IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Keylogging-resistant Visual Authentication Protocol

Prof.Diksha Bhave[1], Pratiksha Bhavsar[2], Surekha Chavan[3], Krutika Gore[4]

Shivajirao S. Jondhale College of Engineering, Dombivli, University of Mumbai, Mumbai, Maharashtra, India[1.2.3.4]

Abstract: The Keystroke logging, referred to as key logging or capturing the strokes of keyboard, is the act of recording which means logging the keys pressed on a keyboard, other way round it is, that the person using the keyboard is unknown about the fact that their actions are being observed. Key logging can also be used to study human–computer interaction. We have large number of key logging methods that range from hardware and software approaches to acoustic analysis. Here we have proposed two visual authentication protocols one is a one-time-password protocol, the other one is password-based authentication protocol. We verify that our protocols are much strong and can with stand to many of the challenging authentication attacks. Our main focus is to highlight the potential of our approach for real-world deployment: whether we can achieve a high level of usability with satisfactory and acceptable results.

Keywords: Key logging, Authentication, Transaction, QR code.

I. INTRODUCTION

Computer security is main subject of concern when we need to focus on large network. Computer security also termed as cyber security or IT security is nothing but protection the information of systems from theft or destruction to the hardware, the software, and to the information stored, as well as from disruption or misdirection of the services provided by the devices. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. A key logger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a file. A key logger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. Key logging can also be used to study human–computer interaction.

Some key logger programs will also record any mail addresses you use and Web site URL you visit.

Key loggers
We have software and hardware key loggers. Most key logger programs are transferred directly onto a user's machine through a secondary storage device, like a DVD drive, or removable storage media, like USB flash drives. The files can also be attached to download from unsecured sources like most other malware, as key loggers are essentially Trojans by nature. The program attaches itself to a commonly used software application, and resides in the main memory. The more sophisticated key loggers are practically invisible on the infected machine, usually running as a background process. As key loggers are highly customizable, the program is usually set to record the activity on the computer after a particular sequence of keystrokes is used. This trigger is used to record session data, like user names and passwords.

Hardware key loggers, on the other hand, are similar to extension sockets; the keyboard is plugged into one end of the device, while the other end is plugged into the keyboard's designated port. The device is then retrieved and the contents examined to extract the recorded data.

Key loggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Key logger devices that monitor the physical keystrokes of a computer user. They then either aggregate the information locally for later retrieval or send it off to a spyware server on the Internet. Some businesses use key loggers, such as with the Spectre Pro system, to monitor employee activity, but the vast majority are applications installed without the user's knowledge as part of a software download or system intrusion. Once a key logger program is embedded in your computer, it's hard to identify that it's there. "Key loggers are difficult to detect, since their very goal is to steal data without being discovered,"

Fortunately, there are preventative measures you can take to search and destroy key loggers or keep them at bay. Thus to keep away our self from malware attacks we implement sophisticated method for security using QR codes.

The goal is to keep User-experience the same as in legacy authentication methods as much as possible, while preventing key logging attacks. Thus, in our protocols, a user does not need to memorize extra information except a traditional security token such as password or PIN, and unlike the prior literature that defends against should-surfing attacks by requiring complex computations and extensive inputs.

In this paper, we show how visualization can improve security as well as convenience by proposing two visual verification conventions: one for password-based authentication, and the other for one-time-password.

DOI 10.17148/IJARCCE.2016.52117

Through thorough investigation, we demonstrate that our conventions are safe to a number of the testing attacks relevant to different conventions in the writing.

A. Scope and Contribution:

Our paper is being adopted for security purpose as we know that as the technology is reaching to milestone with the speed of light with that same progress we also need to be concern about pros and cons. Our paper thus provides a secure aspect to safe our system from key logging. The original contributions of this paper are as follows:

- Two protocols for authentication that utilizes visualization by means of augmented reality to provide both high Security and high usability. We show that these protocols are secure under several real-world attacks including key loggers. Both protocols offer advantages due to visualization both in terms of security and usability.
- Prototype implementations in the form of Android applications which demonstrate the usability of our protocol in real world system.

B. Organization

The rest of this paper is organized as follows. In section 2, proposed model consists of system model and information about bar codes. In section 3, the working of two visual authentication protocols is briefly explained. In section IV reviews the related works from the literature. In section VI, the conclusion is made.

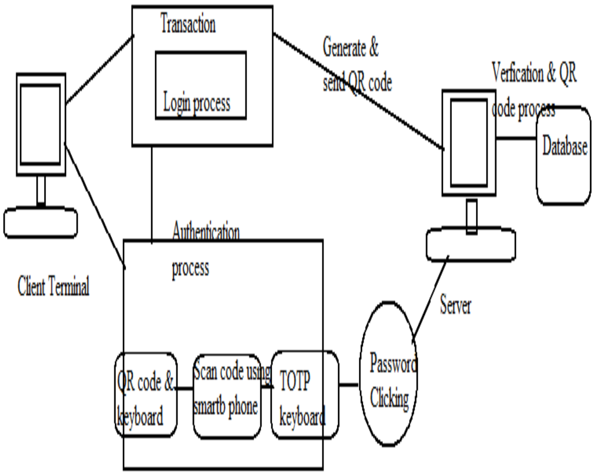
An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. PROPOSED SYSTEM

A .System model:

The system model comprises of four different entities such as a client, a Smart phone, 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 Smart phone 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.

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, and 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 Smart phone 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 Smart phone. The randomized keyboard which looks like a 4x4 matrix with random arrangements of 0-9 digits is displayed in the Smart phone. 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 password is have been arranged in the Smart phone.

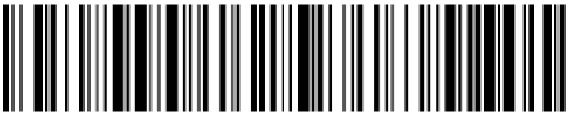
From the client's terminal, only the ID of the keyboard matrix is sent to the server. The server also does not know the password of the client. Based on the ID of the keyboard matrix, the client gets authenticated. If the client clicks on the wrong ID, again the previous steps are repeated by sending 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.

DOI 10.17148/IJARCCE.2016.52117

B.QR codes**:**

A barcode is an optical machine-readable representation of data, and it is widely used in our daily life since it is attached to all types of products for identification. In a nutshell, barcodes are mainly two types: linear barcodes and matrix (or two dimensional, also known as 2D) barcodes. The QR code a widely used 2D barcode can hold 7,089 numeric, 4,296 alphanumeric, or 2,953 binary characters [4], making it a very good high-capacity candidate for storing plain and encrypted contents alike.

Both linear and matrix barcodes are popular and have been widely used in many industries including, but not limited to, automotive industries, manufacturing of electronic components, and bottling industries, among many others.



a. Linear barcode

b. QR code

QR codes those wacky square bar codes that your phone's camera can read can be made extremely useful. Instead of requiring us to type in a long URL, we can point your phone at a QR code and automatically launch a web page. Instead of giving a guest your complicated Wi-Fi password, just log them in via QR code. Instead of worrying about key loggers, you can sign into web sites via QR code and many more.

Features:

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

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 smart phone and scan to know more information about the advertised products. The barcode scanner applications are created which is compatible for smart phones like android.

III. PSEUDO CODE

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 cipher-text C in set C.
- Decrk (·): a decryption algorithm which takes a cipher text C in C and a key k, and outputs a plain-text (or Message) M in the set M.
- 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.

We will consider a bank transaction process where our QR code will be used.

A. Authentication With Time based One-time-password protocol

Initially we used an authentication protocol with a onetime password (OTP).

The protocol works as follows (Bank Transaction):

1)The user wishing to make transaction log in to designated website (login page) which connects to the server through unique ID and password.

2) The server checks the received ID with its password from the database of the user.

3) If the ID and password are correct server prepares a random string TOTP ad limited time slot which is encrypted with public key to obtain:

$$E_{TOTP=}\text{Enc r}(PU_{ID}(TOTP))$$

4) The above every information is embedded in QR code i.e. physically in hidden form by the server and then sends to client.

5) QR code is generated with all above information and sends to client.

6) Now, by using QR code scan application we scan the code given on terminal & the encrypted information is decoded.

Decoded QR code:

$$E_{TOTP=}\text{QRDec }(QR(E_{TOTP}))$$

7) Thus, client now gets the actual embedded information where client can read TOTP string through smart phone by:

$$TOTP=\text{Decrk }(E_{TOTP})$$

Now the TOTP is typed1 in the terminal with a physical keyboard.(Client terminal already has a keyboard matrix to type TOTP)

8) The result which is entered is send to server, which is checked & if it matches what client has send the client is authenticated.

9) If client does not authenticate, denial of access is the only option.

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.

The protocol works as follows:

1) The user wishing to make transaction log in to designated website (login page) which connects to the server through unique ID and password.
2) The server checks the received ID with its password from the database of the user.
3) If the ID and password are correct server prepares a random permutation of a keyboard arrangement, and encrypts it with the public key to obtain:
   E_{KBD} = EncrPU$_{ID}$ (#)
4) The above data is encoded cipher-text with QR encoder to obtain:
   QR E_{KBD} =QREnc (Ek$_{ID}$ (#))
5) The result is send to client with a blank keyboard.
6) At Clients terminal, a QR code (QREKBD) is displayed together with a blank keyboard. Key board is totally blank wherein no alphabet numeric can be entered.
7) The client executes her smart phone application which first decodes the QR code by:
   QRDec (QREKBD) and we get the cipher text (EKBD).
8) The cipher text is then decrypted by smart phone application with the private key of the user to display the result:
   (#= DecrSKID (EKBD)) on the smart phone screen.
9) When the user sees the blank keyboard with the QR code through an application on the smart phone that has a private key, alpha numeric 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 smart phone. 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.
10) The server checks whether the password is correct or not by confirming if the correct buttons have been clicked.

IV. RELATED WORK

There has been a large body of work on the problem of user authentication in general [3], [4], [12], [13], and in the context of e-banking. Of special interest area authentication protocols that use graphical passwords like those reported in [14],[15] and attacks on them reported on various reports. 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 paper. A closely related vein of research is trust establishment for group communication using cognitive capabilities. Examples of such works include SPATE, GAnGS.None of these works use visualization as reported in this work, although they provide primitives for authentication users and establishing trust.Another closely related work is "Seeing-is-Believing

V. ADVANTAGES

1. It supports reasonable image security and usability and appears to fit well with some practical applications for improving online security
2. Preventing Session Hijacking
3. Preventing Key logging.
4. Transaction Verification.
5. Securing Transactions

VI. CONCLUSION

In this paper, we proposed and analyzed the use of two authentication protocols to show how visualization can enhance usability and security. Moreover, these two protocols help to overcome many. Our protocols utilize simple technologies available in most out-of-the-box smart phone devices. We developed android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment and operational settings for user authentication.

This system can be implemented in many real world applications since it utilizes simple technologies and feasible to use as android application.

ACKNOWLEDGMENT

We sincerely wish to thank our project guide **Prof. Diksha Bhave** and our project co-ordinator **Prof. Uttara Gogate** for her ever encouraging and inspiring guidance helped us to make our project a success. Our project guide made us endure with her expert guidance, kind advice and timely motivation which helped us to determine about our project.

We would also like to thank **Dr. J. W. Bakal** as college principal for providing lab facilities and permitting us to go on with our project. We would also like to thank our colleagues who helped us directly or indirectly during our project.

We also express our deepest thanks to our Head of our Computer Department **Prof. P. R. Rodge** whose benevolent helps us making available the computer facilities to us for our project in our laboratory and making it true success. Without his kind and keen co-operation our project would have been stifled to standstill.

REFERENCES

[1] J. Bonneau, C. Harley, P. C. Van Oorschot, and F. Stajano. 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.

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

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

DOI 10.17148/IJARCCE.2016.52117

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

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

[6] 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.

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

[8] 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.

[9] M...Kotadia”Key logger spying at work on the rise, survey says, NET.com”

[10] G.canbek,”Analysis Design and implementation of Key logger and Anti key logger “Gaza University Institute of science and technology Sept 2005, pp.103

[11] www.screenlogger.org

[12] www.networkcomputing.com

[13] Rsa secured. http://www.emc.com/security/rsa-securid.htm.

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

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

DOI 10.17148/IJARCCE.2016.52117