Alec Berney

SEC – 25.05.2022

Authentification

Labo 2

# Questions

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

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

### 3. What can you do to handle Yubilkey losses?

### 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?

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

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