ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Secure Internet-Banking with Visual Authentication Protocols

Dr. S.Saravana Kumar[1], R.Senthil Kumar [2], P.Venkatraman[3], M.Thamodharan[4], S.Vishnu Prashod[5]

Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[1]

Associate Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[2]

UG Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[3,4, 5]

ABSTRACT: The major threat in authentication involved in the banking sector is key logging. Key logging refers to monitoring the action of user without their knowledge and illegally accessing it for their own purpose. It can be done either through hardware, software and acoustic analysis. key logging, an approach to counter key logging by the use of authentication protocols which have not provided desired security. Thus, we propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.

KEYWORDS: Smart phone, QR-code, IMI Security.

I. INTRODUCTION

In addition to advancement in technology and applications, providing security to Net Banking is challenging. In the context of e-banking there are large amount of work and more complexities in providing authentication using graphical password and attacks on them [4]. It is challenging for users to combat key loggers; the only possible method is to use an appropriate security solution [5].The Demerits of Existing System:
[1] Session hijacking, an act of tracing the password which is stored in the server through URL for illegal access.
[2]. Keyboard and mouse events can be traced by OS calls and OSK keystrokes can be monitored by screenshots spywares.
[3]Graphical password with distorted image is difficult to remember.

Thus we go for randomized On-screen keyboard, where key-loggers find it difficult to determine the positions of the numbers which keeps changing every time when smart phones scan the QR-code. A QR code contains black modules (square dots) arranged in a square grid residing on a white background, which can be read by a device (such as a camera) and processed until the image can be appropriately interpreted. QR-code is encrypted and decrypted by RSA algorithm. Server will generate public key on backend and an equivalent private key which is to be entered by user. We also provide additional features such as instant transaction and IMI security.

II. EXISTING SYSTEM

Secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. The attacker is capable of creating a fake server to launch phishing or pharming attacks. Therefore, relying on users to enhance security necessarily degrades the usability. On the other hand, relaxing assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm the users' trust.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

There are many Keylogger types, but in general they can be classified in three categories: hardware, software, and web keyloggers. Hardware keyloggers are plugged in the hardware system, between the input devices and a computer [2]. Web keyloggers are web scripts written in Java and can often open an invisible pop-up window and collect user information. Also, it is possible to embed malicious code into vulnerable web sites to collect data entered by the user.
Today's Keyloggers can record keyboard keys pressed by the keys on the virtual keyboard. Such Keyloggers receive consecutive screenshot from the victim's monitor, and can then identify strokes of the keys.Also today's Keyloggers instead of running through the Startup, they run through Task scheduler (i.e. they run at a specific time and date, e.g. 5 minutes after loading the operating system), or as a Service in objects in which Antivirus software have less control over their actions.
Today's Keylogger's makers are capable to change its assembly by using specialized software after creating their Keylogger, so that it encapsulated. After encapsulating the Keylogger, a lot of security software will not have the ability to identify the new Keylogger.
Another way in which attackers apply Keyloggers to infect their victims is JDB Keylogger. In fact, this type of Keyloggers is combination of Software Keylogger and Web Keylogger. In this approach, attacker created Java file on a website and written running code of the file in Java on the site. Anyone visit the site; Keylogger will taint his operation system.

III. PROPOSED WORK

The proposing two visual authentication protocols: one for password-based authentication, and the other for one-time-password.
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.

(OTP) One-Time-Password

 The OTP protocol generates random numbers for authentication, where the position of the numbers tends to change for every transaction done by the user.

 The QR code will be on the left-hand side and randomized plain keyboard is in right- hand side thus account holder using his android phone to scan the QR code

 The QR code is decrypted using his private key, then the OTP appear on his mobile
, the OTP contain randomized (0 to 9) number placed in different place.

Password-based authentication

 uses a password shared between the Server and the user, and a randomized keyboard.

 User views a randomized (0 to 9) number placed in different place in (4x4) matrix in his android mobile.

 Then the user click the password in randomized plain keyboard using the mouse with the help of OTP if the password is matched then fund/amount is transferred.

QR-CODE

To use QR codes conveniently you must have a smart phone equipped with a camera and a QR code reader/scanner application feature. Luckily, the newer smart phones models available today often have an app pre-installed on them. Now that you have the tools you need, let's get to scanning. Go out and find yourself a code. Get out your phone and open the app downloaded or that already exists. Steady your hand while the QR code is centered on the screen, as soon as it is done scanning whatever information were stored in the QR code should be displayed to the user.

RSA Algorithm

Step: 1. Choose two very large random prime integers: p and q
Step: 2.Compute n and φ(n):

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

n = pq and φ(n) = (p-1)(q-1)

Step:3. Choose an integer e, 1 < e < φ(n) such that:
gcd(e, φ(n)) = 1(where gcd means greatest common divisor)

Step:4. Compute d, 1 < d < φ(n) such that:
ed ≡ 1 (mod φ(n))

- The public key is (n, e) and the private key is (n, d)
- The values of p, q and φ(n) are private
- e is the public or encryption exponent
- d is the private or decryption exponent

Encryption

The cipher text C is found by the equation 'C = M^e mod n' where M is the original message.

Decryption

The message M can be found form the cipher text C by the equation 'M = C^d Mod n'.

Instant Transactions

We provide offline transaction to reduce time consumption and quick access. User generates a file containing account related information when they are in offline .When the user enters online he just uploads the file into application for fund transfer.

IMI Security

The necessity to go for IMI security is to avoid malicious transactions and avoid unauthorized users from fund transaction even after they know the user name and password. The IMEI number is a 15 digit number which is unique for every phone and it is stored in database by registration server. When another malicious user tries to use my username and password in their mobiles then IMI number will vary and thus proper transaction is not possible.

A simple example

This is an extremely simple example and would not be secure using primes so small, normally the primes p and q would be much larger.

1. Select the prime integers q=11, q=3.
2. n=pq=33; φ(n)=(p-1)(q-1)=20
3. Choose e=3
   - Check gcd(3,20)=1
4. Compute d=7

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

o (3)d ≡ 1 (mod 20)

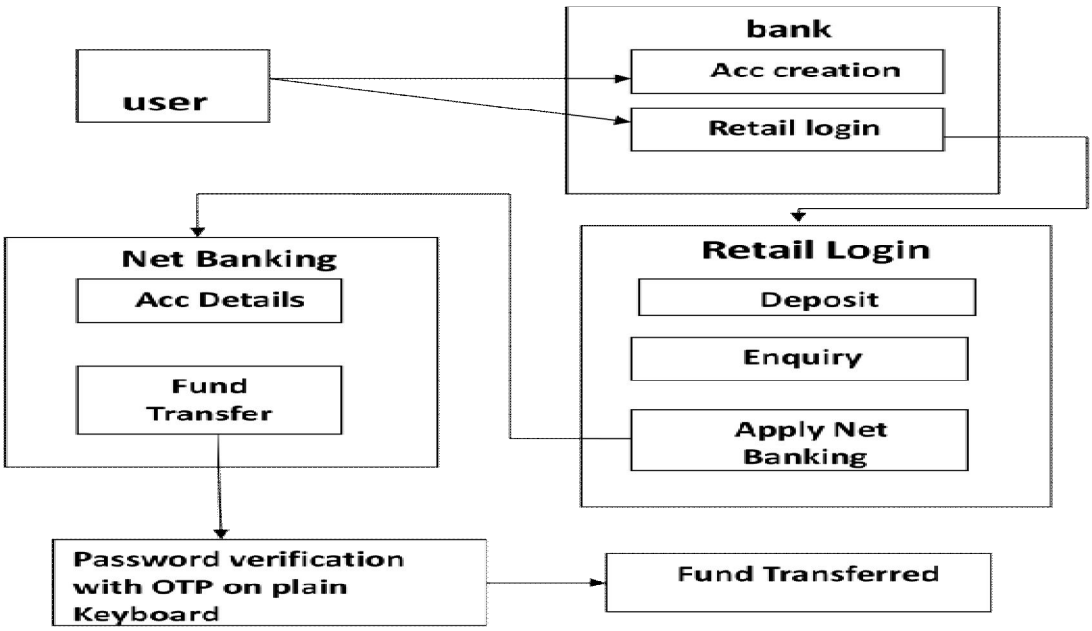
Therefore the public key is (n, e) = (33, 3) and the private key is (n, d) = (33, 7).Now say we wanted to encrypt the message M=7

- $C = M^e \bmod n$
- $C = 7^3 \bmod 33$
- $C = 343 \bmod 33$
- $C = 13$

So now the cipher text C has been found. The decryption of C is performed as follows.

- $M' = C^d \bmod n$
- $M' = 13^7 \bmod 33$
- $M' = 62{,}748{,}517 \bmod 33$
- $M' = 7$

As you can see after the message has been encrypted and decrypted the final message M' is the same as the original message M. A more practical way to use the algorithm is to convert the message to hexadecimal and perform the encryption and decryption steps on each octet individually.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

MODULES

- Create New Account
- Apply Net Banking
- Randomized Onscreen Keyboard

Create New Account

User create a new account in our banking application to give an input for user detail in our new account registration .User detail must be a valid information (ex:-phone-no, Username, etc...) and the form is submitted to corporate.

Apply Net Banking

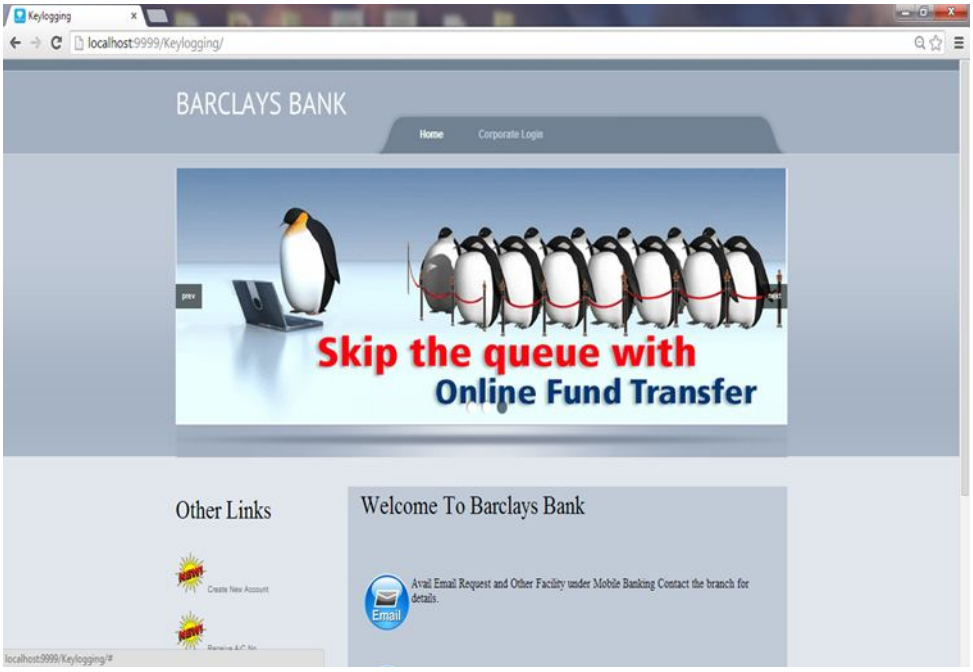
User receives an account number he/she is entering a retail login and applies a net banking as services. This service allows the account holder to view his profile, account details and to transfer the fund in another account.

Randomized Onscreen Keyboard

Account holder transfer the fund in another account he/she enter the account number and amount then before enter the password. Our banking application uses a two visual authentication protocols.

IV. SCREENSHOT

HOME PAGE



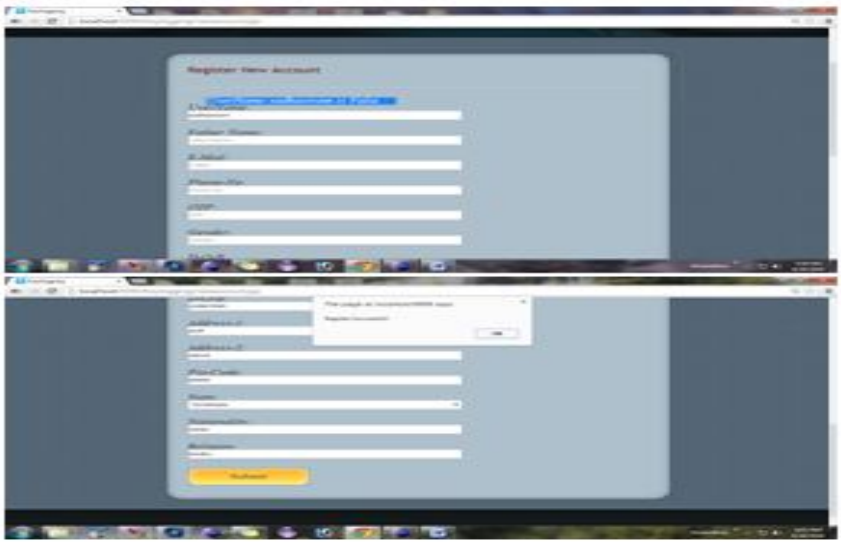
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

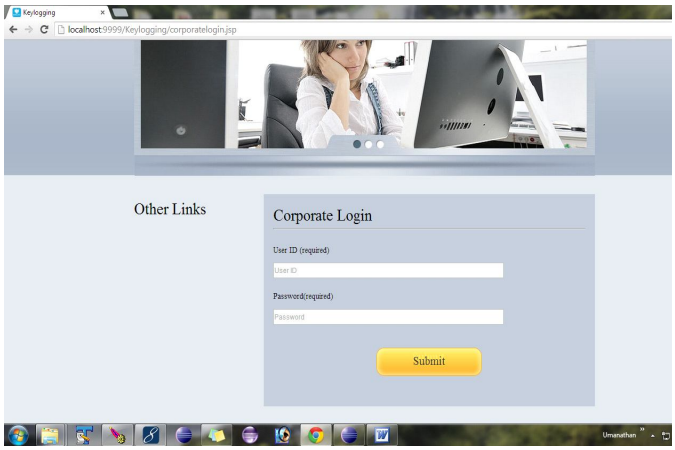
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

REGISTRATION FORM



CORPORATE LOGIN



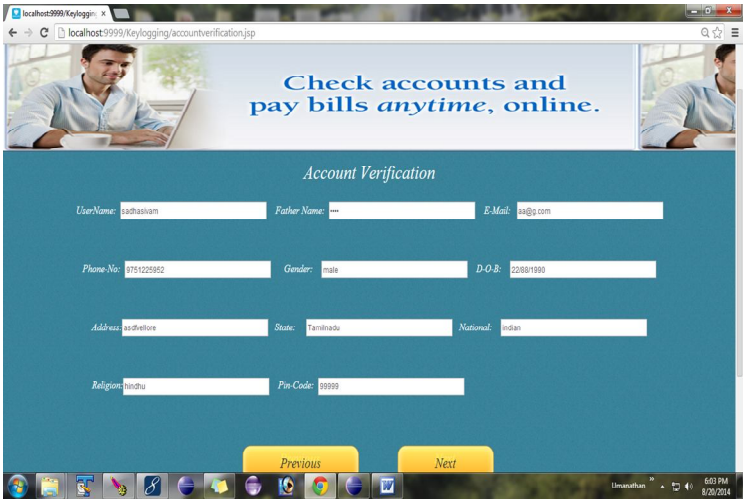
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

ACCOUNT VERIFICATION



SCANNING QR-CODE

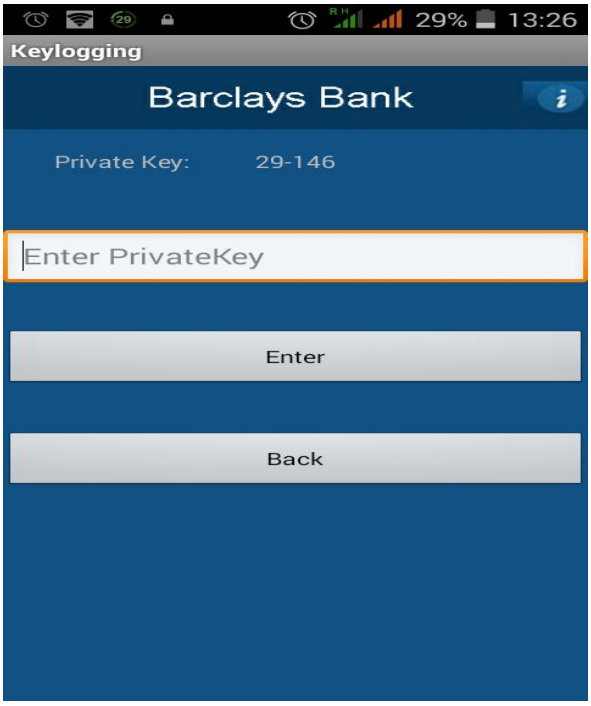
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

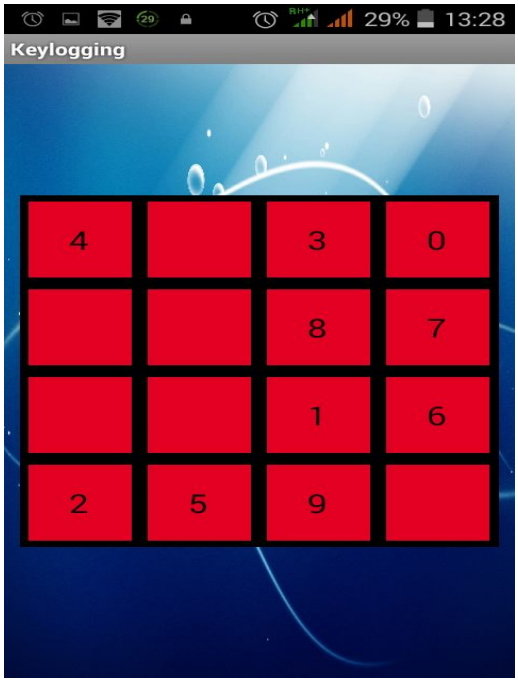
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

DECRYPTION



ONE TIME PASSWORD



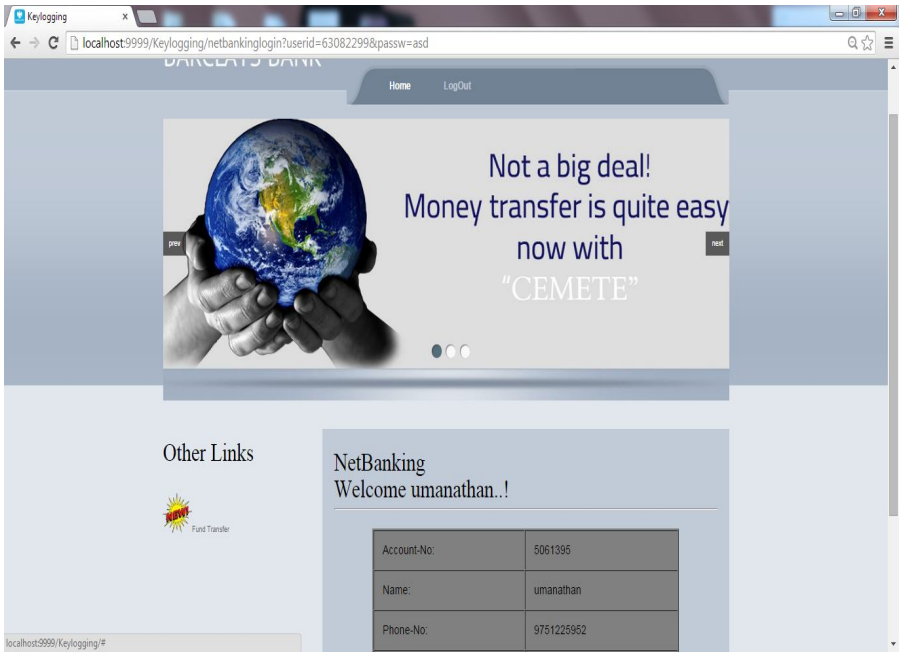
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

FUND TRANSFER



V. CONCLUSION

Thus using visual authentication protocols we provide more security to the banking transaction than ordinary authentication protocols. The additional features to our system is Instant transaction and IMI security.

VI. FUTUREWORK

In future we try to provide alpha-numeric characters as password which will make key loggers difficult to crack the password.

REFERENCES

[1] C. Karlof, U. Shankar, J. D. Tygar, and D. Wagner. Dynamic pharming attacks and locked same-origin policies. In Proc. of ACM CCS, pages 58–71, 2007.
[2] C. Herley and D. Florencio "How to login from an internet cafe without worrying about key loggers". In Proc. of ACM SOUPS, 2006.
[3] E. Hayashi, R. Dhamija, N. Christin and A. Perrig. Use your illusion: secure authentication usable anywhere. In Proc. of ACM SOUPS 2008.
[4] A. Slowinska and H. Bos. Pointless tainting?: evaluating the practicality of pointer tainting. In Proc. of ACM Euro Sys, pages 61–74, 2009.