International Journal of Scientific Research in Computer Science and Engineering
Vol.8, Issue.6, pp.33-37, December (2020)
Research Paper
E-ISSN: 2320-7639

Mobile App security for E-Commerce

Khean Ouk[1*], Kimsoung Lim[2], Sen samnang Ouk[3]

[1]Department of Computer Science, Royal University of Phnom Penh, Phnom Penh, Cambodia*[1]
[2]Department of IT, Emperor Bank PLC, Phnom Penh, Cambodia[2]
[3]Department of IT, Royal University of Phnom Penh, Phnom Penh, Cambodia[3]

**Corresponding Author*: *khean_ouk@yahoo.com.sg Tel: 855-12925849*

Available online at: www.isroset.org

Received: 12/Dec/2020, Accepted: 18/Dec/2020, Online: 31/Dec/2020

***Abstract*:** Today is an e-commerce world that most of the population around the world does business with high tech. A long the way to deal with it, many intruders, hackers and unauthorized users are trying to involve that business by playing a role as the owner to cash money from a bank or transferring from one account or credit card or use device to install App on mobile phone while the password or PIN was hacked or belonged to those guys illegally. The hybrid algorithm of RSA and OTP will be implemented, that is the best model to prevent those mistreated action that cause to infect to the system. A PIN and a password will be encrypted with the hybrid algorithm. In the world, there is a unique MAC address used for each NIC. The authentication can be processed unless the receiver obtained its own MAC address in advance (pre-shared key). This key (MAC address) was sent to a cloud server after establishing a connection and then while the receiver log in to the cloud, the MAC address will be sent to that receiver to compare with its own MAC address automatically. All MAC is stored in a Cloud Database data must encrypt with the OTP.

Keywords: MAC, SIM card, NIC, OTP, Cloud database, e-commerce, PIN, Authentication, hybrid algorithm.

I. INTRODUCTION

In everyday life what we are worrying about is a security breach, not only technology but also own personality. Technology helps our lives to live better and better from day to day, but it can destroy us in a few minutes if it was used unprotected and be unaware of mistreated software.

All assets are organized as e-documents and then sent to keep at the bank, all people's identifications are sent to the database of department at Ministry interior (e-identification).All e-passports are kept at the database at Ministry of Foreign Affairs; All Taxes are kept at department of Tax, the database at ministry of Economics. All academic documents are kept the database of Ministry of Education (e-transcript) and so on. All those things must keep safety are priceless for everyone.

If that information was stolen or the system was hacked and data has been stored as a plain text, all those in formations will be manipulated or read easily. You all lost completely and who are responsible for, will be punished by law or will charge of criminal cases.

To protect all these malicious activities from being spread and infect on the system, all information must be encrypted with the best techniques such a hybrid algorithm. The passwords are used for verification and then authentication.

The following process of encryption and decryption shown below:

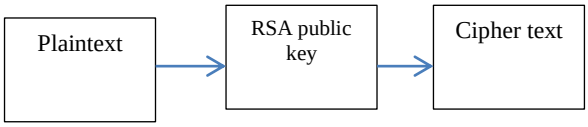

Fig.1. Encryption Process

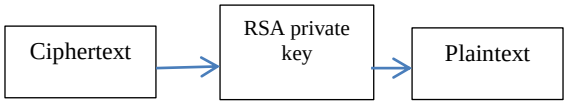

Fig.2. Decryption Process

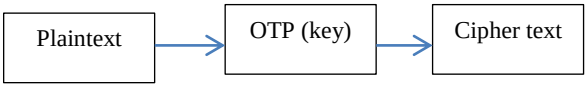

Fig.3. Encryption Process

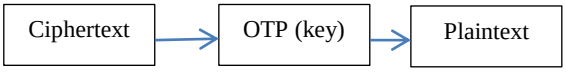

Fig.4. Decryption Process

This paper involves the sections as follows: section I describes the cause to propose this model of Mobile App security for e-commerce, section II describes the impact of security breach, authentication methods, Gesture Puzzle, Secure Lock, Section III describes how to implement the hybrid algorithm and section V describes the result of the implementation of hybrid algorithm and finding the out of

ASCII characters and request to the world experts and Section V is the last section describes that model of security can protect Mobile App absolutely for e-commerce.

II. RELATED WORK

As a reporting on the security breach around the globe, the 2015 information security Breaches Survey reported that 90% of large organizations and 74 of small business has suffered a security breaches that year with an average cost 1.46 to 3.14 m pounds and 75k to 311k pounds respectively.

It required taking countermeasure to ensure the confidentiality, integrity and availability of the information from the unwanted incidents [1]. The best method to protect these incidents to data is encryption with the hybrid algorithm.

The Media Access Control (MAC) is a unique hardware address built-in on the network interface card. It cannot be changed unless the network interface card was removed. Each MAC address has 48 bits long.

Today the best way to store data and spend less money on the ICT infrastructure is a Cloud Storage. It provides the flexibility of accessing data around the globe. The biggest public Cloud is Amazon Web Service (AWS).

Mostly people use mobile App to access the information from the Internet or banking, Microfinance, transferring money, bills, tickets, tax, and payment from each other through the Internet Access. So it will be vulnerable to hackers or attackers. To ensure that only the exact sender and receiver were authorized to withdraw money, the MAC address must be used for verifying the authentication.

Each device that was registered with the database, its MAC address was stored on that database. When the App installed on that phone and then tries to use it. It will send the verification code. If that phone's MAC address matched to database, it will be allowed to use that App. When the receiver will withdraw money from that banking, that key code will be decrypted by the OTP.

The mobile phone platform we are going to use: Android and iOS. The use of passwords is available for all platforms. There are restrictions to passwords. They support the exact length of password and special characters are 6 digits. The Android and iOS support a PIN. The Android and iOS support the length of a PIN is exactly 6 [2].

For authentication, Android uses a Secure Lock that will deny the usage of the device without prior authentication. The Android doesn't provide the API for screen lock replacement. So it is necessary to implement the application as an Android home screen. When a user presses a device's home button, she will directly be passed on to the home screen. This would bypass the authentication application. Secure Lock will then authenticate the user and redirect her to Android's standard home screen [2].

Usability [2]

- Duration: The duration of the authentication process is crucial for user acceptance. It recommends roughly estimate 4 seconds to enter a PIN and 10 second to enter an average password.
- Complexity: Images is much better to remember for humans than texts,

One Time Pad (OTP) is an unbreakable cryptosystem. The text will be converted into ASCII code and then as binary (0.1) as a group of 8 bits represent each character. The length of the text must equal to the length of the key. Once a key was used; it will never use again [3].

The security concern is to take countermeasure as follows:

1- PIN or password will be encrypted with the hybrid algorithm
2- Malware protection uses Gesture Puzzle.
3- Authentication methods using username, password and MAC address and PINs

III. METHODOLOGY

In the communication system, actually all senders and receivers must establish a connection called TCP handshaking or three way-handshaking. It means that both sender and receiver are ready to send and receive the data. The mobile App was installed on each mobile phone. Once it starts to operate by users, it will talk with the Web server to request the service and then the MAC address was sent to a Cloud database (Banking system). Each device has its own MAC address which only layer 2 of the OSI model can read. It is a sub-layer of the OSI model.

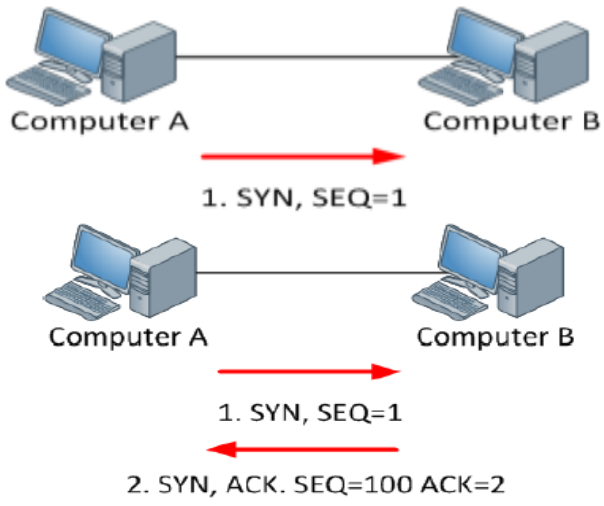

Fig.5. hand-shaking

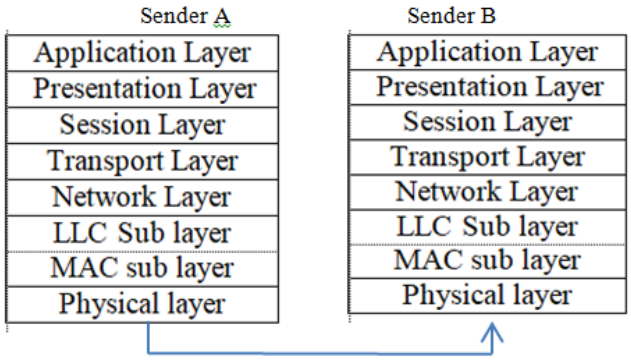

Fig.6. MAC sublayer at Data link layer

A. Terminology:

- PIN: PIN is a Personal Identification Number used to authenticate to the SIM card of the network operator.
- Password: a secret word or phrase that must be used to gain admission to a place or gain access by a system.
- Authentication: The process of allowing you to use the network resources after verifying correctly the PIN or a username and a password.
- MAC: Media Access Control or Hardware addresses built-in on Network Interface card. It is 48 bits long.
- NIC: Network Interface card used to identify the card in a device.
- Plaintext: The text can be read by human
- Ciphertext:The unreadable text by encrypting algorithm
- Encryption: The process of converting a plaintext to the unreadable text with a key by encrypting algorithm.
- Decryption: The process of converting the ciphertext back to the plaintext with a key.
- E-commerce: Electronic commerce.
- SIM card: Subscriber Identity Module used to identify and authenticate subscriber on mobile technology, commonly known as a SIM card.
- Gesture puzzle: used combination of password and picture.
- Secure Lock: it is an Android application Secure Lock that provides four different authentication methods as well as some additional functionality. Secure Lock is intended for a replacement of Android's lock screen.

B. Algorithm

The process of the e-commerce works as follows: The buyers are using their smartphone with the installed Mobile App for e-commerce and then start the App and it requires the users the usernames and passwords for authentication. The communication of the sender and receiver took place before allowing users to input the usernames and passwords for authentication. So the MAC addresses for senders were sent to the cloud storage already and their passwords were stored on the cloud storage too. So the passwords or PINs were encrypted with the hybrid algorithm. The system will encrypt the PIN or password as follows:

- Encryption with RSA public key

Table.1. the encrypted passwords stored on Cloud storage

Password or PIN	Public key	Ciphertext
aaaaaa	(267,187)	qqqqqq
bbbbbb	(267,187)	!!!!!!
cccccc	(267,187)	ÀÀÀÀÀÀ

- Encryption with OTP

Table.2. the encrypted password by hybrid algorithm

Ciphextext	Encrypted with OTP key	Double ciphextext
qqqqqq	1234_@	1CBE.1Q
!!!!!!	1234_$	1~
ÀÀÀÀÀÀ	1234_!	

Note: ÀÀÀÀÀÀ⊕1234_!=266025777274849. It cannot match the ASCII character. It is out of the ASCII character. But it can display the hexadecimal number is f1f2f3f49fe1or 266025777274849in decimal. This is a special case as example above. What is the system to do with that long number?. This point, we need the world experts to help us. We don't know what ASCII character will be?.

We can make a condition that if there will be no character in ASCII character, the system will send the ciphertext that was encrypted by the RSA public key. Otherwise, no key code sent to the receiver. Is it so dangerous?. It draws to conclude that it is a disadvantage of the hybrid algorithm of the RSA and OTP.

The programmers must set the conditional statement to avoid the password with these characters "ÀÀÀÀÀÀ" and a key such as 1234_!. But it is rarely to be like this key because all keys are generated randomly and the used one cannot use it again. If so, the result of this operation gets nothing.

Fortunately, if the operation was not done by any cryptography and then send the text or a key because of being encrypted by the RSA public key already. This became the advantage of using the hybrid algorithm.
Proof:

We are using the online conversion calculator

ÀÀÀÀÀÀ=11000000 11000000 11000000 11000000 11000000 11000000
1234_!=00110001 00110010 00110011 00110100 01011111 00100001

We need to do the XOR operation

Output of XOR
1111000111110010111100111111010010011111111110000 1 equals to 266025777274849 in decimal.

XOR Calculator

Thanks for using the calculator. View help page.

I. Input: binary (base 2)

```
11000000110000001100000011000000011000000011000000
```

II. Input: binary (base 2)

```
11000100110010001100110011010001011111001000001
```

Calculate XOR

III. Output: decimal (base 10)

```
266025777274849
```

There is no character in ASCII that has this value.
So it is out of the ASCII character codes or unprinted character. So there is no result in display in ASCII character.

C. The system works as following process

1- The Users must register their information with the baking system.
2- The banking system record users 'profile such a phone number, full name, position, address, email address, amount of money, MAC address of phone, etc.
3- The banking system sends back the code number to verify. It uses MAC address to identify the authentication. If it is correct, it will allow using that Mobile App.
4- At the receiver, when the user is going to cash money or transferring money. It sends a request to the Banking system by sending the username and password.
5- Then required to input the valid code to do the transaction. That code (PIN) was encrypted since it was sent to the receiver and use the received MAC address to compare with its own MAC address. If it is correct. The transaction was completed. If it is not correct, the transaction was failed. So it must send a request again.
6-

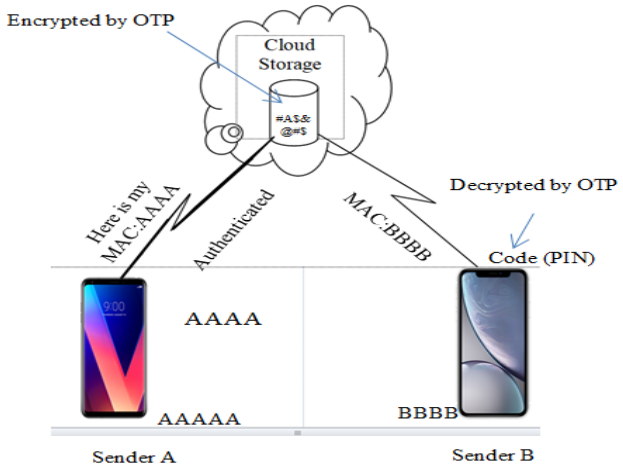

Fig.7. A is sending a MAC to Cloud storage and it is sending a MAC address a receiver.

IV. RESULTS AND DISCUSSION

The system requires the length of the password is an exact 6 digits long. So the number of the keys are 26^6= 308,915,776 keys. The MAC addresses were encrypted with OTP and then stored on the Cloud storage and Cloud Storage was protected by another authentication methods. As a result, the Mobile App is more secured and wildly use for e-commerce over the Internet based on table.1,table.2 in Section III.

The result of encryption of the OTP with a special string such as ÀÀÀÀÀÀ caused to return no ASCII characters. It is out of the ASCII characters that required absolutely the programmers to be aware of such case. It recommends the experts around the world to discover this problem and solve it or adding more symbols or characters that represent those unprinted characters in the ASCII characters.

V. CONCLUSION

It can be drawn to conclude that Mobile App security for e-commerce is better compared to other Mobile App because of being reasons:

The PINs will be encrypted with the hybrid algorithm. The passwords will be encrypted twice even if it is exact 6 digits long. First it is encrypted by RSA public key and then second is encrypted by an OTP key (hybrid algorithm).The authentication uses the encrypted password and the encrypted PIN and uses a MAC address to verify to make sure the receiver exactly.

The guest Puzzle uses against the fake application to ask for username and a password or a PIN.

Even though, the random key of OTP matched to a word that do the XOR operation cannot produce the ASCII character. If it sends the text without encrypting, the text was still secured because it was encrypted by the RSA public key. So it is more secure for this Mobile App. If a hybrid algorithm was not implemented, it is so dangerous because it sends the plaintext to the receiver.

Lastly, it would recommend the experts to solve that case there was no ASCII characters to represent the numbers or extend the ASCII code longer.

REFERENCES

[1].Karyda, Maria,Mitrou,Lilian "DATA BREACH NOTIFICATION:ISSUES AND CHAL-LENGES FOR SECURITY MANAGEMENT",*10th Mediterranean Conference on Information Systems (MCIS)*, 2016.
[2]. Roland Schlöglhofer, Johannes Sametinger, "Secure and Usable Authentication on Mobile Devices", *Proceedings of the 10th International Conference on Advances in Mobile Computing &multimedia*,Bali, 2012.
[3]. Khean Ouk, Kimsoung Lim,Sensamnang Ouk, "Message security and Parity bit recovery", *International Journal of Scientific Research in Computer Science and Engineering*,Vol.8, Issue.5, pp.01-05,2020.

AUTHORS PROFILE

H.E.D.r. Khean Ouk graduated a Bachelor degree of Science in Mathematics in 1994 and Bachelor degree of Computer Science and Engineering in 2001 and master degree of Information Technology in 2006 from Royal University of Phnom Pen and Ph.D. in information technology in 2014, USA. He teaches Computer Networks, Computer Security and Linux System Administration and STEM education at the undergraduate level. His areas of research include Cryptography, STEM Education, and Computer Security, Computer Networks and Programming Languages. He has been working as IT lecturer since 1996 at Royal University of Phnom Penh and advisor to Ministry of Education Youth and Sport in Cambodia by his majesty of the King of Cambodia, his reputation and legacy. He has taught 20000 students at Bachelor Degree of Computer Science and Master of IT students. He published 10 papers with local journal at research department of Royal University of Phnom Penh and wrote and translated more than 20 IT books for teaching at Computer Science Department in Cambodia. Currently he is working as IT consultant to Baccalaureate Examination System in IT at Ministry of Education Youth and Sport in Cambodia, in charge of Digital Education and also work as Chairman of CaNOI(Cambodia National Olympiad in Informatics) and IOI (International Olympiad in Informatics). With the CaNOI/NOI and IOI, he has taught the algorithm and C++ programming for competition.

Mr.Kimsoung Lim graduated a Bachelor degree of Computer Science and Engineering in 2016 at Royal University of Phnom Penh. He works as a deputy IT Manager for M.G.N Emperor banking since 2018. His daily job is to control the system security and system network administration on Linux system and Windows server. His areas of research include vulnerability assessment of system and appliance firewall (F5) and machine learning on how a computer works for specific task for banking. He is pursuing a Master degree of IT Engineering at Royal University of Phnom Penh.

Mr. Sen Samnang Ouk graduated a Bachelor degree of Computer Science and Engineering in 2019 at Royal University of Phnom Penh. Currently he works as a system developer (modify, analyze, Design and implement of Enterprise Service Bus) for Amreth Microfinance since 2019. His areas of research include AI, Machine Learning and Security applications. He is pursuing a Master degree of Computer Science and Engineering at Royal University of Phnom Penh.

