Security in Voip Network Using Neural Network and Encryption Techniques

Ashwini Galande[1], Dattatraya Londhe[2] and Mangesh Balpande[3]

[1,2,3]Affiliation: Assistant Professor

Gharda Institute of Technology, Lavel, Ratnagiri, Maharashtra, India.

Abstract- Voice over Internet Protocol is one of the fastest growing applications. Since VoIP networks are very much vulnerable to attacks, providing security in such networks is a matter of great concern. For secure communication in VoIP network, authentication and integrity of messages must be provided. In this paper, we use a remote password authentication scheme for multi-server environments. The password authentication system is a pattern classification system based on artificial neural network. In this scheme, the users only remember user identity and password numbers to log in to various servers. Users can freely choose their password. Furthermore, the system is not required to maintain a verification table and can withstand the replay attack. For integrity of messages, we use modified AES algorithm in which it will be able to accept variable length packets for encryption and decryption.

Keywords: Asterisk, AES, neural network, password authentication, remote login.

1. Introduction

Voice over Internet protocol allows us to make calls over broadband internet connection instead of regular leased lines. VoIP also provides facilities like sending faxes. It converts audio data into digital signals, divides it into packets and delivers them over respective routes and reassembles them at the receiver [1]. Each packet contains source and destination addresses.

The Session Initiation Protocol (SIP) is a signaling protocol for initiating, managing and terminating voice and video sessions across packet networks. If call is made to computer then there are soft-phones which load VoIP services onto the desktop or laptop. The most fundamental and important thing in the transmission of voice information through IP network, is the authentication of user identity; VoIP cannot end at physical location information to carry out certification and authentication, VoIP terminals because the physical location of information and network are independent of each other to provide for VoIP terminal with mobility. Thus, VoIP can only be resolved through username and password [2].

Asterisk is a private branch exchange (PBX) which acts as a SIP server for establishing calls. This is the technique which is being used and it offers no internal security though it provides external encryption decryption facility which can be only used by a trained professional. All SIP devices are registered with SIP server in sip.conf file for making VoIP calls. Each SIP server i.e. asterisk server should be registered in each other's IAX.conf file and extension is given to each device [3], [4]. If call is made within the network then communication is not through the asterisk server. But if call is made outside the network then communication is through the asterisk server. Hence for availability of servers we need to create multi-server network architecture.

Password authentication is one of the mechanisms that is widely used to authenticate legitimate users. In order to avoid the security problem, some password authentication schemes have been proposed as in [5], [6]. In this paper, we use an efficient remote password authentication scheme based on neural networks. This

Ashwini Galande[1], Dattatraya Londhe[2] and Mangesh Balpande[3]
Tel.: +02356 – 262795 / 97 / 98; fax: 02356 – 262980.
E-mail address: ashwini.pict@gmail.com, dattatraya.londhe@gmail.com, mangesh11.engg@gmail.com.

system identifies the legitimate user in real time using a pattern classification technique and is applicable to multi-server network architecture. In this classification system, the input pattern is the user password and the output is the serviceable servers [7]. Once the password is accepted communication gets established. According to incoming or outgoing data, packets can be encrypted or decrypted using Advance Encryption Standards.

2. Authentication Scheme Using Neural Networks

In this section, we propose a remote password authentication scheme that utilizes a neural network. This scheme is designed for a multi-server environment. In the password authentication process, there are two participants: the SIP users and the various Asterisk Servers (AS). In our scheme, each legitimate user holds only a user identity and its corresponding password. The asterisk server recognizes a user through the neural network. The neural network is trained and the same weights are stored in each asterisk server. The process can be divided into three phases: 1) the registration phase; 2) the login phase; and 3) the authentication phase. Before logging in to asterisk server, a new SIP user must first register some information in sip.conf file of asterisk to become a legitimate user. The registration phase is performed only once. After each legitimate user obtains a valid user identity and password, the user types his identity and password to login to any one of the asterisk servers. In the authentication phase, the servers validate the legitimacy of the remote login SIP user.

The Training Pattern															
Input										The expected output					
password								v		Ser_6	Ser_5	Ser_4	Ser_3	Ser_2	Ser_1
K	g	i	K	a	X	X	D	1	7	0	1	0	0	0	1

Fig.1 The training pattern

In the remainder of this paper, U_1, U_2,…, U_n stands for SIP users and Ser_1,Ser_2,…,Ser_n stand for the various n asterisk servers. ID_i and PW_i stand for the SIP user identity and password of U_i. Initially, AS chooses a large public values of p and g, where p is a large prime and g is a primitive integer number in Galois field *GF*(p). $E_k()$/$D_k()$ defines the AES-like encryption/decryption function using a 128–bits secret key , where AES-like is a symmetrical data encryption standard. It encrypts plaintext in 128 bits and outputs the cipher text in 128 bits[8], [9], [10]. In the following section, the proposed remote password authentication scheme for a multi-server architecture is described.

2.1 The Registration Phase

In the registration phase, the user must first register with the asterisk server. Assuming that the new user U_i is granted registration only from some certain asterisk servers, the steps of registration phase can be described as follows:

1) We allow the new user U_i to choose a login password PW_i freely. The user delivers the PW_i to the asterisk server in a secure manner. The AS then computes the user identity ID_i that satisfies

$$ID_i = E_k(PW_i) \qquad (1)$$

Without the key k, no one can compute the ID_i.

2) In this step, AS adds the training pattern of the new user to reconstruct the network. The network architecture consists of three layers: the input layer, the hidden layer and the output layer. The input units are the password characters and the value v. The password characters can be an English word or a numeral. In addition, the value v is related to the expected output. The output represents the serviceable servers. If the system has m servers, the number of output units is m. The training pattern includes the user's password, v and the expected output value. If the user receives the privilege of service from Ser_i, the *i*th unit of the expected output value denotes one. For illustration, consider a system having six servers and a new user can login to $Ser_1$and Ser_5. The input is shown in Fig. 1. "KgiKaXXD" is the new user's password. The value is

17, which is the binary number for the expected output 010 001. Then, AS collects the registered user's entire training pattern as the training set for the neural network. Before training, according to the mapping table, as shown in Table I, each input character is mapped into a value that ranges from zero to 62. Then, AS normalizes the input value that ranges from zero to one. Once the training process is completed by the AS, AS sends ID_i and v to user U_i and stores the networks weights and the secret key k in each asterisk server. The network model and the details of the training steps are described in the next section. The registration phase is complete up to this point.

2.2 The Login Phase

Assuming that the user wants to login to asterisk server Ser_j, the login phase is performed using the following steps:

1) The user obtains a time sequence T, which is like a timestamp.

2) Afterwards, the user computes W_i from

$$W_i= g^{PW_iT} \bmod p \qquad (2)$$

Then, the user delivers the ID_i, W_i, v and T to the login Asterisk server Ser_j.

TABLE I THE MAPPING TABLE

Character	null	a	b	c	d	e	f	g	h	i
mapping	0	1	2	3	4	5	6	7	8	9
Character	J	k	l	m	n	o	p	q	r	s
mapping	10	11	12	13	14	15	16	17	18	19
Character	t	u	v	w	x	y	z	A	B	C
mapping	20	21	22	23	24	25	26	27	28	29
Character	D	E	F	G	H	I	J	K	L	M
mapping	30	31	32	33	34	35	36	37	38	39
Character	N	O	P	Q	R	S	T	U	V	W
mapping	40	41	42	43	44	45	46	47	48	49
Character	X	Y	Z	0	1	2	3	4	5	6
mapping	50	51	52	53	54	55	56	57	58	59
Character	7	8	9							
mapping	60	61	62							

2.3. The Authentication Phase

In the authentication phase, the server receives W_i, ID_i, v and T at the time T^{I}. The server performs the following tasks to authenticate the user's login request.

1) The server checks the correctness of the timestamp first. If the time interval between T and T^{I} is greater than ΔT, the server rejects the login request. Let ΔT denote the expected legal time interval for transmission delay between the login terminal and the system servers.

2) If the timestamp T is within the valid period, the Ser_j decrypts the ciphertext (ID_i) from

$$PW_i = D_k(ID_i) \qquad (3)$$

Then obtains the user password and the server verifies if the following equation holds:

$$W_i= g^{PW_iT} \bmod p \qquad (4)$$

3) If the previous verification holds, the server authenticates that ID_i and PW_i are valid. Then the server authenticates the service privilege granted by the server. To provide proper service, the server normalizes the password and sends these values as input to derive the output values from the neural network. The outputs obtained represent the privileges that user can receive from the allowed servers. To transfer the output value into a binary number, we can check whether v holds. If the j^{th} output unit is the desired output that approaches one, the server accepts the user for login. The detail experimentation can be found in [7]. In this scheme, the system neither requires password nor verification tables. Each server stores only the same and fixed set of network weights and a secret key k. Each login user has only one pair, ID and PW, to log in into various servers in this system. Therefore, it is suitable for multi-server environments. Furthermore, this scheme validates the legitimacy of a remote login user in real time and can withstand the replay attack.

1.Security in VoIP Calls

Now as password gets accepted, communication is established. We checked for user authentication, now we need to provide message integrity. For this we provide encryption/decryption techniques. Now, the AES algorithm provides a facility in which security can be provided internally. Depending on whether it is incoming or outgoing, packet will be decrypted or encrypted accordingly. When connection is established, two channels are created in channel.c file; one is for incoming data and other for outgoing data. Data in channel.c file is without header so we can encrypt or decrypt that data using AES algorithm. Packets are formed in rtp.c file.

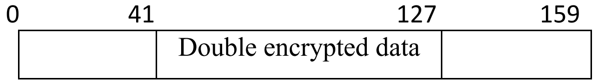

Fig. 3: Data of 160bit length

As data is of variable length and AES algorithm handles 128-bit data, so when data length is not a multiple of 128, it encrypts 128-bit data at a time and for the remaining bits, if it is not 128-bit then move data pointer backwards so that data will be have 128-bits. Hence new and old data is combined to complete the frame of 128-bits where the combined data gets double encrypted, which results in increase in complexity at the time of decryption.

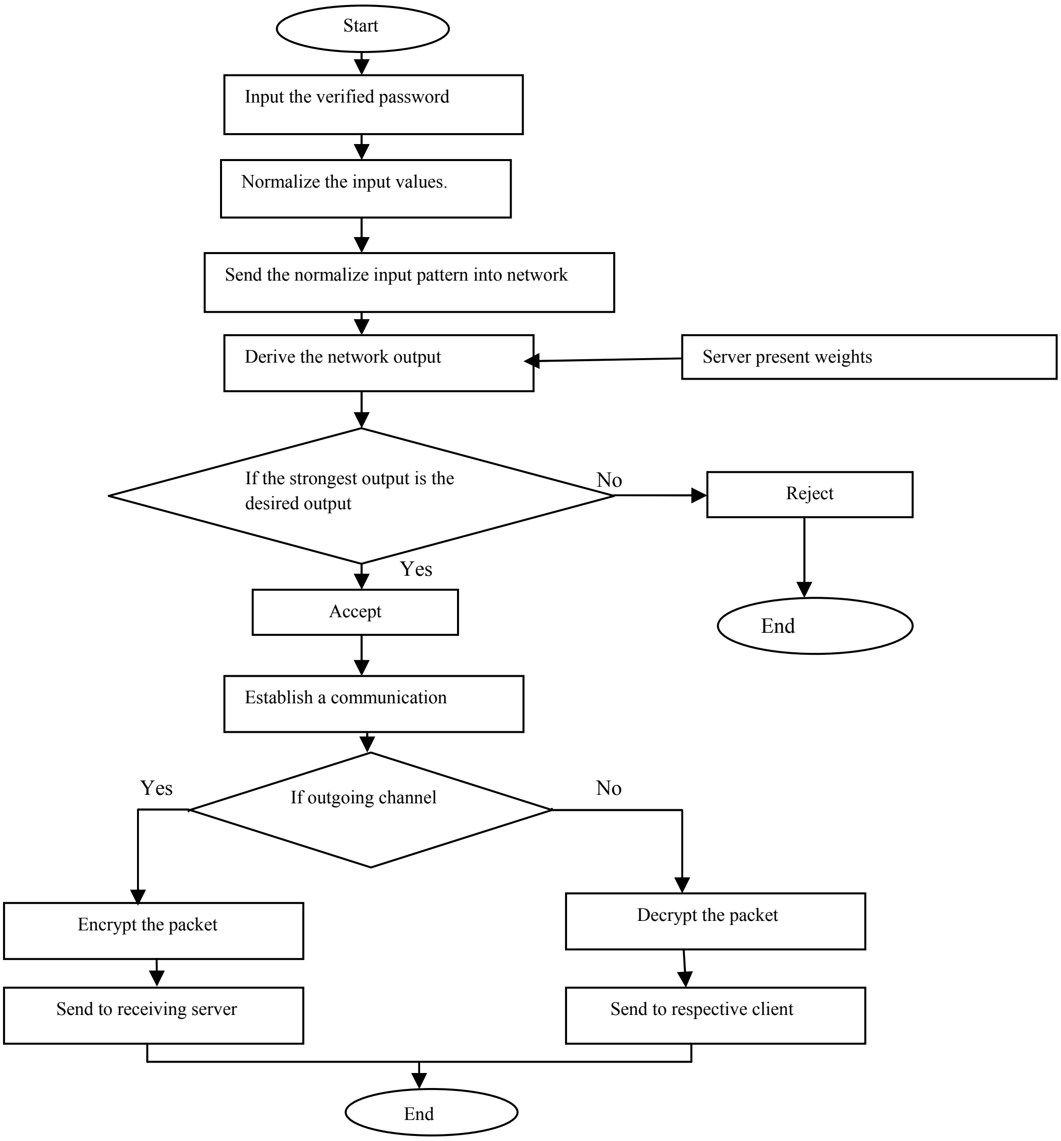
Start
Input the verified password
Normalize the input values.
Send the normalize input pattern into network
Derive the network output
Server present weights
If the strongest output is the desired output
No
Reject
End
Yes
Accept
Establish a communication
Yes
If outgoing channel
No
Encrypt the packet
Decrypt the packet
Send to receiving server
Send to respective client
End

Fig. 2 Overall working of the system

2.Security Analysis

- **Non-Forgability**

Assume that an intruder wants to forge a legal user password to login to asterisk server. The intruder forges a pair (ID, PW) and a timestamp T. However, if (4) does not hold, the server will reject the login request. A legal user wants to access a non-serviceable server. The user delivers the correct ID and PW, but delivers an incorrect value v. The server can resist the attack using the neural network. The server can check if v is equal to the binary number of the classification output.

- **Integrity of Messages**

Ethereal is packet capturing tool, which was used to capture data packets between sender server and receiving server. But data packets were not in audible format.

3. Conclusion

In this paper, we combine two methods for securing VoIP calls, one method is a remote password authentication scheme based on a neural network. In this scheme, the server does not store or maintain password or verification table. The server only stores the weights of the classification network. According to this network, the server can authenticate the validity of the user in real time. And another method is a use of AES algorithm for encrypting and decrypting voice packets. The main advantage of this scheme is that the system users can freely choose their password and the servers are required to retain only the pair user ID and password. The intruder cannot obtain a login password through the open network and replay the password to login to a server and integrity of messages is provided using AES algorithm by encrypting and decrypting data packets.

4. References

[1]. Chris Roberts, “Voice Over IP”, March 2005

[2]. Liancheng Shan, Ning Jiang “Research on security Mechanism of SIP-based VoIP system” Ninth International Conference on Hybrid Intelligent Systems, 2009.

[3]. Paul Mahler, “VoIP Telephony with Asterisk”, Signate, July 2004. (ISBN-10: 0975999206).

[4]. D Gomillion, B Dempster, “Building Telephony Systems with Asterisk”, Packt Publishing, September 2005. (ISBN-10 : 1904811159)

[5]. T. J. Hwang, “Password authentication using public-key encryption,” in Proc. IEEE Int. Carnahan Conf. Security Technol., 1983, pp. 141–144.

[6]. T. C. Wu and H. S. Sung, “Authentication passwords over an insecure channel,” Comput. Security, vol. 15, no. 5, pp. 431–439, 1996.

[7]. Li-Hua Li, Iuon-Chand and Min-Shiang Hwang “A remote password authentication scheme for multiserver architecture using neural network” IEEE transactions on neural networks, vol.12.No.6, November 2001.

[8]. Daemen, J. and Rijmen, V. “Rijndael: The Advanced Encryptiom Standard” Dr. Dobb’s journal, March 2001

[9]. Nathan J Muller “Wireless A-Z” McGraw-Hill (ISBN-10:071410880).

[10]. Yuebin Bai, Syed Aminullah “Towards a Distributed Wireless VoIP Infrastructure” International journal of multimedia and Ubiquitous Engineering, Vol. 2, No. 2, July, 2007.