Password & Security Research

24/09/2014

Stephen Tate

CO600: JustHealth
Supervisor: Yang He

Version 1.5
Last saved by: Ben McGregor
Last saved on: 29/03/2015

Contents

1.0 Introduction

This document will look into different types of passwords and 2 Factor Authentication and discuses what the best possible security is for you applications. Since our app is holding sensitive and personal data we need to ensure that the app is as secure as possible from attacks and hackers but also secure on each patients/ carers smart phone/ tablet or laptop to stop unwanted people being able to open the app if they were to get hold of the phone.

We have many different options when it comes to the password protection:

- Enforcing a password on each device when the app is downloaded
- Enforcing a password on the app when it is opened each time
- Storing the username and enforcing a 4 digit pin when you open the app
- 2 factor authentication with a Google authenticator

Also when it comes to the password options there are a variety of different types:

- Pin number
- Swipe pattern
- 6 digit characters
- Face recognition

2.0 Research

From our research and speaking to both patients and carers a main requirement of our health app are the security and the protection of the data.
This is because it stores very personal and private data about our patients, which they do not want, shared around or to be liable to attacks.
We also feel as a group this application needs to be safe and secure so we have decided to make sure our application has two-factor authentication.

2.1 Two Factor Authentication (2FA)

'Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code'
http://searchsecurity.techtarget.com/definition/two-factor-authentication

2FT allows us to add an extra step to our login screen to ensure the data behind is more secure. If we were not to have this, you would enter your username and password and then you would be logged in, single authentication. 2FA makes the login process more secure.

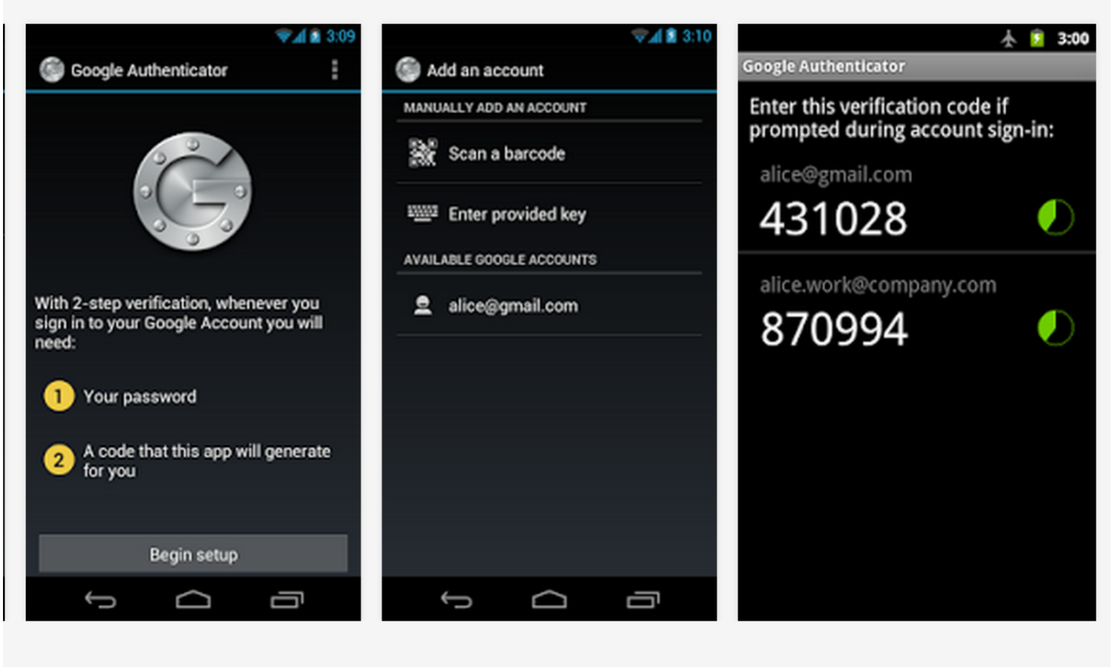
Many big companies such as banks already use 2FA to ensure as much security protection as possible. For example you have physical bankcard and then you also have a security question, pin number or automatically generated number to allow you to log in to your online bank. Twitter also uses 2FA along with Facebook and Linkedin.

"Twitter made the decision to use SMS [to deliver its second factor] because it makes sense from their position," said Jon Oberheide, chief technology officer of Duo Security, which uses apps to prove identity.
http://www.cnet.com/uk/news/two-factor-authentication-what-you-need-to-know-faq/

2.1.1 Google Authenticator

Google authenticator generates a 2FA code directly on your phone. It allows you to be able to verify who you are and protect your account from hijacking by adding another layer of security. This is done by implementing a standard time-based one-time password algorithm.
Google authenticator has over 5,000,000 installs and is supported on any android device 2.2 and up. It is also available of both your computer and mobile device.
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_GB

http://www.howtogeek.com/129014/how-to-use-google-authenticator-and-other-two-factor-authentication-apps-without-a-smartphone/



With 2-step verification, whenever you sign in to your Google Account you will need:

1 Your password

2 A code that this app will generate for you

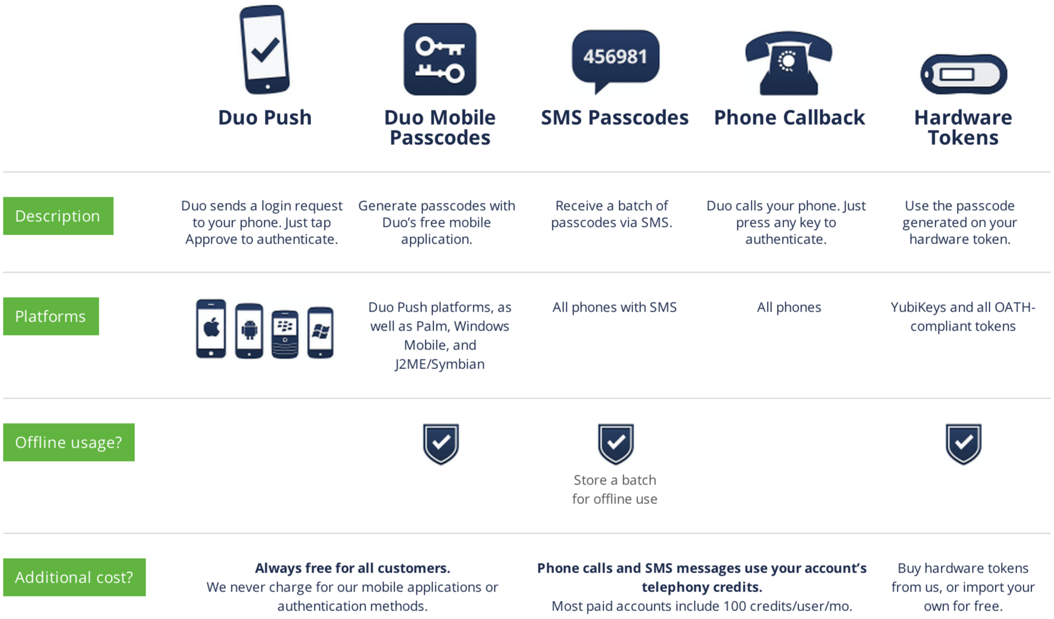
Enter this verification code if prompted during account sign-in:

alice@gmail.com
431028

alice.work@company.com
870994

2.2 Duo Security

Another form of 2FA is Duo. This is a cloud-based so no software to install and also offers a safe and secure 2FA method. This is available on all platforms and offers different types of authentication such as SMS passcodes, phone callback and hardware tokens.



	Duo Push	Duo Mobile Passcodes	SMS Passcodes	Phone Callback	Hardware Tokens
Description	Duo sends a login request to your phone. Just tap Approve to authenticate.	Generate passcodes with Duo's free mobile application.	Receive a batch of passcodes via SMS.	Duo calls your phone. Just press any key to authenticate.	Use the passcode generated on your hardware token.
Platforms		Duo Push platforms, as well as Palm, Windows Mobile, and J2ME/Symbian	All phones with SMS	All phones	YubiKeys and all OATH-compliant tokens
Offline usage?		✓	✓ Store a batch for offline use		✓
Additional cost?	**Always free for all customers.** We never charge for our mobile applications or authentication methods.		**Phone calls and SMS messages use your account's telephony credits.** Most paid accounts include 100 credits/user/mo.		Buy hardware tokens from us, or import your own for free.

https://www.duosecurity.com/product

2.3 Apple's 2FA

Apple also offers 2FA to help secure their customers Apple ID's against hacking. However, since this is only available on apple devices and we developing an android application we have not research this any more.

2.4 Passwords

When looking at password options

- Pin number
- Swipe pattern
- 6 digit characters
- Face recognition

We have decided to not restrict our user to a specific one. This is because our target audience is people with chronic health problems; this consequently means they could have a disability and struggle using a specific password option. Also some users may not like to have a password to access their phone.

3.0 Conclusion

From our research of passwords we have decided to ensure our app is downloaded with 2FA. This will be a password to log into the application Google authenticator. We have decided to work with this because it is the most effective for android, free to use and easy to incorporate into our web and mobile application. Duo security is a very effective method of 2FA however, since it is not free and not specifically built for android we have decided not to use this method.

We have also decided that the application will have the option to turn the Google Authenticator off at the risk and liability of its user.