A Puzzle Based Client-Server Authentication Model with Secure Data Transfer

Laxman Dande[1], Soppari Kavitha[2], Lt. K.Ravindra Babu[3], Akash Singh[4], Kiran Vanam[5]

[1]*working as a Software Engineer with TRY LOGIC Soft Solutions AP Pvt Ltd, with 2 years of experience.*

[2]*working as Head Department of CSE, Professor at Holy Mary Institute of Technology.*

[3]*working as a Associate Professor at KITS, Singapore, Karimnagar, Affiliated to JNTU, Hyderabad, A.P., India.*

[4]*working as a Senior Software Engineer with TRY LOGIC Soft Solutions AP Pvt Ltd, with 3 years of experience.*

[5]*working as a Senior Embedded Engineer with TRY LOGIC Soft Solutions AP Pvt Ltd, with 3 years of experience.*

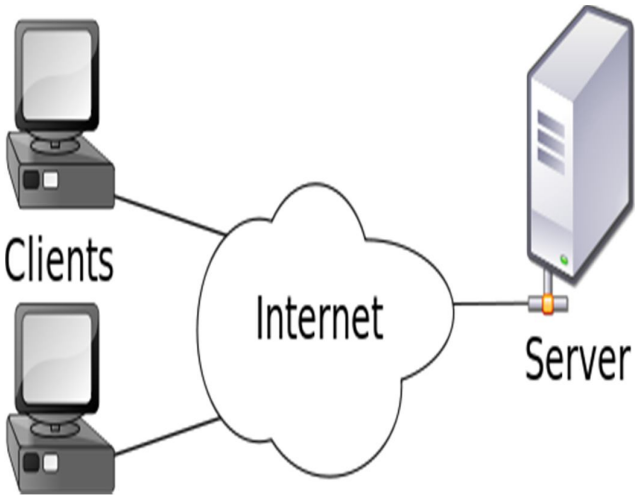
Abstract **-** In the present day scenario, we are seeing that many online applications are attacked by the intruders, and there is no proper solution built for the same. Here in this proposed work we are working on the area which is not only providing security to the data but also it is providing security to the communication link. Communication link here refers to the connection between two computer network bodies i.e. Client and Server. Client is generally a system which is going to request for the data and Server is a machine which takes the request coming in from the client and processes it. Client and Server are two major bodies in the computer networks responsible for network level communication and this information interchange between them is an example of inter-process communication. The language and the rules for communication are defined in a communication protocol and all these protocols operate in the application layer.

The main purpose for working on this area is that we wanted to have a secure communication architecture which is being developed with the below architecture. As there are many attackers who mainly concentrate to crash the server, so to overcome this problem we are designing a framework where a puzzle will be shown to the request sender and only after solving that puzzle the client will be able to request anything to the server. In the next level for improving security i.e. for the data transmission in the network we are taking the help of cryptography and ensuring the second level safety for the data which is travelling in the network.

Index Terms—communication, client, server, protocol, puzzle, attacker, intruders, cryptography.

I. Introduction

A computer network or data network is a telecommunications network which allows computers to exchange information. In computer networks, networked devices transfer data to each other along data connections. The connections between nodes are established using either cable media or by wireless media. Network is nothing but connecting one or many systems together for data transfer. Networks in which certain hosts have special dedicated tasks which are providing services to other computers (in the network) are called client-server networks. The client–server model of processing is a distributed application structure that divides tasks or workloads between the providers of a resource or service, called servers, and the one who requests is called client. The best-known computer network is the Internet. Very often clients and servers communicate over a computer network on separate hardware, but both may reside in the same system.



Client-Server Architecture

A server host executes one or more server programs which share their resources with clients. A client does not share any of its backing, but requests a server's content or service function. Clients therefore setup communication sessions with servers which will be waiting for the incoming requests. Both client and server follow some protocol for the communication and that protocol could be TCP (Transmission Control Protocol) and the other being UDP (User Datagram Protocol). Protocol is nothing but the flow of the program. It is a step by step process for achieving the required outcome. As in the above figure you can see that client and server are connected with a medium called internet. Internet is basically providing the data from server to client. This type of architecture can also be achieved in the LAN (Local Area Network). It is a kind of network where the systems are interconnected and data transfer will be done in the form of packets. Coming with the two protocols mentioned above i.e. TCP and UDP, TCP is more reliable and considerably better when compared to UDP.

TCP is connection oriented protocol means that both client and server can communicate only when the communication link acquired between them and only server will have an identification value which is nothing but port number. Coming with UDP it is connectionless protocol, here server and client are independent i.e. client and server will have unique identification value which is nothing but different port numbers. TCP is more reliable when compared to UDP because of its two main advantages, first being the faster transmission in network and second being acknowledgement for each and every packet that is transmitted over the communication channel. In case of UDP we will not get any acknowledgement for the packets transmitted which is a drawback or can be called as time consuming process.

Game theory is a new advancement in the technology to eliminate the problem of attackers. Attacker is a user in networking domain who just keeps on sending the requests without waiting for the response to the request sent. Attacker is generally a robot operated by the intruder and the main reason behind the process is to crash the server by giving plenty of requests going beyond the response limit. To overcome such kind of problem in networks this concept of game theory was introduced. Game theory or can call it as puzzle based mechanism. As already told that the system is designed in a manner where the attacker main purpose is to send the requests continuously so in order to stop this functionality we are using the puzzle based mechanism here i.e. this concept is mainly used to authenticate the genuine user from the attackers.

II. Proposed work

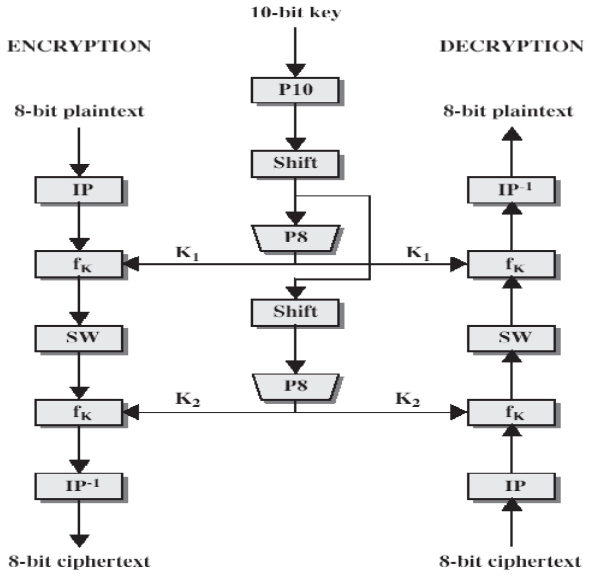
Our proposed work shows the study on how we authenticate the genuine user from the attacker taking the help of puzzle mechanism and later providing security to the data that is travelling on the network. This overall process is carried out in the networking technology with TCP as the communication protocol as it is more reliable than any other communication protocols in the computer networks.

We are going to encrypt the data in the network during the communication process. As data is travelling in the network there is a chance that it could be hacked by the intruder and to overcome this fear we are going to provide security to the data with the cryptography algorithm called DES (Data Encryption Standard). We have many algorithms for providing security to the data but the out of the available we have opted the efficient algorithm i.e. Data Encryption Standard.

Data Encryption Standard is a Symmetric key algorithm which was developed in 1970s at IBM. DES is the archetypal block cipher algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of same length. In case of DES, block size is 64 bits, DES uses a key to customize the transformations, such that decryption can supposedly only be performed by those who know the particular key that was used to encrypt data. The key ostensibly contains 64 bits; however, from which only 56 of these are actually used by the algorithm. 8 bits are used only for checking parity, and are discarded after the process. Hence the effective key length is 56 bits.

The key is nominally stored or transmitted as 64 bits, each with odd parity. As per ANSI X3.92-1981, One bit in each 8-bit byte of the *KEY* may be utilized for error detection during key generation, storage and distribution. Bits 8, 16,..., 64 are ensuring that each byte is of odd parity.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in processing. FIPS-81 specifies several modes for its usage with DES.
Decryption uses the same structure as encryption but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions.)



DES encryption (decryption) algorithm takes 8-bit block of plaintext (cipher text) and a 10-bit key, and produces 8-bit cipher text block. Ciphertext conversion involves 5 functions: an initial permutation (IP); a function f_K, which includes both substitution & permutation and depends on a key input; a simple permutation function that switches (SW) the 2 halves of the data; the function f_K; and finally, a permutation function which is the inverse of the initial permutation (IP^{-1}). Decryption process is similar i.e. the function f_K takes 8-bit key which is obtained from the 10-bit initial one or two times. Key is first subjected to a permutation P10, later shift operation is performed. Output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first sub key (K1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the 2nd sub key K2. DES is a ***block cipher***--meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of equal size. Thus DES results in a ***permutation*** among the 2^64 (read this as: "2 to

the 64th power") possible arrangements of 8 bytes, each of which could be 0 or 1. Each block of 64 bits is divided into two blocks of 4 bytes each, a left half block **L** and a right half **R**. The 64-bit key is permuted according to the below table, **PC-1**. Since the first entry in the table is "57", this means that the 57th bit of the original key **K** becomes the first bit of the operated key **K**+. The 49th bit of the original key becomes the second bit of the calculated key. The 4th bit of the original key is the last bit of the calculated key. Please note only 56 bits of the original key appear in the permuted key.

PC-1

56	49	41	33	25	17	9
2	58	50	42	34	26	18
11	2	59	51	43	35	27
29	11	3	60	52	44	36
62	55	47	39	31	23	15
6	62	54	46	38	30	22
12	6	61	53	45	37	29
23	13	5	28	20	12	4

We get the 56-bit permutation. Next, split this key into left right halves, where each half has 28bits. In the step two we have to encode each 64-bit block of data.

The proposed work gives security not only to data but also to the server. Process is designed to flow in the manner where it will first authenticate the connection between the server and client, only after the client proving its genuinity the connection link will be organized between client and server. The concept implemented here is game theory also referred as puzzle based mechanism. It is nothing but a small game like which involves small amount of time from the user providing with little bit concentration can easily solve the puzzle and thus acquiring the link between client and server; failing this will result to blocking of the accessing rights of that client along with the IP address. Once the IP in the network is blocked, no request from that IP will reach to the server and can never involve in the communication process as it was being operated by intruder. In this manner we are going to block all those IP's which are being operated by intruders or attackers thus giving an opportunity to the genuine user to take the information from server. In the next level process we are taking the help of network security concept which is nothing but cryptography, with which request/response is encrypted and processed to make sure it is in the proper way of transmission and not hacked by the intruders in network. Even if the packet on the network is hacked by intruder, data cannot be revealed easily from it because it is in the encrypted form and can be decrypted only when the key matches, that is actually present at the receiver side, thus we are making the complete application threat safe.

Future Scope: As it is securing the communication link between client and server with a puzzle mechanism. To provide more security for the communication link we can use randomized puzzles i.e. as in the proposed work we are displaying only a single puzzle which can be changed by providing more than one puzzle to the application and application will randomly choose any puzzle from the available ones and present it to the user or client. Clearing this will provide a clear communication channel link to the client with the server and rest of the process goes on in the normal manner.

III. Conclusion

We have concentrated on the network security domain to have a better communication channel between two hosts and there by securing the data transfer with the cryptography technique. We have achieved an attack free architecture which is more reliable and thus can be utilized in the real time applications. As the outcome we can conclude by telling that client and server will get connected only when client solves the puzzle displayed and thus making an effective link after the puzzle success, client can communicate with server for data processing in a more secured manner by employing encryption and decryption technique.

References

M.Naor and A. Shamir, "Visual cryptography," in *Proc. Advances in Cryptography (EUROCRYPT'94)*, 1995, vol. 950, LNCS, pp. 1–12.

R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam. Electron., Commun., Comput. Sci.*,vol. 82, pp. 2172–2177, Oct. 1999.

C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, pp. 481–494, Mar. 2004.

S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion,"*J. Vis. Commun. Image Represent.*, vol. 21, pp. 900–916, Nov.2010.

G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.

F. Liu, C. Wu, and X. Lin, "Step onstruction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

Authors Profile

Laxman Dande working as a Software Engineer at Try Logic Soft Solutions AP Pvt. Ltd with an experience of 2years.

Soppari Kavitha working as a Professor, Head Department of Computer Science Engineering at Holy Mary Institute of Technology, Keesara, Ranga Reddy. Affiliated to JNTU, Hyderabad, A.P., India. My research interests are Image and Data Processing, Information Security.

Lt. Ravindra Babu working as an Associate Professor at Kamala Institute of Technology & Science, Singapur, Karimnagar. Affiliated to JNTU, Hyderabad, A.P., India. My research interests are Network Security, Information Security.

Akash Singh working as a Senior Software Engineer at Try Logic Soft Solutions AP Pvt. Ltd with an experience of 3 years.

Kiram Vanam working as a Senior Embedded Engineer at Try Logic Soft Solutions AP Pvt. Ltd.