Deployment of QR Code for Security Concerns in Banking System

[1]**Dr. A. Suresh,** [2]Shaheen H,[3]Soumya S [4]Archana Nair M
[1]Professor & Head, [2]Assistant Professor, [3,4] UG Scholars
[1,2,3,4]Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, Coimbatore
[1]prisu6esh@yahoo.com, [2]shaheen66@gmail.com, [3]soumyaskhr999@gmail.com,[4]archanan622@gmail.com

Abstract: Revelation of password is a major security problem which affected millions of users and companies .User's passwords has to be protected from being stolen by adversaries. With the cyber security threats currently on the rise, websites are getting easily compromised which prompts administrators to find ways to secure them from the black hat community. A virtual password and QR code concept involving a small amount of human computing is adopted to secure user's passwords in on-line environments. User determined randomized linear generation functions is adopted to secure user's passwords based on the fact that a server has more information than any adversary does. The proposed scheme defends against phishing, key logger, and shoulder-surfing attacks. QR code mechanism is the first one which is able to defend against all three attacks together. In this paper, we discussed how to prevent user's passwords from being stolen by adversaries. Disclosure of password files is a severe security problem that has affected millions of user's. Since leaked passwords make the user target of many possible cyber attacks. Once a password file is stolen by using the password cracking technique is easy to capture most of the plain text passwords. Honey Word (decoy password) are proposed to detect attacks against hashed password databases. For each user account, the valid password of existing user is used as honey words. In this survey paper, study, we study QR code methodology and different attacking scenarios as well as different related approach to secure banking system.

Keywords — Cracking,Authentication,Password,Login,Virtual password

1. Introduction

Password also called as Secret word is the most essential resource for login during the time spent client confirmation. In this study, we separate the virtual password approach and give some analysis about the security of the system. In this respect we have pointed out that the strength of the QR code system. In most of the cases, clients pick simple passwords that can be effortlessly predicted by the attackers. To shield against the first secret key records QR code plays a vital part. It gives guard against the stolen secret key records. Although it is generally believed that password composition policies make passwords difficult to guess, and hence more free from, research has struggled to quantify the level of resistance to guessing provided by different password-composition policies or the individual requirements they comprise. secure system should detect whether a password file leak incident happened or not to take appropriate actions. In this paper, Differentiated QR code mechanisms is proposed in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure user's passwords.

2. Related Works

The merit of the system is that the intruder won't be able to hack the authentic bank user's account. But the drawback of using this technique is fewer authentications. So in our proposed system we focus on securing bank account details. QR code i.e.; machine readable code consisting an array of black and white square used to find URLS and other information's by using the camera of a phone. Thus a recent study was undertaken to research information posted on the web. The online environment have originally been developed assuming an ideal world where all user's are honourable. However, the dark side has emerged and bedevilled the world. This includes spam, malware, hacking, phishing, denial of service attacks, click fraud, invasion of privacy, defamation, frauds, violation of digital property rights, etc. The responses to the dark side of the Internet have included technologies, legislation, law enforcement, litigation, public awareness efforts, etc. when performing a dictionary-based password cracking attack can be a difficult task.

2. Technical Description

2.1. Implementation

2.1.1. Introduction

In this project, QR code system is implemented using some small amount of human computing to provide the security to the banking system.

2.1.2.Implementation Details

Modules

1. **Registration Module**
2. **Login Module**
3. **Secret Little Function Module**
4. **Virtual Password Module**
5. **Transaction Module**

Module Description

Procedure:

Step 1:

Registration Module

In the Registration Module, the users have to make registration here. As per the registration a jar will be downloaded as per the random value. User has to install the jar in the java supporting mobile. Using the jar only we will do the login form. In the jar there will be expression calculation. Expression varies for each jar. Expression will be stored in the database.

Step 2:

Login Module

In the login form the user will give the user name and password first. If the username and password is same means a random key will be sent to the access page. User has to install the jar and enter the random key contain in access page. As per the user expression calculation will be done and viewed in the access code text field. Please enter the value in the website if the value is correct means enter to the user's page.

Step 3:

Secret Little Function Modules:

There will be 11 jars the secret value and secret Function will vary for each jar. Calculation Part in the Secret Little Function module is as Follows: The access code values will be split into 3 parts. We split the value in 3 parts and assign to the 3 variables eg a, b, c. Then a will be added with X variable b will be subtract with x variable and c will be multiplied with x. Here x value will vary for each jar. Assign the value as a1, b1, c1. Secret Function will vary for each user. The expression calculation will be in a1 b1 c1 format only. The values will be passed to the expression and generated code will be generated.

Step 4:

Virtual Password Module

In the Virtual Password module the Secret Function calculation will vary for different jar. The use get the random value and generated value in dynamic format. Virtual means dynamic. Random number keep on changing so that Generated code will also keep on changing dynamically.

Step 5:

Transaction Module

The bankers have to rights for creating new bank accounts for user who wants to keep money on bank. Users may have personal accounts or corporate accounts for doing transactions through online from anywhere in the world. Each user has provides user id and password by bank administrators for doing online transactions.

In this module Account holders are able to do online account transactions like Fund Transfer, With Draw and Deposits. Account holders have to register their personal information and send report their account transaction to Financial Intelligence. And also they can view the summary of Transaction details and view balance of his account.

I. Account Transaction

Here, the account holder can do their account transactions through online. Each transactions has maintained by transaction number. It is unique no.

1.Fund Transfer
2.Withdraw
3.Deposit

II. View Account Information

In this module, account holder can view the account information, balance information and transaction information.

Step 6:

Financial Intelligence

The Financial intelligence people can view the account holder's information from Know your customer. Each Account holder will have unique id. It will generate automatically. The main process is to view and filter money transactions and monitor their transactions information through online. If transactions is suspicious means that record has to maintain separately. It stores at Suspicious Activity report and update status after finishing enquiry

I. Money Transaction Report

In this form, they can view what are all the transactions has made by account holders. It may be withdraw, deposit and fund transfer. They can filter their transactions depends upon their turnover and giving amount on the dynamically.

2.2. Proposed System:

In the proposed a QR code concept involving a small amount of human computing to secure user's Passwords in online environments. We proposed differentiated security mechanisms in which a user has the freedom to choose a QR code scheme ranging from weak security to strong security. The function/program is used to implement the QR code concept with a tradeoff between security and complexity and requires small amount of human computing. However, since simplicity and security conflict with each other, it is difficult to achieve both. We further proposed several functions serving as system recommended functions and provided a security analysis. We analyzed how the proposed schemes defend against phishing, key-logger, shoulder-surfing attacks, and multiple attacks. In user-specified functions, we adopted secret little functions in which security is enhanced by hiding secret functions/algorithms. In conclusion, user-defined functions (secret little functions) are better.

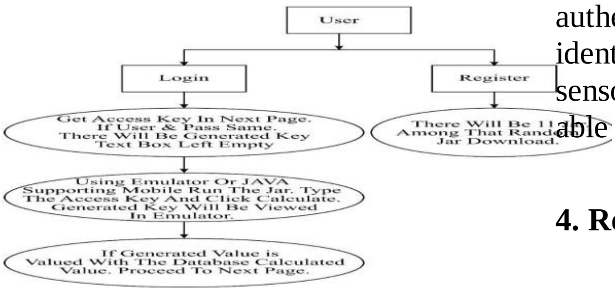
User
Login
Register
Get Access Key In Next Page. If User & Pass Same. There Will Be Generated Key Text Box Left Empty
There Will Be 11 Jar Among That Random Jar Download.
Using Emulator Or JAVA Supporting Mobile Run The Jar. Type The Access Key And Click Calculate. Generated Key Will Be Viewed In Emulator.
If Generated Value is Valued With The Database Calculated Value. Proceed To Next Page.

Fig -1: System Architecture

3. Conclusion and Future Works

Security of the virtual password system has been studied. In QR code based verification approach, it is sure that the intruder won't be able to hack the account of the authentic bank user. The main aim of project is to protect the bank accounts from being hacked by the adversaries. Use of QR code is very beneficial and works for each user accounts. QR code acts against most of the cyber attacks at the same time.In our future work, the software executes successfully by fulfilling the objectives of the project. Further extensions to this system can be made which require, minor modifications. We have planned to design and develop an efficient service to protect user's data privacy is a central question of cloud storage. The inventions can also be implemented in various fields like digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them etc. Apparatus of the invention can be implemented in a computer program product tangibly included in a machine-readable storage device for execution by a programmable processor and method steps of the invention can be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. For future enhancement we planned to implement by using the below hardware components like RFID TAG, BIOMETRIC FINGERPRINT KIT, BARCODE SCANNER etc. Before the voice command controller process it checks whether the login person must be authenticated or not. By using the unique identification components like fingerprint sensor and barcode scanners we will be able to find the authentic user.

4. References

- D. Mirante and C. Justin, —Understanding Password Database Compromises,‖Dept.of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02, 2013.
- F. Cohen, —The Use of Deception Techniques: Honeypots and Decoys,‖ Handbook of Information Security, vol. 3, pp. 646–655, 2006.
- K. Brown, —The Dangers ofWeak Hashes,‖ SANS Institute InfoSec.
- Reading Room, Tech. Rep. 2013.
- [3] M. Hazas, H.Scott, J. Krumm, Location-Aware Computing Comes of Age, IEEE Computer, 37, 2, February 2004.
- [4] A. Ward, A. Jones, A. Hopper, A New Location Technique for the Active Office, IEEE Personal Communications, Vol. 4 (5), October 1997, pp 42-47.
- [5] M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald, Privacy-Aware Location Sensor Networks, USENIX 9th Workshop on Hot Topics in Operating Systems (HOTOS IX), May 2003, pp. 163-167.
- [6] W. Jansen, V. Korolev, S. Gavrila, T. Heute, C. Séveillac, A Framework for Multimode Authentication: Overview and Implementation Guide, NISTIR 7046, August 2003.
- [7] W. Jansen, T. Karygiannis, M. Iorga, S. Gavrila, V. Korolev, Security Policy Management for Handheld Devices, The 2003 International Conference on Security and Management (SAM'03), June 2003.

- [8] Entity Authentication Using Public Key Cryptography, Federal Information Processing Standards Publication (FIPS PUB) 196, U.S. Department of Commerce, National Institute of Standards and Technology, February 1997.
  [9] A.Suresh (2015), "Authorized Third Party Auditing and Integrity Verification in Cloud Computing", International Journal of Research in Science and Technology, (IJRST) ISSN: 2394-9554, *Vol. 2, No.1, Jan-Mar 2015,* pp. 95 – 103.