International Conference on Science, Technology, Engineering & Management
[ICON-STEM'15]
Journal of Chemical and Pharmaceutical Sciences ISSN: 0974-2115

Cryptography with Dynamic Password

G.Sumathy*, B.Angelin Selvamary, K.Dilliammal, R.Jayadurga
Department ofInformation Technology, Jeppiaar Engineering College, Tamil Nadu, India
***Corresponding author:E.Mail:sumathyjayaram@gmail.com**

ABSTRACT

This document is about the Cryptography with Dynamic Password which means providing password instantaneously to the users in their mobile phones when they are accessing their ATM accounts. The password will be available in mobile screen only for few minutes and the user can use that Dynamic password and withdraw money from their account. A new password will be generated in each time of accessing. This provides greater security than normal password method.

Keywords: Information security, Data integrity, Confidentiality, Authentication

INTRODUCTION

Cryptography is one of the most essential tool to secure the information. With the increasing flow of information witnessed like never before, and colossal use of smart cards like Bank cards, insurance cards and health cards, way to identify effective security tools is something that happening almost continuously. Concern for security arise in order to safeguard the users truest and integrity over functioning of certain systems.

Cryptographic Algorithms: Cryptography, imply defined, is the art of combining some input data, called the plaintext, with a user specified password to generate an encrypted output, called cipher text. It is extremely difficult to recover the original plaintext without the encryption password. The algorithms that combine the keys and plaintext are called ciphers. The key modes are three types:

Symmetric key mode: It is divided into 2 type: one is block cipher cryptography technique and the other one is stream cipher symmetric cryptography. The block cipher cryptography technique is more efficient and also secure than the stream method, because block cipher encrypt a whole block at a time whereas with stream ciphers are byte are individually encrypted with no connection to other chunks of data.

Public key mode: It is an asymmetric key mode which requires two separate keys, one of which is secret or private and one of which is public. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to decrypt ciphertext or to create a digital signature.

Hash key mode: A cryptography hash function is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The data is often called the message, and the hash value is called the digest.

Encryption: Cryptographic methods protect the data transferred from one system to another over public networks by encrypting the data using an encryption key. The main goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the encryption keys. The encryption algorithms are:

- AES- Advanced Encryption Standard(128 Bit)
- BlowFish- Block cipher algorithm
- Camellia-128-Bit Symmetric -key block cipher

Decryption: Decryption is the process of converting the cipher text into plain text. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.

Reversing: This is the simplest of all and involves any encryption that isn't 1-way. The encryption method is simply looked at, and then is reversed step by step to turn the password back into plain text.

Dictionary Attack: This now if for encryptions that can't be reversed. Once the encryption method is known, a descriptor can be decoded that uses this method. The cracker has a dictionary file that contains common words or passwords and these are inputted, encrypted using whatever encryption method is being used and compared against the string that is needed to be encrypted.

Hacking in ATM: ATM hacking is done by several techniques for robbery. The main technique used in ATM hacking is “Skimmer”. A skimmer is mounted to the front of the normal ATM card slot that reads the magnetic information of the ATM card number and transmits it to the criminals nearby and a wireless camera is mounted in a position to view ATM PIN entries. The thieves copy the cards and use the PIN numbers to withdraw from many account within short period of time directly from the bank ATM.

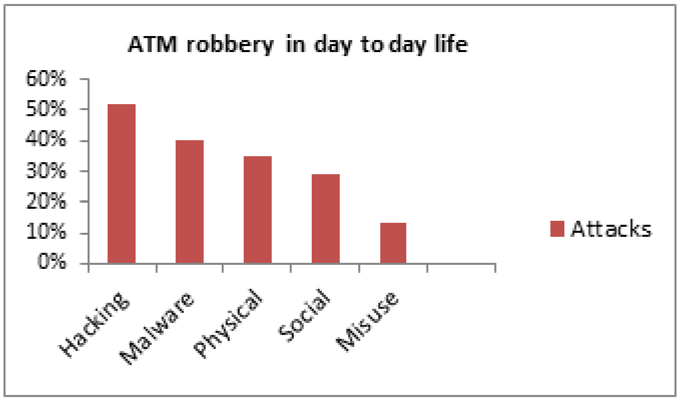

Fig.1.Graph for percentage of total data loss by attack type

Dynamic password: We can see an enormous increase of loss of data(theft) in ATM. So we would like to propose an idea of using dynamic password in ATM. Nowadays ATM systems are hacked by many unwanted activities of hackers. To avoid these losses, the data will be secured by using the mobile communication. The secret password to access the user’s account will be produced at the run time of the process.

A.Use of mobile communication: The ATM pin number will be known only by the user, and they will think that no one could access the card without their permission. But still they are not aware of the hacking techniques like skimmer by which the thief can steal the information about the user’s ATM PIN details. The secret code is like the normal password given by the banks to the card user. Whenever the user tries to get money from the ATM machine, the user has to insert the password as the normal process. But, in our concept the user should have their own mobile phone with them whenever they were inside the ATM room. Then the random secret password will be sent to the user’s mobile number as soon as the user enters the password given by their respective banks and by using that particular number that comes to their mobile only, the user can access and withdraw money from their account.

Characteristics of the mobile communication: The dynamic password will be sent only to the user’s personal contact number.The user can be able to attend the calls during the display of the secret code.The secret code will be sent with the beep sound so the user can identify it easily. The text message which consists of the secret random code cannot be edited or forwarded. The secret code will be present only for a particular time but the intimation will be present permanently.

Use of Dynamic Password: Since the password given with the ATM card only used as a reference it cannot be used as the main secret code to access the account. So, even if the hackers or skimmers steal the data or code at a particular transaction of a user, they cannot use that secret code for the next time, as we are producing the random password at the time of accessing the data. There is a time limit to enter the particular random secret code if the time limit exceeds, the user will not be allowed to access the data. Because of the dynamic password the user have to bring the phone while entering the ATM. So it is also a safest way to handle with money.

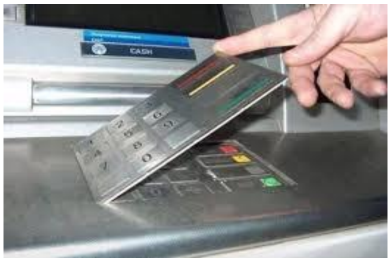

Fig.2.Card reading keyboard to enter pin

Characteristics of Dynamic password: It is the single key to access the account. The ATM is only a reference to identify the user.

It should be a random number.

It should be different for each and every access.

It should be displayed only for a short period in mobile phone.

Disadvantages of normal ATM password: We all know well about the problems that we are facing in the normal ATM accessing system. The thief can steal that password.We can know the theft of the money by the notification sent by the bank when the thief is accessing our account and withdrawing money from our account. But we cannot be able to restrict their activities till we go to the respective bank and do some official avoidance like blocking our ATM card. It cannot be done in all the cases. We may be in the other state or other country. Even if we try to block the card by the phone call to the bank, the thief will already swipes the card for more number of times within a short period. In the normal method there is no rule to have the phone with us. In this case if the users tries to access their ATM, thethief can easily attack the user and they steal their money. In normal ATM system there is no safety precautions to the user but there is safety for the ATM machine.

Advantages of dynamic password: If we are using the dynamic password the data loss will be reduced and without the password that is produced and sent to the user's personal contact number the thief or hacker could not be able to access the card. If the thief tries to use stolen card, the ATM machine will be asking for the secret random password which was sent to the mobile number. By which the user will also be intimated that someone is accessing their card. If we are using the dynamic password the data loss will be reduced and without the phone the thief or hacker could not be able to access the card. The ATM machine will be prompted only for that secret code. That will be available in the mobile screen only for a few minutes. That access will be intimated to the user. Without that password no one could be able to access the card. In the rare cases they also can steal the mobile phone of the user. In such cases the user should be alert and block their respective phone number. In this modernised world even we miss a small memory card in which we don't have any interaction too affects our consciousness. But nowadays phones are like the hand for the people who are using it. So they will know that they have missed their mobile phone. After that they should take the safety actions to block their mobile number. In this method the user doesn't have to block their respective card. This reduces the complexity. So the user will be safe by using the mobile phones inside the ATM especially it is very safe for the working women.

CONCLUSION

Eventually this paper which contains the knowledge about the cryptography with dynamic password explains how the normal ATM system is affected by the thieves as well as it explains about the various techniques that are used for encrypting the plain text and also about the decryption. This paper comprises the solution to avoid the theft activities by using the idea of dynamic password. This paper ensures that no one could be able to access the account of a particular user without their permission. We thought that this technique will be very useful for our developing modernised country.

REFERENCES

Textbook for Students and Practitioners, companion web site contains online cryptography course that covers public-key cryptography, Springer, 2009, Bruce Schneier, Applied Cryptography, 2nd Edition, Wiley, 1996.

Delfs, Hans &Knebl, Helmut, Symmetric-key encryption, Introduction to cryptography: principles and applications. Springer, 2007.

Pelzl&Paar (2010). Understanding Cryptography. Berlin: Springer-Verlag.

Christ of Paar, Jan Pelzl, Introduction to Public-Key Cryptography, Chapter 6 of Understanding Cryptography, A

Piper, Fred and Sean Murphy, Cryptography: A Very Short Introduction ISBN 0-19-280315-8.

Goldreich, Oded. Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.

Merkle, Ralph; Hellman, Martin, Hiding information and signatures in trapdoor knapsacks, 1978.