Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Secure Coding

Laboratoire 2

Authentication

Auteurs:

Soulaymane Lamrani

Responsables:

Alexandre Duc

Nathan Séville

29 mai 2022

Question 1

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

Premier avantage, le mot de passe n'est pas envoyé au serveur, lorsqu'il est rentré par l'utilisateur, il reste sur le client. Donc pour quelqu'un qui écouterait la communication entre le client et le serveur ne verrait pas le mot de passe transiter, dans un canal chiffré ou non.

Deuxième avantage, un challenge généré aléatoirement est envoyé au client, donc chaque tentative d'authentification voit un challenge différent.

Au final, on laisse assez peu de visibilité à un attaquant potentiel, les données n'étant pas en soit critiques.

Question 2

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

1 À l'enregistrement

Car il est demandé dans la consigne du laboratoire d'enregistrer une YubiKey lorsqu'un utilisateur cherche à créer un nouveau compte. Comme on veut utiliser cette YubiKey, le compte a le 2FA activé par défaut, il va donc avoir besoin de cette clé pour faire des opérations sur son compte.

2 À l'authentification

Si le 2FA est activé, il va être demandé à l'utilisateur d'entrer le PIN de la YubiKey pour signer le challenge afin qu'il puisse être vérifié par la YubiKey enregistrée côté serveur pour valider s'il s'agit bien de la bonne personne avec la bonne YubiKey.

3 À la réinitialisation du mot de passe

De la même manière que pour l'authentification, on veut pouvoir être sûr qu'il s'agisse de la bonne personne qui voudrait changer son mot de passe. Comme on est dans un cours de sécurité, on veut plus que juste un token envoyé par email.

On pourrait imaginer demander à l'utilisateur de s'authentifier une fois la réinitialisation du mot passe effetuée, mais avec une YubiKey, un accès à un email et le token reçu, je considère qu'on a suffisamment d'élément pour décider qu'il s'agit bien de la bonne personne.

Question 3

> What can you do to handle Yubilkey losses?

En regardant dans la FAQ de yubico[1], voilà ce qu'on peut trouver

What happens if I lose my YubiKey?

We at Yubico always recommend you to secure your account with an additional YubiKey, please see the section above named "Is it important to have a Spare Key?". This additional YubiKey can be used as a spare key in case your primary YubiKey is misplaced or stolen. If you do not have an additional YubiKey added, it is recommended to have another form of 2FA added to your accounts. Please note, if you do end up being locked out of your account, you will need to contact the service for help with account recovery.

Donc une des solutions serait d'en avoir deux. C'est d'ailleurs l'une des recommandations qui est faite à la question de *Is it important to have a Spare Key*.

Ensuite, il est important de pouvoir regagner accès au compte afin de *dé*-associer la YubiKey pour qu'elle ne puisse plus être utilisée.

[1] https://www.yubico.com/ch/setup/yubikey-5-series/

Question 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?

S'il possède le challenge et la réponse associée, il lui faudra encore avoir les fonctions de hachage utilisées pour le mot de passe et la génération du HMAC.

En passant une série[2] de mot de passe dans la fonction de hachage correspondant, il devra utiliser ce résultat dans une deuxième fonction de hachage utilisant le mot de passe haché et le challenge. C'est ce deuxième résultat qu'il devra comparer à la réponse associée au challenge pour vérifier s'il a trouvé le bon mot de passe.

Pour empêcher ce type d'attaque:

1. Argon2 a été utilisé pour hacher le mot de passe, ralentissant les attaques par brute force.
2. L'utilisation d'un HMAC avec SHA256 pour éviter les collisions.
3. Une politique de mot de passe stricte nécessitant une lettre minuscule, une lettre majuscule, un chiffre, un caractère spécial et une longueur de 8 à 64 caractères.
4. L'utilisation d'un challenge de 128 bits généré aléatoirement.

[2] Série de mot de passe venant d'un dictionnaire de mot de passe « courant » ou un algorithme éventuel de génération de mot de passe suivant des critères que l'attaquant aura décidé (parce que toutes les combinaisons, à moins d'avoir un ordinateur quantique, lui prendra un temps théoriquement impossible à atteindre).

Question 5

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

Liste non exhaustive des avantages d'une application password d'un point de vue de la sécurité:

- Peut empêcher un attaquant de gagner l'accès à l'entièreté du compte comme cet application password ne peut qu'accéder au email.
- Composé de 16 caractères généré automatiquement, donc en avoir une pour chaque client.
- Pas besoin de retenir ce mot de passe.
- Peut facilement être enlever en cas de compromission de l'application cliente.

Pour ce qui est d'un point de vue « logistique », cela nous évite d'avoir à faire un serveur email, l'authentifier et le mettre en marche s'il s'agit juste de faire des tests (et la consigne indique que ce n'est pas trivial, donc je vais faire confiance aux bonnes intentions de l'enseignant[3]).

[3] pas tapé

Question 6

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

Tableau reprit la documentation[4] yubico:

Action	Require MGM	Require PIN	Require PUK	Notes
Generate key pair	x			
Change MGM	x			Require a new MGM
Change retry counters	x	x		Yubico extension. Reset PIN and PUK to defaults
Import private key	x			
Import certificate	x			
Set CHUID	x			
Reset card				Requires both PIN and PUK to be blocked
Verify PIN		x		
Sign data		x		
Decrypt data		x		
Change PIN		x		Requires a new PIN
Change PUK			x	Requires a new PUK
Reset PIN (unblock)			x	Requires a new PIN

[4] https://developers.yubico.com/PIV/Introduction/Admin_access.html

1 Management Key

Il s'agit de la clé qui est nécessaire aux tâches de gestion et administration de la clé, telles que généré et importer des clés et certificats dans les emplacements PIV.

2 PIN

Les fonctionnalités utilisateurs sont gardées par un PIN, qui doivent être saisie par l'utilisateur afin d'effectuer des opérations de clé privée.

Il peut être long de 6 à 8 caractères alphanumériques. S'il est entré faux 3 fois consécutifs, le PIN est bloqué et devient impossible d'être utilsé.

3 PUK

Pour PIN Unblocking Key et possède les même restrictions que le PIN. Si le PIN et le PUK sont les deux bloqués, ils peuvent être réinitialisé avec la management key.
