Gesture based Hybrid Authentication for Smart Device

Mr Mahesh R. Makwana [1] Director Dev M. Rathod [2]
[1] PG Student [2] Director
[1] Computer Engg. Department, Gujarat Technological University. Ahmedabad
[2] Prediqnous Cyber Security and I.T Intelligence Ahmedabad City.

Abstract---Smartphone security is a great concern for security of its information. More than 70% of Smartphone users keep their valuable information like Files, Pictures, Calendars and many more in their smartphone and it has raised the question of security. Smartphone manufactures companies give different kind of authentication methods for security purpose of smartphone. But, as far as security is concerned, still it's not secure as it is supposed to be. Most of the manufactures like Nokia, Samsung, and Apple etc. manufacture smartphone products with gesture based authentication along with other simple techniques. This project presents a new hybrid method for smartphone security. This hybrid method may consist of Tapping, Gesture and Sensor based technologies for authenticating mobile device users. My primary study showed me that it this new technique may be slower and more error prone than existing techniques. However, I believe with practice it could get faster and more accurate. Also, most users will be comfortable and all of them will feel more secured while using this new technique.

Keywords: gesture, security, password, authentication, pattern, touch screen lock.

I. INTRODUCTION

Now a day cell phone is not only for calling purpose but so many things included in that. Because of waste usage, cell phone becomes smart with the help of new technology. Now a day everybody have cell phone and it contain user's sensitive information. This way security of smart device is much important. Legacy approaches to user authentication have not transitioned well to the new world of mobile computing. Complex alphanumeric passcodes can be easily forgotten, are difficult to enter on small touch screen devices, and can be easily observed and replicated by unauthorized on-lookers (also known as 'shoulder surfing' somebody's password) [9]. And because many employees will also use their mobile device to capture personal photos or to check their personal email, there is growing resentment over having to enter a complex passcode just to access a mobile device. Fixmo and Lockheed Martin are solving this challenge with the new Fixmo Secure Gesture technology powered by Mandrake SG™, an innovative solution for strong user authentication based on a unique and easily remembered touch screen gesture [2][3].

In many embodiments, a process to use a combination of gestures including glyphs entered in a touch screen (That may include multi touch or single touch capable touch screens), sounds captured by a microphone, and movements registered by motion sensors may be used in place of a standard text-based password for use with a mobile computing device. The term "gesture" will be applied to any user entered combination of glyphs, movements and sounds that the user enters into the mobile computing device through input devices. A gesture-based signature can be verified as performed by the authentic user (i.e., authenticated) through a series of calculations. Once the gesture-based signature has been authenticated, the gesture-based signature can be substituted for a correct text-based password that is then input into a password field to gain access to a software application or website. Logic to perform gesture identification, comparison, and verification processes may be present within the mobile computing device. This process does not require significant changes to application or website infrastructure.

Smartphones are famous for their versatility in a single day a smartphone may be a barcode reader, a satellite navigation system, a contactless wallet, an email or social network client, a Wi-Fi hotspot, and be used to make a phone call. Given the growing importance of smartphones, we believe it is important to assess the privacy and security risks of these devices. We stress that the risks should be balanced against the potential benefits of smartphones. A description of the many potential benefits in terms of, for example, cost-savings, increased efficiency and a better quality of life is outside the scope of this report [1].

Smartphones have a rich cocktail of features an array of sensors, multiple radio and gigabytes of storage as well as network interfaces and powerful processors [15]. They are often within a meter of their owners 24 hours a day. Actually smartphones have already realized many aspects of the vision of ambient intelligence that covers, for example, providing augmented reality applications, many of the security and privacy issues raised in the context of ambient intelligence apply to smartphones as well[3].

Many respondents are really exposing themselves to great risk by connecting those unlocked mobile devices to sensitive online accounts and applications.

II. BACKGROUND

There are various authentication techniques available in market but each technique has its own importance, advantage and disadvantage.

A. Text-based password:

In case of numeric password four digit passwords have 10,000 possibilities. It is too less so easy to crack by using brute force attack. Many people use same alphanumeric password in his various account so if one password is hack then all other account will lost its security. In old phone gesture recognize facility was not available but now many people are using smartphone and it has gesture recognize facilities like touch screen, camera, mobile accelerometer and gyroscopes etc. [14].

B. Pattern lock:

Now a day's most people are using smartphone and they want a quick access of their device. For that reason by using touch screen we can go toward to gesture. Gesture-based authentication method gives us quick access and provides

large possibilities but it's depending on design of method. Android 3 × 3 matrix lock has 3, 89,112 possibilities. Some method design such way that it need so much calculation and work with large data because of this it consumes much processing power for efficient working [1][2].

C. Hybrid method for authentication:

We are proposing hybrid method for smartphone authentication. We are thinking about hybridization of numeric and gesture-based authentication. This method also apply only touch screen device.

III. III. PROPOSE TECHNIQUE

Our propose method works only for touch screen device. We have virtual numpad with ten digit 0-9, CANCEL and EMERGENCY CALL button. Gestures on each button have five possibilities tap, left, right, up, or down. We have 0-9 key with five gesture so 10 × 5 = 50 unique values and password length is four. Then 50^4 = 62, 50,000 [2].

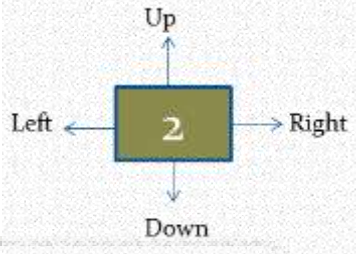

Fig. 1: Each key have five gesture tap, up, down, right, left

A. How it works:

1) *Discontinuous gesture drawing:*

Assume your password 1→3→7→9→ (1 left 3 left 7 left 9 left) then we cannot continuously draw the gesture but we draw the gesture four time on four button and remember we must draw the line at least 0.5 cm long.

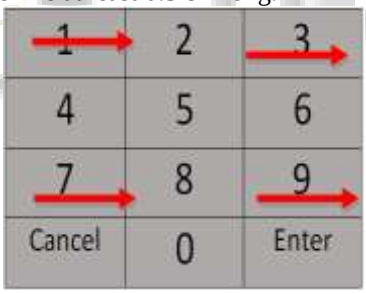

Fig. 2: Example of work as only gesture

2) Continuous gesture drawing:

Assume your password 4→5→8↓9→ (1 left 3 left 7 down 9 left) then we can continuously draw the gesture but here button 5 and button 8 have two gesture so in this case only first gesture will accepted means button 5 have Left and Down two gesture but Left will accepted because it is first drawn on button.

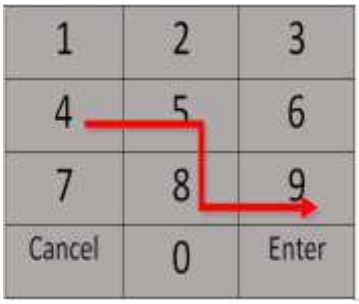

Fig. 3: Example of work as only gesture

B. Threshold length:

If user drowns small gesture on key so we consider as tap gesture to overcome this problem we have to decide some threshold level. There are two possibilities either it is fix value or it is depend on touch screen size of device. We propose 0.5 cm fixed threshold level. So if user drawn gesture greater than 0.5 cm then that is consider as gesture otherwise it is consider as tap.

It might be possible user will not draw gesture on four direction but he prefer any corner then we must decide rule for that also I propose that angle between 0̊ - 89˚ consider as Left, 90˚ - 179˚ consider as Up, 180˚ - 269˚ consider as Right, 2670˚ - 359˚consider as Down. So now user can draw gesture in any direction it is automatically consider as either up, down, left or right.

IV. RELATED WORK

When user try to unlock device at that time each gesture has two points based on these two points we have to calculate the direction of the gesture for that purpose we have to design logic. First of all find difference between last point and first point then compare absolute value of these two points if x is greater than horizontal movement if y is greater than vertical movement occurred. Now we decide direction. If x≥0 in horizontal movement than Right otherwise Left direction. If y≥0 in vertical movement than Down otherwise Up direction.

Fig. 4: Create password

In above figure we can see the digit with direction for testing purpose but finally dot (.) or asterisk (*) will be displayed in password bar.

V. DISCUSSION AND FUTURE WORK

The hybrid technique yielded a lower entry speed and higher error rate compared to the digit lock technique. We expected this as gestures takes more time than taps. Results also showed that most of the input errors were committed while performing the gestures. Two additional factors contributed to the hybrid technique's lower accuracy rate. First, it was often hard for users to memorize the randomly generated passwords. Thus, they often mistyped the numbers or miss performed the gestures. This phenomenon may reduce in real life scenarios when users will select their own passwords. Second, the gestures performed on the bordering keys often ended on the bezel, which caused misrecognition. However, we noticed that after some time users realized that they have to complete the gestures within the screen and the gestures do not have to be that long (≥0.5 cm). This

encouraged them to initiate and complete the gesture within the keys. We did not observe any significant effect of learning, other than on entry speed for gestures, most probably due to insufficient data. However, prior studies showed that users' gesture input performance improve with practice [12]. Encouragingly, most users found the new technique comfortable, and all of them felt more secured while using it.

A. Gesture.key file:

In some case data is more important than device. When user lost his smartphone at that he is varied about sensitive data and personal information etc. (Ex- Project manager or CEO's phone have very sensitive data) so loss of smartphone is does not mean but sensitive data will not goes on wrong hand this thing is important.

Android smartphone pattern password store in gesture.key file and it is in encrypted form. Normally we cannot access that directory. Anybody can access your device if three requirement are satisfy 1) Physical access 2) Rooted phone 3) USB Debugging enable. Have three rooted phone give permission to that directory and USB debugging also enable. Just connect your smartphone to computer and delete gesture.key file and reboot device. Now you can access smartphone without correct pattern.

B. Propose storage method:

We will simply store in text form like 4→5→8↓9→
This password will stored as 4L5L8D9L Then apply SHA1 hashing algorithm. Hash is a single direction function so reverse process is too much difficult and finally we achieve strong security.

Now we know that if these three requirements physical access, rooted phone and USB Debugging enable will be satisfy then our device come under risk and at that time we think about the location of gesture.key file. Device does not understand first option physical access but it is understand second option Rooted phone and third option USB Debugging enable if device found second and third option then automatically give alert to user Please disable USB Debugging. We cannot un-root phone quickly but we can disable USB Debugging quickly.

If somebody want to use USB Debugging facility and he has rooted phone then generate alert for internet connection now gesture.key file remove from device and store it at remote location. When user try to unlock device only hash value will be sent and if correct then give device access.

VI. Conclusion

We presented a new tap and gesture hybrid mobile user authentication scheme that augments four gestures to the conventional digit lock technique. It provides in total 6250000 unique four-symbol password combinations. In beginning phase this technique relatively slower and more error prone. However, most users found the new technique comfortable to use and all of them felt more secured while using it. We study on False Acceptance Rate and False Rejection Rate. False Acceptance Rate is very dangerous for device security and because of False Rejection Rate efficiency will be decrease so it should balance for batter performance. In future we will analyses and if needed then change threshold length 0.5 cm. Users' entry speed and accuracy improve with practice.

References

[1] Bassam Sayed, Issa Traore, Isaac Woungang and Mohammad S. Obaidat, Fellow. "Biometric Authentication Using Mouse Gesture Dynamics" IEEE systems journal, Vol. 7, no. 2, June 2013
[2] Prof. V.J. Kadam, Taj Mohammad A. Raheman, Ajinkya Ajagekar, Sushant B. Patil "Shoulder Shuffling Free Graphical Locker for Android Graphical Pattern Lock with Text Support for Android Devices" In International Journal of Advanced Research in Computer Science, March 2013.
[3] Kailas I Patil, Jaiprakash Shimpi "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices" In International Journal of Innovative Technology and Exploring Engineering Volume-2, Issue-4, March 2013
[4] G. Niranjana' Kunal Dawn "A Novel Gesture Based Graphical Authentication Using Bounding Box and Corner Detection Algorithm" Dept. of computer science and engg, SRM University. 2012 IEEE
[5] Nikhil Arun Pogale, Deepak Ganpatrao Rasekar, Prof. Aditya P. Bakshi "A Secure Authentication Using Graphical Password Authentication System: GPAS" In International Journal of Advanced Research in Computer Science, May 2013
[6] Seongil Lee, Kyohyun Song, and Jiho Choi "Access to an Automated Security System uses Gesture-based Passwords", 2012 15th International Conference on Network-Based Information Systems.
[7] Karthik, K. Varalakshmi, Dr. S. Ravi "A File Authentication System Using Hand Gesture Passcodes",
[8] 2013 In International Journal of Emerging Technologies in Computational and Applied Sciences.
[9] Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister and Nasir Memon "Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices" May 2012, Austin, Texas, USA
[10] Behavio Mobile Security (White Paper) "Applying the BehavioSec technology for Multi-layered Mobile Security"
[11] David Rozado "Using Gaze Based Passwords as an Authentication Mechanism for Password Input" In ICT Centre – CSIRO
[12] Dr. Gail-Joon, Jeong-Jin Seo, Ziming Zhao, Arizona State University. "On the Security of Picture Gesture Authentication"
[13] Zhai, S. and Kristensson, P.-O. Shorthand writing on stylus keyboard. In Proc. CHI '03. ACM (2003), 97-104.Sonia Chiasson, Alain Forget, Robert Biddle, P.C. van Oorschot, "Patterns in click-based graphical passwords" In School of Computer Science, Carleton University, June 2008.
[14] Harshith.C, Karthik R. Shastry, Manoj Ravindran, M.V.V.N.S Srikanth, Naveen Lakshmikhanth "Survey on Various Gesture Recognition Techniques for Interfacing Machines Based On Ambient Intelligence "Department of Information Technology Amrita Vishwa Vidyapeetham Coimbatore, International

Journal of Computer Science & Engineering Survey Vol.1, No.2, November 2010.

[15] Mohammad A. Alia, Adnan A. Hnaif, Hayam K. Al-Anie, Abdelfatah Aref Tamimi "Graphical Password Based On Standard Shapes", Department of Computer Information Systems, Faculty of Science and Information Technology –Al Zaytoonah University of JordanVol 4, No. 2;Feb 2012.

