THREE FACTOR LOGIN

Deepa Yadav[1], Ankit Singh[2], Neha Sharma[3], Palak Shah[4]

[1,2,3,4] *Student, Dept. of Computer Engineering, Thakur Polytechnic, Mumbai-400101, Maharashtra, India*

Abstract – *The design for three factor login authentication protocols is quite challenging, considering that various kinds of root kits reside in the PCs (Personal Computers) to observe user's behaviour and to make the PCs untrusted devices. While promising, is not easy because of their limited capability of computation and memorization, Involving human in authentication protocols. Assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm users' trust. In this paper, we demonstrate how careful visualization design can enhance not only the usability but also the security of authentication. At the end, we put up two visual authentication protocols: one is a login protocol, and other is a password-based authentication protocol. Through exact analysis, we verify that our protocols are not exposed to many of the challenging authentication attacks applicable in the literature. we were able to achieve a high level of usability while satisfying extreme security requirements.*

Key Words: **Android, PHP, Html, MySQL.**

1. INTRODUCTION

The three factor login is a software designed to capture all of a user's keyboard strokes, and then make use of them to mimic a user in financial transactions. For example, if a user types in her password in a bank's sign in box, key logger Interrupt the password. Even worse, key loggers, often root kitted, are hard to detect since they will not show up in task manager process list.

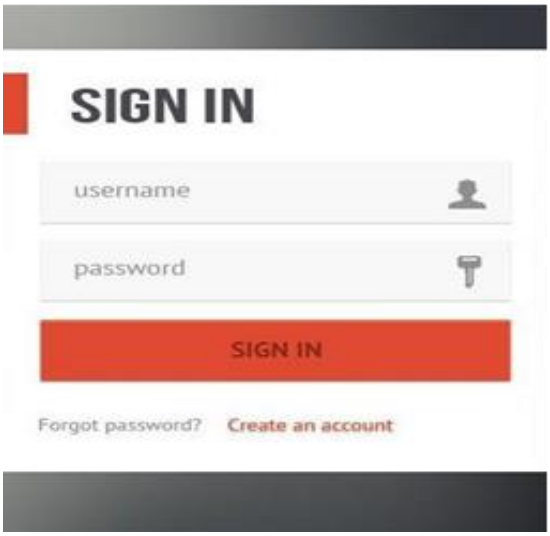
To reduce the key logger attack, onscreen or virtual keyboards with random keyboard arrangements are widely used in practice. Both techniques, by reshuffle alphabets randomly on the buttons, can block simple key loggers. Then, the key logger, which has control over the entire PC, can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Thus, usability is an important factor in designing a human-involving protocol.

CONCEPT

Our approach is to solve the problem and to introduce median device that bridges a human user and a terminal. Interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code.

Step: 1

Goal is to keep the user-experience same as in authentication methods as much as possible, while preventing keylogging attacks. More specifically, our approach visualizes the security process of authentication using a smartphone aided augmented reality.



Step: 2

In second step, the visual participation of users in a security protocol boosts both the security of the protocol and is re-assuring to the user because she feels that she plays a role in the process.

A smartphone with a camera is used To securely implement visual security protocols. Instead of executing the entire

security protocol on the personal computer, the part of security protocol is moved to the smartphone.

The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes

Step:3

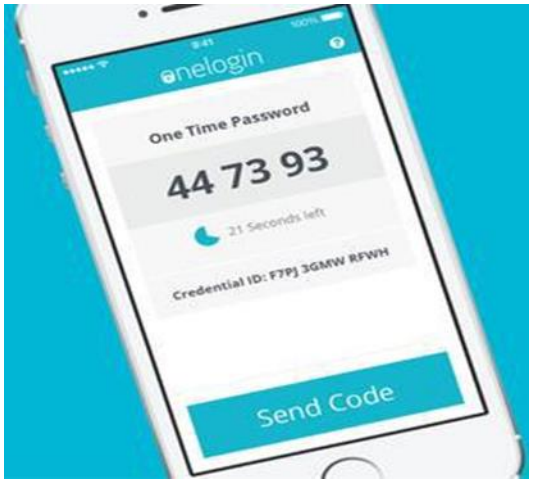


Fig.3 OTP (One Time Pad)

In third steps, OTP is shared to the smartphone in which the account is being logged in with the help of QR Code.it is generated for a limited time after the QR Code has been scanned. we make use of one time password (OTP) that is the password which is valid for the single session. We securely generate and verify the OTP using Smartphone. The generated OTP can be send to a mobile phone in the form of SMS as SMS messaging has a high potential to reach all the customers with a low total cost of ownership or Smartphone can be used as token or platform for creating OTP. Thus we can call it SMS OTP or OTP generated through Smartphone the OTP generated will be valid only for a short period of time and it is generated and verified using Hash Functions and Secured Cryptographic Algorithm such as SHA-1. The system we proposed been implemented and tested successfully

APPLICATIONS

Our protocols are collective and can be applied to a many contexts of authentication.

Some of the Applications:

- Banking System
- E-Commerce System
- E-Governance System
- Login Security
- Securing Transactions

CONCLUSION

The three factor login approach applied on the above system makes it highly secure along with being more user friendly. This system will definitely help to avoid Shoulder shurfing attack, Tempest attack and brute-force attack at the client side. Three factor login system is a definitely time consuming approach, as the user has to traverse through three factor login of security, and will need to refer to his mobile number for the one-time automated generated password. Therefore, this system cannot be a acceptable solution for general security purposes, where time complexity will be an issue. But will definitely be a advantage in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure. In near future not only we will add more features but also make our system customizable.

REFRENCES

[1] Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication, Author: Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi.

[2] S3PAS: A Scalable Shoulder-Surfing Resistant Textual Graphical Password Authentication Scheme, Author: Huanyu Zhao and Xiaolin Li.