VOL 2 (2018) NO 3 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Secure Login Mechanism for Online Banking

Ahmad Syahir [#], Chuah Chai Wen [#]

[#] *Information Security Interest Group (ISIG), Faculty Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Malaysia*
E-mail: amadsyahir20@yahoo.com, cwchuah@uthm.edu.my

Abstract— **Login is one of the important security features in online banking. This research investigates the mechanism for an existing online banking in Malaysia including the design of the login mechanism, the encryption algorithm used for the password and the security level of the login mechanism. This research provides a result of analyzing data between five online banking in terms of their security features. These analyzing data will be used for proposing secure password encryption in online banking. The mathematic is used to evaluate the security level for these secure login applications. Output from the mathematical analysis is the probability that the adversary may break the security of login application.**

Keywords—**login, online banking, security, adversary.**

I. INTRODUCTION

Online banking is an electronic payment system. This electronic payment system allows an individual to perform electronic transactions through the banking system. The electronic transactions perform is through a variety of access devices and links of communication as shown in Fig 1.

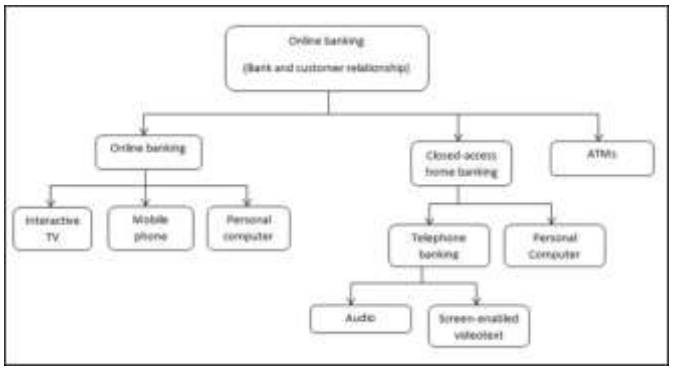

Fig. 1 Communication methods and access devices in online banking [1].

Online banking services enable customers to do all routine transactions such as account transfers, balance inquiries, bill payments, and some online loan or credit card applications. Online banking gives customers the ability to access their account online anytime, anywhere as long as there is an internet connection.

The problem related to manual banking is if there are many people at the bank, the people will have longer waiting time to wait for their turn. As the Internet rapidly grows, user much prefers to do online banking, but online banking also provides weakness for those careless users who not aware regarding the security policy provided by each of online banking.

There are three objectives for this research that are to compare the security of password encryption used by CIMB Clicks, Maybank2u, i-Muamalat, Bank Islam IB and MyBSN, to analyse the selected online banking and to evaluate and propose a secure password mechanism that has better security level compared with the CIMB Clicks, Maybank2u, my-Muamalat, Bank Islam IB and MyBSN.

The scope for this research focussed on CIMB Clicks, Maybank2u, i-Muamalat, Bank Islam IB and MyBSN. Besides that, the analyzing data has focused on login security policy, such as a password requirement (combination of alphabet, number and symbol) and length of the password used by these five online banking. Other scope is on what type of data security used by the online banking such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and so on.

This paper consists of five main sections. The first section describes the introduction of online banking, problem statement, objectives and scope of the research. The second section presents a literature review of login security for online banking. Next section presents the methodology used for this research where we choose five online banking. The fourth section is result and discussion. Lastly, we conclude the research and propose future work.

II. LITERATURE REVIEW

This chapter discusses the theoretical background of this research. The theoretical background is included the structure of login for online banking and the difference of login security

mechanism used by MayBank2u, CIMB Click, Bank Islam, MyBSN, and i-Muamalat. The result for comparison of login security features between five online banking is shown in Table1.

TABLE I
COMPARISON BETWEEN SECURITY FEATURES FOR FIVE ONLINE BANKING IN MALAYSIA

Characteristic	**CIMB Click [2]**	**Maybank 2u [3]**	**MyBSN [4]**	**i-Muamalat [5]**	**Bank Islam IB [6]**
Type of username identification	Secure word	Security Image & caption	Text	Security image	Private word
Length of username (characters)	8-32	6-16	8-12	6-12	6-10
Length of password (character)	8	8-12	6-12	8-12	8-18
Field type for password	Alphabet & Number	Capital letter, alphabet, number and symbol except spaces.	Uppercase/ lowercase alphabet, numbers and/or special characters	Upper case, lower case, digit and special characters	Alphabet & digit
Type of encryption	3-DES with key length of 168-bit.	AES (Advanced Encryption Standard) with key length of 192 bits.	3-DES with key length of 168-bit.	3-DES with key length of 168-bit.	3-DES with key length of 168-bit.

A. Cryptography

Cryptography is the science of secret writing [6]. The words cryptography comes from two Greek words that are "Kryptos" means hidden and "Graphia" means writing. Cryptography hides information by transforming a plaintext into an unreadable format which called as cipher text so that only the person who owns a secret key can decrypt the message into plaintext and read it [7]. Nowadays, cryptography is achieved by encryption using algorithms that have a key to encrypt and decrypt information. The encryption used by online banking was to protect user information. In general, the longer the key is, the more difficult it is to crack the password.

1) AES

AES is referenced as Rijndael [8]. AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001 [9].

AES is a symmetric block cipher. AES uses the same key for both encryption and decryption. The encryption for AES depends on key length. If the key size used is 128 bits, then the number of rounds is 10 rounds of processing consists of 10 rounds of processing, 12 rounds for 192 bits and 14 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The overall structure of AES is shown in Fig 2.

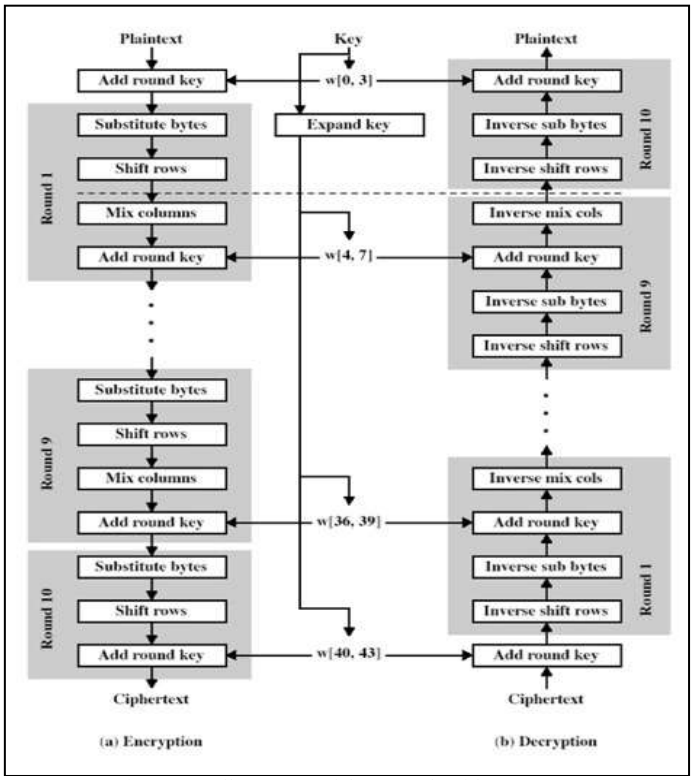

Fig. 2 Overall structure of the AES algorithm [8, 9].

2) TDES

Triple Data Encryption Standard (TDES) was first published in 1999 as a standard ANS X9.52 and named Triple Data Encryption Algorithm (TDEA)[12]. TDES was created because DES algorithm, invented in the early 1970s with 56-bit key, turned out to be not strong enough to protect information, as it is easy to break using modern computers. The effective security TDES provides is only 112 bits to prevent meet-in-the-middle attacks.

The process of encryption and decryption of TDES is explained in Fig 3 and Fig 4. TDES algorithm uses three iterations of common DES ciphers. TDES receives a secret 168-bit key, which is divided into three 56-bit keys.

1. Encryption using the first secret key
2. Decryption using the second secret key
3. Encryption using the third secret key

Encryption:

c = E3 (D2 (E1 (m)))

Decryption:

m = D1 (E2 (D3 (c)))

Using decryption in the second step during encryption provides backward compatibility with the common DES algorithm. In this case first and second secret key or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)

c = E3 (D3 (E1 (m))) = E1 (m)

It is possible to use TDES cipher with a secret 112-bit key. In this case first and third secret keys are the same. It is stronger than simply DES encrypting used twice (with two 56-bit keys) because it protects against meet-in-the-middle attacks.

c = E1 (D2 (E1 (m)))

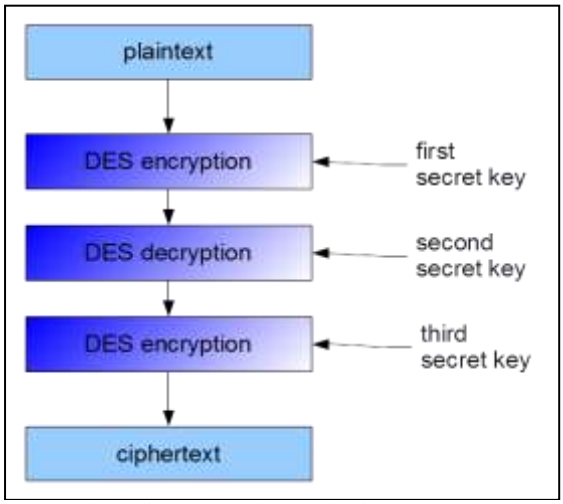

Fig. 3 The process of encryption in TDES [12].

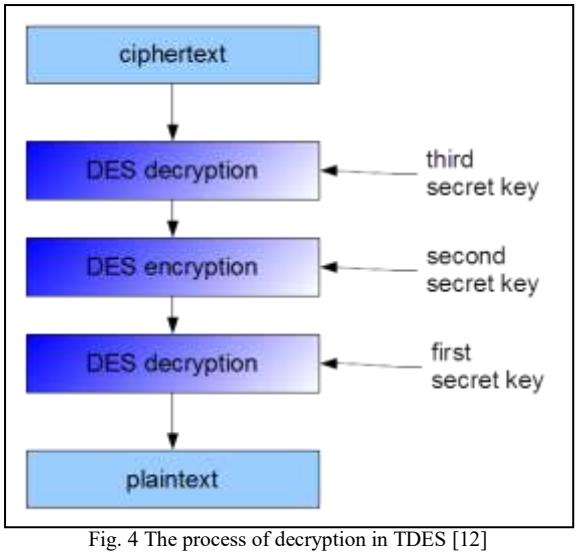

Fig. 4 The process of decryption in TDES [12]

3) Password-Based Key Derivation Function (PBKDF2)

Password-Based Key Derivation Function 2 (PBKDF2) is a key derivation function that is a part of RSA Laboratories Public-Key Cryptography Standards (PKCS) series. In cryptography, PKCS is a group of public-key cryptography standards published by RSA Security Inc, in the early of 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm. PBKDF2 used to replace an earlier standard, which is PBKDF1 that could only produce derived keys up to 160 bits long. The algorithm of PBKDF2 is described in Table II.

TABLE II
THE ALGORITHM OF PBKDF2 [13]

Parameters and Symbol:
hLen - Digest size of the hash function.
Ui - Intermediate variable
CEIL (x) - The ceiling of x is the smallest integer that is greater than or equal to x.
‖ - Concatenation
⊕ - Bit-wise exclusive -or.
T<0, 1…, r-1> - The truncation of the binary string T that retains its first r bits.
Inputs:
p Password. s Salt. n Length of derived key in bits, at most (232-1)× hLen. PRF HMAC with an approved hash function. c Iteration count.
Output:
Key derived key in n bits.
Steps:
1. if $(n > (232 - 1) \times hLen)$ 2. Return an error indicator and stop 3. $h = CEIL(n/hLen)$ 4. $r = n - (h - 1) * hLen$ 5. $for\ i = 1\ to\ h\ Do$ 6. $Ti = U0 = PRF(p, salt\|\|i);$ 7. $for\ j = 1\ to\ c\ Do$ 8. $Uj = PRF(p, Uj - 1)$ 9. $Ti = Ti \oplus Uj$

B. General Attacks on Login of Online Banking: Brute Force Attack

A brute force attack is an attempt to gain access to user account by trying every combination of alphabets, numbers or symbols consistently to discover a user's password [14]. The number of possible combinations of letters, numbers, and symbols, require a long time to complete the brute force attack. The higher the key length of encryption used such as 64-bit, 128-bit or 256-bit encryption, the longer it can take to brute force the password. The amounts of possible characters for a password are:

1. Alphabets (A-Z and a-z) – 52 characters
2. Numbers (0-9) – 10 characters
3. Special characters – 32 characters

The amount of time to brute force attack can be calculated with the following formula as shown in Fig 5:

Total of time to brute force attack the password = (Number of possible characters$^{(password_length)}$ x time taken to encrypt the password) / No. of seconds in one Year

Fig. 5 The amount of time to brute force attack in years.

The code for time execution that we used to calculate time to do a brute force attack on the password is C code that is taken from Internet Engineering Task Force (IETF).

III. RESEARCH METHODOLOGY

A. Research Design of Login Online Banking based on PBKDF2

In this section, the security test's design for the proposed login online banking PBKDF2 are designed. This research design is used to evaluate total time needed for brute force attack on password encryption using the proposed online banking system using PBKDF2 together with five existing online banking encryption scheme. The research design is shown in Fig 6.

Firstly, data such as password that contains combination of different type of characters are encrypted using three different ciphers. The ciphers are AES, DES and PBKDF2. The outputs are ciphertexts. Time of the encryption for each cipher is recorded. The time needed as it is used as the benchmark to know the time needed to brute the password for the last phase. Lastly, given the ciphertext, the attacker need to find the corresponding password by using brute force attack.

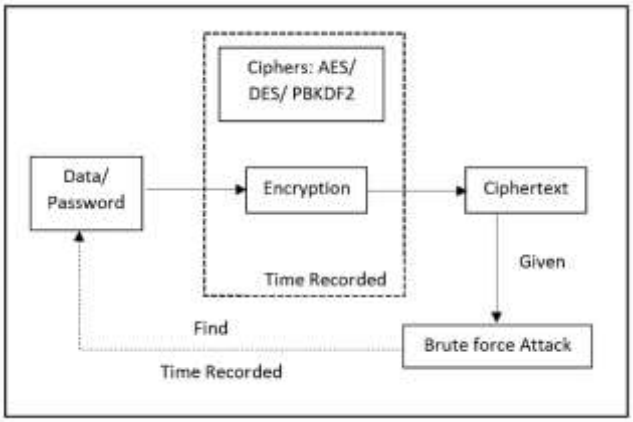

Fig. 6 Research Design of Login Online Banking based PBKDF2

For all three experiments, the execution time is recorded for each of 100 trials. The average time (mean) and standard deviation for each type of encryption is recorded in Table 3. The execution time was captured using CLOCK MONOTONIC (which can be found in the programming language C library). All the simulations were performed on a machine with the following specifications: Intel (R) Core (TM) i3-2370M CPU @ 2.40GHz, 2.40 GHz, 6GB RAM and running a 64 bit Windows operating system.

IV. RESULT AND DISCUSSION

A. Software Performance Analysis for AES, TDES and PBKDF2

The performance of AES, TDES and PBKDF2 are shown in Table III. The software performance analysis is used to measure the time taken to brute force the password. For all three experiments, the time is recorded for each of 100 times. The average (mean) and standard deviation for each experiment are shown in Table III.

TABLE III
THE TIME TAKEN TO BRUTE FORCE THE PASSWORD

Experiment	Key length		Time (ns)
AES	192 bits	*x*	54411.48
		S	3518.489
TDES	168 bits	*x*	359848.3
		S	26059.83
PBKDF2	256 bits	*x*	21469380
		S	2152846

*Performance time is in nanosecond *x* and *S* are sample mean and standard deviation respectively

B. Security Analysis against Brute Force Attack on Password of Online Banking

The security analysis also included PBKDF2 is as the proposal security analysis against brute force attack on password to examine whether PBKDF2 can slow down the time taken to brute force attack. The analysis of password requirements such as the length of the password and complexity of the password is being analyses according to type of encryption for each type of online banking. The length of password that used in this research is 6-8 characters which are the minimum length of the password for each of the online banking. The length of the password for PBKDF2 also used same length of password which is 8 characters. The time needed to brute force the password was recorded in Table IV and Fig 7.

TABLE IV
TIME TAKEN TO BRUTE FORCE THE PASSWORD

Type of encryption	Key length (bits)	Type of banks	Possible combinations of password (characters)	Time needed to brute force the password (years)
AES	192	MayBank2u	$\mathbf{94^8}$	10517
TDES	168	CIMB Clicks	$\mathbf{36^8}$	32
		MyBSN	$\mathbf{94^6}$	69556
		i-muamalat	$\mathbf{94^8}$	69556
		Bank Islam IB	$\mathbf{94^8}$	32
PBKDF2	256	Proposed Cipher	$\mathbf{94^8}$	4147126

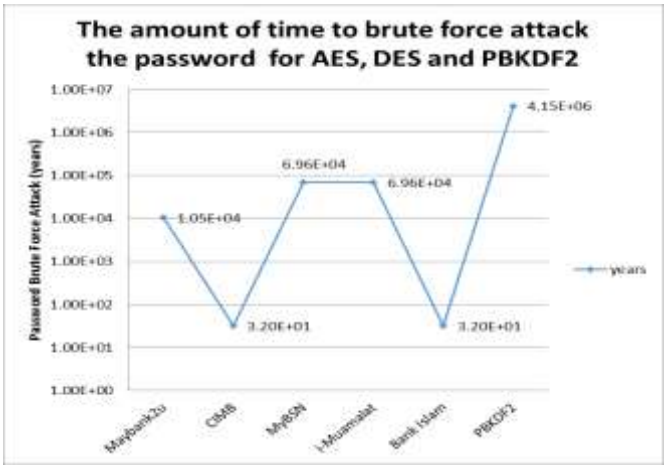

Fig. 7 Time taken for brute force attack on AES, TDES and PBKDF2.

C. Result and Discussion

The result shows that the time taken to do a brute force attack on AES, TDES and PBKDF2. For overall, the result shows that the longest time taken to brute force the password is PBKDF2 with time taken is approximately 4 million years. The shortest time taken to do a brute force attack the password is CIMB Clicks and Bank Islam IB which is 32 years due to least probability combinations of the password which is alphabets and number. The result shows that the proposed mechanisms of PBKDF2 can be used to slow down the time to brute force attack as compared to AES and TDES.

V. CONCLUSIONS AND FUTURE WORK

This research has achieved the main objective which to propose an alternative secure password mechanism based on

analysed of security for the type encryption used by the online banking. PBKDF2 were used as an alternative secure mechanism that used to slow down the process of brute force attack on password encryption. PBKDF2 also proposed to be used in the login mechanism as it is the properties of confidentiality, which design just for encrypt the password.

The performance is being analyses based on the time taken to brute force attack the password and the probability of guessing password with the combination type of password such as alphabet, number and special characters. The length of password also important as it can influence the total of different combination and time taken to encrypt the password.

For the future work, since the time taken to brute force attack the password is too long, the other type of attack on the type of encryption can be used which is dictionary attack. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document by systematically entering every word in a dictionary as a password.

ACKNOWLEDGMENT

This research was supported by RMC UTHM and Gates IT Solution Sdn. Bhd.

REFERENCES

[1] A. Berger, *The Economic Effects of Technological Progress: Evidence from the Banking Industry*, Journal of Money, Credit, and Banking, Vol 35, No. 2, pp 141 – 176, 2003.
[2] CIMB Clicks, (2017). URL: https://www.cimbclicks.com.my/
Maybank2u, (2017). URL: http://www.maybank2u.com.my/
[3] MyBSN, (2017). URL: https://www.mybsn.com.my/
[4] i-muamalat, (2017). URL: https://www.i-muamalat.com.my/
[5] Bank Islam Malaysia, (2017). URL: https://www.bankislam.biz/
[6] L. D. Smith, *Cryptography: The Science of Secret* Writing, Publisher Courier Corporation, 1955.
[7] W. Stallings, *Cryptography and Network Security: Principles and Practices 7th Edition*, Pearson Education India, 2017.
[8] J. Daemen, and V. Rijmen, *AES Proposal: Rijndael*, 1999.
[9] NIST, *Advanced Encryption Standard (AES)*, 2001.
[10] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon. Oxford University Press.
[11] NIST, *Data Encryption Standard (DES)*, 1999.
[12] NIST, *Recommendation for the Triple Data Encryption Algorithm (TDEA)*, 2012.
[13] B. Kaliski, *RFC2898: PBCS#5, Password-based Cryptography Specification version 2.0.* Technical report, Internet Engineering Task Force, 2000.
[14] K. S. M. Moe, and T. Win, *Improved Hashing and Honey-based Stronger Password Prevention Against Brute Force Attack*, Electronics and Smart Devices (ISESD), 2017 International Symposium, pp 1 – 5, 2017.