Fingerprinting WLAN Access Points for Mitigating Evil Twin Attacks (Bachelor/Master Thesis)

Background

In order to connect to WLAN networks, clients scan for networks in the vicinity and then choose a network that they know based on its name and security settings. Especially for open (unencrypted) networks, it is trivially easy to mimic the characteristics of another access point and thus "clone" the network. Clients that know this network will then be tricked into connecting to it. This is known as an "Evil Twin" attack.

Objectives

This thesis aims to implement and evaluate fingerprinting methodologies for Access Points to mitigate Evil Twin attacks. Various characteristics of the access point (e.g. header information, supported features, timings) and the network's environment (e.g. nearby networks, geolocation) can be used to assess the likelihood of a nearby access point being "real" or "fake". When choosing a network to connect to, this information can be used to reduce the chance of connecting to an evil twin.

Objectives of a possible thesis includes:

- Literature Review: In-depth examination of the current state of research into WLAN Evil Twin attacks, AP fingerprinting and other mitigations
- Mitigation Design: Choice of suitable characteristic(s) to monitor and development of a fingerprinting method to distinguish real and fake APs
- Software Development: Development of an Android application or modification of the underlying Android system to consider fingerprinting results when choosing the network to connect to
- Evaluation: Analyze the performance of the fingerprinting mechanism in distinguishing real and fake networks
- Documentation: Thoroughly documenting the research process, findings, and strategies employed to navigate and resolve challenges encountered during the study.

The exact scope of the project depends on the thesis type (Bachelor/Master).

Requirements

Candidates should be interested in wireless networking and Android development. Ideally, they should possess programming skills in C/C++ and/or Java/Kotlin. Prior experience with Android app development and/or Android system modification is beneficial, but not strictly required. Familiarity with setting up and troubleshooting WLAN under Linux as well as compilation and installation of alternative Android distributions is also beneficial (e.g. custom ROMs like Graphene OS).

Application Process

All applications must be submitted through the application website INTERAMT:
https://www.interamt.de/koop/app/trefferliste?partner=339
(Abschlussarbeiten Bachelor / Master)
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-WLAN-AP-FP" 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.