PKEX protocol Analysis

Meireles Lopes, Steve
steve.meireles.001@student.uni.lu
022148763b

Skrobot, Marjan
marjan.skrobot@uni.lu

September 2024

Secondary Language: German

1 Abstract

In the current day and age IoT is increasingly growing. Most people have interacted with IoT devices in some form. While smartphones are the most prominent IoT devices, many others exist, such as smart fridges, temperature sensors, IP cameras, and more. The more our environment is getting smart, the more people are concerned about the security behind these devices and ask themselves if they really should equip themselves with more devices that could potentially get hacked. This raises the question: What security protocols are used in the communication between IoT devices? Are these protocols secure by design or are there improvements that could be made? To answer these questions, the paper is going to look at the solution "Wi-Fi Easy Connect" from the WiFi Alliance[2][1][4] which is a worldwide network of companies that are responsible for a lot of the certification programs that are used by most of the population for example Wi-Fi 6[3]. The objective of this paper is to analyze the protocols used in the "Wi-Fi Easy Connect" solution with a particular focus on the protocol PKEX which employs a shared Code, Key, Phrase, or Word to establish a secure connection between the communicating devices.

References

[1] WiFi Alliance. *Who is WiFi Alliance?* URL: https://www.wi-fi.org/who-we-are.

[2] WiFi Alliance. *Wi-Fi Easy Connect.* URL: https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect.

[3] Wikipedia the free encyclopedia. *Wi-Fi 6*. URL: https://en.wikipedia.org/wiki/Wi-Fi_6.

[4] Wikipedia the free encyclopedia. *Wi-Fi Alliance*. URL: https://en.wikipedia.org/wiki/Wi-Fi_Alliance.