Next-Generation Wi-Fi Hotspots: Network Discovery and Authentication (Bachelor/Master Thesis)

Background

Open Wi-Fi networks are ubiquitous, but using them is cumbersome: For each new location, users must manually identify a suitable network, connect their device and then sign in or accept the terms and conditions. In combination with security and privacy issues, this leads many users to rely on mobile internet access using 4G or 5G instead.

A number of improvements to Wi-Fi collectively called “Hotspot 2.0” or “Wi-Fi passpoint” aim to make Wi-Fi hotspots similarly easy and secure: Using new standards, Wi-Fi clients can automatically scan for suitable access points, connect and authenticate using established credentials. Authentication is performed using either the SIM card or single-sign-on account (e.g. Google or Microsoft account). This strong authentication, in combination with state-of-the-art encryption, offers a significant security improvement over traditional unencrypted hotspots. Because connection establishment is completely automatic, this allows users to remain seamlessly connected even when moving between different Wi-Fi networks. In some cases, this could entirely replace more expensive 4G or 5G mobile networks.

Objectives

The goal of this thesis is to examine the technical aspects of network discovery and client authentication in Passpoint / Hotspot 2.0 networks. To this end, a functioning test setup consisting of Wi-Fi routers, clients and an authentication backend should be developed. Then, the behavior of clients and network components should be evaluated regarding security and privacy.

The main tasks of this thesis are the following:

- Literature review of current work on next-generation Wi-Fi hotspots and their network discovery and authentication mechanisms
- Practical implementation of a working test setup that offers a next-generation Wi-Fi hotspot and allows clients to connect using different authentication methods
- Evaluation of the behavior of client devices, access points and authentication backends
- Documentation of the research process, experimental setup, findings, and challenges encountered during the work

Requirements

Candidates should possess knowledge of networking protocols and communication technologies as well as basic programming skills (e.g. Bash, C, Python). Familiarity with and interest in Linux as well as practical experience with (wireless) network administration are beneficial. Experience with network analysis tools (e.g. Wireshark) and RADIUS servers (e.g. FreeRADIUS) is a plus.

Application Process

All applications must be submitted through the application website INTERAMT:
https://www.interamt.de/koop/app/trefferliste?partner=339
(Abschlussarbeiten Bachelor / Master; Pflichtpraktika)
Carefully note the information provided on the site to avoid any issues with your application.
Your application should include

- a short CV
- a current transcript of records
- the keyword “T3-SC-HS2.0” as a comment

For any questions or further details regarding this thesis and the application process, please feel free to contact ZITiS T3 (t3@zitis.bund.de) or PD Dr. Corinna Schmitt.