International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Novel Approaches for Keylogging-Resistant Visual Authentication Protocols

Prof. Priyanka Mane[1],Prabhakar Avhad[2],Devarsh Khedkar[3]

Ravikant Jadhav[4],Abhijit Gogre[5]

Genba Sopanrao Moze College of Engineering, Balewadi,Pune(India)

ABSTRACT

The Keystroke work, mentioned as key work or capturing the strokes of keyboard, is that the act of recording which suggests work the keys ironed on a keyboard, alternative approach spherical it's, that the person victimization the keyboard is unknown regarding the actual fact that their actions ar being discovered. Key work can even be wont to study human–computer interaction. We've sizable amount of key work ways that vary from hardware and software package approaches to acoustic analysis. Here we've planned two visual authentication protocols one could be a one-time-password protocol, the opposite one is password-based authentication protocol. We have a tendency to verify that our protocols are a lot of robust and may with stand to several of the difficult authentication attacks. Our main focus is to spotlight the potential of our approach for real-world deployment: whether or not we will reach a high level of usability with satisfactory and acceptable results.

Keywords: Keylogging, QR Code, Shoulder-Surfing Attack, QR code.

I.INTRODUCTION

Computer security is main subject of concern after we have to be compelled to concentrate on massive network. laptop security conjointly termed as cyber security or IT security is nothing however protection the knowledge of systems from larceny or destruction to the hardware, the software system, and to the knowledge keep, similarly as from disruption or misdirection of the services provided by the devices. It includes dominant physical access to the hardware, similarly as protective against damage that will return via network access, information and code injection, and because of malpractice by operators, whether or not intentional, accidental, or because of them being tricked into deviating from secure procedures. A key lumberman could be a sort of police investigation software system (considered to be either software system or spyware) that has the potential to record each keystroke you create to a file. A key lumberman recorder will record instant messages, e-mail, and any data you kind at any time mistreatment your keyboard. Key work may also be wont to study human–computer interaction. Some key lumberman programs will record any mail addresses you employ and data processor uniform resource locator you visit. Key loggers we've software system and hardware key loggers. Most key lumberman programs ar transferred directly onto a user's machine through a auxiliary storage device, sort of a optical disc drive, or removable storage media, like USB flash drives. The files may also be hooked up

to transfer from unsecured sources like most alternative malware, as key loggers ar basically Trojans naturally. The program attaches itself to a ordinarily used software system application, and resides within the main memory. The a lot of subtle key loggers ar much invisible on the infected machine, typically running as a background method. As key loggers ar extremely customizable, the program is sometimes set to record the activity on the pc when a specific sequence of keystrokes is employed. This trigger is employed to record session information, like user names and passwords. Hardware key loggers, on the opposite hand, ar the same as extension sockets; the keyboard is obstructed into one finish of the device, whereas the opposite finish is obstructed into the keyboard's selected port. The device is then retrieved and also the contents examined to extract the recorded information. Key loggers, as a police investigation tool, ar typically employed by employers to make sure workers use work computers for business functions solely. Key lumberman devices that monitor the physical keystrokes of a soul. during this paper, we have a tendency to show however visualisation will improve security similarly as convenience by proposing 2 visual verification conventions: one for password-based authentication, and also the alternative for one-time-password. Through thorough investigation, we have a tendency to demonstrate that our conventions ar safe to variety of the testing attacks relevant to totally different conventions within the writing.

II.PROBLEM STATEMENT

We will propose and analyze the use of authentication protocols to show how visualization can enhance usability and security. Moreover, these protocols help to overcome many attack problems. 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

III.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.

IV. EXISTING SYSTEM

To mitigate the key logger attack, virtual or onscreen keyboards with random keyboard arrangements square measure wide employed in follow. Each technique, by rearranging alphabets every which way on the buttons, will frustrate straightforward key loggers. Sadly, the key logger, that has management over the whole laptop, will simply capture each event and skim the video buffer to form a mapping between the clicks and also the new

alphabet. Another mitigation technique is to use the keyboard golf stroke interference technique by heavy the keyboard interrupt vector table. However, this system isn't universal and might interfere with the software package and native drivers. Considering that a key logger sees users' keystrokes, this attack is sort of just like the shoulder-surfing attack. to forestall the shoulder-surfing attack, several graphical positive identification schemes are introduced. However, the common theme among several of those schemes is their unusability: they're quite difficult for someone to utilize them. for a few users, the usability is as necessary because the security, so that they refuse to alter their on-line dealings expertise for higher security. The shoulder-surfing attack, however, is totally different from keylogging within the sense that it permits associate assailant to envision not solely direct input to the pc however additionally each behaviour a user makes like touching some components of screen.

V.DISADVANTAGES OF EXISTING SYSTEM

1. Existing system has less security
2. Usability of the existing system was not good.
3. Existing system does not Resist challenging attacks, such as the key-logger and malware attacks.

VI.PROPOSED SYSTEM

Our approach to determination the matter is to introduce associate degree intermediate device that bridges an individual's user and a terminal. Then, rather than the user directly invoking the regular authentication protocol, she invokes a a lot of refined however easy protocol via the intermediate serving to device. each interaction between the user associate degreed an intermediate serving to device is visualised employing a fast Response (QR) code. The goal is to stay user-experience a similar as in gift authentication ways the maximum amount as potential, whereas preventing key logging attacks. Thus, in our protocols, a user doesn't got to memorise additional info except a standard security token like word or personal identification variety (PIN), and in contrast to the previous literature that defends against should-surfing attacks by requiring advanced computations and intensive inputs. a lot of specifically, our approach visualizes the safety method of authentication employing a smartphone-aided increased reality. The visual involvement of users during a security protocol boosts each the safety of the protocol and is re-assuring to the user as a result of she feels that she plays a job within the method. To firmly implement visual security protocols, a Smartphone with a camera is employed. Rather than execution the whole security protocol on the private pc, a part of security protocol is moved to the smartphone. This visual image of some a part of security protocols enhances security greatly and offers protection against hard-to-defend against attacks like malware and keylogging attack, whereas not degrading the usability. However, we tend to note that our goal isn't securing the authentication method against the shoulder-surfing aggressor United Nations agency will see or compromise at the same time each devices over the shoulder, however rather to create it laborious for the mortal to launch the attack.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Contribution to projected System: we tend to area unit generating QR code from Encrypted text that may be useful for creating system a lot of sturdy towards hacker. once login with success on-line looking portal are show to user from that user can purchase the merchandise. we tend to area unit giving color choice theme at the time of login for validation of the user

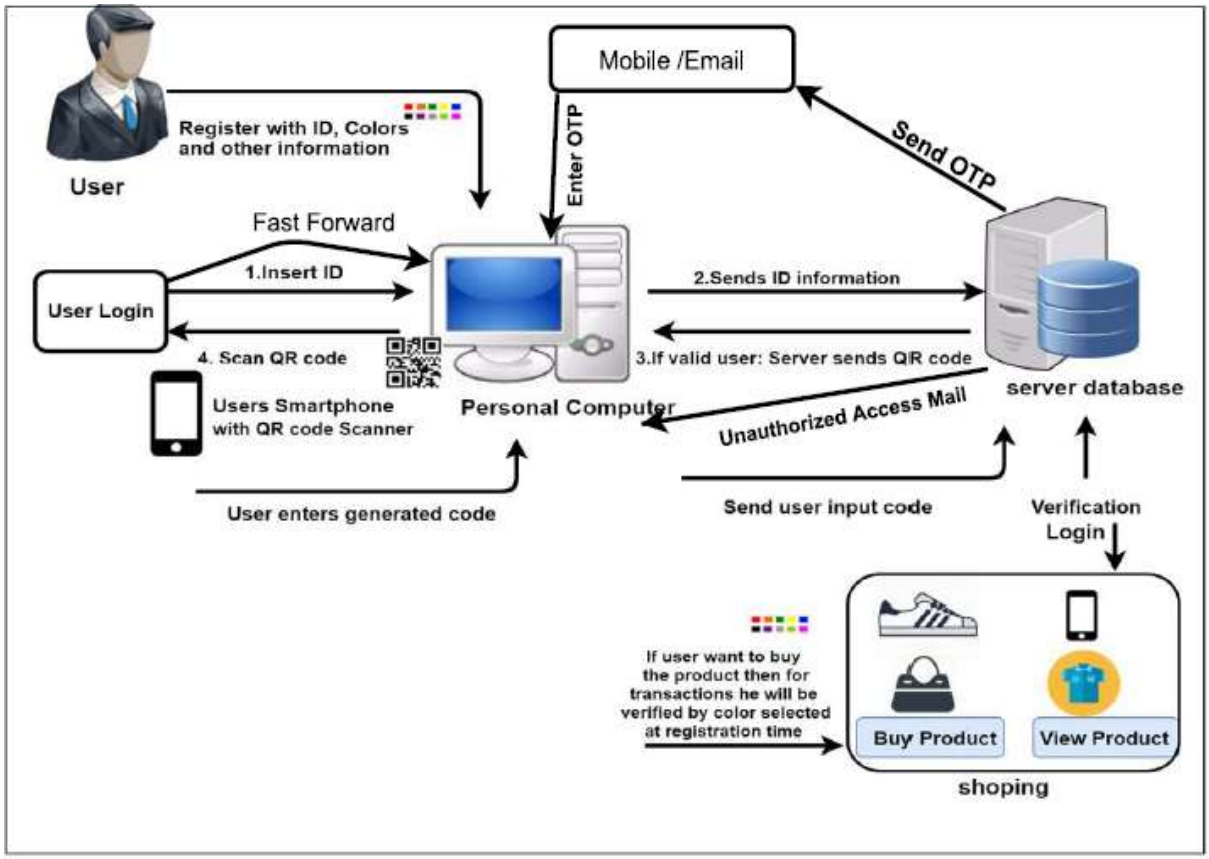

Fig 1: System Architecture

VII. ADVANTAGES

1. In this project we demonstrate how visualization can enhance not only security but also usability by proposing two visual authentication protocols
2. Improve the user experience
3. Resist challenging attacks, such as the key-logger and malware attacks.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

VIII.ALGORITHM AND TECHNIQUES

1. QR Code Generation:

QR codes have three parameters: Datatype, size (number of 'pixels') and error correction level. How many information can be stored there also depends on these parameters. For example the lower the error correction level, the

more information can be stored, but the harder the code is to recognize for readers.

The maximum size and the lowest error correction give the following values:

Numeric only Max. 7,089 characters

Alphanumeric Max. 4,296 characters

Binary/byte Max. 2,953 characters (8-bit bytes).

Random String Generation Technique

```
char[] chars = "1234567890abcdefghijklmnopqrstuvwxyz".toCharArray();
StringBuilder sb = new StringBuilder();
Random random = new Random();
for (int i = 0; i < 20; i++) {
 char c = chars[random.nextInt(chars.length)];
   sb.append(c);
}
String output = sb.toString();
```

Store Random String in Output Veriable, and Generate QR-Code using Random String.

2.AES Algorithm

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data the data to be encrypted. This array we call the state array.

- You take the following AES steps of encryption for a 128-bit block.

1) Derive the set of round keys from the cipher key.

2) Initialize the state array with the block data (plaintext).

3) Add the initial round key to the starting state array.

4) Perform nine rounds of state manipulation.

5) Perform the tenth and final round of state manipulation.

6) Copy the final state array out as the encrypted data (QR code).

These algorithm are used to file content are convert plaint text to cipher text(QR code)

System Methodology

Let W be the whole system which consists

Input = {U,M, C, k, S, Pvk, Pbk, M}.

1. Let u is the set of number of users.
   U= {u1,u2,…..un}.
2. k is the secret key used for encryption.
3. M is the message sent from the set M.
4. C is the cipher-text in the set C
5. S is the signature generated for sending message.
6. Pvk is the private key.

IX.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.

REFERENCES

[1.] D. Boneh and X. Boyen, “Short Signatures without Random Oracles,” Proc. Advances in Cryptology (EUROCRYPT), pp. 56-73, 2004.

[2.] J. Bonneau, C. Herley, P.C. Van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” Proc. IEEE Symp. Security and Privacy (SP), pp. 553-567, 2012.

[3.] J. Brown, “ZBar Bar Code Reader, ZBar Android SDK 0.2,” http://zbar.sourceforge.net/, Apr. 2012.

[4.] C.-sH.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,” Proc. ACMMOBICOM, pp. 92103, 2008.

[5.] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. 12th European Symp. Research in Computer Security (ESORICS), 2008.