www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 6 Issue 3 March 2017, Page No. 20641-20646*
*Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.45*

# Visual Authentication Protocol With QR Generation And Image Processing

***Prof. Archana Jadhav, Neemish Chavan, Ashish Chavan, Lokesh Bhoir, Balkrishna Naik***
Computer Department, Alard College Of Engineering, Pune
**Archana.Rasal700@Gmail.Com**
Computer Department, Alard College Of Engineering, Pune
**Cneemish@Gmail.Com**
Computer Department, Alard College Of Engineering, Pune
**Ashish361994@Gmail.Com**
Computer Department, Alard College Of Engineering, Pune
**Lokeshbhoir4@Gmail.Com**
Computer Department, Alard College Of Engineering, Pune
**Nviraj63@Gmail.Com**

**Abstract** – *The design of secure authentication protocols is quite difficult, considering that varied types of root kits reside in PC's (Personal Computers) to look at user's behavior and to create PCs un-trusted devices. Involving human in authentication protocols, whereas promising, isn't straightforward because of their restricted capability of computation and acquisition. Therefore, wishing on users to reinforce security necessarily degrades the usability. On the opposite hand, quiet assumptions and rigorous security style to enhance the user expertise will cause security breaches that may harm the users trust. In this paper, we tend to demonstrate however careful visualization style will enhance not solely the safety however conjointly the usability of authentication. thereto finish, we tend to propose two visual authentication protocols: one may be a one-time-password protocol, and therefore the alternative may be a password-based authentication protocol. Through rigorous analysis, we tend to verify that our protocols area unit proof against several of the difficult authentication attacks applicable within the literature. what is more, mistreatment an in depth case study on a epitome of our protocols, we tend to highlight the potential of our approach for real-world deployment: we tend to were able to win a high level of usability whereas satisfying rigorous security necessities.*

**KEYWORDS:** Keyboards, Visualization Usability Keylogger Authentication ,Smartphone

## 1. INTRODUCTION

Hospitals are very important part of our lives, providing best medical facilities to people suffering from various diseases. But keeping track of all the activities and records is very error prone and inefficient. It is also very less efficient and time consuming process observing the continuous increasing population and number of people visiting the hospital. Recording and maintaining the records are highly unreliable and error prone and very less efficient. It is also not economically and technically hard to maintain the records on paper. The main aim of project is to provide paper-less up to 90%. It also aims at providing low cost reliable, feasible and efficient automation of the existing system. There are various Keylogging attacks, extending from hardware and software based methods to acoustic examination. Including human in authentication and verification protocols, while guaranteeing, is not simple in light of their restricted capacity of calculation and remembrance of details. Quick Response (QR) codes seem to appear everywhere now a days. Using the QR codes is one of the most intriguing ways of digitally connecting consumers to the

internet via mobile phones since the mobile phones have become a basic necessity thing of everyone. For creating QR codes, the admin will enter text into a web browser and will get the QR code generated. While QR codes have many advantages that make them very popular, there are several security issues and risks that are associated with them. Running malicious code, stealing users' sensitive information and violating their privacy and identity theft are some typical security risks that a user might be subject to in the background while he/she is just reading the QR code in the foreground. A security system for QR codes that guarantees both users and generators security concerns will be implemented. The project exhibits how careful visualization outline can improve the security as well as the convenience of authentication.

## 2. LITERATURE SURVEY

### 2.1 2014-"Keylogging-resistant Visual Authentication Protocols"

**Author : DaeHun Nyang, Aziz Mohaisen, Jeonil Kang**

To mitigate the keylogger attack, virtual or onscreen key-boards with random keyboard arrangements are widely used in practice. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple keyloggers. Unfortunately, the keylogger, which has control over the entire PC, can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Another mitigation technique is to use the keyboard hooking preven-tion technique by perturbing the keyboard interrupt vector table. However, this technique is not universal and can interfere with the operating system and native drivers.Considering that a keylogger sees users' keystrokes, this attack is quite similar to the shoulder-surfing attack. To prevent the shoulder-surfing attack, many graphical password schemes have been introduced in the literature. How-ever, the common theme among many of these schemes is their unusability: they are quite complicated for a person to utilize them [1].

### 2.2 2012- "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,"

**Author : J. Bonneau, C. Herley, P.C. Van Oorschot, and F. Stajano**

Our focus is user authentication on the web, specifically from unsupervised end-user client devices (e.g., a personal computer) to remote verifiers. Some schemes examined involve mobile phones as auxiliary devices, but logging in directly from such constrained devices, which involves different usability challenges among other things, is not a main focus. Our present work does not directly examine schemes designed exclusively for machine-to-machine authentication, e.g., cryptographic protocols or infrastructure such as client public-key certificates. Many of the schemes we examine, however, are the technologies proposed for the human-to-machine component that may precede machine-tomachine authentication. Our choice of web authentication as target application also has significant implications for specific schemes, as noted in our results [2].

### 2.3 2011-"SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment"

**Author : M. Farb, M. Burman, G. Chandok, and J. McCune**

We envision SafeSlinger as a general approach to bootstrap secure digital communication. First, we enable groups of up to 10 individuals of physically co-located users to securely bootstrap trust by slinging keys between their devices (a one-time operation).1 SafeSlinger can also support remote exchanges, as long as users can authenticate the other individuals, e.g., via telephone communication or live video conference. Second, SafeSlinger supports secure

phone-to-phone messaging and file transfer, providing both secrecy and authenticity. Once users' devices hold each other's public keys, the SafeSlinger user experience is comparable to that of traditional SMS and MMS messaging today. Third, SafeSlinger enables secure introductions without physical meetings by allowing a common acquaintance to facilitate a mutual introduction using SafeSlinger file transfer. Fourth, we enable other applications to use the SafeSlinger API to add their public key to a contact entry. Now, when a user slings its updated contact list entry to another user, each application's public key is automatically included, and the receiver's corresponding application can extract the public key. This mechanism can enable applications such as secure email, secure SMS, and encrypted file sharing to solve the problem of securely exchanging the public key without requiring a leap of faith.2 Contributions. SafeSlinger is the first complete system that provides privacy-preserving and secure group credential exchange without any external trusted parties, restricting the exchanged information to other group members only. SafeSlinger is also the first secure group credential exchange system that can be used remotely over a telephone or video conferencing line. SafeSlinger is designed to be easy to use and defend against all attacks we are aware of. We implement SafeSlinger as an open-source project and make it available for free on Android and iOS app stores [3].

### 2.4 2011- "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers"

**Author : M. Mannan and P.C. van Oorschot**

e Internet services, online banking often requires only a bank card number (as userid) and password for authentication. Users input these credentials to a bank website to access their accounts. An attacker can easily collect these long-term secrets by installing a keylogger program on a client PC, or embedding a JavaScript keylogger on a compromised website. As plaintext sensitive information is input to a client PC, malware on the PC has instant access to these (reusable) long-term secrets. We argue (as do others – e.g. see Laurie and Singer , Kursawe and Katzenbeisser that for some common applications, passwords are too important to input directly to a typical user PC on today's Internet; and that the user PC should no longer be trusted with such plaintext long-term secrets, which are intended to be used for user authentication to a remote server. Additionally, phishing attacks can collect plaintext reusable userid-password pairs even if a user's PC is malware-free (through e.g. domain name hijacking, or the Kaminsky DNS-flaw. To safeguard a long-term password, we build on the following simple idea: use a hand-held personal device, e.g., a cellphone or PDA to encrypt the password (combined with a server generated random challenge) under the public key of an intended server, and relay through a (possibly untrusted) PC only the encrypted result in order to login to the server website. This simple challenge-response effectively turns a user's long-term password into a one-time password in such a way that long-term passwords are not revealed to phishing websites, or keyloggers on the untrusted PC[5].

### 2.5 2012- "Vigilare: Toward Snoop-Based Kernel Integrity Monitor"

**Author : H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek, and B.B. Kang**

Most of the existing solutions to kernel integrity monitoring make use of snapshot analysis schemes; they are usually assisted by some type of hardware component that enables saving of the memory contents into a snapshot, and then perform an analysis to find the traces of a rootkit attack. HyperSentry , Copilot, and HyperCheck are exemplary approaches on snapshot-based kernel integrity monitoring. A custom Peripheral Component Interconnect (PCI) card to create snapshots of the memory via Direct Memory

Access (DMA) in Copilot, and the System Management Mode (SMM) are utilized to implement the snapshotbased kernel integrity monitors in HyperCheck and HyperSentry. Snapshot-based monitoring schemes in general have an inherent weakness because they only inspect the snapshots collected over a certain interval, missing the evanescent changes in between the intervals. The term transient attack refers to attacks which do not leave persistent traces in memory contents, but it still achieves its goal by using only momentary and transitory manipulations.

**2.6 2011- "TOTP: Time-Based One-Time Password Algorithm"**

**Author : D. MRaihi, S. Machani, M. Pei, and J. Rydell**

Document describes an extension of the One-Time Password (OTP) algorithm, namely the HMAC-based One-Time Password (HOTP) algorithm,as defined in RFC 6238, to support the time-based moving factor.The HOTP algorithm specifies an event-based OTP algorithm, where the moving factor is an event counter. The present work bases the moving factor on a time value. A time-based variant of the OTP algorithm provides short-lived OTP values, which are desirable for enhanced security.The proposed algorithm can be used across a wide range of network applications, from remote Virtual Private Network (VPN) access and Wi-Fi network logon to transaction-oriented Web applications. The authors believe that a common and shared algorithm will facilitate adoption of two-factor authentication on the Internet by enabling interoperability across commercial and open-source implementations.

**2.7 2013 - "Designing Leakage- Resilient Password Entry on Touchscreen Mobile Devices,"**

**Author : Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng**

We implement three variants of CoverPad and evaluate them with an extended user study. This study includes additional test conditions related to time pressure, distraction, and mental workload. These test conditions simulate common situations for a dailyused password entry scheme, which have not been evaluated in the prior literature. We design new experiments to examine their influence based on previous work in psychology literature. Experimental results show the influence of these conditions on user performance and the practicability of our proposed scheme

**2.8 2000 - "Extensions to an Authentication Technique Proposed for the Global Mobility Network"**

**Author: Levente Buttyán, Constant Gbaguidi, Sebastian Staamann, and Uwe Wilhelm.**

In , an authentication technique has been proposed for use in the so-called global mobility network (GLOMONET), which provides a personal communication user with global roaming service. Authentication technique consists of the following two phases:

- *roaming-service-setup phase*, in which authentication that is required to set up the roaming-service environment is performed by the visited (roamed) network, the home net-work, and the roaming user;
- *roaming-service-provision phase*, in which authentication that is necessary to provide the roaming service within the visited network is performed only by the visited network and the roaming user.

The motivation for this two-phase model is to have the home network involved in the authentication process only once, during the roaming-service-setup phase. In this phase, a

secret key is established between the visited network and the roaming user with the help of the home network. This secret key is used later in the roaming-service-provision phase to authenticate the roaming user and the visited network to each other without any contribution from the home network. Thus, as long as the roaming user stays in the region of the visited network, authentication can be performed without contacting the home network of the roaming user (unlike, for instance, in the GSM system, where the visited network often has to obtain challenge-response pairs from the home network in order to authenticate the roaming user .

**2.9 2010- " Authenticated Group Key Transfer Protocol Based on Secret Sharing"**

**Author : Lein Harn and Changlu Lin**

Each user needs to register at KGC to subscribe the group key transfer service and to establish a secret withKGC. Thus, a secure channel is needed initially to share this secret with each user. Later, KGC can transport the group key and interact with all group members in a broadcast channel.The confidentiality of group key distribution is informa-tion theoretically secure; that is, the security of this transfer of group key to each group member does not depend on any computational assumption.The authentication of the group key is achieved by broadcasting a single authentication message to all group members.

**2.10 2011-"A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems"**

**Author : Xinyi Huang, Yang Xiang Ashley Chonka, Jianying Zhou, and Robert H. Deng**

Most early authentication mechanisms are solely based on password. While such protocols are relatively easy to implement, passwords (and human generated passwords in particular) have many vulnerabilities. As an example, human generated and memorable passwords are usually short strings of characters and (sometimes) poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time. Due to these concerns, hardware authentication tokens are intro-duced to strengthen the security in user authentication

## 3. EXISTING SYSTEM

Whenever a user types in her password in a bank's signin box, the keylogger intercepts the password. The threat of such keyloggers is pervasive and can be present both in personal computers and public kiosks; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a user's password is likely to be stolen in these computers. Even worse, keyloggers, often root kitted, are hard to detect since they will not show up in the task manager process list.

## 4. PROPOSED SYSTEM

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 keylogging attacks.

## 5. CONCLUSION

We proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. Proposed two of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our

protocols utilize simple technologies available in most out-of-the box Smartphone devices.

## REFERENCES

[1]2014-"Keylogging-resistant Visual Authentication Protocols" - IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 11 Author : DaeHun Nyang, Aziz Mohaisen, Jeonil Kang.

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

[3]2011- "SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment" Technical Report CMU- CyLab-11-021, Carnegie Mellon Univ. Author : M. Farb, M. Burman, G. Chandok, and J. McCune.

[4]2011- "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers" J. Computer Security, vol. 19, no. 4, pp. 703-750. Author : M. Mannan and P.C. van Oorschot.

[5]2012- "Vigilare: Toward Snoop-Based Kernel Integrity Monitor" Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 28-37. Author : H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek, and B.B. Kang.

[6]2011- "TOTP: Time-Based One-Time Password Algorithm" RFC 6238 Author : D. MRaihi, S. Machani, M. Pei, and J. Rydell.

[7]2013 - "Designing Leakage- Resilient Password Entry on Touchscreen Mobile Devices," Proc. Eighth ACM SIGSAC Symp. Information, Computer and Comm. Security (ASIACCS), pp. 37-48
Author : Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng

[8]2010- " Authenticated Group Key Transfer Protocol Based on Secret Sharing" Author : Lein Harn ChangluLin

[9]2011- "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems" Author : Xinyi Huang, Yang Xiang Ashley Chonka, Jianying Zhou, and Robert H. Deng