TIMER INDUCED PATTERN SECURITY FOR CRITICAL SYSTEM

Sumran S[1], Venkat A P[2], Vijayarangan S G[3], Vijay Krishna N[4], B.Kiran Bala[5]

[1-4]Final Year, Bachelor of Engineering, Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India.
[5]Assistant Professor, Department of computer science and Engineering, K.Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India.

ABSTRACT

There have been a number of systems proposed to secure our mobile phones. It includes passwords with alphabets and numbers and latest development called patterns. But the pattern can be easily eavesdropped by noticing the hand movement of the user even though the pattern may be set to be invisible leading to insecurity. But in our system we have overcome it by merely including a timer to each dot. The user can choose any kind of pattern from the matrix and also can choose any amount time to each dot until which the finger has to be idle in that. The number of dots on which the timer is to be activated is purely user's choice - it can be one or all or some of the user desired pattern. The timing to each pattern is also completely user's wish - different timings to different dots. As there is to be a limit to everything, the time can be maximum up to five seconds, contemplating about emergency situations. This prohibits third parties to lurk into patterns and access one's personal data maliciously as one cannot concentrate on both the timing and the pattern. With this there will be no weak passwords. It only requires the user to have a strong memory power to remember the timings with the pattern.

1.INTRODUCTION

Smartphones and tablets have become an essential part of our everyday life. The main advantage of these devices is that they are not bounded by time or place. They are designed to be portable, convenient, entertaining, and support people in their daily activities. They could be used for communication, socialising, and most recently m-banking, m- payments and m-health, among numerous other purposes. Mobile devices are ubiquitous and in most cases, are the gateway to accessing numerous user applications. The activities carried out on the devices result in storage of personal and highly sensitive data about their users and people associated with them. Thus, making it essential to restrict access to the devices by implementing a reliable and convenient access control to prevent unauthorised access and misuse. Several schemes have been used such as; PIN, Password, Pattern and most recently, Biometrics.

The devices face numerous challenges ranging from memory shortage to external threats. Pfleeger and Pfleeger in categorised threats to a system into human and nonhuman. Nonhuman threats are caused by phenomena that are out of human control such as; component failure (e.g. processor chip). However, human threats are directed to cause harm to the system and the user (in some cases). Such threats include; data theft or corruption, misuse of device and unauthorised access. Traditional methods such as; PIN and Password are the widely used authentication methods and they do not seem to go away soon. The extent to which they secure devices have been significantly studied [1, 10, 11, 12].

Two of the measures of assessing the security are a) practical assessment based on the resistance to threats and b) theoretical assessment based on the measure of password space and randomness. No system is secured if an imposter knows the password, else, they would have to keep guessing until they find the correct password and the point is to make it as difficult as possible in terms of time and effort. Pattern Unlock were introduced as an alternative to PIN and Password because they are graphical, more usable and memorable. In Pattern Unlock, the user is presented with a 3x3 grid and the password is how the nodes are connected. Grid arrangements and unlock conditions by Android restrict access to some nodes, for instance, the topleft node cannot be connected to the bottom-right node unless via the middle node.

Further, this affects the number of usable patterns based on lengths. For example, a pattern of length 5 will only have 7,152 valid patterns available. Even when the length is 9, the total patterns available is 140,704.These numbers are much smaller compared with 6-digit PIN (106) and 5-digit Password (365).

We conducted and present in this paper, a comprehensive study on the security of pattern unlock authentication on both theoretical and practical measurement levels. Further, the characteristics of the patterns were evaluated in terms of actual nodes distribution, lengths and pattern space to understand what is viable for the users. The correlation between users and the patterns they choose was also analysed. For instance, are the patterns chosen based on association with something personal (name, alphabet or number).

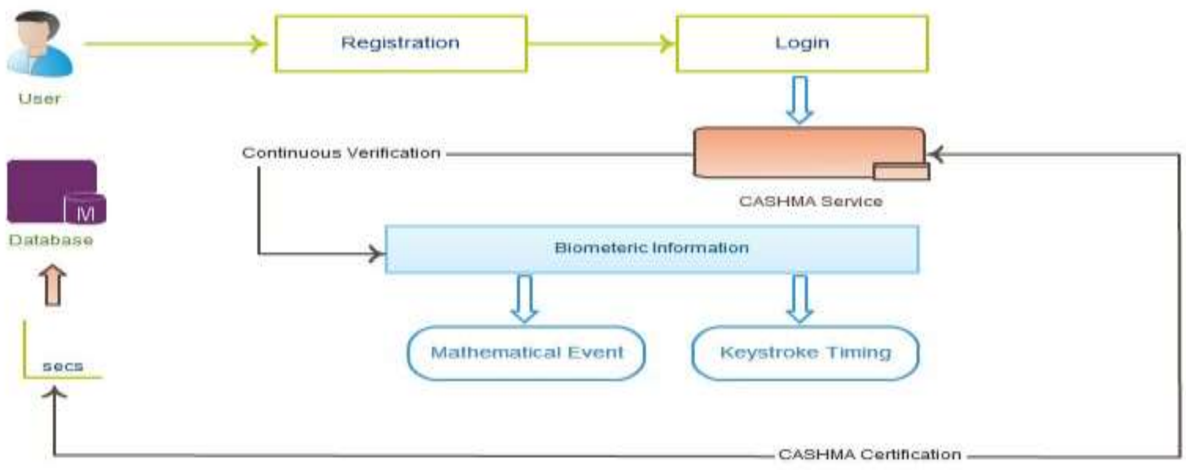
2.PROPOSED SYSTEM

To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multimodal biometric continuous authentication.

We proposed CASHMA for usable and highly secure user sessions is a continuous sequential a single biometric modality at once is presented to the system multimodal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently.

The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data.

2.1Architecture Diagram



3.MODULES DESCRIPTION

3.1 Account Creation

The registration module allows the user to enter the personal details of his/her for future reference of authenticating the user by verifying the details and allowing them access the data in the database. This script is used for register and login to website using PatternLock. The design is completely responsive Very simple steps to use Login and Register on your website.

3.2login Verification

The Login Module is a portal module that allows users to type a user name and password to log in. This module can be placed on anymodule tab to allow users to log in to the system.The user details and the security pattern which the user provided in the registration phase is verified in the login module.Only if the provided data and the pattern matches the data in the database, the user is allowed to enter the system.

If the given details does not match even one of the data the user will not be allowed to enter the system and access the data.

3.3keystroke Dynamics

The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. Keystroke dynamics is a behavioral biometric.

It measurements available from almost every keyboard can be stored even recorded to Dwell timing of key pressed and the time between "key up" and the right next "key down". Keystroke dynamics can be used for authentication, then it is used mostly together with user ID / password credentials as a form of multifactor authentication**.**

Another use is as a very specific form of surveillance. There exist software solutions which, often without end-users being aware of it, track keystroke dynamics for each user account. This tracking, historization of keystroke dynamics is then used to analyse whether accounts are being shared or in general are used by people different from the genuine account owner.

Reasons for such an implementation could be verification of users following security procedures (password sharing) or to verify that no software licenses are being shared (especially for SAAS applications).

The saved keystroke timing data is then processed through a unique and specific neural algorithm, which determines a primary pattern for future comparison.

3.4 Cashma Authentication

Password collection by keystroke and related malware is increasing at an alarming rate. The attacker can make them stop working heuristics to impute missing latency values or only selected latencies from a victim, to generate desired text or system commands.

It provides a trusted path to the user for obtaining authentication credentials. Although generally stateless, it can store temporary session keys and may optionally act as a password manager. This page could be completely under the control of spyware, or it could be controlled by an online site in-the-middle.

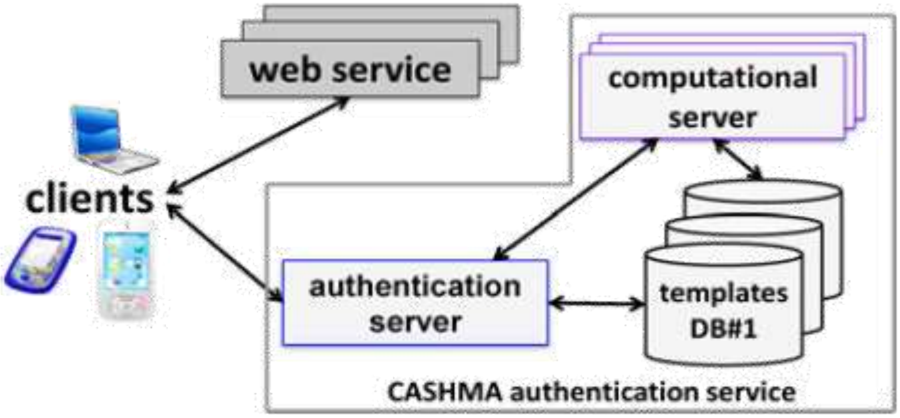


Figure.1-CASHMA Authentication service

An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax.[1] It is the most important layer of protection needed for secure communication within computer networks.

A Protocol has to involve two or more parties and everyone involved in the protocol must know the protocol in advance.All the included parties have to follow the protocol.A protocol has to be unambiguous - each step must be defined precisely.A protocol must be complete - must include a specified action for every possible situation.

3.5 Misspelt Word

Calculate the rate of Misspelt word when the user types the text wrongly. This performs the step when the number of times each of the words whose misspellings are being identified was found in the entire text body is counted and recorded. The attacking can be found then this recorded rate match with the original latency of the text. The attack can be found and mitigated when the calculated score does not match with the original record of data.

3.6 Continuous Verification

It provides a perfect match (or mis-match) between the continuous verification system and the authentication. Each of the keystrokes is calculated as per the system de-signed. Continuous verification, some keystrokes typed during the verification phase may not have reference signatures in the template. It happen because the enrollment text used for building the template may not have all the letter pairs present in the 26-by-26 matrix. This problem can be resolved by performing verification using letter pairs that are common to the template and the verification text.

One way to perform session tracking is to leverage the information that comes with User authorization. When a web server restricts access to some of its resources to only those clients that log in using a recognized username and password. After the client logs in, the username is available to a servlet through getRemoteUser()**.**

When use the username to track the session. Once a user has logged in, the browser remembers her username and resends the name and password as the user views new pages on the site. A servlet can identify the user through her username and they're by Track her session.

The biggest advantage of using user authorization to perform session tracking is that it's easy to implement. Simply tell the protect a set of pages, and use getRemoteUser() to identify each client. Another advantage is that the technique works even when the user accesses your site form or exists her browser before coming back.

The biggest disadvantage of user authorization is that it requires each user to register for an account and then log in each time the starts visiting your site. Most users will tolerate registering and lagging in as a necessary evil when they are accessing sensitive information, but it's all overkill for simple session tracking. Other problem with user authorization is that a user cannot simultaneously maintain more than one session at the same site.

3.7 Keystroke Timing

We present the keystroke timing information, if the typed the text this is text, the attacker records a series of timestamps time when was pressed, (time when was released), and so on. The participants were allowed to make spelling mistakes, typographical errors and if they chose, could correct them using Backspace or Delete keys. The key-stroke data collection software provided for typing copy and self texts. The results additionally show that effective keystroke forgeries can be created with as low as 20 to 100 characters of text and keystroke timing information.

A timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Every logical operation in a computer takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input.

4. CONCLUSION

The pattern lock mechanism provides high security and is the most acceptable authentication method for most devices that consists of sensitive data.It resides between security and users comfort.Although it provides high security the pattern can be easily traced by bruteforce method.To enhance the security of the pattern lock method the timer was added and proved to be efficient in a way that only the pattern is trackable but not with timer.Even the use of shorter,obvious patterns that consists of minimum number of dots can be efficient enough to secure the data.

REFERENCES

1. Nasiru Ibrahim; Harin Sellahewa,"Touch gesture-based authentication: A security analysis of Pattern Unlock" , International Conference on Identity,Security and Behavior Analysis (ISBA),2017

2.Anwar Ur Rehman; Muhammad Awais; Munam Ali Shah "Authentication analysis using input gestures in touch-based mobile devices" , 2017 23rd International Conference on Automation and Computing (ICAC),2017

3.Muhammad Shahzad; Alex X. Liu; Arjmand Samuel ,"Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures" , IEEE Transactions on Mobile Computing,2017

4.Patchara Pattanakimhun; Nopporn Chotikakamthorn; Winyu Chinthammit,"Interactive public display using mobile web client" , 2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE),2017

5.Ahmed Ramadan; Hamed Hemeda; Amany Sarhan,"Touch-input based continuous authentication using gesture-level and session-level features" , ,2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),2017

6.V. Balaji; K. S. Kuppusamy ,"Towards accessible mobile pattern authentication for persons with visual impairments",International Conference on Computational Intelligence in Data Science(ICCIDS),2017

7.B.Kiran Bala, A Novel Approach to Generate a Key for Cryptographic Algorithm, Journal of Chemical and Pharmaceutical Sciences, Special Issue 2: February 2017, Pages 229-231.

8.B.Kiran Bala, A Novel Approach to Identify the Micro calcification Images, Journal of Chemical and Pharmaceutical Sciences, SpecialIssue2: February 2017, Pages 190-192.

9.B.Kiran Bala, J Lourdu, Multimodal Biometrics using Cryptographic Algorithm, European Journal of Academic Essays,2014, pages 6-10

10.Bala B. K, Kumar A. B. The Combination of Steganography and Cryptography for Medical Image Applications. Biomed Pharmacol J 2017;10(4).

11.B.Kiran Bala, Biometrics for Mobile Banking, International Journal of Technology and Engineering System, 2011, Volume 2, Issue 1,Pages95-97.

12.B.Kiran Bala, R.Sasikumar, Identification Of Cancer From The Mammogram Images By Using Frequency Domain Approaches,International Journal of ChemTech Research, April 2017, Volume 10 No.5.

13.B.Kiran Bala, T.m.nithya, Remedy For Disease Affected Iris In Iris Recognition, International Journal of Research in Engineering and Technology, November Issue 2012, ISSN: 2319 – 1163, page No. 332-334.

14.B. Kiran Bala and R. Sasi Kumar, Different Variety of Tomato Cultivation without Soil by Using Internet of Things Research, Biosci. Biotech. Res. Comm. 10(4): 802-804 (2017).

15.Bala B.K, Audithan S, Wavelet and curvelet analysis for the classification of micro calcification using mammogram images, 2 nd International Conference on Current Trends in Engineering and Technology, 2014.

16.Kiran Bala B, Audithan S, Kannan G and Raja K, Frequency Domain Approaches for Breast Cancer Diagnosis, Australian Journal of Basic and Applied Sciences, 10 (2), 2016, 93-96.