PAKE protocols and Decoy passwords

Saturday 6$^{\text{th}}$ January, 2024 - 18:37

Steve Meireles Lopes
University of Luxembourg
Email: steve.meireles.001@student.uni.lu

This report has been produced under the supervision of:
Marjan Skrobot
University of Luxembourg

Abstract—

Index Terms—

1. Introduction

1.1. Overview

Since the invention of personal computers, a username and password combination has been one of the most used authentication methods until today. Even though it is known that it has various drawbacks and weaknesses; including, humans being bad at making up strong and unpredictable passwords which makes it vulnerable to dictionary attacks.

1.2. Related Work

2. Honeywords

3. PAKE protocols

3.1. EKE

3.2. PAPKE

4. SweetPAKE

5. Application

5.1. Design

5.2. Implementation

6. Conclusion

7. References

8. Appendix