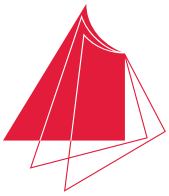


Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Analysis of a Reference Implementation of the ActivityPub Standard with a view on security

Bachelor Thesis of

Armin Kunkel

at the Faculty of Computer Science and Business Information Systems
Subject Area Distributed Systems (DSYS)

Reviewer: Prof. Dr. rer. nat. Christian Zirpins
Advisor: M. Sc. Robert Schäfer

01. December 2018 – 31. March 2019

University of Applied Sciences
Faculty for Computer Science and Business Information Systems
Moltkestr. 30
76133 Karlsruhe

I declare that I have developed and written the enclosed thesis completely by myself, and have not used sources or means without declaration in the text.

Karlsruhe, January 18, 2019

. . . . . .

(Armin Kunkel)

Abstract

English abstract.

Zusammenfassung

Deutsche Zusammenfassung

Contents

1. Introduction

- Justification of this work

Centralization of data and trust in individual instances is ubiquitous today. In the Internet there is a wealth of social networks such as Facebook, Twitter, Google+, Instagram or Pinterest which mostly retain the right to the data you get from their users and last but not least sell this data for advertising purposes. It is also easier for criminals and secret services to access the entire database, since centralised networks usually also have a central database or access point. When the access to this central point is reached, the whole database can be read.

What does decentralized mean? In politics, decentralization „is the transfer of central government tasks to subnational or subsidiary level(s)“[**wikipedia-decentralization-politics**]. In the energy industry, one speaks of „decentralized power generation“if the power is also generated at the places where it is consumed. An example of this would be a hydroelectric power plant that supplies electricity to the surrounding villages or cities[**wikipedia-decentralization-e** In computer science, decentralization means the distribution of data over several independent servers.

By allocating tasks to sub-national or subsidiary levels, the central government level is relieved of its burden and thus has more resources for other tasks. When hydroelectric power plants are built close to villages and towns, there is no need to transport electricity over long distances, which reduces the loss of electricity when it is transported over the power grid. Decentralisation of social networks brings various advantages. One advantage is the scalability of decentralized social networks. By adding more instances, new resources can be made available to the network. Another advantage is that there is no central control body that can be corrupted by criminals, economic lobbyists or government authorities.

The aim of the work is to implement the distributed server-to-server protocol as a prototype and to test the security standards for the ActivityPub protocol recommended by the World Wide Web Consortium (W3C) community. In addition, the work should give an overview of the basics of the protocol and how the relevant components are to be understood. The security standards used relate to the authentication of the client against the server and additionally the server to each other, as well as ensuring the manipulation-free transmission of content.

1.1. Motivation

With central social networks, e.g. Facebook, the company has control over data. Due to decentralization, data remains with the individual instances of the social network. Although the databases in central networks can be distributed and the network can also be decentralized, the data still belongs to one company. In addition, central social networks cannot easily exchange content with other networks. With a protocol like ActivityPub, distributing and accessing content and sharing activities across multiple social networks is made possible.

ActivityPub consists of two parts. The client-to-server protocol, also called „Social API“ , and the promoted server-to-server protocol. Through the ActivityPub W3C recommendation in early 2018 and the Social Web Working Group (SWWG) working group of the W3C and others, the dissemination of the protocol is promoted.

The network effect is a term derived from economics. One example is the telephone network. The more people own a phone, the greater the benefit for each individual phone owner[**network effect**]. Transferred to ActivityPub this means as much as: „The more networks implement the standard, the greater the benefit for a single network and ultimately for individual users“.

Protocols such as „Diaspora Federation and OStatus“ provide access to decentralized social content and enable the publication of social content. The standard recommended in March last year by W3C called „ActivityPub“ was developed on the basis of the knowledge in dealing with the OStatus and Pump.io protocol[**activityPub**].

ActivityPub is like „OStatus“ a protocol for decentralized social networks and is examined in this Bachelor thesis.

2. Basics for the secure implementation of decentralised social networks

This chapter gives an overview of general basics of social networks. It roughly explains what social networks are meant for, highlights the difference between centralized and decentralized social networks, and discusses security aspects.
A cryptography subchapter is then introduced in which the procedures required for secure implementation are explained. It starts with a short introduction to cryptography and then briefly the Rivest-Shamir-Adleman (RSA) procedure and a general description of signature algorithms.
Finally the ActivityPub standard is introduced and classified, components of the protocol are described, the functionality of the client-to-server as well as server-to-server communication and associated standards are briefly explained.

2.1. General principles of social networks

2.1.1. Difference between centralised and decentralised social networks

2.1.2. Security aspects of social networks

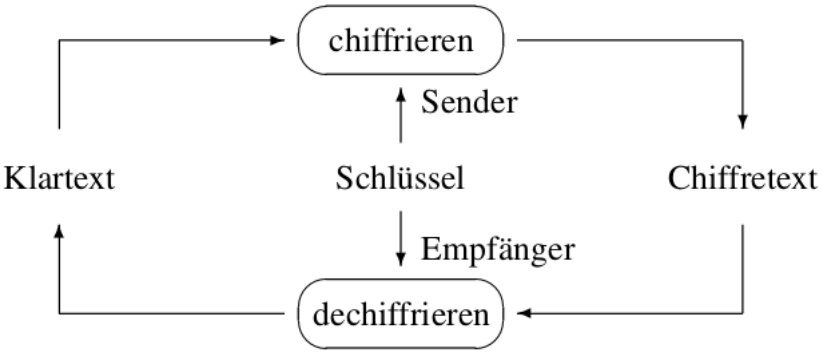
2.2. cryptography

„The term cryptography refers to the science of secret writing“.[1] One speaks of symmetric encryption when a message is encrypted in plain text by the sender with a secret key known to both parties and decrypted by the recipient with the same key.[2]

2.2.1. RSA

Asymmetric encryption is the term used when, instead of having a common key that has to be exchanged in advance, the participants each have a pair of keys (public and private keys). The RSA method is one such asymmetric encryption method developed by the three mathematicians named after it in 1977. The RSA method is probably the most commonly used public-key cryptosystem.
Example 1. The interlocutors Alice and Bob, who both have a key pair, communicate

[1] Dietmar Wätjen, 2018, p.1
[2] Cf. Dietmar Wätjen, 2018, p.1



Quelle: (Wätjen, 2018, S.1)

Figure 2.1.: Symmetric en- and decryption

with each other. Alice encrypts a message text with Bob's public key and sends the encrypted message to Bob. The latter in turn can decrypt the message with his private key.[3]

2.2.2. Signatures

So-called signatures can be used to ensure authenticity. The procedure briefly described above can not only be used to encrypt and decrypt messages, but also to sign them.
Instead of the public key, the private key is used to generate a signature, in this case. This can then be verified with the public key of the corresponding private key.
Example 2. Bob wants to send a message to Alice and make sure it hasn't been changed along the way. He uses his private key and applies it to a message to generate a signature. Both he transmits to Alice. Bob's public key can be used to verify that the message has been transmitted correctly.

2.3. ActivityPub Standard

ActivityPub defines two protocol layers, as well as concepts, collections and interactions for decentralized social networks. A protocol layer is the client-to-server protocol (Social API) to enable clients to access a server and receive requests. The second protocol layer consists of the promoted server-to-server protocol (Federation Protocol), which allows the individual instances of decentralized social networks to exchange content with each other. ActivityPub is based on already existing recommendations of the W3C, which were partly also developed by the SWWG like e.g. ActivityStreams Core and ActivityStreams Vocab.

Other technologies such as JSON Linked Data are also used to ensure extensibility. New ontologies (vocabularies) can be used to add syntactic definitions and semantic descriptions to the existing ones[**activityPub**]. These vocabularies can be specified in the

[3]Cf. Dietmar Wätjen, 2018, p.73 f.

context of the JSON Linked Data object. ActivityPub uses the ActivityStreams 2.0 vocabulary which is extended by ActivityStreams Vocab.

2.3.1. Elements of the protocol

The client-to-server and promoted server-to-server protocol can be implemented independently. The former consists of a client and server part.

In ActivityPub users are represented as „actuators“(actors). These can be not only individuals, but also applications, organizations, groups and services[**activityStreamsCore**]. Each actuator object must have a „Inbox“ and „Outbox“, which must be ordered collections, as well as an ID and a type[**activityPub**]. The ID must be globally unique. This can be guaranteed by a domain and protocol related URI or IRI such as „https://example.org/users/alice“or „https://example.org/users/alice/áŷýà/2“.

The type of an actuator (e. g. "type": "Create") can vary between the five mentioned above.

2.3.2. Authentication and data integrity

The standard does not define any mechanisms for authentication and for ensuring data integrity. However, there are „Best Practices“ for the implementation of these requirements.

On the one hand, client to server authentication uses „OAuth 2.0“ Tokens, on the other hand, on the server side, „HTTP“ or „Linked Data Signatures“to ensure data integrity.

„Data integrity includes measures to ensure that proprietary data cannot be removed or altered by unauthorized persons during processing or transmission. It ensures the consistency, accuracy and trustworthiness of the data throughout its lifetime and ensures that the relevant data of a data stream can be reconstructed.“[4]

If an object is not only to be sent from the client to the server, but also forwarded between servers, a procedure other than HTTP signatures is required to ensure data integrity. The „Best Practices“ recommend for such cases „Linked Data Signatures“. The biggest difference between HTTP signatures and „Linked Data Signatures“ is what data is used to create the signature. For HTTP signatures, these are the headers. With „Linked Data Signatures“ , the object itself, i.e. the payload of an HTTP request, can also be used for signing instead of just the headers.

[4][**data-integrity**]

2.3.3. Related standards and components

ActivityPub uses the ActivityStreams data syntax and vocabulary. In addition, another security vocabulary[5] can be used to have definitions for providing a public key, signatures, encrypted content, and more. On April 22, 2016, the „W3C Community Group“ published a draft report. It defines new syntax and semantics to enable Internet-based applications to encrypt, decrypt, digitally sign and verify linked data. It also contains vocabulary for creating and managing a decentralized public key infrastructure over the Internet[**security-vocab-linked-data**]. A use case is retrieving a user's public key, using its object actuators to verify a message sent by users.

JSON Linked Data is an extension of the JSON format to represent linked data. JSON itself is a format that is often used on the web to exchange data. In essence, ActivityStreams 2.0 are also JSON Linked Data objects. The ActivityStreams 2.0 context defines different classes and properties, not all of which are used. Typical classes are „Activity“, „Link“ and „OrderedCollection“. An example ActivityStreams 2.0 object looks like this:

Listing 2.1: Example ActivityStreams 2.0 Object

2.4. Fediverse

A network of networks is therefore referred to as a network interconnection, or „federated network“.

A promotion is the association of something. Germany, for example, is a subsidised federal state linking 16 federal states. A network of networks is therefore referred to as a network interconnection, or „federated network“.

„Fediverse“ is a suitcase word from „Federated“ and „Universe“. Historically, the term has only included microblogging platforms that support the OStatus protocol. More about OStatus **S. 3.2.1**. Meanwhile the Fediverse contains more than just microblogging platforms like Mastodon[6] but also social networks (e.g. GNU Social[7]), as well as „Video hosting“ (PeerTube[8]),„Content publishing“ Platforms, like Wordpress, and many more.[**fediverse**]

The „Fediverse“ is all about free (open source) software instead of commercial products. You can also choose which administrator you want to give control over your data instead of relying on a single instance.[**fediverse**]

According to the Fediverse Network Report 2018, which is available online, the total number of reachable instances has increased from 2,756 to 4,340. This corresponds to

[5] An ontology that defines security aspects such as public keys, signatures, and more
[6] `https://mastodon.social/about`
[7] `https://gnu.io/social/`
[8] `https://joinpeertube.org/en/`

growth of 58%. The number of users rose from 1,786,036 to 2,474,601 (39%). Further details can be found in the Network Report. It should be added that the network report is incomplete and may contain bugs.[**fediverse-report**]

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. Appendix

A.1. First Appendix Section

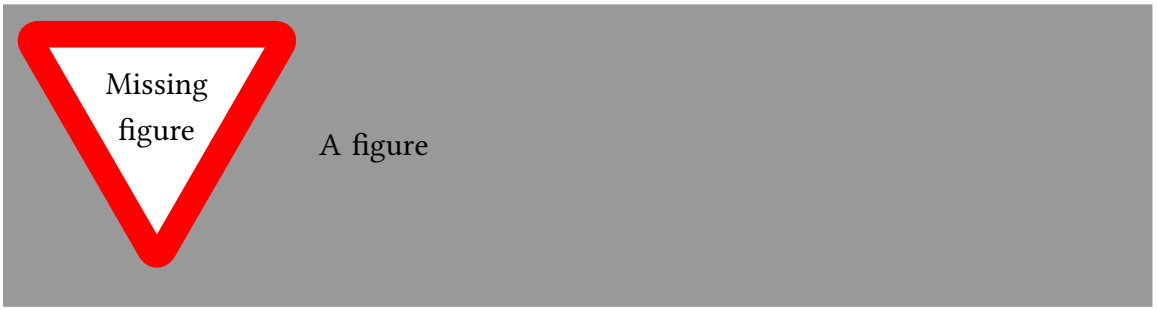


Figure A.1.: A figure

...