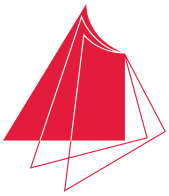


Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Analyse einer Referenzimplementierung des ActivityPub Standards mit Blick auf die Sicherheit

Bachelor Thesis von

Armin Kunkel

an der Fakultät für Informatik und Wirtschaftsinformatik
Fachrichtung Verteilte Systeme (VSYS)

Erstgutachter: Prof. Dr. rer. nat. Christian Zirpins
Betreuer: M. Sc. Robert Schäfer

01. Dezember 2018 – 31. März 2019

Hochschule Karlsruhe Technik und Wirtschaft
Fakultät für Informatik und Wirtschaftsinformatik
Moltkestr. 30
76133 Karlsruhe

Ich versichere wahrheitsgemäß, die Arbeit selbstständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Änderungen entnommen wurde.

Karlsruhe, 17. Januar 2019

. . . . . .

(Armin Kunkel)

Zusammenfassung

Deutsche Zusammenfassung

Inhaltsverzeichnis

1. Einleitung

Zentralisierung von Daten und das Vertrauen auf einzelne Instanzen ist heutzutage allgegenwärtig. Im Internet gibt es eine Fülle an sozialen Netzwerken wie Facebook, Twitter, Google+, Instagram oder Pinterest die zumeist das Recht an den Daten, die Sie von ihren Nutzer bekommen, behalten und nicht zuletzt diese Daten auch verkaufen für z. B. Werbezwecke. Für Kriminelle sowie Geheimdienste ist es außerdem leichter an die gesamte Datenbank zu kommen, da bei zentralisierten Netzwerken meist auch eine zentrale Datenbank, bzw. ein zentraler Zugriffspunkt, vorhanden ist. Wenn der Zugriff auf diesen zentralen Punkt erreicht ist kann die ganze Datenbank ausgelesen werden.

Was bedeutet nun dezentral? In der Politik wird unter Dezentralisierung „die Übertragung zentral staatlicher Aufgaben auf subnationale oder subsidiäre Ebene(n) verstanden“[**wikipedia-dez**
In der Energiewirtschaft spricht man von einer „dezentralen Stromerzeugung“, wenn der Strom an den Stellen wo er verbraucht auch erzeugt wird. Ein Beispiel hierfür wäre ein Wasserkraftwerk, dass den Strom für die umgebenen Dörfer oder Städte liefert[**wikipedia-dezentralisie**
In der Informatik versteht man unter Dezentralisierung das verteilen von u. A. Daten über mehrere unabhängige Server hinweg.

Durch die Verteilung der Aufgaben auf sub-nationale oder subsidiäre Ebene wird die zentral staatliche Ebene entlastet und hat somit mehr Ressourcen für andere Aufgaben. Beim Errichten von Wasserkraftwerken nahe an Dörfern und Städten entfällt der Transport des Stroms über größere Distanzen und somit verringert sich der Verlust beim Transport über das Stromnetz. Dezentralisieren von sozialen Netzwerken bring verschiedene Vorteile mit sich. Ein Vorteil ist die Skalierbarkeit bei dezentralen sozialen Netzwerken. Durch das hinzufügen weiterer Instanzen können dem Netzwerk neue Ressourcen bereitgestellt werden. Ein weiterer Vorteil liegt darin, dass keine zentrale Kontrollinstanz vorhanden ist welche korrumpiert werden kann, sei es durch Kriminelle, wirtschaftliche Interessenvertreter oder staatliche Autoritäten.

Ziel der Arbeit ist es die Implementierung des verteilten Server-zu-Server Protokolls als Prototyp vorzunehmen und die bis dato von der World Wide Web Consortium (W3C) Gemeinschaft empfohlenen Sicherheitsstandards für das ActivityPub Protokoll zu prüfen. Darüber hinaus soll die Arbeit einen Überblick über die Grundlagen des Protokolls geben und wie die relevanten Bestandteile zu verstehen sind. Die verwendeten Sicherheitsstandards beziehen sich auf das Authentifizieren vom Client gegenüber dem Server und zusätzlich der Server untereinander, sowie das Sicherstellen der manipulationsfreien Übertragung von Inhalten.

@Zirpins Was genau soll im oberen Absatz weiter erklärt werden???

1.1. Motivation

Bei zentralen sozialen Netzwerken, z.B. Facebook, besitzt die Kontrolle über Daten das Unternehmen. Durch die Dezentralisierung bleiben Daten bei den einzelnen Instanzen des sozialen Netzwerkes. Die Datenbanken bei zentralen Netzwerken können zwar verteilt sein und auch das Netzwerk könnte dezentral angelegt sein, trotzdem gehören die Daten einem Unternehmen. Außerdem können bei zentralen sozialen Netzwerken nicht ohne weiteres Inhalte mit anderen Netzwerken ausgetauscht werden. Mit einem Protokoll wie ActivityPub wird das Verteilen sowie der Zugriff auf Inhalte und der Austausch von Aktivitäten über mehrere soziale Netzwerke hinweg ermöglicht.

ActivityPub besteht aus zwei Teilen. Dem Client-zu-Server Protokoll, auch „Social API“ genannt, und dem förderierten Server-zu-Server Protokoll. Durch die ActivityPub W3C Empfehlung Anfang 2018 und die Social Web Working Group (SWWG) Arbeitsgruppe des W3C sowie weiteren, wird die Verbreitung des Protokolls vorangebracht.

Der Netzwerkeffekt ist ein aus der Volkswirtschaftslehre stammender Begriff. Als Beispiel sei das Telefonnetz genannt. Umso mehr Leute ein Telefon besitzen, umso höher ist der Nutzen für jeden einzelnen Telefon Besitzer[**netzwerkeffekt**]. Übertragen auf ActivityPub bedeutet das soviel wie: „Je mehr Netzwerke den Standard implementieren, desto höher ist der Nutzen für ein einzelnes Netzwerk und im Endeffekt für die einzelnen Nutzer“.

Protokolle wie „Diaspora Federation und OStatus“ bieten den Zugriff auf dezentral gespeicherte soziale Inhalte und ermöglichen das veröffentlichen von sozialen Inhalten. Der im März letzten Jahres vom W3C empfohlene Standard namens „ActivityPub“ wurde auf Basis des Wissens im Umgang mit dem OStatus und Pump.io Protokoll entwickelt[**activityPub**].

Quelle für dezentralen Zugriff

ActivityPub ist wie „OStatus“ ein Protokoll für dezentrale soziale Netzwerke und wird in dieser Bachelor Arbeit untersucht.

2. Grundlagen zur sicheren Umsetzung dezentraler sozialer Netzwerke

Allgemeine Grundlagen zu Sozialen Netzwerken/Social Media und deren Sicherheitsaspekte

Welche Klassen von Anwendungen und Implementierungen gibt es allgemein bei sozialen Netzwerken? Einordnen von ActivityPub!!

Dieses Kapitel gibt einen Überblick über allgemeine Grundlagen von sozialen Netzwerken. Es wird grob erläutert für was soziale Netzwerke gedacht sind, der Unterschied zwischen zentralen und dezentralen sozialen Netzwerken herausgestellt sowie auf Sicherheitsaspekte eingegangen.
Im Anschluss wird ein Kryptographie Unterkapitel eingeführt in dem die benötigten Verfahren für die sichere Umsetzung erläutert werden. Begonnen wird mit einer kurzen Einführung in Kryptographie und darauf folgend kurz das Rivest-Shamir-Adleman (RSA) Verfahren sowie eine allgemeine Beschreibung von Signatur Algorithmen gegeben.
Zuletzt wird der ActivityPub Standard eingeführt sowie eingeordnet, Bestandteile des Protokolls beschrieben, die Funktionsweise der Client-zu-Server sowie Server-zu-Server Kommunikation und zugehörige Standards kurz erläutert.

2.1. Allgemeine Grundlagen sozialer Netzwerke

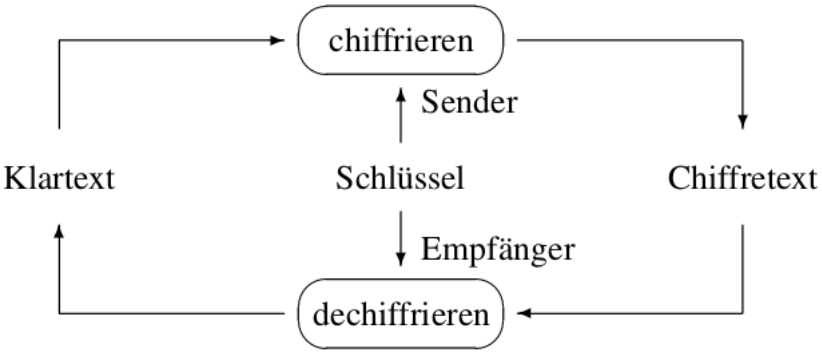
2.1.1. Unterschied zentraler zu dezentralen sozialen Netzwerken

2.1.2. Sicherheitsaspekte sozialer Netzwerke

2.2. Kryptographie

„Unter dem Begriff Kryptographie ist die Wissenschaft vom geheimen Schreiben zu verstehen“.[1] Man spricht von symmetrischer Verschlüsselung wenn eine Nachricht im Klartext vom Sender mit einem geheimen Schlüssel, welcher beiden Parteien bekannt ist, verschlüsselt und vom Empfänger, mit demselben Schlüssel, entschlüsselt wird.[2]

[1] Dietmar Wätjen, 2018, S.1
[2] Vgl. Dietmar Wätjen, 2018, S.1



Quelle: (Wätjen, 2018, S.1)

Abbildung 2.1.: Symmetrische Ver- und Entschlüsselung

2.2.1. RSA

Von asymmetrischer Verschlüsselung ist die Rede, wenn die Teilnehmer anstatt einen gemeinsamen Schlüssel zu haben, der im vor hinein ausgetauscht werden muss, jeder ein Schlüsselpaar (öffentlicher und privater Schlüssel) besitzt. Das RSA Verfahren ist ein solches asymmetrisches Verschlüsselungsverfahren welches von den drei namens gebenden Mathematikern 1977 entwickelt wurde. Das RSA Verfahren ist wohl das am häufigsten verwendete Public-Key-Kryptosystem.
Beispiel 1. Die Gesprächspartner Alice und Bob, welche beide ein Schlüsselpaar besitzen, miteinander kommunizieren. Alice verschlüsselt einen Nachrichtentext mit dem öffentlichen Schlüssel von Bob und sendet die verschlüsselte Nachricht an Bob. Dieser kann seinerseits mit seinem privaten Schlüssel die Nachricht entschlüsseln.[3]

2.2.2. Signaturen

Für die Sicherstellung der Authentizität können sogenannte Signaturen verwendet werden. Das oben kurz erläuterte Verfahren kann nicht nur zum Ver- und Entschlüsseln von Nachrichten benutzt werden, sondern auch zum signieren.
Dabei wird statt des öffentlichen Schlüssels, der private Schlüssel benutzt um eine, in diesem Fall, Signatur zu erzeugen. Diese kann dann mit dem öffentlichen Schlüssel des zugehörigen privaten Schlüssels verifiziert werden.
Beispiel 2. Bob möchte eine Nachricht an Alice schicken und sichergehen, dass diese auf dem Weg nicht verändert wurde. Er verwendet seinen privaten Schlüssel und wendet diesen auf eine Nachricht an um eine Signatur zu erzeugen. Beides übermittelt er an Alice. Mit dem öffentlichen Schlüssel von Bob kann die fehlerfreie Übertragung der Nachricht verifiziert werden.

[3]Vgl. Dietmar Wätjen, 2018, S.73 f.

2.3. ActivityPub Standard

ActivityPub definiert zwei Protokollschichten, sowie Konzepte, Sammlungen und Interaktionen für dezentrale soziale Netzwerke. Eine Protokollschicht ist das Client-zu-Server Protokoll (Social API), um Clients den Zugriff auf einen Server zu ermöglichen sowie zum entgegennehmen von Anfragen. Die zweite Protokollschicht besteht aus dem förderierten Server-zu-Server Protkoll (Federation Protocol), welches den einzelnen Instanzen von dezentralen sozialen Netzwerken den Austausch von Inhalten untereinander gestattet. ActivityPub setzt auf bereits bestehende Empfehlungen des W3C auf, welche teilweise auch von der SWWG entwickelt wurden wie zB. ActivityStreams Core und ActivityStreams Vocab.

Auch andere Technologien wie JSON Linked Data werden benutzt um die Erweiterbarkeit zu gewährleisten. Über neue Ontologien (Vokabulare) können weitere syntaktische Definitionen und semantische Beschreibungen zu den bestehenden hinzugefügt werden[**activityPub**]. Diese Vokabulare können im Kontext des JSON Linked Data Objektes, angegeben werden. Bei ActivityPub wird das ActivityStreams 2.0 Vokabular verwendet welches durch ActivityStreams Vocab erweitert wird.

2.3.1. Bestandteile des Protokolls

Das Client-zu-Server sowie förderierte Server-zu-Server Protokoll können unabhängig voneinander implementiert werden. Ersteres besteht aus einem Client und Server Teil.

In ActivityPub werden Benutzer als „Aktoren“(actors) dargestellt. Diese können nicht nur Personen, sondern auch Applikationen, Organisationen, Gruppen und Services sein[**activityStream**
Jedes Aktoren Objekt muss eine „Inbox“ und „Outbox“, welche geordnete Sammlungen sein müssen, sowie eine ID und ein Typ besitzen[**activityPub**]. Die ID muss global einzigartig sein. Dies kann garantiert werden durch eine Domänen und Protokoll bezogene URI oder IRI wie zum Beispiel „https://example.org/users/alice“oder „https://example.org/users/alice/áŷýà/2“.
Der Typ eines Aktor (z.B. "type": "Create") kann variieren zwischen den fünf oben genannten.

2.3.2. Authentifizierung und Datenintegrität

Für die Authentifizierung und zum sichern der Datenintegrität definiert der Standard keine Mechanismen. Es gibt allerdings „Best Practices“ für die Umsetzung dieser Anforderungen.

Zum einen werden bei der Client-zu-Server Authentifizierung „OAuth 2.0“ Tokens benutzt, zum anderen auf der Server Seite „HTTP“ oder „Linked Data Signatures“zur Sicherstellung der Datenintegrität.

OAuth 2.0

Datenintegrität

„Die Datenintegrität umfasst Maßnahmen damit geschützte Daten während der Verarbeitung oder Übertragung nicht durch unautorisierte Personen entfernt oder verändert werden können. Sie stellt die Konsistenz, die Richtigkeit und Vertrauenswürdigkeit der Daten während deren gesamten Lebensdauer sicher und sorgt dafür, dass die relevanten Daten eines Datenstroms rekonstruierbar sind.“[4]

HTTP Signaturen

Um sicherzustellen das HTTP Anfragen beim Transport nicht verändert wurden, können HTTP Signaturen verwendet werden. Bei diesen wird ein kryptografischer Algorithmus benutzt um

Linked Data Signaturen

Wenn ein Objekt nicht nur vom Client zum Server gesendet, sondern auch zwischen Servern untereinander weitergeleitet werden soll wird zum Sicherstellen der Datenintegrität ein anderes Verfahren benötigt als HTTP Signaturen. Die „Best Practices“ empfehlen für solche Fälle „Linked Data Signatures“. Der größte Unterschied zwischen HTTP Signaturen und „Linked Data Signatures“ besteht darin, welche Daten zum Erstellen der Signatur verwendet werden. Bei HTTP Signaturen sind es die Kopfzeilen. Mit „Linked Data Signatures“ kann auch das Objekt selbst, also der Payload einer HTTP Anfrage, anstatt nur die Kopfzeilen, zum signieren verwendet werden.

2.3.3. Zugehörige Standards und Komponenten

ActivityPub benutzt die ActivityStreams Daten Syntax und das Vokabular. Zusätzlich kann ein weiteres Sicherheitsvokabular[5] benutzt werden um Definitionen zum Bereitstellen eines öffentlichen Schlüssels, Signaturen sowie Verschlüsselten Inhalten u.v.m. zu haben. Am 22 April 2016 hat die „W3C Community Group“ einen Entwurfsbericht herausgebracht. Durch diesen wird neue Syntax und Semantik definiert um Internet basierten Applikationen das Verschlüsseln, Entschlüsseln sowie digitale signieren und verifizieren von verlinkten Daten (Linked Data) zu ermöglichen. Es enthält auch Vokabeln für die Erstellung und Verwaltung einer dezentralen Public-Key-Infrastruktur über das Internet[**security-vocab-linked-data**]. Ein Anwendungsfall ist das holen des öffentlichen Schlüssels eines Nutzers, über dessen Aktoren Objekt, um eine von Nutzer gesendete Nachricht zu verifizieren.

JSON Linked Data ist eine Erweiterung des JSON Formates um verlinkte Daten zu Repräsentieren. JSON an sich, ist ein Format welches im Web häufig Anwendung findet um Daten auszutauschen. Im Kern sind ActivityStreams 2.0 auch JSON Linked Data Objekte. Der ActivityStreams 2.0 Kontext definiert verschiedene Klassen und Eigenschaften, von denen nicht alle benutzt werden. Typische Klassen sind „Activity“, „Link“ und „OrderedCollection“. Ein Beispiel ActivityStreams 2.0 Objekt sieht wie folgt aus:

[4] [**data-integrity**]
[5] Eine Ontologie die Sicherheitsaspekte definiert wie öffentliche Schlüssel, Signaturen u.v.m.

Listing 2.1: Beispiel ActivityStreams 2.0 Objekt

2.4. Fediverse

Als erstes soll der Begriff „förderiertes Netzwerk“ von Förderation hergeleitet werden.

Unter einer Förderation versteht man den Verbund von etwas. Deutschland ist z. B. ein förderierter Bundesstaat, welcher 16 Bundesländern verbindet. Ein Verbund von Netzwerken wird demnach als Netzwerkverbund, oder auch „förderiertes Netzwerk“, bezeichnet.

„Fediverse“ ist ein Kofferwort aus „Federated“ und „Universe“. Historisch gesehen beinhaltete der Begriff nur Microblogging Plattformen die das OStatus Protokoll unterstützen. Mehr zu OStatus **S. 3.2.1**. Mittlerweile beinhaltet das Fediverse mehr als nur Microblogging Plattformen wie Mastodon[6] sondern auch soziale Netzwerke (z. B. GNU Social[7]), sowie „Video hosting“ (PeerTube[8]),„Content publishing“ Plattformen, wie Wordpress, und viele weitere.[**fediverse**]

Im „Fediverse“ dreht sich alles um freie (Open Source) Software anstelle von kommerziellen Produkten. Zudem kann ausgesucht werden welchem Administrator man die Kontrolle über seine Daten geben möchte, anstatt auf eine einzelne Instanz vertrauen zu müssen.[**fediverse**]

indirektes online Zitat!!!

Laut dem Fediverse Netzwerkreport 2018, welcher online zur Verfügung steht, hat sich die Gesamtanzahl der erreichbaren Instanzen von 2.756 auf 4.340 erhöht. Dies entspricht einem Wachstum von 58%. Die Nutzeranzahl ist von 1.786.036 auf 2.474.601 gestiegen (39%). Weitere Details sind im Netzwerk Report nachzulesen. Es ist hinzuzufügen das der Netzwerkreport unvollständig ist und Fehler beinhalten kann.[**fediverse-report**]

[6] https://mastodon.social/about
[7] https://gnu.io/social/
[8] https://joinpeertube.org/en/

3. Analyse bestehender Ansätze

3.1. Vergleich bestehender Implementierungen

3.2. Verwandte Protokolle

3.2.1. OStatus

- OStatus
- Diaspora Federation

4. Entwurf einer Lösung für sichere Server-zu-Server Interaktion mit ActivityPub

4.1. Entwurfsentscheidung

4.2. Technische Architektur

5. Implementierung eines ActivityPub Prototyps

5.1. Server-zu-Server Protokoll

6. Evaluation

6.1. Anwendungsbeispiel

6.2. (Performanzmessungen)

6.3. Disskusion von Vor- und Nachteilen der Lösung

7. Zusammenfassung und Ausblick

A. Anhang

A.1. First Appendix Section

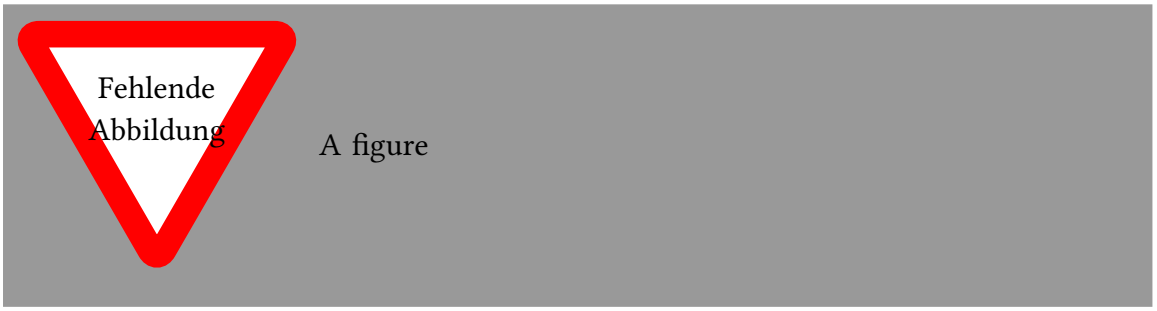


Abbildung A.1.: A figure

...