Une image contenant texte, Police, Graphique, capture d’écran

Description générée automatiquement

Luca Zacheo

luca.zacheo@heig-vd.ch

**CAA – Encrypted File System**

**Mini-Project**

**Résumé**

The goal of this laboratory is to implement a shared encrypted network file  
system

Table des matières

[1. Architecture cryptographique 2](#_Toc153375089)

[1.1 Création de compte 2](#_Toc153375090)

# 1. Architecture cryptographique

## 1.1 Création de compte

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquementActions lorsque le formulaire de création de compte pour un nouvel utilisateur est soumis :

Éléments entrés par l’utilisateur : ***username****,* ***master password***

1. Le ***username*** est haché avec Sha3-256 et tronqué à la moitié pour être utilisé comme sel à la prochaine étape.
2. Le ***master password*** est haché et étiré avec un sel correspondant au ***username*** haché à l’étape précédente en passant par un KDF, ici Argon2Id.
3. La valeur salée sortante du KDF précédent nous donne une **Master Key** de 128 bits
4. La **Master Key** est étirée une fois de plus à une longueur de 256 bits à l'aide KDF basé sur HMAC, HKDF et nous donne la **Streched Master Key**.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquementLa **Master Key** et la **Streched Master Key** ne sont jamais stockées ni transmises au serveur, elles restent côté client.

Génération du **Master Password Hash** :

Avec le ***master password*** entré par l’utilisateur et la **Master Key** générée précédemment à l’étape 3) on va maintenant générer un **Master Password Hash.** En utilisant une fois de plus Argon2Id.

On va donc hacher le ***master password*** avec comme sel la **Master Key.**

Le **Master Password Hash** résultant est lui envoyé au serveur.

Une image contenant texte, diagramme, Police, capture d’écran

Description générée automatiquementGénération de la **Protected Symmetric Key** :

Une clé symétrique de 512 bits (**Symmetric Key**) et un **IV** de 64 bits sont générés avec un générateur de nombres pseudo-aléatoires cryptographiquement sûr (CSPRNG).

La **Symmetric Key** est ensuite chiffrée avec ChaCha20-Poly1305 en utilisant la **Streched** **Master Key** générée précédemment à l’étape 4) comme clé et l’**IV**. La clé résultante est appelée la **Protected Symmetric Key**.

La **Protected Symmetric Key** est la clé principale associée à l'utilisateur et est envoyée au serveur à la création du compte.

Génération de la **Protected Private Key** :

Une paire de clé asymétrique (**Generated RSA Key Pair**) et un autre **IV** sont également générés avec un CSPRNG lorsque l'utilisateur crée son compte.

La **Private Key** générée est chiffrée avec ChaCha20-Poly1305 en utilisant la **Symmetric Key** générée précédemment comme clé et l’**IV**. La clé résultante est appelée la **Protected Private Key**.

La **Protected Private Key** est envoyée au serveur à la création du compte.

La paire de clés générée est utilisée quand l'utilisateur décide de partager ou de consulter des données avec une autre personne.

## 1.2 Log in

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquementActions lorsque le formulaire de connexion est soumis :

Éléments entrés par l’utilisateur : ***username****,* ***master password***