Iphone Pin Password Unsecured

I. Introduction

Technology has become imbued in our everyday lives. Humans are overwhelmingly dependent on their technological devices. These devices perform a wide range of actions such as finding information, interpersonal communication, and other purposes of entertainment and expression. Even though small, and compact, these devices are able to hold an unquantifiable number of private and confidential information. Such information includes digital currency. With applications such as Apple Pay, PayPal, and Zelle, this information can be accessed by merely bypassing a user's device password.

The most popular and widely used password scheme is the knowledge-based scheme, which is further subdivided into two subcategories; graphical-based and alphanumeric character set based (text-based). [2] We commonly use Personal Identification Number (pin) for our passwords. For iPhone, it commonly uses a 4 number pin, with longer characters being possible for a user. For their security, after multiple attempts, the device will be locked out. The device gives a timer until the user can be able to put in their password.

However, a flaw is that the pin password can be easily bypassed. Despite the popularity of blacklists and the positive impact on textual passwords, our results show that currently employed PIN blacklists are ineffective against a throttled attacker, in both the enforcing and non-enforcing setting.[1] This is a significant flaw due to the security issue that it can bring up. Guessing is then limited (or throttled) to, e.g., just 10, 30, or 100 attempts in a reasonable time window, such as a few hours[1]. In these few hours, it can induce a malicious attack on the victims. Many people already signed to accounts, keep password information on their devices, and use these devices as way to make payments.

II. Proposed method

The method that I chose to implement in order to help increase the security of the iPhone pin password is to add a two-factor authentication feature. The idea is to create different types of passwords that the user would have to authenticate before unlocking their devices.

The passwords would use a pin and a graphical password. Graphical passwords are useful since these systems have been shown to improve memorability without sacrificing input time or error rates while also maintaining a high resistance to brute force and guessing attacks.[3] The user would be able to set up a graphical password by selecting four images out of a selection of twenty images. The graphical password would also randomize the image positions in order to help secure the password from an individual who is memorizing the positions of the images.

III. Future plan

A. Week 1 [Jan 23 - Jan 28]

Investigate more relevant researches for this topic.

B. Week 2 [Jan 29 – Feb 4]

Using other different type of password to see which would be best

C. Week 3 [Feb 5 – Feb 11]

Implement the password systems and connect to pin password

D. Week 4 [Feb 12 – Feb 18]

Conncet password to pin and having a simulationn of the system

E. Week 5 [Feb 19 – Feb 25]

Try to use other common attack to bypss the system to test the security

F. Week 6 [Feb 26 – Mar 4]

Compare previously received data from pin password to tow factor autenication system.

G. Week 7 [Mar 5 – Mar 11]

Sample users data with the system

H. Week 8 [Mar 12 – Mar 18]

Create different graphs and charts for the final presentation from user data

I. Week 9 [Mar 18 -Mar 25]

Prepare the final presentation slide.

REFERENCES

[1] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth and A. J. Aviv, "This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 286-303, doi: 10.1109/SP40000.2020.00100.

[2] M. Ali et al., "A Simple and Secure Reformation-Based Password Scheme," in IEEE Access, vol. 9, pp. 11655-11674, 2021, doi: 10.1109/ACCESS.2020.3049052.

[3] A. Bianchi, I. Oakley and H. Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 380-389, June 2016, doi: 10.1109/THMS.2015.2487511.