEC sind Datenintegrität und Authentizität, was durch Signaturen umgesetzt wird. Die NSEC3-Erweiterung schützt zudem DNS-Server durch ein Hash-Verfahren vor dem Auslesen des Domainnamensraums. Die von NSEC3 zugesicherte Privatheit kann allerdings durch den Einsatz von GPU-Berechnung effizient angegriffen werden.
Ferner wird mit aktiven Messmethoden die Verbreitung von DNSSEC untersucht, die nach anfänglicher Zurückhaltung deutlich zugenommen hat. Auf der Serverseite gibt es mehr als fünf Millionen mit DNSSEC signierte Domainnamen, die jedoch teilweise unsicher oder aufgrund von Wartungsfehlern nicht mit DNSSEC erreichbar sind. Auf der Clientseite ist die Validierungsquote in den letzten drei Jahren weltweit von rund 1% auf 21% gestiegen.

Keywords: Domain Name System, DNSSEC, IT-Sicherheit, Internetzensur, Hash-Angriffe

1 Einleitung

Das *Domain Name System* (DNS) ist ein im Internet verteilter Namensdienst, der Domainnamen auf IP-Adressen, Dienstbezeichner oder andere Ressourcen abbildet. Die meisten Internetbasierten Anwendungen hängen vom DNS ab, um Hostnamen und Serveradressen abzurufen, z. B. das World Wide Web, E-Mail oder Voice over IP. Sollte die Namensauflösung nicht zur Verfügung stehen, ist auch die Konnektivität der Anwendungen eingeschränkt. Ein sicherer und zuverlässiger Betrieb des DNS ist daher für das Internet essentiell.

Die ursprüngliche DNS-Spezifikation sah keine Sicherheitsmechanismen vor, um vor gefälschten DNS-Antworten zu schützen. Durch DNS-Spoofing kann ein Angreifer Verbindungsversuche zum falschen Host umleiten, um z. B. einen Phishing-Angriff durchzuführen oder E-Mails umzuleiten. Als Abhilfe führte die *Internet Engineering Task Force* die *Domain Name System Security Extensions* (DNSSEC) ein [Ar05], die die Datenintegrität und Authentitizät von DNS-Antworten durch kryptographische Maßnahmen gewährleisten sollen.

Das Ziel der in diesem Beitrag vorgestellten Dissertation [Wa15] ist es, die Sicherheitsdefizite des DNS zu untersuchen und zu verstehen, welche Auswirkungen die Einführung von

[1] Englischer Titel der Dissertation: „The Impact of DNSSEC on the Internet Landscape“[Wa15]

[2] Universität Duisburg-Essen, matthaeus.wander@uni-due.de

DNSSEC hat. Das methodische Vorgehen besteht in der Durchführung von messbasierten Analysen.

2 Domain Name System und DNSSEC

Das Domain Name System bildet eine global verteilte Namensdatenbank. Die Systemarchitektur besteht aus Resolvern (Clients) und Servern, wobei die Verwendung von zwischengeschalteten Resolvern als Proxy-Server mit Cache gängig ist. Der Namensraum ist hierarchisch als Baum strukturiert. Die Verwaltung der Wurzel (*root*) erfolgt zentral durch die *Internet Corporation for Assigned Names and Numbers*, die die Verantwortung über Top-Level-Domains an andere Organisationen delegiert. Die Top-Level-Domain-Betreiber wie z. B. DENIC (`de`) wiederum delegieren registrierte Domains (`beispiel.de`) an Endnutzer, darunter natürliche Personen, Unternehmen oder andere Organisationen.

DNSSEC fügt digitale Signaturen in DNS-Antworten ein, die mittels asymmetrischer Kryptosysteme wie z. B. RSA oder ECDSA erzeugt und überprüft werden [Ar05]. Die öffentlichen Schlüssel sind Teil des Namensraums, wobei die Authentizität eines Schlüssels durch eine hierarchische Verkettung sichergestellt wird: eine Domain authentifiziert den Schlüssel einer Subdomain, indem der Fingerprint (Hashwert) des Subdomain-Schlüssels signiert wird. Zur Validierung einer Domain-Signatur authentifiziert ein DNSSEC-Resolver die Schlüsselkette von der zu validierenden (Sub-)Domain bis hin zum Root-Schlüssel. Der öffentliche Teil des Root-Schlüssels ist DNSSEC-Resolvern wohlbekannt und dient als Vertrauensanker (*Trust Anchor*). Das Vertrauensmodell von DNSSEC entspricht damit dem Baum, der aus der hierarchischen Delegierung von Domains folgt. Die Autorität einer Domain beschränkt sich auf ihren jeweiligen Teil des Namensraums, wobei Root über den vollständigen Namensraum verfügt.

Die Sicherheitsgarantien von DNSSEC beschränken sich auf authentische und unveränderte DNS-Namensauflösungen. Anwendungen müssen daher weiterhin Verschlüsselungsprotokolle wie TLS oder SSH zur Absicherung der Anwendungsdaten verwenden. DNSSEC ermöglicht allerdings das Bootstrapping von anwendungsbasierten Sicherheitsmechanismen, z. B. durch Authentifikation von digitalen Zertifikaten. Mehrere solcher Erweiterungen sind als *DNS-based Authentication of Named Entities* (DANE) spezifiziert, um z. B. für die Übertragung von E-Mails TLS-Verschlüsselung zu erfordern und vor Downgrade-Angriffen zu schützen [DH15].

3 Sicherheitsanalyse

Ohne die Verwendung von kryptographischen Sicherheitsverfahren ist DNS-Spoofing für Angreifer trivial möglich, sofern der Inhalt einer DNS-Anfrage mitgehört wird (*On-Path-Angreifer* oder *In-Path-Angreifer*). Das Spoofing ist ohne Kenntnis der Anfrage (*Off-Path-Angreifer*) aufwendig, da zufällig gesetzte Felder in der Anfrage erraten werden müssen, indem eine große Anzahl von unterschiedlichen gefälschten DNS-Antworten gesendet wird. Die Erfolgswahrscheinlichkeit eines Angriffs steigt deutlich, sollte der Resolver

mehrfach dieselbe Anfrage senden. Diese Variante des DNS-Spoofings ist in der Literatur als *Birthday-Angriff* bekannt, wobei das üblicherweise zitierte mathematische Modell des Geburtstagsparadoxons die Wahrscheinlichkeit unterschätzt und der Angriff, den wir als *Courier-Angriff* bezeichnen, tatsächlich noch effektiver ist. Zum Schutz vor Courier-Angriffen sollten Resolver identische Anfragen erkennen und zurückhalten.

Neben der Möglichkeit eine Anwendung zum falschen Server umzuleiten, ist es mit DNS-Spoofing auch möglich, den Zugang zu einer Website zu sperren. Eine mögliche Sperrmethode ist hierbei das Blacklisting von gesperrten Domainnamen auf den Resolvern der Netzzugangsanbieter. Diese Methode wird in vielen Ländern eingesetzt, z. B. in der Türkei während der Sperrung von Twitter und Youtube im März 2014, ist jedoch für Internetnutzer vergleichsweise einfach zu umgehen. Eine andere Methode ist *DNS-Injection*, bei der sämtliche DNS-Nachrichten im Netz überwacht werden und gefälschte DNS-Antworten für gesperrte Domainnamen gesendet werden. DNS-Injection ist technisch anspruchsvoller in der Implementierung, allerdings schwieriger für den Nutzer zu umgehen und dadurch effektiver.

3.1 Messbasierte Studien zu DNS-Injection

Durch messbasierte Analysen wird in dieser Arbeit die systematische Durchführung von DNS-Injection-Angriffen in China und im Iran zum Zweck der Internetzensur belegt. Bei den dazu entwickelten Messmethoden kann sich der Ausgangspunkt der Messung außerhalb der von den Sperrfiltern betroffenen Netze befinden. Dadurch ist es z. B. möglich DNS-basierte Sperren von sozialen Medien im Iran zu beobachten. Kurz nach der Wahl von Irans Präsident Hassan Rohani war etwa von August bis Oktober 2013 eine zeitweise Rücknahme der Sperren sozialer Medien in den meisten iranischen Netzen zu sehen (Abb. 1). Die Erkennung einer gefälschten DNS-Antwort ist anhand der darin enthaltenen IP-Adresse möglich, die mit einem Abfrage-Algorithmus effizient ermittelt werden können.

DNS-Injection kann prinzipiell Dritte in anderen Ländern unbeabsichtigt beeinträchtigen, wenn das Routing von Dritten durch ein von der Sperre betroffenes Netz erfolgt. Die folgende Studie untersucht den möglichen Einfluss des chinesischen Sperrfilters auf Dritte. Eine großflächige Messung mit 255 002 offenen Resolvern außerhalb von China ergab, dass 6 % vom chinesischen Sperrfilter betroffen sein können, wenn sie eine südkoreanische Domain auflösen (unterhalb `kr` oder der internationalisierten Variante `xn--3e0b707e`). Dies ergibt sich daraus, dass der Top-Level-Domain-Betreiber KRNIC einen gespiegelten Anycast-Knoten seines DNS-Servers in Beijing betreibt. Dieser Server beantwortet allerdings abhängig von der aktuellen Routing-Konfiguration auch Anfragen aus anderen Ländern, so in der Messung u. a. aus Rumänien, Italien, Iran und Panama. DNS-Injection betraf in der Vergangenheit auch die deutsche Top-Level-Domain `de`, zu der Anycast-Knoten u. a. in Beijing und Hongkong betrieben werden, ist nach einer Anpassung der Routing-Konfiguration jedoch nicht mehr nachweisbar. Hongkong ist selbst nicht direkt vom chinesischen DNS-Sperrfilter betroffen, was durch Messungen vor Ort aus zwei Hongkonger Netzen heraus bestätigt werden konnte. DNS-Injection ist dann in der Pra-

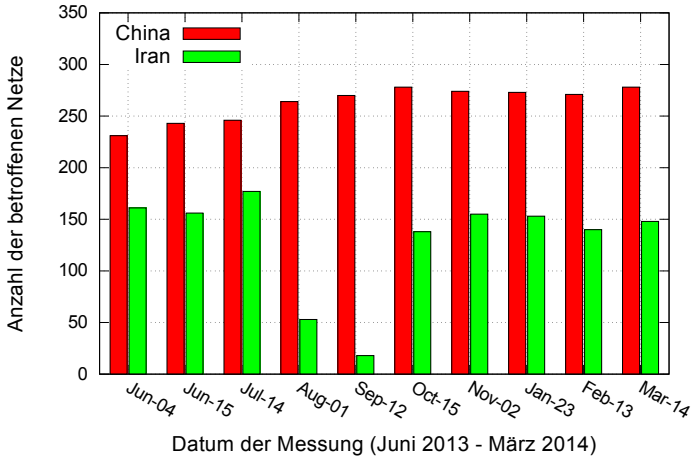

Abb. 1: Gefälschte Antworten für `facebook.com` im Zeitverlauf.

xis nachweisbar, wenn sich der Zielserver in einem Land befindet, in dem Netzbetreiber aktive Internetsperren einsetzen. Für Inhaltsanbieter und Internetdienstleister ist dies neben dem Hosting von replizierten DNS-Servern auch beim Aufbau von Content Delivery Networks relevant. Ein Teil der oben genannten Forschungsergebnisse wurde im Open-Access-Journal *IEEE Access* im Jahr 2014 veröffentlicht [Wa14a].

3.2 DNSSEC und Angriffe auf NSEC3-Privatheit

Mit DNSSEC kann ein validierender Resolver DNS-Spoofing-Angriffe erkennen, wobei die Sicherheit von der Wahl des asymmetrischen Kryptosystems, der Schlüssellänge und der Vertrauenswürdigkeit der Autoritäten in der Namenshierarchie abhängt. DNSSEC stellt die Integrität und Authentizität der DNS-Antworten sicher, trägt jedoch nicht zur (fehlenden) Privatheit von DNS bei: Anfragen und Antworten werden im Klartext übermittelt. Dadurch ist die Privatsphäre von Internetnutzern gefährdet [He14]. Darüber hinaus ermöglicht DNSSEC das Auslesen der vollständigen DNS-Datenbank einer Domain, da negative Antworten mit Namensfehler Informationen über existierende Domainnamen preisgeben, die sich per *Zone Enumeration* systematisch auslesen lassen. Die DNSSEC-Erweiterung NSEC3 versucht das Auslesen der Serverdatenbank zu verhindern, indem durch eine Hashfunktion unkenntlich gemachte Namen zurückgegeben werden.

In dieser Arbeit werden drei GPU-basierte Angriffsmethoden auf die NSEC3-Hashfunktion vorgestellt, um effizient die Hashwerte zu Klartextnamen zurückzurechnen. Alle drei Methoden basieren auf dem Prinzip Klartextkandidaten zu iterieren, zu denen der NSEC3-Hashwert berechnet wird. Der berechnete Hashwert wird mit den Hashwerten verglichen, die zuvor vom DNS-Server ausgelesen wurden. Zur Optimierung der GPU-Speicherzugriffe besteht der Hashwertvergleich aus einer Bloomfilter-Abfrage und bei positivem Ergebnis der Abfrage aus einer binären Suche.

Der *Brute-Force-Angriff* iteriert den Suchraum vollständig, ist jedoch bei einer Länge von mehr als 10 Zeichen rechenaufwendig und damit unpraktikabel. Der *Wörterbuch-Angriff* iteriert eine vorgegebene Liste von Klartextkandidaten. Die GPU-Berechnung ist dabei so performant, dass selbst Wörterbücher mit mehreren Millionen Einträgen innerhalb von Sekunden berechnet werden. Um die Effektivität zu vervielfachen, erzeugt der Wörterbuch-Angriff weitere Klartextkandidaten durch das Einfügen von Zeichenfolgen in Wörter. Als Zeichenfolgen werden die häufigsten n-Gramme verwendet, die wiederum aus dem Wörterbuch hergeleitet sind. Der *Markow-Ketten-Angriff* verwendet ein statistisches Modell bereits bekannter Domainnamen, um weitere wahrscheinliche Klartextkandidaten herzuleiten. Das statistische Modell lässt sich durch die Anwendung des Brute-Force-Angriffs mit kurzen Wortlängen ermitteln.

Mit diesen Methoden wird erstmals ein Angriff auf die Top-Level-Domain `com` präsentiert, bei dem mit einer GPU 64 % der NSEC3-Hashwerte in fünf Tagen gebrochen wurden (Abb. 2). Der Wörterbuchangriff war die effizienteste Methode und fand innerhalb von 14 Stunden die Klartextnamen zu 62 % der NSEC3-Hashwerte.

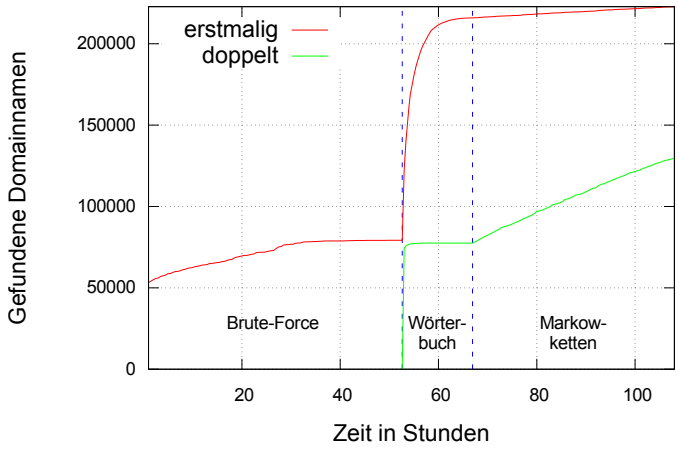

Abb. 2: NSEC3-Hashangriff auf Top-Level-Domain `com`.

Der Nutzen von NSEC3 ist in der Praxis fraglich, da der Einsatz signifikante Mehrkosten hinsichtlich CPU-Zeit und Nachrichtenlänge verursacht. Die Anzahl der Iterationen ist in der Hashfunktion als Parameter vorgesehen, um den Rechenaufwand einer Hashberechnung und damit den Schutz der Privatheit zu erhöhen, was allerdings auch die eigenen CPU-Kosten des Serverbetreibers erhöht. Tatsächlich steigt mit der Erhöhung der Iterationen sogar die relative Effizienz einer GPU gegenüber einer CPU (Abb. 3). Die NSEC3-Angriffe wurden beim *IEEE International Symposium on Network Computing and Applications* (NCA) im Jahr 2014 publiziert, wo sie mit dem *Best Student Paper Award* ausgezeichnet wurden [Wa14b].

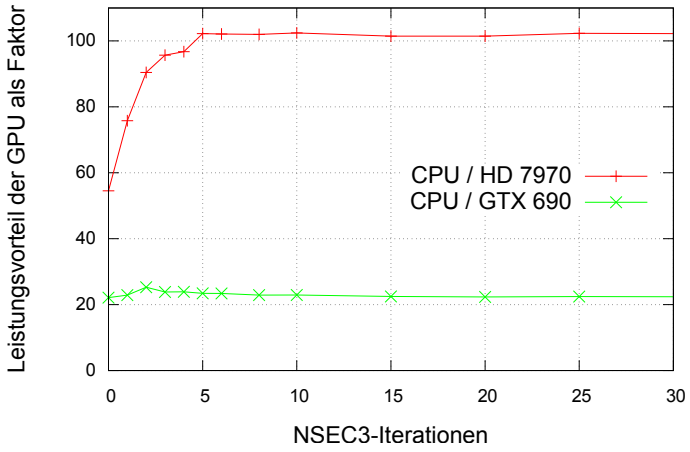

Abb. 3: Performance-Vergleich Vierkern-CPU zu GPU.

4 Verbreitung von DNSSEC

Der Einsatz von DNSSEC erfordert serverseitig die Signierung von Domains und clientseitig die Validierung von Domains und deren Signaturen. Die folgenden beiden Studien erfassen die Verbreitung auf beiden Seiten.

4.1 Serverseitige Verbreitung

Mithilfe der NSEC3-Angriffe aus Abschnitt 3.2 ist es erstmals möglich, die Anzahl der mit DNSSEC signierten Domains vollständig zu erfassen: Anfang 2015 gab es 5,1 Millionen DNSSEC-signierte Domains (Tab. 1). Die Verbreitung von DNSSEC schwankt signifikant zwischen Top-Level-Domains aufgrund von finanziellen und anderen Anreizen der Betreiber, wobei die meisten signierten Domains unterhalb der niederländischen Top-Level-Domain zu finden sind.

TLD	Konfiguration	Signierte Domains
1. `nl`	NSEC3, opt-out, $i = 5$	2 279 702
2. `br`	verschiedene	566 694
3. `cz`	NSEC3, $i = 10$	448 984
4. `com`	NSEC3, opt-out, $i = 0$	426 182
5. `se`	NSEC	349 514
[642 weitere Top-Level-Domains mit DNSSEC]		
Gesamt:		5 146 705

Tab. 1: Top-Level-Domains mit den meisten DNSSEC-signierten Domains.

Aus der Menge aller 5,1 Millionen Domains ermitteln wir die Klartextnamen mit den oben erläuterten NSEC3-Angriffen. Nach drei Wochen Rechenaufwand mit vier Grafikkarten erhalten wir den Klartextnamen von 3,4 Millionen Domains, um weitere Analysen durchzuführen. Fast alle Domains (> 99 %) sind mit RSA signiert. 13 674 (0,4 %) der Domains verwenden unsichere 512-bit lange RSA-Schlüssel, von denen einer zu Demonstrationszwecken innerhalb von drei Wochen mit einer Mehrkern-CPU gebrochen wurde[3]. 3,1 Millionen Domains (92 %) verwenden mindestens einen 1024-bit langen RSA-Schlüssel, die nach dem gegenwärtigen Stand der Wissenschaft und Technik als nicht mehr ausreichend sicher gelten. Die Empfehlung lautet an dieser Stelle auf eines der Elliptische-Kurven-Kryptosysteme umzusteigen, da sie bei kürzerer Nachrichtenlänge ein höheres Sicherheitsniveau als RSA bieten. Darüber hinaus sind 21 198 (0,6 %) der Domains aufgrund von Wartungsfehlern fehlerhaft signiert und können mit DNSSEC nicht aufgelöst werden.

4.2 Clientseitige Verbreitung

Land	Datenpunkte	ab 2012/05	2013	2014	bis 2015/03
1. Schweden	7 236	$56.4\% \pm 2.7$	$55.3\% \pm 1.5$	$55.9\% \pm 2.6$	$58.1\% \pm 4.5$
2. Tschechien	5 019	$30.6\% \pm 2.8$	$33.7\% \pm 2.0$	$41.4\% \pm 2.6$	$52.1\% \pm 4.3$
3. Finnland	2 060	$13.5\% \pm 3.4$	$25.7\% \pm 3.1$	$37.3\% \pm 3.6$	$45.4\% \pm 6.8$
4. Ukraine	12 010	$1.8\% \pm 0.6$	$33.9\% \pm 1.0$	$21.8\% \pm 2.0$	$13.9\% \pm 4.4$
5. USA	86 546	$13.5\% \pm 0.5$	$19.2\% \pm 0.4$	$26.6\% \pm 0.5$	$38.0\% \pm 0.9$

Tab. 2: Länder mit der höchsten DNSSEC-Validierungsquote ($\pm$ 95 % Konfidenzintervall).

Die Anzahl der validierenden Clients ist durch eine dreijährige webbasierte Messung von 2012 bis 2015 erfasst (Tab. 2). Nach Bereinigung der Messdaten liegen 841 026 Datenpunkte mit 556 875 eindeutigen IPv4-Adressen vor. Ähnlich wie bei der serverseitigen Verbreitung liegt auch bei der Validierung eine geographisch unterschiedliche Verteilung vor. Schweden gehört zu den frühen Anwendern von DNSSEC, wobei die Verbreitung in anderen Ländern teilweise erheblich zugenommen hat. Die Validierungsquote von 44 in der Messung vertretenen Ländern stieg im Median von 1 % (2012) auf 21 % (2015). Offen ist hierbei allerdings, ob die Validierung nahe bei den Endgeräten stattfindet, um unvertraute Kommunikationswege vollständig abzusichern. Falls die DNSSEC-Validierung lediglich auf DNS-Resolvern des Netzzugangsanbieters oder anderer Anbieter stattfindet, so ist der Kommunikationsweg zum Endnutzer angreifbar. Eine frühere Fassung dieser Studie wurde bei der *Passive and Active Measurement Conference* (PAM) im Jahr 2013 veröffentlicht [WW13].

5 DNS-Caching

Obwohl DNSSEC Ende-zu-Ende-Sicherheit bietet, erschweren zwischengeschaltete Resolver mit Cache den Einsatz von DNSSEC-Validierung auf Endgeräten. Wird eine An-

[3] Zustimmung des Domaineigentümers liegt vor.

frage aufgrund eines Validierungsfehlers wiederholt, so geben zwischengeschaltete Resolver dieselbe fehlerhafte Antwort aus dem Cache erneut zurück. Das kann z. B. durch einen Spoofing-Angriff verursacht werden, inbesondere aber auch durch eine fehlerhafte Server-Konfiguration (siehe oben: 0,6 % fehlerhafte Domains). Durch das Caching hat ein Endgerät in diesem Fall keine Möglichkeit die Namensauflösung zu wiederholen, um z. B. einen anderen Server anzufragen oder eine neue DNS-Antwort nach Korrektur des Konfigurationsfehlers zu erhalten. Im Ergebnis führt dies zu einem Denial of Service auf dem Endgerät.

Andererseits trägt DNS-Caching zur Performance und Skalierarbeit des Domain Name Systems bei, wie in dieser Arbeit mit messbasierten Simulationen gezeigt wird. Ein DNS-Resolver, der in einem Campusnetz 10 000 Clients bedient, senkt die durchschnittliche Anzahl externer Anfragen pro Cache Miss von 2,04 auf 1,32 und reduziert die durchschnittliche Auflösungszeit im 75ten Perzentil von 42 ms auf 14 ms. Daher sollten Endgeräte standardmäßig die vorhandene DNS-Infrastruktur mit Caching nutzen, bei Validierungsfehlern jedoch selbständig die DNSSEC-Zielserver anfragen, um im Cache gespeicherte, fehlerhafte DNS-Antworten zu umgehen.

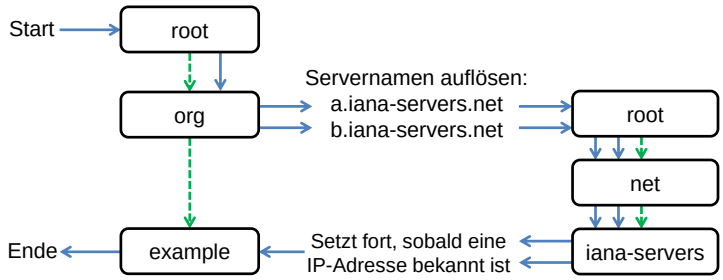

Abb. 4: Ein Resolver folgt Subdomain-Delegierungen (gestrichelte Linien), wobei zur Auflösung von Servernamen ggf. weitere Abfragen erforderlich sind (durchgezogene Linien).

Zur Ermittlung der Effektivität von DNS-Caching wird erstmals ein Simulationsmodell verwendet, das die Kosten von Folgeanfragen (Auflösung von sog. *Out-Of-Bailiwick*-Servernamen und CNAME-Aliassen) berücksichtigt. Diese sind u. a. dann notwendig, wenn der für eine Subdomain zuständige Server selbst einer anderen Domain angehört und somit zunächst der Servername aufgelöst werden muss, bevor die ursprüngliche Namensauflösung fortgesetzt wird (Abb. 4). Dadurch wird zusätzliche Netzwerklast verursacht: ohne die Auflösung von Out-Of-Bailiwick-Servernamen wären pro Namensauflösung durchschnittlich 1,58 statt 2,04 Anfragen notwendig. Daraus folgt die Empfehlung an Administratoren, *In-Bailiwick*-Servernamen mit *Glue Records* für Domain-Delegierungen zu verwenden.

6 Fazit und Ausblick

DNS-Spoofing ist ein Angriff auf die Namensauflösung des Domain Name Systems, um Clients auf den falschen Server umzuleiten oder um Zugang zu Servern und Websites zu sperren. Eine Variante des Spoofings ist DNS-Injection, das in China und im Iran einge-

setzt wird und in dieser Arbeit durch aktive Messungen im Internet nachgewiesen wurde. DNS-Injection kann auch den Netzwerkverkehr von Dritten in anderen Ländern stören, wenn deren Traffic durch ein von DNS-Injection betroffenes Netz geleitet wird. In der Praxis ist dies dann nachweisbar, wenn sich der Zielserver in China oder im Iran befindet, wobei dies auch replizierte Anycast-Knoten einschließt. DNSSEC schützt vor DNS-Spoofing und vor den unbeabsichtigten Auswirkungen von DNS-Injection auf Dritte. Innerhalb der von DNS-Injection betroffenen Netze schützt DNSSEC nur bedingt, da zwar falsche Antworten erkannt werden, aber Denial-of-Service-Angriffe möglich sind.

Das Vertrauensmodell von DNSSEC setzt voraus, dass ein Domainbetreiber den übergeordneten Domain-Autoritäten volles Vertrauen entgegenbringt (insbesondere Top-Level-Domain und Root). In Zukunft könnten Mechanismen eingeführt werden, um die Abhängigkeit zu reduzieren. So könnten z. B. stabil betriebene länderspezifische Top-Level-Domains ihre öffentlichen Schlüssel als Vertrauensanker selbständig verteilen, ohne dass Root dies beeinflussen oder überschreiben kann.

Privatheit ist bei DNSSEC lediglich in der NSEC3-Erweiterung berücksichtigt, die die Serverdatenbank vor Offenlegung schützen soll. Durch GPU-basierte Angriffe auf die NSEC3-Privatheit ist jedoch eine effiziente Wiederherstellung der Datenbank möglich. Serverbetreiber sollten daher in einer Kosten-Nutzen-Analyse abwägen, ob die moderate Verlangsamung des Angreifers die zusätzlichen Betriebskosten beim Einsatz von NSEC3 rechtfertigt. Als Abhilfe könnten GPU-Beschleuniger für DNS-Server entwickelt werden, damit Servern mehr Rechenlast für die NSEC3-Hashfunktion zur Verfügung steht. Durch die Entlastung der CPU für andere Aufgaben wäre der Server zudem weniger anfällig für Denial-of-Service-Angriffe durch NSEC3.

DNSSEC ist in der Praxis sowohl serverseitig (Signierung) als auch clientseitig (Validierung) verbreitet. Neben einigen Domains mit unsicheren Schlüssellängen verwendet die Mehrheit 1024-bit lange RSA-Schlüssel, die als nicht mehr ausreichend sicher gelten. Elliptische-Kurven-Kryptosysteme mit 256-bit langen Schlüsseln sind hierzu eine sinnvolle Alternative mit höherem Sicherheitsniveau. Ein Teil der Domains ist fehlerhaft signiert, was in Zukunft z. B. durch Domain-Monitoring und robuste Administrationswerkzeuge behoben werden könnte.

Bei der clientseitigen Verbreitung ist derzeit noch unklar, inwieweit DNSSEC-Validierung bis zu den Endgeräten durchgedrungen ist. Dies wäre notwendig, um aus DNSSEC einen Nutzen über die sichere Namensauflösung hinaus zu ziehen, z. B. für die Authentifikation von digitalen Zertifikaten mit DANE. Problematisch sind bei einer Validierung auf dem Endgerät zwischengeschaltete Cache-Komponenten, da diese zwar die Performance und Skalierbarkeit verbessern, aber durch das Zwischenspeichern von falschen Antworten die Verfügbarkeit senken.

Weiterer Forschungsbedarf besteht darin, wie ein universeller Transport von DNSSEC-Nachrichten bis zu allen Endgeräten umgesetzt werden kann. So könnten z. B. automatische Tunneling-Lösungen Validierung auf Endgeräten ermöglichen, auch wenn DNSSEC-Nachrichten aufgrund von dazwischen geschalteten Middleboxen nicht zuverlässig transportiert werden können.

Literaturverzeichnis

[Ar05] Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S.: , DNS Security Introduction and Requirements. RFC 4033, März 2005.

[DH15] Dukhovni, V.; Hardaker, W.: , SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS). RFC 7672 (Proposed Standard), Oktober 2015.

[He14] Herrmann, Dominik: Beobachtungsmöglichkeiten im Domain Name System: Angriffe auf die Privatsphäre und Techniken zum Selbstdatenschutz. Dissertation, Universität Hamburg, 2014.

[Wa14a] Wander, Matthäus; Boelmann, Christopher; Schwittmann, Lorenz; Weis, Torben: Measurement of Globally Visible DNS Injection. Access, IEEE, 2:526–536, 2014.

[Wa14b] Wander, Matthäus; Schwittmann, Lorenz; Boelmann, Christopher; Weis, Torben: GPU-Based NSEC3 Hash Breaking. In: Network Computing and Applications (NCA), 2014 IEEE 13th International Symposium on. IEEE, S. 137–144, 2014.

[Wa15] Wander, Matthäus: The Impact of DNSSEC on the Internet Landscape. Dissertation, Universität Duisburg-Essen, 2015.

[WW13] Wander, Matthäus; Weis, Torben: Measuring Occurrence of DNSSEC Validation. In: Passive and Active Measurement, Jgg. 7799 in Lecture Notes in Computer Science, S. 125–134. Springer Berlin Heidelberg, 2013.

Matthäus Wander promovierte an der Universität Duisburg-Essen und ist dort derzeit als Lehrender tätig. Zu seinen Forschungsinteressen gehören IT-Sicherheit, Rechnernetze und Internetmessungen. Während seiner Tätigkeit als wissenschaftlicher Mitarbeiter veröffentlichte er auch Forschungsarbeiten über Peer-to-Peer-Techniken. Davor war er bis 2009 als Functional Safety Engineer beim TÜV NORD tätig. Das Studium der Angewandten Informatik schloss er 2008 mit Diplom ab.