Enhanced Password Authentication for Web Services

Kumar K[1]Aishwarya R[2]Amulya A Shetty[3]Kavana U[4]Manasa M[5]
Department of Computer Science &Engineering
Visvesvaraya Technological University, Belagavi, Karnataka, India

Abstract—*Textual passwords remain the most usually Employed client verification system, and possibly will keep on being so for a considerable length of time to come. Despite the notable security and convenience issues concerning textual passwords, none of the various proposed confirmation options seem to have accomplished an adequate level of appropriation to rule within a reasonable time-frame. Most clients have numerous records on web where each record is secured by a secret key. To keep away from the headache in recalling and dealing with an extensive rundown of various and disconnected passwords, most clients basically utilize a similar watchword for numerous records. The current cybercrimes development is a major issue, a great many individuals turn into the casualty of cybercrime and the clear majority of them can't be counteracted effectively just by solid passwords. The assaults incorporate key logging, beast compelling, speculating assaults, replay assault. In this paper, we will talk about a confirmation conspire in which we can handle any such assaults and give a protected verification over uncertain and low-security arranges by utilizing the USSD code.*

Keywords—Authentication, password, Textual passwords, USSD

I. INTRODUCTION

In the clear majority of authentication systems, textual password schemes are the dominant choice for authenticating end users, despite the well-known security issues concerning passwords, and the inconvenience incurred by end users in remembering multiple passwords for different accounts [2]. Commonly, clients tend to pick simple to-recall passwords that are additionally simple for foes to figure. Indeed, passwords are to be faulted for some, current information breaks.End clients are regularly constrained to pick "solid" passwords (e.g., through secret word meters).

Existing password schemes lack mechanisms providing users with means to narrow down the range of candidate passwords as users are only provided with “all-or nothing” feedback upon submitting login credentials. This in turn can leave legitimate users with no option but to guess their passwords through a “trial-and- error” process. Submit password recovery requests, or resort to other verification methods to regain access to their accounts. This eventually increases the amounts of cognitive effort, time, and resources required to memorize new passwords, or to contact system administrators and request their help in resetting passwords.

In this paper text-based authentication is proposed which uses Persuasive Technology. It is a way to motivate and influence people to create a password that is hard to guess which in the proposed system is done using a combination of static (user’s choice) and dynamic (system generated) [1]. Also, the scheme authenticates the user by session passwords [5] which for every login is different and not useful after the session is closed. It provides robustness against various attacks such as man-in-the-middle attack, SQL injections, brute-force attack, keyloggers.

II. OBJECTIVES

Motivated by the expected persistence of textual passwords, as well as the importance of mitigating security and usability issues relating to them, this paper proposes to create a competent system to ensure the password security of the user by using the dynamically produced value which is appended to the user’s static password which enables extra certainty of the safety of the user. The main objective here is to create a user-friendly system which is understood and applied from a lay man to an enterprise level user.

III. RELATED WORK

For instance, a huge 272.3 million stolen client names and passwords were as of late exchanged on the web, including some from the greatest email suppliers (e.g., Google, Yahoo, and Microsoft) [7].

Verizon’s 2016 Data Breach Investigations Report (DBIR) analyses more than 100,000 data security incidents across 82 countries and continues to provide food for thought. [6]

The DBIR found that “63% of confirmed data breaches involved weak, default or stolen passwords”. Moreover, the “capture and/or reuse of credentials is used in numerous incident classification patterns”, from “highly targeted attacks” to “opportunistic malware infections”.

As the DBIR found, “social engineering remains worryingly effective” as a means of harvesting user credentials. According to Verizon, “almost a third (30%) of phishing messages were opened—up from 23% in 2014. And 12% of targets went on to open the malicious attachment or click the link—about the same as 2014 (11%).” These incidents could have been prevented with better user awareness.

IV. PROPOSED SYSTEM

The proposed authentication system authenticate user and authenticate a session. The merits of this system are that it is resistant to few attacks -shoulder surfing attack, man-in-the-middle attack, brute-force attack, keyloggers as well as SQL injections which are highly performed b unauthorized user or hacker. These attacks are overcome by using the Dynamically generated value which is used as session password as well as login password. The authentication consists of two main phases, they are

- Registration phase
- Login phase

A. Registration

In the Registration process, the users fill the details and sets the static password. Corresponding to this an entry is created in the database which stores all the details including the

recovery questions. The use then needs to verify his enrolled phone numbers by dialing the USSD code. After successful verification a registration confirmation message is sent to the user.

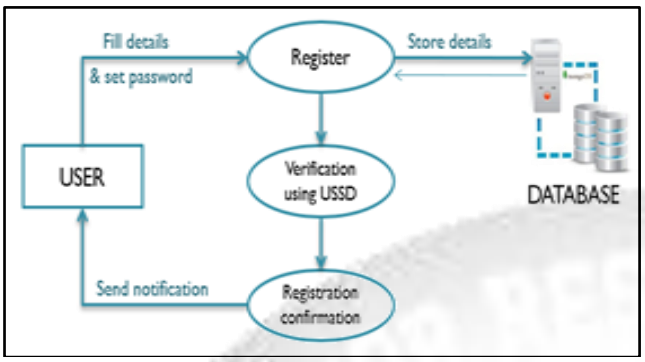

Fig. 1: Registration process

B. *Login*

In the login process, the user enters his credentials which is verified with the database. On clicking the next button and dialing to the USSD through any one of the registered phone numbers, the UIC is sent as an alert message to the user's phone. On the appending the UIC correctly to the static password, the user successfully logs in.

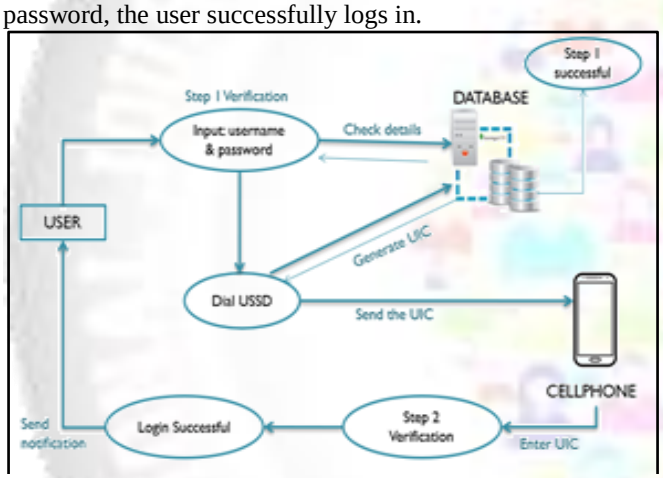

Fig. 2: Login process

V. Technology Stack

A. *USSD*

USSD (Unstructured Supplementary Service Data) is a GSM technology used to send text between a mobile phone and an application program in the network [3]. Applications may include prepaid roaming or mobile chatting. USSD is like SMS, but, unlike SMS, USSD transactions occur during the session only. USSD messages are up to 182 alphanumeric characters long [4]. Unlike SMS messages, USSD messages create a real-time connection during a USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS.

B. *GSM*

GSM (Global System for Mobile communication) is a standard developed by the European Telecommunication Standards Institute (ETSI). GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot.

C. *MongoDB*

MongoDB is a free and open-source cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with schemas. It is written in c, c++, JavaScript. It provides, high performance, high availability, and easy scalability. MongoDB works on concept of collection and document. It uses internal memory for storing the working set, enabling faster access of data.

D. *NODE.js*

Node.js is a source, cross platform JavaScript run-time environment for executing JavaScript code server-side. Historically, JavaScript was used primarily for client-side scripting, in which scripts written in JavaScript are embedded in a webpage's HTML, to be run client-side by a JavaScript engine in the user's web browser. Node.js enables JavaScript to be used for server-side scripting, and runs scripts server-side to produce dynamic web page content before the page is sent to the user's web browser.

VI. Conclusion

The proposed system mitigates few of the vulnerabilities in the existing system.

1) As the static password set by the user is very simple it can be easily remembered by the user.
2) The dynamically generated password is sent in a very secure way to the user's mobile phone and hence the chances of tracking the password is reduced.
3) The proposed system methodology is easy to understand and accessible by all kinds of users.
4) The proposed system has a very few constraints.

References

[1] Geetanjali Bhola, Divjot Kaur, Mahesh Raj, "Dynamic Password Authentication Protocol Using Android Device and One-Way Function", WiSPNET conference,2017 IEEE.

[2] Saravanakumar M. E. and Anupriya Mohan, "Single Password, Multiple Accounts" in the Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN), August 2008.

[3] Krithiga Lakshmi1, Himanshu Gupta2, JayanthiRanjan, "USSD – Architecture Analysis, Security threats, Issues and Enhancements", 2017 International Conference on Infocom Technologies and Unmanned Systems (ICTUS'2017), Dec. 18-20, 2017, ADET, Amity University Dubai, UAE.

[4] "A Model for the Delivery of SMS and USSD Location-based Mobile Advertising Using Network-based Positioning", IIMC International Information Management Corporation, 2016.

[5] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A Shoulder Surfing Resistant Image-based Authentication System with Temporal Indirect Image Selection", Proc. Of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188- 194.

[6] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
[7] J. Fontana, Another Breach, Another Dollar: Is it Time to Kill the Password? accessed on May 10, 2016. [Online]. Available: http://zd.net/1QT593G