IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

KEYLOGGING: The Enhanced Attack Resistant Visual Authentication System

Brahmaji Godi[1], Yuvasree Bammidi[2], Kotni Manikanta Vara Prasad[3]
Swetha Pilla[4], Kilimi Chidananda Reddy[5]
[1]Assistant Professor, Department of Computer Science and Engineering, Ragh Institute of Technology, Dakamarri, Visakhapatnam, Andhra Pradesh, India
[2,3,4,5]B.Tech Scholar(CSE) in Department of Computer Science and Engineering, Ragh Institute of Technology, Dakamarri, Visakhapatnam, Andhra Pradesh, India

Abstract

Key logging or keyboard catching is the activity of duplicate (or logging) the keys hit on a keyboard, regularly private with the goal that the particular using the keyboard is apathetic that their doings are being watched. It comparably has astoundingly solid uses in request of human computer collaboration. We indicate how wary representation outline can propel the security and in addition the reasonableness of validation. We propose two visual validation conventions: one is a one-time-secret word convention, and the other is a watchword based confirmation convention. Our approach for genuine scheme: we had the limit accomplish a peculiar condition of convenience while fulfilling thorough security necessities.

Keywords: Key Logging, Authentication Protocols, Acoustic Analysis, Visual Authentication, Security.

I. Introduction

Keylogging shows a phenomenal test to security administrators. Not at all like standard worms and infections, certain sorts of keyloggers are everything aside from hard to find. Keyloggers are a sort of malware that harmfully track client data from the solace endeavoring to recover individual and private data. Developing machine use for fundamental business and individual exercises utilizing the Internet has made doable treatment of keylogging essential. Cybercriminals have anecdotal different calendars to get touchy data from your endpoint gadgets. Then again, few of them are as powerful as keystroke logging. Keystroke logging, for the most part called keylogging, is the hold of engraving characters. The information got can join report content, passwords, client ID's, and other conceivably tricky bits of data. Utilizing this approach, an attacker can get basic information without breaking into an established database or record server. A keylogger is altering, proposed to catch the bigger piece of a client's help strokes, and a while later make utilization of them to duplicate a client in cash related exchanges. For example, at whatever concentrations a client sorts in her watchword in a bank's sign in box, the keylogger gets the puzzle word. The danger of such keyloggers is unavoidable and can be show both in PCs and open corners; there are continually conditions where it is basic to perform money related exchanges utilizing an open machine paying little mind to how the best concern is that a client's watchword is inclined to be stolen in these machines. By a long shot more repulsive, keyloggers, as often as possible root kitted, are precarious to recognize since they won't show up in the task chief system list. To soothe the keylogger attack, virtual or onscreen comforts with irregular reassure blueprints are for the most part used as a piece of training. The two strategies, by reconsidering letter sets arbitrarily on the gets, can puzzle essential keyloggers. Sadly, the keylogger, which has control over the whole PC, can without quite a bit of an extend catch each event and read the video cradle to influence a mapping between the snaps and the new letter to set. Another balance system is to use the comfort trapping neutralizing activity technique by irritating the reassure meddles with vector table. Then again, this system is not general and can meddle with the working structure and neighborhood drivers. It is deficient to depend just on cryptographic procedures to neutralize attacks which intend to cheat customers' visual experience while living in a PC. Despite the way that every single fundamental datum is securely passed on to a customer's machine, the attacker living on that customer's machine can without quite a bit of an extend watch and change the information and show real looking yet deceptive information. Human customer's commitment in the security tradition is now and again vital to keep this kind of attacks however individuals are terrible at obfuscated estimations and don't have an adequate memory to review cryptographically strong keys and checks. In like manner, usability is a basic variable in delineating a human including tradition.

II. Related Work

To the fundamental of our vision, our conventions are the head of their kind to apply representation for enhancing security and straightforwardness of utilization of validation conventions permitting to the way expressed in this paper. A painstakingly associated vein of research is confidence establishing for amass correspondence utilizing insightful abilities. Cases of such works contain SPATE [3], GAnGS [1], and Safe Slinger [2]. None of these works propensity

representation as expressed in this work, despite the fact that they convey primitives for verification clients and making trust. Elective firmly related work is ―Seeing-is-Believing (SiB) [3] (stretched out in [4]), which utilizations visual channels of 2D barcodes to attack the man-in-the-center attack in gadget blending. In any case we use comparable to devices by methods for the 2D barcodes for data image, and the visual channel for coordinating this data, our conventions are extra broad than those proposed in [3]. Our conventions are specially crafted to the issue settings close by, e-keeping money, with a different confidence and attack show than that utilized as a part of [3]—which impacts into disparate assurances. To stop against phishing, Parno et al. prescribed the use of trusted gadgets to accomplishes hared verification and expel dependence on flawless client conduct [5]. Marginally influenced upon in this paper are keyloggers as potential attacks for approvals burglary, which are educated in [6], and supplementary malwares which are educated in [7]. Display: Capturing System-Wide Information Flow for Malware Detection and Analysis. Creators: Heng Yin, Dawn Song,Manuel Egele, Christopher Kruegel, Engin Kirda Description: Malicious projects keep an eye on clients' conduct and trade off their protection. Indeed, even code from respectable sellers, similar to Google Desktop and Sony DRM media player, may perform undesirable activities. Tragically, existing systems for location malware and investigating obscure code tests square measure rare and have crucial weaknesses. we tend to watch that malevolent information access and process conduct is that the basic characteristic of different malware classes rupturing clients' protection (counting keyloggers, catchword criminals, arrange sniffers, covering secondary passages, spyware and rootkits), that isolates these vindictive applications from generous code. we tend to propose a framework, Panorama, to find and investigate malware by catching this rudimentary trait. In our concentrated investigations, Panorama with progress identified all the malware tests and had just a couple of false positives. additionally, by misuse Google Desktop as a contextual investigation, we tend to demonstrate that our framework will precisely catch its information access and process conduct, and that we will ensure that it will transmit delicate information to remote servers in bound settings[10].

III. Keylogging-Resistant Visual Authentication Protocols

We assessment the representations for algorithms used in our protocols as structure blocks. Our scheme employs the following algorithms:

1) Encrk (•): an encryption algorithm which takes a key k and a message M from set M and yields a cipher-text C in the set C.

2) Decrk (•): a decryption algorithm which takes a cipher text C in C and a key k, and yields a plaintext (or message) M in the set M.

3) Sign (•): a signature generation algorithm which takes a private key SK and a message M from the set M, and yields a signature σ.

4) Verf (•): a signature verification algorithm which takes a public key PK and a signed message (M, σ), and yields valid or invalid.

5) QREnc (•): a QR encoding algorithm which takes a string S in S and yields a QR code.

6) QRDec (•): a QR decoding algorithm which takes a QR code and yields a string S in S.

A. Authentication with Random Strings:

In Cutting-edge, we present an authentication protocol with a one-time password (OTP). The subsequent protocol referred to as Protocol 1 depend on on a strong supposition; it marks use of aarbitrary string for authentication.

The protocol works as follows:

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

2) The server drafts the ID to recover the user's public key (P KID) from the database. The server then choices a fresh arbitrary string OT P and encodes it with the public key to find EOT P = EncrP KID (OT P).

3) In the terminal, a QR code QREOT P is showedwarning the user to type in the string.

4) The user decodes the QR code with EOT P = QRDec (QREOT P). Since the arbitrary string is encrypted with user's public key (P KID), the user can deliver the OTP string only complete her smartphone by OTP = Decrk (EOT P) and type in the OTP in the terminal with a physical keyboard.

5) The server authorizations the outcome and if it ties what the server has sent previous, the user is authenticated.

Else, the user is denied. In this protocol, OTP is any mixture of alphabets or numbers whose length is 4 or more liable on the security level necessary.

B. An Authentication Protocol with Password and Randomized:

In the similar manner Onscreen Keyboard Our another protocol, which is mentioned to as Protocol 2, practices a password collective between the server and the user, and a randomized keyboard. A high-level event-driven code significant the protocol is shown in Figure 3.

The protocol works as follows:

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

2) The server checks the acknowledged ID to recover the user's public key (P KID) from the database. The server makes π, aarbitrary permutation of a keyboard arrangement, and encodes it with the public key to get EKBD = EncrPKID (π). Then, it converts the ciphertext with QR encoder to get QREKBD = QREnc (EkID (π)). The server directs the result with a blank keyboard.

3) In the user's terminal, a QR code (QREKBD) is showed collected with a blank keyboard. Since the onscreen keyboard does not have any alphabet on it, the user cannot input her password. Now, the user performs her smartphone application which principal decodes the QR code by relating QRDec (QREKBD) to become the ciphertext (EKBD). The ciphertext is then decrypted by the smartphone application with the private key of the user to show the result (π = DecrSKID (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, alphanumeric 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.

Mostly transactions are done through online only. But for time consuming and quick transaction we proposed offline transaction. In offline transaction user generate one file, inside that file user acc-no, transaction amount, and etc are available. Those details are prepared by user when they are in offline. When user entered into online, they just load this file into the applications for fund transaction.

IV. System and Threat Model

A. System Model

The system model comprises of four different entities such as a client, a smartphone, a client's terminal (PC) and a server. The client is a user or an ordinary human with limited capabilities of remembering cryptographic credentials such as keys and performing complex mathematical computations. A client's terminal is a client's PC which is used to connect to a server for performing financial transactions. The client has the smartphone which stores the public key certificate of the server or digital certificate equipped with a camera. The server is the system entity belongs to the financial institution which interacts with the user by performing all the back-end operations.

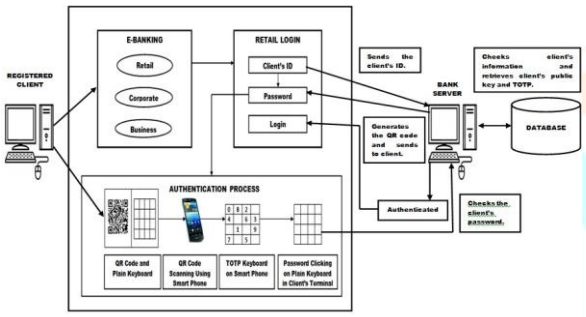

Fig. 1. shows the overall system architecture. Here, the e-banking is taken as an example to show how the authentication process works.

The client or an user is registered in a particular bank for performing online transactions and provided with the unique client ID and password. The registered client can log on to particular bank site. The client must enter into retail login. When the client sends the unique ID to the server, the server checks the client's information from the bank database. If the client's information is correct, the server retrieves the public key and fresh random time-based one-time-password (TOTP) from the database.

The server generates the QR code which comprises of unique client ID, public key, TOTP and time slot. Then the QR code is sent to the client. On client's terminal, the QR code is displayed. Now, the client has to take his smartphone in which the QR code scanning application is already installed. The QR code has to be scanned. After scanning the QR code, the decoded information will be displayed in the smartphone. The randomized keyboard which looks like a 4x4 matrix with random arrangements of 0-9 digits is displayed in the smartphone.

On the client's terminal the password box is replaced with the 4x4 blank keyboard matrix. Now, the client has to just click on the rows or columns of the blank keyboard matrix by seeing where is password has been arranged in the smartphone. From the client's terminal, only the ID of the keyboard matrix is sent to the server. The server also does not know the password of the client. Based on the ID of the keyboard matrix, the client gets authenticated. If the client clicks on the wrong ID, again the previous steps are repeated by sending a newly generated QR code to the client. And also if the client fails to login within the allotted time slot, the server will automatically generates a new QR code with new TOTP. After the client gets authenticated, the client can enjoy all the e-banking services.

B. Trust and Attacker Models

The following must be assumed to ensure that the entities of the system are secure and trusted. First, the channel between server and client's terminal is secured with an SSL or HTTPS connection. Second, the server is assumed to be immune to several attacks. So, the attacker concentrates on the client. Third, the keylogger attacker resides on the client's terminal. The attacker is capable of capturing the security of the system.

The attacker has full control over the client's terminal. So,

1. The attacker can capture client's credential information such as password, private key and TOTP.

2. The attacker can perform session hijacking by showing a fake genuine looking webpage in financial transactions. Therefore the authenticated session can be hijacked by the attacker.

C. Comparison of Quick Response Code with Linear Barcode

QR code is developed by Japanese Denso Wave corporation in 1994. It is a two dimensional barcode. There are 40 versions and four levels of error correction in QR code. The barcodes are attached to all sort of products for identification which is a optical machine-readable representation of data. Linear barcodes are one dimensional and have a limited capacity of coding 10 to 22 characters. The QR code has the high capacity which can hold 7,089 numeric, 4,296 alphanumeric, and 2,953 binary characters [1]. QR Code has been approved as an AIM Standard, a JIS Standard and an ISO standard. So QR Code is being used in a wide variety of applications, such as manufacturing, automotive, logistics, sales, and other business applications. The QR code has the efficiency to decode all types of information such as website URL, contact address, phone number, geographical location, a text message, s calendar event, etc. some of the features of QR code are given as follows:

- High capacity encoding of data
- High-speed reading

- Chinese encoding capability
- Readable from any direction from 360 degree
- Dirt and Damage Resistant
- Structured Append Feature

Fig. 2. Barcode

Fig. 3. QR code

At first, the QR code has been designed to be used in automotive industries. But now, it has been widely used in the advertisement so that a client can use the smartphone and scan to know more information about the advertised products. The barcode scanner applications are created which is compatible for smartphones like android and ios.

V. Proposed Work:

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Then, instead of the user directly invoking the regular authentication protocol, she invokes a more sophisticated but user-friendly protocol via the intermediate helping device. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing key logging attacks.

It Support reasonable Image security and usability and appears to fit well with some practical applications for improving online security.

VI. Conclusion

In this paper, we proposed and studied the use of user determined visualization to advance security and accessibility of authentication protocols. Furthermore, we have revealed two understandings of protocols that not only progress the user knowledge but also counterattack motivating attacks, such as the key logger and malware attacks. Our protocols make use of modest technologies existing in most out-of-the-box Smartphone devices. We advanced Android application of a prototype of our protocol and make evident its possibility and likely in practical world arrangement and working surroundings for user authentication. Our work certainly opens the entrance for numerous other guidelines that we would like to examine as a future work. Firstly our plan is to gadget our protocol on the smart glasses such as the Google glass, and conduct the user study. Second, we plan to examine the design of other Protocols with more rigorous concert requirements using the identical tools provided in this work.

References

[1] BS ISO/IEC 18004:2006. Information Technology. Automatic Identification and Data Capture Techniques. ISO/IEC, 2006.

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

[3] 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.

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

[5] 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.

[6] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu. Yagp: Yet another graphical password strategy. In Proc. of ACM ACSAC, pages 121– 129,2008.

[7] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal, 1988.

[8] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal, 1988.

[9] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig. Use your illusion: secure authentication usable anywhere. In Proc. of ACM SOUPS, 2008.

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