Analysis of Performance of a Novel Visual Authentication Protocol over Various Attacks

Kancharana Asha Kiran [#1], Nagireddy Vyshnavi [#2], G. Sankara Rao[*3]
*B.Tech Student [#1], B.Tech Student [#2], Assistant Professor [*3]*
Department of Computer Science & Engineering,
Gayatri Vidhya Parishad College of Engineering For Women,
NH 5, Near Kommadi Junction, Madhurawada,
Visakhapatnam, Andhra Pradesh 530048

Abstract: **In current day's security plays a very vital role in each and every aspect of human life. As security plays a very crucial role in all aspects of life, a lot of illegal users try to access the information of unknown users illegally. To avoid this problem there were various new techniques proposed in order to store the data safely on remote machines.Eventhough there was no exact system which clearly provides complete security over the local and remote system storage. So it is a big challenge to design a secure authentication protocols. As we all know that till today each and every user try to provide password based security for their accounts, as it doesn't achieve high security because of guessing or dictionary attacks. There is no system which has multi level of security to provide secrecy for the sensitive data. In this paper we for the first time have implemented a novel security system by involving the visual authentication protocols for storing the data safely inside the system. For this we have taken image as primary security for storing and accessing the data. Also we have implemented a new pattern mechanism which was implemented for the first time in order to provide more security for the sensitive data. By conducting various experiments on the proposed approach we finally came to a conclusion that this technique was implemented for the first time in order to give high level of security for the sensitive data.**

Keywords: **Data Encryption, Authentication, Guessing Attacks, Dictionary Attacks, Visual Protocols.**

1. Introduction

Now a days there were a lot of security primitives that are available in literature to provide highest level of security for the sensitive data which is stored on various local or remote servers, but they failed in achieving highest level of security in various applications. In the current days the main fundamental task of a security admin is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. One of the challenges that occur in the current days is the design of secure authentication protocols as we know that there is a lot of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Also involving human beings in authentication protocols as a promising approach, but it is not easy because of their limited capability of computation and memorization. Therefore rely on users to enhance security of the application mainly degrades the usability. In this paper, we mainly demonstrate how careful visualization design can enhance not only the security but also the usability of authentication protocol. To that end, we propose two main visual authentication protocols:

I. One is a one-time-password protocol, and
II. The other is a password-based authentication protocol.

After a deep analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature. Furthermore, using an extensive case study on a prototype of our protocols, we highlight the potential of our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.

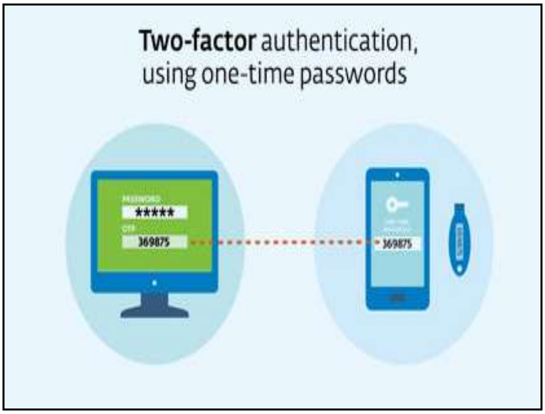
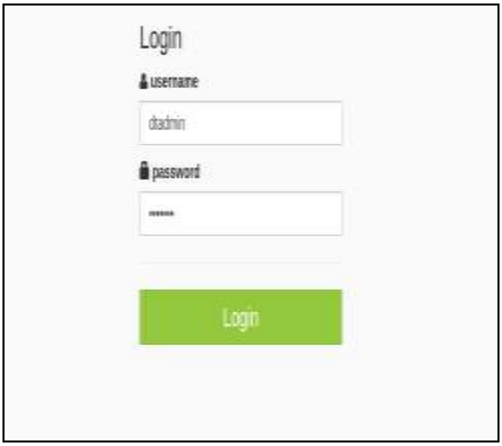


Figure 1.Two Factor Authentication using One-Time Passwords

From the figure 1, we can get a clear idea that user while he need to get login into in this site, he need to substitute the code which is displayed either in mobile device or from any other sources like email id and so on. If the code is correctly substituted in the box given below then the page will be directed to the successful login, if not page will be directed to the error page.


Login

username

dtadmin

password

******

Figure 2.Represents the Admin Interface with User id and Password forgetting Login into the account.

From the above figure 2, we can clearly get an idea that password based authentication protocol gives almost more security for the user at the time of login. As this password scheme is available in all websites both in commercial or open source, the user need to register first with all his credentials including the user name and password and he need to enter all the things in his login time. Sometimes the user may forget his password what he gave at the time of registration, then it is a big problem to identify that password manually, so there will be a facility to retrieve the password what the user forgets by clicking on forget password option.

2. Background Knowledge

In this section we will find the background work that was carried out and studied in order to implement this current paper. In this section we will find the various security factors that are related to providing security for the valuable data,one among them is AI Hard problem.

2.1 Hard AI Problem

First we can discuss about the AI-Hard or AI-Complete problems that was available in the field of Artificial Intelligence. AI-complete problems are hypothesized to include computer vision, natural language understanding, and dealing with unexpected circumstances while solving any real world problem[2],[3],[4].Currently, AI-hard problems cannot be solved with modern computer technology alone, but would also require human computation[11].

The following are the AI-Hard and AI-Complete problems that are hypothesized. They are as follows:

A) Computer vision also some of sub problems like object recognition.

B) Problem like Natural language understanding

C) Some of the problems like text mining, machine translation, and word sense disambiguation.

D) Another Problem like dealing with unexpected circumstances while solving any real world problem, whether it's navigation or planning or even the kind of reasoning done by expert systems.

2.2 Effects of Key Logger: In order to reduce the effect of key logger attack, there was a new technique adapted by almost all the users who use the computers like virtual or onscreen keyboards with random keyboard arrangements. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple key loggers. Unfortunately, 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. Another mitigation technique is to use the keyboard hooking prevention technique by perturbing the keyboard interrupt vector table [13]. However, this technique is not universal and can interfere with the operating system and native drivers. Considering that a key logger sees users‘keystrokes, this attack is quite similar to the shoulder-surfing attack.

In order to prevent the shoulder-surfing attack, many graphical password schemes have been introduced in the literature [11], [12]. However, the common theme among many of these schemes is their unusability: they are quite complicated for a person to utilize them. For some users, the usability is as important as the security, so they refuse to change their online transaction experience for higher security. The shoulder-surfing attack, however, is different from key logging in the sense that it allows an attacker to see not only direct input to the computer but also every behavior a user makes such as touching some parts of screen. To adopt shoulder-surfing resistant schemes for prevention of key logger is rather excess considering the usability. Notice that while defending against the shoulder surfing attack is out of the scope of this work, and could be partly done using other techniques from the literature intended for this purpose, the promising future of smart glasses (like Google glasses) makes the attack irrelevant to our protocols if it is to be implemented using them instead of mobile phones.

2.3 Security Using Cryptography Techniques: Cryptography is that the study of techniques for secure communication inside the presence of third parties (called hackers/intruders) lots of sometimes, it's relating to constructing and analyzing protocols that block adversaries [5], [6] varied aspects in knowledge security like data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Current cryptography exists at the intersection of the disciplines of arithmetic, technology, and technology. Applications of cryptography embrace ATM cards, laptop passwords, and electronic commerce. Cryptography before the fashionable age was effectively similar with cryptography, the conversion of information from a decipherable state to apparent nonsense. The mastermind of associate degree encrypted message shared the secret writing technique needed to recover the primary knowledge exclusively with meant recipients, thereby precluding unwanted persons from doing the same. Since warfare I and thus the appearance of the laptop, the methods accustomed perform cryptography became increasingly advanced and its application a lot of widespread [5]-[10].

From the below figure 3, we can clearly find out that for encrypting a plain text we need a key based on the type of algorithm and once the data is encrypted with the help of a key this will be send to the receiver .The receiver will receive the encrypted data and he now try to decrypt the data with the key that was specified by the sender and then finally view the data in the form of plain text.

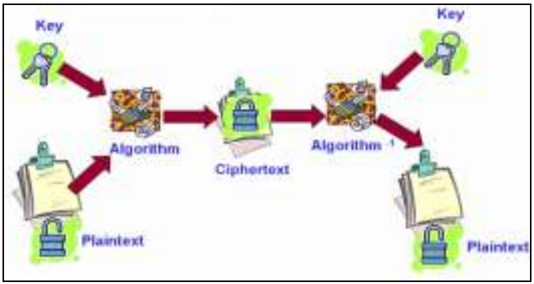


Figure. 3. Represents the Process of Encryption and Decryption of Valuable or Sensitive Data

3. Proposed Novel Key- Logging Resistant Visual Authentication Protocol (NKRVAP)

In this section we mainly describe about the proposed NKRVAP algorithm which is mainly used for providing security for our application while storing and retrieving valuable data to and from the system. Here in this section we describe two protocols for user authentication with visualization. Before getting into the details of these protocols, we review the notations for algorithms used in our protocols as building blocks. Our system utilizes the following algorithms:

Encrk(.) Function: Here this function is mainly used to represent an encryption algorithm which takes Following parameters like a key k and a message M from set M and outputs a ciphertext C in the set C.

Decrk(.) Function: Here this function is mainly used to represent a decryption algorithm which takes a ciphertext C in C and a key k, and outputs a plaintext (or message) M in the set M.

Sign (.) Function : Here a new function like signature generation algorithm which takes a private key SK and a message M from the set M, and outputs a signature σ

Verf (.) Function : A signature verification algorithm which takes a public key PK and a signed message (M, σ), and returns valid or invalid.

QREnc(.) Function : A QR encoding algorithm which takes a string S in S and outputs a QR code.

QRDec(.) Function : A QR decoding algorithm which takes a QR code and returns a string S in S.

4. Authentication with Random Strings

In this section, we introduce an authentication protocol with a onetime password (OTP). The following protocol relies on a strong assumption; it makes use of a random string for authentication. The protocol works as follows:

1) The user connects to the server and sends her ID.

2) The server checks the ID to retrieve the user‘s public key (PKID) from the database. The server then picks a fresh random string OTP and encrypts it with the public key to obtain EOTP = EncrPKID (OTP).

3) In the terminal, a QR code QREOTP is displayed prompting the user to type in the string.

4) The user decodes the QR code with EOTP = QRDec(QREOTP). Because the random string is encrypted with user‘s public key (PKID), the user can read the OTP string only through her smart phone by OTP = Decrk(EOTP) and type in the OTP in the terminal with a physical Keyboard.

5) The server checks the result and if it matches what the server has sent earlier, the user is authenticated. Otherwise, the user is denied.

5. Implementation Modules

Implementation is the stage where theoretical design is converted into programmatically way. Generally in the implementation stage we will divide the application into number of modules in order to make the application develop very easily. We have implemented the proposed concept on Java Platform in order to show the performance this proposed multi keyword ranked based search over encrypted cloud data. The front end of the application takes JSP, HTML and Back-end takes My SQL Server 5.0 .Here we have used a QR Image Blocks for developing the pattern. The main reason why we have used QR Blocks is the pattern can be very secure as the blocks will not display the position if they were selected or dragged to the end user externally. So that is the reason why we used the QR Blocks.The application is divided mainly into following 4 modules. They are as follows:

1. Graphical Security Module
2. Avoiding Key loggers Attacks Module
3. Avoiding Shoulder Surfing Attack Module
4. File Security Module

1. **Graphical Security Module** In this module, users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. Avoiding Key loggers Attacks Module
Key loggers are popular and widely reported in many contexts. In our protocols, input is expected by the user, and in every protocol one or another type of input is required. Our protocols—while designed with the limitations and shortcoming of users in mind, and aim at easing the authentication process by means of visualization are aimed explicitly at defending against the key logger attacks. Here, we further elaborate on the potential of using key loggers as an attack, and the way they impact each of the two protocols.

3. Avoiding Shoulder Surfing Attack Module: Shoulder-surfing resistance is not within our scope. However, in this section, we investigate the possibility and the effectiveness of shoulder surfing attacks. The shoulder surfing is a powerful attack in the context of password-based authentication and human identification, . In this attack, the attacker tries to know credentials, such as passwords or PINs (personal identification numbers) by stealthily looking over the shoulder of a user inputting these credentials into the systems.

4. File Security Module

There has been a large body of work on the problem of user authentication in general and in the context of e-banking. Of special interest are authentication protocols that use graphical passwords like those reported in and attacks on them reported in . To the best of our knowledge, our protocols are the first of their type to use visualization for improving security and usability of authentication protocols as per the way reported in this Project.

.

6. Conclusion

In this paper, for the first time we define a new level of security for the use of user driven visualization to improve security and user-friendliness of authentication protocols. Moreover, we have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the key logger and malware attacks. Such a protocol our proposed protocol clearly tells that this is the first time to implement such a new pattern of dragging QR codes, each drag will calculate the moves in which the user made while storing the data and the same will be used while retrieving the data. By conducting various experiments on our proposed system and its feasibility and potential in real-world deployment, we came to an conclusion that this is mostly suited for user authentication.

References

[1]. Shapiro, Stuart C. (1992). Artificial Intelligence In Stuart C. Shapiro (Ed.), *Encyclopedia of Artificial Intelligence* (Second Edition, pp. 54–57). New York: John Wiley. (Section 4 is on "AI-Complete Tasks".)

[2] .Roman V. Yampolskiy. Turing Test as a Defining Feature of AI-Completeness . In Artificial Intelligence, Evolutionary Computation and Metaheuristics (AIECM) --In the footsteps of Alan Turing. Xin-She Yang (Ed.). pp. 3-17. (Chapter 1). Springer, London. 2013. http://cecs.louisville.edu/ry/TuringTestasaDefiningFeature04270003.pdf

[3]. Luis von Ahn, Manuel Blum, Nicholas Hopper, and John Langford. CAPTCHA: Using Hard AI Problems for Security. In Proceedings of Eurocrypt, Vol. 2656 (2003), pp. 294-311.

[4]. *Bergmair, Richard (January 7, 2006). "Natural Language Steganography and an "AI-complete" Security Primitive".* CiteSeerX*:* 10.1.1.105.129. (unpublished ?)

[5] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,”Proc. 13th ACM Conf. Computer and Comm. Security (CCS ’06), 2006.

[6] Y.-C. Chang and M. Mitzenmacher, “Privacy Preserving Keyword Searches on Remote Encrypted Data,” Proc. Third Int’l Conf. Applied Cryptography and Network Security, 2005.

[7] A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. IEEE Security and Privacy, 4:21–29, March 2006.

[8] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda. Panorama: capturing system-wide information flow for malware detection and analysis. In Proc. of ACM CCS, 2007.

[9]N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall, 2003.

[10]E. Rescorla. SSL and TLS: designing and building secure systems.Addison-Wesley, 2001.

[11] R. Dhamija and A. Perrig, ―Déjà Vu: A user study using images for authentication,‖ in Proc. 9th USENIX Security, 2000, pp. 1–4.

[12] D. Weinshall, ―Cognitive authentication schemes safe against spyware,‖ in Proc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[13]R. Pemmaraju. Methods and apparatus for securing keystrokes from being intercepted between the keyboard and a browser. Patent 182,714.

About the Authors

Kancharana Asha Kiran completed her 4 years B.Tech in Dept of CSE at Gayatri Vidhya Parishad College of Engineering For Women, NH5, Near Kommadi Junction, Madhurawada, Visakhapatnam. Her area of interest includes Networking and Security.

Nagireddy Vyshnavi completed her 4 years B.Tech in Dept of CSE at Gayatri Vidhya Parishad College of Engineering For Women, NH5, Near Kommadi Junction, Madhurawada, Visakhapatnam. Her area of interest includes Networking and Security.

G. Sankara Rao is currently working as an Assistant Professor in Department of Computer Science & at Gayatri Vidhya Parishad College of Engineering For Women, NH5, Near Kommadi Junction, Madhurawada, Visakhapatnam. He has more than 10 years of experience in teaching field. His resarch interest includes Wireless Sensor Networks,Networking and Security.