Task 3.1

a)

1. Biometric authentication[[1]](#footnote-1)

The biometric authentication is based on the human unique biological characteristics. The most popular might be fingerprint scanner, voice recognition and iris scanner; still there are many more unique characteristics. E.g. a fingerprint scanner is found nearly on every device nowadays, like smartphones or notebooks. It is widely known that the fingerprint of every human is unique. So the fingerprint scanner creates a digital likeness of the fingerprint and authenticates the human by mapping it to the registered fingerprint image.

+ Fast authentication, only have to use one finger

- Loss of finger

Popular product: Apple IPhone (5s and newer)

2.

b)[[2]](#footnote-2)

Googles offers an account confirmation in 2 steps for their google accounts to users. The first step is the normal password authentication. The only restriction on the password is that it has to be at least 8 characters long. The second step provides an authentication mostly over the user’s telephone. Therefore a 6 long digit code is send to the telephone via SMS, phone call or a specially designated app. A login is only possible, if both steps are performed. Alternatively the second step can also performed offline, by downloading a list of backup-codes which can be used in case the telephone is not accessible. Another option is to use a Security Key with the open standard “FIDO Universal 2nd Factor (U2F)”. Usually this security key comes within an USB HID and can be added to a user’s google account. To authenticate it is only necessary to pluck in the security key.

Advantages:

* Even if the password of step 1 is thieved, your account can be still save through the second authentication step
* The security of your account doesn’t depends as much on the password strength, thus weakly chosen passwords don’t have a high severity
* Attackers have to gain access to a physical object (telephone, security key) to pierce through the second authentication phase

Disadvantages:

* For the second authentication phase, only a 6 long digit code is send to your device. It wouldn’t take long to crack this code through a brute force attack
* Attackers can also gain access to physical objects like the registered security key, or the telephone. Therefore the attack isn’t based any longer on a technical, thus a physical level
* The account authentication takes more time
* More circumstances when losing the telephone

1. Global source for this segment: “http://searchsecurity.techtarget.com/definition/biometric-authentication” [↑](#footnote-ref-1)
2. Global source for this segment: “https://www.google.com/landing/2step/#tab=why-you-need-it” [↑](#footnote-ref-2)