International Journal of Science Engineering and Advance Technology

Novel Visual Authentication Protocols to Defend Key Logging Issues

Chava Niharika[1], N. Madhu Bindu[2]
[1]M.Tech (CSE), MVR College of Engineering and Technology, A.P., India.
[2]Asst Professor, Dept. of Computer Science & Engineering, MVR College of Engineering and Technology, A.P., India.

***Abstract* — The best approach to accomplish secure correspondence is to have validation convention, which is a sort of cryptographic convention with the reason for confirming substances. The configuration of secure validation conventions is entirely testing, considering that different sorts of root packs dwell in PCs (Personal Computers) to watch client's conduct and to make PCs untrusted gadgets. Including human in confirmation conventions, while promising, is difficult as a result of their constrained capacity of calculation and retention. Subsequently, depending on clients to upgrade security essentially corrupts the convenience. Then again, unwinding presumptions and thorough security configuration to enhance the client experience can prompt security ruptures that can hurt the clients' trust. In this paper, we show how cautious perception outline can upgrade the security as well as the ease of use of confirmation. To that end, we propose two visual confirmation conventions: one is an one-time-secret word convention, and the other is a watchword based verification convention. Through thorough examination, we check that our conventions are resistant to a large portion of the testing confirmation assaults pertinent in the writing. Moreover, utilizing a broad contextual analysis on a model of our conventions, we highlight the capability of our methodology for true organization: we could accomplish an abnormal state of ease of use while fulfilling stringent security necessities.**

***Keywords* — Authentication, Smartphone, Malicious code,**
Keylogger.

I.INTRODUCTION

Validation is an imperative part of framework security. It affirms the personality of any client attempting to sign on to a space or get to network assets. Windows Server 2003 family verification empowers single sign-on to all system assets. With single sign-on, a client can sign on to the space once, utilizing a solitary secret key or shrewd card, and verify to any PC in the domain.Threats against electronic and budgetary administrations can be grouped into two noteworthy classes: accreditation taking and channel breaking assaults [10]. Accreditations, for example, clients' identifiers, passwords, and keys can be stolen by an aggressor when they are ineffectively overseen. For instance, an inadequately oversaw (PC) contaminated with a pernicious programming (malware) is a simple focus for certification assailants [11], [6]. Then again, channel breaking assaults—which take into account listening stealthily on correspondence in the middle of clients and a monetary foundation—are another type of misuse [12]. While established channel breaking assaults can be anticipated by the correct use of a security channel, for example, IPSec [13] and SSL (secure attachments layer) [3], late channel breaking assaults are all the more difficult. To be sure, "keylogging" assaults—or those that use session seizing, phishing and pharming,and visual falseness—can't be tended to by basically empowering encryption.

Chief among this class of assaults are keyloggers [14], [6], [4]. A keylogger is programming intended to catch the greater part of a client's console strokes, and after that make utilization of them to mimic a client in budgetary exchanges. For instance at whatever point a client sorts in her secret word in a bank's signin box, the keylogger captures the watchword. The danger of such keyloggers is pervasive and can be available both in PCs and open stands; there are dependably situations where it is important to perform monetary exchanges utilizing an open PC despite the fact that the greatest concern is that a client's secret key is prone to be stolen in these PCs. Much more dreadful, keyloggers, frequently rootkitted, are difficult to distinguish since they won't appear in the undertaking chief procedure list. To relieve the keylogger assault, virtual or onscreen consoles with irregular console game plans are generally utilized as a part of practice. Both systems, by improving letter sets arbitrarily on the catches, can disappoint basic keyloggers. Sadly, the keylogger, which has control over the whole PC, can without much of a stretch catch each occasion and read the video cushion to make a mapping between the snaps and the new letters in order. Another alleviation system is to utilize the console perturbing so as to snare counteractive action method the console interfere with vector table [7]. Notwithstanding, this method is not widespread and can meddle with the working framework and local drivers. Considering that a keylogger sees clients' keystrokes, this assault is very like the shoulder-surfing assault. To keep the shoulder-surfing assault, numerous graphical secret key plans have been presented in the writing [5], [8]. Notwithstanding, the normal subject among a large portion of these plans is their unusability: they are entirely confused for a man to use them. For a few clients, the ease of use is as imperative as the security, so they decline to change their online exchange experience for higher security. The shoulder-surfing assault, then again, is not quite the same as keylogging as in it permits an assailant to see direct information to the PC as well as each conduct a client makes, for example, touching a few sections of screen. To receive shoulder-surfing safe plans for avoidance of keylogger is fairly overabundance considering the ease of use. Notice that while protecting against the shouldersurfing assault is out of the extent of this work, and could be mostly done utilizing different systems from the writing planned for this reason, the promising eventual fate of keen glasses (like Google glasses) makes the assault immaterial to our conventions on the off chance that it is to be actualized utilizing them rather than cell telephones. It is insufficient to depend just on cryptographic methods to counteract assaults which mean to mislead clients' visual experience while living in a PC. Regardless of the fact that all important data is safely conveyed to a client's PC, the aggressor dwelling on that client's PC can without much of a stretch watch and modify the data and show legitimate looking yet beguiling data. Human client's association in the security convention is now and again important to keep this sort of assaults however people are bad at confounded estimations and don't have an adequate memory to recall cryptographically solid keys and marks. Consequently, ease of use is an imperative element in outlining a human-including convention [9].

Our way to deal with taking care of the issue is to present a moderate gadget that scaffolds a human client and a terminal. At that point, rather than the client specifically conjuring the normal confirmation convention, she summons a more advanced yet easy to understand convention by means of the middle helping gadget. Each connection between the client and a middle offering gadget some assistance with being imagined utilizing a Quick Response (QR) code. The objective is to keep client encounter the same as in legacy confirmation strategies however much as could be expected, while avoiding keylogging assaults. Along these lines, in our conventions, a client does not have to remember additional data aside from a customary security token, for example, secret key or PIN, and not at all like the former writing that protects against ought to requiring so as to surf assaults complex calculations and broad inputs. All the more particularly, our methodology imagines the security procedure of verification utilizing a smartphoneaided expanded reality. The visual contribution of clients in a security convention supports both the security of the convention and is consoling to the client in light of the fact that she feels that she assumes a part all the while. To safely actualize visual security conventions, a cell phone with a camera is utilized. Rather than executing the whole security convention on the PC, some portion of security convention is moved to the cell phone. This representation of some piece of security conventions improves security significantly and offers assurance against difficult to-shield against assaults, for example, malware and keylogging assault, while not debasing the ease of use. On the other hand, we take note of that our objective is not securing the verification process against the shouldersurfing assailant who can see or trade off all the while both gadgets over the shoulder, yet rather to make it hard for the enemy to dispatch the assault.

I. Problem Statement

The outline of secure validation conventions is entirely testing, considering that different sorts of root packs dwell in PCs (Personal Computers) to watch client's conduct and to make PCs untrusted gadgets. Including human in validation conventions, while promising, is difficult in light of their restricted capacity of calculation and retention. In this way, depending on clients to improve security fundamentally debases the ease of use. Then again, unwinding suppositions and thorough security outline to enhance the client experience can prompt security breaks that can hurt the clients' trust. In this Project, we show how cautious representation configuration can upgrade the security as well as the ease of use of confirmation. To that end, we propose two visual confirmation conventions: one is an one-time-secret word convention, and the other is a watchword based validation convention. Through thorough examination, we check that our conventions are safe to a large number of the testing confirmation assaults pertinent in the writing. Moreover, utilizing a broad contextual investigation on a model of our conventions, we highlight the capability of our methodology for true sending: we could accomplish an abnormal state of ease of use while fulfilling stringent security prerequisites.

II.Proposed approach

In this Project, we attempt to enhance perception outline can improve the security as well as the ease of use of verification. To that end, we propose two visual validation conventions: one is an one-time-secret word convention, and the other is a watchword based confirmation convention. Through thorough investigation, we confirm that our conventions are invulnerable to a significant number of the testing confirmation assaults pertinent in the writing. Besides, utilizing a broad contextual investigation on a model of our conventions, we highlight the capability of our methodology for certifiable organization: we could accomplish an abnormal state of convenience while fulfilling stringent security prerequisites.

III.Related Work

A. System Model

Our framework model comprises of four unique substances (or members), which are a client, a cell phone, a client's terminal, and a server. The client is a conventional human, restricted by human's weaknesses, including constrained capacities of performing complex calculations or recollecting modern cryptographic certifications, for example, cryptographically solid keys. With a client's terminal, for example, a desktop PC or a portable workstation, the client can sign in a server of a monetary foundation (bank) for budgetary exchanges. Additionally, the client has a cell phone, the third framework element, which is outfitted with a camera and stores an open key endorsement of the server for advanced mark check. At last, the server is the last framework element, which has a place with the budgetary establishment and performs back-end operations by connecting with the client (terminal or cell phone) for the benefit of the bank. Expecting a cell phone element in our framework is not an unrealistic presumption, since most mobile phones these days qualify (as far as preparing and imaging capacities) to be the gadget utilized as a part of our work. In our framework, we accept that there is no immediate channel between the server and the cell phone. Additionally, we take note of that in a large portion of the conventions proposed in this paper, a cell phone does not utilize the correspondence channel—unless generally is expressly expressed—so a cell phone can be supplanted by any gadget with a camera and some legitimate preparing power, for example, an advanced camera, a compact music player with camera (iPod touch, or versatile device with the previously stated capacities) or a savvy/glasses.

B. Trust and Attacker Models

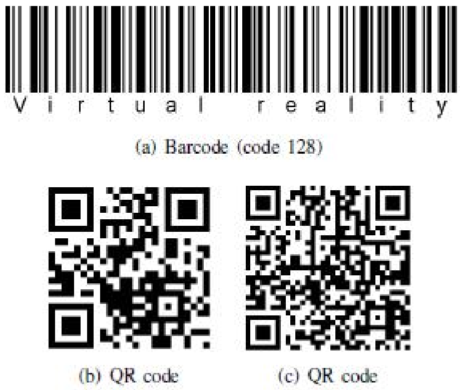
For the trusted entities in our system, we assume the following:

To start with, we accept that the channel between the server and the client's terminal is secured with a SSL association, which is truth be told an exceptionally practical supposition in most electronic managing an account frameworks. Second, we accept that the server is secured by each methods and is insusceptible to each assault by the aggressor; henceforth the assailant's worry is not breaking into the server but rather assaulting the client. At long last, as for the keylogger assault, we accept that the keylogger dependably lives on the terminal. Concerning the assailant model, we expect a malignant aggressor with high motivating forces of breaking the security of the framework. The aggressor is fit for doing any of the accompanying: _ The assailant has a full control over the terminal. In this manner, – While dwelling in a client's terminal, the assailant can catch client's certifications, for example, a watchword, a private key, and OTP (one time secret key) token string. – The assailant can betray a client by demonstrating a certifiable looking page that really exchanges cash to the aggressor's record with the caught certifications that she acquired from the bargained terminal. – Or, soon after a client effectively gets verified with a substantial accreditation, the assailant can seize the confirmed session. _ The aggressor is fit for making a fake server to dispatch phishing or pharming assaults. For the cell phone in Protocol 1, we accept that it is constantly trusted and invulnerable to bargain, which implies no malware can be introduced on it. Notice that this suspicion is in accordance with different suppositions made on the cell phone's reliability when utilized as a part of comparable conventions to those introduced in this paper [3], [2], [4]. We, be that as it may, take note of that unwinding this presumption still could give a sure level of security with Protocol 2. Convention 2 utilizes two components (secret word and the cell phone), and subsequently, the supposition can be casual so that the terminal as well as cell phone could be traded off (one of them at once however "not both together"). The non-synchronous bargain suspicion clearly prohibits the shoulder-surfing aggressor.

In our conventions, we likewise accept a few cryptographic primitives. For instance, in all conventions, we accept that a client has a couple of open/private keys utilized for message marking and check. In Protocol 1, we accept that the server has the ability of creating one time cushions, utilized for verification. In Protocol 2, we accept clients have passwords utilized for their verification. Notice that these suspicions are not outlandish also, since most managing an account administrations utilize such cryptographic certifications. For instance, with most managing an account administrations, the utilization of computerized testaments issued by the bank is exceptionally normal. Moreover, the utilization of such cryptographic certifications and keeping up them on a cell phone does not require any specialized foundation at the client side, and is suited for wide assortment of clients. Further subtle elements on these certifications and their utilization are clarified alongside the particular convention where they are utilized as a part of this paper.

C. Linear and Matrix Barcodes

A standardized tag is an optical machine-meaningful representation of information, and it is generally utilized as a part of our day by day life since it is connected to a wide range of items for recognizable proof. More or less, scanner tags are for the most part two sorts: straight standardized tags and network (or two dimensional, otherwise called 2D) standardized identifications. While direct scanner tags—appeared in Figure 1(a)— have a restricted limit, which relies on upon the coding procedure utilized that can extend from 10 to 22 characters, 2D standardized tags—appeared in Figure 1(b) and Figure 1(c)— have higher limit, which can be more than 7000 characters. For instance, the QR code—a generally utilized 2D standardized identification—can hold 7,089 numeric, 4,296 alphanumeric, or 2,953 twofold characters [4], making it a decent high-limit possibility for putting away plain and encoded substance alike. Both straight and network standardized tags are well known and have been broadly utilized as a part of numerous commercial ventures including, yet not constrained to, car businesses, assembling of electronic segments, and packaging businesses, among numerous others. Because of their more noteworthy limit, grid standardized identifications are even proactively utilized for ad so that a client who has a cell phone can without much of a stretch sweep them to get some nitty gritty data about promoted items. This model of ad—and different venues of utilizing these standardized tags as a part of zones that are in contact with clients—made the requirement for standardized identification's scanners grew particularly for cell phones. As needs be, this prompted the formation of numerous famous business and free standardized tag scanners that are accessible for cell phones, for example, iPhone and Andriod phones alike.



(a) Barcode (code 128)

(b) QR code (c) QR code

Fig. 1. Three different barcodes encoding the statement "Virtual reality". (a) is a linear barcode (code 128), and (b) and (c) are matrix barcodes (of the QR code standard). While (b) encodes the plain text, (c) encodes an encrypted version using the AES-256 encryption algorithm in the cipher-block chaining (CBC) mode (note this last code requires a password for decryption).

KEYLOGGING-RESISTANTVISUAL AUTHENTICATION PROTOCOLS

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(): an encryption algorithm which takes a key k and a message M from set M and outputs a ciphertext C in the set C.
Decrk(): 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 (): a signature generation algorithm which takes a private key SK and a message M from the set M, and outputs a signature _.
Verf(_): a signature verification algorithm which takes a public key PK and a signed message (M;), and returns valid or invalid.
QREnc(_): a QR encoding algorithm which takes a string S in S and outputs a QR code.
QRDec(_): a QR decoding algorithm which takes a QR code and returns a string S in S.

Any public key encryption scheme with IND-CCA2 (Indistinguishability against Adaptive Chosen Ciphertext Attacker) security would be good for our application.

A public key encryption scheme with IND-CCA2 adds random padding to a plaintext, which makes the ciphertext different whenever encrypted, even though the plaintext is the same [1]. This restriction on the type of the used public key encryption scheme will prevent an attacker from checking whether his guess for the random layout is right or not. Thus, the security of the scheme is not dependent on the number of possible layouts but the used encryption scheme. If no such encryption is used, the adversary will be able to figure out the layouts used because he will be able to verify a brute-force attack by matching all possible plaintexts to the corresponding ciphertext. On the other hand, when such encryption is used, the 1-1 mapping of plaintext to cipher text does not hold anymore and launching the attack will not be possible at the first place. Also, any signature scheme with EUF-CMA (existential-unforgeability against adaptive chosen-message attacker) can be used to serve the purpose of our system. For details on both notions of security, see [14]. In particular, and for efficiency reasons, we recommend the short signature in.

A. Authentication With Random Strings

In this section, we introduce an authentication protocol with a onetime password (OTP). The following protocol (referred to as Protocol 1 in the the rest of the paper) 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 smartphone 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. In this protocol, OTP is any combination of alphabets or numbers whose length is 4 or more depending on the security level required.

B. An Authentication Protocol with Password and Randomized Onscreen Keyboard Our second protocol, which is referred to as Protocol 2 in the rest of this paper, uses a password shared between the server and the user, and a randomized keyboard. A high-level event-driven code describing the protocol is shown in Figure 1. The protocol works as follows:
1) The user connects to the server and sends her ID.
2) The server checks the received ID to retrieve the user's public key (PKID) from the database. The server prepares , a random permutation of a keyboard arrangement, and encrypts it with the public key to obtain EKBD = EncrPKID (). Then, it encodes the ciphertext with QR encoder to obtain QREKBD = QREnc(EkID ()). The server sends the result with a blank keyboard.
3) In the user's terminal, a QR code (QREKBD) is displayed together with a blank keyboard. Because the onscreen keyboard does not have any alphabet on it, the user cannot input her password. Now, the user executes her smartphone application which first decodes the QR code by applying QRDec(QREKBD) to get the ciphertext (EKBD). The ciphertext is then decrypted by

the smartphone application with the private key of the user to display the result (= ecrSKID(EKBD)) on the smartphone's screen.

4) When the user sees the blank keyboard with the QR code through an application on the smartphone that has a private key, alphanumerics appear on the blank keyboard and the user can click the proper button for the password. The user types in her password on the terminal's screen while seeing the keyboard layout through the smartphone. The terminal does not know what the password is but only knows which buttons are clicked. Identities of the buttons clicked by the user are sent to the server by the terminal.

5) The server checks whether the password is correct or not by confirming if the correct buttons have been clicked.

.IV.Conclusion

In addition, we have indicated two acknowledge of conventions that enhance the client experience as well as oppose testing assaults, for example, the keylogger and malware assaults. Our conventions use basic innovations accessible in most out-of-the-container cell phone gadgets In this paper, we proposed and examined the utilization of userdriven perception to enhance security and ease of use of validation conventions. We created Android use of a model of our convention and show its attainability and potential in genuine arrangement and operational settings for client verification. Our work to be sure opens the entryway for a few different headings that we might want to examine as a future work. Above all else, we will probably actualize our convention on the brilliant glasses, for example, the google glass, and direct the client study.

VREFERENCES

[1] —. Google authenticator. http://code.google.com/p/google-authenticator/.

[2] —. Rsa securid. http://www.emc.com/security/rsa-securid.htm.

[3] Cronto. http://www.cronto.com/.

[4] —. BS ISO/IEC 18004:2006. information technology. Automatic identification and data capture techniques. ISO/IEC, 2006.

[5] —. ZXing. http://code.google.com/p/zxing/, 2011.

[6] D. Boneh and X. Boyen. Short signatures without random racles. In Proc. of EUROCRYPT, pages 56–73, 2004.

[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajan . The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.

[8] J. Brown. Zbar bar code reader, zbar android sdk 0.2. http://zbar. sourceforge.net/, April 2012.

[9] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate 'n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.

[10] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.

[11] D. Crockford. The application/json media type for javascript object notation (json). ttp://www.ietf.org/rfc/rfc4627.txt?number=4627, July 2006.

[12] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proc. of USENIX Security, 2004.

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

[14] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig. Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, CMU, 2011.

Ms.Ch.Niharika is a student of MVR College of Engineering & Technology, Paritala. Presently she is pursuing her M.Tech [Computer Science and Engineering] from this college and she received her B.Tech from Nimra womens college of Engineering, affiliated to JNT University, Kakinada in the year 2012. Her area of interest includes Computer Networks and Object oriented Programming languages and information security, all current trends and techniques in Computer Science.

Mrs.N.Madhu Bindu, well known Author and excellent teacher Received M.Tech (CSE) from JNT University, Kakinada.she is working as Assistant Professor in Department of Computer science and Engineering , MVR college of Engineering and Technology. She is an active member of UACEE. .She has 5 years of teaching experience in this college. To her credit couple of publications both national and international conferences /journals . Her area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.