www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-2, Issue-1, Feb- 2014
Technical Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Randomly Generated Algorithms and Dynamic Connections

Harmanpreet Singh[1*], Amritpal Singh Danewalia[2], Deepak Chopra[3], Naveen Kumar N[4]

[1*,2,3,4]*Department of Computer Science Engineering*

VIT University, Vellore, Tamil Nadu

Received: 08 Jan 2014 | Revised: 28 Jan 2014 | Accepted: 22 Feb 2014 | Published: 28 Feb 2014

Abstract-In the modern computer world, maintaining the information is very difficult. Some interrupts may occur on the local system (attack) or network based systems (network attack). Without security measures and controls in place, our data might be subjected to an attack. Several passive attacks like wire-tapping, port scanning etc. are well known that are used to monitor communication between nodes and also further used in other types of active attacks like man-in-the-middle attack etc. The man-in-the-middle attack, in cryptography and computer security is a form of active eavesdropping in which independent connections are made by the attacker with the victims so that attacker can relay messages between them. The entire conversation is controlled by the attacker making the victims believe that they are communicating with each other privately. Our approach to stop these types of attack is described as, once the initial authentication is done between the communicating nodes, they can start communicating using some standard encryption algorithm like DES, TEA or public key cryptography. But instead of using the same static communication channel and encryption algorithm, we will switch between different algorithms after a certain interval of time which has already been available with nodes.

Keywords—Communication System Security, Computer Network Security, Data Security, Internetworking, Network

I. INTRODUCTION

In the connected world, everyone is aware of the term 'network', which is being considered as a connection of independent computers. The basic idea of network is to allow people to get connected even if they are geographically distant from each other. Connection also includes sending of data in any direction i.e. it is designed to send data both back and forth.

Sometimes the data exchanged is private; therefore we must ensure network security irrespective of the size of the data or network. The main aim of network security is to protect the data from unauthorized access i.e. from the users that don't have the privilege to access the data, so that misuse of data can be prevented. We need to ensure network security because of the characteristics of network to have remote access. For example, a hacker could be easily identified if physical access would be vital but the presence of networks allows this security aspect to be bypassed.

As a result of which it is very important to maintain stringent security policies, irrespective of the type and size of the network, so that potential losses can be prevented.

In this paper, we are proposing to provide network security to the communication between two nodes. As many passive attacks present are used to monitor communication between nodes and also this analysis of communication further used in other types of active attacks like man-in-the-middle attack. Our approach to stop these types of attack is described as, once the initial authentication is done between the communicating nodes, they can start communicating using some standard encryption algorithm like DES, TEA or public key cryptography. But instead of using the same static communication channel and encryption algorithm, we will switch between different algorithms after a certain interval of time which has already been available with nodes as switching between algorithms reduces the risk of prediction of on-going communication between different stations.

Corresponding Author: Harmanpreet Singh

II. SECURITY IN COMMUNTICATION SYSTEMS

Network security is an important aspect in communication systems. In order to prevent potential losses which may occur through misuse of data, network security must be ensured.

Some of these potential pitfalls include:

Unauthorized access to private data: Almost every business, institution or organization has the need to keep certain critical information away from the competitor's eyes and wants only its own members to have an access to that information.

Manipulation of data: Data irrespective of its size holds an utmost importance to both organizations and individuals. Any type of manipulation or destruction of data can cause an organization to get blighted [5].

Thereby to prevent breach of data over the communication channel we intend to provide network security by randomly switching between different cryptographic algorithms.

CRYPTOGRAPHY

This is a technique used to secure the data using encryption and decryption of the data [2].

A. Encryption

This is method to encode the message in such a way that, the data is not vulnerable to third party attack.

B. Decryption

This method is used to decode the encrypted data using the reverse of the technique used to encrypt the data.

Basically there are two cryptographic techniques being used i.e. asymmetric cryptography and symmetric cryptography.

C. Symmetric Cryptography

Symmetric cryptography involves one shared key both for encryption and decryption of messages [4].

D. Asymmetric Cryptography

Asymmetric cryptography makes use of two such keys, namely private and public key.

Both these techniques have advantages and disadvantages which are as follows-

Advantages of symmetric cryptography-

1). Simple: It's easy to carry out this type of encryption. All it involves is specification from user and sharing of the secret key before user begins to encrypt and decrypt messages.
2). Fast: It's faster to implement symmetric key cryptography rather than implementing asymmetric key cryptography.
3). Uses less computer resources: Usage of computer resources is quite less in single key cryptography. [2][4].

Disadvantages of symmetric cryptography-

1) Need to establish a secure channel for sharing of key.
2) Too many keys: Asymmetric cryptography involves generation of a new key while communicating with different parties which creates problem in management of keys. Moreover security of all keys requires extra effort.

Advantages of asymmetric cryptography-

1). Convenience: As it involves two keys i.e. public key for encryption and private key for decryption, thus eradicating the problem of distributing the shared key among communicating parties. Public keys are broadcast while private keys are kept secret.
2). Detection of tampering. [3]

Disadvantages of asymmetric cryptography-

1) *Speed:* Asymmetric cryptography is slow compared to symmetric cryptography making it infeasible in decrypting bulk or complicated messages.
2) *Requires more computer resources:* In implementation, public key cryptography requires a lot more computer resources than single key cryptography [3].

III. SELECTION OF ALGORITHMS

We tend to select algorithms which are simple, fast and easy to implement and at the same time are able to provide the required network security (encryption). The basic idea is to make use of the advantages of both symmetric and asymmetric algorithms while at the same time overcoming their respective disadvantages. As our approach involves switching between different algorithms which requires an overhead of time, therefore, we are keen on using the symmetric algorithms over asymmetric algorithms as they are fast and require less computer resources. The proposed approach fills in the gap of that extra security which has been considered an added advantage of asymmetric algorithms. Algorithms like TEA, SEED, and BLOWFISH etc. have been used for the implementation purposes [6].

IV. METHODOLGY

We provide solution as follows:

The encryption algorithm is randomly selected at one node and correspondingly decryption algorithm has been selected over the other node.

For the next message, a new encryption algorithm has been used to encrypt the data, the algorithm selected randomly. Similarly the receiver chooses the corresponding decryption algorithm and receives the message. This synchronization of the selection of corresponding encryption and decryption algorithms can be either achieved by passing the algorithm number along with the encrypted message or by some pre-shared algorithm.

The security has been achieved because no one knows when which algorithm is used. So no one can decrypt the message.

The selection of encryption algorithms is random. It could either be achieved by the use of rand () function or by linear congruential method i.e. r=(a*r+b)%m where a and b are large prime numbers and m is 232 or 264 .The initial value of r is seed. If you get over the same seed you get the same sequence of random variables. The choice of numbers being generated by rand () provides pseudo-random numbers whilethe latter technique is the most suitable way of generating random numbers.

IV.DESIGN AND IMPLEMENTATION

Setting up the UDP communication

Here are a few steps involved in using sockets:

1. Firstly, Socket is created
2. Next step involves identification of socket (name it)
3. On the server, wait for a message
4. On the client, send a message
5. Send a response back to the client (optional)
6. Close the socket [7].

Randomly select the encryption/decryption algorithm

Implementation of first algorithm

In this particular algorithm, encryption is done as follows, firstly each word in the string is reversed and then it is encrypted as follows: 0 being added to the 1st element, 1 being added to 2nd element, 3 being added to the subsequent element and son. Adding numbers here signify the fact that the alphabet is shifted towards right as many times as the number and is replaced with the new alphabet obtained. This marks the encryption of data.

For decryption from the alphabet at 1st position 0 is subtracted and from the alphabet at second position 1 is subtracted and son. Subtracting here signifies that the alphabet is shifted as many times towards the left as the number and is replaced with the new alphabet obtained.

Now each word obtained is reversed. This marks the decryption of data.

Implementation of second algorithm

Tiny Encryption Algorithm (TEA) operates on two 32-bit unsigned integers (could be derived from a 64-bit data block) and uses a 128-bit key. It has a Feistel structure with a suggested 64 rounds, typically implemented in pairs termed cycles. It has an extremely simple key schedule in which all of the key material is mixed in exactly the same way for each cycle. Different multiples of a magic constant are used to prevent simple attacks based on the symmetry of the rounds. The magic constant, 2654435769 or 9E3779B916 is chosen to be 232/ϕ, where ϕ is the golden ratio. The general logic circuit implementation is given as[1]:

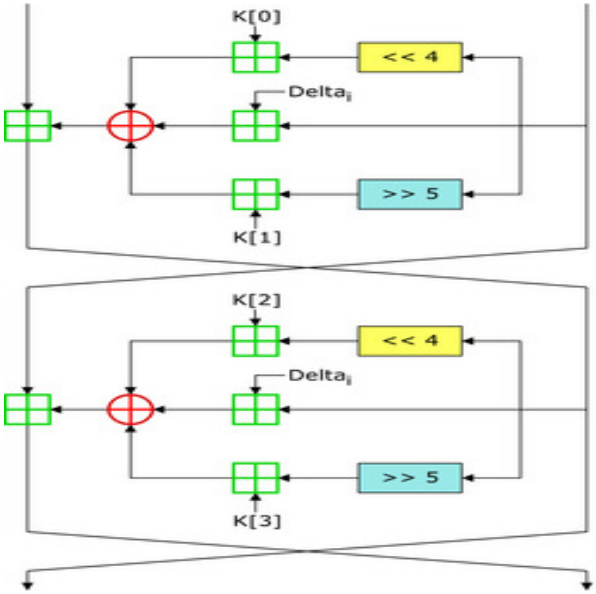

Fig: Logic circuit of TEA Algorithm

Implementation of Third algorithm

In this algorithm, firstly there is an array which contains all possible alphabets, numbers, and special symbols not necessarily in the same order. Also there is another array which contains the values of keys; these both arrays are already shared between the communicating nodes. Now at the encrypting part the input string to be encrypted is taken each character wise and compared with the array which contains all possible variables, now from this comparison index is found i.e. the index value at which the given input value resides in the first array, this index is XOR with the key value, which resides in the second array. This marks the encryption of data. For decrypting reverse operation is performed. The advantage of this algorithm is that it is simple to implement therefore it consumes less computer resources.

V. CONCLUSION AND FUTURE WORKS

As the proposed solution overcomes the problems faced by the common cryptographic techniques and hence making the communication more reliable. This solution makes use of advantages of both symmetric and asymmetric algorithms thus overcoming their respective drawbacks.

Future work includes optimization of the algorithms being used and betterment of the random number generation technique.

VI .ACKNOWLEDGEMENTS

Our sincere thanks to all the faculty members, acquaintances and friends who helped us bring this work across.

REFERENCES

[1]. Derek Williams, "The Tiny Encryption Algorithm (TEA), CPSC **6128** – Network Security", Columbus State University, **2008**.

[2]. Prof K. Govinda, Dr.E. Sathiyamoorth, "Multilevel cryptography technique using graceful codes", Journal of Global Research in Computer Science, **2011**.

[3]. Matt Blumenthal, Encryption: "Strengths and Weaknesses of Public-key Cryptography", Department of Computing Sciences, Villanova University, Villanova, PA 19085 CSC 3990 – Computing Research Topics

[4]. Niraj Kumar, Prof. Sanjay Agrawal, "Issues and Challenges in Symmetric Key based Cryptographic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, **2013**.

[5]. C. Onwubiko, A. P. Lenaghan, "Managing Security Threats and Vulnerabilities for small to Medium Enterprises", IEEE International Conference on Intelligence and Security Informatics **2007**.

[6]. H Sathu, Network Security: "A Layered Approach", NZ Journal of Applied Computing & Information, **2002**.

[7]. Yunhong GU, Robert L. Grossman, "UDP-based data transfer for high-speed wide area networks", Science Direct, **2007**.

