Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Authentication for securing network Using Passwords with Tree

Gurusharan Kaur
Department of Mathematics
Barkatullah University,
Bhopal, India

Dr. Rizwana Jamal
Hod, Department of Mathematics
Safia Science College,
Bhopal, India

Abstract - The proposed work aims to enhance authorization and authentication process by using multilevel authentication to protect network from spiteful user and unauthorized access, implement security measure to protect data. It will also provide service level security.
We provide a simple yet powerful demonstration of how a sturdy change in graphical password interface can provides security. We propose a latest and slightly different method to calculate password which cannot be easily crack by brute force attack.

Keywords - Multilevel Authentication, Service Level Security, password, brute force attack.

I. Introduction

Until recently computer and network security has been formulate as a technical problem. However, it is now widely recognized that most security mechanisms cannot succeed without taking into account the user (Patrick, Long, & Flinn, 2003). A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, are possible substitutes. This paper reports on research aimed to design a new kind of graphical password system, alphanumeric passwords. The significance of this research is the provision of a flexible graphical password system.

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess, they should be changed frequently, and should be different on different accounts of the same user. Key should not be written down or stored in plain text. Encrypted key should also not easily decrypt.

Satisfying these requirements is almost impossible for users. Consequently, users ignore the requirements, leading to poor password practices.
There are various types of attack methods and therefore technologies are developed to provide security to internet and network.

Computer security attributes	**Attack methods**	**Technology for Internet security**
Confidentiality	Eavesdropping, Hacking, Phishing ,DoS and IP spoofing	IDS , firewall, cryptography system, IPsec and SSL
Integrity	Virus, Worms , Trojans , Eavesdropping , Dos and IP spoofing	IDS, firewall Anti malware software , IP sec and SSL
Privacy	Email bombing , spamming, hacking Dos and cookies	IDS, firewall Anti malware software , IP sec and SSL

Normally Cryptographic systems are classified along three independent dimensions:

1. Kind of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Substitution, in which each element in the plain text is mapped into another element. Second is transposition in which elements in the plaintext are rearranged. The fundamental constraint is that no information be lost.

2. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. The method is asymmetric if the sender and the receiver each uses a different key ,two key, or public-key encryption.

3. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Classical encryption techniques:
The two basic components of classical ciphers are substitution and transposition. Then other systems illustrate that combines both substitution and transposition.

Substitution techniques:
This is a technique in which letters of plaintext are replaced by or by numbers and symbols. If plaintext is viewed as a sequence of bits, then substitution involves swap plaintext bit patterns with cipher text bit patterns.

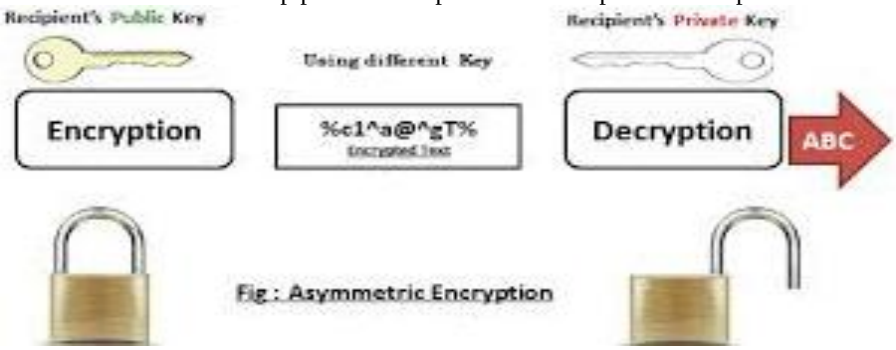
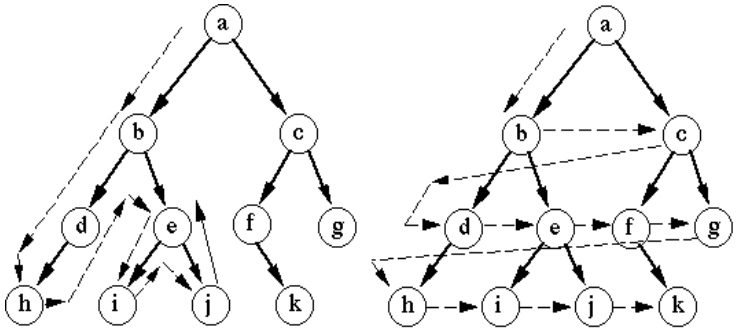


Fig : Asymmetric Encryption

Caesar Cipher
Caesar Cipher replaces each letter of the message by a predetermined letter or a predetermined distance away. We refer the security and usability problems associated with alphanumeric passwords. We are try to use basic concept of tree to secure data.



Depth-first search Breadth-first search

How to draw tree using Inorder and preorder sequence:-
Let us consider the below traversals:
Inorder sequence: D B E A F C
Preorder sequence: A B D E C F
In a Preorder sequence, leftmost element is the root of the tree. So we know 'A' is root for given sequences. By searching 'A' in Inorder sequence, we can find out all elements on left side of 'A' are in left subtree and elements on right are in right subtree. So we know below structure now.


```
          A
         / \
        /   \
       D B E   F C
```

We recursively follow above steps and get the following tree.

```
       A
     /  \
    /    \
   B      C
  /\     /
 /  \   /
D    E F
```

II. RELATED WORK

There are technology developed to secure network like firewall, IDS, Antimalware software but still there is a need to develop a secure cryptographic system. Since it is not probable to present all the methods, very vital and popular methods were presented. It is seen that the modified Hill cipher Encryption and Decryption requires generating random Matrix, which is basically the power of security. As we know in Hill cipher Decryption requires inverse of the matrix. Hence while decryption one problem arises that is. Inverse of the matrix does not always exist. Then if the matrix is not invertible then encrypted text cannot be decrypted. But the downside is completely abolish in modified Hill cipher algorithm. At the same time, this method requires the cracker to find the inverse of many square matrices which is not computationally easy.
In the existing methods of cryptography there are many disadvantage like

1. Calculation are too long
2. Complexity of algorithm decreases the throughput of CPU.
3. Complexity increases but reliability does not ensure users that it can be used in any sensitive areas.

III. PROPOSED WORK

It is not a symmetric key algorithm. In the proposed algorithm we are not directly sending the data in encrypted form. But instead of this we are sending some data on the basis of which we have to draw tree to calculate password. It is not easy to guess by the intruders that the data we are sending is "actually what it is".

we have to draw tree to calculate password. It is not easy to guess by the intruders that the data we are sending is "actually what it is". Tree traversal method of depth first search is used which is having three methods

a. Inorder
b. Preorder
c. Postorder

Method of Encryption

1. Send some plaintext in reverse order to the receiver
2. Donot specify what it is
3. It is only known by the receiver and sender what it is.

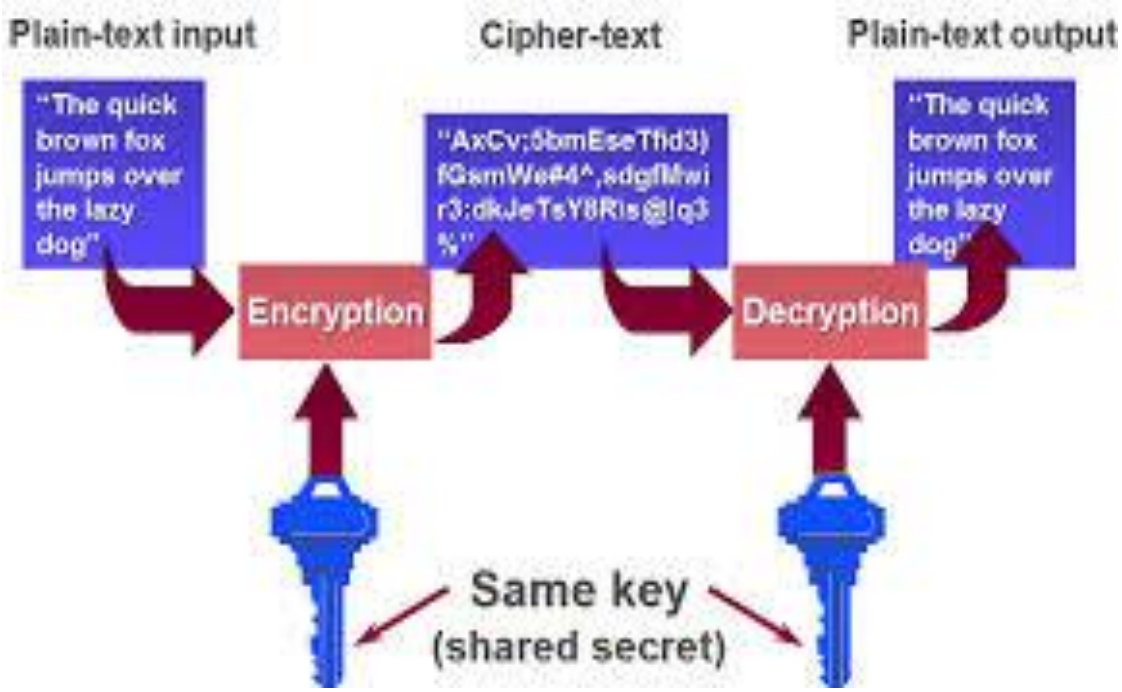
Method of Decryption

1. The received data is actually inorder and preorder sequences in reverse order send by the sender.
2. Now the receivers have to reverse the received data first.
3. Calculate tree node, left node and right node on the basis of which we draw a tree.
4. Now we get a tree.
5. Calculate Breadth first search of the tree.
6. Now calculate reverse order of the received data which is actually the password.
7. For every new transaction we change the method of reversing the data in alternate. i.e for 1^{St} transaction reversed breadth first search is the password and for 2^{nd} transaction direct breadth first search is the password.

Algorithm : build Tree()

1) Pick an element from Preorder. Increment a Preorder Index Variable (preIndex in below code) to pick next element in next recursive call.
2) Create a new tree node tNode with the data as picked element.

3) Find the picked element's index in Inorder. Let the index be inIndex.
a. visiting the node first, then its children (pre-order traversal): a b d h e i j c f k g
b. visiting the children first, then the node (post-order traversal): h d i j e b k f g c a
c. visiting some of the children, then the node, then the other children (in-order traversal): h d b i e j a f k c g and make the built tree as left subtree of tNode.
4) Call buildTree for elements before inIndex\
5) Call buildTree for elements after inIndex and make the built tree as right subtree of tNode. return tNode.



Advantage of the algorithm

1. We are not directly applying encryption methods on the actual data.
2. Receivers have to do many calculations on the received data to get the actual data.
3. Proposed method is not required complex calculation for encryption and decryption.
4. Actual password is in hidden form.
5. If data can be fetched by the intruders then they donot know what to do with this data, they sometimes think that it is key and on the basis of which they are trying to do all hit and trials on that data, which is only helpful to draw tree and fetch and retrieve actual password which is keep save.
6. Not need to do calculation at both ends, i.e by sender as well as receiver.

IV. CONCLUDING REMARKS AND FUTURE WORK

The proposed scheme is resistant to security attacks in networking. The scheme provides multilevel authentication.
There are numerous methods of conventional cryptography, and since it is not probable to present all the methods, very vital and popular methods were presented. It is seen that the modified Hill cipher Encryption and Decryption requires generating random Matrix, which is basically the power of security. As we know in Hill cipher Decryption requires inverse of the matrix. Hence while decryption one problem arises that is. Inverse of the matrix does not always exist. Then if the matrix is not invertible then encrypted text cannot be decrypted. But the downside is completely abolished in modified Hill cipher algorithm. At the same time, this method requires the cracker to find the inverse of many square matrices which is not computationally easy. In future we can also enhance the same security method with special characters and alphanumeric strings.

REFERENCES

[1] Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp 234-238, 2009
[2] Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic EncryptionScheme, On Line March 2007, www.citeseer.ist.psu.edu.
[3] Bluekrypt 2009: Cryptographic Key length Recommendations,http://www.keylength.com

[4] Blum L., Blum M , Shub M. : A simple unpredictable pseudo random numbergenerator , SIAM J. compute , 1986, 15, (2), pp 364-383.
[5] Brics: Universally comparable notions of key exchange and secure channels, LectureNotes in Computer Science, Springer, Berlin, March 2004.
[6] Sage.math.Washington.edu/home/jetchev/Public.html/docs/jetchev-talk.ppt- Broadcast encryption schemes.
[7] Brassard G.: Modern Cryptology , a tutorial lecture Notes on computer science , (325) ,(spring-verlas) .
[8] Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.
[9] Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non specialists, EURASIP Journal,Vol 07, Article 10
[10] Donavan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations

