IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10482

"J-Script Plug-in" (Android Pattern Lock Simulator)

Mr. Santosh Divekar[1], Atharva Bhosale[2], Hrishikesh Kanade[3] Neha Raut[4]

Sakshi Sardar[5], Atharva Ingale[6]

Lecturer, CO, AISSMS's Polytechnic, Pune, Maharashtra, India[1]

Student, CO, AISSMS's Polytechnic, Pune, Maharashtra, India[2-6]

ABSTRACT: Pattern lock has been widely used in smartphones as a simple and effective authentication mechanism, which however is shown to be vulnerable to various attacks. In this paper, we design a novel authentication system for more secure pattern unlocking on smartphones. This project is written in J-script and click are automatically recognized by the code and no external configurations are required. Android pattern lock is still popularly used for mobile user authentication. Unfortunately, however, many concerns have been raised regarding its security and usability. User-created patterns tend to be simply structured or reduced to a small set. Complex patterns are hard to memorize. Input patterns are susceptible to various attacks, such as guessing attacks, smudge attacks, and shoulder surfing attacks. Our basic idea starts from turning the lock pattern into public knowledge rather than a secret and leveraging touch dynamics. Users do not need to create their own lock patterns or memorize them. Instead, our system shows a public pattern along with guidance on how to draw it. All the user needs to do for authentication is to draw the pattern as shown. For adversaries, the above-mentioned attacks are rendered useless by this new mechanism. Specifically, we study how to generate the public patterns and how to perform authentication. You have probably seen this on a touchscreen smartphone you have 9 dots and you have to draw a pattern. It works great: drawing a shape on a small touch screen is far easier than typing on those small keyboards AND far easier to remember too. Once you've got used to it, typing passwords in general gets pretty annoying A proof of concept project illustrating the use of the Android Pattern Lock Screen inside a HTML

Keywords: "J-script", "Android", "Smartphone", "HTML", "Pattern Lock", "9 dots

I. INTRODUCTION

Graphical passwords, like the Android Pattern Lock, are a popular security mechanism for mobile devices. The mechanism was proposed as an alternative to text-based passwords, since psychology studies have recognized that the human brain have a superior memory for remembering and recalling visual information. This thesis aims to explore the hypothesis that human characteristics influence users' choice of graphical passwords. A collection of 3393 user-created patterns were analysed in order to examine the correlation between people's choice of pattern and their characteristics, like hand size, age, gender and handedness. This thesis first gives a detailed summary of related research on graphical passwords. Then it shows how an online survey was used for collecting user-selected passwords and information about the respondents. Lastly, the thesis explains how the data was analysed in terms of length and visual complexity in order to gain further insight in users' choice of passwords. Although the data could not provide significant evidence to accept the hypothesis, the results show that password strength significantly varies between gender, age and IT experience. Additionally, analysis of all the collected patterns shows a significant bias towards the selection of pattern starting position.

Patterns created in the training mode can be as valid as the other pattern types collected later in the survey. The patterns created in training mode might be the first patterns that pop into the respondent's mind, hence avoiding respondents to trying to overcompensate as a cause of being under pressure. As far as this research know, there are not found any research on how people think when asked to create a password or being asked to give away a password. It is believed that asking people to "give away" 45 a password or pattern will introduce the effect of people overcompensating by creating longer passwords than typically created.

As you might be aware that it's a pretty popular feature on Android devices to have a pattern lock. You can set a pattern lock for your device which gets unlocked only by matching it again. We've tried to replicate the same for the web, so that we can have fun for some time. This can as well be used to authenticate your website.

The pattern in now impossible to crack, even the FBI couldn't crack it. That is why we have introduced it in place of passwords in the web sites.

Touch and click are automatically recognized by the code and no external configurations are required. Creates lock patterns for use with Android's built-in pattern lock.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10482

II. LITERATURE SURVEY

1. Sometimes passwords are difficult to be remembered if they are lengthy, there are many reasons why the password can be replaced with a pattern like if they are alpha-numeric they are difficult to remember, user can forget his password if it lengthy and not easy to remember as well as typing on those small keyboards become pretty uninteresting when you have an option.
2. Standalone JavaScript library to transform a standard password input box of a HTML form into a 9-dot pattern lock. Targeted at mobile web applications where drawing a pattern on the touchscreen is far easier than typing in a password. Works on every major desktop and mobile browser.
3. The usability of the survey was being tested before starting collecting data for different purposes. First, when sending out the survey, there is no much room for changing the layout and content of the survey. The layout and content should be looking the same for all respondents. A change in the formulation or a change in the layout can cause respondents to interpret a question differently. Second, the survey is in a non-controlled environment, meaning that knowing who the participants are and where they are from are not known. The questions and layout need to be created as universal and as intuitive as possible. The questions, the flow, and the graphical elements should be intuitive across different countries and cultures. The usability testing is divided in two main parts: usability testing in a controlled environment and usability testing in an uncontrolled environment. Beside the specific usability tests performed, it has also been performed testing on the selected icons as well as the wireframes created in the preliminary work. A summary of usability test of the icons will be provided in this section. The usability test performed on the wireframes provided in Appendix A resulted in the first implemented version being tested in this study.

III. REQUIREMENTS

When addressing the difficulties of collecting patterns, it is important to define requirements for the survey application. This section will walk through a list of requirements specified for the survey. Each requirement are being described in detail below.

R1: The survey should be able to stand for all commutation to the respondents: One-way communication
R2: The survey should be considered as trustworthy: Trustworthiness
R3: The survey should be implemented on a technical device reflecting the environment of the Android Lock Pattern: Environment of use
R4: The survey should be easy to understand and easy to complete: Complexity and length
R5: The survey should be visual appealing: Visual appearance
R6: The survey should be provided easy navigation between the questions: Navigation
R7: The survey should provide high security: Security

IV. ACTION/PROJECT PLAN AND DISCUSSION

Firstly, you have to open the file index.html with any of your default browsers .You will be presented with a 9-dot android like pattern. You have to record the pattern.Try drawing a correct pattern using mouse or your fingers (for touch screen devices). If you draw a correct pattern then, press unlock button an alert will be displayed as access granted.If the pattern is wrong then access is denied, you have to redraw the pattern

Pattern Creation Time

- **(a)** Gives the pattern creation time in seconds for the three pattern types. By looking at the average creation time for patterns, patterns created for bank accounts have the highest creation time of 9.42 seconds while patterns created for smartphones have an average creation time of 8.24 seconds.
- **(b)** shows the average pattern creation time in seconds for respondents experienced with the Android Unlock Pattern. The graph reveals that both patterns created for shopping account and banking account are not affected by the participants experience with the Android Unlock pattern.

Pattern Length

- **(a)** summarizes the average nodes selected to form a pattern for the each distinch pattern type. The average length is 5.54, 5.40, and 5.92 for patterns created for shopping accounts, smartphones, and bank accounts, respectively. The patterns created for bank accounts have a higher average length than patterns created for shopping and smartphone. The numbers from the graph also show that patterns created from smartphone has the smallest average pattern length. The difference in average pattern length for patterns created for

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

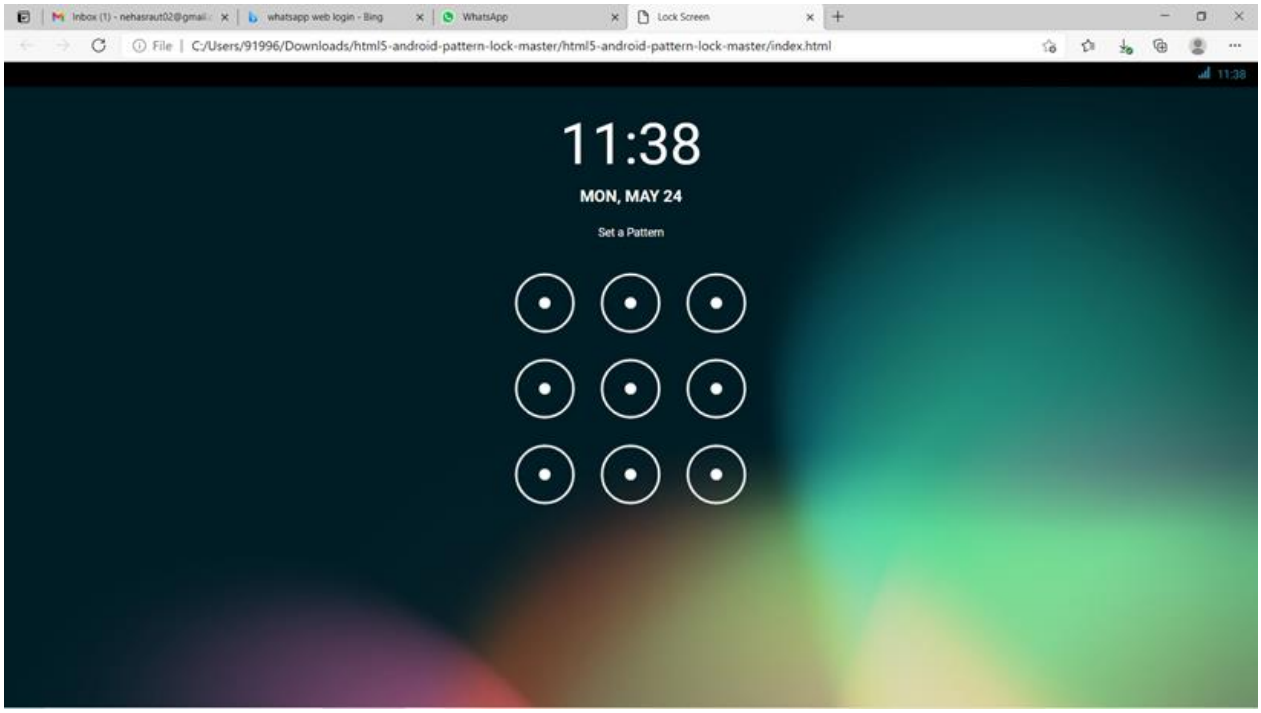
DOI 10.17148/IJARCCE.2021.10482

smartphones and banking accounts are on average 0.52 nodes. Patterns created for shopping accounts are slightly longer than patterns created for smartphones but constitute not a significant difference between the two types.

(b) is a pattern length distribution indicating what pattern length that are more often selected by the population

Association Elements

An association element is something a person know or recognize, and can used as an element to ease the process of remembering a password. This is a known technique used by users when creating alphanumeric passwords and PIN codes. Alphanumeric passwords are often known being created containing personal information like names and dates for support the creator in remembering the password. The same strategy are being observed for PIN codes where the use of codes forming a date often occurs. The dataset collected in this research are being scanned for patterns corresponding to association elements. By going through the alphabet, it was found 12 types of patterns corresponding to the visual representation of letters from the alphabet. Out of the 12 letters, 9 patterns had a significant number of appearances. Figure 5.6 shows the 8 most common patterns having the same visual representation as letters from the alphabet. Beside the letters C, L, M, N, O, S, U and Z, letters like G, J and W also appeared in the data set. By iterating through the sequences corresponded to letter, 385 out of 3393 patterns in the dataset matched a letter. The number of patterns matching a letter from the alphabet constitutes 11.4% of the collected patterns.



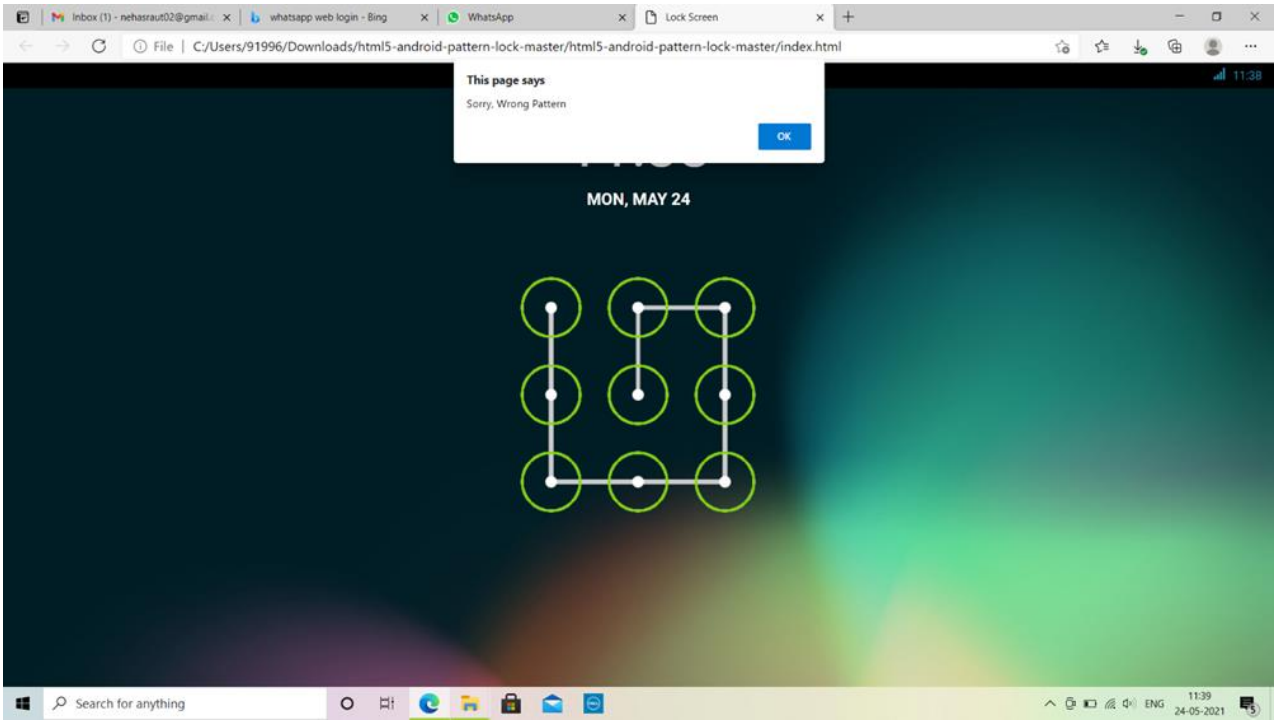
IJARCCE

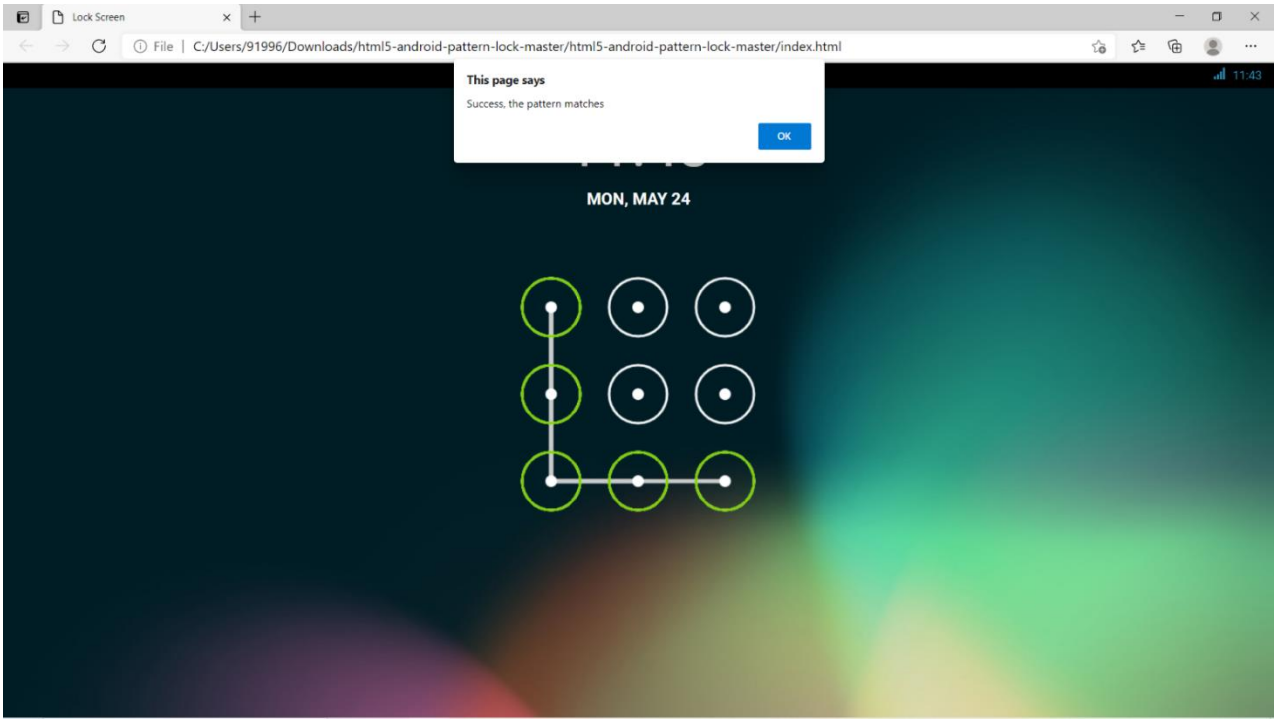
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10482





IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10482

VI. CONCLUSION

The main objective of the project is to replace the password field in the web page with pattern lock just like the android pattern lock. I had taken a wide range of literature review in order to achieve all the tasks, where I came to know about some of the products that are existing in the market. The portability of the application has been achieved by using some of the latest JSSE technologies. I will implement these functionalities using Canvas api's in future. As a result, the product has been successfully developed in terms of extendability, portability, and maintainability and tested.

REFERENCES

[1] S. Uellenbeck, M. Durmuth, C. Wolf, and T. Holz, ¨ "Quantifying the security of graphical passwords: the case of android unlocks patterns," in Proceedings of the 20th ACM Conference on Computer and Communications Security, 2013.
[2] Z. Sroczyński, ''Pattern lock evaluation framework for mobile devices: Human perception of the pattern strength measure,'' in Proc. Int. Conf. Man–Mach. Interact. Cham, Switzerland: Springer, 2017, pp. 33–42.
[3] D. Kunda and M. Chishimba, ''A survey of android mobile phone authentication schemes,'' in Mobile Networks and Applications (On-Line). 2018, pp. 1–9.
[4] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, and P. Gasti, ''HMOG: New behavioral biometric features for continuous authentication of smartphone users,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 877–892, May 2016.
[5] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in Proceedings of the 9th ACM Symposium on Usable Privacy and Security, 2013.
[6] R. C. Atkinson and R. M. Shiffrin, "Human memory: A proposed system and its control processes," The psychology of learning and motivation, vol. 2, 1968