Digital Business University
of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Informationstechnik für Cyber- & IT-Security

Wintersemester 2024/25

Sichere Namensauflösungen: Die Rolle von DNS over TLS (DoT), DNS over HTTPS (DoH) & DNSSEC

Studienarbeit

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
Prof. Dr. Mukayil Kilic

7. Februar 2025

Inhaltsverzeichnis

Abkürzungsverzeichnis

CIA	Confidentiality, Integrity, Availability
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoQ	DNS over QUIC
DoS	Denial of Service
DoT	DNS over TLS
DS	Delegation Signer
FQDN	Fully Qualified Domain Name
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
MITM	Man-in-the-Middle
NSEC	Next Secure
NTP	Network Time Protocol
ODoH	Oblivious DNS over HTTPS
RFC	Request for Comments
RRSIG	Resource Record Signature
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLD	Top Level Domain
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

1 Einleitung

Ohne DNS kein Internet – so könnte eine kurze Zusammenfassung über die Bedeutung des für die Namensauflösung genutzten, global verbreiteten Systems lauten. Womöglich wäre das Internet auch ohne den Einsatz eines DNS nutzbar; fraglich wäre allerdings, ob es dann eine solch enorme Verbreitung gefunden hätte. Die Rolle des DNS ist insofern eine besonders wichtige, da sie die Anwendung erleichtert, Prozesse optimiert und alle Fäden des Internets zusammenhält.

Das DNS gilt als einer der Urväter des Internets und wurde schon früh für seine Einfachheit und seinen hohen Wirkungsgrad bewundert. Mit der fortlaufenden Expansion des Internets und der Tatsache, dass immer mehr Menschen Zugang dazu erhielten und Organisationen mit dem Aufbau eigener Netzwerke begannen, entwickelte sich auch die Rolle des DNS stetig weiter. Nicht zuletzt geriet es durch seine Popularität auch immer mehr in den Fokus von Angreifern, die in dem essenziell wichtigen System Angriffsziele für die dahinterliegenden Infrastrukturen und nicht zuletzt deren Nutzer*innen und Organisationen fanden.

1.1 Problemstellung

Im Jahr 2009 wurde *Twitter* (heute: *X*) Opfer eines *Social Engineering*-Angriffs durch die iranische Cyber-Armee, bei dem DNS-Einträge verändert wurden und dadurch der gesamte Datenverkehr auf eine Propaganda-Website umgeleitet wurde (Hudaib & Hudaib, 2014). Sieben Jahre später wurde der gleiche DNS-Hoster Ziel eines erfolgreichen DDoS-Angriffs, bei dem Dienste wie *Netflix*, *PayPal* und *Spotify* für längere Zeit nicht erreichbar waren (Bushart et al., 2018).

Dies sind nur zwei Beispiele, die aufzeigen, welch wichtige Rolle das DNS für das Internet einnimmt. Gleichzeitig offenbart es, dass auch das DNS Schwächen hat, die mitunter enorme Auswirkungen haben können und durch die der Bedarf an sicheren Namensauflösungen ansteigt. Diese Arbeit befasst sich daher mit folgenden Fragestellungen: Wie kann klassisches DNS abgesichert werden, um sichere Namensauflösungen zu ermöglichen? Und welche Rolle spielen Technologien wie DoT, DoH und DNSSEC, wenn es darum geht, Vertraulichkeit und Integrität zu gewährleisten?

1.2 Inhalte der Arbeit

Kapitel 2 befasst sich zunächst mit den Grundlagen des DNS und listet mögliche Angriffsvektoren auf. DoT und DoH werden anschließend in Kapitel 3 vorgestellt und es wird aufgezeigt, welche Möglichkeiten im Rahmen der Verschlüsselung von DNS-Anfragen sie bieten. Maßnahmen zur Sicherstellung der Integrität durch DNSSEC werden anschließend in Kapitel 4 vorgestellt, bevor in Kapitel 5 alle Inhalte zusammengefasst und zukünftige Weiterentwicklungen aufgegriffen werden.

2 Domain Name System (DNS)

Das *Domain Name System (DNS)* ist eine redundante, hierarchische, verteilte Datenbank, die zur Weitergabe von Informationen über Domänennamen verwendet wird (Liska & Stowe, 2016, S. 1). Sie findet hauptsächlich zur *Namensauflösung* im Internet Anwendung, indem ein verteiltes Netz an miteinander verbundenen *DNS-Servern* den Weg eines Domänennamens zu einer konkreten *Internet Protocol (IP)-Adresse* aufzeigt.

2.1 Domänenname

Den Grundbestandteil eines Domänennamens bildet die Wurzel (**Root**), die immer leer ist. Die Domäne oberster Stufe wird **Top Level Domain (TLD)** genannt, gefolgt von der **Second Level Domain**. Weitere Stufen werden entsprechend hochgezählt. Der gesamte Domänenname wird auch als *Fully Qualified Domain Name (FQDN)* bezeichnet (Liska & Stowe, 2016).

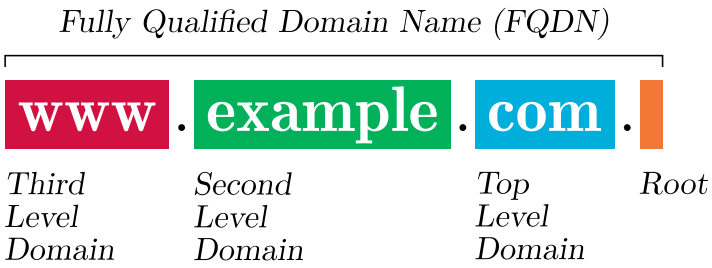

Abbildung 1: Aufbau eines Domänennamens

2.2 DNS-Server

Wenn im Zuge einer Namensauflösung eine sog. *DNS-Query* versendet wird, erfolgt die Abfrage unter Einbeziehung verschiedener DNS-Server (nach Liska und Stowe (2016)):

- **Rekursiver Nameserver** (auch *DNS-Resolver*): Er wird in der Regel von einem *Internet Service Provider (ISP)* oder in einem lokalen Netzwerk betrieben und fungiert als primäre Anlaufstelle für die Namensauflösung. Eingehende DNS-Queries beantwortet er direkt oder leitet sie an einen der 13 Root-Server weiter.
- **Root-Server**: Sie verwalten maßgebliche Informationen über Domänen und sind auf der ganzen Welt verteilt. Außerdem existieren eine Reihe von **TLD-Root-Servern**, die für jede verfügbare TLD spezifische Domänendaten verwalten.
- **Autoritativer Nameserver**: Er verwaltet alle Informationen eines konkreten Domänennamens. Dies muss er in Form einer Registrierung bei dem zuständigen TLD-Root-Server anmelden, damit dieser ihn bei der Namensauflösung anfragt.

2.3 Angriffsvektoren des klassischen DNS

Das DNS zählt zu einem der essenziellen Bestandteile des Internets, das für alle Benutzer*innen zugänglich sein soll. Entsprechend wird vorausgesetzt, dass DNS-Server öffentlich erreichbar und einfach zu bedienen sind. Dadurch bietet es eine breite Angriffsfläche für Attacken jeglicher Art (Usman Aijaz et al., 2020).

2.3.1 Cache Poisoning

Ein DNS-Server speichert aufgelöste Daten zu einem Domänenname für eine gewisse Zeit, der sog. *Time to Live (TTL)*, in seinem Zwischenspeicher (*Cache*). Liegen noch keine Daten im Cache, beginnt der DNS-Server mit der Namensauflösung. Dabei kann es vorkommen, dass ihm ein anderer DNS-Server falsche Informationen übermittelt, die nun für die im TTL angegebene Dauer in seinem Cache gespeichert sind.

Böswilliges Cache Poisoning wird auch als *DNS-Spoofing* bezeichnet (Bansal et al., 2020). Es kann dazu führen, dass Benutzer*innen auf bösartige Seiten geleitet werden, über die ein Angreifer sensible Daten abgreifen kann (Usman Aijaz et al., 2020).

2.3.2 Packet Sniffing & Packet Interception

Beim klassischen DNS werden DNS-Queries und entsprechende Antworten als unverschlüsselte und unsignierte *User Datagram Protocol (UDP)*-Pakete versendet. Dieser Datenverkehr kann von jedem mitgelesen werden, der ebenfalls Zugriff zum Netzwerk hat (Usman Aijaz et al., 2020). *Man-in-the-Middle (MITM)*- oder andere Abhörangriffen (sog. *Eavesdropping*) erlauben darüber hinaus, den Datenverkehr nach Belieben zu verändern und zu manipulieren (Bansal et al., 2020; Liska & Stowe, 2016).

2.3.3 Denial of Service (DoS)

Schwach konfigurierte DNS-Server sind häufig anfällig für *Denial of Service (DoS)*- und *Distributed Denial of Service (DDoS)*-Angriffe. Dabei werden gefälschte DNS-Queries versendet, deren Antworten eine größere Datenmenge als gewöhnlich enthalten, wodurch mehr Ressourcen gebunden und in der Folge gültige Anfragen verweigert werden können (Bansal et al., 2020). Einzelne Formen von DoS-Angriffen gegen das DNS werden anschaulich in Bushart et al. (2018, S. 142–147) aufgezeigt.

2.3.4 DNS-Hijacking

Wenn die DNS-Einstellungen eines Geräts oder Netzwerks aktiv durch Angreifer oder Schadsoftware verändert werden, kann dies dazu führen, dass Nutzer*innen zu gefälschten oder schädlichen Webseiten geleitet werden, ohne es zu bemerken. Damit hat sich DNS-Hijacking wiederholt als eine der größten Bedrohungen für das DNS erwiesen (Houser et al., 2021).

3 Verschlüsselung von DNS-Anfragen

Gemäß der *Confidentiality, Integrity, Availability (CIA)-Triade* ist Verschlüsselung eine wichtige Maßnahme zur Sicherstellung der Vertraulichkeit. Mit dem *Request for Comments (RFC)* 7258 wurde deutlich, dass Verschlüsselung auch eine wichtige Maßnahme bei der Gestaltung von Internetprotokollen darstellt (Farrell & Tschofenig, 2014). Entsprechend wurde es notwendig, das klassische DNS zu erweitern.

3.1 DNS over TLS (DoT)

Als erste Reaktion auf die Veröffentlichung des RFC 7258 wurde etwa zwei Jahre später *DNS over TLS (DoT)* als RFC 7858 veröffentlicht (Hu et al., 2016).

3.1.1 DNS-Transaktionen durch sicheren TLS-Kanal

Mit DoT werden DNS-Queries innerhalb eines verschlüsselten *Transport Layer Security (TLS)*-Kanals über Port 853 mithilfe des *Transmission Control Protocol (TCP)* übertragen (Badhwar, 2021; Hu et al., 2016). Dabei findet eine aktive Authentifizierung durch TLS-Zertifikate zwischen Client und DNS-Server statt. Damit diese miteinander kommunizieren können, erfolgt vor der eigentlichen Transaktion ein *TLS-Handshake*. Da jegliche DNS-Transaktionen direkt in den sicheren TLS-Kanal eingebettet sind, können übermittelte Daten von außen nicht ausgelesen und verändert werden (Bertola et al., 2020).

DoT ist ein wirksames Mittel gegen Packet Sniffing und Packet Interception. Es ist außerdem eine erste wichtige Maßnahme zur Vermeidung von DNS-Spoofing, da durch die Verschlüsselung auch die Integrität der übermittelten Daten erhöht wird (OECD, 2022). Obwohl DoT bereits Vertraulichkeit und (in Teilen) Integrität gewährleistet, ist es wichtig zu erwähnen, dass dadurch weder Cache Poisoning noch DNS-Hijacking wirksam bekämpft werden können (Badhwar, 2021).

3.1.2 Downgrade durch SSL-Stripping

Wenn der separat genutzte Port durch ISPs oder Firewalls geblockt ist, weil etwa zusätzliche Freigabeverfahren notwendig sind oder eine *Blocklist* angewendet wird, kann *Secure Sockets Layer (SSL)-Stripping* auftreten. Dabei wird explizit von verschlüsseltem DoT auf unverschlüsseltes DNS gewechselt, um DNS-Queries weiterhin zu ermöglichen. Dies hat zur Folge, dass DoT aktiv ausgehebelt wird (Bertola et al., 2020).

3.2 DNS over HTTPS (DoH)

Ein weiterer Schritt in Richtung sicherer Namensauflösungen erfolgte mit dem als RFC 8484 veröffentlichten *DNS over HTTPS (DoH)* (Hoffman & McManus, 2018).

3.2.1 Sichere Namensauflösung per HTTPS

Bei DoH wird zur Kommunikation das verschlüsselte *Hypertext Transfer Protocol Secure (HTTPS)* über TCP-Port 443 eingesetzt. Dieses wird auch für den üblichen Datenverkehr in Netzwerken verwendet (Bertola et al., 2020). DNS-Queries werden dabei über einen *Uniform Resource Identifier (URI)* an einen öffentlichen DNS-Server versendet; beispielsweise stellt Google unter `https://dns.google/dns-query` einen solchen DoH-kompatiblen Server bereit (Huang et al., 2020).

Üblicherweise erfolgt der Prozess bei der Kommunikation über DoH in zwei Phasen. Zunächst wird eine unverschlüsselte, klassische DNS-Query versendet, um den URI aufzulösen. Dessen Domänenname dient dabei nicht nur zur Namensauflösung des eigentlichen DoH-Servers, sondern ermöglicht auch seine Identitätsprüfung durch Verifikation des SSL-Zertifikats. Für die weitere Kommunikation wird nun eine verschlüsselte TLS-Verbindung aufgebaut, über die anschließend einzelne DNS-Queries mittels `GET` oder `POST` ausgeführt werden können (Huang et al., 2020).

3.2.2 Hohe Kompatibilität

Eine der zentralen Eigenschaften von DoH ist die gemeinsame Nutzung von Port 443, der in aller Regel von ISPs und Firewalls nicht blockiert wird. Dadurch ist es im Vergleich zu DoT weniger anfällig für SSL-Stripping und erreicht zudem eine hohe Kompatibilität bei Geräten und in (öffentlichen) Netzwerken. (Bertola et al., 2020). Wie auch bei DoT verhindert DoH Packet Tracing und Packet Interception und reduziert das Risiko für DNS-Spoofing, was insbesondere in öffentlichen Netzwerken (Flughäfen, Hotels etc.) von wichtiger Bedeutung für den Schutz der eigenen Daten ist (Bertola et al., 2020; Blidborg & Gunnarsson, 2020).

3.2.3 Sicherheits- und Datenschutzbedenken

Die Bereitstellung öffentlicher DoH-Server beschränkt sich zumeist auf einige wenige große Anbieter wie Google oder Cloudflare, was in puncto Tracking und Datenaggregation problematisch sein kann (Bertola et al., 2020). Schon 2019 wurden daher Maßnahmen zur Implementierung öffentlicher, zentraler DoH-Server entworfen und Vorschläge zur Dezentralisierung entwickelt (Livingood et al., 2019). Darüber hinaus kann Zentralisierung zu einem Sicherheitsproblem werden, wenn durch dessen Nutzung ein lokaler DNS-Resolver umgangen wird und interne Informationen stattdessen an den zentralen DoH-Server geteilt werden (Blidborg & Gunnarsson, 2020).

In Organisationen besteht darüber hinaus die Gefahr, dass ein beispielsweise eingesetztes *Intrusion Detection System (IDS)* ein- und ausgehende DNS-Transaktionen nur noch sehr schwer analysieren kann, da sie mit üblichem Web-Traffic vermischt werden (Blidborg & Gunnarsson, 2020). Nicht zuletzt stellt die initiale Namensauflösung in der ersten Phase von DoH ein weiteres Sicherheitsproblem dar (Huang et al., 2020).

4 Maßnahmen zur Integrität von DNS-Transaktionen

Wie im vorangegangenen Kapitel dargestellt, reicht Verschlüsselung allein nicht aus, um sichere Namensauflösungen durchzuführen. Obwohl DNS-Transaktionen durch DoT und DoH vertraulich durchgeführt werden können, fehlt ein Mechanismus zur Feststellung der Integrität und Authentizität.

4.1 Domain Name System Security Extensions (DNSSEC)

Lange bevor überhaupt Entwürfe hinsichtlich der Verschlüsselung von DNS-Anfragen publiziert wurden, erschien bereits im Jahr 1999 die erste Version der *Domain Name System Security Extensions (DNSSEC)* als RFC 2535 (Eastlake 3rd, 1999). Es folgten weitere Veröffentlichungen als RFC 4033, 4035, 4036, 5155 und 6840 (Badhwar, 2021).

4.1.1 Integrität durch kryptografische Signaturen

Mit DNSSEC wurde erstmals ein Mechanismus zur Validierung gültiger DNS-Transaktionen bereitgestellt. Ein DNSSEC-kompatibler DNS-Server sendet neben der Antwort auf eine DNS-Query auch eine kryptografische Signatur (sog. *Resource Record Signature (RRSIG)*) mit, anhand derer die Integrität der Nachricht überprüft werden kann (Bansal et al., 2020).

Das Signieren und Validieren erfolgt über private und öffentliche Schlüssel der einzelnen DNS-Server und folgt damit dem Prinzip der *Public-Key-Verschlüsselung*. Der Signaturprozess beginnt dabei stets beim Root-Server, dessen öffentlicher Schlüssel üblicherweise im DNS-Resolver hinterlegt ist. Für jeden beteiligten DNS-Server bis hin zum zonenverantwortlichen autoritativen Nameserver erfolgt die Weitergabe eines öffentlichen Schlüssels als sog. `DNSKEY`-Record immer vom vorausgehenden DNS-Server. Sog. *Delegation Signer (DS)*-Records ermöglichen dabei eine sichere Verbindung zwischen den einzelnen DNS-Zonen. Dadurch wird eine Vertrauenskette (*chain of trust*) aufgebaut, welcher der anfragende Client ultimativ vertrauen kann (Liska & Stowe, 2016; Usman Aijaz et al., 2020).

4.1.2 Validierung der Nicht-Existenz eines Domänennamens

Üblicherweise können DNS-Server nicht beweisen, dass ein nicht existierender Domänenname tatsächlich nicht vorhanden ist. Dies schafft Raum für Cache Poisoning, indem ein Angreifer die Nicht-Existenz ausnutzt und hierfür einen gefälschten DNS-Eintrag vorgibt, etwa durch einen gezielten MITM-Angriff. Zur Vorbeugung eines solchen Angriffs wurde in DNSSEC die Angabe von *Next Secure (NSEC)*-Records integriert. Hierbei werden alle in der aktiven DNS-Zone verfügbaren Domänennamen als einzelne `NSEC`-Records aufgelistet, sodass die Nicht-Existenz eines Domänennamens verifiziert werden kann, wenn dieser nicht abgebildet ist (Badhwar, 2021; Bansal et al., 2020).

4.1.3 Schwachstellen von DNSSEC

DNSSEC bietet keinen effektiven Schutz vor DDoS-Angriffen. Tatsächlich ist es im Vergleich zum klassischen DNS anfälliger dafür, weil die übermittelten Datenmengen aufgrund der zusätzlichen `DNSKEY`-, `DS`- und `RRSIG`-Records viel größer sind. Damit können bei DNSSEC deutlich einfacher sog. *Amplification-Angriffe* gefahren werden (Badhwar, 2021; Bansal et al., 2020; OECD, 2022).

Eine weitere Problematik besteht in der Offenlegung potenziell geheimer Informationen aus einer DNSSEC-kompatiblen Zone. Bei dem als *Zone Walking* bekannten Angriff werden explizit alle verfügbaren Domänennamen einer Zone über `NSEC`-Records bekannt gegeben, wodurch einzelne Subdomains ermittelt und bestimmte Schemata erraten werden können. Eine Lösung stellen moderne Weiterentwicklungen wie `NSEC3` und `NSEC5` dar, bei denen zusätzliches Hashing eingesetzt wird (Badhwar, 2021; Liska & Stowe, 2016).

Wie jeder übermittelte DNS-Record haben auch DNSSEC-Signaturen eine Ablaufzeit (TTL). Erhält ein Angreifer die Möglichkeit, die Systemzeit eines DNS-Resolvers zu manipulieren, so ist DNSSEC anfällig für diese Form von *Network Time Protocol (NTP)*-Attacken, da durch die Veränderung der Systemzeit Signaturen und Schlüssel vorzeitig als ungültig erscheinen (Badhwar, 2021).

Darüber hinaus bietet DNSSEC keine Vertraulichkeit und Verfügbarkeit des DNS, sondern sichert lediglich die Integrität der übermittelten Nachrichten (OECD, 2022).

4.2 Kombination von DoT/DoH und DNSSEC

Die Vorteile von DoT und DoH in Kombination mit den Möglichkeiten, die sich durch den Einsatz von DNSSEC ergeben, stellen eine solide Basis für den Einsatz sicherer Namensauflösungen im DNS dar. DoT/DoH sichern Vertraulichkeit, indem DNS-Transaktionen über einen sicheren, verschlüsselten Kanal durchgeführt werden, und DNSSEC sorgt für die Integrität der übermittelten Nachrichten, indem diese mit einer kryptografischen Signatur versehen werden. Die Technologien sorgen insgesamt für einen guten Schutz vor vielen verbreiteten Angriffen wie Cache Poisoning, DNS-Spoofing, Packet Sniffing und Packet Interception. Dennoch bieten sie keinen ausreichenden Schutz vor DoS- und DDoS-Angriffen und ermöglichen weiterhin DNS-Hijacking. Verglichen zum klassischen, ungeschützten DNS sind sie jedoch bereits ein großer und wichtiger Schritt in Richtung eines sichereren DNS (Usman Aijaz et al., 2020).

5 Zusammenfassung

5.1 Ergebnisse

DoT, DoH und DNSSEC verfolgen unterschiedliche Ziele in der Anwendung. Jede Technologie nimmt eine wichtige Rolle bei der Etablierung sicherer Namensauflösungen ein. Allerdings ist es nicht ausreichend, nur eine der Technologien zu verwenden; erst durch ihre Symbiose entfalten sie ihr ganzes Potenzial. DoT und DoH stellen hierbei die Vertraulichkeit der übersendeten DNS-Transaktionen sicher, indem Verschlüsselung eingesetzt wird; DNSSEC kann als Technologie zur Sicherstellung der Integrität übermittelter Nachrichten angewendet werden. So decken die Technologien gemeinsam zwei Drittel der CIA-Triade ab und stellen einen wichtigen Schritt in Richtung sicherer Namensauflösungen im DNS dar.

Cache Poisoning, DNS-Spoofing, Packet Sniffing und Packet Interception sind nur einige wenige Angriffsvektoren, denen die vorgestellten Technologien entgegenwirken. Offen bleiben etwa DoS- und DDoS-Angriffe sowie DNS-Hijacking, das als eine der größten Bedrohungen für das DNS gilt. Nicht alle Schwachstellen lassen sich also gänzlich lösen; nichtsdestotrotz ist beispielsweise der Einsatz von DoH mittlerweile weit verbreitet und hat sich quasi etabliert. Ein etwas sichereres DNS ist immer noch besser geeignet als ein unsicheres, unverschlüsseltes DNS. Es gilt aber weiterhin, Technologien für ein noch besseres DNS zu finden, um alle Benutzer*innen des Internets vor weiteren Angriffen zu schützen.

5.2 Ausblick

Eine relativ neuartige Technologie ist *Oblivious DNS over HTTPS (ODoH)*. Es soll verhindern, dass DoH-Server Kenntnis von Absender und Ziel einer DNS-Query erhalten. Hierzu wird ein zusätzlicher Proxy-Server zwischen Client und DoH-Server geschaltet, sodass der ursprüngliche Absender für den DoH-Server unerkannt bleibt. Der Proxy-Server hingegen sieht nur den Absender, nicht jedoch den tatsächlich angefragten Domänennamen. Die Technologie, die als RFC 9230 veröffentlicht wurde, trägt somit wesentlich zu mehr Datenschutz bei (Singanamalla et al., 2020).

Ebenfalls interessant ist die Entwicklung von *DNS over QUIC (DoQ)* (RFC 9250), bei der anstelle von TCP das von Google entwickelte QUIC-Protokoll für die Namensauflösung verwendet wird. Es zeichnet sich durch eine bessere Performance aus, da es mit schnellerem Handshake und zeitgleich weniger Latenz arbeitet und darüber hinaus Multiplex-Verbindungen ermöglicht (Badhwar, 2021).

In Bezug auf DNSSEC gilt es, die Entwicklung von *Post-Quantum DNSSEC* im Auge zu behalten. Dabei handelt es sich um Maßnahmen, um langfristige Sicherheit durch stärkere Signaturen zu gewährleisten und dadurch der zunehmenden Rechenpower von Quantencomputern entgegenzuwirken (Müller et al., 2020).

Literaturverzeichnis

Badhwar, R. (2021). Domain Name System (DNS) Security. In *The CISO's Next Frontier* (S. 207–212). Springer International Publishing.

Bansal, M. K., Sethumadhavan, M., Kumar, Y., Singh, P. K., Paprzycki, M., Sood, S., Pljonkin, A., Hong, W.-C., Hong, W.-C., Kumar, Y., Singh, P. K., Sood, S., Pljonkin, A., & Paprzycki, M. (2020). Survey on Domain Name System Security Problems - DNS and Blockchain Solutions. In *Futuristic Trends in Networks and Computing Technologies* (S. 634–647, Bd. 1206). Springer Singapore Pte. Limited.

Bertola, V., Elmerot, C., Greer, C., Grob, T., Hubert, B., Koetter, P. B., Landefeld, K., Pohlmann, P. D. N., Rickert, T., & Strotmann, C. (2020). *Discussion Paper: DNS over HTTPS* (Techn. Ber.). eco – Association of the Internet Industry.

Blidborg, E., & Gunnarsson, C. (2020). Cache Poisoning in DNS over HTTPS clients.

Bushart, J., Rossow, C., Stamatogiannakis, M., Holz, T., Bailey, M., Ioannidis, S., Bailey, M., Holz, T., Ioannidis, S., & Stamatogiannakis, M. (2018). DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. In *Research in Attacks, Intrusions, and Defenses* (S. 139–160, Bd. 11050). Springer International Publishing AG.

Eastlake 3rd, D. E. (1999). Domain Name System Security Extensions. https://doi.org/10.17487/RFC2535

Farrell, S., & Tschofenig, H. (2014). Pervasive Monitoring Is an Attack. https://doi.org/10.17487/RFC7258

Hoffman, P. E., & McManus, P. (2018). DNS Queries over HTTPS (DoH). https://doi.org/10.17487/RFC8484

Houser, R., Hao, S., Li, Z., Liu, D., Cotton, C., & Wang, H. (2021). A comprehensive measurement-based investigation of DNS hijacking. *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*, 210–221.

Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., & Hoffman, P. E. (2016). Specification for DNS over Transport Layer Security (TLS). https://doi.org/10.17487/RFC7858

Huang, Q., Chang, D., & Li, Z. (2020). A comprehensive study of {DNS-over-HTTPS} downgrade attack. *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*.

Hudaib, A. A. Z., & Hudaib, E. (2014). DNS advanced attacks and analysis. *International Journal of Computer Science and Security (IJCSS)*, *8*(2), 63.

Liska, A., & Stowe, G. (2016). *DNS Security: Defending the Domain Name System* (1. Aufl.). Elsevier Science & Technology Books.

Livingood, J., Antonakakis, M., Sleigh, B., & Winfield, A. (2019). *Centralized DNS over HTTPS (DoH) Implementation Issues and Risks* (Internet-Draft Nr. draft-

livingood-doh-implementation-risks-issues-04) (Work in Progress). Internet Engineering Task Force. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/04/

Müller, M., de Jong, J., van Heesch, M., Overeinder, B., & van Rijswijk-Deij, R. (2020). Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. *ACM SIGCOMM Computer Communication Review*, *50*(4), 49–57.

OECD. (2022). Security of the Domain Name System (DNS): An introduction for policy makers. *OECD Digital Economy Papers*, (331).

Singanamalla, S., Chunhapanya, S., Vavruša, M., Verma, T., Wu, P., Fayed, M., Heimerl, K., Sullivan, N., & Wood, C. (2020). Oblivious dns over https (odoh): A practical privacy enhancement to dns. *arXiv preprint arXiv:2011.10121*.

Usman Aijaz, N., Misbahuddin, M., Raziuddin, S., Shukla, S., Unal, A., Mishra, D. K., Jat, D. S., Shukla, S., Unal, A., Jat, D. S., & Mishra, D. K. (2020). Survey on DNS-Specific Security Issues and Solution Approaches. In *Data Science and Security* (S. 79–89, Bd. 132). Springer.

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Studienarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der Übersicht verwendeter (gen)KI-Tools habe ich sämtliche eingesetzte (gen)KI-Tools, deren Einsatzform sowie die jeweils betroffenen Teile der Arbeit einzeln aufgeführt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Übersicht verwendeter (gen)KI-Tools

Die (gen)KI-Tools habe ich, wie im Folgenden dargestellt, eingesetzt.

(gen)KI-Tool	**Einsatzform**	**Betroffene Teile der Arbeit**
ChatGPT	Generierung von ersten Ideen für eine geeignete Gliederung	Gesamte Arbeit
	Generierung von Zusammenfassungen verschiedener Literaturwerke	Gesamte Arbeit

Münster, 7. Februar 2025

Elias Häußler