

PAKE protocols and Decoy passwords

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

Skrobot, Marjan
`marjan.skrobot@uni.lu`

September 2024

Secondary Language: German

1 Abstract

1.1 Scientific:

The scientific question answered in this project will be: How to detect if a password file is in possession of intruders and at the same time prevent phishing attacks? First of all this paper goes into technologies used to alarm the system administrator if an attacker has unauthorized access to the password file. Afterward, it covers how this is combined with PAKE (Password Access Key Exchange) to prevent phishing attacks.

1.2 Technical:

The technical part will be a system that alarms the system administrator of potential attackers having the password file. It uses the technical properties picked up by the scientific part. The project will be written in Python and it will implement PAKE that ensures further security for the password file to prevent for example phishing attacks.