**HOCHSCHULE für Angewandte Wissenschaften LANDSHUT**

**UNIVERSITY of Applied Sciences**

**FAKULTÄT Informatik**

**HOCHSCHULE LANDSHUT**

FAKULTÄT INFORMATIK

**Echtzeitbasierte Netzwerkdatenanalyse zur Ermittlung verwendeter Root Zertifikate**

**Masterarbeit**

vorgelegt von

**Sebastian Bilda**

aus Landshut

eingereicht am: .......................

Betreuer: Johann Uhrmann

# Erklärung zur Masterarbeit

Name, Vorname   
der/des Studierenden: …………………………………………….

Hiermit erkläre ich, dass ich die Arbeit selbständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Landshut, den ……………. …..………………………………….  
 (Unterschrift der/des Studierenden)

Abstract

Inhaltsverzeichnis

[Erklärung zur Masterarbeit - 4 -](#_Toc66520168)

[Abstract - 6 -](#_Toc66520169)

[Inhaltsverzeichnis - 7 -](#_Toc66520170)

[1 Einleitung - 8 -](#_Toc66520171)

[1.1 Problemstellung und Motivation - 8 -](#_Toc66520172)

[1.2 Zielsetzung - 10 -](#_Toc66520173)

[2 Grundlagen - 11 -](#_Toc66520174)

[2.1 Public Key Infrastructure - 11 -](#_Toc66520175)

[2.2 Zertifizierungsstellen - 11 -](#_Toc66520176)

[2.3 Digitale Zertifikate - 13 -](#_Toc66520177)

[2.3.1 X.509 Zertifikate - 13 -](#_Toc66520178)

[2.3.2 Format und Semantik von Zertifikaten - 14 -](#_Toc66520179)

[2.3.3 Zertifikats Revokation Listen (CRL) - 15 -](#_Toc66520180)

[2.4 Transport Layer Security - 15 -](#_Toc66520181)

[2.4.1 TLS Handshake - 15 -](#_Toc66520182)

[2.4.2 TLS Record - 16 -](#_Toc66520183)

[2.5 Windows Certificate Trust Store - 16 -](#_Toc66520184)

[3 Hauptteil - 18 -](#_Toc66520185)

[3.1 Stand der Forschung - 18 -](#_Toc66520186)

[3.2 Methodik/Vorgehensweise - 19 -](#_Toc66520187)

[3.3 Implementierung - 22 -](#_Toc66520188)

[3.3.1 Anforderungsanalyse - 22 -](#_Toc66520189)

[3.3.2 Aufbau und Struktur - 22 -](#_Toc66520190)

[3.3.3 Probleme bei der Implementierung? - 23 -](#_Toc66520191)

[3.4 Ergebnisse - 23 -](#_Toc66520192)

[4 Fazit - 27 -](#_Toc66520193)

[4.1 Zusammenfassung - 27 -](#_Toc66520194)

[4.2 Reflexion - 27 -](#_Toc66520195)

[4.3 Ausblick - 27 -](#_Toc66520196)

[Literaturverzeichnis - 28 -](#_Toc66520197)

[Abbildungsverzeichnis - 29 -](#_Toc66520198)

[Listingverzeichnis - 30 -](#_Toc66520199)

[Anhang - 31 -](#_Toc66520200)

# Einleitung

## Problemstellung und Motivation

Jede Person muss sich selbst mittels eines Personalausweises identifizieren können. So eine ähnliche Funktion besitzen digitale Zertifikate in der Online-Welt. Die Authentizität des Kommunikationspartners wird mit einer Prüfung seines Zertifikats sichergestellt. Diese Zertifikate werden von Zertifizierungsstellen (CAs) ausgestellt, denen der Nutzer (Client, Browser, Betriebssystem) vertraut. Zertifikate sind aus dem Internet nicht mehr wegzudenken. Sie erhöhen die Sicherheit beim „surfen“, identifizieren ihren Besitzer, enthalten allgemeine Informationen über diesen und von größter Bedeutung, sie ermöglichen es zusammen mit der Public Key Infrastruktur (PKI), Informationen im WWW sicher und verschlüsselt zu übertragen. Verschlüsselte Verbindungen werden in der Regel durch TLS-basierte Authentifizierung von mindestens einem Kommunikationspartner abgesichert. Die Zertifikate werden von sogenannten Zertifizierungsstellen (Root Certificate Authority) ausgestellt, denen jeder Browser und jedes System „vertraut“. Aus jüngsten Ereignissen, ist jedoch bekannt, dass ein Unternehmen, dass auch eine TLS-Zertifizierungsstelle betreibt, im staatlichen Auftrag Menschenrechtsaktivisten durch Sicherheitslücken angreift.

Somit kann aus diesem Zusammenhang die Menge an vordefinierten Zertifizierungsstellen in Systemen oder Browsern in Frage gestellt werden. An dem Beispiel von dem Unternehmen Dark Matter kann das Problem spezifiziert werden, dass durch eine Phishing Mail auf eine Website leitet auf der Malicious Code heruntergeladen wird, diese Website wurde zum Beispiel von einer CA signiert die mit Hackingaktivitäten in Verbindung steht, d. h. mein System vertraut dieser Website und keine Meldung über die Sicherheit ihrer Daten kommt. Zusätzlich können MiM-Angriffe leichter vorgenommen werden, und der Angreifer kann die gesamte Kommunikation mitlesen.

Es gibt verschiedene Ansätze diesem Problem entgegenzuwirken. Zum einen eine Initiative von Google namens Certificate Transparenzy, die durch eine zusätzliche öffentliche Instanz, auf der alle neu registrierten Zertifkate in einem kryptografischen Verfahren gespeichert sind, um ein erneutes Ausstellen eines Zertifikates für eine Domain zu verhindern. Dieses Verfahren wird im Abschnitt Stand der Forschung nochmal genauer erklärt. Zum anderen gibt es die Möglichkeit über den CAA Record die Zertifkate genauer zu überprüfen.

Oder, was in dieser Masterarbeit untersucht werden soll, man versucht durch eine Einschränkung der Zertifizierungsstellen das Surfen im Internet noch sicherer zu machen.

Es gibt derzeit keinen etablierten Mechanismus, um dieses Vertrauen feingranularer zu konfigurieren oder überhaupt zu verifizieren, ob dieses Vertrauen notwendig bzw. gerechtfertigt ist. Natürlich ist es möglich diese Liste manuell anzupassen, jedoch bringt dies viel Aufwand mit sich und nach welchen Kriterien werden die Zertifizierungsstellen bewertet? Jede Person muss sich selbst mittels eines Personalausweises identifizieren können. So eine ähnliche Funktion besitzen digitale Zertifikate in der Online-Welt. Die Authentizität des Kommunikationspartners wird mit einer Prüfung seines Zertifikats sichergestellt. Diese Zertifikate werden von Zertifizierungsstellen (CAs) ausgestellt, denen der Nutzer (Client, Browser, Betriebssystem) vertraut. Zertifikate sind aus dem Internet nicht mehr wegzudenken. Sie erhöhen die Sicherheit beim „surfen“, identifizieren ihren Besitzer, enthalten allgemeine Informationen über diesen und von größter Bedeutung, sie ermöglichen es zusammen mit der Public Key Infrastruktur (PKI), Informationen im WWW sicher und verschlüsselt zu übertragen. Verschlüsselte Verbindungen werden in der Regel durch TLS-basierte Authentifizierung von mindestens einem Kommunikationspartner abgesichert. Die Zertifikate werden von sogenannten Zertifizierungsstellen (Root Certificate Authority) ausgestellt, denen jeder Browser und jedes System „vertraut“. Aus jüngsten Ereignissen, ist jedoch bekannt, dass ein Unternehmen, dass auch eine TLS-Zertifizierungsstelle betreibt, im staatlichen Auftrag Menschenrechtsaktivisten durch Sicherheitslücken angreift.

Somit kann aus diesem Zusammenhang die Menge an vordefinierten Zertifizierungsstellen in Systemen oder Browsern in Frage gestellt werden. An dem Beispiel von dem Unternehmen Dark Matter kann das Problem spezifiziert werden, dass durch eine Phishing Mail auf eine Website leitet auf der Malicious Code heruntergeladen wird, diese Website wurde zum Beispiel von einer CA signiert die mit Hackingaktivitäten in Verbindung steht, d. h. mein System vertraut dieser Website und keine Meldung über die Sicherheit ihrer Daten kommt. Zusätzlich können MiM-Angriffe leichter vorgenommen werden, und der Angreifer kann die gesamte Kommunikation mitlesen.

Mißbrauch mit ca certificaten

<https://resources.sei.cmu.edu/asset_files/WhitePaper/2001_019_001_496192.pdf>

Beschreibung eines Vorfalls bei dem VeriSign signierte Zertifikate an unberechtigte Personen ausgestellt hat die sich als Microsoft Mitarbeiter ausgegeben haben und somit Programmcode damit signieren konnten, um diesen dann unter Windows ohne Probleme auszuführen.

Oder, was in dieser Masterarbeit untersucht werden soll, man versucht durch eine Einschränkung der Zertifizierungsstellen das Surfen im Internet noch sicherer zu machen.

Es gibt derzeit keinen etablierten Mechanismus, um dieses Vertrauen feingranularer zu konfigurieren oder überhaupt zu verifizieren, ob dieses Vertrauen notwendig bzw. gerechtfertigt ist. Natürlich ist es möglich diese Liste manuell anzupassen, jedoch bringt dies viel Aufwand mit sich und nach welchen Kriterien werden die Zertifizierungsstellen bewertet?

## Zielsetzung

Aufgrund der oben genannten Problemstellung soll deshalb hier ein Analyse Werkzeug programmiert werden, das anhand von einem Netzwerkverkehr Mitschnitt diese Zertifizierungsstellen extrahiert und dann in den jeweiligen Systemen automatisiert angepasst wird. Des Weiteren soll anhand der Netzwerkverkehrs Auswertungen erstellt werden, die die Anzahl der ausgestellten Zertifikate einer Certificate Authorities (CA) graphisch darstellt. Auf welche Zeit konvergiert die Anzahl der tatsächlich verwendeten CA’s? Auswertung der Häufigkeit einer CA in Bezug auf einen Haushalt. Auswertung welche CA’s verwendet werden. Diese Statistiken sollen eine Basis dafür bilden, um die Anzahl der Zertifizierungsstellen in den Systemen einzuschränken.

# Grundlagen

In diesem Kapitel sollen die Grundlagen für das Verständnis der Arbeit beschrieben werden und die Schlüsselbegriffe definiert. Wie in der Zielsetzung oben beschrieben geht es um Netzwerke, dem SSL/TLS Protokoll, digitale Zertifikate und Zertifizierungsstellen. Diese Themengebiete sollen nun grundlegend erläutert werden.

Vorerst soll geklärt werden was eine PKI (Public Key Infrastructure) ist und wofür diese da ist. Weitergehend werden Zertifikate, Arten von Zertifikaten und deren Aufbau und Inhalt erläutert.

## Public Key Infrastructure

Eine Public Key Infrastructure (PKI) oder auf Deutsch übersetzt – *Infrastruktur für öffentliche Schlüssel* – ist "das gesamte Konstrukt rund um die Absicherung der Datenkommunikation und die Identitätskontrolle im Netzwerk mithilfe von Zertifikaten". [[6]](#_CTVL001db152e864b5f482587a8c80e6c73c7c7) Mit Hilfe einer PKI wird die Sicherheit der Kommunikation durch Authentifizierung, Datenverschlüsselung und digitale Signaturen erhöht. Grundsätzlich beruhen die Dienste einer PKI auf der ordnungsgemäßen Verwendung von öffentlichen/privaten Schlüsselpaaren. Die öffentliche Komponente dieses Schlüsselpaars wird in Form eines Public-Key-Zertifikats ausgestellt und kann in Verbindung mit dem entsprechenden Algorithmus zur Verifizierung einer digitalen Signatur, zur Verschlüsselung von Daten oder zu beidem verwendet werden. [[2]](#_CTVL00153b2fcd3a0084b6c938e85d9d05fb933)

## Zertifizierungsstellen

Zertifizierungsstellen stellen digitale Zertifikate aus, mit denen sichere Client – Server Verbindungen hergestellt werden können. Sie sind die Basis der Vertrauenshierachie im Internet. In einem Jahr werden Millionen von digitalen Zertifikaten ausgestellt und dazu verwendet sicher über das Internet zu kommunizieren sowie die zu übermittelten Daten zu verschlüsseln [[5]](#_CTVL0011c37d5f5ef394e4e9b513cfc2256b9eb). Digitale Zertifikate werden im Einzelnen im Abschnitt 2.3 näher erläutert. Neben dem Ausstellen von Zertifikaten hat eine Zertifizierungsstelle vorher die Aufgabe den Antragssteller zu überprüfen ob dieser berechtigt ist und die Inhalte unversehrt sind. Abhängig davon stellt die CA (Certificate Authority) das Zertifikat aus oder lehnt es ab. Bei Ausstellung wird das auszustellende Zertifikat von der CA mit deren privaten Schlüssel signiert, um es vor Manipulation zu schützen. Zum anderen ist sie dafür zuständig Zertifikatssperrlisten zu erstellen, welche den Client ermöglicht die Gültigkeit eines Zertifikats festzustellen. Die Sperrlisten werden ebenfalls digital signiert damit eine Manipulation ausgeschlossen werden kann [[6]](#_CTVL001db152e864b5f482587a8c80e6c73c7c7).

## Digitale Zertifikate

Beginnen möchte ich mit dem Begriff Zertifikat, der nach Peter Kleop folgendermaßen definiert ist:

“Ein digitales Zertifikat bindet einen öffentlichen Schlüssel an eine Entität (Benutzer, Organisation, Computer) und beinhaltet zusätzliche Informationen, wie Sperrlisteninformationen und vieles mehr." [[6]](#_CTVL001db152e864b5f482587a8c80e6c73c7c7)

Digitale Zertifikate sind ein Teil des Fundaments der IT-Sicherheit. Durch sie werden Public-Key-Infrastrukturen realisiert [[3]](#_CTVL001c7a0e911136a4948ba26a11b5b4b369f). Im Folgenden soll, der am häufigsten verwendeten Standard für Zertifikate beschrieben und technisch erläutert werden.

### X.509 Zertifikate

Ein X.509 Public-Key-Zertifikat ist eine Datenstruktur, welche die Bindung zwischen einem öffentlichen Schlüssel und einer Entität darstellt. Die Entität ist der Besitzer des Schlüsselpaars. Die Entität kann z.B. eine Person, ein Client-System oder ein Internet Server sein. Ein X.509-Zertifikat ist hierarchisch in einer Baumstruktur aufgebaut. Der Aufbau wird in einem ASN.1- Modul [X.680] beschrieben. ASN.1 ist eine abstrakte Beschreibungssprache für Datenstrukturen, die zunächst unabhängig von deren konkreter Darstellung ist. Ein spezifisches ASN.1-Modul definiert den syntaktischen Aufbau von Datenstrukturen auf Basis der vordefinierten Datentypen. Für X.509 Zertifikate, Sperrlisten und OCSP-Antworten kommen die Distinguished Encoding Rules (DER) zur Anwendung, welche eindeutig festlegen, wie die Inhalte der in den ASN.1 Strukturen definierten Felder binär zu kodieren sind. Die DER Kodierung ist eine sogenannte Tag-Length-Value (TLV) Kodierung, in der jedes Feld im jeweiligen Kontext durch einen Tag-Wert identifiziert wird, gefolgt von einem Feld welches die Länge seines Wertes enthält, auf welches der Wert selbst folgt. Dabei existieren sogenannte „constructed“ Felder, bei denen der Value wiederum TLV Strukturen enthalten kann. (<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf?__blob=publicationFile&v=4>)

### Format und Semantik von Zertifikaten

Die Datenstruktur eines Zertifikates wird in Abbildung 1: Zertifikat Datenstruktur dargestellt.

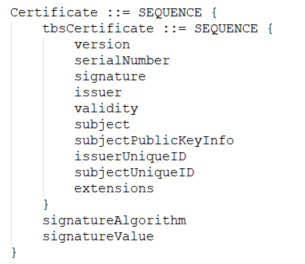


Abbildung : Zertifikat Datenstruktur (https://tools.ietf.org/html/rfc5280)

Ein Zertifikat besitz als oberste ebene also einmal das Feld *tbsCertificate*, welches die Namen Antragstellers und des Antragaustellers enthalten sowie einen öffentlichen Schlüssel, eine Zeitperiode der Gültigkeit und noch weitere Informationen. Das *signatureAlgorithm* Feld beinhaltet den kryptographischen Algorithmus, der von der jeweiligen Zertifizierungsstelle zum Signieren des Zertifikats verwendet wurde. Der *signatureValue* enthält die konkrete digitale Signatur der Zertifizierungsstelle. Mit dieser werden die Informationen des *tbsCertificate* Feldes valide. Die CA bestätigt die Verbindung zwischen öffentlichem Schlüsselmaterial und dem Besitzer des Zertifikats [[10]](#_CTVL001d5c79b06c57248eba60a0476eec9d243).

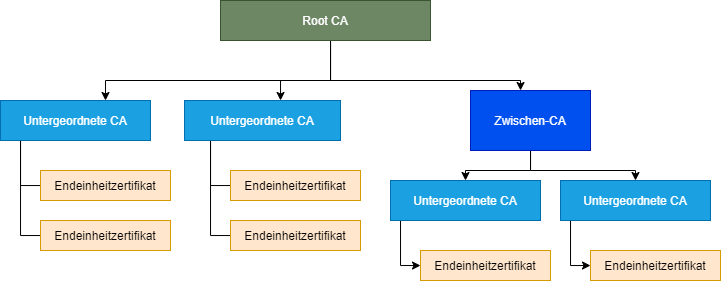
Nun die einzelnen Zertifikatsfelder:

* version
* serialNumber
* signature
* issuer
* validity
* subject
* subjectPublicKeyInfo
* issuerUniqueID
* subjectUniqueID
* extensions -> Typen, Verwendungszweck!!

### Zertifikats Revokation Listen (CRL)

### Zertifikatsketten

Hierarchie der Zertifizierungsstellen [[5]](#_CTVL00113970a7232cc4c8daaca9ca2c215bc1f):



Was bedeuten die einzelnen und wofür sind diese da?

**Root CA**: Höchste Hierarchieebende, dient als Vertrauensanker. Nur wenn das Entity Certificate mit einem Root CA Certificate verkettet ist und dieses Root CA im Betriebssystem oder Browser eingebettet ist, ist es vertrauenswürdig.

**Untergeordnete CAs**: Zwischen Root und Endeinheitszertifikat, Unterscheidung der Zertifikatstypen **Verweis auf kapitel Zertifikate -> extensions/Typen** (SSL/TLS- und S/MIME-CAs). Standortabhängig, Schlüsselabhängig (RSA/ECC).

**Endeinheitszertifikat**: Zertifikate auf Servern, Computern, kryptographischer Hardware und Geräten installiert (z. B. SSL/TLS für Server, Code Signing, Clientzertifkate, digitale Signatur, Authentifizierung.

Bild von einer Kette gezeigt im Firefox zur Verdeutlichung.

## Transport Layer Security

TLS (Transport Layer Security) ist der Nachfolger von SSL (Secure Sockets Layer), dabei handelt es sich um einen Standard. In der aktuellen Version 1.3 hat TLS das primäre Ziel eine Verbindung zwischen zwei kommunizierenden Anwendungen zu gewährleisten. Die einzige Anforderung an die darunterliegende Transportschicht ist ein zuverlässiger, ordnungsgemäßer Datenstrom. Grundsätzlich besteht TLS aus zwei Komponenten [[11]](#_CTVL0011a0cbc393be1440db94f8c9466880599):

* TLS Handshake Protocol (2.4.1)
* TLS Record Protocol (2.4.2)

TLS ist unabhängig vom Anwendungsprotokoll, d. h. die Protokolle höherer Ebenen können transparent darauf aufsetzten, zum Beispiel HTTP das TLS verwendet wird zu HTTPS. Der Standard beschreib nicht wie die höheren Protokolle die Sicherheit mit TLS hinzufügen oder der TLS-Handshake zu initiieren ist [[11]](#_CTVL0011a0cbc393be1440db94f8c9466880599).

### TLS Handshake

Der TLS Handshake ist der Start zum Schlüsselaustausch und ab dann wird verschlüsselt zwischen den beiden Parteien kommuniziert.

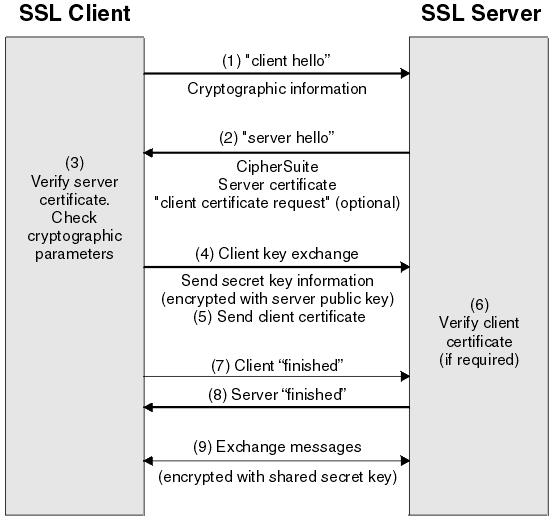


Abbildung : TLS Hanshake.jpg [[1]](#_CTVL001580143ecd2134301baf4e216f79fc6b3)

### TLS Record

## Windows Certificate Trust Store

Der Windows Zertifikatsspeicher kann über die Zertifkatsverwaltung aufgerufen werden und dient zur Auflistung der Vertrauenswürdigen und nicht vertrauenswürdigen Zertifikate. Wie aber Tom Aafloen in einem Blogbeitrag von Microsoft Security Solutions [[7]](#_CTVL0017c99aedcbcf44a1393d3676581811584) beschreibt wird in der Zertifikatsverwaltung von Windows nur ein Teil der Zertifikate angezeigt, denen der User auch vertraut. Anhand eines Beispiels, bei der er eine Website aufruft die aktuelle Jobs in Hong Kong zeigt, verdeutlicht er, dass falls eine Website von einer CA signiert wurde, die nicht in der lokalen Zertifikatsverwaltung enthalten ist, wird eine Verbindung zu Windows Update hergestellt, um zu prüfen ob es dort aufgeführt ist. Ist dies der Fall wird es dem lokalen Speicher hinzugefügt. Aafloen betont am Ende seines Beitrages, er wisse nicht, ob das „Verstecken“ der vertrauenswürdigen CA’s den Benutzern nicht einen falschen Eindruck über die Sicherheit oder Kontrolle gibt.

Es sollte zumindest jedem absolut klar sein, dass das, was in der Oberfläche der Zertifikatsverwaltung nur eine Teilmenge aller Zertifikate ist.

Ist es dann überhaupt möglich die Zertifikate über die Zertifikatsverwaltung feingranularer zu definieren, wenn der Abgleich mit einer Onlinedatenbank die Gültigkeit von Zertifikaten verifiziert?

# Hauptteil

Im ersten Abschnitt dieses Kapitels wird der Stand der Forschung erläutert, welche Möglichkeiten in Frage kommen können, um das Vertrauen in die Zertifizierungsstellen nicht völlig in deren Hände zu legen.

## Stand der Forschung

Google’s Certificate Transperancy (CT) eine gute Alternative die Sicherheit basierend auf HTTPS und dem SSL/TLS Protokoll zu erhöhen. Der grundlegende Ansatz ist, dass jedes Ausgestellte Zertifikate an einen öffentlich zugänglichen Logserver gesendet wird, der die Zertifikate in einer Merkle-Baum-Datenstruktur abspeichert und diese somit fest verwurzelt sind. Ist nun ein Angreifer in Besitz eines gefälschten Zertifikates einer Domain gekommen das schon ein existierendes Zertifikat in den Logserver hat, kann daraufhin über den Wurzelknoten bestimmt werden ob dies das gleiche Zertifikat ist. Dennoch gibt es einige Aspekte zu beachten. CT funktioniert nur wenn auch auf der Website das Flag für den expect CT Header gesetzt ist und es ist nicht in allen Browsern implementiert (Mozilla beschreibt Performanceprobleme beim Einsatz von CT). [[4]](#_CTVL00189262c0c9793494fb5aa41a90a440cea)

Perl, Fahl et al. 2014 [[9]](#_CTVL0013aaf6c163c024423ac9d58b71c58140f) analysierten auf einen internetweiten Datensatz von 48 Millionen HTTPS-Zertifikaten gestützt und diese mit Trust Stores aller großen Browser- und Betriebssystemhersteller verglichen. Dabei konnten Sie 140 CA-Zertifikate identifizieren, die in zwölf Trust Stores aller wichtigen Plattformen enthalten sind und niemals zum Signieren von Zertifikaten verwendet werden, die in HTTPS eingesetzt werden. Basierend auf diesen Erkenntnissen wird vorgeschlagen diese CA-Zertifikate zu entfernen oder einzuschränken.

**Hier noch genauer darauf eingehen was aus diesem paper die conclusion ist und in wiefern ich mich in der thesis davon abgrenze. Echtzeicht, heimnetzwerk,**

In dieser Arbeit soll es aber um die feingranularere Einstellung eines einzelnen PC’s und den Endbenutzer gehen, bei denen sich in jedem Fall noch weitere Einschränkungen treffen lassen können, sollten als in einem großen Universitätsnetzwerk.

## Methodik/Vorgehensweise

Die Datenerhebung findet mittels eines Fritzbox Router statt. Dieser ist in der Lage den Netzwerkverkehr mitzuschneiden. Der Netzwerkmitschnitt wird einmal über eine Woche lang mitgeschnitten und für die Evaluation dann nochmalig eine Woche. Da es sich in dieser Thesis auf ein Hausnetzwerk beschränkt reicht diese Menge an Netzwerkverkehr.

Aufbau des Heimnetzwerks:

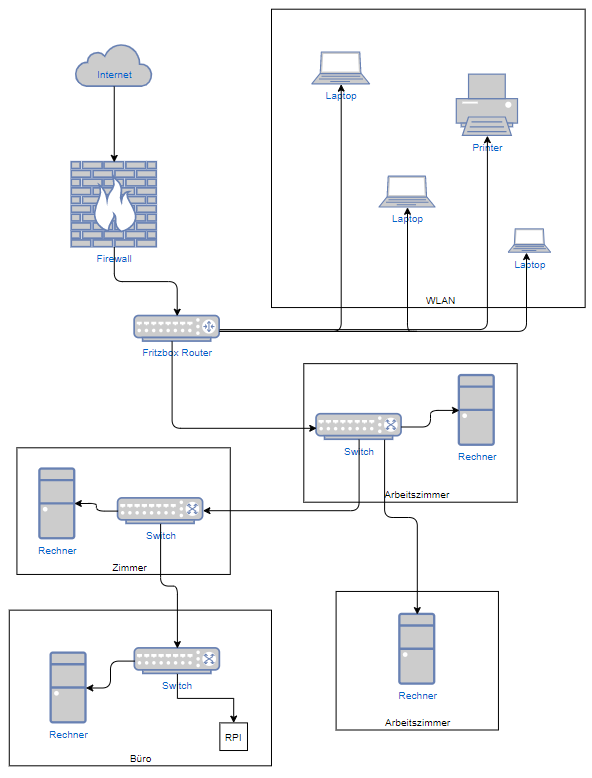


Abbildung : Aufbau des Heimnetzwerks

Das Heimnetzwerk ist in diesem Fall ein relativ großes.

**Zwei Ansätze der Implementierung**

* C/C++ => Benötigte Bibliotheken: Pcapplusplus, Matplotplusplus, openssl, pthreads. Versuch das Programm in der Programiersprache C/C++ zu schreiben. Das Reassemblen der TCP Stream ist hier ein bisschen schwierig. Für die Implementierung werden die Bibliotheken „pcap“ und „openssl“ verwendet. Für erstere gibt es einen Wrapper für C++, das PcapPlusPlus Projekt [[8]](#_CTVL0010e6234adcf88411baf750b7d038802a0). Somit kann Objektorientiert und modular entwickelt werden, was die Erweiterbarkeit und Wartbarkeit steigern.
* Python => Benötigte Abhängigkeiten: dpkt, netifaces, treelib, cryptography, bs4, requests, coloredlogs, pcapy, matplotlib, numpy. In Python existiert bereits von PeterMosman ein tls protocol analyzer, den ich auf meine bedürfnisse angepasst habe und daraufhin das Extrahieren und Parsen der Zertifikatsketten in die jeweiligen Datenstrukturen.

Entscheidung für die Programmiersprache Python, da es sich mit dieser leichter umsetzten lässt und die Erweiterbarkeit und Lesbarkeit des Codes besser ist.

Struktur für eine Aufstellung einer Zertifizierungsstellenkette, um einen graphischen Eindruck von dieser zu erhalten. Des Weiteren soll eine graphische Aufbereitung aller Zertifikatsketten inklusiv den intermediaten Zertifikaten als „Baum“ dargestellt werden.

Um die Überflüssigen Zertifizierungsstellen in den Systemen zu entfernen (verschieben), wird ein Skript erstellt, das diese feingranulare Einstellung automatisiert übernommen werden kann.

Zur Evaluierung soll am Ende überprüft werden, ob die feingranulare Einstellung der Zertifizierungsstellen ohne Einschränkungen des Endbenutzers stattfindet, d. h. es wird erneut über einen Zeitraum von 2 Wochen mittels dem Raspberry PI ein Mitschnitt des Netzwerkverkehrs erstellt und daraufhin ausgewertet.

Ebenso wird ein Mitschnitt eines einzelnen Rechners vorgenommen und ausgewertet, um einen Vergleich zu haben.

## Implementierung

### Anforderungsanalyse

* Die Zertifikate der Root Zertifizierungsstellen sollen in das Programm eingelesen werden.
* Das Programm soll über Argumenten Parameter entweder eine Pcap-datei erhalten oder eine Netzwerkadresse, an der das Programm dann in Echtzeit den Netzwerkverkehr mitschneiden kann.
* In beiden Fällen von zwei (Datei/Netzwerkadresse) sollen dann die TLS-Handshake Nachrichten extrahiert werden (-> inspiriert/angelehnt an Peter Moosmann GitHub)
* Im Verlauf des Programms werden dann die Zertifikatsnachrichten expliziert inspiziert und das jeweilige Root Zertifikat gesucht.

### Aufbau und Struktur

Des Weiteren muss zu Beginn ein Prototyp einer C/C++ Anwendung implementiert werden, der bestimmte Teilbereiche aus dem Netzwerkverkehr extrahiert und in eine Form bringt, um statistische Auswertungen möglich zu machen. Die Implementierung soll alle TLS Handshake Pakete finden und daraus die Zertifikate extrahieren. Da das TLS Protokoll auf Basis der TCP Protokoll übertragen wird, muss ein Reassemblen der Pakete sichergestellt werden. Die Struktur der Daten wird wie folgt aufgebaut:

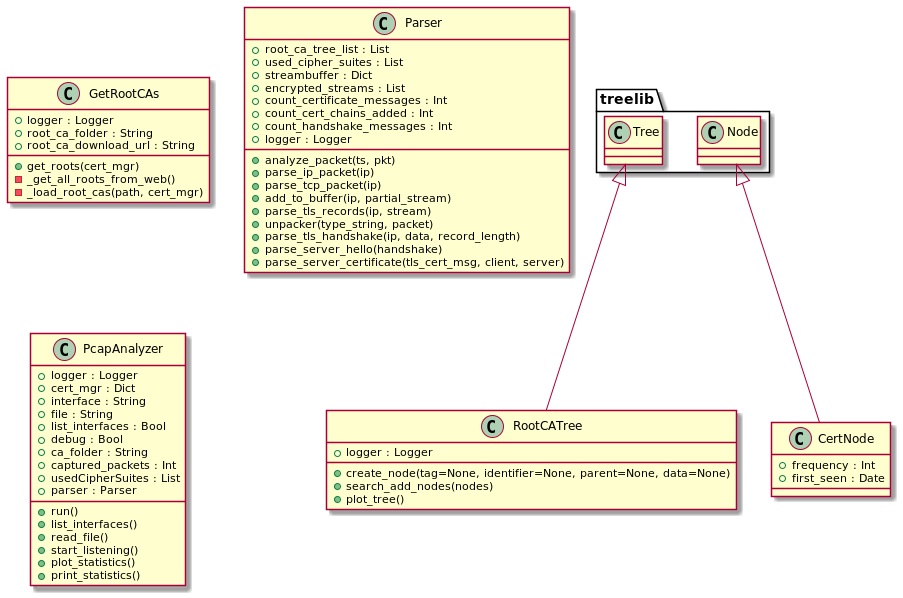


Abbildung : Klassendiagram

### Probleme bei der Implementierung?

## Ergebnisse

Bei der Analyse von Pcap Dateien kann es vorkommen das manche Webseiten noch mit einem älteren Root CA Zertifikat signiert wurden und manche schon mit einer neuen Version. Als Beispiel hier USERTrust RSA Certification Authority in der fritzbox.pcap Datei.

Für die statistische Auswertungen sollen folgende Fragen beantwortet werden:

Werden alle hinterlegten Zertifizierungsstellen verwendet? Wie viele davon werden verwendet?

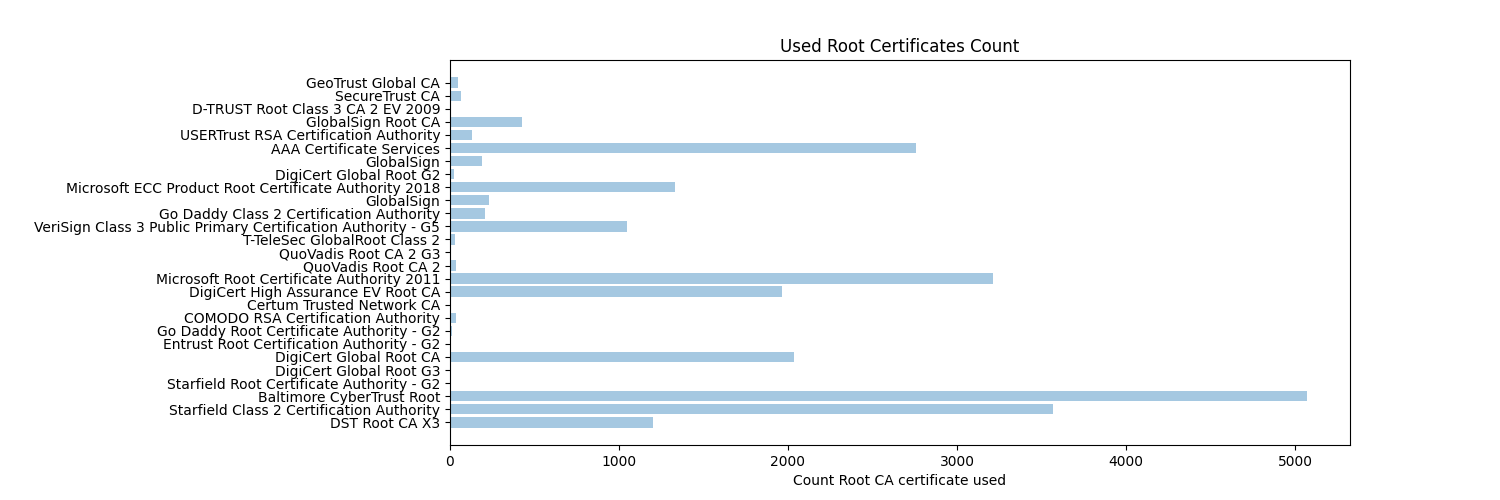


Abbildung : Verwendete Root Zertifizierungsstellen

Auf welche Zeit konvergiert die Anzahl der CA’s?

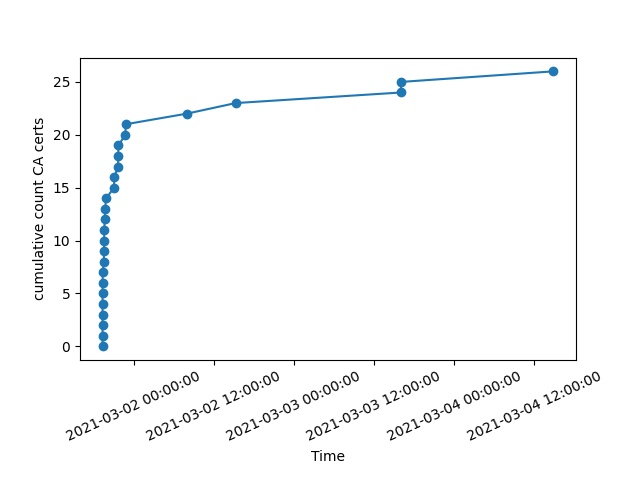


Abbildung : Konvergenz der Zertifizierungsstellen

Welche CipherSuites verwenden die meisten Server?

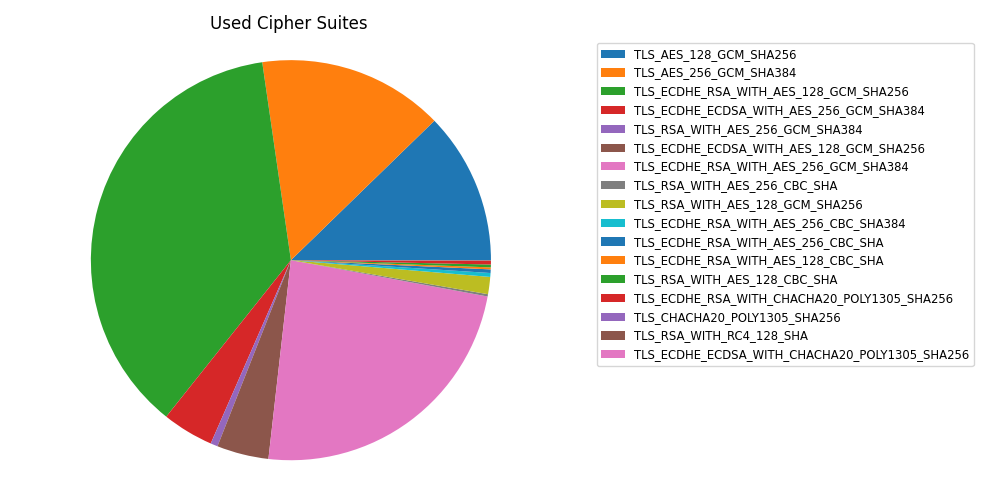


Abbildung : Verwendete Cipher Suites

Welche Länder waren vertreten?

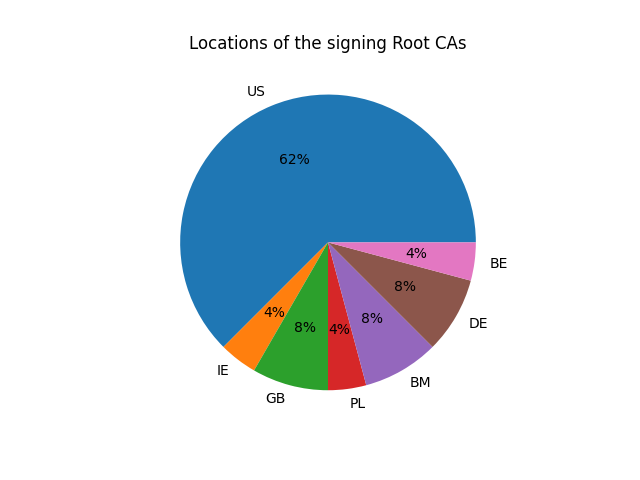


Abbildung : Lokalität der Zertifizierungsstellen

Wie viele Seiten waren dabei die kein Zertifikat enthalten haben?

Gibt es Springer in den Domains (Wechsel der Server)?

Was war die Frage der Thesis?

Wie wurde sie beantwortet? Was sind die konkreten Erkenntnisse aus den verschiedenen Statistiken?

Welche neuen Fragen gibt es?

# Fazit

## Zusammenfassung

## Reflexion

## Ausblick

Literaturverzeichnis

[1] 2014. *An overview of the SSL or TLS handshake*. https://​www.ibm.com​/​support/​knowledgecenter/​en/​SSFKSJ\_8.0.0/​com.ibm.mq.sec.doc/​q009930\_.htm. Accessed 1 March 2021.

[2] Anastasios Arampatzis. 2020. *The Difference between Root and Intermediate Certificates | Venafi*. https://​www.venafi.com​/​blog/​what-difference-between-root-certificates-and-intermediate-certificates. Accessed 30 December 2020.

[3] Bundesamt für Sicherheit in der Informationstechnik. BSI Technische Richtlinie TR-02103: X.509 Zertifikate und Zertifizierungspfadvalidierung.

[4] 2020. *Certificate Transparency*. https://​www.certificate-transparency.org​/​. Accessed 7 July 2020.

[5] GlobalSign GMO Internet, Inc. 2020. *Zertifizierungsstellen & Vertrauenshierarchien | GlobalSign*. https://​www.globalsign.com​/​de-de/​ssl-information-center/​zertifizierungsstellen-vertrauenshierarchien. Accessed 9 March 2021.

[6] Kloep, P. 2020. *PKI und CA in Windows-Netzwerken*. *Das umfassende Handbuch*. Rheinwerk Computing.

[7] Microsoft Security Solutions. 2013. *Which Root CAs do you really trust?* https://​mssec.wordpress.com​/​2013/​01/​31/​which-root-cas-do-you-really-trust/​. Accessed 29 December 2020.

[8] 2020. *PcapPlusPlus - a multiplatform C++ library for capturing, parsing and crafting of network packets*. https://​pcapplusplus.github.io​/​. Accessed 7 July 2020.

[9] Perl, H., Fahl, S., and Smith, M. 2014. You Won’t Be Needing These Any More: On Removing Unused Certificates from Trust Stores. In *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 307–315.

[10] Tools.ietf.org, Rfcmarkup Version 1.129d On. 2021. *RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. https://​tools.ietf.org​/​html/​rfc5280. Accessed 13 March 2021.

[11] Tools.ietf.org, Rfcmarkup Version 1.129d On. 2021. *RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3*. https://​tools.ietf.org​/​html/​rfc8446. Accessed 13 March 2021.

**Abbildungsverzeichnis**

[Abbildung 1: Zertifikat Datenstruktur (https://tools.ietf.org/html/rfc5280) - 14 -](#_Toc66520292)

[Abbildung 1: TLS Hanshake.jpg [1] - 16 -](#_Toc66520293)

[Abbildung 2: Aufbau des Heimnetzwerks - 20 -](#_Toc66520294)

[Abbildung 3: Klassendiagram - 23 -](#_Toc66520295)

[Abbildung 4: Verwendete Root Zertifizierungsstellen - 24 -](#_Toc66520296)

[Abbildung 5: Konvergenz der Zertifizierungsstellen - 25 -](#_Toc66520297)

[Abbildung 6: Verwendete Cipher Suites - 25 -](#_Toc66520298)

[Abbildung 7: Lokalität der Zertifizierungsstellen - 26 -](#_Toc66520299)

**Listingverzeichnis**

**Anhang**