Masterstudiengang

Informatik

Globale Anwendung von Certificate Authorities

Masterarbeit

vorgelegt von

Tobias Weiden

aus Attenkirchen

Inhaltsverzeichnis

Abstract. Mithilfe von TLS/SSL wird ein Großteil der vertrauenswürdigen Kommunikation zwischen Client und Server im Internet sichergestellt. Diese beruhen auf der Public Key Infrastrukture und den darin enthalten Certificate Authorities und Zertifikaten. Allerdings ist es bekannt, dass durch eine missbrauchte Zwischen-CA Man-in-the-Middle-Angriffe durchgeführt werden können. Dafür muss der Angreifer zwischen Client und Server positioniert sein. In dieser Masterarbeit wird untersucht, ob sich die Zertifikate und CAs je nach Standort des Nutzers unterscheiden. Dazu wird eine VPN-Verbindung zu Server-Standorten auf der ganzen Welt aufgebaut und mit diesen Internet-Zugängen die Zertifikatsketten der Top-Domänen nach Alexa und Cisco gesammelt. Für die TLS-Handshakes wird ZMap bzw. ZGrab2 genutzt. In der anschließenden Analyse werden die Zertifikate der Domänen und (Sub-)CAs zwischen den genutzten VPN-Standorten verglichen. Es stellt sich heraus, dass fast alle Zertifikate der gleichen Domänen übereinstimmen und damit auch die der (Sub-)CAs. Allerdings variiert die Aussagekraft dieser Analyse je nach VPN-Standorten, da insbesondere bei den afrikanischen und asiatischen Standorten die Menge der erfolgreichen TLS-Handshakes vergleichsweise deutlich geringer ist. Somit empfiehlt sich eine strikte Umgangsweise mit (Sub-)CA-Zertifikaten und Misstrauen gegenüber Zertifikate, die von anderen (Sub-)CAs ausgestellt werden als gewohnt.

1 Einleitung

Von E-Commerce und Online-Banking zu (intimer) Kommunikation via Email oder Chat: All diese Internet-Transaktionen werden millionenfach jeden Tag durchgeführt. Der Browser-Nutzer sieht ein Schloss in der Adresszeile und die Farbe dieser ändert sich. Es zeigt: diese Aktionen werden durch SSL geschützt. [38]

Secure Socket Layer (SSL) und als Nachfolger Transport Layer Security (TLS) sichern als Verschlüsselungs-Protokoll eine vertrauenwürdige Kommunikation über das Internet. Hierbei können Nutzer/Clients die Identität des gewünschten Servers über ein X.509 digitales Zertifikat kontrollieren. Diese werden von einer Certificate Authority (CA) ausgestellt, welcher der Nutzer vertrauen muss, um dann auch von der Identität des zertifizierten Servers überzeugt zu sein. In der Praxis hat ein Browser oder ein Betriebssystem eine Liste an CAs schon als vertrauenswürdig voreingestellt. Jedes Zertifikat, das von einem dieser CAs ausgestellt wurde, wird gleichsam vertraut. Hinzu kommt, dass es keine Einschränkung gibt, welchen Servern oder Domänen ein Zertifikat ausgestellt werden darf. Somit könnte eine kompromittierte, als vertrauenswürdig eingestufte CA Zertifikate für alle Websites ausgeben und sich somit als diese ausgeben. [20]

Diese CAs werden zusammengenommen als Public Key Infrastructure (PKI) bezeichnet. Sie werden so genannt, weil in einem Zertifikat neben dem Namen des Zertifizierten und des Herausgebers auch der Public Key des Zertifizierten enthalten ist. Diesen nutzen wir, um unsere Nachricht zu verschlüsseln, welche dann nur mit dem dazu passenden Private Key entschlüsselt werden kann. Dieser sollte nur im Besitz des Zertifizierten liegen. Diese PKI ist also aufgrund der Gleichberechtigung der CAs und deren Ausstellungsfähigkeiten nur so sicher, wie die schwächste CA. Allerdings wird die PKI immer größer, mit mehr CAs, Zwischen-CAs und Zertifikaten. Das Problem dabei ist, dass nicht dokumentiert ist, welche Zertifikate die jeweilige CA alle ausgestellt haben. Wir wissen erst von einem Zertifikat, wenn wir diesem "begegnen", also ein Server uns dieses beim Verbindungsaufbau zusendet. Es kann also auch

ein Zertifikat für eine Domäne ausgestellt werden ohne, dass diese davon weiß. [15]

Nun ist es nicht unüblich, dass wir auch im Ausland Dienste im Internet nutzen. Allerdings gibt es hier die theoretische Gefahr, dass ein Man-in-the-Middle-Angriff durchgeführt werden kann, wenn bspw. dort eine Regierung die SSL-Verbindung zu unserem Wunsch-Server abfängt und mittels einem Zertifikat, ausgegeben von der eigenen CA für den vermeintlichen angesprochenen Server, sich als gewünschtes Ziel ausgibt. Hierfür müsste natürlich die CA in unserer vordefinierten Liste als vertrauenswürdig eingestuft werden. Außerdem wäre ein solches Vorgehen leicht zum Täter zurückzuverfolgen. Allerdings beinhalten die Listen von u.a. Mozilla (Firefox) und Microsoft deutlich mehr als hundert CAs, darunter auch viele Nicht-Kommerzielle oder von Regierungen. Es macht auch Sinn, dass bspw. Bewohner von Estland sicher und verschlüsselt Dienste ihres Staates online nutzen können, allerdings wäre es zumindest fragwürdig, wenn bspw. in Amerika sich heimische Banken mit Zertifikaten, ausgegeben von eben dieser estländischen CA, identifizieren. Dennoch würde dies dem Nutzer im Browser nicht auffallen, da auch diese CA als vertrauenswürdig eingestuft wurde, und somit auch das Zertifikat der Bank als sicher gilt. [15][38]

Natürlich können je nach Region, in der man sich befindet, unterschiedliche Zertifikate von verschiedenen CAs genutzt werden. Daher ergibt sich folgende **Forschungsfrage**:

> Unterscheiden sich CAs an verschiedenen Standorten, sodass mögliche Man-in-the-Middle-Angriffe verhindert werden können?

Hierbei soll lediglich eine Analyse bezüglich der Nutzung an CAs und Zertifikaten erfolgen, nicht eine qualitative Beurteilung, welche CAs und Zertifikate als vertrauenswürdig eingestuft werden können.

1.1 Zielsetzung

In dieser Arbeit soll begründet werden, ob sich die genutzten CAs und dementsprechend auch (Zwischen-)Zertifikate je nach Ort des Clients unterscheiden. Dabei sollen eine für die alltägliche Nutzung des Internets repräsentative Anzahl an Adressen oder Domänen von mehreren Standorten aus nach SSL-Verbindungen angefragt werden. Dabei werden, wenn eine TLS-Verbindung vom Server unterstützt wird, die Zertifikatsketten vom Server an den Client gesendet, welche dann in einer Datenbank gesichert werden. Diese können dann hinsichtlich Verbreitung und Nutzung nach Adresse oder Domäne und Standort des Clients verglichen werden.

Aus diesen Daten kann dann entschieden werden, ob ein hypothetischer Man-in-the-Middle-Angriff erkannt werden kann und/oder durch mögliche Gegenmaßnahemen verhindert werden kann.
Hierbei könnte sich einerseits herausstellen, dass die genutzten CAs von allen oder den meisten Standorten bei den jeweiligen Domänen gleich sind. Dann würde sich ein gewisses Misstrauen empfehlen, sollte man einer anderen CA beim SSL-Aufbau begegnen. Hier empfiehlt es sich also eher ein White-Listing (Explizite Erlaubnis für vertrauenswürdige CAs) der gefundenen CAs.
Andererseits kann sich herausstellen, dass bspw. nur an einem Standort Zertifikate einer herausgebenden CA genutzt werden. Dadurch kann der Nutzer selbst entscheiden, ob er dieses Verhalten für misstrauen-erregend hält und diese CA lieber blockiert bzw. aus der White List herausnimmt.
Letztlich können sich Zertifikate und CAs an allen oder vielen Orten stark unterscheiden. Dies macht ein explizites Blockieren schwierig, würde aber von einer gewissen Lokalität der CAs zeugen bzw. der lokal differenzierten Nutzung von Zertifikaten und CAs seitens der Server-Betreiber. Natürlich muss das Ergebnis dieser Arbeit nicht eindeutig in einem dieser Szenarien enden, sondern kann durchaus eine Misch- oder Zwischenform sein, sodass auch die Analyse hinsichtlich Blockieren differenzierter ausfallen muss.

SSL ist essenziell für die sichere Kommunikation im Internet und das Vertrauen in die Zertifikate bzw. die ausstellenden CAs notwendig. Allerdings haben Studien gezeigt, dass Nutzer im Umgang mit verschlüsselten Internetseiten mehr Wert auf professionelles Design einer Website legen als auf Sicherheits-Hinweise und insbesondere Warnungen ignorieren. [35][37] Es kann also davon ausgegangen werden, dass die meisten Nutzer auch kein begründetes Vertrauen in CAs haben, abgesehen von den größten Unternehmen wie VeriSign oder lokal bekannte Organisationen wie bspw. der deutschen Telekom. Allerdings könnten Nutzer basierend auf ihrem Allgemeinwissen hinsichtlich der geographischen Nutzung und Herkunft entscheiden, ob eine CA in ihren Augen Vertrauen verdient. [38] Um diesen Entscheidungsprozess zu unterstützen, könnte diese Arbeit quantitative Informationen bereitstellen, inwiefern diese Entscheidungen überhaupt getroffen werden müssen und wie.

Es ist bekannt, dass in China die Regierung mithilfe von Internet Providern ihre Bürger kontrolliert und Inhalte im Internet filtert, bevor diese dem Nutzer bereitgestellt werden. [42] Auch in Russland soll eine ähnliche Infrastruktur aufgebaut werden. [6][13] Hier wäre es nicht abwegig, auch von möglichen Man-in-the-Middle-Angriffen mit kompromittierten CAs auszugehen. Würde sich nun in dieser Arbeit herausstellen, dass bspw. bestimmte CAs hauptsächlich in Russland oder China genutzt werden, könnte ein Nutzer sich basierend auf seiner Meinung zu

diesen Ländern entscheiden, diesen CAs zu vertrauen oder nicht.

Hierbei gilt zu bedenken, dass die Arbeit lediglich eine quantitative Übersicht über die lokale Nutzung von Zertifikaten und CAs geben soll und keine qualitative Beurteilung hinsichtlich der Vertrauenswürdigkeit.

1.2 Definitionen

1.2.1 SSL und TLS

TLS (Transport Layer Security) wurde entworfen, um eine sichere Kommunikation zwischen zwei Endpunkten über eine Verbindung herzustellen. Es ist ein Standard festgelegt von der Internet Engineering Task Force (IETF).
TLS erlaubt eine sichere Kommunikation über das Internet zwischen Server und Client gegenüber Lausch-, Manipulations- und Fälschungs-Angriffen. Die Verbindung stellt daher die folgenden Eigenschaften sicher:

- Authentifizierung:
  Der Server ist immer authentifiziert, der Client optional auch.
- Vertraulichkeit:
  Die über die Verbindung gesendeten Daten sind nur für die beiden Endpunkte sichtbar.
- Integrität:
  Daten, die über die Verbindung gesendet wurden, können nicht von einem Angreifer unbemerkt modifiziert werden.

TLS besteht hauptsächlich aus zwei Komponenten: Zum einen aus dem Handshake Protocol, in welchem die Authentifizierung stattfindet, die kryptographischen Details vereinbart werden und die Grundlagen für den gemeinsamen Schlüssel (zur Ver- und Entschlüsselung des späteren Datenverkehrs) festgelegt werden. Zum anderen gibt es danach das Record Protocol, welches die vorher festgelegten Parameter nutzt, um den Datenverkehr zwischen den beiden Parteien zu sichern.

Das TLS Handshake Protocol wird vom Client begonnen. Dieser sendet ein ClientHello mit den notwendigen clientseitigen Materialien (Random Nonce), um einen gemeinsamen Schlüssel herzustellen, und den zur Verfügung stehenden Protokoll-Versionen. Nachdem der Server dieses verarbeitet hat und die kryptographischen Parameter festgelegt hat, antwortet dieser mit einem ServerHello. Diese Nachricht beinhaltet die vereinbarten Verbindungs-Parameter und mit dem

ServerHello und ClientHello können die beiden Parteien die gemeinsamen Schlüssel erstellen. Alle nachfolgende Kommunikation findet nun verschlüsselt statt.
Wenn eine zertifikat-basierte Authentifizierung des Clients gewünscht ist, kann der Server auch ein CertificateRequest senden. Jetzt beginnt die Authentifikations-Phase: Der Server kann nun Zertifikate oder Public Keys übertragen, um sich zu identifizieren. In diesem Fall wird eine Signatur über den Handshake mit dem Private Key erstellt, um zu bestätigen, dass der Zertifikats- bzw. Public-Key-Besitzer den Handshake getätigt hat.
Bei gesendetem CertificateRequest vom Server sendet der Client diese ebenfalls. Zum Schluss wird ein Finished gesendet, in dem der ganze Handshake bestätigt wird.

In der Authentifikations-Phase kann eine ganze Liste an Zertifikaten übermittelt werden, die sich der Reihe nach zertifizieren. Auf TLS können zusätzlich höhergelegene Protokolle genutzt werden. Wie allerdings die Initialisierung von TLS und Authentifizierung durch die ausgetauschten Zertifikate bewertet werden, liegt allerdings bei den Nutzern (und Erstellern von darüber liegenden Protokollen). [32]

Inzwischen ist TLS in der Version 1.3 verfügbar. Zusammen mit Version 1.2 wird diese vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen. Im Gegensatz dazu werden TLS 1.0 und 1.1 sowie das Vorgänger-Protokoll SSL (Secure Socket Layer) in den Versionen 1.0, 2.0 und 3.0 nicht mehr empfohlen. Grund hierfür sind unter anderem unzureichende Schlüssellängen (ausrechenbar) oder andere Sicherheitslücken bzw. bekannte Angriffe. Genutzt wird TLS hauptsächlich im Internet für HTTPS, FTPS oder IMAPS [36]

Über das Internet werden Dinge gekauft, es werden private Konversationen geführt und vieles mehr. Dazu verlässt man sich auf die Sicherheit von TLS. TLS steht im Internet über den Protokollen IP und TCP. Mit diesen werden Daten in kleine Pakete geteilt und versendet. Dabei bieten diese Protokolle aber keine Sicherheiten. Somit kann jeder, der Zugang zu den genutzten Kommunikationswegen hat, diese Datenpakete auslesen oder gar verändern. Mittels TLS werden die Daten verschlüsselt, sodass diese, wenn ein Angreifer Zugang zu diesen bekommt, nicht gelesen oder verändert werden können.
Zudem hilft TLS zu verhindern, dass sich Angreifer als eigentlich gewünschte Verbindungspartner zu auszugeben. Dazu baut es auf Zertifikate und ein dahinterstehendes PKI (Public Key Infrastructure). [33]

Für die Authentifizierung unterstützt TLS Zertifikate nach dem X.509-Standart. Ein TLS-Nutzer vertraut einer Liste von CA-Zertifikaten. Jedem Zertifikat, das von einem dieser in der Liste enthaltenen CA-Zertifikaten signiert wurde, vertraut der Nutzer auch. Der Server (oder auch der Client, wenn gefordert) kann neben dem eigenen Zertifikat eine ganze Zertifikatskette

mit-übermitteln, um so eine Vertrauensbasis zu schaffen. [7]

1.2.2 Zertifikat

Bei der symmetrischen Kryptografie nutzen beide kommunizierende Parteien den gleichen geheimen Schlüssel, sowohl zur Ver- als auch Entschlüsselung. Ein großes Problem ist hierbei der Austausch dieses geheimen Schlüssels, da dieser über einen sicheren Weg ausgetauscht bzw. festgelegt werden muss. Die asymmetrische Kryptografie scheint hierbei den Ausweg anzubieten: Jede Partei hat einen privaten Schlüssel, den nur sie nutzt, und einen öffentlichen Schlüssel, der für die Kommunikationspartnern gedacht ist. Mit dem privaten Schlüssel können Nachrichten entschlüsselt werden, die mit dem öffentlichen Schlüssel verschlüsselt wurden, und andersherum.
Man könnte nun davon ausgehen, dass man einfach die öffentlichen Schlüssel ohne Geheimhaltung mit potenziellen Kommunikationspartnern austauscht und somit eine sichere verschlüsselte Unterhaltung möglich ist. Allerdings ist hier das Problem der Authentizität des öffentlichen Schlüssels: Wenn man einen öffentlichen Schlüssel per Email oder im Internet erhält, kann man sich sicher sein, dass dieser wirklich der gewünschten Zielpartei zugehörig ist?
Um die asymmetrische Verschlüsselung also nutzen zu können, muss die Bindung des öffentlichen Schlüssels an eine Partei sicher sein. Diese Zuordnung kann man aber nicht (immer) einfach selber überprüfen. In der nicht-digitalen Welt tritt dieses Problem auch auf: Wie prüft man bspw. den Namen und das Geburtsdatum einer Person? Man fragt bei einer dritten Person nach, die dies beurteilen kann. Da dies aber umständlich ist, wird dies durch Dokumente gelöst, die von einer vertrauenswürdigen Instanz als richtig gekennzeichnet wurde bspw. mit Unterschrift. Dieses Kennzeichen muss natürlich überprüfbar sein.

In der digitalen Welt wird dies mit einem digitalen Zertifikate gelöst. Dieses ist ein digitales Dokument, in welchem eine Instanz durch eine digitalen Signatur einen Sachverhalt bestätigt. Die digitale Signatur entspricht hierbei einer Unterschrift mittels privatem Schlüssel. Somit kann jeder, der in besitz des öffentlichen Schlüssels ist, diese Signatur überprüfen. Beim Zertifikat wird die signierende Instanz als Certificate Authority (CA) bezeichnet. Damit nun einem Zertifikat vertraut werden kann, muss vorher der CA vertraut werden und dessen öffentlicher Schlüssel bekannt sein, wobei hier die Authentizität auf anderem Wege sichergestellt sein muss.

TLS unterstützt in der aktuellen Version nur Zertifikate des X.509-Standards, mit welchem sich der Server (und auch Client, wenn gefordert) authentifiziert. Diese Zertifikate wurden ursprünglich erstellt, um Personen eindeutig zu identifizieren, weshalb sie einen Distinguished Name (DN) enthalten. Dieser ist hierarchisch aufgebaut und enthält dabei Informationen wie

Land, Bundesland, Stadt, Organisation und Namen. Da dies aber angesichts digitaler Identitäten (bspw. Email-Adressen, Domänen) nicht immer sinnvoll ist, können alternative IDs hinzugefügt werden.
Dies wird als *subject* im Zertifikat gespeichert. Der öffentliche Schlüssel des Zertifizierten ist als *subjectPublicKeyInfo* enthalten. Dies ist der zu zertifizierende Inhalt. Dementsprechend ist auch der Zertifizierende mit seiner Identität als *issuer* im Zertifikat zu finden. Die Signatur des *issuers* über dieses Zertifikat für das *subject* ist unter *signature enthalten*. Die Gültigkeit des Zertifikats ist auf eine Dauer beschränkt, als *validity* zu finden. Sollte ein Zertifikat ungültig werden, so kann dieses mit der *serialNumber* und dem *subject* eindeutig identifiziert werden.
Um ein Zertifikat für bestimmte Anwendungen zu restriktieren, kann die Erweiterung *Key Usage* und *Extended Key Usage* gesetzt werden. So kann bspw. ein Zertifikat auf die Nutzung für Email-Verschlüsselungen oder Authentifizierung eines Servers beschränkt werden. Auch kann mit der Erweiterung *Basic Constraint* festgelegt werden, ob ein Zertifikat dazu genutzt werden kann, weitere Zertifikate auszustellen bzw. zu signieren und wie lang eine darauffolgende Zertifikatskette sein darf. Mittels der Erweiterung *Name Constraint* kann eingeschränkt oder explizit erlaubt werden, welche Bereiche des Namens mit diesem Zertifikat weiter zertifiziert werden darf (bspw. das Land im DN).

Ein TLS-Benutzer benötigt eine Liste an CA-Zertifikaten, denen er direkt vertraut, die sogenannte Zertifikatsliste. Dadurch vertraut er auch allen Zertifikaten, die von diesem signiert werden. Somit hängt die Sicherheit von TLS von der Überprüfung der Zertifikate seitens des Nutzers ab. [7]
Bevor ein Nutzer auf die Authentizität und Validität eines Zertifikates und des darin enthaltenen Public Key vertraut, sollte sich dieser mit den Richtlinien und der Arbeit der CA kritisch auseinander setzen. Der Nutzer hat nur wenige Verantwortungen, darunter die Auswahl der vertrauten CAs (und Besorgung dessen Public Keys). Hingegen haben Administratoren von CAs sehr große Möglichkeiten und können daher auch Fehler machen, die weitreichende Folgen haben.

Durch die Signatur, die das ganze Zertifikat bestätigt, und zeitliche Gültigkeit eines Zertifikates und bei vorhandenen CA-Zertifikate kann ein Nutzer die Validität eines Zertifikats unabhängig überprüfen. Daher können Zertifikate auch über unsichere oder nicht vertrauenswürdige Verbindungen verwendet werden. [9]

1.2.3 PKI

Im X.509-Standard ist eindeutig festgelegt, wie ein Zertifikat geprüft werden muss, um festzustellen, dass es gültig ist. Dazu gehört die Überprüfung, ob die Zertifikatskette bei einem Zertifikat endet, welchem der Nutzer vertraut. Eine Zertifikatskette entsteht dadurch, dass mehrere Zertifikate sich nacheinander erzeugen und signieren. Eine CA kann ein Zertifikat erstellen und diesem das Recht ermöglichen, mit diesem weitere Zertifikate auszustellen. Hierbei entspricht die nun neu berechtigte CA der Sub-CA und die übergeordnete CA der Parent-CA. Auch eine Sub-CA kann weitere Zertifikate mit diesem Recht erstellen und so eine Kette an Zertifikaten und Sub-CAs ermöglichen. Hierzu wird die Erweiterung *Basic Constraint* genutzt. Der Nutzer vertraut einer Menge an CAs und allen Zertifikaten die diese ausstellt oder in einer Zertifikatskette bei ihr enden. In diesem Fall wird diese als Root-CA bezeichnet. Hier ist ein transitives Vertrauen gegeben, also der Nutzer vertraut der CA an, das Privileg Zertifikate auszustellen weiterzugeben. Dies hat den Vorteil, dass es größer skalierbar ist und verteilt angewendet werden kann. Im Gegensatz dazu steht das direkte Vertrauen. Hier vertraut der Nutzer einer CA nur dem direkt zertifizierten Inhalt.
Neben der Prüfung, ob ein Zertifikat auf eine vertraute CA zurückzuführen ist, muss auch geprüft werden, ob dieses überhaupt noch gültig ist: Zum einen ist auf die Gültigkeitsdauer (*validity*) zu achten, zum anderen ob das Zertifikat nicht widerrufen wurde, wenn bspw. der zugehörige geheime Schlüssel gestohlen wurde. Hierfür müssen die Certificate Revocation List (CRL) überprüft werden. Diese werden auch im X.509-Standard spezifiziert: Eine CRL enthält dabei die Informationen über die CA, die diese erstellt hat, und welche Zertifikate widerrufen wurden, also nicht mehr gültig sind.

Ein Zertifikat durchgeht folgenden Lebenszyklus:

1. Registrierung des Benutzers und Überprüfung des Zertifikatsinhaltes
2. Erstellung des Zertifikats
3. Veröffentlichung des Zertifikats
4. Nutzung des Zertifikats
5. Eventuell Widerruf des Zertifikats
6. Erneuerung des Zertifikats nach Ablauf der Gültigkeitsdauer [vgl. 7]

Für das Management von diesem Zyklus wird eine Infrastruktur benötigt: *Public Key Infrastructur* (PKI). Durch die PKI wird eine authentifizierte Bindung eines öffentlichen Schlüssels an einen Namen, also ein Zertifikat, ermöglicht. Eine PKI besteht aus verschiedenen Elementen

und Teilnehmern: Zum einen gibt es die Benutzer, eine Instanz, die auf der einen Seite Zertifikate benötigt und auf der anderen Seite andere Zertifikate überprüfen will. Zudem gibt es die CA, die für die Zertifizierung selber und auch den Widerruf dieser ausgegebenen Zertifikate zuständig ist. Bevor eine CA ein Zertifikat für einen Benutzer ausstellt, muss dessen Identität überprüft werden. Hierfür ist die *Registration Authority* (RA) zuständig. Wenn Benutzer Anträge zur Zertifizierung stellen, sammelt die RA diese, überprüft sie und leitet sie an die CA weiter, welche dann die entsprechenden Zertifikate erstellt und signiert. Wenn ein Zertifikat widerrufen werden soll, kann der Benutzer oder die RA dies bei der CA anfordern. Für die Veröffentlichung der (widerrufenen) Zertifikate wird dann ein Verzeichnisdienst genutzt.

Zwei Punkte sollte eine PKI gewährleisten können: Zum einen die Sicherheit der internen Abläufe. Ausgestellte Zertifikate sollten in ihrem Inhalt stimmen, sonst kann dies Ausgenutzt werden, um Benutzer zu täuschen. Zum anderen sollte die Sicherheit des Signaturschlüssels sichergestellt werden. Würde ein Signaturschlüssel einer CA kompromittiert werden, also der geheime Schlüssel einem Angreifer in die Hände fallen, so kann dieser Zertifikate ausstellen, denen die Benutzer vertrauen. Daher müssen besondere Schutzmaßnahmen, wie eine physikalische Isolation, für diesen getroffen werden. [7]

Außerdem kann eine CA, die Verantwortung für das Widerrufen von Zertifikaten, also das Veröffentlichen dieser, an eine weitere Entität weitergeben. So können verschiedene Schlüssel für das Ausstellen von Zertifikaten und Widerrufen dieser verwendet werden, was einen zusätzlichen Schutz bei einem Angriff darstellt.

Zertifikate von CAs können unterteilt werden in:

- *Cross-certificates*:
  Hierbei sind issuer und subject des Zertifikats verschiedene CAs. Diese vertrauen sich daher gegenseitig und stellen Zertifikate für einander aus.
- *Self-issued certificates*:
  Hier sind issuer und subject die selbe Entität. Dies wird genutzt um Änderungen vorzunehmen
- *Self-signed certificates*:
  Diese entsprechen dem self-issued Certificate, wobei allerdings die Signatur des Zertifikats mit dem darin enthaltenen Public Key überprüft werden kann. Dies wird oft genutzt, um die Grundlage für eine mögliche Zertifikats-Kette zu legen.

Normalerweise werden Zertifikate nach Ablauf ihrer Gültigkeitsdauer (validity) ungültig. Allerdings kann es zu Ereignissen kommen, dass diese schon vorher nicht mehr vertrauenswürdig

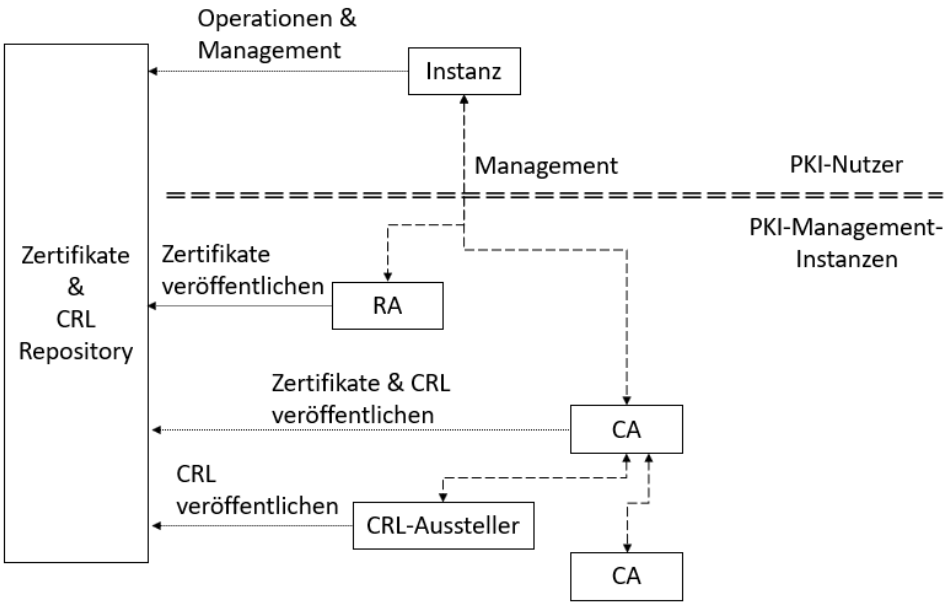

Abbildung 1.1: PKI-Instanzen nach [9]

sind. Dann werden sie zu der jeweiligen CRL hinzugefügt. CRLs sind Listen, die widerrufene Zertifikate auflisten und identifizieren. Sie sind zeitlich markiert und von der CA oder einer anderen verantwortlichen Entität (*CRL issuer*) signiert und öffentlich zugänglich gemacht. Dadurch können auch diese über unsichere Kommunikationswege abgerufen werden.

Eine Notwendigkeit für das PKI ist, dass der Benutzer mit den Public Keys und weiteren Informationen über die vertrauenswürdigen CAs initialisiert wird. Dies wird benötigt, um mit Zertifikaten und damit Public Keys von anderen Stellen des PKIs zu interagieren bzw. diese zu überprüfen. Welchen CAs vertraut wird, ist eine sehr sicherheits-kritische Frage. Davon hängt ab, ob darunterliegenden Zertifikaten vertraut wird. Allerdings liegt diese Frage außerhalb der Zertifikats-Spezifikation X.509.
Die Frage, welchen und wie vielen CAs vertraut wird, ist nicht unerheblich. Sollte eine dieser CAs bzw. dessen Private Key kompromittiert werden, muss der Nutzer die Informationen dazu überarbeiten. Dies stellt eine Herausforderung dar, insbesondere wenn vielen CAs vertraut wird. Wird hingegen zu wenigen oder gar nur eine CA vertraut, so kann der Nutzer nur mit einem sehr beschränkten Teil des PKIs interagieren.

Für die Sicherheit und das Vertrauen in die PKI und Zertifikate ist die Überprüfung der Subjects seitens der CAs und RAs enorm wichtig. Sind diese Verfahren nicht nachvollziehbar oder erscheinen unzureichend, so leidet auch das Vertrauen in die ausgestellten Zertifikate darunter. Diese Überprüfungen sind insbesondere dann wichtig, wenn Sub-CAs mit dem Recht, selber

Zertifikate auszugeben, authentifiziert werden.
Auch gilt es für CAs zu überprüfen, welche Entwicklungen in der Kryptographie stattfinden, um starke Verschlüsselungen zu ermöglichen. Bspw. sollte hier auf Algorithmen und Schlüssellängen geachtet werden. CAs sollten keine Zertifikate mit zu schwacher Signatur. [9]

1.2.4 VPN

Für diese Arbeit wird ein virtuelles privates Netzwerk genutzt. Ein Netzwerk besteht aus einer Anzahl an Teilnehmern, die untereinander kommunizieren können. „Privat“ impliziert, dass diese Kommunikationswege kontrolliert und geschützt sind und im Vergleich zum Gegenstück „öffentlich“ nicht für jeden zugänglich, nutzbar und/oder einsehbar sind. Das prominenteste Beispiel für ein öffentliches Netzwerk ist wohl das Internet. Hier kann jeder (mit entsprechendem Zugang) mit jedem anderen Teilnehmer kommunizieren, sofern dieser es zulässt.
Nun kann ein privates Netzwerk bspw. durch eigene Infrastruktur innerhalb einer Organisation aufgebaut werden. Solange diese an einem Ort gebündelt ist, stellt dies kein all zu großes Problem dar. Wenn die Organisation allerdings geographisch weit verteilt ist, so wird eine entsprechende Infrastruktur sehr kostenintensiv. Hier kann ein virtuelles privates Netzwerk (VPN) genutzt werden. „Virtuell“ entspricht hierbei der Bedeutung „Simuliert“. Es werden Funktionen von etwas, was nicht vorhanden ist, simuliert. Die hier simulierte Funktion entspricht dem Privaten, also der schützenden Eigenschaft bzw. der Zugangskontrolle. Das VPN ist kein komplett separates Netzwerk, sondern simuliert dies innerhalb eines öffentlichen oder geteiltem Netzwerk. Es erlaubt eine private Kommunikation zwischen mehreren Teilnehmern in einem Umfeld mit weiteren Teilnehmern, die diese Kommunikation nicht nachvollziehen können. Dies kann bspw. durch Verschlüsselung der Daten erreicht werden.
Eine Methode, um ein VPN aufzubauen, ist das *Tunneling*. Hierbei wird von einer Quelle zu einer Destination eine Verbindung (Tunnel) aufgebaut. Innerhalb dieser werden Pakete, eigens für diesen Tunnel entworfen, versendet. In diesen Datenpaketen werden die eigentlichen Daten (nach dem „normalen“ Format formatiert) umschlossen. Diese überliegende Schicht wird bei der Quelle um die Daten herumgelegt und erst an der Destination entpackt. Von dort werden die eigentlichen Daten dann weiterverarbeitet oder versendet. [18]

Man kann dies natürlich auch andersherum betrachten:
In einem virtuellen Netz werden also Netze bzw. Netzteilnehmer über einem größeren fremden Netz zusammengeschlossen. Hiermit sollen private, nicht öffentliche bekannte Adressen verbunden werden. Allerdings werden die Daten über eine fremde Netzinfrastruktur ausgetauscht, weshalb sich zwei potenzielle Gefahren ergeben: Zum eine gibt es andere Benutzer in dem

fremden Netz, die das virtuelle Netz angreifen könnten, und zudem kann der Betreiber der genutzten Netzinfrastruktur diese nutzen, um das die Daten des virtuellen Netzes anzugreifen. Um dies zu verhindern, nutzt man ein *virtuelles privates Netzwerk* (VPN). Hierbei gibt es zum einen die Möglichkeit, die Verbindungen durch den Netzbetreiber von anderen Benutzern des Netz abgrenzen zu lassen. Dadurch würde zumindest die erste Gefahr gebannt. Dies würde allerdings nicht mögliche Angriffe des Netzbetreibers verhindern. Dagegen können kryptographische Mechanismen genutzt werden, um die Daten zu schützen. Dies ist auch insbesondere hilfreich, wenn die virtuellen Netze über das Internet aufgebaut werden sollen, bei dem mehrere Netzbetreiber involviert sind. Eine Möglichkeit, ein kryptographisch gesichertes Netz aufzubauen, ermöglicht TLS. [7]

Mittels VPN kann also eine scheinbar direkte sichere Verbindung zwischen zwei Punkten erstellt werden. Somit kann eine Entität, der VPN-Client, an einem Netzwerk teilnehmen, indem er sich mit dem VPN-Server verbindet und diesen nutzt. Der VPN-Server ist Teil des gewünschten Netzes. Mit diesem verbindet sich der VPN-Client mittels kryptographischen Verfahren, um die Integrität der Kommunikation zu wahren. Der VPN-Client erhält dann von dem VPN-Server eine Adresse aus dem gewünschten Netz, die den Client dort repräsentiert. Möchte der VPN-Client nun innerhalb des Netzes kommunizieren, so erstellt er Datenpakete, adressiert an die Wunsch-Destination in diesem Netz und mit der Adresse als Absender, die vom VPN-Server zugeteilt wurde. Diese Datenpakete werden nun an den VPN-Server durch den VPN-Tunnel (mit vorher etabliert Kryptographie) versendet. Der VPN-Server entpackt die ursprünglichen Datenpakete und versendet diese. Analog verfährt der VPN-Server, wenn dieser Datenpakete erhält, die an die Adresse gerichtet ist, die der VPN-Server an den VPN-Client vergeben hat. Die erhaltenen Datenpakete sendet dann der VPN-Server über den Tunnel an den VPN-Client.

Man kann über einen VPN-Server, der eine Verbindung zum Internet hat, auch alle Zugriffe auf das Internet laufen lassen. Somit kann man seine Zugriffe nahezu anonymisieren. Mittels eigenen Anbietern kann man sich per VPN mit einem Server verbinden, sodass die eigene IP-Adresse nur noch zum Datentransfer mit dem VPN-Server genutzt wird. Für die weitergeleiteten Zugriffe im Internet wird dann die vom VPN-Server zugeteilte IP-Adresse genutzt. Somit kann der ein Service Provider die Zugriffe (abgesehen vom Zugriff auf den VPN-Dienst) im Internet nicht mehr einsehen. Allerdings muss dafür dem VPN-Provider das Vertrauen entgegengebracht werden, welches man dem Service Provider damit entzieht: Das dieser nicht die Nutzerdaten mit den Zugriffen sichert bzw. missbraucht.

Eine Open-Source-Implementierung für VPNs ist OpenVPN. Um die Daten zu schützen wird hier SSL/TLS genutzt. Für den Transport hingegen wird UDP oder TCP genutzt. [22]

Inzwischen gibt es immer mehr VPN-Anbieter, mit denen sich Nutzer im Internet bewegen. Damit soll die Privatsphäre gesichert und Zensuren oder Geo-Blocking umgangen werden. Diese Zensuren können dabei zum einen auf Staaten zurückgehen, aber auch von den jeweiligen Dienst-Anbietern je nach Ort des Nutzers durchgeführt werden. Zweites wird Geo-Blocking genannt, also Blockieren eines Angebots basierend auf der geographischen Position des Nutzers. Mittels VPN-Provider soll es ermöglicht werden, die eigenen Zugriffe aufs Internet über andere Wege, oft eigens auswählbare Standorte in verschiedenen Ländern, zu führen, um die Blockade von Inhalten zu umgehen. Hier wird die Technik zur Erstellung von VPNs genutzt, um dem Nutzer eine geschützte Verbindung zu den Servern des VPN-Providers zu ermöglichen und von diesen aus anonymisiert und mit (lokal) anderem Internet-Zugriff durchzuführen.
Allerdings scheint es auch bei VPN-Providern Probleme hinsichtlich der Sicherheit der Daten und auch der angebotenen geographischen Standorte der Server zu geben. Insbesondere der zweite Punkt ist kritisch im Rahmen dieser Arbeit zu beachten, da ein VPN-Anbieter hauptsächlich genutzt wird, um von verschiedenen geographischen Standorten aus Informationen zu gewinnen. [23]

2 Hauptteil

2.1 Stand der Forschung

Die sichere Kommunikation im Internet beruht meist auf Secure Socket Layer (SSL). Dabei werden Public Keys zum Verschlüsseln der Daten genutzt, welche dann nur mithilfe des Private Keys des Ziel-Partners wieder entschlüsselt werden können. Um sicher diese Public Keys des gewünschten Ziel-Servers zu erhalten, stützt man sich auf die Public Key Infrastructure (PKI).

Wenn ich eine sichere Verbindung zu einem Server aufbauen möchte, sendet mir dieser sein Zertifikat. Dieses beinhaltet dabei den Namen des Zertifizierten (meist eine IP-Adresse oder Domäne), dessen Public Key, den Namen des Herausgebers und dessen Signatur. Der Herausgeber wird Certificate Authority genannt und jeder Browser oder Betriebssystem enthält eine vordefinierte Liste an vertrauenswürdigen CAs. Allerdings geben nicht nur diese CAs Zertifikate aus, sondern auch intermediate bzw. subordinate (Zwischen-)CAs. Dies sind dritte Parteien, denen ein Zertifikat von einer CA ausgestellt wurde mit dem Recht, selbst Zertifikate auszustellen. Somit kann eine Kette an Zertifikaten (certificate chain) entstehen, die vom Zertifikat des angesprochenen Servers (leaf certificate) über die Zertifikate der Sub-CAs bis zum Zertifikat der ersten CA (root CA) gehen. Jeder Browser oder Betriebssystem hat eine vordefinierte Liste von vertrauenswürdigen Wurzel-Zertifikaten. Sobald wir also von unserem Ziel-Server die Zertifikats-Kette erhalten können wir nachprüfen, ob diese bei einem für uns vertrauenswürdigen Wurzel-Zertifikat endet. Ist dies der Fall gilt das Zertifikat als gültig und wir vertrauen diesem. [20][34]

Die PKI besteht aus diesem System an Zertifikaten und CAs. Wie sich die PKI über die Zeit verändert, wurde schon innerhalb von und im Vergleich zwischen verschiedenen Studien erarbeitet: Hierbei fällt vor allem auf, dass dieses stetig wächst. Das heißt, dass die Zahl an einzigartigen Zertifikaten und CAs steigt. Es wurde schon der gesamte IPv4-Adressraum als auch die Alexa-Top-1-Millionen-Domänen gescannt. Es fällt auf, dass bei der Studie von Durmeric et al. von 2013 über 95% der vertrauten Zertifikate und 99% der Hosts mit vertrauenswürdigen Zertifikaten aus nur 10 Ländern kommen, ein Großteil allein aus den USA. Auch

wurden mehr als 90% der Zertifikate von den 10 größten CAs ausgestellt zurückgehend auf nur 4 root certificates. Über 75% der Zertifikate lassen sich sogar auf nur 3 Organisationen zurückführen (Symantec, GoDaddy & Comodo). [15]

Während Scans von Zertifikaten zwar mit Hinblick auf die PKI insgesamt und auf die zeitliche Veränderung schon durchgeführt wurden, ist ein offener Punkt, ob sich die PKI hinsichtlich des Standortes des Clients ändert bzw. unterscheidet. Dies ist auch mit Blick auf die Problematik eines Man-in-the-Middle-Angriffs interessant:

Ein Man-in-the-Middle-Angriff (MitM) ist ein aktiver Angriff, in dem der Angreifer den Inhalt der Kommunikation zwischen den eigentlichen Parteien abfängt und sich diesen gegenüber als der jeweilig andere ausgibt. Mit Blick auf einen MitM-Angriff auf eine SSL-Verbindung gibt es viele verschiedene Methoden, die Kommunikation zwischen Client und Server abzufangen. Einige sind durchaus etabliert (bspw. DNS-Spoofing). Der Client identifiziert sich gegenüber dem Server über die Daten, die er ihm verschlüsselt übermittelt (bspw. Name & Passwort). Der entscheidende Teil ist also, ob sich der Angreifer erfolgreich als Server ausgeben kann. Dafür muss er ein eigenes Zertifikat mit dem Server-Namen und eigenem Public-Private-Key-Paar an den Client übergeben, welchem dieser dann vertraut. Gelingt dies, kann der Angreifer sich dem Server gegenüber als der eigentliche Client ausgeben (mit dessen Anmelde-Daten) und dessen Aktionen (modifiziert) ausführen. [26]

Wie solch ein Angriff von Staatsseite gelingen kann, zeigt Soghoian et al. auf. So kontrollieren einige Staaten eigene (nicht-kommerzielle) vertrauenswürdige CAs oder könnten rechtlich andere vertrauenswürdige CAs zwingen, dass diese Zertifikate für fremde Server ausstellen, um diese für einen Angriff zu nutzen. [38] Die nötige Infrastruktur, um die Kommunikation zwischen Client und Server abzufangen, gibt es bspw. schon in China. Dort werden an verschiedenen Stellen Filter mithilfe von Internet-Providern schon durchgesetzt und Inhalte für den Client entfernt. [42] Ähnliches plant auch Russland. [6][13] Natürlich kann der Angreifer auf verschiedenen Ebenen die Kommunikation zwischen Client und Server abfangen: Sowohl näher an der Client-Seite als auch nahe am Server, sowie eher mittig dazwischen. [2]

Dies sind nicht nur theoretische Gefahren. So hat 2012 die CA Trustwave zugegeben, subCA-Zertifikate an Firmen zu verkaufen, sodass diese ihre Mitarbeiter mittels eigens erstellter Zertifikate ausspionieren konnte. Ebenso wurde 2013 bekannt, dass die CA Turktrust eine subCA für eine Regierungsstelle ausgegeben hatte, welche dann einen MitM-Proxy installiert hatte. Nach Angaben von Turktrust war dies ein Fehler und betraf auch nur die Mitarbeiter der Regierungsstelle. [34]

Als Abwehr gegen MitM-Angriffe könnte man dynamisch die Zertifikate vergleichen, wenn man neben dem Aufbau der eigenen Verbindung parallel eine oder mehrere Verbindungen mittels Tor über andere Wege zum Server herstellt. [2] Alternativ kann man beobachten, ob sich das Herkunftsland des Zertifikats bzw. des Ausstellers (CA) ändert bei der häufigeren Nutzung eines Servers (Dass sich Zertifikate durch ihre beschränkte Lebensdauer ändern, ist somit vordefiniert und nicht sinnvoll zu überprüfen). [38] Dahingehend wäre es interessant, ob sich die Zertifikate und CAs abhängig vom Ort des Clients unterscheiden. Dies wird in dieser Arbeit untersucht.

2.2 Auswahl der Technologien

Um zu prüfen, inwieweit sich Zertifikate und Zertifikats-Aussteller also CAs, insbesondere Root-CAs, sich unterscheiden, müssen zunächst Zertifikate von verschiedenen Standorten aus gesammelt werden.

2.2.1 Zmap

Zum Sammeln der Zertifikate in großer Menge wird ZMap, genauer ZGrab2, genutzt. ZMap ist ein modularer Open-Source-Scanner, mit dem der IPv4-Adress-Raum schnell abgefragt werden kann. Internet-weite Scans wurden schon oft genutzt, um bspw. Angriffsmöglichkeiten aufzudecken oder Entwicklungen festzustellen. Bisher wurden hauptsächlich Technologien wie Nmap genutzt, wofür allerdings große Ressourcen, in Form von Zeit oder Rechnern, benötigt wurden. Mit ZMap hingegen soll mit einem einzelnen Rechner bei entsprechenden Internet-Zugang (1 GB) der ganze IPv4-Adressraum, beschränkt auf einen expliziten Port, innerhalb von 45 Minuten abgefragt werden können. Hierbei soll der Verlust an Daten möglichst gering sein. Bei Tests der Hersteller wurden 98% der Adress-Anfragen erfolgreich beantwortet, sogar bei höchster Scan-Geschwindigkeit und lediglich einer einzelnen abgesendeten Anfrage pro Adress-Host.
ZMap ist modular, es können die Erstellung der Pakete, die an die Adressen gesendet werden, und die Auswertung und Darstellung der zurückkommenden Ergebnisse individuell angepasst werden. So können auch TLS-Handshakes durchgeführt werden und die Antworten, insbesondere Zertifikate, gesammelt werden. So konnten über ein Jahr hinweg regelmäßig der ganze IPv4-Raum gescannt werden, um das Ökosystem um Zertifikate und CAs zu analysieren. [16]

Während mit ZMap die IPv4-Adressen mit abgefragt werden können, ob diese verfügbar sind,

können mit dem Applikations-Scanner ZGrab Daten für verschiedene Anwendungs-Protokolle zusammengetragen werden. So kann bspw. das ein TLS-Handshake durchgeführt werden und die Antwort von der angesprochenen IPv4-Adresse bzw. dem Host als lesbare JSON-Daten erfasst werden. [14] ZGrab bzw. der Nachfolger ZGrab2 [8] kann dabei als Eingangsdaten explizit die Ausgaben von einem vorangegangenen ZMap-Scan nutzen oder eigenständig mit den Funktionen bereitgestellt von ZMap agieren. Mit ZGrab werden also über alle Host bzw. gewünschte Adressen Daten über die Verbindung und den Inhalt auf der Anwendungsebene (in unserem Fall TLS) gesammelt. So kann ZGrab innerhalb von 6 Stunden und 20 Minuten HTTPS-Handshakes mit dem ganzen IPv4-Raum durchführen und eine TLS-Verbindung mit allen Verfügbaren SMTP-Hosts innerhalb von ca. 3 Stunden etablieren und abfragen. [8][14]

Als Input, also abzufragenden Raum, wird in unserem Fall nicht der ganze IPv4-Raum genutzt, sondern die eine Millionen meistbesuchten Domänen. Diese können als Text-Datei an ZGrab übergeben werden. Es wird das TLS-Modul genutzt und der Port 443 angesprochen. Dabei wird für jede Domäne ein StartTLS-Vorgang durchgeführt und die Antworten als JSON-Datei ausgegeben. In dieser Output-Datei sind dann auch unter anderem die Zertifikatsketten und das Zertifikate, welche die Domänen präsentieren, enthalten. [8]

2.2.2 Top Domänen

Da die Abfrage von allen IPv4-Adressen, die nicht reserviert sind (ca. 588 Millionen), deutlich zu zeit-intensiv ist, wie in Abbildung 2.2 gezeigt wird, werden nur die meist genutzten Domänen überprüft. Dazu wurden zum einen die Alexa Top-Sites-Liste (hier die ersten ca. 700.000 Adressen) und die Top-1-Millionen-Domänen-Liste von Cisco. [10]
Die Alexa Top-Seiten bestehen dabei aus Domänen. Diese basieren auf anonymen Mustern von Internet-Nutzern weltweit. Wo eine Website auf der Liste steht, wird aus der Anzahl der einzigartigen Nutzern und den Aufrufen der Seiten der letzten 3 Monate errechnet. [4] Die Daten stammen dabei sowohl von Internet-Nutzern, die verschiedene Plugins für Browser nutzen, und von den Website-Betreibern, die ein Alexa-Skript auf ihren Seiten nutzen. [1]

Die Cisco Umbrella 1M List wird ähnlich errechnet. Hier werden Daten von ca. 65 Millionen Nutzern aus über 165 Ländern genutzt. Es wird für jede Domäne die Anzahl der einzigartigen Besuchern anhand der IP-Adresse dieser gesammelt und gegeneinander aufgewogen. Dadurch ergibt sich eine Rangliste. Es werden dabei alle aufgerufene Ports verfolgt, nicht nur bspw. Port 80 für Web-Browser. Somit können alle Protokolle beachtet werden.[24] Die Daten stammen aus über 30 Daten-Centern und in Zusammenarbeit mit verschiedenen Internet Service Providern. [41]

Die Listen wurden jeweils am 25.03.2020 abgefragt.

2.2.3 PureVPN

Um die Zertifikate und CAs für die gleichen Domänen in verschiedenen Ländern zu vergleichen, muss eine Internetverbindung von den jeweiligen Standorten geschaffen werden. Da es leider außerhalb der Möglichkeiten dieser Arbeit liegt, persönlich in verschiedene Länder auf verschiedenen Kontinenten zu reisen, müssen die Internet-Zugänge anderweitig geschaffen werden.

Zunächst war geplant, dies mithilfe der verschiedenen Server-Standorte von AWS zu schaffen. Diese verfügen über 22 verschiedene Server-Standorte, bei welchen sich AWS-EC2-Instanzen erstellen lassen. Dies sind virtuelle Rechner an den jeweiligen Servern mit lokalem Internetzugang. So könnte man die Scans auf verschiedenen AWS-EC2-Instanzen durchführen können. [3] Allerdings verstößt dies gegen AWS Acceptable Use Policy, in der Crawling und Monitoring untersagt sind. Auf Nachfrage wäre es notwendig gewesen, für alle angesprochenen Domänen die Betreiber um Erlaubnis zu fragen, ob diese mit der vergleichbar geringen Menge an TLS-Anfragen (eine pro Standort) einverstanden wären. Dies wäre allerdings bei über einer Millionen von abzufragenden Domänen ein zu hoher Aufwand, wobei nicht einmal sicher gestellt wäre, dass alle Betreiber auf diese Anfragen reagieren würden. [5]

Daher fiel die Wahl auf eine andere Technik bzw. Anbieter, um Internet-Zugänge von verschiedenen Standorten zu ermöglichen: Ein VPN-Anbieter. Auch hier wurden mit Verweis auf die Terms of Service von vielen Anbietern die geplanten Scans abgelehnt. [11][25][27]
Auch auf explizite Rückfrage, wurde von PureVPN bestätigt, dass die Scans mit ihren VPN-Verbindungen erlaubt sind. PureVPN ermöglicht Verbindungen in hunderte verschiedene Länder. Allerdings sind hierbei viele Verbindungen nur zu virtuellen Servern möglich. Bei diesen virtuellen Standorten sind keine physischen Server in den angegebenen Standorten, sondern geo-IP-Datenbanken so manipuliert werden, dass diese IP-Adressen mit den virtuellen Standpunkten verbinden. In unserem Fall sollten nur Verbindungen zu „physischen Standorten“ genutzt werden, da es um den tatsächlichen Internet-Zugang geht. In der Studie von Khan et al. wird auch PureVPN überprüft, aber wird nicht negativ erwähnt. [23][29]
Um Verbindungen zu den jeweiligen VPN-Servern herzustellen können zum einen die eigene PureVPN-App genutzt werden als auch andere VPN-Protokolle, darunter die Implementation OpenVPN. Diese wird auch von PureVPN empfohlen, daher wurden beide Methoden für diese Arbeit genutzt. [30][31]

Bei beiden Verfahren gibt es die Möglichkeit der Verbindung mit den Protokollen User Datagram Protocol (UDP) und Transmission Control Protocol (TCP). Der Unterschied liegt hier hauptsächlich daran, dass bei TCP eine Verbindung erstellt und aufrecht erhalten wird („verbindungsorientiert"), während UDP „verbindungslos" ist. Daher ist UDP schneller, aber TCP an sich verlässlicher. Es sind die hauptsächlich verwendeten Protokolle im Internet. Beide Protokolle bieten selber keine Möglichkeit der Verschlüsselung, diese kann aber in den von ihnen verpackten Inhalten stattfinden. [7][28]

Um die Effizienz der beiden VPN-Implementationen und jeweiligen Protokolle zu vergleichen, wurde zu Beginn der Datensammlung zunächst jeweils ein Scan mit dem VPN-Server in Montreal (Kanada) durchgeführt: Es fällt auf, dass die PureVPN-eigene Implementation scheinbar

VPN-Implementierung	TCP/UDP	Timeout	connection-timeout	io-timeout	success	unknown-error
OpenVPN	UDP	10s	313.734	202.056	1.056.777	58.934
OpenVPN	TCP	10s	1.006.154	328.696	278.320	18.472
PureVPN	TCP	10s	1.606.686	763	23.690	558
PureVPN	TCP	100s	1.603.959	648	26.624	467
PureVPN	UDP	100s	1.571.369	4.078	48.796	7.452

Abbildung 2.1: Vergleich der VPN-Implementierungen für den VPN-Server Montreal (Kanada)

deutlich weniger verlässlicher für unser Vorhaben scheint, als OpenVPN. Dies tritt sogar auf, obwohl die Zeit zum Timeout auf von 10 auf 100 Sekunden erhöht wurde. Zudem ist das vermeintlich unsichere Protokoll UDP in diesem Fall mit OpenVPN die bessere Wahl: Es ergeben sich mit über einer Millionen erfolgreichen TLS-Handshakes ca. 4 mal so viele positive Ergebnisse als mit der Kombination OpenVPN und TCP.

Aus diesen Gründen wurden die Scans nach Möglichkeit mit OpenVPN-Verbindungen zu den VPN-Servern durchgeführt, allerdings sind hier die Ergebnisse bezüglich den Protokollen TCP und UDP sehr unterschiedlich: Im Diagramm sind alle Scans für aller Standorte enthalten. Zu fast allen ausgewählten Server-Standorten konnten Verbindungen via OpenVPN jeweils mittels TCP und UDP aufgebaut werden. Lediglich zu einem Standort konnte eine Verbindung nur via OpenVPN und TCP aufgebaut werden und zu zwei Servern nur Verbindungen via PureVPN-Implementierung.
Es zeigt sich zum einen, dass die OpenVPN-TCP-Verbindungen am längsten Zeit für einen kompletten Scan benötigen, ähnlich die OpenVPN-UDP-Variante. Generell steigt die Dauer der Scans (inkonsistent) mit mehr erfolgreichen TLS-Handshakes. Die PureVPN-Implementierungen, zumindest mit UDP, können auch durchaus brauchbare Ergebnisse liefern, sind allerding weit entfernt von den erfolgreicheren Scans.
Außerdem zeigt sich eine Inkonsistenz in den Scans je nach Protokoll. So gibt es vereinzelte

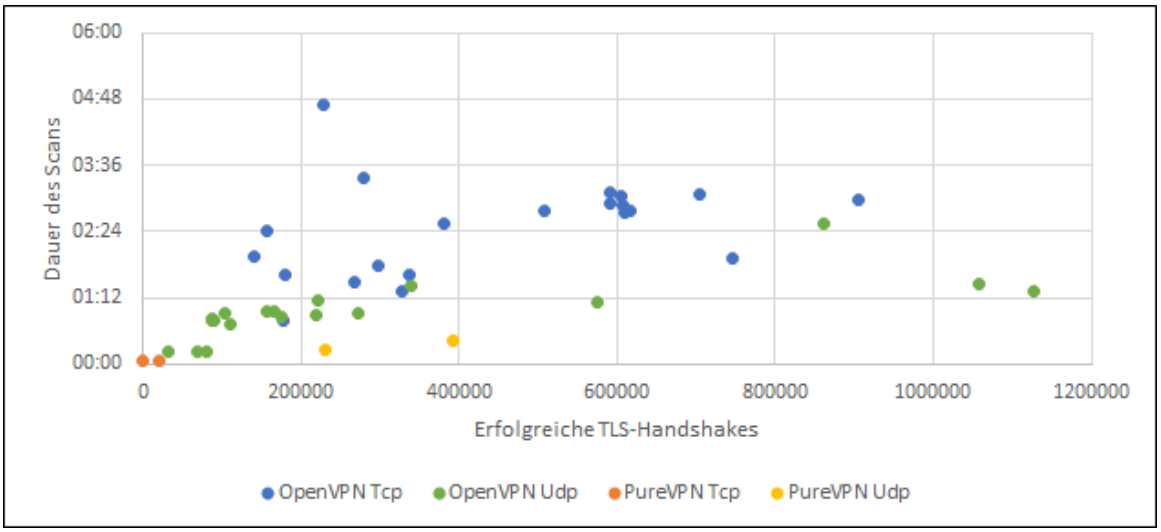

Abbildung 2.2: Vergleich der VPN-Implementierungen für alle Scans nach Dauer und erfolgreichen TLS-Handshakes

sehr gute (nach TLS-Handshakes gemessen) Scans mithilfe von UDP, allerdings auch eine eher schlechte Basis. Die Scans mit TCP scheinen konsistenter, auch in einem guten Bereich (siehe die Scans um 600.000 Handshakes).

Hier zeigt sich auch der Grund, warum die Scans innerhalb dieser Arbeit nur die Top-Domänen behandeln und nicht den ganzen IPv4-Raum: Die meisten guten Scans benötigen zwischen zwei und drei Stunden für fast 2 Millionen IPv4-Adressen. Für über 500 Millionen (nicht reservierte) IPv4-Adressen müssten so für einen nutzbaren Scan zwischen 500 und 750 Stunden (zwischen ca. 20 und 30 Tagen) eingeplant werden. Hinzu kommt die Problematik, dass die Verbindungen zu den VPN-Servern durchaus abbrechen und somit ein Scan erneut begonnen werden muss.

2.3 Durchführung der Scans

Aus der Liste der verfügbaren Server werden folgende ausgewählt, um einen Scan durchzuführen: In den USA werden die Server für Los Angeles, New York und Washington ausgewählt, um eine Vergleichbarkeit innerhalb eines (wenn auch großen) Landes herzustellen. Zudem Montreal (Kanada), Mexiko City (Mexiko) und Sao Paulo (Brasilien) vom Kontinent (Nord- und Süd-)Amerika. Aus Afrika werden die Server in Suleja (Nigeria) und Johannesburg (Südafrika) genutzt. In Asien werden die Server-Standorte in Chennai (Indien), Seoul (Südkorea), Hongkong und Bangkok (Thailand) verwendet. Insbesondere Hongkong als Chinesische Sonderverwaltungszone [12] (In China herrschen starke Kontrollen des Internets [42]) und Thailand

sowie Südkorea, in denen landesweite Zensuren vorhanden sind, sind hier interessant. [23]

In Europa werden Server innerhalb der EU mit den Standorten Frankfurt (Deutschland), Paris (Frankreich), Warschau (Polen), Stockholm (Schweden) und Madrid (Spanien) genutzt. Hinzu kommen die beiden Standorte London (UK) und Zürich (Schweiz) [17], sowie Istanbul (Türkei) und Moskau (Russland), die hinsichtlich landesweiter Zensuren und gefälschter Zertifikate [23] [34] oder Einschränkung des Internets besonders interessant sind. [6][13] Zudem wird auch ein Server in Sydney (Australien) verwendet. Es war außerdem geplant, Scans über Server von San Jose (Costa Rica) und Peking (China) durchzuführen, allerdings konnte keine VPN-Verbindung mehr zu diesen erstellt werden, als die Scans durchgeführt werden sollten.

Um zu Überprüfen, ob die VPN-Server tatsächlich an dem angegebenen Standort sind, wurde zum einen die IP-Adresse überprüft. Hierzu wurde IP2Location genutzt. Hierbei werden die genutzten IP-Adressen mit einer Datenbank abgeglichen und somit der geographische Standort ermittelt. Fast alle Standorte stimmten überein. Einzig der Server, der angeblich in Suleja (Nigeria) ist, wurde in Lagos (Nigeria) verortet und der Server aus Sydney (Australien) wurde in Brisbane (Australien) verortet. [21]

Da aber durchaus solche Datenbanken manipuliert werden, um eine IP-Adresse mit einem anderen geographischen Standort zu verbinden als den tatsächlichen [23], werden die Standorte noch auf eine weitere Weise überprüft:

Dazu wird das Netzwerk RIPE Atlas genutzt. Es besteht aus vielen kleinen Hardware-Geräten bei Freiwilligen und Anker-Punkten in Datencentern. Diese Punkte werden mit ihrem Standort registriert und für jeden zur Verfügung gestellt, um mit diesen verschiedene Messungen durchzuführen. Hier werden die Punkte mit *ping* angesprochen. Mittels IP-echo-Nachrichten wird die Zeit gemessen, welche diese vom Anwender zum gewählten Punkt und zurück benötigen. Hierzu wurden nach Möglichkeit Punkte in jeder Stadt wie die gewählten Server-Standorte verwendet. Zu jedem dieser Punkte wurden mit jeder VPN-Verbindung via *ping* 10 Pakete gesendet und das Ergebnis mit dem niedrigsten Wert gesichert. Ein Durchschnittswert wäre hier nicht sinnvoll, da instabile Verbindungen und somit Ausreißer den Wert deutlich verändern können. Dies würde mehr die Stabilität überprüfen, hier soll aber die potenziell kürzeste Verbindungs-Strecke herausgefunden werden. [39] Als Referenz wurde zusätzlich google.com überprüft. Die Auflistung der Standorte mit den 3 niedrigsten ping-Werten sehen wie folgt aus:

Standort	Niedrigste Ping		2.-niedrigste Ping		3.-niedrigste Ping		Ping google.com
Washington DC*	160	Montreal	201	San Jose	202	New York	100
Los Angeles	167	Los Angeles	219	Mexiko City	234	New York	153
New York	123	New York	131	Montreal	183	Los Angeles	91
Montreal	110	New York	116	Montreal	166	Mexiko City	100
Mexiko City	226	Los Angeles	229	New York	229,1	Montreal	131
San Jose	227	San Jose	282	Mexiko City	332	New York	398
Sao Paulo	227	Sao Paulo	399	Mexiko City	405	Los Angeles	308
London	28	London	36	Paris	39	Frankfurt	53
Paris	40	Frankfurt	51	Zürich	54	Paris	31
Frankfurt	13	Frankfurt	21	Zürich	26	London	13
Stockholm	35	Stockholm	54	Frankfurt	55	Moskau	34
Zürich	26	Zürich	32	Frankfurt	41	Paris	31
Madrid	49	Madrid	65	Paris	77	London	49
Moskau	64	Moskau	82	Warschau	111	Zürich	125
Warschau	32	Warschau	48	Frankfurt	66	Stockholm	59
Istanbul	262	Istanbul	296	Frankfurt	308	Zürich	3889
Suleja*	122	Lagos	194	Johannesburg	215	London	122
Johannesburg	192	Johannesburg	361	Paris	369	London	197
Peking*	308	Hong Kong	363	Seoul	464	Los Angeles	297
Seoul	229	Hong Kong	322	Sydney	377	Seoul	210
Hong Kong	220	Hong Kong	304	Seoul	383	Mumbai	306
Chennai*	224	Hong Kong	253	Mumbai	282	Seoul	193
Bangkok*	432	Hong Kong	464	Frankfurt	508	Moskau	290
Sydney	310	Sydney	549	Seoul	577	New York	366

Tabelle 2.1: Die ping-Ergebnisse in Millisekunden: Für jeden Standort werden die drei niedrigsten ping-Werte angezeigt, sowie der Wert für google.com. Für die Standorte, die mit * markiert sind, sind keine RIPE-Atlas-Punkte in der selben Stadt vorhanden. In rot sind markiert sind übereinstimmende Standorte

Offensichtlich haben die meisten Standorte die schnellste Verbindung zu RIPE-Atlas-Punkten, die am selben Standort liegen. Auch bei den VPN-Standorten ohne direkte RIPE-Atlas-Punkte sind Verbindungen zu „Ersatz-“Punkten sehr schnell, wie bei Chennai (Ersatzpunkt in Mumbai) und Suleja (Ersatzpunkt in Lagos) ersichtlich ist. Interessant ist, dass die Standorte in Seoul und Mexiko City (Ping-Resultat zu Mexiko-City-Punkt: 269ms) bedeutend langsamere Verbindungen zu ihren jeweiligen Punkten haben. Interessant ist zudem, dass das ping-Resultat für google.com fast immer relativ gute Zeiten zeigt. Dies lässt darauf schließen, dass der Service an mehreren Standorten ansprechbar ist und nicht nur über einen lokalen Serverpunkt erreichbar ist.

Zwei Scans wurden für jeden VPN-Server-Standort durchgeführt, einmal mit einer OpenVPN-TCP-Verbindung und einmal mit einer OpenVPN-UDP-Verbindung wenn möglich. Einzig für die Standorte Istanbul und Lagos/Suleja war eine Verbindung nur mittels PureVPN-Anwendung möglich. Als Ziel-Port für die zusammengefasst 1,7 Millionen Domänen aus der Alexa- und Cisco-Liste wurde Port 443 ausgewählt. Dieser wird angeboten für HTTPS und bildet somit die Grundlage für fast alle sichere Web-Kommunikation wie Online-Banking, -Shopping und für Emails. [15]

Nach den Scans mittels ZGrab2 wurde jeweils neben der JSON-Datei ausgegeben, wie lange der Scan benötigt hat und wieviele erfolgreiche TLS-Handshakes durchgeführt wurden. Nach Kontinenten kategorisiert ergibt sich folgendes Diagramm:

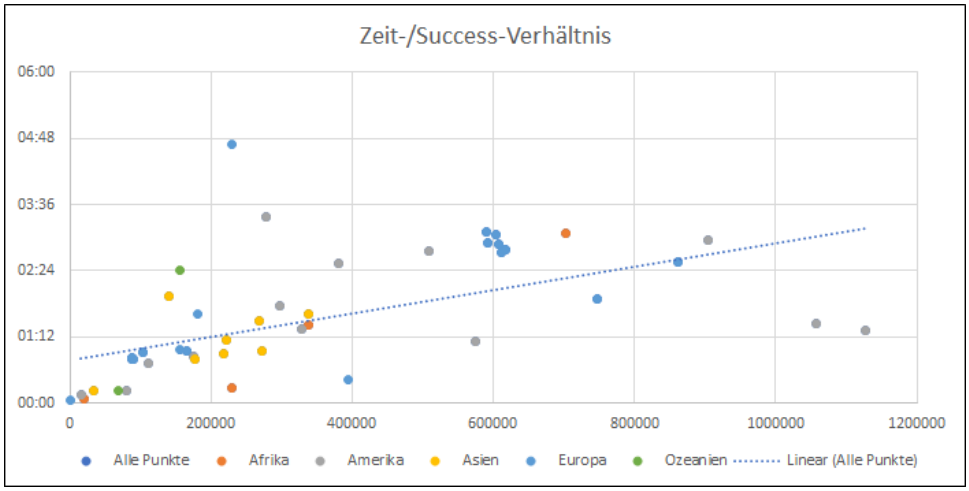

Abbildung 2.3: Alle Scan-Ergebnisse mit Zeit und erfolgreichen TLS-Handshakes nach Kontinenten kategorisiert.

Wie schon vorher erwähnt, steigt die Dauer der Scans durchschnittlich mit den positiven Ergebnissen. Die mit Abstand besten Ergebnisse (hinsichtlich TLS-Handshakes) stammen aus Amerika (Los Angeles, Montreal), aber auch ein großer Teil von den europäischen Scans ist durchaus erfolgreich. Der Rest (insbesondere Asien) haben deutlich weniger erfolgreiche Scans beinhaltet.

Die JSON-Dateien werden zur weiteren Analyse nun als JSON-Werte in eine psql-Datenbank eingefügt, wenn die einzelnen Zeilen als gültige JSON übersetzt werden können, zusammen mit einem Text-Wert für den Standort. Es werden allerdings nur pro Standort eine Datei (mit den meisten erfolgreichen TLS-Handshakes) verarbeitet, um die Vergleichbarkeit der Daten möglichst zu erhalten, da so die Anfragen nur von einem Server und IP-Adresse stammen. Dabei werden nur erfolgreiche TLS-Handshakes gesichert, um die Datenbank möglichst schlank zu halten. Es treten pro Domäne jeweils verschiedene Status auf:

- success: Der TLS-Handshake wurde erfolgreich durchgeführt.
- connection-timeout: Die Zeit bis zu einem Timeout (standardmäßig 10 Sekunden) ist abgelaufen, bspw. weil der LookUp (also Übersetzung der Domäne zur IP-Adresse) nicht funktioniert hat.

- io-timeout: Fehlermeldung: „EOF“ (Keine weiteren Daten zu lesen) oder „Connection reset by peer“ (Der Server hat die Verbindung zurückgesetzt [40]
- unknown-error: Fehlermeldung: „Remote Error“ oder „Internal Error“

Vergleicht man diese ergeben sich folgende Diagramme:

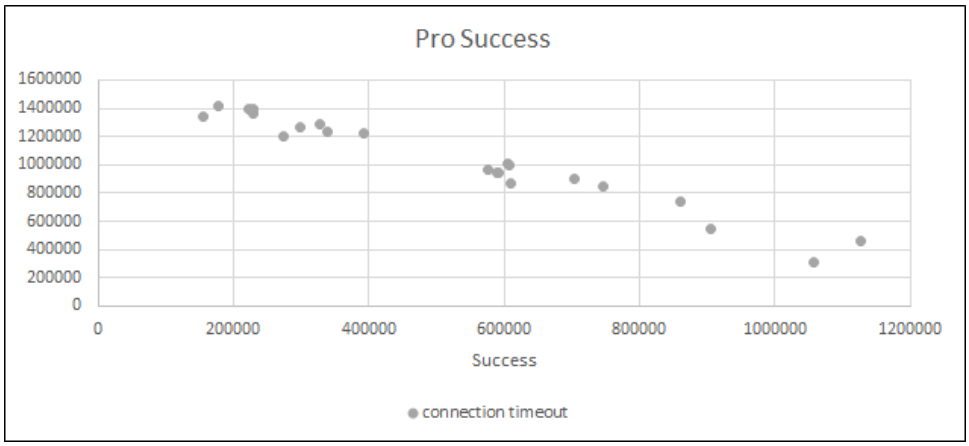

Abbildung 2.4: Pro Scan das Verhältnis zwischen erfolgreichen TLS-Handshakes und Timouts.

Hier wird es logischerweise deutlich, dass bei einer größeren Zahl an erfolgreichen TLS-Handshakes die Anzahl an Timeouts sinkt.

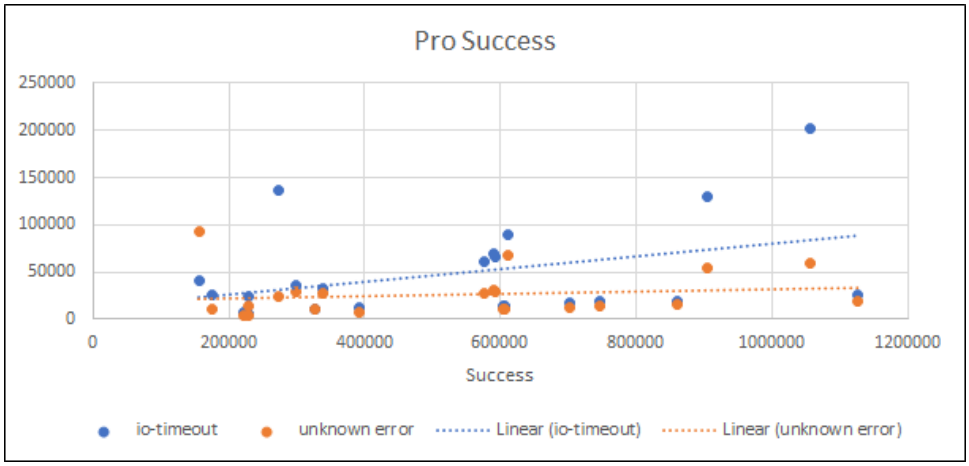

Abbildung 2.5: Pro Scan das Verhältnis zwischen erfolgreichen TLS-Handshakes und io-timeouts und unknown errors.

Interessanter Weise steigen die Fehler *io-timeout* und *unknown-error* durchschnittlich mit der Anzahl an erfolgreichen TLS-Handshakes. Es werden scheinbar mehr Server erreicht, wodurch

auch das Potenzial für solche Fehler innerhalb der Verbindung steigt. Allerdings treten diese Fehler in deutlich kleinerer Menge auf als die *connection-timeouts*.

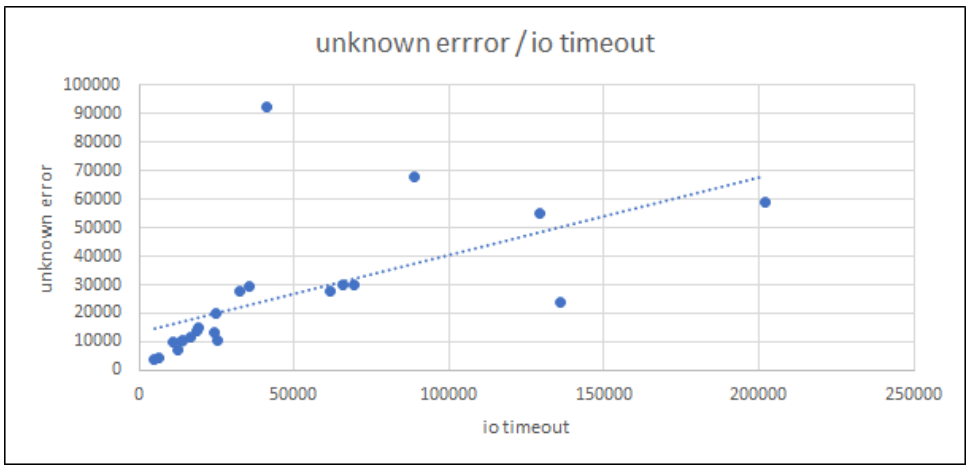

Abbildung 2.6: Pro Scan das Verhältnis zwischen io-timeouts und unknown errors.

Die Anzahl an *io-timeouts* und *unknown errors* steigen zusammen großteils linear, was die erste Hypothese stützt, dass diese jeweils steigen, wenn die Anzahl an aufgebauten Verbindungen steigt. Dies liegt natürlich auch daran, dass die dazugehörigen Fehler-Begründungen nur bei anfangs aufgebauter Verbindung auftreten können.

2.4 Analyse

Nachdem alle erfolgreichen TLS-Handshakes in eine psql-Datenbank übertragen wurden, können diese nun analysiert werden.

2.4.1 Domänen

Zunächst, um eine bessere Vergleichbarkeit zu späteren tieferen Analysen zu schaffen, sollte der Blick darauf gerichtet werden, ob die Domänen mit erfolgreichem TLS-Handshake sich überschneiden. Die Zusammenstellung bzw. Überschneidung dieser nach den VPN-Standorten gruppiert ist wie folgt:

Kontinent			Afrika	Afrika	Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	Asien	Asien	Asien	Asien	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Ozeanien
	Land		Nigeria	Südafrika	Brasilien	Kanada	Mexiko	USA	USA	USA	HongKong	Indien	Südkorea	Thailand	Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	Australien
		Stadt	Suleja	Johannesbur	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Hong Kong	Chennai	Seoul	Bangkok	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Sydney
Afrika	Nigeria	Suleja	229832	149263	48514	214671	63281	227651	191087	125133	56091	32871	47216	43470	125473	129671	132581	123957	188071	130996	173182	96408	45153	34819
Afrika	Südafrika	Johannesbur	149263	703146	178832	653015	189029	699221	556634	387785	216661	97227	174338	133386	381879	389248	385026	390409	544378	398399	465834	252967	139691	91403
Amerika	Brasilien	Sao Paulo	48514	178832	297939	278824	139943	296430	241959	136508	151376	92740	119622	84864	158308	152183	175603	150042	227879	163871	184283	92241	69218	50759
Amerika	Kanada	Montreal	214671	653015	278824	1056777	305494	1048557	845015	534340	314125	165123	253916	205059	548666	550392	592014	560975	801619	562908	694707	366454	215379	150030
Amerika	Mexiko	Mexiko City	63281	189029	139943	305494	327779	325916	272769	102091	127283	111619	107321	92447	165978	177324	188760	151492	257798	168197	249157	116298	69863	52815
Amerika	USA	Los Angeles	227651	699221	296430	1048557	325916	1126581	896760	570240	335237	174901	271377	219378	584762	586858	604596	599459	853792	604435	742172	389543	226995	154446
Amerika	USA	New York	191087	556634	241959	845015	272769	896760	904209	443792	263047	146648	191488	187516	457127	469932	499943	474514	706753	466023	610153	318658	184975	131377
Amerika	USA	Washington	125133	387785	136508	534340	102091	570240	443792	575192	175880	54808	143177	97182	335333	323715	332596	329649	450319	345971	355497	214176	108533	85456
Asien	HongKong	Hong Kong	56091	216661	151376	314125	127283	335237	263047	175880	337823	77012	125726	89539	177883	177696	195219	184456	256611	186582	199672	105426	79444	59039
Asien	Indien	Chennai	32871	97227	92740	165123	111619	174901	146648	54808	77012	176435	63265	57902	88242	90868	103560	80973	142527	94781	129105	62477	37519	26036
Asien	Südkorea	Seoul	47216	174338	119622	253916	107321	271377	191488	143177	125726	63265	272767	72184	149768	147500	160197	149271	201865	155243	165915	93131	61782	42753
Asien	Thailand	Bangkok	43470	133386	84864	205059	92447	219378	187516	97182	89539	57902	72184	221125	116454	114246	137370	108287	174637	111989	160367	77962	43325	37107
Europa	Deutschland	Frankfurt	125473	381879	158308	548666	165978	584762	457127	335333	177883	88242	149768	116454	590252	325519	337447	326406	466194	336474	396231	212814	118355	90294
Europa	Frankreich	Paris	129671	389248	152183	550392	177324	586858	469932	323715	177696	90868	147500	114246	325519	591936	343497	333970	474074	342358	401679	217960	112458	84481
Europa	Polen	Warschau	132581	385026	175603	592014	188760	604596	499943	332596	195219	103560	160197	137370	337447	343497	610480	333004	492893	343231	421502	227454	120528	93582
Europa	Russland	Moskau	123957	390409	150042	560975	151492	599459	474514	329649	184456	80973	149271	108287	326406	333970	333004	604359	469323	340720	392124	215490	119823	81596
Europa	Schweden	Stockholm	188071	544378	227879	801619	257798	853792	706753	450319	256611	142527	201865	174637	466194	474074	492893	469323	861468	479655	605280	321280	169848	123783
Europa	Schweiz	Zuerich	130996	398399	163871	562908	168197	604435	466023	345971	186582	94781	155243	111989	336474	342358	343231	340720	479655	607770	413228	224911	121646	79890
Europa	Spanien	Madrid	173182	465834	184283	694707	249157	742172	610153	355497	199672	129105	165915	160367	396231	401679	421502	392124	605280	413228	746667	283501	151518	113591
Europa	Türkei	Istanbul	96408	252967	92241	366454	116298	389543	318658	214176	105426	62477	93131	77962	212814	217960	227454	215490	321280	224911	283501	393279	74500	54537
Europa	UK	London	45153	139691	69218	215379	69863	226995	184975	108533	79444	37519	61782	43325	118355	112458	120528	119823	169848	121646	151518	74500	228445	33003
Ozeaninen	Australien	Sydney	34819	91403	50759	150030	52815	154446	131377	85456	59039	26036	42753	37107	90294	84481	93582	81596	123783	79890	113591	54537	33003	155711

Tabelle 2.2: Die Zahl der sich überschneidenden Domänen, gruppiert nach VPN-Standorten und pro Zeile farblich nach der Menge hervorgehoben. Um so stärker das Feld ausgefüllt ist, umso höher ist die Schnittmenge zwischen den Domänen der beiden Standorte relativ zu der Anzahl der Domänen des links stehenden VPN-Standorts.

Man erkennt hier sehr schnell, dass die Standorte mit den meisten erfolgreichen TLS-Handshakes auch oft für die meisten Übereinstimmungen der Domänen sorgen. Zu beachten sind die vermeintlich positiven Ausreißer, die entstehen, wenn die Standorte mit sich selbst verglichen werden. Um es übersichtlicher und genauer analysieren zu können, werden im folgenden die Ergebnisse nach Kontinenten analysiert:

Kontinent			Afrika	Afrika	
	Land		Nigeria	Südafrika	
		Stadt	Suleja	Johannesburg	Domänen
Afrika	Nigeria	Suleja	229832	149263	229832
Afrika	Südafrika	Johannesbur	149263	703146	703146
Amerika	Brasilien	Sao Paulo	48514	178832	297939
Amerika	Kanada	Montreal	214671	653015	1056777
Amerika	Mexiko	Mexiko City	63281	189029	327779
Amerika	USA	Los Angeles	227651	699221	1126581
Amerika	USA	New York	191087	556634	904209
Amerika	USA	Washington	125133	387785	575192
Asien	HongKong	Hong Kong	56091	216661	337823
Asien	Indien	Chennai	32871	97227	176435
Asien	Südkorea	Seoul	47216	174338	272767
Asien	Thailand	Bangkok	43470	133386	221125
Europa	Deutschland	Frankfurt	125473	381879	590252
Europa	Frankreich	Paris	129671	389248	591936
Europa	Polen	Warschau	132581	385026	610480
Europa	Russland	Moskau	123957	390409	604359
Europa	Schweden	Stockholm	188071	544378	861468
Europa	Schweiz	Zuerich	130996	398399	607770
Europa	Spanien	Madrid	173182	465834	746667
Europa	Türkei	Istanbul	96408	252967	393279
Europa	UK	London	45153	139691	228445
Ozeanien	Australien	Sydney	34819	91403	155711

Tabelle 2.3: Überschneidende Domänen für die VPN-Standorte in Afrika. Pro Reihe werden die Domänen relativ zur höchsten Übereinstimmung (Höchster Wert hat der Standort zu sich selbst) farblich markiert.

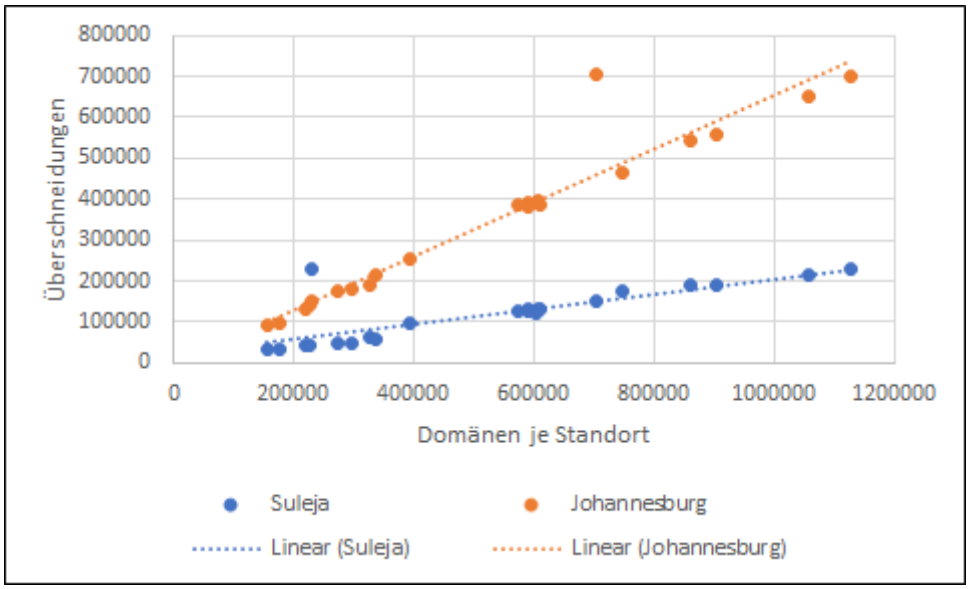

Abbildung 2.7: Überschneidende Domänen pro Domänen je VPN-Standort für afrikanische Server-Standorte.

Für die Standorte in Afrika wird deutlich, dass die Domänen am stärksten übereinstimmen, wenn der verglichene VPN-Standort eine möglichst große Menge an erfolgreichen VPN-Handshakes, also eine größere Menge an Domänen, hat. Außerdem scheint es keine bemerkenswerten (positiven) Ausreißer zwischen den beiden Afrikanischen Standorten zu geben: So ist die Überschneidung von Suleja mit Johannesburg vergleichbar mit den Überschneidungen von Suleja mit Standorten, die ähnlich große Domänen-Mengen haben wie Johannesburg. Eher fällt diese Überschneidung im Vergleich zu Suleja-Madrid ab.

Kontinent			Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	
	Land		Brasilien	Kanada	Mexiko	USA	USA	USA	
		Stadt	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Domänen
Afrika	Nigeria	Suleja	48514	214671	63281	227651	191087	125133	229832
Afrika	Südafrika	Johannesbur	178832	653015	189029	699221	556634	387785	703146
Amerika	Brasilien	Sao Paulo	297939	278824	139943	296430	241959	136508	297939
Amerika	Kanada	Montreal	278824	1056777	305494	1048557	845015	534340	1056777
Amerika	Mexiko	Mexiko City	139943	305494	327779	325916	272769	102091	327779
Amerika	USA	Los Angeles	296430	1048557	325916	1126581	896760	570240	1126581
Amerika	USA	New York	241959	845015	272769	896760	904209	443792	904209
Amerika	USA	Washington	136508	534340	102091	570240	443792	575192	575192
Asien	HongKong	Hong Kong	151376	314125	127283	335237	263047	175880	337823
Asien	Indien	Chennai	92740	165123	111619	174901	146648	54808	176435
Asien	Südkorea	Seoul	119622	253916	107321	271377	191488	143177	272767
Asien	Thailand	Bangkok	84864	205059	92447	219378	187516	97182	221125
Europa	Deutschland	Frankfurt	158308	548666	165978	584762	457127	335333	590252
Europa	Frankreich	Paris	152183	550392	177324	586858	469932	323715	591936
Europa	Polen	Warschau	175603	592014	188760	604596	499943	332596	610480
Europa	Russland	Moskau	150042	560975	151492	599459	474514	329649	604359
Europa	Schweden	Stockholm	227879	801619	257798	853792	706753	450319	861468
Europa	Schweiz	Zuerich	163871	562908	168197	604435	466023	345971	607770
Europa	Spanien	Madrid	184283	694707	249157	742172	610153	355497	746667
Europa	Türkei	Istanbul	92241	366454	116298	389543	318658	214176	393279
Europa	UK	London	69218	215379	69863	226995	184975	108533	228445
Ozeaninen	Australien	Sydney	50759	150030	52815	154446	131377	85456	155711

Tabelle 2.4: Überschneidende Domänen für die VPN-Standorte in Amerika. Pro Reihe werden die Domänen relativ zur höchsten Übereinstimmung (Höchster Wert hat der Standort zu sich selbst) farblich markiert.

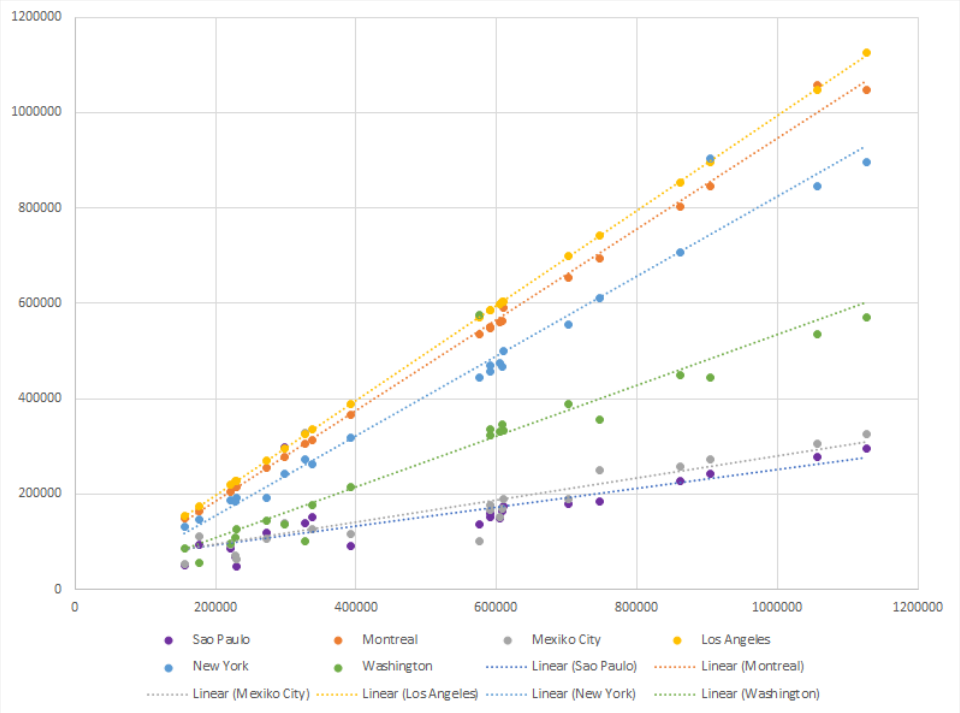

Abbildung 2.8: Überschneidende Domänen pro Domänen je VPN-Standort für amerikanische Server-Standorte.

Ähnlich sieht es bei den VPN-Standorten in Amerika aus: Je mehr ein Standort an erfolgreichen TLS-Handshakes besitzt, umso größer ist auch die Übereinstimmung. Negativer Ausreißer ist hier die Überschneidung Washington-Mexiko-City, die deutlich weniger gemeinsame Domänen haben als vergleichbare Überschneidungen wie Washington mit Sao Paulo, Suleja, Hongkong oder Seoul. Außerdem sind die Überschneidungen von Sao Paulo besonders mit Server-Standorten mit wenig erfolgreichen TLS-Handshakes inkonstant. Dass Montreal und Los Angeles kaum Varianz bei den Überschneidungen besitzen und sogar die Punkte der Überschneidungen der Standorte mit sich selbst auf den Linien von Los Angeles und Montreal liegen, lässt sich mit der hohen Menge an TLS-Handshakes begründen. Dies könnte darauf hin deuten, dass diese mit fast allen Domänen einen TLS-Handshake abgeschlossen habe, die es überhaupt ermöglicht haben. Dies zeigt sich auch in den der jeweiligen Spalte in der Tabelle 2.2, wo eine extrem hohe Übereinstimmung mit allen anderen Standorten zu finden ist.

Kontinent			Asien	Asien	Asien	Asien	Ozeaninen	
	Land		HongKong	Indien	Südkorea	Thailand	Australien	
		Stadt	Hong Kong	Chennai	Seoul	Bangkok	Sydney	Domänen
Afrika	Nigeria	Suleja	56091	32871	47216	43470	34819	229832
Afrika	Südafrika	Johannesbur	216661	97227	174338	133386	91403	703146
Amerika	Brasilien	Sao Paulo	151376	92740	119622	84864	50759	297939
Amerika	Kanada	Montreal	314125	165123	253916	205059	150030	1056777
Amerika	Mexiko	Mexiko City	127283	111619	107321	92447	52815	327779
Amerika	USA	Los Angeles	335237	174901	271377	219378	154446	1126581
Amerika	USA	New York	263047	146648	191488	187516	131377	904209
Amerika	USA	Washington	175880	54808	143177	97182	85456	575192
Asien	HongKong	Hong Kong	337823	77012	125726	89539	59039	337823
Asien	Indien	Chennai	77012	176435	63265	57902	26036	176435
Asien	Südkorea	Seoul	125726	63265	272767	72184	42753	272767
Asien	Thailand	Bangkok	89539	57902	72184	221125	37107	221125
Europa	Deutschland	Frankfurt	177883	88242	149768	116454	90294	590252
Europa	Frankreich	Paris	177696	90868	147500	114246	84481	591936
Europa	Polen	Warschau	195219	103560	160197	137370	93582	610480
Europa	Russland	Moskau	184456	80973	149271	108287	81596	604359
Europa	Schweden	Stockholm	256611	142527	201865	174637	123783	861468
Europa	Schweiz	Zuerich	186582	94781	155243	111989	79890	607770
Europa	Spanien	Madrid	199672	129105	165915	160367	113591	746667
Europa	Türkei	Istanbul	105426	62477	93131	77962	54537	393279
Europa	UK	London	79444	37519	61782	43325	33003	228445
Ozeaninen	Australien	Sydney	59039	26036	42753	37107	155711	155711

Tabelle 2.5: Überschneidende Domänen für die VPN-Standorte in Asien. Pro Reihe werden die Domänen relativ zur höchsten Übereinstimmung (Höchster Wert hat der Standort zu sich selbst) farblich markiert.

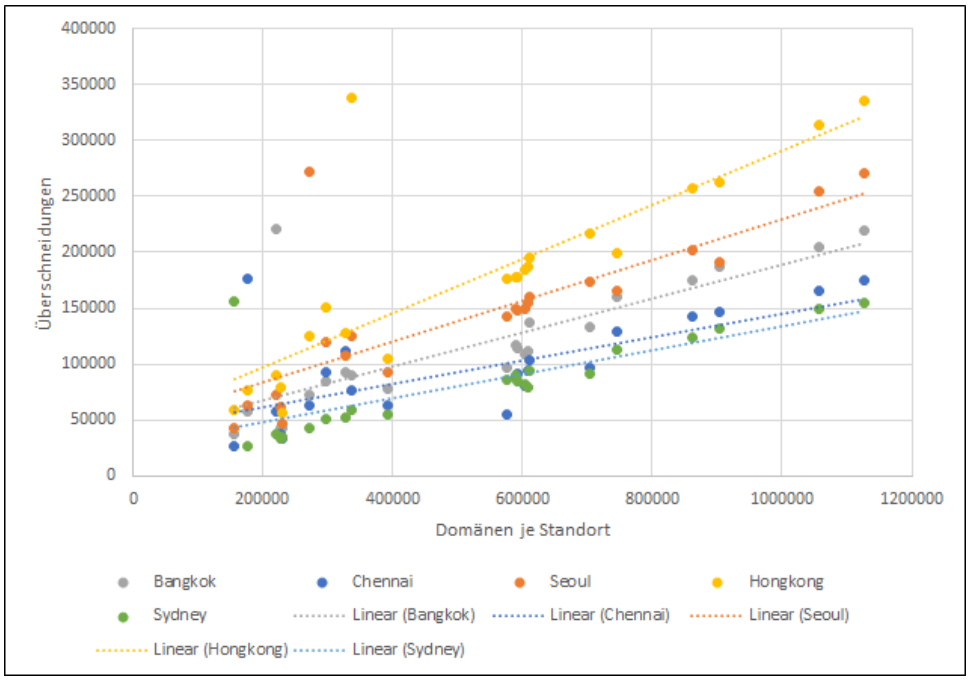

Abbildung 2.9: Überschneidende Domänen pro Domänen je VPN-Standort für asiatische Server-Standorte.

Auch bei den asiatischen Standorten fällt die relative starke Varianz bei Übereinstimmungen mit Servern mit wenig erfolgreichen TLS-Handshakes auf. Dies merkt man auch bei den Werten für Sydney, wo die Steigung verhältnismäßig steiler ist, aber einen deutlich tieferen Start-Punkt besitzt. Bemerkenswert ist hier die vor allem die geringe Übereinstimmung von Chennai und Washington.

Kontinent			Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	
	Land		Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	
		Stadt	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Domänen
Afrika	Nigeria	Suleja	125473	129671	132581	123957	188071	130996	173182	96408	45153	229832
Afrika	Südafrika	Johannesbur	381879	389248	385026	390409	544378	398399	465834	252967	139691	703146
Amerika	Brasilien	Sao Paulo	158308	152183	175603	150042	227879	163871	184283	92241	69218	297939
Amerika	Kanada	Montreal	548666	550392	592014	560975	801619	562908	694707	366454	215379	1056777
Amerika	Mexiko	Mexiko City	165978	177324	188760	151492	257798	168197	249157	116298	69863	327779
Amerika	USA	Los Angeles	584762	586858	604596	599459	853792	604435	742172	389543	226995	1126581
Amerika	USA	New York	457127	469932	499943	474514	706753	466023	610153	318658	184975	904209
Amerika	USA	Washington	335333	323715	332596	329649	450319	345971	355497	214176	108533	575192
Asien	HongKong	Hong Kong	177883	177696	195219	184456	256611	186582	199672	105426	79444	337823
Asien	Indien	Chennai	88242	90868	103560	80973	142527	94781	129105	62477	37519	176435
Asien	Südkorea	Seoul	149768	147500	160197	149271	201865	155243	165915	93131	61782	272767
Asien	Thailand	Bangkok	116454	114246	137370	108287	174637	111989	160367	77962	43325	221125
Europa	Deutschland	Frankfurt	590252	325519	337447	326406	466194	336474	396231	212814	118355	590252
Europa	Frankreich	Paris	325519	591936	343497	333970	474074	342358	401679	217960	112458	591936
Europa	Polen	Warschau	337447	343497	610480	333004	492893	343231	421502	227454	120528	610480
Europa	Russland	Moskau	326406	333970	333004	604359	469323	340720	392124	215490	119823	604359
Europa	Schweden	Stockholm	466194	474074	492893	469323	861468	479655	605280	321280	169848	861468
Europa	Schweiz	Zuerich	336474	342358	343231	340720	479655	607770	413228	224911	121646	607770
Europa	Spanien	Madrid	396231	401679	421502	392124	605280	413228	746667	283501	151518	746667
Europa	Türkei	Istanbul	212814	217960	227454	215490	321280	224911	283501	393279	74500	393279
Europa	UK	London	118355	112458	120528	119823	169848	121646	151518	74500	228445	228445
Ozeaninen	Australien	Sydney	90294	84481	93582	81596	123783	79890	113591	54537	33003	155711

Tabelle 2.6: Überschneidende Domänen für die VPN-Standorte in Europa. Pro Reihe werden die Domänen relativ zur höchsten Übereinstimmung (Höchster Wert hat der Standort zu sich selbst) farblich markiert.

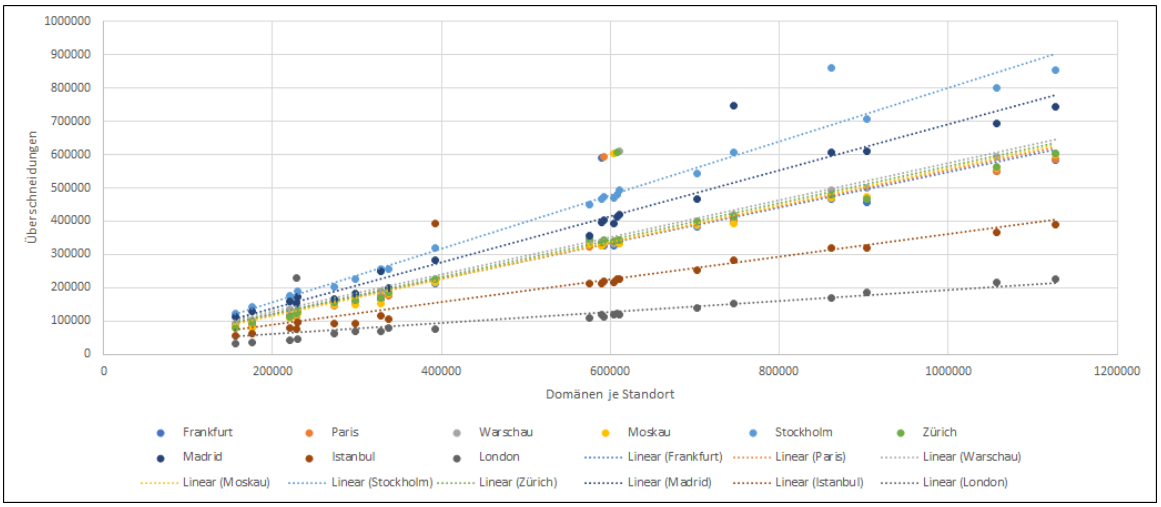

Abbildung 2.10: Überschneidende Domänen pro Domänen je VPN-Standort für europäische Server-Standorte.

Bei VPN-Server-Standorte hingegen schient es keine bemerkenswerten Varianzen zu geben. Die Punkte sammeln sich jeweils an den markierten linearen Steigungen, was dafür spricht, dass hier zwar in unterschiedlichen Menge erfolgreiche TLS-Handshakes durchgeführt wurden, aber in einem sich ähnelnden Pool an Domänen. Dieser weißt weder eine zu große Ähnlichkeit auf, noch eine bemerkenswerte Differenz.

2.4.2 Herkunftsländer der CAs

Zählt man die angegebenen Ländern aus den CA-Zertifikaten, so erhält man folgende Übersicht:

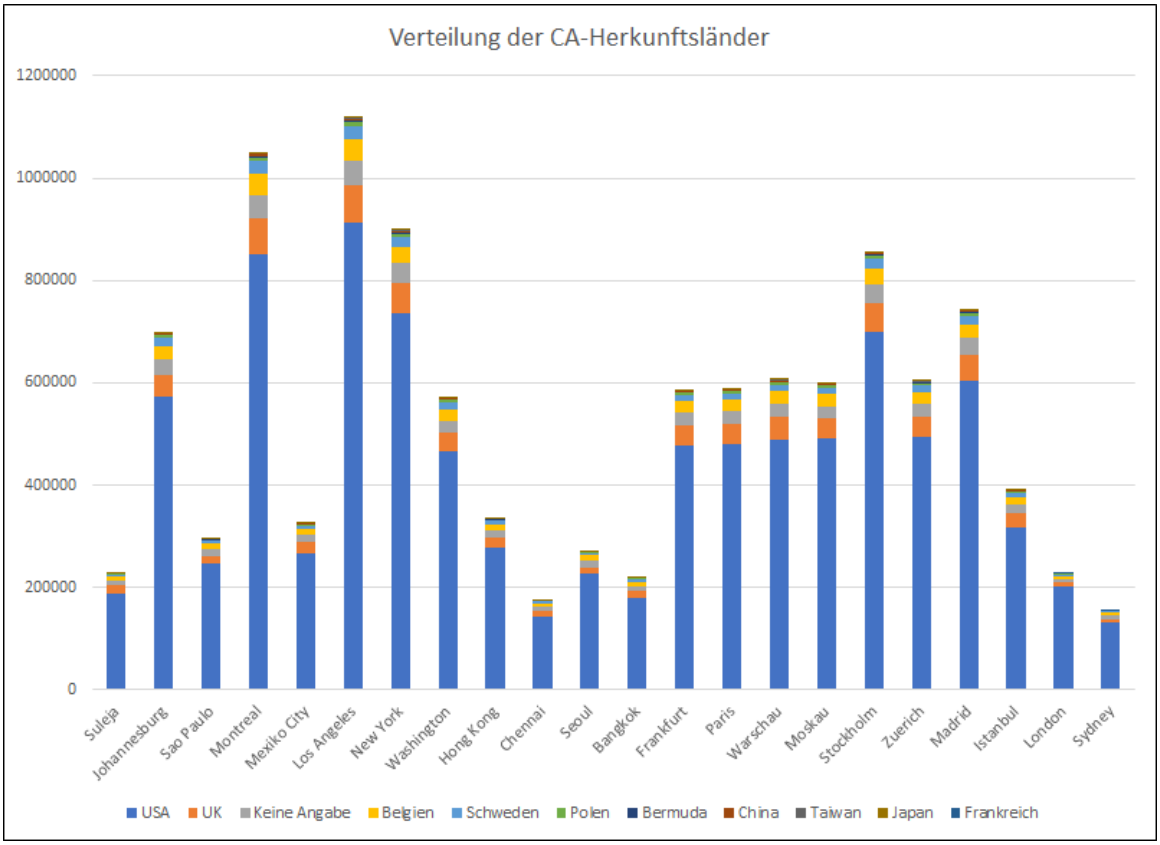

Abbildung 2.11: Die Verteilung der Top 10 der angegebenen Länder der CAs.

Hier fällt hauptsächlich die extreme Dominanz der USA auf. Das Verhältnis, CAs aus den USA zu kumulierten Top 10 Ländern der CAs, erscheint dabei sehr stabil um die 82%. Einzige Abweichungen sind die VPN-Standorte London und Sydney mit 88% und 85%. Dies kann allerdings in der verhältnismäßigen geringen Menge (insbesondere London im Vergleich mit den anderen europäischen Standorte) der erfolgreichen TLS-Handshakes begründet liegen. Interessanter sind die Ergebnisse, wenn die USA ausgerechnet werden:

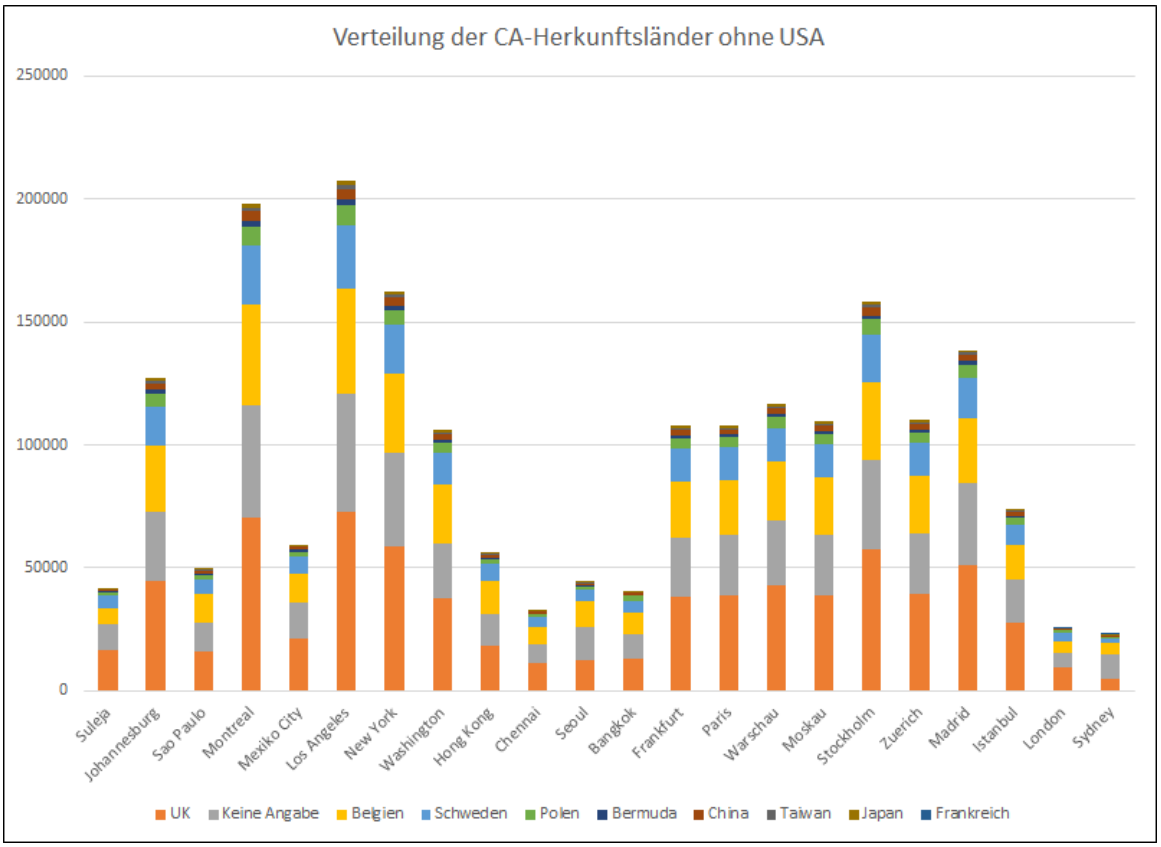

Abbildung 2.12: Die Verteilung der Top 9 der angegebenen Länder der CAs ohne die USA.

Das Verhältnis der Menge an CAs aus Großbritannien im Vergleich zu den ganzen Top 10 Ländern ist in der Regel um die 6,5%. Einzig in Suleja mit 7,5% ist das Verhältnis höher, allerdings in Seoul (4,7%), London (4,1%), was besonders bemerkenswert ist, und Sydney (3,3%) ist das Verhältnis merklich niedriger. Erstaunlicher Weise ist Belgien an Platz 3 der meisten CA-Herkunftsländer mit meist zwischen 3,5% und 4% Anteil an den Top 10 Ländern. Ausnahmen sind hier Suleja (3%), London (2,3%) und Sydney (3,1%), die allesamt verhältnismäßig wenig erfolgreiche TLS-Handshakes erreicht haben. Schweden stellt fast immer 2% der CA-Herkunftsländer, auch hier weichen London (1,4%) und Sydney (0,9%) stark ab. Dies lässt darauf schließen, dass die Domänen, die mit der VPN-Verbindung in Großbritanien und Australien erfolgreich einen TLS-Handshake durchgeführt haben, vornehmlich CAs aus den USA verwenden bzw. von diesen (bzw. deren Sub-CAs) unterzeichnet wurden und somit eventuell eine Besonderheit der VPN-Server darstellt. Zudem ist ein nicht unerheblicher Teil der CA-Zertifikate ohne angegebenes Land, in dem die CA ist.

Vergleicht man die CA-Länder für die TLS-Handshakes mit den gleichen Domänen nach den VPN-Standorten erhält man folgende Grafiken:

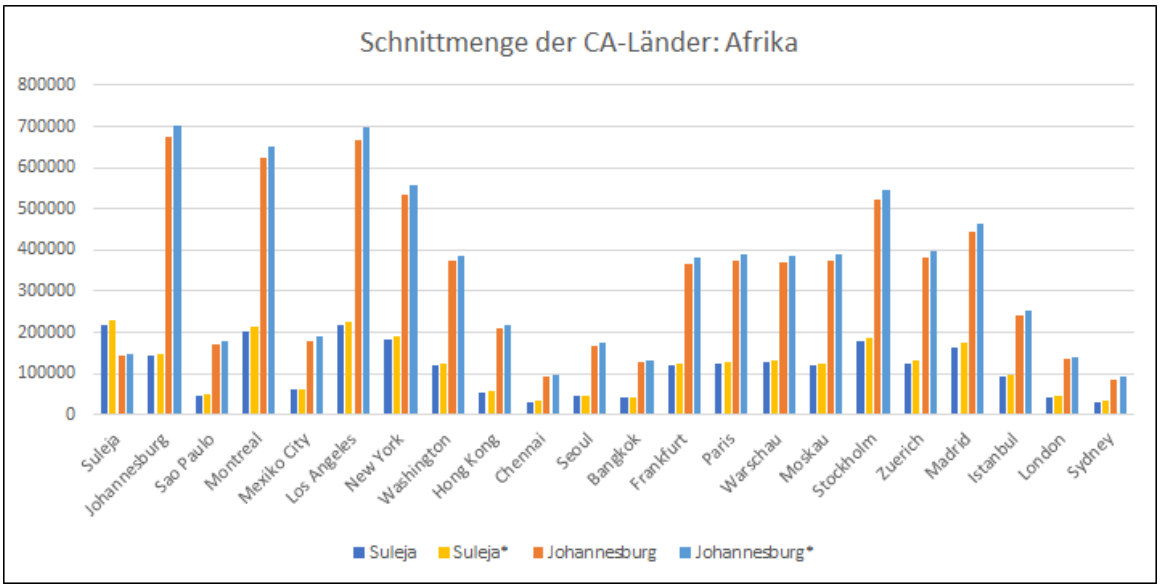

Abbildung 2.13: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die afrikanischen VPN-Standorte.

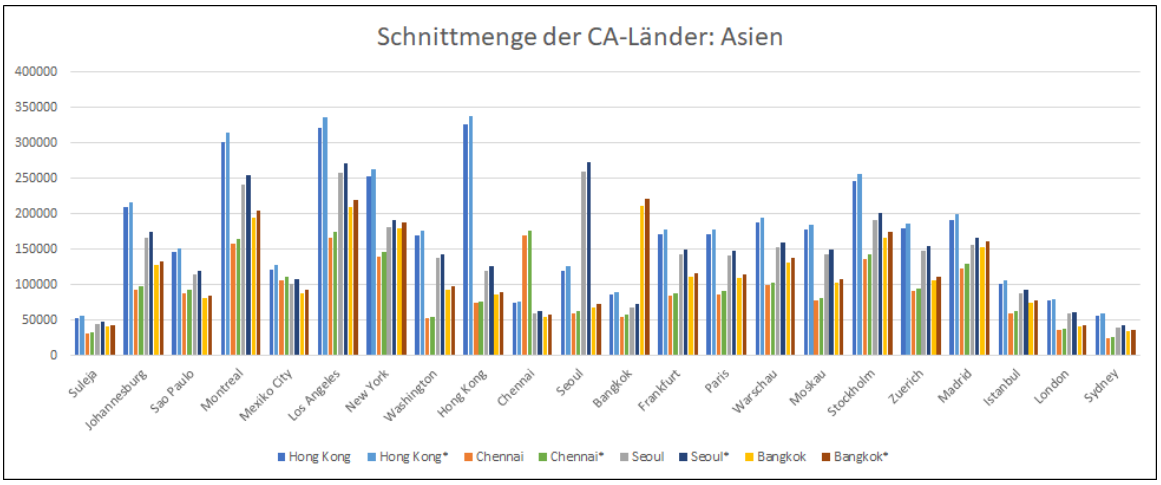

Abbildung 2.14: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die asiatischen VPN-Standorte.

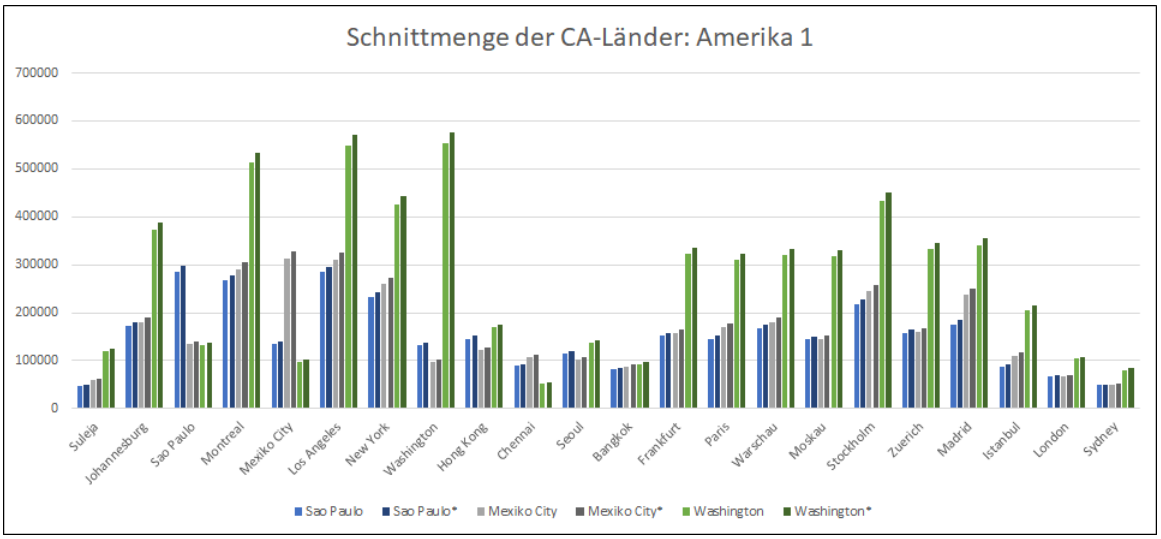

Abbildung 2.15: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die amerikanischen VPN-Standorte.

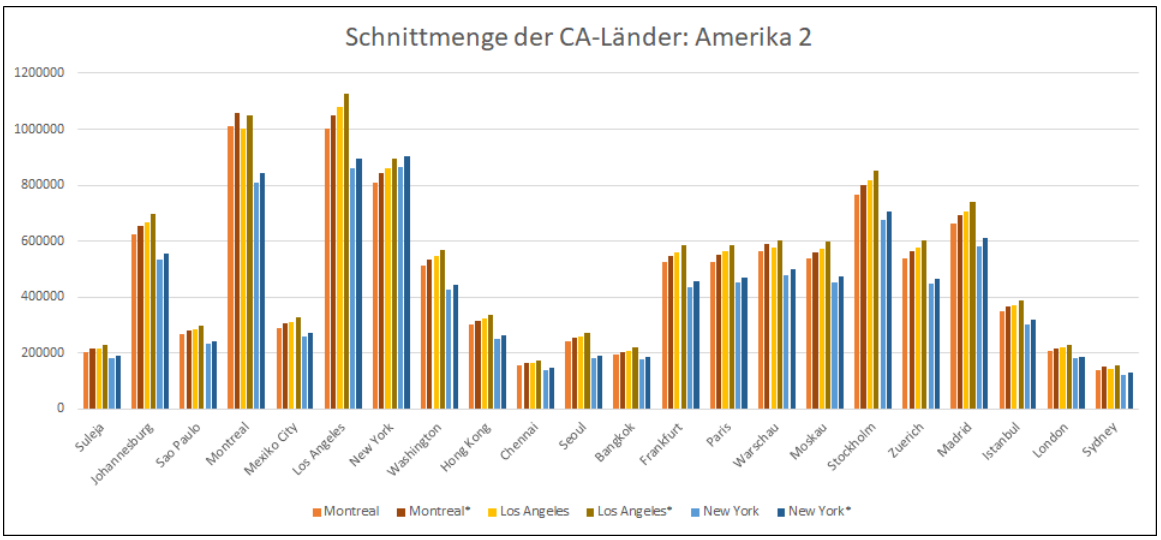

Abbildung 2.16: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die amerikanischen VPN-Standorte.

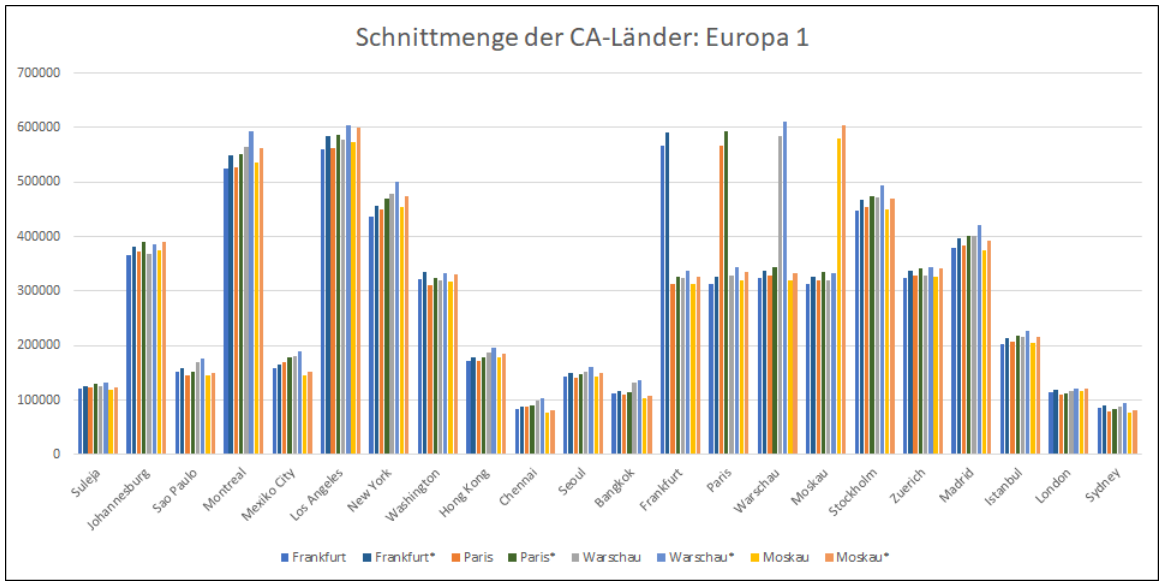

Abbildung 2.17: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die europäischen VPN-Standorte.

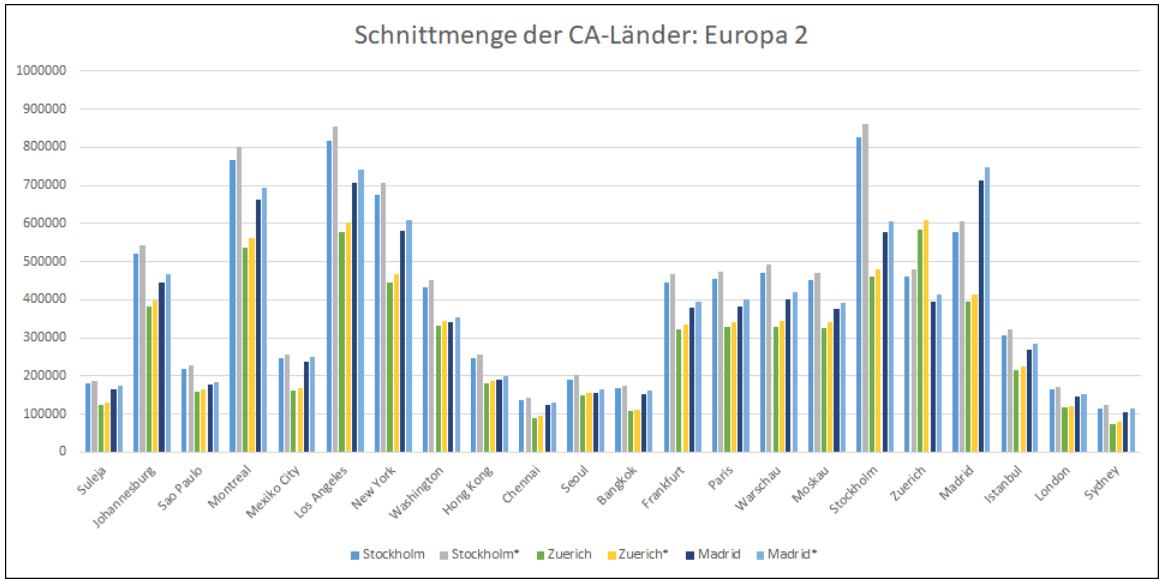

Abbildung 2.18: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die europäischen VPN-Standorte.

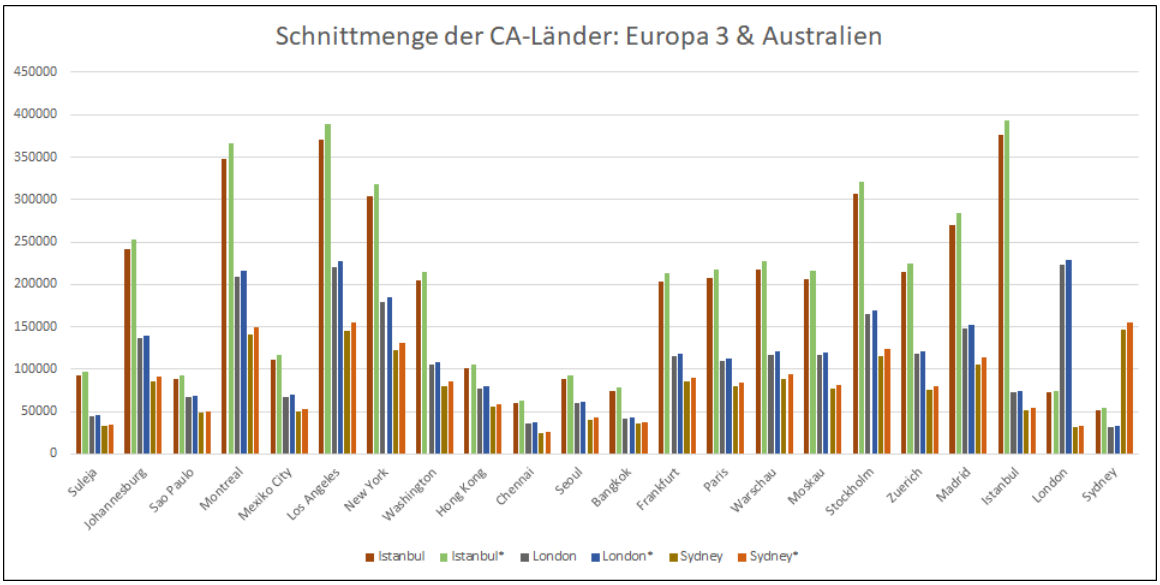

Abbildung 2.19: Ein Vergleich zwischen der Anzahl der erfolgreichen TLS-Handshakes zwischen zwei VPN-Standorten mit gleichen Domänen (mit * markiert) und zusätzlich mit dem gleichen CA-Land für die europäischen und australischen VPN-Standorte.

Es fällt auf, dass durchgehend ein kleiner Unterschied zwischen den Überschneidungen nach Domänen und Überschneidungen nach Domänen und CA-Ländern. Dieser entsteht dadurch, dass die CAs „ohne Land“ nicht unter sie zweite Überschneidung fallen. Dies verstärkt aber den Verdacht, dass die VPN-Standorte in London und Sydney nur Besonderheiten im TLS-Verbindung-Aufbauen besitzen, die CAs sich aber nicht an sich unterscheiden.

2.4.3 CA-Common Name

Sammelt man für alle Standorte jeweils die Top 10 der meist genutzten CA-Common Names so fallen vorallem zwei auf: Zum einen beruhen ca. 35% bis 40% der Zertifikate auf der CA „Let's Encrypt Authority X3“. Leichte Abweichungen sind bei Sao Paulo, Hongkong und Seoul bei denen nur ca. 30% auf dieser CA beruhen. Stärkere Ausreißer sind hier Sydney (49%) und London (22%), was ihre bisherigen Gemeinsamkeiten (in ihrer Abweichung) hinsichtlich der CA-Länder konterkariert. Die zweit-bedeutsamste CA ist „CloudFlare Inc ECC CA-2“. Auf diese gehen ca. 20% der Zertifikate zurück. Hier weichen Suleja, Istanbul und Sydney mit ca 16% ab und Sao Paulo, Hongkong und Seoul mit 26% bis 28% ab. Starker Ausreißer ist hier wieder London mit einem Anteil von 38%. Erschreckend hingegen ist, dass bei fast allen VPN-Standorten 7% bis 8% der Zertifikate (verglichen mit den Top 10 CAs) auf CAs zurückgehen,

bei dem der Common Name des Subjects leer ist! Auch hier weicht London wieder stark ab mit nur 4%.

Common Name der CA	Anzahl aller Zertifikate darauf zurückgehend	Anteil zu allen Zertifikaten (11.619.972)
Let's Encrypt Authority X3	3098563	26,7%
CloudFlare Inc ECC CA-2	1865513	16,1%
Ohne Common Name	671809	5,8%
GTS CA 1O1	583785	5,0%
COMODO RSA Certification Authority	565368	4,9%
USERTrust RSA Certification Authority	525913	4,5%
Starfield Services Root Certificate Authority - G2	472550	4,1%
DigiCert SHA2 Secure Server CA	427289	3,7%
DigiCert Global Root CA	294282	2,5%
AddTrust External CA Root	253665	2,2%

Tabelle 2.7: Die Zahl der Top 10 Common Names der CAs im Vergleich zur Gesamtzahl der TLS-Handshakes.

Außerdem wird im folgenden verglichen, wie das Verhältnis zwischen überschneidenden TLS-Handshakes zwischen zwei TLS-Standorten hinsichtlich Domänen-Name und die überschneidenden TLS-Handshakes zusätzlich nach dem gleichen Common Name:

Kontinent			Afrika	Afrika	Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	Asien	Asien	Asien	Asien	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Ozeaninen
	Land		Nigeria	Südafrika	Brasilien	Kanada	Mexiko	USA	USA	USA	HongKong	Indien	Südkorea	Thailand	Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	Australien
		Stadt	Suleja	Johannesbur	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Hong Kong	Chennai	Seoul	Bangkok	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Sydney
Afrika	Nigeria	Suleja	93,8%	94,0%	93,7%	93,0%	93,2%	93,4%	93,2%	93,4%	94,1%	93,4%	93,0%	93,4%	93,7%	93,1%	93,3%	93,3%	93,3%	93,9%	93,7%	93,7%	96,0%	92,7%
Afrika	Südafrika	Johannesburg	94,0%	94,5%	94,7%	93,9%	93,9%	93,8%	94,0%	94,3%	94,8%	94,2%	93,9%	94,2%	94,3%	93,9%	94,2%	94,1%	94,1%	94,4%	94,1%	94,1%	96,4%	93,6%
Amerika	Brasilien	Sao Paulo	93,7%	94,7%	94,8%	94,4%	94,3%	94,4%	94,2%	94,8%	94,4%	93,9%	94,4%	94,2%	94,2%	94,4%	94,8%	94,7%	94,4%	94,7%	94,2%	93,9%	96,1%	94,2%
Amerika	Kanada	Montreal	93,0%	93,9%	94,4%	94,1%	94,1%	94,3%	94,2%	94,1%	94,1%	93,3%	94,0%	93,3%	93,4%	93,8%	93,7%	93,8%	93,6%	94,0%	93,6%	93,2%	95,7%	92,8%
Amerika	Mexiko	Mexiko City	93,2%	93,9%	94,3%	94,1%	94,2%	94,1%	94,1%	94,0%	93,9%	93,3%	93,6%	93,6%	93,6%	94,1%	94,2%	94,0%	93,8%	94,0%	93,8%	93,3%	95,7%	93,2%
Amerika	USA	Los Angeles	93,4%	93,8%	94,4%	94,3%	94,1%	94,3%	94,4%	94,3%	94,2%	93,4%	94,0%	93,5%	93,7%	94,1%	94,1%	93,9%	93,9%	93,9%	93,6%	93,5%	95,8%	92,9%
Amerika	USA	New York	93,2%	94,0%	94,2%	94,2%	94,1%	94,4%	94,2%	93,9%	93,9%	93,3%	93,9%	93,5%	93,5%	94,0%	93,9%	93,8%	93,7%	94,1%	93,8%	93,3%	95,6%	92,6%
Amerika	USA	Washington	93,4%	94,3%	94,8%	94,1%	94,0%	94,3%	93,9%	94,3%	94,3%	93,6%	94,4%	93,8%	93,8%	94,1%	94,4%	94,3%	94,1%	94,5%	94,1%	93,6%	95,6%	93,0%
Asien	HongKong	Hong Kong	94,1%	94,8%	94,4%	94,1%	93,9%	94,2%	93,9%	94,3%	94,8%	94,2%	94,2%	94,4%	94,6%	94,1%	94,4%	94,3%	94,2%	94,8%	94,5%	94,2%	96,5%	94,0%
Asien	Indien	Chennai	93,4%	94,2%	93,9%	93,3%	93,3%	93,4%	93,3%	93,6%	94,2%	94,0%	93,3%	93,9%	93,8%	93,4%	93,7%	93,4%	93,4%	93,9%	93,8%	93,4%	95,7%	93,6%
Asien	Südkorea	Seoul	93,0%	93,9%	94,4%	94,0%	93,6%	94,0%	93,9%	94,4%	94,2%	93,3%	94,2%	93,5%	93,7%	94,1%	94,0%	94,0%	93,7%	94,0%	93,3%	93,1%	96,1%	93,7%
Asien	Thailand	Bangkok	93,4%	94,2%	94,2%	93,3%	93,6%	93,5%	93,5%	93,8%	94,4%	93,9%	93,5%	93,9%	93,8%	93,5%	93,7%	93,6%	93,6%	94,1%	93,8%	93,6%	95,8%	93,8%
Europa	Deutschland	Frankfurt	93,7%	94,3%	94,2%	93,4%	93,6%	93,7%	93,5%	93,8%	94,6%	93,8%	93,7%	93,8%	94,1%	93,5%	93,8%	93,7%	93,6%	94,3%	94,0%	93,7%	96,2%	93,3%
Europa	Frankreich	Paris	93,1%	93,9%	94,4%	93,8%	94,1%	94,1%	94,0%	94,1%	94,1%	93,4%	94,1%	93,5%	93,5%	94,0%	93,9%	93,9%	93,6%	94,1%	93,7%	93,3%	95,7%	93,0%
Europa	Polen	Warschau	93,3%	94,2%	94,8%	93,7%	94,2%	94,1%	93,9%	94,4%	94,4%	93,7%	94,0%	93,7%	93,8%	93,9%	94,2%	94,2%	94,0%	94,4%	94,0%	93,5%	95,8%	93,0%
Europa	Russland	Moskau	93,3%	94,1%	94,7%	93,8%	94,0%	93,9%	93,8%	94,3%	94,3%	93,4%	94,0%	93,6%	93,7%	93,9%	94,2%	94,1%	94,0%	94,3%	93,9%	93,5%	96,0%	93,1%
Europa	Schweden	Stockholm	93,3%	94,1%	94,4%	93,6%	93,8%	93,9%	93,7%	94,1%	94,2%	93,4%	93,7%	93,6%	93,6%	93,6%	94,0%	94,0%	94,0%	94,2%	93,9%	93,4%	95,9%	92,9%
Europa	Schweiz	Zuerich	93,9%	94,4%	94,7%	94,0%	94,0%	93,9%	94,1%	94,5%	94,8%	93,9%	94,0%	94,1%	94,3%	94,1%	94,4%	94,3%	94,2%	94,5%	94,2%	94,0%	96,4%	93,3%
Europa	Spanien	Madrid	93,7%	94,1%	94,2%	93,6%	93,8%	93,6%	93,8%	94,1%	94,5%	93,8%	93,3%	93,8%	94,0%	93,7%	94,0%	93,9%	93,9%	94,2%	94,1%	93,7%	96,2%	92,9%
Europa	Türkei	Istanbul	93,7%	94,1%	93,9%	93,2%	93,3%	93,5%	93,3%	93,6%	94,2%	93,4%	93,1%	93,6%	93,7%	93,3%	93,5%	93,5%	93,4%	94,0%	93,7%	93,9%	96,0%	92,7%
Europa	UK	London	96,0%	96,4%	96,1%	95,7%	95,7%	95,8%	95,6%	95,6%	96,5%	95,7%	96,1%	95,8%	96,2%	95,7%	95,8%	96,0%	95,9%	96,4%	96,2%	96,0%	96,4%	95,2%
Ozeaninen	Australien	Sydney	92,7%	93,6%	94,2%	92,8%	93,2%	92,9%	92,6%	93,0%	94,0%	93,6%	93,7%	93,8%	93,3%	93,0%	93,0%	93,1%	92,9%	93,3%	92,9%	92,7%	95,2%	93,2%

Tabelle 2.8: Verhältnis von sich überschneidenden TLS-Handshakes nach Domains und nach zusätzlich dem CA-Common-Name.

Der Prozentsatz liegt durchgehend bei 92% oder höher. Ein großer Teil der fehlenden Übereinstimmungen lassen sich auch hier auf leere Common Names zurückverfolgen. Dies lässt vermuten, dass die CAs zwischen allen Standorten relativ gleich genutzt werden.

2.4.4 Serialnumber des CA-Zertifikats

Nun stellt sich die Frage, ob die CAs nicht nur in ähnlicher Menge genutzt werden, sondern ob die Zertifikate der Domänen auch auf die gleichen Zertifikate dieser CAs zurückgehen, oder diese mehrere Zertifikate nutzen und dies ggf. in unterschiedlichen Regionen. Dazu vergleicht man die sich überschneidenden TLS-Handshakes zwischen zwei TLS-Standorten hinsichtlich Domänen-Name und die überschneidenden TLS-Handshakes zusätzlich nach der gleichen SerialNumber (eindeutige Nummer für ein Zertifikat) der CA-Zertifikate, erhält man folgende Ergebnisse:

Kontinent			Afrika	Afrika	Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	Asien	Asien	Asien	Asien	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Ozeaninen
	Land		Nigeria	Südafrika	Brasilien	Kanada	Mexiko	USA	USA	USA	HongKong	Indien	Südkorea	Thailand	Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	Australien
		Stadt	Suleja	Johannesbur	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Hong Kong	Chennai	Seoul	Bangkok	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Sydney
Afrika	Nigeria	Suleja	96,16%	95,94%	95,12%	94,38%	94,47%	94,56%	94,63%	95,36%	96,04%	95,52%	93,79%	95,57%	96,05%	94,99%	95,02%	95,40%	95,41%	95,71%	95,50%	95,95%	97,46%	93,35%
Afrika	Südafrika	Johannesburg	95,94%	96,61%	96,24%	95,14%	95,32%	95,32%	95,26%	96,12%	96,67%	96,10%	94,99%	96,18%	96,43%	95,67%	95,76%	96,10%	96,03%	96,41%	96,07%	95,93%	97,64%	94,33%
Amerika	Brasilien	Sao Paulo	95,12%	96,24%	96,61%	95,74%	95,81%	95,86%	95,74%	96,60%	96,05%	95,53%	95,42%	95,81%	95,76%	96,12%	96,28%	96,58%	96,24%	96,28%	95,75%	95,29%	97,10%	95,44%
Amerika	Kanada	Montreal	94,38%	95,14%	95,74%	96,30%	95,68%	96,17%	96,23%	95,84%	95,33%	94,66%	95,15%	94,75%	94,94%	95,90%	95,26%	95,52%	95,35%	95,29%	94,85%	94,45%	96,46%	93,38%
Amerika	Mexiko	Mexiko City	94,47%	95,32%	95,81%	95,68%	96,22%	95,83%	95,88%	95,77%	95,29%	94,80%	94,74%	95,21%	95,05%	96,16%	95,49%	95,71%	95,54%	95,45%	95,22%	94,72%	96,61%	94,09%
Amerika	USA	Los Angeles	94,56%	95,32%	95,86%	96,17%	95,83%	96,40%	96,27%	95,99%	95,44%	94,78%	95,33%	94,95%	95,10%	96,05%	95,35%	95,66%	95,51%	95,48%	95,06%	94,63%	96,52%	93,42%
Amerika	USA	New York	94,63%	95,26%	95,74%	96,23%	95,88%	96,27%	96,43%	95,82%	95,37%	94,83%	95,06%	94,93%	95,06%	96,05%	95,35%	95,63%	95,50%	95,37%	95,06%	94,66%	96,53%	93,25%
Amerika	USA	Washington	95,36%	96,12%	96,60%	95,84%	95,77%	95,99%	95,82%	96,71%	96,08%	95,56%	95,79%	95,70%	95,96%	96,34%	96,38%	96,61%	96,41%	96,34%	95,78%	95,50%	96,88%	93,72%
Asien	HongKong	Hong Kong	96,04%	96,67%	96,05%	95,33%	95,29%	95,44%	95,37%	96,08%	96,84%	96,32%	95,13%	96,47%	96,65%	95,67%	95,88%	96,16%	95,99%	96,43%	96,01%	96,09%	97,85%	95,37%
Asien	Indien	Chennai	95,52%	96,10%	95,53%	94,66%	94,80%	94,78%	94,83%	95,56%	96,32%	96,27%	94,22%	96,11%	96,07%	95,20%	95,40%	95,47%	95,52%	95,76%	95,55%	95,56%	97,38%	95,26%
Asien	Südkorea	Seoul	93,79%	94,99%	95,42%	95,15%	94,74%	95,33%	95,06%	95,79%	95,13%	94,22%	95,66%	94,58%	94,69%	95,53%	94,98%	95,27%	94,93%	95,20%	94,38%	93,97%	96,55%	94,17%
Asien	Thailand	Bangkok	95,57%	96,18%	95,81%	94,75%	95,21%	94,95%	94,93%	95,70%	96,47%	96,11%	94,58%	96,22%	96,09%	95,32%	95,47%	95,59%	95,68%	95,89%	95,74%	95,62%	97,23%	95,13%
Europa	Deutschland	Frankfurt	96,05%	96,43%	95,76%	94,94%	95,05%	95,10%	95,06%	95,96%	96,65%	96,07%	94,69%	96,09%	96,57%	95,52%	95,62%	95,90%	95,87%	96,26%	95,88%	96,03%	97,72%	94,20%
Europa	Frankreich	Paris	94,99%	95,67%	96,12%	95,90%	96,16%	96,05%	96,05%	96,34%	95,67%	95,20%	95,53%	95,32%	95,52%	96,49%	95,79%	96,05%	95,90%	95,84%	95,40%	95,04%	96,78%	93,68%
Europa	Polen	Warschau	95,02%	95,76%	96,28%	95,26%	95,49%	95,35%	95,35%	96,38%	95,88%	95,40%	94,98%	95,47%	95,62%	95,79%	96,28%	96,26%	96,10%	96,00%	95,54%	95,12%	96,77%	93,81%
Europa	Russland	Moskau	95,40%	96,10%	96,58%	95,52%	95,71%	95,66%	95,63%	96,61%	96,16%	95,47%	95,27%	95,59%	95,90%	96,05%	96,26%	96,56%	96,42%	96,25%	95,86%	95,40%	97,13%	93,87%
Europa	Schweden	Stockholm	95,41%	96,03%	96,24%	95,35%	95,54%	95,51%	95,50%	96,41%	95,99%	95,52%	94,93%	95,68%	95,87%	95,90%	96,10%	96,42%	96,42%	96,24%	95,84%	95,47%	97,08%	93,73%
Europa	Schweiz	Zuerich	95,71%	96,41%	96,28%	95,29%	95,45%	95,48%	95,37%	96,34%	96,43%	95,76%	95,20%	95,89%	96,26%	95,84%	96,00%	96,25%	96,24%	96,57%	96,22%	95,79%	97,41%	93,99%
Europa	Spanien	Madrid	95,50%	96,07%	95,75%	94,85%	95,22%	95,06%	95,06%	95,78%	96,01%	95,55%	94,38%	95,74%	95,88%	95,40%	95,54%	95,86%	95,84%	96,22%	96,14%	95,44%	97,18%	93,55%
Europa	Türkei	Istanbul	95,95%	95,93%	95,29%	94,45%	94,72%	94,63%	94,66%	95,50%	96,09%	95,56%	93,97%	95,62%	96,03%	95,04%	95,12%	95,40%	95,47%	95,79%	95,44%	96,17%	97,48%	93,52%
Europa	UK	London	97,46%	97,64%	97,10%	96,46%	96,61%	96,52%	96,53%	96,88%	97,85%	97,38%	96,55%	97,23%	97,72%	96,78%	96,77%	97,13%	97,08%	97,41%	97,18%	97,48%	97,85%	96,00%
Ozeaninen	Australien	Sydney	93,35%	94,33%	95,44%	93,38%	94,09%	93,42%	93,25%	93,72%	95,37%	95,26%	94,17%	95,13%	94,20%	93,68%	93,81%	93,87%	93,73%	93,99%	93,55%	93,52%	96,00%	94,19%

Tabelle 2.9: Verhältnis von sich überschneidenden TLS-Handshakes nach Domains und nach zusätzlich der CA-Zertifikat-SerialNumber. In grün markiert sind die Felder, die einen gleichen oder höheren Prozentsatz haben als bei der Tabelle 2.8

Der Prozentsatz liegt durchgehend bei 92% oder höher. Alle Felder weisen sogar eine höhere Übereinstimmung auf als beim Vergleich mit TLS-Handshakes nach den CA-Common-Names. Begründet ist dies zum Teil darin, dass CA-Zertifikate ohne Common Name dennoch die gleiche SerialNumber nutzen. Dies stärkt das Bild, dass die CAs und auch deren Zertifikate zwischen allen Standorten relativ gleich genutzt werden.

2.4.5 Serialnumber der Zwischenzertifikate

Aufgrund der Wurzelstruktur des PKI bzw. der Zertifikatsketten, scheint es sehr logisch und nachvollziehbar, dass die CA-Zertifikate übereinstimmen. Doch dies entwertet in gewisser Weise auch die Bedeutung der letzten Ergebnisse. Daher ist es nun sinnvoll die Zertifikate der (Sub-)Certificate Authorities bzw. die Zwischenzertifikate (auch mittels der SerialNumber) zu überprüfen. Im folgenden wird analog zur Tabelle 2.9 das Verhältnis pro VPN-Standort-Paar zwischen Überschneidung an Domänen und Überschneidung zusätzlich der SerialNumber des ersten Zwischen-Zertifikats, also des Zertifikats, das genutzt wurde, um das Zertifikat der Domäne zu signieren, welches letztendlich zur sicheren Verschlüsselung der TLS-Verbindung genutzt wird:

Kontinent			Afrika	Afrika	Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	Asien	Asien	Asien	Asien	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Ozeaninen
	Land		Nigeria	Südafrika	Brasilien	Kanada	Mexiko	USA	USA	USA	HongKong	Indien	Südkorea	Thailand	Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	Australien
		Stadt	Suleja	Johannesbur	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Hong Kong	Chennai	Seoul	Bangkok	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Sydney
Afrika	Nigeria	Suleja	96,16%	95,94%	95,12%	94,38%	94,47%	94,56%	94,63%	95,36%	96,04%	95,52%	93,79%	95,57%	96,05%	94,99%	95,02%	95,40%	95,41%	95,71%	95,50%	95,95%	97,46%	93,35%
Afrika	Südafrika	Johannesburg	95,94%	96,61%	96,24%	95,14%	95,32%	95,32%	95,26%	96,12%	96,67%	96,10%	94,99%	96,18%	96,43%	95,67%	95,76%	96,10%	96,03%	96,41%	96,07%	95,93%	97,64%	94,33%
Amerika	Brasilien	Sao Paulo	95,12%	96,24%	96,61%	95,74%	95,81%	95,86%	95,74%	96,60%	96,05%	95,53%	95,42%	95,81%	95,76%	96,12%	96,28%	96,58%	96,24%	96,28%	95,75%	95,29%	97,10%	95,44%
Amerika	Kanada	Montreal	94,38%	95,14%	95,74%	96,30%	95,68%	96,17%	96,23%	95,84%	95,33%	94,66%	95,15%	94,75%	94,94%	95,90%	95,26%	95,52%	95,35%	95,29%	94,85%	94,45%	96,46%	93,38%
Amerika	Mexiko	Mexiko City	94,47%	95,32%	95,81%	95,68%	96,22%	95,83%	95,88%	95,77%	95,29%	94,80%	94,74%	95,21%	95,05%	96,16%	95,49%	95,71%	95,54%	95,45%	95,22%	94,72%	96,61%	94,09%
Amerika	USA	Los Angeles	94,56%	95,32%	95,86%	96,17%	95,83%	96,40%	96,27%	95,99%	95,44%	94,78%	95,33%	94,95%	95,10%	96,05%	95,35%	95,66%	95,51%	95,48%	95,06%	94,63%	96,52%	93,42%
Amerika	USA	New York	94,63%	95,26%	95,74%	96,23%	95,88%	96,27%	96,43%	95,82%	95,37%	94,83%	95,06%	94,93%	95,06%	96,05%	95,35%	95,63%	95,50%	95,37%	95,06%	94,66%	96,53%	93,25%
Amerika	USA	Washington	95,36%	96,12%	96,60%	95,84%	95,77%	95,99%	95,82%	96,71%	96,08%	95,56%	95,79%	95,70%	95,96%	96,34%	96,38%	96,61%	96,41%	96,34%	95,78%	95,50%	96,88%	93,72%
Asien	HongKong	Hong Kong	96,04%	96,67%	96,05%	95,33%	95,29%	95,44%	95,37%	96,08%	96,84%	96,32%	95,13%	96,47%	96,65%	95,67%	95,88%	96,16%	95,99%	96,43%	96,01%	96,09%	97,85%	95,37%
Asien	Indien	Chennai	95,52%	96,10%	95,53%	94,66%	94,80%	94,78%	94,83%	95,56%	96,32%	96,27%	94,22%	96,11%	96,07%	95,20%	95,40%	95,47%	95,52%	95,76%	95,55%	95,56%	97,38%	95,26%
Asien	Südkorea	Seoul	93,79%	94,99%	95,42%	95,15%	94,74%	95,33%	95,06%	95,79%	95,13%	94,22%	95,66%	94,58%	94,69%	95,53%	94,98%	95,27%	94,93%	95,20%	94,38%	93,97%	96,55%	94,17%
Asien	Thailand	Bangkok	95,57%	96,18%	95,81%	94,75%	95,21%	94,95%	94,93%	95,70%	96,47%	96,11%	94,58%	96,22%	96,09%	95,32%	95,47%	95,59%	95,68%	95,89%	95,74%	95,62%	97,23%	95,13%
Europa	Deutschland	Frankfurt	96,05%	96,43%	95,76%	94,94%	95,05%	95,10%	95,06%	95,96%	96,65%	96,07%	94,69%	96,09%	96,57%	95,52%	95,62%	95,90%	95,87%	96,26%	95,88%	96,03%	97,72%	94,20%
Europa	Frankreich	Paris	94,99%	95,67%	96,12%	95,90%	96,16%	96,05%	96,05%	96,34%	95,67%	95,20%	95,53%	95,32%	95,52%	96,49%	95,79%	96,05%	95,90%	95,84%	95,40%	95,04%	96,78%	93,68%
Europa	Polen	Warschau	95,02%	95,76%	96,28%	95,26%	95,49%	95,35%	95,35%	96,38%	95,88%	95,40%	94,98%	95,47%	95,62%	95,79%	96,28%	96,26%	96,10%	96,00%	95,54%	95,12%	96,77%	93,81%
Europa	Russland	Moskau	95,40%	96,10%	96,58%	95,52%	95,71%	95,66%	95,63%	96,61%	96,16%	95,47%	95,27%	95,59%	95,90%	96,05%	96,26%	96,56%	96,42%	96,25%	95,86%	95,40%	97,13%	93,87%
Europa	Schweden	Stockholm	95,41%	96,03%	96,24%	95,35%	95,54%	95,51%	95,50%	96,41%	95,99%	95,52%	94,93%	95,68%	95,87%	95,90%	96,10%	96,42%	96,42%	96,24%	95,84%	95,47%	97,08%	93,73%
Europa	Schweiz	Zuerich	95,71%	96,41%	96,28%	95,29%	95,45%	95,48%	95,37%	96,34%	96,43%	95,76%	95,20%	95,89%	96,26%	95,84%	96,00%	96,25%	96,24%	96,57%	96,22%	95,79%	97,41%	93,99%
Europa	Spanien	Madrid	95,50%	96,07%	95,75%	94,85%	95,22%	95,06%	95,06%	95,78%	96,01%	95,55%	94,38%	95,74%	95,88%	95,40%	95,54%	95,86%	95,84%	96,22%	96,14%	95,44%	97,18%	93,55%
Europa	Türkei	Istanbul	95,95%	95,93%	95,29%	94,45%	94,72%	94,63%	94,66%	95,50%	96,09%	95,56%	93,97%	95,62%	96,03%	95,04%	95,12%	95,40%	95,47%	95,79%	95,44%	96,17%	97,48%	93,52%
Europa	UK	London	97,46%	97,64%	97,10%	96,46%	96,61%	96,52%	96,53%	96,88%	97,85%	97,38%	96,55%	97,23%	97,72%	96,78%	96,77%	97,13%	97,08%	97,41%	97,18%	97,48%	97,85%	96,00%
Ozeaninen	Australien	Sydney	93,35%	94,33%	95,44%	93,38%	94,09%	93,42%	93,25%	93,72%	95,37%	95,26%	94,17%	95,13%	94,20%	93,68%	93,81%	93,87%	93,73%	93,99%	93,55%	93,52%	96,00%	94,19%

Tabelle 2.10: Verhältnis von sich überschneidenden TLS-Handshakes nach Domains und nach zusätzlich der ersten Sub-CA-Zertifikat-Serialnumber. In grün markiert sind die Felder, die einen gleichen oder höheren Prozentsatz haben als bei der Tabelle 2.9

Auch hier ist die Übereinstimmung bei jedem einzelnen VPN-Standort-Paar mindestens genauso hoch wie bei der CA-SerialNumber-Übereinstimmung aus Tabelle 2.9.

2.4.6 Zertifikate der Domänen

Nun bleibt die Frage, ob sich die Zertifikate der Domänen selber bei verschiedenen VPN-Standorten unterscheiden. Dazu wird hier auch wieder das Verhältnis gebildet zwischen den Übereinstimmungen nach Domänen und Übereinstimmungen zusätzlich nach den Domänen-Zertifikate (genauer nach den eindeutigen SerialNumbers). Diese werden dann mit den Prozentsätzen aus Tabelle 2.10 verglichen:

Kontinent			Afrika	Afrika	Amerika	Amerika	Amerika	Amerika	Amerika	Amerika	Asien	Asien	Asien	Asien	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Europa	Ozeaninen
	Land		Nigeria	Südafrika	Brasilien	Kanada	Mexiko	USA	USA	USA	HongKong	Indien	Südkorea	Thailand	Deutschland	Frankreich	Polen	Russland	Schweden	Schweiz	Spanien	Türkei	UK	Australien
		Stadt	Suleja	Johannesbur	Sao Paulo	Montreal	Mexiko City	Los Angeles	New York	Washington	Hong Kong	Chennai	Seoul	Bangkok	Frankfurt	Paris	Warschau	Moskau	Stockholm	Zuerich	Madrid	Istanbul	London	Sydney
Afrika	Nigeria	Suleja	100,00%	98,20%	93,50%	88,78%	91,96%	89,66%	88,97%	94,01%	98,73%	98,72%	91,28%	98,41%	98,96%	92,04%	93,55%	95,54%	93,91%	96,67%	94,50%	99,65%	99,47%	97,52%
Afrika	Südafrika	Johannesbur	98,20%	100,00%	95,27%	90,64%	93,70%	91,50%	90,67%	95,64%	98,92%	98,95%	93,04%	99,30%	98,85%	94,02%	95,27%	96,89%	95,54%	98,06%	96,13%	98,23%	98,64%	99,00%
Amerika	Brasilien	Sao Paulo	93,50%	95,27%	100,00%	95,29%	98,47%	95,80%	95,49%	98,66%	95,28%	95,31%	97,35%	95,43%	94,89%	98,42%	99,00%	97,96%	98,85%	96,81%	98,09%	94,04%	92,88%	94,84%
Amerika	Kanada	Montreal	88,78%	90,64%	95,29%	100,00%	97,28%	99,13%	99,60%	94,99%	89,75%	91,17%	97,03%	91,59%	90,59%	96,40%	95,07%	93,45%	94,65%	92,39%	94,31%	89,35%	84,09%	90,58%
Amerika	Mexiko	Mexiko City	91,96%	93,70%	98,47%	97,28%	100,00%	97,77%	97,16%	97,97%	93,34%	94,02%	99,11%	93,95%	93,42%	99,39%	98,00%	96,42%	97,84%	95,20%	97,15%	92,50%	90,21%	93,85%
Amerika	USA	Los Angeles	89,66%	91,50%	95,80%	99,13%	97,77%	100,00%	98,97%	95,61%	90,60%	91,68%	97,47%	92,13%	91,23%	96,94%	95,53%	94,07%	95,28%	93,07%	94,91%	90,15%	85,52%	91,18%
Amerika	USA	New York	88,97%	90,67%	95,49%	99,60%	97,16%	98,97%	100,00%	94,82%	89,65%	90,98%	97,11%	91,58%	90,64%	96,39%	94,91%	93,38%	94,59%	92,44%	94,31%	89,49%	84,79%	90,55%
Amerika	USA	Washington	94,01%	95,64%	98,66%	94,99%	97,97%	95,61%	94,82%	100,00%	94,75%	94,16%	97,11%	95,41%	94,95%	97,96%	98,41%	98,01%	98,15%	97,06%	97,33%	94,37%	91,77%	95,57%
Asien	HongKong	Hong Kong	98,73%	98,92%	95,28%	89,75%	93,34%	90,60%	89,65%	94,75%	100,00%	99,58%	92,73%	99,34%	99,30%	93,42%	94,71%	96,22%	94,95%	97,36%	95,41%	98,77%	99,11%	98,62%
Asien	Indien	Chennai	98,72%	98,95%	95,31%	91,17%	94,02%	91,68%	90,98%	94,16%	99,58%	100,00%	92,79%	99,36%	99,35%	93,48%	95,06%	96,26%	95,14%	97,46%	95,97%	98,77%	99,05%	98,49%
Asien	Südkorea	Seoul	91,28%	93,04%	97,35%	97,03%	99,11%	97,47%	97,11%	97,11%	92,73%	92,79%	100,00%	93,45%	92,44%	98,55%	97,13%	95,43%	97,09%	94,36%	96,62%	91,66%	88,50%	92,35%
Asien	Thailand	Bangkok	98,41%	99,30%	95,43%	91,59%	93,95%	92,13%	91,58%	95,41%	99,34%	99,36%	93,45%	100,00%	99,12%	94,06%	95,48%	96,47%	95,67%	97,76%	96,37%	98,40%	98,85%	98,86%
Europa	Deutschland	Frankfurt	98,96%	98,85%	94,89%	90,59%	93,42%	91,23%	90,64%	94,95%	99,30%	99,35%	92,44%	99,12%	100,00%	93,48%	94,80%	96,35%	95,16%	97,51%	95,68%	98,98%	99,34%	98,42%
Europa	Frankreich	Paris	92,04%	94,02%	98,42%	96,40%	99,39%	96,94%	96,39%	97,96%	93,42%	93,48%	98,55%	94,06%	93,48%	100,00%	98,23%	96,71%	98,05%	95,58%	97,32%	92,50%	89,01%	93,60%
Europa	Polen	Warschau	93,55%	95,27%	99,00%	95,07%	98,00%	95,53%	94,91%	98,41%	94,71%	95,06%	97,13%	95,48%	94,80%	98,23%	100,00%	97,53%	98,82%	96,38%	98,06%	94,00%	91,10%	94,83%
Europa	Russland	Moskau	95,54%	96,89%	97,96%	93,45%	96,42%	94,07%	93,38%	98,01%	96,22%	96,26%	95,43%	96,47%	96,35%	96,71%	97,53%	100,00%	97,66%	98,39%	96,69%	95,68%	95,38%	96,62%
Europa	Schweden	Stockholm	93,91%	95,54%	98,85%	94,65%	97,84%	95,28%	94,59%	98,15%	94,95%	95,14%	97,09%	95,67%	95,16%	98,05%	98,82%	97,66%	100,00%	96,87%	98,56%	94,24%	91,14%	95,15%
Europa	Schweiz	Zuerich	96,67%	98,06%	96,81%	92,39%	95,20%	93,07%	92,44%	97,06%	97,36%	97,46%	94,36%	97,76%	97,51%	95,58%	96,38%	98,39%	96,87%	100,00%	97,48%	96,80%	96,39%	98,06%
Europa	Spanien	Madrid	94,50%	96,13%	98,09%	94,31%	97,15%	94,91%	94,31%	97,33%	95,41%	95,97%	96,62%	96,37%	95,68%	97,32%	98,06%	96,69%	98,56%	97,48%	100,00%	94,78%	91,13%	95,98%
Europa	Türkei	Istanbul	99,65%	98,23%	94,04%	89,35%	92,50%	90,15%	89,49%	94,37%	98,77%	98,77%	91,66%	98,40%	98,98%	92,50%	94,00%	95,68%	94,24%	96,80%	94,78%	100,00%	99,48%	97,75%
Europa	UK	London	99,47%	98,64%	92,88%	84,09%	90,21%	85,52%	84,79%	91,77%	99,11%	99,05%	88,50%	98,85%	99,34%	89,01%	91,10%	95,38%	91,14%	96,39%	91,13%	99,48%	100,00%	97,89%
Ozeaninen	Australien	Sydney	97,52%	99,00%	94,84%	90,58%	93,85%	91,18%	90,55%	95,57%	98,62%	98,49%	92,35%	98,86%	98,42%	93,60%	94,83%	96,62%	95,15%	98,06%	95,98%	97,75%	97,89%	100,00%

Tabelle 2.11: Verhältnis von sich überschneidenden TLS-Handshakes nach Domains und nach zusätzlich der Domain-Zertifikat-Serialnumber. In grün markiert sind die Felder, die einen gleichen oder höheren Prozentsatz haben als bei der Tabelle 2.10, in rot mit niedrigerem Wert

Bemerkenswerter Weise sind auch hier die Verhältnisse mit mindestens 80% sehr hoch. Allerdings ist die Varianz der Zertifikate hier deutlich größer. So gibt es genauso Verhältnisse, die höher sind als in Tabelle 2.10 und damit größerer Übereinstimmungen als bei den Sub-CAs, als auch deutlich niedrige Verhältnisse. Erstes scheint auf den ersten Blick unlogisch, da ja die Zertifikate der Domänen andere SerialNumbers beinhalten müssten, wenn diese von unterschiedlichen Sub-CAs ausgestellt wurden. Allerdings lässt sich dies damit erklären, dass diese Zertifikate selbst ausgestellt wurden und daher keine Zertifikatskette und somit auch keine (Sub-)CA per TLS-Handshake übergeben.
Zudem lässt sich hier erstmals eine markante regionale Zusammengehörigkeit feststellen: So sind die afrikanischen TLS-Standorte sehr ähnlich und auch die amerikanischen (hier bilden allerdings Sao Paulo, ggf. weil Südamerikanisch, und Washington gewisse Ausnahmen). Auch in Asien sind die Ähnlichkeiten abgesehen von Seoul, welches dafür klare Übereinstimmungen mit den amerikanischen Servern hat, bemerkenswert hoch. Dabei ist die Übereinstimmung mit den afrikanischen VPN-Standorten, sowie denen in Sydney, Istanbul und London extrem hoch. Dies könnte allerdings auch in der generell geringen Menge an erfolgreichen TLS-Handshakes begründet sein bei all diesen Orten.
Sehr schön kann man diese „Regionalität“ bei den europäischen VPN-Server-Standorten erkennen. Hier ist in einem großen Block die Übereinstimmung extrem hoch. Einzig Frankfurt fällt hier aus dem Raster, genauso wie die vorher schon erwähnten London und Istanbul. Festzuhalten sind hier noch die erstaunlich hohen Ergebnisse von Frankreich mit den (nord-)amerikanischen Servern. Zudem weisen die TLS-Handshakes aus Sydney mit fast allen anderen Standorten eine sehr hohe Übereinstimmung auf. Gerade hier sollte bedacht werden, dass die Anzahl an erfolgreichen TLS-Handshakes relativ niedrig war.

2.4.7 Zusammenführung

Zwar weisen die Ergebnisse aus Tabelle 2.11 insgesamt erstaunlich hohe Werte auf, was die Übereinstimmung der Domänen-Zertifikate betrifft, und auch eine gewisse Regionalität ausdrückt. Aber es sollte dabei immer bedacht werden, dass die Ergebnisse schon vorgefiltert sind, ob die Domänen selbst übereinstimmen, und vor allem, dass die Varianz an erfolgreichen TLS-Handshakes enorm ist, wie Tabelle 2.2 deutlich macht.
Dennoch scheint es auch international eine gewisse Einheit an verwendeten Zertifikaten und aktiven (Sub-)CAs zu geben, was ein doch bemerkenswertes Ergebnis ist.

3 Zusammenfassung

Um einen repräsentativen Vergleich von X.509-Zertifikaten von verschiedenen Standorten aus zu gewinnen, wurden die als zu überprüfende Domänen mittels Top-Listen von Alexa und Cisco zusammengetragen. Mittels VPN-Verbindungen und ZMap wurde versucht von verschiedensten Standorten aus mit diesen Domänen TLS-Handshakes durchzuführen. Diese wurden gesammelt und die erfolgreichen TLS-Handshakes zwischen verschiedenen Standorten verglichen. Zunächst nach Domänen, um eine Vergleichbarkeit zwischen den erhaltenen Zertifikatsketten zu schaffen. Diese wurden dann von den CAs bis zu den Server-Zertifikaten verglichen, wobei bemerkenswert hohe Übereinstimmungen festgehalten wurden.

3.1 Bewertung der Ergebnisse

Aus den gesammelten Daten ist klar hervorgegangen, dass die von Domänen verwendeten Zertifikate und damit auch deren Zertifikatsketten und letztendlich auch die signierenden CAs zu einem sehr hohen Teil an verschiedensten Standorten auf der Welt übereinstimmen. Zwar gibt es hinsichtlich Domänen-Zertifikate durchaus mehr Verschiedenheiten zwischen den genutzten VPN-Standorten als bei den (Sub-)CA-Zertifikaten, aber selbst hier sind die Werte mit oftmals 90% Übereinstimmung sehr hoch. Dies lässt, insbesondere wenn man die stärkeren Ähnlichkeiten nach Regionen wie Europa oder (Nord-)Amerika mit einbezieht, darauf schließen, dass zumindest ein nicht unbedeutender Teil von Domänen mehrere Zertifikate für TLS-Verbindungen nutzt, je nachdem wo die Verbindung aufgebaut wird und damit möglicher Weise andere (geographisch lokale) Server anspricht. Dennoch werden hier scheinbar oft die gleichen (Sub-)CA-Zertifikate genutzt, was für eine absichtliche Unterteilung seitens der Domänen-Betreiber spricht.
Man sollte aber bei der Bewertung und Analyse bedenken, dass die Anzahl der Domänen, mit denen ein erfolgreicher TLS-Handshake durchgeführt und somit dessen Zertifikate/-sketten gesammelt wurden, sehr stark nach den VPN-Standorten variieren. So bilden zwar insbesondere die Standorte in Nordamerika mit 900.000 bis 1.100.000 und die Standorte in Europa mit

600.000 bis 800.000 gesammelten TLS-Handshakes von ca. 1.700.000 verschiedenen Domänen eine gute Basis zum Vergleichen, aber die Standorte in Afrika, Asien, sowie aus Brasilien, der Türkei, Großbritanien und Australien mit oftmals nur 200.000 bis 300.000 gesammelten Daten bieten nur eine sehr kleine Menge für Vergleiche. Diese Vergleiche sollten daher mit Vorsicht behandelt werden.
Allerdings zeigen sich sogar hier bei den „schwächeren“ VPN-Standorten je nach Region Übereinstimmungen bei den erfolgreich angesprochenen Domänen, wie Ergebnissen für Afrika (Tabelle 2.3), oder sie sind in der großen Ergebnis-Mengen aus Amerika und Europa enthalten (siehe Tabelle 2.5). Generell zeigt sich an den Standorten in Amerika und Europa, dass hier die Überschneidung der Domänen auch im Hinblick auf die große Zahl der erfolgreichen TLS-Handshakes sehr groß ist. Dies lässt insbesondere bei den (Verhältnissen zwischen den) Ergebnissen von Montreal, Los Angeles und New York (siehe Tabelle 2.4) darauf schließen, dass sich hier der Grenze bzw. Anzahl an Domänen, die überhaupt eine TLS-Verbindung ermöglichen, stark angenähert wurde.

3.2 Ausblick und weiterführende Arbeit

Bedenkt man die schon bekannt gewordene Ausnutzung der Public Key Infrastructure durch kompromittierte bzw. missbrauchte Sub-CAs [34], stellen die Ergebnisse einen interessanten Gewinn dar: Da die Überschneidung von Zertifikaten der Domänen und insbesondere der Sub-CAs so extrem ist auch im Vergleich von verschiedensten Standorten, können Internet-Nutzer ihre Liste an vertrauenswürdigen CAs deutlich restriktiver auslegen und diese sogar mehr auf Sub-CAs einschränken. Dies kann gerade dann hilfreich sein, wenn eine Reise bevorsteht oder man einem Netzwerk bzw. dem genutzten Internet-Zugang misstraut. So können für persönlich sicherheitsrelevante Websites die Sub-CAs genauer ausgewählt werden. Dies setzt allerdings voraus, dass eine als sicher eingestufte Verbindung zu diesen schon besteht bzw. genutzt wurde und so die relevanten (SubCA-)Zertifikate überhaupt identifiziert werden können.

Allerdings ist es gerade in dieser Hinsicht schaden, dass mit der VPN-Verbindung in Länder, die von Zensuren oder Unsicherheiten bedroht sind, wie bspw. die Türkei, Russland oder Hongkong [6][12][13][23][42] keine großen Mengen an erfolgreichen TLS-Handshakes gesammelt werden konnten. Hier ist zum einen interessant, wo der Grund liegt, dass so eine geringe Anzahl an Domänen gesammelt wurde. Dies kann zum einen an möglichen Zensuren bzw. Restriktionen seitens der Internet Provider dort, fehlenden Angeboten seitens der Domänen(-Betreibern) oder an der Stabilität/Leistung der VPN-Verbindung selber liegen. Daher wäre es interessant,

diese TLS-Scans mittels anderer Methoden bspw. durch eine persönliche Anwesenheit dort oder durch virtuelle Rechner in Servern in diesen Ländern. Ähnliche Scans mithilfe von anderen Methoden wären daher sinnvolle Ergänzungen zu dieser Arbeit, um einen genaueren Einblick in diesen Aspekt zu gewinnen.
Ebenso wäre es interessant, jeweils die gesamten IPv4- oder gar IPv6-Adress-Räume zu analysieren, denn die in dieser Arbeit abgefragten Domänen sind international relevant, weshalb sie überhaupt in den Top-Listen von Alexa und Cisco enthalten sind. Es stellt sich daher die Frage, ob andere angesprochene Adressen auch international erreichbar sind und ob auch hier die Übereinstimmungen der Zertifikate und CAs erhalten bleiben.

Grundsätzlich werden durch die Ergebnisse dieser Arbeit eine stärkere Restriktion der (Sub-)CAs bzw. derer Zertifikate, die als vertrauenswürdig behandelt werden, bestärkt. Dies fordert allerdings, so wie das PKI aufgebaut ist und der gemeine Umgang mit den vertrauenswürdigen Zertifikatslisten ist [15][38] bzw. deren große Mengen an standardmäßig beinhalteten Zertifikaten, ein hohes Engagement und auf Eigeninitiative beruhendes Verhalten bzw. Arbeit seitens der Nutzer. Diese werden allerdings selten ohne direkte bzw. sichtbare Gefahr diesen Aufwand betreiben. Dabei ist es nach den Ergebnissen dieser Analyse offensichtlich sinnvoll, um sich vor Man-in-the-Middle-Angriffen zu schützen, da sich die Zertifikate nicht nach Lokalität ändern. Wenn eine Sicherheit gegenüber Man-in-the-Middle-Angriffe ohne solch einen persönlichen Aufwand gefordert ist, könnte bspw. Crossbear genutzt werden. Dies ist eine Anwendung, die analog zu dieser Arbeit mehrere TLS-Handshakes über verschiedene Wege mit einem gewünschten Server bzw. Domäne durchführt und die Zertifikate dann vergleicht. Die Anwendung macht sich dabei den Gedanken zu nutze, dass bei dem MitM-Angriff der Angreifer sich zwischen Client und Server befindet und somit über andere Wege umgangen werden kann. Somit müssen die Zertifikate von verschiedenen Verbindungswegen verglichen werden. Sind diese unterschiedlich, so besteht die Gefahr eines MitM-Angriffs. [19] Eben diese Analyse bzw. dieser Rückschluss von der Übereinstimmung der Zertifikate auf die Authentizität unterstützt das Ergebnis dieser Arbeit.

Somit beantwortet sich auch die zu Beginn der Arbeit gestellten Frage, dass sich die Zertifikate an unterschiedlichen überschneiden und sich dieser Umstand zu nutze gemacht werden kann, um Man-in-the-Middle-Angriffe auf das TLS-Protokoll zu verhindern, indem bspw. dynamisch auf andere Wege erfasste Zertifikate für einen Ziel-Server auf Übereinstimmung überprüft werden oder vor Reisen bzw. Nutzung von potenziell unsicheren Netzwerk-Zugängen die vertrauenswürdigen Zertifikate deutlich strenger nach eigenen Bedürfnissen ausgewählt werden.

Literaturverzeichnis

[1] alexa. (2020). About Us, Adresse: https://www.alexa.com/about (besucht am 24. 05. 2020).

[2] M. Alicherry und A. D. Keromytis, „Doublecheck: Multi-path verification against man-in-the-middle attacks," in *2009 IEEE Symposium on Computers and Communications*, IEEE, 2009, S. 557–563.

[3] amazon. (2019). Globale Infrastruktur, Adresse: https://aws.amazon.com/de/about-aws/global-infrastructure/ (besucht am 05. 01. 2020).

[4] ——, (2020). Alexa Top Sites, Adresse: https://aws.amazon.com/de/alexa-top-sites/ (besucht am 24. 05. 2020).

[5] aws. (Sep. 2016). AWS Acceptable Use Policy, Adresse: https://d1.awsstatic.com/legal/acceptable-use-policy/ACCEPTABLE%20USE%20POLICY_de.pdf (besucht am 05. 01. 2020).

[6] S. Bigalke, *Russland will sich vom globalen Internet abkoppeln*, Süddeutsche Zeitung, 11. Apr. 2019. Adresse: https://www.sueddeutsche.de/digital/russland-internet-zensur-abschottung-telegram-opposition-ueberwachung-1.4404609 (besucht am 02. 02. 2020).

[7] R. Bless, S. Mink, E.-O. Blaß, M. Conrad, H.-J. Hof, K. Kutzner und M. Schöller, *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen*. Springer-Verlag, 2006.

[8] J. Cody, D. Adrian, R. Stradling, J. Rudenberg und Z. Durumeric. (2020). ZGrab2, Adresse: https://github.com/zmap/zgrab2 (besucht am 23. 05. 2020).

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. T. Polk u. a., „Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.," *RFC*, Jg. 5280, S. 1–151, 2008.

[10] M. Cotton, L. Vegoda, R. Bonica und B. Haberman, „Special-purpose IP address registries," *IETF, April*, S. 2070–1721, 2013.

[11] CyberGhost. (2020). AGB, Adresse: https://www.cyberghostvpn.com/de_DE/agbs (besucht am 25. 05. 2020).

[12] L. Deuber, *Peking verteidigt restriktives Vorgehen in Hongkong*, S. Zeitung, Hrsg., Mai 2020. Adresse: https://www.sueddeutsche.de/politik/china-hongkong-sicherheitsgesetze-1.4916076 (besucht am 26. 05. 2020).

[13] dpa, *Internet in Russland nun unter Staatskontrolle*, Süddeutsche Zeitung, 1. Nov. 2019. Adresse: https://www.sueddeutsche.de/service/internet-internet-in-russland-nun-unter-staatskontrolle-dpa.urn-newsml-dpa-com-20090101-191101-99-535980 (besucht am 02. 02. 2020).

[14] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey und J. A. Halderman, „A search engine backed by Internet-wide scanning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, S. 542–553.

[15] Z. Durumeric, J. Kasten, M. Bailey und J. A. Halderman, „Analysis of the HTTPS certificate ecosystem," in *Proceedings of the 2013 conference on Internet measurement conference*, 2013, S. 291–304.

[16] Z. Durumeric, E. Wustrow und J. A. Halderman, „ZMap: Fast Internet-wide scanning and its security applications," in *Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13)*, 2013, S. 605–620.

[17] EU. (2020). Länder, Adresse: https://europa.eu/european-union/about-eu/countries_de (besucht am 25. 05. 2020).

[18] P. Ferguson und G. Huston, *What is a VPN?* Revision, 1998.

[19] R. Holz, T. Riedmaier, N. Kammenhuber und G. Carle, „X. 509 forensics: Detecting and localising the SSL/TLS men-in-the-middle," in *european symposium on research in computer security*, Springer, 2012, S. 217–234.

[20] L. S. Huang, A. Rice, E. Ellingsen und C. Jackson, „Analyzing forged SSL certificates in the wild," in *2014 IEEE Symposium on Security and Privacy*, IEEE, 2014, S. 83–97.

[21] IP2Location. (2020). Identify Geographical Location by IP Address, Adresse: https://www.ip2location.com/ (besucht am 25. 05. 2020).

[22] M. Kappes, *Netzwerk-und Datensicherheit: eine praktische Einführung*. Springer, 2007.

[23] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich und N. Vallina-Rodriguez, „An empirical analysis of the commercial vpn ecosystem," in *Proceedings of the Internet Measurement Conference 2018*, 2018, S. 443–456.

[24] O. Lystrup, *Cisco Umbrella releases free top 1 million sites list*, 2016. Adresse: https://umbrella.cisco.com/blog/cisco-umbrella-1-million (besucht am 23. 05. 2020).

[25] NordVPN. (Aug. 2019). Terms of Service, Adresse: https://nordvpn.com/terms-of-service/ (besucht am 25. 05. 2020).

[26] R. Oppliger, R. Hauser und D. Basin, „SSL/TLS session-aware user authentication–Or how to effectively thwart the man-in-the-middle,“ *Computer Communications*, Jg. 29, Nr. 12, S. 2238–2246, 2006.

[27] ProtonVPN. (Dez. 2019). Terms and Conditions of Service, Adresse: https://protonvpn.com/terms-and-conditions (besucht am 25. 05. 2020).

[28] PureVPN. (Juni 2019). Difference Between TCP and UDP Internet Protocols, Adresse: https://support.purevpn.com/difference-between-tcp-and-udp (besucht am 25. 05. 2020).

[29] ——, (Apr. 2020). PureVPN Servers List/Hostnames, Adresse: https://support.purevpn.com/vpn-servers (besucht am 25. 05. 2020).

[30] ——, (Apr. 2020). Setup PureVPN App on Linux, Adresse: https://support.purevpn.com/article-categories/getting-started/linux (besucht am 25. 05. 2020).

[31] ——, (2020). Setup PureVPN App on Linux, Adresse: OpenVPN%20-%20Open%20Source%20VPN%20Protokoll (besucht am 25. 05. 2020).

[32] E. Rescorla und T. Dierks, „The transport layer security (TLS) protocol version 1.3,“ 2018.

[33] I. Ristic, *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. Feisty Duck, 2013.

[34] S. B. Roosa und S. Schultze, „Trust darknet: Control and compromise in the internet's certificate authority model,“ *IEEE Internet Computing*, Jg. 17, Nr. 3, S. 18–25, 2013.

[35] S. E. Schechter, R. Dhamija, A. Ozment und I. Fischer, „The emperor's new security indicators,“ in *2007 IEEE Symposium on Security and Privacy (SP'07)*, IEEE, 2007, S. 51–65.

[36] B. für Sicherheit in der Informationstechnik (BSI), „Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen,“ *Report, Bundesamt für Sicherheit in der Informationstechnik (BSI)*, 2020.

[37] J. Sobey, R. Biddle, P. C. Van Oorschot und A. S. Patrick, „Exploring user reactions to new browser cues for extended validation certificates,“ in *European Symposium on Research in Computer Security*, Springer, 2008, S. 411–427.

[38] C. Soghoian und S. Stamm, „Certified lies: Detecting and defeating government interception attacks against SSL,“ in *Proceedings of ACM Symposium on Operating Systems Principles*, 2010, S. 1–18.

[39] R. N. Staff, „Ripe atlas: A global internet measurement network,“ *Internet Protocol Journal*, Jg. 18, Nr. 3, 2015.

[40] I. Support. (Juni 2018). Connection reset by peer: socket write errorërror message, Adresse: https://www.ibm.com/support/pages/connection-reset-peer-socket-write-error-error-message (besucht am 25. 05. 2020).

[41] C. Umbrella. (2020). Cloud network activity, Adresse: https://umbrella.cisco.com/why-umbrella/global-network-and-traffic (besucht am 24. 05. 2020).

[42] X. Xu, Z. M. Mao und J. A. Halderman, „Internet censorship in China: Where does the filtering occur?“ In *International Conference on Passive and Active Network Measurement*, Springer, 2011, S. 133–142.

Abbildungsverzeichnis

Tabellenverzeichnis