Towards Quick Response and Secure Online Banking Transactions

Using Data Compression and Cryptography

Nuha Abdullah Zammarah
Department of Information System. Kulliyyah of Information and Communication Technology.
International Islamic University Malaysia
Kuala Lumpur, Malaysia
nuha_rose_963@hotmail.com

Asadullah Shah
Department of Computer Science. Kulliyyah of Information and Communication Technology.
International Islamic University Malaysia
Kuala Lumpur, Malaysia
asadullah@kict.iium.edu.my

Abstract*—Online banking transactions have become one of the common daily tasks. Security is very important to accomplish these tasks. There are a lot of frauds and threats for online banking transactions that need to be studied, discovered and come out with the proposal of suitable solutions. It has been found that the main problem is in the connection channel between the end-user and the bank. Data compression and cryptography are integrated to be used for securing the online banking transactions efficiently. The two processes have different priorities. Security is the first priority for cryptography while decreasing the file size is the first priority for compression. This paper is going to review and address the current issues involving the online banking security by introducing the new Quick And Secure (QAS) process that has impacted and accelerated the online banking transactions and set the bar high for a new frontier encryption algorithm.

Keywords*—online banking, security breaches, security vulnerability, data compression, cryptography.

I. Introduction

In this era of globalization, the world is becoming highly interconnected with the internet and its related application. Therefore, internet is becoming more important. Internet-based electronic banking, is also called online banking, is a new channel for the banking business development. Nowadays, online banking becomes the preferred choice for many customers, because users can pay utility bills and transfer funds without having to go to a bank branch. There are a continuously growing number of customers using online banking because of the ease of use and time saving. Banks also encourage their customers to use online banking since it can lower banks' operating costs. So, the demand for online banking has increased and the number of people who rely on online transactions has tremendously increased.

However, various frauds and attacks for online banking are also increasing quickly in recent years. According to [1], the necessity for a reliable security for online transactions is ever than before and online systems providing banking services should offer strong security because of the confidential information involved, in addition to attacks against online banking authentication mechanisms.

The security issues can be summed up in two categories: system security and information security issues [2]. The online banking transactions need a connection between two sides. These two sides are bank side and client side. System security issue is on the bank server side which is completely secured and has no vulnerability. This is because most of the banks nowadays use very strong security system for online services and have no attack in the bank server side so far. The information security measures should not only based on technologies but also the security awareness of both customers and the organizations and the information security policy structures of the organizations. This is because installing anti-viruses program in the client side and using strong and secure system in the bank side are not enough without awareness. So, keep the customers safe and secured is one of the Customers' responsibilities [3]. For the security based on technologies, the client side is one of the vulnerabilities. In the client side, even if strong client-side security is employed, these transactions are vulnerable to manipulation by malware [4] because the client PC is usually used for input and output of sensitive information such as Personal Identification Number (PINs)/passwords, amounts, account numbers, and so on. So, it is obvious that online banking is vulnerable to threat.

In the recent years, it has been proved that current online banking is highly insecure. This is because all the currently used countermeasures implemented by banks are vulnerable to some kind of attack, mainly to the recent and powerful last generation Trojans. The two main kinds of attacks are man in the middle (MITM) attack and Malicious Software (MSW) [5]. These attacks target the connection channel between the bank and the user. This is because the connection channel is not completely protected. One of the reasons behind the vulnerability to man in the middle

(MITM)/Malicious Software (MSW) attacks of online banking are due to the interaction with the user through the display and keyboard of the potentially unsafe client PC [6].

Each year a new software or hardware is created to protect and secure the online banking transactions offset by the emergence of new hackers. As the professional study how to protect and secure the information that transmit through the internet, the hackers or attackers also study how to break the protection. Therefore, we should always look for new approach difficult to be understood and penetrated. Currently, there are two main kinds of attacks which are man in the middle (MITM) attack or Malicious Software (MSW). These attacks target the connection channel between the bank and user. There are many kinds of approaches in the online banking. Some of the modern approaches are mobile transaction number (mTAN), Financial Transactional IC Card Reader (FINREAD), AXS-Card, Internet Smart Card (ISC) and Zone Trusted Information Channel (ZTIC) [6]. Some of these approaches are useful for one kind of attack and useless for the other. For example, AXS-Card does not have any protection from MITM attacks and ISC does not have any protection from MSW. In addition, some approaches are expensive such as FINREAD. Moreover, some of them Slower Transaction Speed such as ZTIC. So, it is obvious that there has not been an approach that has all these good features such as the affordability, high security and the quick response. Therefore, this paper looks for new approach that is useful for all kinds of attacks and speed up the transactions with high level of protection and security. This approach is Quick And Secure (QAS) process that integrates data compression and cryptography to increase the information security transmissions without decreasing the efficiency. This process helps to delay the hackers due to many layers of compressions and encryptions and the integration between them may confuse the hackers. PHP code is implemented for this process to investigate the multi-layers procedure.

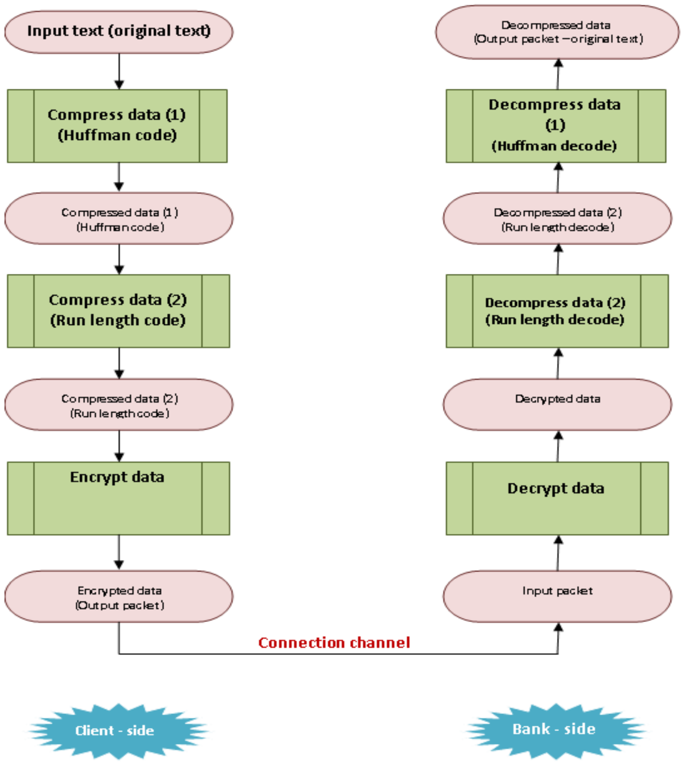
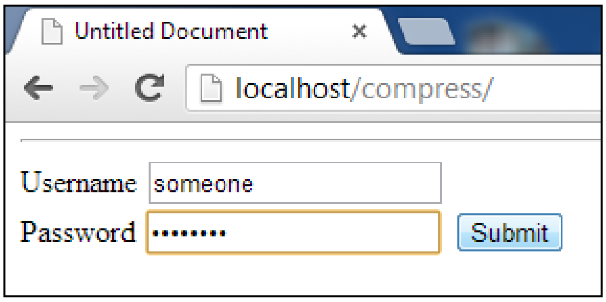

Input text (original text)
Compress data (1) (Huffman code)
Compressed data (1) (Huffman code)
Compress data (2) (Run length code)
Compressed data (2) (Run length code)
Encrypt data
Encrypted data (Output packet)
Connection channel
Input packet
Decrypt data
Decrypted data
Decompress data (2) (Run length decode)
Decompressed data (2) (Run length decode)
Decompress data (1) (Huffman decode)
Decompressed data (Output packet –original text)
Client - side
Bank - side

Figure 1: QAS process

II. QAS APPROACH

However the QAS approach is to protect online banking especially at the user side, the proposed approach within the integration of compression and the encryption is supposed to be applied in both sides but in opposite direction. So, this approach with all its details must be known by only the client and the bank sides. Before doing any online banking transactions, each customer needs to open an account. So, every time he needs to do any kind of transactions he just logins first and then goes ahead. The logging in sends the username and the password to the bank server for the access. And then user starts the transaction and sends the required information such as receiver's account number and amount for transferring money or bill's account number and amount for bill payment and so on. The integration is applied only to that data of information input by the user side. It should be note that all the entering data will be consider as text and nothing will be consider as numbers because we do not need to do any mathematical operations on the numeric data.

The integration of the compression and the encryption can be done in two approaches; compression-then-encryption and encryption-then-compression. Sharma and Gandhi (2012) reported that applying compression before encryption is more efficient because of many convinced reasons; compressing last does not reduce the file size much, compressing should decrease the effectiveness of some



Username someone
Password •••••••••

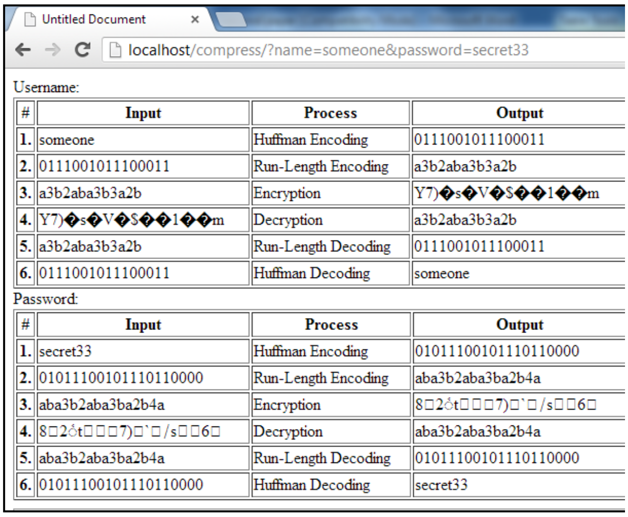
Figure (2): input data in the client computer

attacks, brute force attacks takes longer, the opponents gets less cyphertext to analyze, and what obtained has a corresponding plaintext with fewer redundancies and regularities [7]. So, the integration approach or QAS process implements data compression first and then encryption. In the compression process, two layers are included, Huffman code and Run-length code. The choice and the use of Huffman code in this stage are due to the high efficiency of compression for text. In spite the Haffman code implementation is longer than other, this does not slow the process because it is applied to a small-size packet. Then the output is compressed with the Run-length code after it is converted into text again using a certain algorithm. The use of Run-length is to increase the number layers. The next stage of encryption, two layers of secure are used, Secure Hash Algorithm-256 (sha-256) and base64 encode, to also increase the number of secure layers up to four. So, after compression and encryption, the packet is sent to the bank's server through internet connection channel.

In the bank's server side; first of all the QAS process decodes the receiving packet using base64 decode and then decrypt using sha-256 decryption. Followed by decompression using Run-length decode first and then decompress again by using Huffman decoding to get the original input text by the user. So, the use of different individual processes in the compression and the encryption for QAS, as shown in Figure 1, is understood by only the client and the bank sides.

III. RESULT AND DISCUSSION

PHP code is used for QAS process to be applied for different input text. Two strings of text is used as user's input in the username and password fields for the implementation of the code as shown in Figure 2. Assuming the user enters the username and password, the user name is "someone" and the password is "secret33", the output of the implementation of the processes is given in Figure 3. The output of the client side seems as only due to the encryption because it is cyphertext. This is a significant point that let the hacker's decoder think it is encrypted only. In addition, the use of compression before the encryption is not expected by the hackers because the transferred data is of small size. This small size enables us to investigate the use of different encryption codes and compression codes in different sequence and in different number of layers to obtain the best QAS.



Username:

#	Input	Process	Output
1.	someone	Huffman Encoding	0111001011100011
2.	0111001011100011	Run-Length Encoding	a3b2aba3b3a2b
3.	a3b2aba3b3a2b	Encryption	Y7)�s�V�$��1��m
4.	Y7)�s�V�$��1��m	Decryption	a3b2aba3b3a2b
5.	a3b2aba3b3a2b	Run-Length Decoding	0111001011100011
6.	0111001011100011	Huffman Decoding	someone

Password:

#	Input	Process	Output
1.	secret33	Huffman Encoding	01011100101110110000
2.	01011100101110110000	Run-Length Encoding	aba3b2aba3ba2b4a
3.	aba3b2aba3ba2b4a	Encryption	8□2ổt□□□7)□`□/s□□6□
4.	8□2ổt□□□7)□`□/s□□6□	Decryption	aba3b2aba3ba2b4a
5.	aba3b2aba3ba2b4a	Run-Length Decoding	01011100101110110000
6.	01011100101110110000	Huffman Decoding	secret33

Figure (3): the output of implementation of QAS process

IV. CONCLUSION AND FUTURE WORK

This paper proposed an integrated approach made from the compression and the encryption to obtain the QAS online banking. In the client side, The compression was chosen to be first in the process within two layers of different codes and the encryption was the next within also two layers of different codes. A simple familiar username and password are chosen as application for the approach. The output showed that the integration of the compression and the encryption produces more ambiguity for the hacker. This is a motivation for more investigations that could be done with different processes of compression and encryption with different sequences to obtain the best QAS for this approach.

References

[1] Hiltgen A. ; Kramp T. ; Weigold T. ; "Secure Internet-banking Authentication," IEEE Security and Privacy, vol. 4, no. 2, 2006, p. 21-29.

[2] Lao G. and Wang X., "Study of Security Mechanisms in Personal Internet Banking – Take China Merchants Bank as an Example", IEEE 2010, International Conference on Computational Intelligence and Software Engineering-CiSE,2010, vol.1, DOI:10.1109/CISE.2010.5676896

[3] Karim Z., Rezaul K., Hossain A.,"Towards Secure Information Systems in Online Banking", IEEE,Internet Technology and Secured Transactions, ICITST 2009,p.1 -6.

[4] Currie M.,"In-the-wire authentication: Protecting client-side critical data fields in secure network transactions", IEEE 2009, 2nd International Conference on Adaptive Science & Technology, p. 232-237. ISBN 978-1-4244-3523-4/09/$25.00.

[5] Delgado O., Fu ́ster-Sabater A., and Sierra J.M., "ANALYSIS OF NEW THREATS TO ONLINE BANKING", ACTAS DE LA X RECSI, SALAMANCA, 2008. p.337-344.

[6] Hisamatsu A., Pishva D., and Nishantha G.G.D., ”Online Banking and Modem Approaches Toward its Enhanced Security”, Advanced Communication Technology (ICACT), 2010, vol. 2, p. 1459- 1463,ISBN 978-89-5519-146-2.

[7] Sharma M. and Gandhi S.,”Compression and Encryption: An Integrated Approach”, International Journal of Engineering Research & Technology IJERT 2012, ISSN: 2278-0181, Vol. 1 Issue 5, July – 2012, p. 1-7.