Secure Authentication Protocol for Distant Access

Petar Ts. Antonov[1] and Valentina R. Antonova[2]

***Abstract* – In this report we propose a secure dialogue authentication protocol with passwords, under which password images can be preserved on the server, and every distant access is carried out by different key-word, transmitted through the channels in type.**

***Keywords* – Authentication protocol, cryptographic algorithms with public key.**

I. INTRODUCTION

As well known, the measures for authentication aim at provision of sufficiently secure procedures to establish the legality of the access to the resources. The users are legalized by introducing some authentic information, intended for the protection scheme of the respective resource. In the capacity of authentication information passwords are used most often. At the same time, the majority of attempts for illegal access to the resources are aimed at theft and destruction of precisely these passwords [1, etc.]. This imposes serious approach to the choice of the passwords themselves as well as to the development of specific protocols for authentication.

II. SECURE AUTHENTICATION PROTOCOL

For determination we consider information – communication system, including server and distant clients, using for connection some kind of WAN-technology. The server must operate the orders of many clients that have legal registration and reject the attempts for illegal access.

To the server S is assigned a pair of public K_{PS} and secret K_{SS} keys, in accordance with some of the known and secure asymmetric cryptographic algorithms (cryptographic algorithms with public key). This applies to every legal client X, who must also have available his own public K_{PX} and secret K_{SX} keys.

The public keys of the registered clients are preserved on the server in the first row of a two-row authentication matrix, whose second row is empty at fist (the file with these keys is not necessary to be protected as the keys themselves are accessible).

Using the mentioned above, the procedure of the considered protocol for authentication can be described in the following way [2]:

1. Client X establishes communication with the server S and originally legitimizes himself by his own public key K_{PX}.
2. The server S finds the field with K_{PX} in the first row of its authentication matrix and in the corresponding field in the second row of the same column of the matrix writes down generated by it accidental binary word T_X, that is to be used as password and is unique for each new séance for authentication of client X.
3. The server ciphers T_X with the public key K_{PX} of X, i.e. $E = F_E (T_X, K_{PX})$ and sends the cipher message E to X.
4. The client X deciphers the received cipher message E with his own secret key and restores T_X from the correlation $F_D(E, K_{SX}) = T_X$.
5. Further X ciphers T_X with the known public key K_{PS} of the server and sends to it the cipher message $E^* = F_E (T_X, K_{PS})$, together with the key K_{PX}.
6. The server deciphers E* with its own secret key, i.e. $F_D(E^*, K_{SS}) = T_X$, whereupon it compares the calculated value of T_X with the one, initially written down in step 2 and at coincidence it deletes T_X from the matrix and allows the access, and at lack of coincidence – deletes T_X and breaks off the connection.

The clients and the server can use only one asymmetric cryptographic algorithm, but it is possible that separate clients work with different algorithms of that kind. In the last case, in the authentication matrix of the server should be kept also information about the type of the asymmetric algorithm of every registered client, and on the server itself should be juxtaposed corresponding pair of public and secret keys for every algorithm used. At his original registration the client should choose one of the asymmetric algorithms that the server offers, whereupon he should generate his own pair of keys and submit his public key to the server.

In this case, the generated by the server accidental words T_X are preserved only for the time of the procedure for authentication. As this time is very short, then for T_X the danger of being revealed and meanwhile used for illegal access by an eventual offender is very little, too. But for still greater security, the words T_X can be preserved in ciphered type with the help of some known symmetric cryptographic algorithm, like DES, for example. In this situation, it is not necessary for the length of T_X to be greater than 64 bits, as ciphering and deciphering with DES is fulfilled upon binary blocks of that size. But because of the short time of existence of the words T_X, the ciphering can be done with weaker, but quicker algorithm than DES, whereupon the length of T_X will be decreased. This will lead to increase in productivity without considerable offence in security.

The main advantages of the authentication protocol, stated above, come to the following:

- No secret information about the client is preserved constantly on the server, but only their popular public keys.

[1]Peter Ts. Antonov is with the Department of Computer Science and Engineering, Technical University of Varna, 1, Studentska Str., 9010 Varna, Bulgaria, E-mail: peter.antonov@ieee.org

[2]Valentina R. Antonova is with the Department of Computer Science and Engineering, Technical University of Varna, 1, Studentska Str., 9010 Varna, Bulgaria,E-mail:valyvarna@yahoo.com

- New clients are registered simply, only by their public keys.
- The procedure is dialogue and at every new attempt for access different accidental word T_X is exchanged, which means that the offender can not use a heard and recorded legal current séance for establishing a connection and getting afterwards illegal access.
- During the time of dialogue through the communication channels only the open public key of the client is transmitted and the generated by the server accidental word T_X, which is in ciphered by the server or the client type, can not be deciphered by eventual offender.
- The accidental words T_X, used for passwords, are preserved by the server for a very short interval of time, which brings to minimum the danger of being caught.
- There could be additionally provided in the protocol periodic control of the access during legally established séances of connection and at every new control will be generated a new value of T_X.
- Modification is possible, introducing interruption of initially established connection and second invitation by the client or reverse invitation by the user.
- In essence the protocol represents a complete authentication scheme as it includes also the method for generation and preservation of passwords themselves.

Bellow we propose and give convincing argumentation on an effective variety of the authentication protocol considered, where the use of cryptographic algorithms with public keys is avoided, and the operations ciphering and deciphering are replaced by operations in modular arithmetic.

To the server is juxtaposed a sufficiently large prime number Q and an accidentally chosen number K in the interval [0, Q-1]. The number Q is known to all of the clients, and K is going to be used as a secret key of the server. A client X chooses two accidental numbers A and B in the same interval [0, Q-1]. The number A will perform the role of identifier of the client X, and B – his password for access.

The client calculates $H=A^B \text{mod} Q$ and registers himself in the server with the pair A and H. The server maintains a 3-row authentication matrix with number of columns equal to the number of clients registered. In the first field of the column for client X stays the number A, in the second field - $D=H^K \text{mod} Q$, and the third field remains empty.

At every attempt of client X to obtain access to resources of the server the following successive steps of the protocol will be realized:

1. X establishes communication with the server and inputs his own identification number A.
2. The server generates an accidental number T in the interval [0, Q-1], writes down this number in the empty field of the column for X in the authentication matrix and calculates $C=(A^K \text{mod} Q)^T \text{mod} Q$, whereupon sends C to the client.
3. The client calculates $F=C^B \text{mod} Q$ and returns to the server the pair A and F.
4. On receiving A and F, the server calculates $F^*=D^T \text{mod} Q$, compares F and F* and if F=F*, permits the access.

The veracity of final assertion of step 4 is based on the fact, that:

$$F = \left(\left(A^K \bmod Q\right)^T \bmod Q\right)^B \bmod Q \quad \text{and} \tag{1}$$

$$F^* = \left(\left(A^B \bmod Q\right)^K \bmod Q\right)^T \bmod Q, \tag{2}$$

so the equation F=F* can be proved easily using the known in modular arithmetic correlation

$$XY \bmod Z = \left(X \bmod Z . Y \bmod Z\right) \bmod Z . \tag{3}$$

The scheme of realization of the presented authentication protocol is shown visually in fig. 1, where the separate consecutive steps, fulfilled by the server and the client, are marked.

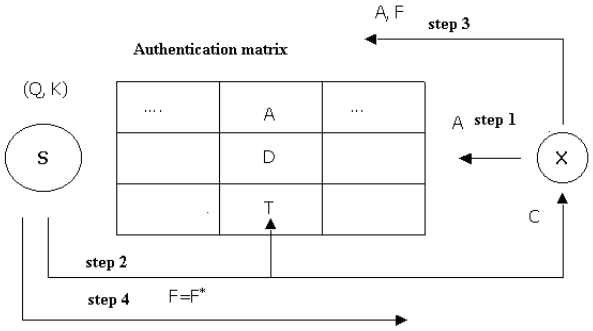

Fig. 1.

III. Conclusion

It can be seen that with this procedure in the authentication matrix of the server are not preserved any passwords, but their images, calculated on the basis of clients' identifiers, the actual passwords and the secret key of the server. Besides, during the dialogue different numbers are exchanged, depending on the numbers T, which are accidentally generated for every new attempt for access. In this way the security of the authentication protocol is guaranteed against evil-minded access to the authentication matrix as well as against eventual hearing by an offender in the communication channel.

References

[1] Кландер, Л. *Защита от хакери и най-добрите хакерски трикове и техники*, Прев. от англ. – София, СофтПрес-ООД, 1999.

[2] Антонов, П. Ц., В. Р. Антонова. "Протокол за защитено използване на пароли", ТЕЛЕКОМ'1999, Сб. докласди, Варна, България, 1999.

[3] Антонов, П. Ц., С. В. Малчев, *Криптография в компютърните комуникации*, Варна, 2000.

[4] Schneier, B. *Applied Cryptography. Protocols, Algorithms and Source Code in C*, John Wiley & Sons Inc., 1996.