ISSN:3030-3621

IDENTIFICATION AND AUTHENTICATION

Orzikul Shukurov
Tashkent University of Information Technologies
named after Muhammad Al-Xorazmiy,

Annotation: *One of the most common authentication schemes is simple authentication, which is based on the use of traditional multi-factor passwords. The procedure for simple authentication of a user on a network can be imagined as follows. A user trying to use the network types his or her ID and password on a computer keyboard.*

Key words*: network, DES algorithm, authentication, time synchronization, one-time password-based authentication, Security.*

A matching record is found in the database for the user ID stored on the authentication server, the password is found and compared with the password entered by the user. If they match, authentication is considered successful and the user receives the legal (legal) status and the rights defined for his status through the authorization system and permission to use network resources.

A simple authentication scheme using a password is shown in Figure 1. Obviously, the authentication option by transmitting the user's password without encryption does not guarantee even a minimal level of security. To protect the password, it is necessary to encrypt it before transmitting it over an unprotected channel. For this, the scheme includes encryption E_k and decryption D_k tools. These tools are controlled by a shared secret key K. User authentication is based on comparing the password P_A sent by the user with the initial value P_A stored on the authentication server. If the values P_A and P_A match, the password P_A is considered valid, and the user A is considered legitimate. Authentication server

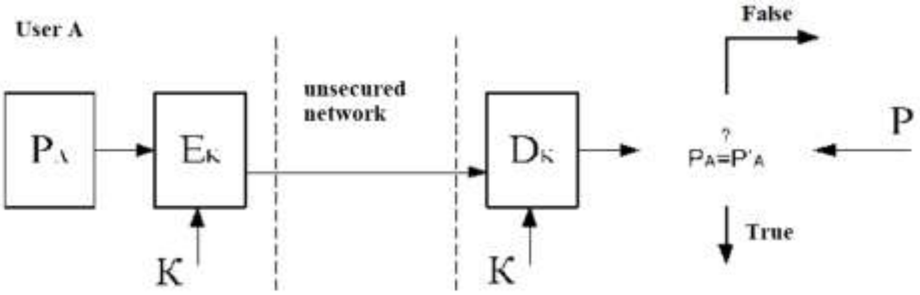

Figure 1. Simple authentication using a password.

Simple authentication schemes are distinguished not only by the transmission of passwords, but also by the types of their storage and verification. The most common method is the method of storing user passwords in system files, in the open state. In this case, read and write protection attributes are set for the files (for example, by specifying the appropriate privileges in the operating system access control list). The system compares the password entered by the user with the record stored in the password file. This method does not use cryptographic mechanisms such as encryption or one-way functions. The disadvantage of this method is the possibility of an attacker with administrator privileges in the system, as well as system files, including password files. From a security point of view, it is convenient to transmit and store passwords using one-way functions. In this case, instead of the open form of the password, the user must send its image, obtained using the one-way function h(.). This modification guarantees that the adversary cannot reveal the password through its image, since the adversary faces an insoluble numerical problem.

Simple authentication systems based on multi-factor passwords have low resilience, since the authentication information in them is collected from a relatively small set of meaningful words. The validity period of multi-factor passwords should be determined by the organization's security policy, and such passwords should be changed regularly. Passwords should be chosen so that they are not in the dictionary and are difficult to guess. In authentication based on one-time passwords, different passwords are used for each request. A dynamic one-time password is only valid for one use in the system. Even if someone intercepts it, the password is useless. Typically, an authentication system based on one-time passwords is used to verify remote users. One-time password generation can be implemented using hardware or software. Hardware devices based on one-time passwords are miniature devices with a microprocessor installed on the outside, similar to payment plastic cards. Such cards, usually called keys, have a keyboard and a small display window.

The following methods of using one-time passwords for user authentication are known:

1. Using a timestamp mechanism based on a uniform time system.

2. Using a list of random passwords common to the legal user and the verifier and a reliable synchronization mechanism for them.

3. Using a pseudorandom number generator with the same initial value common to the user and the verifier.

An example of the first method is the SecurID authentication technology. This technology was developed by SecurityDynamics and is implemented on the servers of a number of companies, in particular, CiscoSystems. The authentication scheme using time synchronization is based on an algorithm for generating random numbers after a certain time interval. The authentication scheme uses the following two parameters: a secret key, which is a unique 64-bit number assigned to each user and stored on the authentication server and on the user's hardware key; the current time value. When a remote user tries to use the network, he is prompted to enter a personal identification number (PIN). The PIN consists of four decimal digits and a six-digit random number displayed on the hardware key display. The server uses the PIN entered by the user to perform a random number generation algorithm based on the user's secret key in the database and the current time value. Then the server compares the generated number with the number entered by the user.

If these numbers match, the server allows the user to use the system.

This authentication scheme requires strict time synchronization of the hardware key and

the server. Since the hardware key can operate for several years, and therefore the compatibility of the server's internal clock with the hardware key can gradually deteriorate.

To solve this problem, Security Dynamics uses the following two methods:

• When developing a hardware key, its deviation from the norm of the timer frequency

is precisely measured. This deviation value is taken into account as a parameter of the server algorithm;

• The server monitors the codes generated by a particular hardware key and

adapts to this key when necessary.

Another problem is associated with this authentication scheme. The random number generated by the hardware key is considered a valid password for a short period of time. Therefore, in general, a short-term situation may occur when a hacker can intercept the PIN code and use it to access the network. This is the weakest point of the authentication scheme based on time synchronization.

Another option for authentication using a one-time password is authentication using the “challenge-response” scheme.

When a user tries to use the network, the server sends him a request in the form of a random number. The user’s hardware key decrypts this random number using, for example, the DES algorithm and the user’s private key stored in the memory of the hardware key and in the server’s database. The random number - the request - is returned to the server in encrypted form. The server, in turn, encrypts the random number it generated using the same DES algorithm and the user’s private key obtained from the server’s database. Then the server compares the encryption result with the number from the hardware key. If these numbers match, the user is allowed to use the network. It should be noted that the “challenge-response” authentication scheme is more complicated to use than the authentication scheme using time synchronization.

The second method of using one-time passwords for user authentication is based on the use of a list of random passwords common to the user and the verifier and a reliable synchronization mechanism for them. The partitioned list of one-time passwords is a sequence or string of secret passwords, each password is used only once.

This list must be distributed in advance between the parties to the authentication exchange. According to one variant of this method, a challenge-response table is used. This table contains the requests and responses used by the parties for authentication, and each pair must be used only once.

The third method of using a one-time password for user authentication is based on the use of a pseudo-random number generator with the same initial value, common to the user and the verifier. There are the following implementation options for this method:

• a sequence of changing one-time passwords. In the next authentication session, the user creates and transmits a password encrypted with the secret key obtained from the password of the previous session for this session;

• a sequence of passwords based on a one-way function. The essence of this method is the sequential use of a one-way function (the famous Lampart scheme). From a security point of view, this method is preferable to the method of sequentially changing passwords.

One of the most common one-time password-based authentication protocols is the S/Key (RFC1760) protocol, standardized on the Internet. This protocol is implemented in many systems that require remote user authentication, in particular, Cisco's TACACS+ system.

Literature

1. https://www.researchgate.net/publication/319536428_Identification_and_Authentication
2. Blessing, Moses & Olusegun, John. (2024). The Impact of Software-Defined Networking (SDN) on Traditional Network Architectures: Opportunities and Challenges.
3. Danish, Muhammad & Shahid, Shaheryar & Ghafar, Abdul & Hamid, Khalid & Ali, Noman & Ghani, Amarah & Ibrar, Muhammad & Mandan, Sikandar. (2025). Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN. 3. 18-36. 10.63075/wdpwrr31.