SEC Labo2 Authentication

Autheur: Fabio da Silva Marques

Date: 29.05.2022

Questions

1. What are the advantages of a challenge-response authentication compared to a weak authentication protocol ?

   > Le mot de passe n'est jamais envoyé en clair au serveur, donc impossible de récupérer le mot de passe en interceptant le trafique.

2. In your application, when do you require the user to input its Yubikey? Justify.

   > - Au moment de la création du compte afin de récupérer la clé publique et l'envoyer au serveur
   > - Au moment de la connexion si connexion 2FA activée. De cette façon si un attaquant a récupéré le mot de passe il ne pourra pas se connecter.
   > - Au moment du reset du mot de passe si connexion 2FA est activée. De cette façon si un attaquant a compromis l'email d'un utilisateur il ne peut pas réinitialiser son mot de passe.

3. What can you do to handle Yubilkey losses?

   > On pourrait mettre en place un système de `Shamir Secret Sharing` qui utiliserais des questions secrettes en tant que "shares" pour récupérer la clé privée de la yubikey (comme vu en cours de CAA).

4. An attacker recovered the challenge and the associated response (in the password authentication). How does this allow an attacker to perform a bruteforce attack? What did you implement to make this attack hard?

   > En récapitulatif l'attaquant a en ça possession: le sel du mdp, un challenge en clair, le hash du challenge. L'attaquant ne connais donc pas la clé pour générer le hash du challenge mais il peut la bruteforcer car il s'agit du hash du mdp. Avec toutes ces informations il peut essayer de bruteforcer des mots de passe en les hashant à l'aide sel pour obtenir la clé pour le challenge et ensuite hasher le challenge jusqu'à trouver la bonne clé. Pour rendre cette attaque la plus lente possible on utilise argon2 pour hasher le mot de passe, ce qui permet d'augmenter le temps nécessaire au calcul d'un hash et ainsi augmenter le cout d'une telle attaque.

5. For sending the email, what are the advantages of using an application password?

   > Premièrement ça permet de ne pas publier les crédentials sur un repo dans le cas ou on fait du versioning avec github par exemple.
   > Ensuite ça permet de laissser la possibilité a chaque utilisateur d'avoir ça propre configuration/credentials.
   > Pour finir ça permet de séparer tout ce qui est configurations de la partie logique du code.

6. In the Yubikey, what is the purpose of the management key, the pin and the puk?

> - Management key: permet de modifier les configurations de la yubikey
> - pin: permet de dévérouiller la lecture de la clé privée
> - puk: permet de réinitialiser le pin