Authenticating Clients without using their Login IDs through Mind Metrics

D. B. K. Kamesh*, K. Rama Krishna and J. K. R. Sastry

Department of Electronics and Computer Engineering, K.L. University, Vaddeswaram - 522502, Guntur District, Andhra Pradesh, India; kameshdbk@kluniversity.in, kurapati438@gmail.com, drsastry@kluniversity.in

Abstract

Background/Objectives: The main objective of this paper is to provide a novel method of identification and authentication of a user through a process of enhancing the password level protection to provide authorised use of the resources hosted on the WEB. Methods/Statistical Analysis: The authentication process that uses mind metrics has been implemented within ARM7 Micro controller which is made to act as central server. The process of authentication and the implementation of the same have been explained through an architectural diagram. Software which has been written using KEIL IDE is burnt into a Micro controller and the implementation of an authentication process has been implemented through a GSM device connected to a Micro controller. Findings: A novel approach that considers a Personnel secret token known as mind metrics has been presented. The server sends across the mind metrics to the user after completing the identification phase and the user from then uses password and mind metrics to carry secured communication between the user and the server. Applications/Improvements: The method has been implemented both as a software and hardware solution. The software solution has been implemented within a GSM application for enabling text message notification.

Keywords: ARM, Authentication, KEIL IDE, Key Loggers, Login systems, Mind Metrics

1. Introduction

Theft identity is an attack done by intruders to steal the legitimate information of the user. The stolen legitimate information is used to perform a wide range of malign activities. Now-a-days the most common way used by the user to get access to their secured information is through authenticating using usernames and passwords. The identification and password should be entered by the user to access information and perform the tasks that they intend. To keep the password protected from an attacker, the password should adhere to some rules determined by the server e.g. minimum length of the string, use of capital and special characters etc. Regrettably the main disadvantage in hard-to-crack password is remembering it by the user. Many users choose their password close to their private life, making it easy for the attackers to easily crack the passwords. Many users write their passwords on notepad files which can be easily intercepted by the attackers. The breaching of the password is easy when a user logs on to unsecured web sites. To counter these drawbacks many authentication methods have been presented which could provide partial protection to the user.

User identification followed by verification is one of the most commonly used logical validation mechanisms that recognise a user within a computer network, system, website, software, and internet etc. Each user has a unique identification regardless of the scenario in which the context of a user arises. A user may use different types of Login IDs that include an email address, mobile number, user name etc. The Login IDs are used by the user for many purposes and therefore become inefficacious to keep them a secret. It is easy for an attacker to access the Login IDs and therefore can compromise on the passwords. At present there are many attacking systems which reveal the secret information some of which include Brute force attack, Phishing, Rainbow Table Attack, Key Loggers, Guessing etc.

* Author for correspondence
Authenticating Clients without using their Login IDs through Mind Metrics

in seconds. Guessing only happens when the user is known to the attacker intimately and the attacker will be able to guess the information using the information that he knows such as date of birth, date of joining etc. Attackers can also use the combination of social engineering and guessing to fetch password from the user.

- **Brute Force Attack**: In this method, the assailant try every possible combination of numbers, letters, special characteristics and alpha-numeric combinations till the right combination of password is matched with the user. It is a very long process and it takes more time as it depends on the complexity of the password.

- **Rainbow Table Attack**: A rainbow table is a huge pre-computed list of hashes for every possible consolidation of characters. The most familiar uses hashing algorithm in web database to store password is MD5. Password hash is a password that will be processed through mathematical algorithms and transformed into something which is not recognizable. A hash is a way of encryption. If the password is hashed once, there is no way to get back the original string from the hash string. In these attacks hashed characters are used as passwords.

- **Phishing**: It is the most earliest and easy method used by attackers to hack an account details. In this method, attacker send counterfeit pages of websites like fake online banking and social media pages to the victim. If the user unknowingly logs in with his details, all the secret information is accessed by the attacker.

- **Key Loggers**: This attack occurs when the user Logins into their account from the cyber café or from other computers. In this method the attacker send key logger or rat to the victim. This allows monitoring everything done by the user by the attacker and moreover attacker can also control the victim's computer.

Figure 1 correlates the ordinary password-based system, which is very much vulnerable to the attacks that have been discussed above. The ordinary password-based system allows everyone to try openly with known Login IDs without any restriction. An attack on the password hash table will turn out to be catastrophic not just to the user but the entire system. No matter how hard the security analysts are trying their best to retaliate the attacks from the attackers, there are still possible ways to compromise an account if not the worse, the entire system, a web site or a host. The security should be started from the fundamental, i.e. from the user itself.

There are a number of ways to compromise the user account either by using technical or non-technical methods. To protect the Login ID, password and other personal details present in the system from attackers, there should be robust alternative methods for identification of a user in a unique manner. The technology used for identification is referred to as Mind metrics token. The title “mind metrics” is contrived due to its similarity to the biometrics. In the case of biometrics, only the legitimate user possessing the physical character (e.g. finger print) can pass through the identification stage. Similarly, with the mind metrics identification technique, a user can pass through the identification stage in an authorized and a secured manner, subjegated to the overall security of the system in use. Without the use of mind metrics secret key, the user can't pass the identification stage and move on to the next process, i.e. verification stage.

In the past a number of authentication schemes have been presented meant for authenticating the server or the clients. Some of the authentication schemes presented are related to group communication, multi-communication, service authentication, integrated user authentication, brokerage based authentication, mutual authentication in case of IOT, authentication for clouds and multi-clouds, CAPTCHA based authentications. None of these systems are multi-phased and server initiated and as such has not addressed the real time notification systems using the devices like GSM.

The rest of the paper is further divided into proposed methodology, system design and system implementation sections. Conclusions are drawn in the final section.
2. Proposed Methodology

Figure 2 depicts a mind metric based password based system. An extra entity is incorporated to enhance the system security. The additional entity is one the IDs distributed by the server to the user, where one of the Login IDs is legitimate for the user’s account. To shield the attacker from accessing the Login IDs of the user, the system ensures that the Login IDs are partially made dubious. This won’t be a problem for the legitimate user, as he can still recognize the legitimate Login ID and access it.

The mind metrics password based authentication system is implemented within a GSM module, which enables the text messaging service and in turn enhances the security greatly over the conventional systems. The text messaging service by GSM notifies the user whenever there is an unauthorized access to his account by the attackers, be it from any of the forms. This warns the user beforehand, where the user can prevent the attack even before the attack taking place. So instead of damage control, the proposed scheme emphasizes on damage prevention. An additional security scheme based on a TIMER also has been included into the model. If the user/attacker cannot enter/validate his password or mind metric token within 30 seconds of entering the mail id, the system automatically shuts down and redirects back to the home page. This technique will be of great use practically as the attacker usually relies on Brute Force attack and the odds of an attacker cracking the password using Brute Force attack within first 30 seconds of launching the attack and trying all the passwords in the list is practically not feasible.

3. System Design

3.1 System Architecture

Figure 3 depicts the System Architecture of the proposed methodology. In this system an ARM processor LPC 2148, has been used which acts like a central processor. The entire information received from the input, Matrix key pad, is processed by the processor and later displayed using LCD display, 20*4 Graphical LCD. A Lock Value and an Alarm have been introduced with the aid of their respective drivers. Alarm notifies whenever there’s a wrong/unauthorized access to the account. GSM module is used for transmitting real time warnings or messages that can be conveyed to the user, via his cell phone. To facilitate the GSM and LPC 2148 communication, a Max 232 IC is used to convert signals from a serial port to the signals used in TTL compatible digital logic devices/circuits. The oscillation required for the working of LPC 2148 is provided by an in-built oscillator, which generates the required frequency pulses. The modules used in this architecture include ARM-7 Processor with LPC 2148 Controller, 220*4 LCD Display, MAX232, GSM/GPRS SIM900a module and Matrix key pad.

Figure 2. Mind metrics based password system.

Figure 3. System architecture.

3.1.1 ARM-7 Processor WITH LPC 2148 Controller

The ARM 7 processor is used along with LPC 2148 controller. ARM 7 processor embedded with LPC 2148 is used for both processing and controlling the data. It has been seen that the speed of ARM 7 is quite faster and is found to be adequate to complete the authentication process. It also carries an on-chip memory and ADC, which greatly reduces the hardware size of the total system.
3.1.2 20*4 LCD Display
They are many display devices that can be used for displaying the authentication content. Among them LCD displays is one of the most widely used display devices used by the user. Most of the LCD displays available in the market are 16 x 2. LCD displays are capable of displaying 2 lines in which each line can accommodate 16 characters. The graphical LCD is constructed by the grid of pixels. The common resolution present in GLCD is 128 x 64. In GLCD there are 64 horizontal lines in which each line has up to 128 pixels. These pixels are made up of monochrome that each pixel can either be ON or OFF. The pixels which are in ON state looks are presented in dark colour whereas the remaining pixels are presented in OFF mode.

3.1.3 MAX 232
The MAX 232 is an integrated circuit which converts a signal to TIA-232 (RS-232) serial port signal which is suitable for using it in TTL digital compatible logical circuits. The MAX 232 is a combination of transmitter/receiver and it commonly converts over TX, RX, RTS and CTS signals.

3.1.4 GSM/GPRS SIM900a Module
GSM/GPRS is also known as resilient Quad-band mobile phone, which mainly works on a different frequency of 850/900/1800/1900 MHZ and it is also helpful and utilized to get access through the internet as well as oral communication as it contains an amplifier and a little loud speaker as a combination and it is also helpful in SMSs.

3.1.5 Matrix Key Pad
This is a 16-button key board that provides a useful human interface component connected to a Micro controller. It has an excellent price and performance ratio. It is simpler to interface any Micro controller. Data entry for embedded systems is done through matrix keypad which uses a combination of four rows and four columns to provide button states to the host device.

4. System Implementation

4.1 Simulation on KEIL Micro-Vision Software
The KEIL software has been used to write the programs in both Assembly language and embedded C for different modules that are interfaced with a Micro controller. The Micro-vision IDE is a development platform for the window-based software that combines a robust editor and a project manager. Micro-vision is an integrated tool that integrates all the components which include a “c” compiler, macro assembler, linker/locator, HEX file generator etc.

4.2 Implementation on ARM 7 Processor
Figure 4 depicts the hardware module of the system. One can enter the data through the matrix key pad. The input is fed into the ARM processor, where it processes the data. One can observe the GSM module connected to the ARM processor, which notifies the user whenever there’s an unauthorized access to the account. MAX 232 IC is placed
in between the GSM module and ARM processor, which helps in providing an interface between the two entities. GLCD screen acts as a display device, which enables the user to interact with the system. The final output is driven to this GLCD screen by the processor.

4.3 System Evaluation

4.3.1 Level of Safety
By making mind metrics token lengthy and complicated, the level of protection for authentication of accounts can be enhanced. The high-complexity token can be constructed by combining special keys, wilful misspellings etc. Mind metrics is also known as double-protection system where the users are provided with two independent passwords. So, mind metrics has more advantages than the conventional password system.

4.3.2 Security
Mind metrics has the capability for storage of multiple files like token hash files, password hash files, index file separately to enhance the protection and weaken the vulnerability of the attackers. Attacker can't attack the user account until the attacker obtains the password information altogether. Cracking the account becomes very difficult if the length of a token is much greater than the password.

4.3.3 Usability
Unlike biometrics, mind metrics does not require any specialized hardware. If the user types the token correctly, the account access is granted. If in case the token is revealed in any way, the user has an advantage to re-register for a new token. Conventional password systems can be easily upgraded to mind metrics password system just by adding the identification server to the existing password system.

5. Conclusions
Use of mind metrics password based authentication system along with a GSM module which enables the text messaging service, enhances the security greatly over the conventional systems. This text messaging service by GSM notifies the user whenever there is an unauthorized access to his account by the attackers, be it from any of the forms.

6. Acknowledgements
We are grateful for the constant help and assistance provided by K L University. We acknowledge the ESSN (Embedded System and Sensor Networks) research group of our University for the kind of support extended.

7. References
1. Naveen K, Sarvanan S, Lavanya M, Vaithyanathan V. Improved CAPTCHA based authentication for E-mail ID. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–4.
2. Sklavos N, Efstathiou C. SecurID Authenticator: On the hardware implementation efficiency. 14th IEEE International Conference on Electronics, Circuits and Systems; Marrakech. 2007 Dec. p. 589–92.
3. Alzomni M, Josang A, McCullagh A, Foo E. Strengthening SMS based authentication through usability. International Symposium on Parallel and Distributed Proceeding with Applications; 2008 Dec. p. 683–8.
4. Rybnik M, Tadedzki M, Saeed K. A key stroke dynamics based system for user identification. 7th Computer Information Systems and Industrial Management Applications; Ostrava. 2008 Jun. p. 225–30.
5. Manasa S, Mullaimalar P, Gnanaprakash Singh GB, Manivannan SS. Securing online bank transactions from phishing attacks using MFA and secure session key. Indian Journal of Science and Technology. 2015 Jan; 8(S2):123–6.
6. Guna J, Humar I, Pogapnik M. Intuitive gesture based user identification system. 35th International Conference on Telecommunications and Signal Processing (TSP); 2012 Jul. p. 629–33.
7. Gautam T, Jain A. Analysis of brute force attacks using TG datasheet. IEEE SAI Intelligent Systems Conference (IntelliSys); 2015 Oct. p. 984–8.
8. Vu AD, Han JI, Nguyen HA, Kim YM. A homogeneous parallel brute force cracking algorithm on the GPU. International Conference on ICT Convergence (ICTC) 2011 Sep. p. 561–4.
9. Tatlı EI. Cracking more password hashes with patterns. IEEE Transactions on Information Forensics and Security. 2015 Apr; 10(8):1656–65.
10. Catuogno L, Castiglione A, Palmieri F. Honeypot system with honey word-driven fake interactive sessions. International Conference on High Performance Computing and Simulation (HPCS); Amsterdam. 2015 Jul. p. 187–94.
11. Ganesh Kumar D, Rajasekaran S, Prabu R. PB verification and authentication for server using multi communication. Indian Journal of Science and Technology. 2016 Feb; 9(5):1–6.
12. Hong S. Multi-factor user authentication on group communication. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–6.
13. Thiagarajan M, Raveendra C, Thiagarasu V. Web service authentication and multilevel security. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–7.
14. Park JK, Lee HS, Kim SJ, Park JP. A study on secure authentication system using integrated user authentication service. Indian Journal of Science and Technology. 2015 Sep; 8(23):1–6.
15. Choi JH, Lee SH, Kim MK. Integrated user authentication method using BAC (Brokerage Authentication Centre) in multi-clouds. Indian Journal of Science and Technology. 2015 Oct; 8(25):1–7.
16. Usha Devi G, Vishnu Balan E, Priyan MK, Gokulnath C. Mutual authentication scheme for IoT application. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–5.
17. Padma E, Rajalakshmi S. An efficient strategy to provide secure authentication on using TPM. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–8.
18. Sudhan SKHH, Saravanan Kumar S. An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–5.
19. Naveen K, Saravanan S, Lavanya M, Vaithyanathan V. Improved CAPTCHA based authentication for E-mail ID. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–4.
20. Khan AS, Fisal N, Bakar ZA, Salawu N, Maqbool W, Ullah R, Saldar H. Secure authentication and key management protocols for mobile multihop WiMAX Networks. Indian Journal of Science and Technology. 2014 Mar; 7(3):282–95.
21. Sulthana ESS, Kanmani S. Implementation and evaluation of SIFT descriptors based finger-knuckle-print authentication system. Indian Journal of Science and Technology. 2014 Mar; 7(3):374–82.
22. Manjusha R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015 Apr; 8(S7):220–7.
23. Kim Y, Song Y, Lee J. Vehicular authentication security mechanism modelling using petri net. Indian Journal of Science and Technology. 2015 Apr; 8(S7):443–7.
24. Kumari S. Real time authentication system for RFID Applications. Indian Journal of Science and Technology. 2014 Mar; 7(S3):47–51.
25. Somu N, Gangaa A, Shankar Sriram VS. Authentication service in Hadoop using one time pad. Indian Journal of Science and Technology. 2014 Apr; 7(S4):56–62.
26. Ganeshkumar K, Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. Indian Journal of Science and Technology. 2014 Oct; 7(S6):1–5.
27. Vishnuvardhan Rao K, Anita Angeline A, Kanchana Bhaaskaran VS. Design of a 16-bit RISC processor. Indian Journal of Science and Technology. 2015 Aug; 8(20):1–7.