HEIG VD HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD

Département des Technologie de l'information
et de la communication (TIC)
Filière Télécommunications
Orientation Sécurité de l'information

Bachelor Thesis

Password Authenticated Key Exchange (PAKE)

Author	**Julien Béguin**
Supervisor	Prof. Alexandre Duc
Academic year	2021-2022

Yverdon-les-Bains, September 24, 2021

Specification

Context

Password authenticated key exchange (PAKE) are very powerful cryptographic primitive. They allow a server to share a key with a client or to authenticate a client without having to know or to store the client's password. For this reason, they provide better security guaranties for initializing a secure connection using password than usual mechanism where the password is transmitted to the server and then compared to an hash. Despite its theoretical superiority, PAKEs are not implemented enough in the industry. Many old PAKE were patented or got broken which might have hurt the adoption of this primitive.

Goals

1. Outline existing PAKE, including the old one. This include SRP, OPAQUE, KHAPE, EKE, OKE, EKE varient (PAK, PPK, PAK-X,), SNAPI and PEKEP. Also look for other less known PAKE.
2. Study in details the main PAKE — EKE, SRP, OPAQUE, KHAPE — and understand their differences.
3. Choose one of the modern PAKE to implement. The choice is based on the properties of the PAKE, the existence of implementations for this PAKE and/or the existence of standards for this PAKE.
4. Design an interesting use case were using a KAPE is more appropriate than using a classical authentication method. The advantages of the PAKE are detailed in the report.
5. Implement the chosen PAKE and the use case using the desired programming language

Deliverables

- Implementation of the chosen PAKE with the use case
- Report containing :
  - State of the art of PAKEs,
  - Description of the use case,
  - Advantages of using a PAKE over a classical authentication method for this use case,
  - Implementation details

Contents

1 | Introduction

2 | State of the art

3 | Conclusion

List of Figures

List of Tables