% Abschlussarbeit

% Autor_in

% Prüfer_in

% Betreuer_in

Fakultät für
Informatik und
Mathematik

HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Authentifizierung von Systemen: Beschreibung eines Verfahrens zur sicheren Generierung, Verwahrung und Aktualisierung von Zertifikaten

Richard Reik

Bachelorarbeit Informatik

Prüfer:
Prof. Dr. , Hochschule München

Betreuer:
Dr. , Firma GmbH

01.03.2018

Erklärung

Richard Reik, geb. 27.08.1998 (IF8, SS 2021)

Hiermit erkläre ich, dass ich die Bachelorarbeit 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.

München, 01.03.2018

. . . . . .

Unterschrift

Zusammenfassung

(Worum geht es?) Sicherheit ist ein Thema das zunehmend an Wichtigkeit gewinnt, vor allem im Internet wird kommunikation zunehnemend verschlüsselt. Nachrichten die heutzutage unverschlüsselt verschickt werden sind nichtmehr die Regel sondern stellen eine Ausnahme dar. Daher ist es wichtig zu verstehen wie Sicherheit gewährleistet werden kann, auch wenn Geräte sich nichtmehr in eigener Hand befinden.

Zielstellung dieser Arbeit ist verwalten von Zertifikaten, welche benutzt werden können um jene Sicherheit zu gewährleisten. Dabei soll besonderenDie sichere Erstellung, Aktualisierung und Speicherung von Zertifikaten. Problemstellung: Forschungsfrage:

(Wie bin ich vorgegangen?) Methoden:

(Was sind meine wichtigsten Ergebnisse?) Ergebnisse/Fazit:

(Was bedeuten meine Ergebnisse?) Diskussionsgrundlage/Empfehlung:

Das ACME Protokol wird verwendet um es Servern zu ermöglichen

Tabelle 1: Informationsverlust in %, realer Datensatz

k	l	t	Informationsverlust
2	-	-	-64,288 %
3	-	-	-69,002 %
4	-	-	-69,008 %
4	3	-	-69,233 %
4	5	-	-69,652 %
4	-	0,7	-70,164 %
4	-	0,1	-70,409 %
4	-	0,01	-82,463 %

Danksagungen

Interdum et malesuada fames ac ante ipsum primis in faucibus. Aliquam congue fermentum ante, semper porta nisl consectetur ut. Duis ornare sit amet dui ac faucibus. Phasellus ullamcorper leo vitae arcu ultricies cursus. Duis tristique lacus eget metus bibendum, at dapibus ante malesuada. In dictum nulla nec porta varius. Fusce et elit eget sapien fringilla maximus in sit amet dui.

Mauris eget blandit nisi, faucibus imperdiet odio. Suspendisse blandit dolor sed tellus venenatis, venenatis fringilla turpis pretium. Donec pharetra arcu vitae euismod tincidunt. Morbi ut turpis volutpat, ultrices felis non, finibus justo. Proin convallis accumsan sem ac vulputate. Sed rhoncus ipsum eu urna placerat, sed rhoncus erat facilisis. Praesent vitae vestibulum dui. Proin interdum tellus ac velit varius, sed finibus turpis placerat.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Nicht ausgerichtet

API: **A**pplication **P**rogramming **I**nterface

JSON: **J**ava**S**cript **O**bject **N**otation

Ausgerichtet

API	**A**pplication **P**rogramming **I**nterface
JSON	**J**ava**S**cript **O**bject **N**otation

1 | Einleitung mit Zitat

1.1 Hintergrund

Das ist die Einleitung. Quisque finibus aliquet cursus. Integer in pellentesque tellus. Duis eu dignissim nulla, a porttitor enim. Quisque vehicula leo non ultrices finibus. Duis vehicula quis sem sit amet sollicitudin. Integer neque est, pharetra et auctor vel, iaculis interdum lectus.

Um ein Zitat in den Text aufzunehmen, füge einfach den in der references.bib-Datei gezeigten Zitatschlüssel hinzu. Der Stil des Zitats wird durch die Datei ref_format.csl bestimmt. Zum Beispiel findest Du in *The Living Sea* Bilder vom *Calypso* [1].

In neque mauris, maximus at sapien a, iaculis dignissim justo. Aliquam erat volutpat. Praesent varius risus auctor est ultricies, sit amet consequat nisi laoreet. Suspendisse non est et mauris pharetra sagittis non porta justo. Praesent malesuada metus ut sapien sodales ornare.

1.2 Der Mittelteil

Das ist der Mittelteil. Phasellus quis ex in ipsum pellentesque lobortis tincidunt sed massa. Nullam euismod sem quis dictum condimentum. Suspendisse risus metus, elementum eu congue quis, viverra ac metus. Donec non lectus at lectus euismod laoreet pharetra semper dui. Donec sed eleifend erat, vel ultrices nibh.

Nam scelerisque turpis ac nunc mollis, et rutrum nisl luctus.

Duis faucibus vestibulum elit, sit amet lobortis libero. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Sed at cursus nibh. Sed accumsan imperdiet interdum. Proin id facilisis tortor. Proin posuere a neque nec iaculis. Suspendisse potenti. Nullam hendrerit ante mi, vitae iaculis dui laoreet eu.

Cras eleifend velit diam, eu viverra mi volutpat ut. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec finibus leo nec dui imperdiet, tincidunt ornare orci venenatis. Maecenas placerat efficitur est, eu blandit magna hendrerit eu.

1.2.1 Unterabschnitt des Mittelteils

Das ist ein Unterabschnitt des Mittelteils. Quisque sit amet tempus arcu, ac suscipit ante. Cras massa elit, pellentesque eget nisl ut, malesuada rutrum risus. Nunc in venenatis mi. Curabitur sit amet suscipit eros, non tincidunt nibh. Phasellus lorem lectus, iaculis non luctus eget, tempus non risus. Suspendisse ut felis mi.

1.3 Zusammenfassung der Kapitel

Dies ist ein kurzer Überblick darüber, was in jedem Kapitel geschrieben wurde. **Kapitel 1** gibt einen Hintergrund über duis tempus justo quis arcu consectetur sollicitudin. **Kapitel 2** diskutiert morbi sollicitudin gravida tellus in maximus. **Kapitel 3** diskutiert vestibulum eleifend turpis id turpis sollicitudin aliquet. **Kapitel 4** zeigt wie phasellus gravida non ex id aliquet. Proin faucibus nibh sit amet augue blandit varius.

2 | Literaturübersicht mit Mathe

2.1 Einleitung

Das ist die Einleitung. Duis in neque felis. In hac habitasse platea dictumst. Cras eget rutrum elit. Pellentesque tristique venenatis pellentesque. Cras eu dignissim quam, vel sodales felis. Vestibulum efficitur justo a nibh cursus eleifend. Integer ultrices lorem at nunc efficitur lobortis.

2.2 Der Mittelteil

Das ist die Literaturübersicht. Nullam quam odio, volutpat ac ornare quis, vestibulum nec nulla. Aenean nec dapibus in mL/min^{-1}. Mathematical formula can be inserted using Latex:

$$f(x) = ax^3 + bx^2 + cx + d \tag{1}$$

Nunc eleifend, ex a luctus porttitor, felis ex suscipit tellus, ut sollicitudin sapien purus in libero. Nulla blandit eget urna vel tempus. Praesent fringilla dui sapien, sit amet egestas leo sollicitudin at.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Sed faucibus pulvinar volutpat. Ut semper fringilla erat non dapibus. Nunc vitae felis eget purus placerat finibus laoreet ut nibh.

2.3 Fazit

Das ist das Fazit. Donec pulvinar molestie urna eu faucibus. In tristique ut neque vel eleifend. Morbi ut massa vitae diam gravida iaculis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.

- erstes Element der Liste
- zweites Element der Liste
- drittes Element der Liste

3 | Architektur

Zur Darstellung der Umsetzung der erweiterung zum ACME Protokol ist es wichtig voher zu erklären wie eine ACME Challenge aussieht und an welchen Punkten angesetzt werden kann. Dabei soll auch verdeutlicht werden welche Gefahren und Herrausforderungen bei jeder Änderung negiert oder hinzugefügt werden. Dabei werden zuerste die Hintergründe geklärt bevor das Verfahren anhand der DNS Challenge beschrieben werden soll.

3.1 Hintergründe

3.1.1 ACME

ACME steht für Automatic Certificate Management Enviroment. Wie der Name schon vermuten lässt handelt es sich hierbei um Software die Verwendet werden kann um Zertifikate automatisch ausstellen und verwalten zu können. Die Idee hierzu stammt aus der lästig werdenden Handarbeit die Entsteht wenn für mehrer Server per Hand eine neues Zertifikate ausgestellt werden soll. Das Verfahren wird im RFC-8555 definiert und stellt neben einer internen CA zum austellten von Zertifikaten auch ein Validierungssystem dar, mit dessen Hilfe sichergestellt werden kann dass nur die korrekten Instanzen ein Zertifikat erhalten.

3.1.2 Nonce

ACME verwendet Replay Noncen um sicher zu stellen dass die Anwendung vor Replay Angriffen geschützt ist. Auf jede valide Anfrage an den Server antwortet dieser mit einer Replay Nonce im JWS Header, welche für den nächsten Request verwendet werden kann. Da dieses Prinzip für jede Anfrage gilt wird sie im weiteren Verlauf der Bachelorarbeit nicht explizit für jeden Schritt im Protokol genannt.

3.1.3 JWS

Um unnötige Informationen zu vermeiden soll auch hier im weiteren Verlauf nicht weiter aufgelistet werden wie die Signatur aussieht oder welche Header mitgeschickt werden. Die Ausnahme stellen hier Informationen die dem Client über den Header des Server Requests mitgeschickt werden.

3.2 Schritt 0: Die erste Nonce

Wie im vorheringen Absatz beschrieben wird die Nonce vom Server zur verwendung mitgeschickt, allerdings falls diese veraltet oder noch kein Valider Request gesendet wurde braucht es eine Möglichkeit Replay Noncen abzufragen. Dazu stellt jeder ACME Server eine kleine Übersicht mit allen Relevanten URLs zur Verfügung. Darunter befindet sich auch eine URL um einen Account zu erstellen, sowie eine um eine Nonce anzufragen. Jede ACME Kommunikation beginnt also mit dem anfragen der Replay-Noncen URL.

3.3 Schritt 1: Account erstellen

Jeder Request wird fest an einen Account gebunden und so muss, falls das noch nicht in einere anderen Session passiert ist ein neuer Account erstellt werden.

Dazu sendet der Client in seiner JWS Payload Mail addressen die mit diesem Account verknüpft werden sollen, sowie eine Bestätigung das der Client mit den Nutzungsbedinugen einverstanden ist. Optional kann hier auch ein bereits vorhandenes Konto verknüpft werden. Da noch keine KID vorhanden ist wird hier im Header an dessen Stelle JWK mit dem entsprechendem Privaten Schlüssel an den Server gesendet. Der Server antwortet in der Payload mit dem Status des Accounts, sowie mit der KID des Client und der entsprechenden URL des Accounts.

3.4 Schritt 2: Order platzieren

Mit den Informationen aus Schritt 1 kann der Client nun eine Order aufgeben. Dazu sendet er in der Payload ein Array mit allen Ordern die er aufgeben möchte, sowie einen Zeitlichen Rahmen in dem die Validierung durchgeführt werden soll, an den Server. Dabei wird in dem Array nicht nur definiert mit welchem Verfahren sondern auch mit gegen welchen Wert die Validierung stattfinden soll. In der Antwort schickt der Server den Status, wann die Anfrage ungültig wird, sowie ein Array an Links zur Validierung der Order. Für jede Order wird ein Link erstellt. Zusätzlich antwortet der Server mit einer Finalisierungs URL die im späteren Verlauf benötigt wird.

3.5 Schritt 3: Challenge aktivieren

Je nachdem um welchen Typ von Challenge es geht ist dieser Schritt unterschiedlich. Bei der DNS Challenge wird nun eine Nachricht an den Server geschickt um ihn wissen zu lassen das jetzt eine Validierung durchgeführt werden kann. Der Server antwortet mit einem Wert den der Client entschlüsselt in einem TXT Dokument, für den Server zugänglich abspeichert. Der Server kann nun dieses Dokument anfragen und so bestimmen das der Client tatsächlich die Kontrolle über die angegebene DNS besitzt.

3.6 Schritt 4: Challenge erfüllen

Auch dieser Schritt ist abhängig von der jeweiligen Challenge, grob kann gesagt werden dass die Challenge erfüllt wird und der Server den Status für diese Challenge anpasst.

3.7 Schritt 5: CSR wird an den Server geschickt

Wird der Status für diese Order als Valide erkannt, also alle Challenges wurden erfüllt, so kann der Client sein Certifikat anfragen. Dazu sendet er dem Server eine CSR aus welcher dieser ein Certifkat erstellt.

3.8 Schritt 6: Certifikat wird erhalten

Das im Schritt 5 erstellte Zertifikat wird auf dem Server gespeichert und kann vom Client angefordert werden. Dazu sendet er einen POST-AS-GET Request an die im letzten Schritt mitgeteilte URL. Der Server Antwortet mit dem Certifiat im Body der Antwort.

3.9 Weitere mögliche Schritte

Damit ist die Kommunikation abgeschlossen. Der Client kann nun über den erstellten Account die Certifikate aktualisieren lassen, ohne die Challenges noch einmal durchlaufen zu müssen. Der Client kann den Server bitten den Account zu löschen oder ein Certifikat zu wiederrufen.

4 | Ablauf

Die Kommunikation zwischen Client und Server wird durch Replay-noncen sowie durch JWS gesichert. Um die Kommunikation zu initialisieren muss der Client eine Replay-Nonce vom Server erfragen und zusätzlich ein Schlüssel paar erstellen. Der Öffentliche Schlüssel wird dabei zum Signieren der Nachrichten verwendet wohingegen mit dem Privaten Teil die Nachricht verschlüsselt wird mit einem ebenso anzugebenen Verfahren. (TODO: prüfen ob das stimmt, TODO: Prüfen ob das schon in Grundlagen abgedeckt werden kann). Jeder ACME Server beinhaltet eine URL die per Browser auch ohne Verschlüsselungen oder Replay-noncen erreicht werden kann, bei pebble ist das unter /14000/dir. Hier kann unter anderem Ausgelesen werden mit welcher URL ein Get-Account request erstellt werden kann.

Da jeder Request mit JWS verschlüsselt wird und jedes mal eine Replay Nonce mitgeschickt wird, welche der Servers im letzten Response mitgeschickt hat, wird darauf verzichtet dies bei jedem Schritt erneut zu erwähnen.

Es gibt im ACME Protokol keinen GET Request, da dieser keine Payload und damit auch keine Sicherheit bieten würde. Jeder Request der als GET Request fungieren soll ist tatsächlich nur ein POST Request in dem die Payload des JWS leer ist. Die einzige Ausnahme hierzu stellt die Anfrage an die Übersichtsseite /14000/dir.

4.0.1 Account erstellen

Client: Die Payload des Get-Account requests beinhaltet neben einem Array an Mail Addressen die mit diesem Konto verknüpft werden sollen, nur eine bestätigung der TermsOfService. Server: Der Server antwortet mit einem "201 Created" und teilt dem Client im Response Body die für ihn geltende Order-List-URL sowie seine Account-URL mit mit. Anhand dieser URL kann der Client eine Übersicht über seine aktuellen Order mithilfe eines POST-AS-GET Requestes erhalten.

4.0.2 New-Certificate Request

Client: Nun können für diesen Account Zertifikate angefragt werden. Dazu sendet der Clinet in der Payload ein Array von Identfiern sowie ein NotBefore und NotAfter an den Server. Die Identfier bestehen aus einmal dem "Typ", also dem Ferfahren mit welchem die Verifiziert werden soll. Sowie einem Value gegen den getested werden kann. NotBefore steht für den frühsten Zeitpunkt in dem die Challenge stattfinden soll und NotAfter stellt die Zeitliche Obergrenze dar. (TODO: Prüfen ob notBefore und NotAfter stimmen). Server: Der Sever antwortet mit "status", "expires", "notBefore", "notAfter", den Identifiern sowie "authorizations" und "finalize".

4.0.3 Start Challenge

Client: Durch den letzten Request kann der Client den Server nach der soeben

5 | Untersuchung von Angriffsvektoren

In diesem Kapietel sollen die Möglichen Angriffsvektoren besprochen werden die bei dem DNS sowie dem IP verfahren bestanden, sowie neue die durch die neue Methode erst hinzugekommen sind. Dabei wird unterteilt in Vektoren die in allen Verfahren relevant sind, jene die speziell auf das neue Verfahren zugeschnitten sind und abschließend sollen mögiche Einfallstore besprochen werden.

5.1 Was sind Angriffsvektoren

Einfallstore.

5.2 Altbekannte Angriffsvektoren

1. Replay Angriffe (Replay noncen)
2. JWS (Man in the Middle Angriffe, da Signatur den Content schützt. Änderungen ohne die Singatur ungültig zu machen sind nicht möglich)
3. dos (Server abhänging. Nicht sicher ob Teil meiner BA)
4. Sozial Hacking (fällt flach da Automatisiert)

5.2.1 Neuartige Angriffsvektoren

1. Impersonation Angriff Vor dem ersten Schritt: Er kann erfolgreich einen Account anlegen und eine Order senden, allerdings wird hier der Value überprüft und die Order verweigert Nach den ersten zwei Schritten: Die Account sowie die Order URL sind unbekannt. Anfragen können nicht geschickt werden. (Falls doch bekannt kann die Challenge nicht erfüllt werden, da den Private Key nur der Klient kennt) Nach dem Vallidieren: MÖGLICH? URL wird benötigt, sowie JWS Values, keine weitere Sicherheit

2. MitM Kommunikation verschlüsselt, JWS, Private Keys nur auf Client/Server. Allerdings, was ist wenn der Client als zwischen speicher funktioniert. Wenn er den JWS Wert lesen kann, ist er in der Lage die Kommunikation mit zu verfolgen -> Nutzen unklar

3. Continues Validation durch Zertifikate Chaining ?

4. Server Impersonation Möglich die gesammte Kommunikation zu faken -> Gerät wird nutzlos

5. Physischen Schaden bsp: TPM Chip entfernen, oder zerstört

6. Abschießen des Daemon (Zertifikate können nicht mehr ausgestellt werden)

7. Server DB kaputt machen (Daten verlust) / Datenbank mit falschen Daten füttern

8. Was passiert wenn ein Angreifer einen Stick einfügt und über diesen Bootet? / Was passiert wenn der TPM Chip abgebaut wird und wo anders eingesetzt wird?

6 | Finale Untersuchung

6.1 Einleitung

Das ist die Einleitung. Sed vulputate tortor at nisl blandit interdum. Cras sagittis massa ex, quis eleifend purus condimentum congue. Maecenas tristique, justo vitae efficitur mollis, mi nulla varius elit, in consequat ligula nulla ut augue. Phasellus diam sapien, placerat sit amet tempor non, lobortis tempus ante.

6.2 Methode

Donec imperdiet, lectus vestibulum sagittis tempus, turpis dolor euismod justo, vel tempus neque libero sit amet tortor. Nam cursus commodo tincidunt.

6.2.1 Unterabschnitt 1

Das ist der erste Teil der Methodik. Duis tempor sapien sed tellus ultrices blandit. Sed porta mauris tortor, eu vulputate arcu dapibus ac. Curabitur sodales at felis efficitur sollicitudin. Quisque at neque sollicitudin, mollis arcu vitae, faucibus tellus.

6.2.2 Unterabschnitt 2

Das ist der zweite Teil der Methodik. Sed ut ipsum ultrices, interdum ipsum vel, lobortis diam. Curabitur sit amet massa quis tortor molestie dapibus a at libero. Mauris mollis magna quis ante vulputate consequat. Integer leo turpis, suscipit ac venenatis pellentesque, efficitur non sem. Pellentesque eget vulputate turpis. Etiam id nibh at elit fermentum interdum.

6.3 Ergebnisse

Das sind die Ergebnisse. In vitae odio at libero elementum fermentum vel iaculis enim. Nullam finibus sapien in congue condimentum. Curabitur et ligula et ipsum mollis fringilla.

6.4 Auseinandersetzung

Das ist die Auseinandersetzung mit den Ergebnissen. Curabitur gravida nisl id gravida congue. Duis est nisi, sagittis eget accumsan ullamcorper, semper quis turpis. Mauris ultricies diam metus, sollicitudin ultricies turpis lobortis vitae. Ut egestas vehicula enim, porta molestie neque consectetur placerat. Integer iaculis sapien dolor, non porta nibh condimentum ut.

6.5 Schlussfolgerung

Das ist die Schlussfolgerung des Kapitels. Nulla sed condimentum lectus. Duis sed tempor erat, at cursus lacus. Nam vitae tempus arcu, id vestibulum sapien. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.

7 | Fazit

7.1 Zusammenfassung der Arbeit

Zusammenfassend pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nunc eleifend, ex a luctus porttitor, felis ex suscipit tellus, ut sollicitudin sapien purus in libero. Nulla blandit eget urna vel tempus. Praesent fringilla dui sapien, sit amet egestas leo sollicitudin at.

7.2 Zukünftige Arbeit

Es gibt mehrere mögliche Richtungen, um diese Arbeit zu erweitern. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam gravida ipsum at tempor tincidunt. Aliquam ligula nisl, blandit et dui eu, eleifend tempus nibh. Nullam eleifend sapien eget ante hendrerit commodo. Pellentesque pharetra erat sit amet dapibus scelerisque.

Vestibulum suscipit tellus risus, faucibus vulputate orci lobortis eget. Nunc varius sem nisi. Nunc tempor magna sapien, euismod blandit elit pharetra sed. In dapibus magna convallis lectus sodales, a consequat sem euismod. Curabitur in interdum purus. Integer ultrices laoreet aliquet. Nulla vel dapibus urna. Nunc efficitur erat ac nisi auctor sodales.

Anhang 1: Einige Extras

Füge Anhang 1 hier hinzu. Vivamus hendrerit rhoncus interdum. Sed ullamcorper et augue at porta. Suspendisse facilisis imperdiet urna, eu pellentesque purus suscipit in. Integer dignissim mattis ex aliquam blandit. Curabitur lobortis quam varius turpis ultrices egestas.

Anhang 2: Noch mehr Extras

Füge Anhang 2 hier hinzu. Aliquam rhoncus mauris ac neque imperdiet, in mattis eros aliquam. Etiam sed massa et risus posuere rutrum vel et mauris. Integer id mauris sed arcu venenatis finibus. Etiam nec hendrerit purus, sed cursus nunc. Pellentesque ac luctus magna. Aenean non posuere enim, nec hendrerit lacus. Etiam lacinia facilisis tempor. Aenean dictum nunc id felis rhoncus aliquam.

Literatur

[1] Tom Pollard; Marvin Reimer; David San; Arco Mul; Matthew Gwynfryn Thomas; Jakub Nowosad; Dennis Weissmann; W. Caleb McDaniel. 2016. *Template for writing a PhD thesis in Markdown*. Tom Pollard. Abgerufen 1. November 2017 von https://github.com/tompollard/phd_thesis_markdown/tree/v1.0