

An Enhanced Countermeasure Technique for Deceptive Phishing Attack

K. Selvan¹, Dr. M. Vanitha²

Research Scholar and Assistant Professor, Department of Computer Science,
JJ College of Arts and Science (Autonomous), Pudukkottai, TamilNadu

Assistant Professor, Head, Department of Information Technology,
JJ College of Arts and Science (Autonomous), Pudukkottai, Tamilnadu

Abstract: *The trust on internet and e-banking are more affected and attacked by fraudulent activities performed by fake web sites. When their look and feel is similar to legitimate web sites users spoofed very much. Online criminal activity are using the collection of social engineering methods such as messages and emails to make the users to disclose their sensitive information such as personal details, username password, etc. The strong techniques are required to avoid fraudulent fund attacks. In the proposed work Multi Factor Authentication (MFA) and secure session key generation using Gaussian distribution to reduce the attacks caused by the attackers. Multi Factor Authentication technique authenticates the users using user's finger print image recognition and secret question answer. After successful authentication of user using Multi Factor Authentication technique, session key generated using Gaussian distribution is sent to user's mobile phone. User proceeds with the transaction only after entering the session key received. Every time user attempts their authentication the counter measure will perform and made action when user attempt more than 3 times. By incorporating above mentioned techniques users can perform online transactions safely and securely.*

Keywords: Authentication, Phishing, MFA, Counter Measure, Banking.

1. Introduction

Phishing is a social engineering attack where the attacker looks for weakness in the users and steals their personal information. The term Phishing originated from two words Preaching (hacking of Phone calls which are the earliest method of hacking).

Previous work in the context of website phishing has shown that users tend to ignore the absence of security indicators and fall victim of the attacker. Consequently, the research community has deemed personalized security indicators as an ineffective phishing detection mechanism.

Phishing attacks are classified in to 2 major types. Malware and deceptive phishing attacks. Malware phishing attack happens by installing the destructive software in the system of the user. In Deceptive phishing attacks, false emails are sent to the user's inbox. one is through making the software strong enough to identify such fake emails and websites and alerting the users.

A server receives identifying information of a user of a client device and data encrypted with a public key of a group, where the encrypted data includes an encrypted session key for secure content. The server determines whether the user is a member of the group using the identifying information of the user. If the user is a member of the group, the server decrypts the encrypted session key using a private key of the group, and causes the client device to obtain a session key to access the secure content.

The purpose of this project is to develop a secure multi-factor authentication that would provide high security in their own web-applications. The risks of using static passwords to authenticate users show more and more security risks with the development of hacking.

Multifactor Authentication is the latest secure authentication technique. Since Single-factor authentications (SFA) have been used widely. It is not secure enough for online financial transactions. Single factor authentication has been around for a while now. Yet it's not enough for having any meaningful security. The solution is to have multi-factor authentication which includes following authentication factors: Username, Question Answer Verification, Image Authentication, Password .The security levels are increased by using multiple authenticating factors. Multi-factor authentication adds more Security because the user must provide more than one secret Entity i.e. the security question.

2. Related Work

S. Manasa et al proposed, Multi Factor Authentication (MFA) technique used has four phases of authentication as shown in the above section. The MFA enhanced the security level of online bank transactions against phishing attacks. Hackers are prevented successfully to a large extent from accessing the legitimate user's transactions. The Gaussian distribution based session key generation also enhances the security of online bank transactions [1].

Niharika Guptaas et al proposed, Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as an application and the other of which is typically something memorized, such as a security code or password. In this context, the two factors involved are sometimes spoken of as something you have and something you know. The need for encrypting Passwords comes from fact that we need to protect passwords of users . The users then will be prevented from attacks like brute force attack, phishing, Distributed Denial of Service (DDOS) through password encryption and multifactor authentication(via One Time Password and image security at registration).[2]

Vyanktresh Dorlikar et al proposed the techniques began with Basic Authentication, which considers user name and password system to Multifactor Authentication which considers knowledge factors, possession factors and inherence factors. The Multifactor Authentication technique is most secured among discussed authentication modes. Other secured techniques such as Windows Authentication and Secured Socket Layer are developed and used in the internet or the system usage authentication. The authentication techniques in smart phones such as Biometrics, Facial Recognition, Voice Control access and location tracking are also developed and widely used in individual capacity along with organizational level [3].

Di Liu et al proposes a two factors user authentication scheme for Beijing medical registration platform, in order to safeguard user privacy information on the platform and protect against attacker abuse. The SMS-OTP solution is chosen as the optimal way for user authentication of the Beijing medical registration platform. This scheme helps the platform to make up user authentication process during user log on [4].

Amr Farouk et al present an investigation on the authentication mechanisms in grid computing environment. Authentication mechanism in grid computing environment has to be secure and robust, moreover it should fulfill the requirements of large scale distributed and heterogeneous grid computing environment [5].

3. Proposed Work

In proposed work, we proposed Multi Factor Authentication (MFA) and secure session key generation using Gaussian distribution with counter measure to reduce the attacks caused by the phishers. MFA technique authenticates the users using user's signature image recognition and secret question answer. The user needs to enter username in the bank's login web page; if it is matched the user is provided with exact registered user's signature image along with 3 altered signature images and is asked to select his correct signature image for authentication. If it is successfully matched, the user is redirected to answer the secret question which is known only to him. In the above 2 steps of authentication, user tries to attempt wrong credentials, his/her net banking account will be blocked. After successful authentication of user using MFA technique, session key is generated using Gaussian distribution and sent to user's mobile phone [6]. User proceeds with the transaction only after entering the session key received. In every time the counter measure will perform to measure the user authentication level. Finally, user successfully logs out after performing secure and safe transaction.

4. Methodology Used

A. User Authentication

This is the first module of all applications which contains the user registration and login and administrator's login. In the previous stages, an unknown user also can block the valid user account without knowing the password of the account holder [7].

B. Fingerprint Recognition

A fingerprint is the group of ridges and furrows of all or any part of finger. Through various studies it has been observed that each person has its own fingerprint and doesn't change during whole life. Hence, they are unique for every individual. A fingerprint quality is damaged when, our fingerprint cuts or burns. But after some time it is come back in its original quality. So it is used for identification and verification of any persons and used by many organizations.

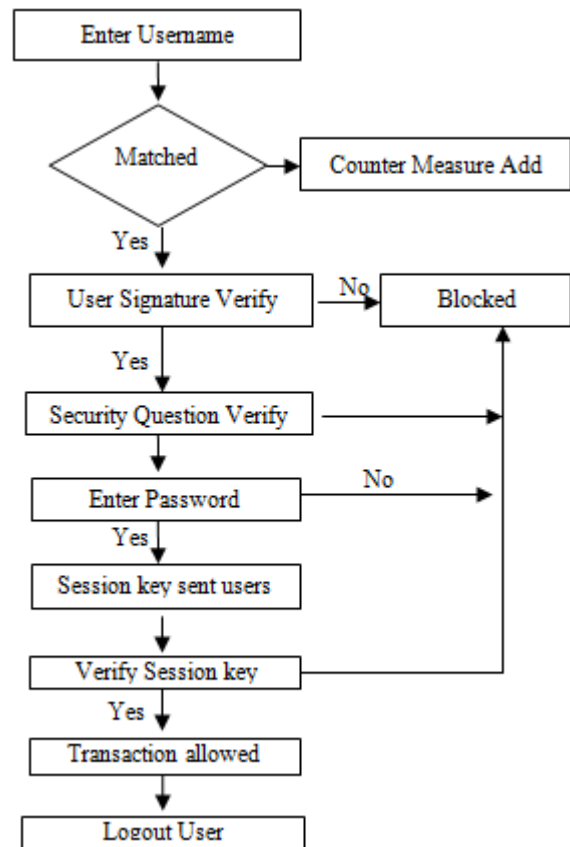


Figure 1: System Architecture for Proposed System

Fingerprint Modes: - It has two modes.

- Fingerprint Verification: - In this, two fingerprints are compare by using some methods and verify original fingerprint.
- Fingerprint Identification: - After verification, system automatically identify the person.

In my thesis I have used both modes.

Fingerprint Matching: - In fingerprint matching minutiae points are extracted from both the fingerprints and calculate the similarities between two fingerprint images.

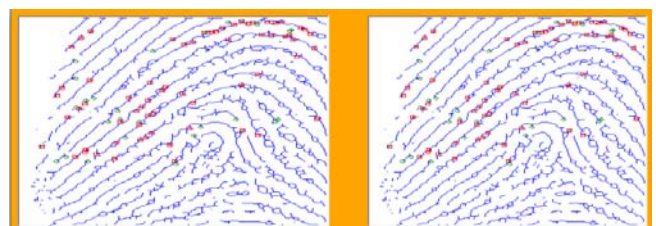


Figure 2: Fingerprint Template

C. Generation of Random Numbers using Gaussian distribution

Some existing methods for generating standard normal random numbers discussed in this section. A new algorithm to generate standard normal random numbers is also proposed and is named.

Method-1: Sum of Uniform Random Variables

The simplest way of generating normal variables is an application of the central limit theorem. The central limit theorem is a weak convergence result that expresses the fact that any sum of many small independent random variables is approximately normally distributed. Use of the central limit theorem on $U(0,1)$ random variables provide a simple method for closely approximating normal random variants. The following algorithm is used to generate the standard normal variables [8].

1. Generate 12 independent uniform numbers,

$$U_1, U_2 \dots U_{12} \sim iid U(0,1)$$

$$2. \text{Return } Z = \sum_{i=1}^{12} U_i - 6.$$

This method requires 12 uniform random variables to generate a single standard normal random number.

D. Counter Measure

Meanwhile there are a lot of protection mechanisms against Phishing and online scammers. These proposals can roughly be separated into two categories: modifications of the traditional authentication and authorization-method (PIN/TAN) on the one hand and approaches that try to reduce the probability of a scammer being successful without changing the procedure on the other hand [10].

5. Experimental Results

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

- Knowledge factors ("things only the user knows"), such as passwords
- Possession factors ("things only the user has"), such as ATM cards
- factors ("things only the user is"), such as biometrics

A. Usernames and Passwords

The most common method for user identification is username password. The idea behind this is user has a unique identifier and also one password, when user authenticates, user provides his unique identifier and password. The user is only one who knows the password, so he is authenticated. This approach is very simple as assigning a unique identifier and user supply password [9].

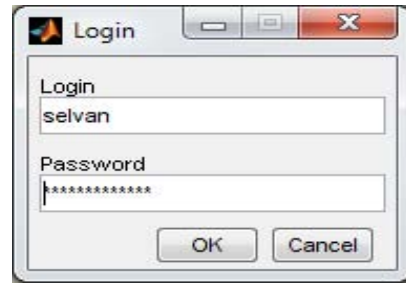


Figure 3: User Authentication

Figure 3 shows simple authentication that is user enter unique identifier, here is email and secret password. This is most widely used method for authentication but this is not a secure. Password should be difficult to guess. So it is difficult to user to remember password.

B. One-Time Password

One-Time Password approach is similar to the simple username password. This method uses client side generator and server. Generator accepts a secret password from user and concatenates it with some information sent from the server in control of the authentication various computations and hashes are performed on the user's secret password which can be verified by computations by each end of the communication. This type of system can protect against passive attacks against which basic password systems maybe vulnerable.



Figure 4: OTP Verification

C. Fingerprint Recognition

Biometric technologies are most commonly combined with a password or a token to produce a multifactor authentication system. Fingerprints are classified as physiological characteristics. The rate of movement, such as the pattern of typing on a computer keyboard is classified as a physical characteristic. During the enrollment process, a sample of data relating to the user's characteristics is gathered and stored in the biometric-based system as the template.

Algorithm

Input: Gray-scale Fingerprint image.

Output: Verified fingerprint image with matching score.

- 1) Fingerprint is binarized
- 2) Thinning on binarized image
- 3) Minutiae points are extracted. Data matrix is generated to get the position, orientation and type of minutiae.
- 4) Matching of test fingerprint with template
- 5) Matching score of two images is computed, if matching score is 1 images are matched and if it is 0 then they are mismatched.



Figure 5: Fingerprint Region Grow

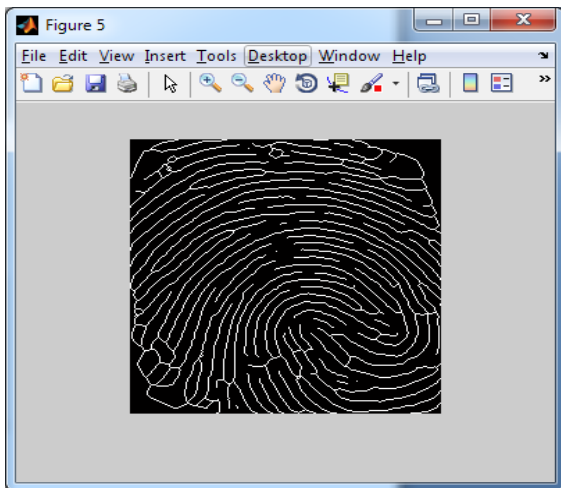


Figure 6: Vector Prediction for Finger print Template

D. Session Key Generation

This is an authentication service that makes use of a Session Key in addition to the conventional ID and password for personal identification. User can use this Session Key for better security during online transaction by generating special password to their system. User can perform authentication by entering an Session Key displayed by the system application in addition to their normal ID and Password. The Session Key passwords are specific to each user, and a new password is generated every minute. Even if the password is obtained by a third party fraudulently, it cannot be used outside its lifetime.

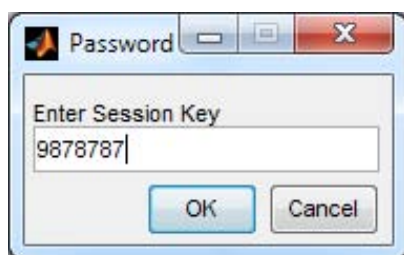


Figure 7: Session Key Verification

E. Countermeasure

When the intruder tries to modify any data or create any malicious event, the intruder is not permitted to perform the activities since intrusion is done with unauthorized user name and password. If the changes are done with

unauthorized access then the information of the intruder are gathered and it is being sent to the administrator in the secure manner. From those details the intruder can be identified very easily and any further action performed by the intruder can be blocked thus preventing code injection. The details like IP address, hostname, date, time, path, etc., are reported.

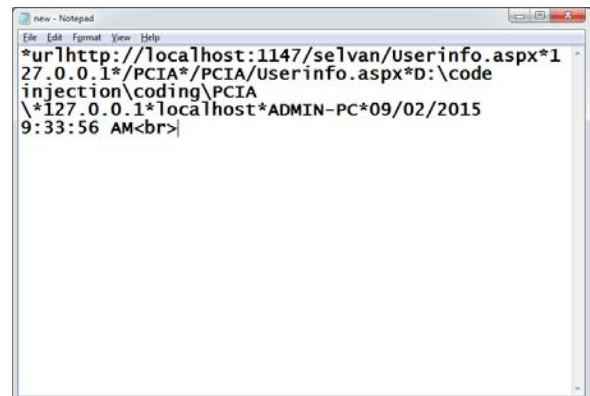


Figure 8: Phisher Detection

6. Conclusion and Future Work

Multifactor authentication provides better security to customers by making use of more than one form of authentication to validate a transaction. Although not mandatory, banking services should consider the implementation of multifactor authentication as it provides better security for their customers using their online services. They must understand that the costs of providing the security may be compensated by customer confidence and smaller losses from thefts. Banking need to perform a risk assessment to determine the type of authentication required. However, institutions must take into consideration customer acceptance and the ease of development of the technology, as tokens may need to be distributed during enrolment. They need to be aware that criminals may simply switch to other forms of frauds that do not require usage of the internet.

There are few areas in which the research is complete and this is no exception. The proposals made here depend on a number of assumptions as to the feasibility of creating the device and the cost of manufacture. Before any sort of deployment can be considered these are critical questions which need to be answered. From surveying similar technology it is likely to be possible, but that was not the focus of this research.

References

- [1] Securing Online Bank Transactions from Phishing Attacks using MFA and Secure Session Key by S. Manasa, P. Mullaimalar, G. B. Gnanaprakash Singh and S. S. Manivannan.
- [2] Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography by Niharika Gupta and Rama Rani.
- [3] A Survey on Authentication Techniques and User Recognition by Vyanktresh Dorlikar, Anjali Chandavale.
- [4] A Two Factor User Authentication Scheme for Medical Registration Platform by Di Liu, Zhi-Jiang, Zhang Ni Zhang.

- [5] Authentication Mechanisms in Grid Computing Environment: Comparative Study by Amr Farouk, Ahmed A. Abdelhafez and Mohamed M. Fouad.
- [6] Dhanalakshmi R, Prabhu C, Chellapan C. Detection of phishing websites and secure transactions. IJCNS. 2011; 1(11):15–21.
- [7] Belabed A, Aimeur E, Chikh A. A personalized whitelist approach for phishing webpage detection. 2012 Seventh International Conference on Availability, Reliability and Security; 2012 Aug 20–24. p. 249–54.
- [8] Chaudhari S, Tomar SS, Rawat A. Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for web mail access in multi trust networks. 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC); 2011 Apr 22–24. p. 27–32.
- [9] Hazlewood V, Kovatch P, Ezell M, Johnson M, Redd P. Improved grid security posture through multifactor authentication. 2011 12th IEEE/ACM International Conference on Grid Computing (GRID); 2011 Sept 21–23. p. 106–13.
- [10] Mohammed MM, Elsadig M. A multi-layer of multi factors authentication model for online banking services. 2013 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE); 2013 Aug 26–28. p. 220–4.