VAPE - An autonomous, serverless communication platform honoring privacy and data sovereignty.

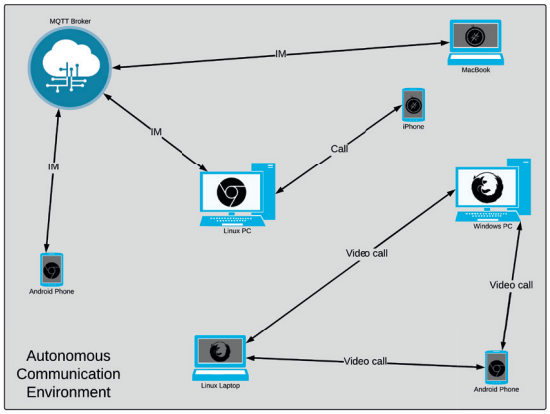
Degree programme: BSc in Computer Science | Specialisation: Distributed Systems and IoT
Thesis advisor: Prof. Dr. Reto Koenig

We think that the current state of communication should be reconsidered. We no longer only have exchanges between humans but more and more the field of IoT takes its place as a worthy partner in communication platforms. Because of that, the amount of data exchanged and its importance is growing by the day. Therefore, we want to provide a secure and decentralized communication platform.

Summary

In a world, where communication has shifted from personal conversations to bytes in the form of text, audio and video, it is important that our privacy is still guaranteed and the user has the data sovereignty. There are many communication systems available, which provide a solution. Unfortunately, most of them are owned by big companies which like to gather user information for own purposes or even sell them.
With this bachelor thesis, we show that communication can still be private and secure without any centralized trust.

To prove our point, we developed a secure, lightweight protocol, which allows instant messaging, audio and video conversations and is extensible to be used for IoT devices.
All communication is end-to-end encrypted and integrity must be ensured.
The platform will be built for human users as well as for machines, more precisely for IoT devices.
Technology wise, open standards should be preferred so that most environments and languages are able to participate.



VAPE Topologie

The protocol is built to work without any centralized server or application.
Clients communicate directly via WebRTC peer connections or indirectly via a signalling service, such as MQTT.
Thanks to a hybrid encryption schema and signatures, even indirect messages are secure and do not leak their content.
Defining the protocol wasn't enough for us, we also wanted to show that it works in the real world, that's why we implemented the protocol as a JavaScript library and built a web application which uses such library.
This web application works in all modern browsers which support WebCrypto, IndexedDB and WebRTC.

Conclusions

We are happy with what we achieved. The VAPEcore library (what we call the implementation of the protocol) provides an API to create different kinds of clients which are based on web technologies.
Furthermore, the protocol is based on open standards, allowing future libraries to be written in most languages. Therefore, the possibilities of VAPE are huge.
As with most projects we had some ups and downs, but in the end, we believe in the protocol and platform we developed and would like to see it grow further.

Joris Baiutti
joris.baiutti@gmail.com

Sascha Patrick Wittwer
sascha.wittwer@bluewin.ch