Homework 9

50.520: Systems Security

User Authentication

Question 1

Design and implement a simple version of the HoneyWords system [1]. Users of the system should be able to

- create accounts,
- authenticate to the front-end server by sending their (username, password) pairs.

The system should raise an alarm for malicious logins (i.e., when there is evidence that an incorrect, cracked, password is used). Communication between actors (users, front-end server, and HoneyChecker) should be realized with TCP.

Demonstrate the system and analyze its security. (Keep in mind that an adversary known how your system works internally.)

Question 2

Study how Dropbox stores passwords [2]. Compare security of their solution with the password storage of your operating system.

[1] https://people.csail.mit.edu/rivest/pubs/JR13.pdf
[2] https://blogs.dropbox.com/tech/2016/09/how-dropbox-securely-stores-your-passwords/