An Improved Security Approach For User authentication

1B.Suresh, 2R.Sailaja
Dept. of CSE, Sri Sai Aditya Institute of Science and Technology, Surampalem, Kakinada, East Godavari District, A.P, India.

ABSTRACT:

A Key logger is software intended to imprison all of a user’s keyboard strokes, and then create use of them to mimic a user in financial transactions. Threats next to electronic and financial services can be secret into two major classes: credential stealing and channel breaking attacks. Credentials such as users’ identifiers, passwords, and keys can be stolen by an attacker when they are inadequately administered. Even if all required information is firmly delivered to a user’s computer, the attacker inhabits on that user’s computer can effortlessly scrutinize and alter the information and show valid-looking yet not to be trusted information. Human user’s contribution in the security protocol is sometimes obligatory to foil this type of attacks but humans are not good at thorny calculations and do not have a plenty memory to remember cryptographically strong keys and signatures. Our approach to resolve the dilemma is to pioneer a transitional device that bridges a human user and a terminal.

KEYWORDS: Authentication, Smartphone, Malicious code, Key logger.

I. INTRODUCTION:

Relying on users to improve safety of necessity humiliates the usability. On the other hand, calming suppositions and thorough refugeint end to perk up the user experience can show the way to safety breaches that can harm the users’ trust. In this paper, we display how vigilant hallucination design can improve not only the security but also the usability of authentication [1]. To that end, we recommend two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. From first to last painstaking analysis, we authenticate that our protocols are protected to many of the challenging authentication attacks appropriate in the literature. Also, using awide case study on a prototype of our protocols, considering that a key logger sees users’ keystrokes, this attack is pretty comparable to the shoulder-surfing attack[2]. To avert the shoulder-surfing attack, many graphical password schemes have been introduced in the literature. Yet, the universalsubject matterin the middle of many of these schemes is their insurability: they are rather complicated for a person to utilize them [3].

II. RELATED WORK:

Parno et al. not compulsory the exercise of trusted devices to achieve shared confirmation and eradicates dependence on perfect user behaviour. A little touched upon in this paper are key loggers as budding attacks for credentials stealing, which are reported and other malwares which are reported in. In this paper we have publicized that our protocols are sheltered even when one of the participants in the authentication process (the terminal or smart phone) is cooperation [4].

III. LITERATURE SURVEY:

THE AUTHOR, Haichang Gao (ET .AL), AIM IN [1], Alphanumeric passwords are extensively used in computer and network authentication to defend users privacy. Though it is well known that long, text based passwords are hard for people to keep in mind, while shorter ones are at risk to attack. Graphical password is a talented solution to this problem. Draw-A-Secret (DAS) is a typical functioning based on the user drawing on a grid canvas. At present, too many restrictions result in reduction in user practice and avert its popularity. A novel graphical password strategy Yet Another Graphical Password (YAGP) inspired by DAS is proposed in this paper. The proposal has the advantages of free drawing positions, strong shoulder surfing resistance and large password space [5,6].

THE AUTHOR, Eiji Hayashi (ET .AL) AIM IN [2], our scheme relies on the human aptitude to be familiar with a dishonoured version of a before seen image. We exemplify how misshapes images can be used to preserve the usability of graphical password systems while creation them more elastic to social engineering or observation attacks. Since it is hard to mentally “revert” a degraded image, without knowledge of the original image, our system gives a strong line of defencenext tocharlafatan access, while preserving the desirable memorability properties of graphical password schemes. By low-fidelity tests to help in the design, we put into practice prototypes of Use Your
Illusion as an Ajax-based web service and on Nokia N70 cellular phones. We display that, apart from their age or gender; users are very skilled at make out degraded versions of self-chosen images, even on diminutive displays and after time periods of one month. Our results point to those graphical passwords with misshapen images can achieve equal error rates to those by traditional images, but only when the original image is known [7,8].

IV. PROBLEM DEFINITION:

The intend of secure authentication protocols is rather demanding, bearing in mind that assorted kinds of root kits reside in PCs (Personal Computers) to observe user’s behaviour and to make PCs untrusted devices. Connecting human in authentication protocols, while talented, is not easy since of their incompleteability of calculation and memorization. Consequently, relying on users to improve security of necessity degrades the usability. On the other hand, calming assumptions and exact security design to get better the user knowledge can show the way to protection breaks that can hurt the users’ trust. It is non Security for Stored data [9,10].

V. PROPOSED APPROACH:

We show how cautiousdream design can improve not only the safety but also the usability of authentication. To that end, we suggest two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. During exact examination, we confirm that our protocols are resistant to a lot of the demanding authentication attacks appropriate in the literature. In addition, using awidespread case study on a prototype of our protocols, we underline the probable of our come near for real-world deployment: we were talented to realize a high level of usability while rewarding stringent security requirements. It holds uplogical Image security and usability and emerges to fit well with some no-nonsense applications for on the road to mending online safety.

VI. SYSTEM ARCHITECTURE:

VII. PROPOSED METHODOLOGY:

**ENCRYPTION:** An encryption algorithm which takes a key k and a message M from set M and outputs a ciphertext C in the set C.

**DECRIPTION:** A decryption algorithm which takes a ciphertext C in C and a key k, and outputs a plaintext M in the set M.

**SIGNATURE:** A signature generation algorithm which takes a private key SK and a message M from the set M, and outputs a signature.

**VERIFICATION:** A signature verification algorithm which takes a public key PK and a signed message, and returns valid or invalid.

**QREncryption:** A QR encoding algorithm which takes a string S in S and outputs a QR code.

**QRDecryption:** A QR decoding algorithm which takes a QR code and returns a string S in S.

**AUTHENTICATION ALGORITHM**

**STEP1:** The user connects to the server and sends her ID.

**STEP2:** The server checks the ID to retrieve the user’s public key from the database. The server then picks a fresh random string OTP and encrypts it with the public key to obtain EOTP.

**STEP3:** A QR code QREOTP is displayed prompting the user to type in the string.

**STEP4:** The user decodes the QR code with EOTP because the random string is encrypted with user’s public key, the user can read the OTP string and type it in the terminal with a physical keyboard.

**STEP5:** The server checks the result and if it matches what the server has sent earlier, the user is authenticated. Otherwise, the user is denied.
VIII. RESULTS:

The outcome illustrates the QR code downloading after successful registration.

IX. ENHANCEMENT:

To improve proposed methodology performance ring signature provides anonymity of user. Which means that the verifier knows that the user is a member of a ring, but he doesn’t know exactly who the user is.

X. CONCLUSION:

We have given away two realizations of protocols that not only perk up the user practice but also oppose challenging attacks, such as the key logger and malware attacks. Our protocols make the most of uncomplicated knowledge available in most out-of-the-box Smartphone devices. We developed Android application of an example of our protocol and make obvious its possibility and likely in real-world deployment and operational settings for user authentication. Our work really opens the door for quite a few other directions that we would like to explore as a future work.

XI. FUTURE WORK:

At long last, investigating client mulls over that will profit by a wide arrangement and acknowledgement of our conventions would be a parallel future work to consider too.

XII. REFERENCES:


Mr B.Suresh is a student of Sri Sai Aditya Institute of Science and Technology. Presently he is pursuing his M.Tech [Computer Science] from this college and he received his B.Tech from Sri Sai Aditya Institute of Science of Technology, Surampalem, affiliated to JNT University, Kakinada in the year 2013. His area of interest includes computer networks and Information Security, all current trends techniques in Computer Science.

Mrs. R. Sailaja, M.Tech, (Ph.D), well known Author excellent teacher received B.Tech from Andhra University and M.Tech (SE) from JNT University Kakinada is working as sr. Assistant professor, Department of CSE, Sri Sai Aditya Institute of Science and technology. She is an Active member of CSI. She has 5 years of teaching experience in various engineering colleges. To her credit couple of publication both national and international conferences/journals. Her area of interest includes Information Security, computer Networks, Operating Systems and other advances in Computer Applications.