University of Zurich[UZH]

Department of Informatics

University of Zürich
Department of Informatics
Binzmühlestr. 14
CH-8050 Zürich
Phone. +41 44 635 43 11
Fax +41 44 635 68 09
www.ifi.uzh.ch/dbtg

UZH, Dept. of Informatics, Binzmühlestr. 14, CH-8050 Zürich

Prof. Dr. Michael Böhlen
Professor
Phone +41 44 635 43 33
Fax +41 44 635 68 09
boehlen@ifi.uzh.ch

Zürich, 15. September 2021

MSc Thesis
Topic: Digital Message in a Bottle

The main idea of this project is to build a platform for a covert electronic communication service that works independently of the internet. As we have seen in the past, authoritarian regimes have no difficulties in shutting down parts of the internet to prevent communication (this has recently happened in Iran and in the Kashmir region of India, just to give examples). The goal of this project is to design a system that can be kept running in a scenario in which the internet is shut down. As a consequence, the components of the system should be cheap and fairly easy to set up, run, and maintain. Additionally, we cannot rely on constant connectivity between different parts of the network, so it is not possible to run standard internet protocols. Nevertheless, we want to make sure that messages will eventually spread through the network and will reach the intended recipients. Ideally, the network should offer anonymity, be hard to compromise, and resist attempts to censor content. These last three points are hard to implement, so partial solutions would already be sufficient here. Overall, the project can be broken down into different tasks:

Tasks

1. Low-level infrastructure: This task is about creating the infrastructure to run the network on. Important subtasks are the bootstrapping of an ad-hoc wireless network on devices to create nodes capable of servicing light-client requests in a fault-tolerant way and the deployment of distributed Elixir to serve as a basis to implement network protocols. A short range wireless signal protocol, such as Bluetooth, WiFi, or a similar technology, will be employed as a default protocol to transmit data between devices. The goal is to be able to post a Twitter-like message to the network and sharing it with as many nodes as possible and to build a minimum viable product as a proof of concept, evaluating its strenghths and weaknesses.

2. Communication protocols: once the hardware infrastructure is in place, some robust communication protocol needs to be implemented. This task can be broken down into several subtasks, such as developing message routing strategies, addressing, congestion control, and reliable data storage. As already mentioned, this is not just a matter of deploying standard internet protocols. The goal for this task is to define and test mechanisms for lightweight networking, providing fast and reliable communications.
3. Optional tasks: In addition to the routing, there are a number of security-related issues, such as anonymity, authentication, data confidentiality, and data integrity, to name some examples. It is not expected that all of the security-related issues will be fully addressed in this project (as they could easily make up a project on their own).
4. Write the thesis.
5. Present the thesis in a group meeting (25 minutes presentation).

Supervisor: Sven Helmer (helmer@ifi.uzh.ch)

Start date: 1 October 2021

End date: 31 March 2022

University of Zurich
Department of Informatics

Prof. Dr. Michael Böhlen
Professor