International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 39-47

Identification and Authentication

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Identification is the process of identifying a user by his or her identifier (name). This is the first function performed when a user tries to access a network. The user provides the system with its identifier upon request, and the system checks its presence in its database. Authentication is the process of verifying the authenticity of a reported user, process, or device. This verification allows the user (process or device) to be sure that it is real.*

Keywords: Identification, authentication, administration, authorization, masquerade, repetition, forced delay.

INTRODUCTION

1. Basic concepts and classification

2. Password-based authentication

3. Biometric identification and authentication of users

Basic concepts and classification

Identification is the process of identifying a user by his or her ID. This is the first function performed when a user tries to access a network. The user provides the system with its identifier upon request, and the system checks its presence in its database.

Authentication is the process of verifying the authenticity of a reported user, process, or device. This verification allows the user (process or device) to be sure that it is real. In the process of authentication, the examining party makes sure that the audited party is genuine, and the audited party is actively involved in the exchange of information. Typically, a user verifies their identity by entering unique, unknown information about themselves (such as a password or certificate).

Identification and authentication are interrelated processes of identifying and verifying the authenticity of subjects (users). It is up to the system to allow a particular user or process to use system resources. After identifying and authenticating the subject, authorization will begin.

Authorization is the process of giving a subject certain authority and resources in the system, that is, authorization defines the scope of the subject's actions and the resources it uses. If the system cannot reliably distinguish an authorized person from an unauthorized person, the confidentiality and integrity of the information in that system may be compromised. Authentication and authorization procedures are inextricably linked to user traffic management procedures.

Accounting is the act of recording a user's actions on a network, including his or her attempts to use resources. From the security point of view, the information in this report is very important for the disclosure, analysis and appropriate response to security incidents in the network.

The protection of data transmission channels requires the mutual authentication of the subjects, ie the mutual confirmation of the authenticity of the subjects connected through communication channels. Authentication is usually done at the beginning of the session, during the connection of subscribers. The term "connect" refers to a logical connection between two entities in a network. The purpose of this procedure is to ensure that the connection is made with the legal entity and that all information reaches the intended destination.

METHODS

An entity may present various grounds to the system to substantiate its authenticity. Depending on the grounds on which the subject provides, the authentication process can be divided into the following categories:

- on the basis of knowing something. Examples include passwords, PINs (Personal Identification Numbers), and secret and public keys displayed in "question and answer" protocols;

- on the basis of ownership of something. Typically, these are magnetic cards, smart cards, certificates, and touch memory devices;

- on the basis of some inviolable characteristics. This category includes methods based on the user's biometric characteristics (voices, retina and retina, fingerprints, palm geometry, etc.). Cryptographic methods and tools are not used in this category. Beometric characteristics are used to control the use of a building or any technique.

A password is something that the user and his partner in the exchange of information know. Passwords can be exchanged between the user and his partner for mutual authentication. In the authentication of a plastic card and smart card holder, the personal identification number PIN is a tried and tested method. The secret value of the PIN code is only the card e must be known.

Dynamic - (one-time) password - a password that is not used at all after one use. In practice, a constant variable value based on a permanent password or base phrase is usually used.

Inquiry system - one of the parties initiates authentication by sending a unique and unpredictable "request" value to the other party, and the other party sends a response calculated using a query and a secret. Since both parties have the same secret, the first party can verify the answer of the other party.

Certificates and digital signatures - If certificates are used for authentication, the use of a digital signature on these certificates is required. Certificates are issued by the responsible person of the user organization, the certificate server or an external trust organization. A number of public key management infrastructure PKIs (Public Key Infrastructures) have emerged to distribute public key certificates over the Internet. Users can get different level certificates.

Authentication processes can also be categorized according to the level of security provided. According to this approach, authentication processes are divided into the following types:

- authentication using passwords and digital certificates;

- Strict authentication based on cryptographic methods and tools;

- authentication processes (protocols) with the ability to prove with zero knowledge;

- biometric user authentication.

From a security point of view, each of the above allows you to solve specific problems. Therefore, authentication processes and protocols are actively used in practice. At the same time, it should be noted that the interest in authentication, which has the property of proving with zero knowledge, is more theoretical than practical. Perhaps in the near future they can be actively used to protect the exchange of information.

The main attacks on authentication protocols are:

- masquerade (impersonation). By attempting to present himself as another person, the user intends to have the opportunity and privilege of action by that person;

- interleaving attack. A person with a malicious intent participates in the process of authentication exchange between the two parties during this attack with the intention of modifying the traffic. There are two types of substitutions: two

once the authentication between the users is successful and the connection is established, the intruder will remove one of the users and continue working on his behalf;

- replay attack. Authentication information is repeated by one of the users;

- reflection attak. One of the options of the previous attack is that during the attack, the intruder returns the information that was intercepted during this session of the protocol.

- forced delay. A person with bad intentions will catch some information and pass it on after a while.

- chosen text attack. A malicious person tries to capture information about long-term cryptographic keys by intercepting authentication traffic.

The following methods are used to build authentication protocols to prevent the above attacks:

- use of mechanisms such as "question and answer", time stamps, random numbers, identifiers, digital signatures;

- link the authentication result to the next actions of users within the system. An example of such an approach would be the exchange of secret session keys used during subsequent authentication of users during the authentication process;

- Periodically perform authentication procedures within the established communication session, etc.

The question-and-answer mechanism is as follows. If user A wants to make sure that the message he receives from user B is not false, he adds an unpredictable element - a query X (for example, some random number) - to the message sent by user V. User V must perform a specific operation (for example, calculating a function f (X)) on this operation in response. This cannot be done in advance because user V does not know what random number X will appear in the query. User A, who receives the result of user V action, can be sure that user V is real. The disadvantage of this method is that it is possible to determine the pattern between the request and the answer.

Password-based authentication

One of the most common authentication schemes is simple authentication, which is based on the use of traditional multiple passwords. Network A simple user authentication procedure can be imagined as follows. When a user tries to use the network, he types his ID and password on the computer keyboard. This information is sent to the authentication server for processing. A reference is found in the database for the user ID stored on the authentication server, from which the password is found and compared with the password entered by the user. If they comply, the authentication is considered successful and the user receives legal status and access to the rights and network resources defined for his status through the authorization system.

A simple authentication scheme using a password is shown in Figure 1.

Obviously, the authentication option by transferring 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 through an unprotected channel. To do this, the circuit includes encryption Single and decryption Dk tools.

Figure 22.1. Simple authentication using a password

These tools are controlled by a shared secret key K. User authentication

The password sent by the user is the first stored on the authentication server with the PA

value

If the A P values match, the password PA is real,

user A is legitimate.

Simple authentication organization schemes not only transfer passwords, but also store them and types of verification. The most common method is to store users' passwords in system files in an open state. This sets the read and write protection attributes for the files (for example, by describing the appropriate privileges in the operating system usage checklist). 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 that the intruder has access to system privileges, as well as system files, including password files.

Simple authentication systems based on multiple passwords have low tolerance,

because they did not have a relatively large number of authentic words

from the collection. The expiration date of multiple passwords is in the organization's security policy and such passwords should be changed regularly. Passwords are like that choose them so that they are not in the dictionary and are difficult to find.

For each request to use authentication based on one-time passwords

different passwords are used. A one-time dynamic password is only valid for one-time use of the system.

If, even if someone catches it, the password doesn't work. Usually one-time passwords based authentication system is used to verify remote users.

The generation of one-time passwords can be done by hardware or software method possible. Disposable passwords are plastic payment devices

implemented in the form of miniature devices with a microprocessor similar to the cards increases. These cards, commonly referred to as keys, have a keyboard and a small display has a window.

Here's how to use one-time passwords to authenticate users

known methods:

1. Use a time stamp mechanism based on a single time system.

2. Random passwords that are common to both the legal user and the checker

list and use their reliable synchronization mechanism.

3. Use a pseudo-random number generator with the same initial value that is common to both the user and the controller.

An example of the first method is SecurID authentication technology. The technology was developed by Security Dynamics and implemented on the servers of a number of companies, including Cisco Systems.

The authentication scheme using time synchronization is based on an algorithm that generates random numbers after a certain period of time. The authentication scheme uses the following two parameters:

• A unique 64-bit secret key assigned to each user and stored on the authentication server as well as the user's hardware key;

• Current time value.

When a remote user tries to use the network, he is prompted to enter his personal identification number and PIN. The PIN consists of four decimal digits and six digits of a random number displayed on the hardware key display. The server uses the PIN entered by the user to access the data executes a random number generation algorithm based on the user's secret key and the current time value. The server then compares the generated number with the number entered by the user. If these numbers match, the server allows the user to use the system.

Using this authentication scheme requires strict time synchronization of the hardware key and the server. This is because the hardware switch will work for several years and therefore the compatibility of the hardware key with the server's internal clock may gradually deteriorate.

Security Dynamics uses the following two methods to solve this problem:

• When a device switch is developed, its deviation from the timer frequency is accurately measured. This value of the deviation is taken into account as a parameter of the server algorithm;

• The server monitors the code generated by a particular hardware key and adapts to that key as needed.

There is something wrong with this authentication scheme. The device is a real password for a small period of time generated by a random number of keys. Therefore, in general, there may be a short-term situation where 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.

Biometric identification and authentication of users

Recently, biometric authentication has become widespread, allowing reliable user authentication by measuring a person's physiological parameters and characteristics, as well as behavioral characteristics.

Biometric authentication methods have the following advantages over traditional methods:

- high level of authentication reliability due to the rarity of biometric features;

- inseparability of biometric signs from a healthy person;

- Difficulty of falsification of biometric signs.

The biometric algorithms that are actively used in user authentication are:

• fingerprints;

• Geometric shape of the hand claw;

• The shape and size of the face;

• Voice features;

• Patterns of the bow and retina.

From the consumer's point of view, the biometric authentication system is characterized by the following two parameters:

• R Error-rejection rate FRR (false-reject rate);

• Fal (alarm rate) FAR (false-alarm rate).

An error denial occurs when the system does not verify the identity of a legitimate user (usually a FRR value of about 100). Error confirmation occurs when the system verifies the identity of an illegal user (typically the FAP value is about one in 10,000). These two coefficients are related to each other: each of the error negation coefficients corresponds to a certain error confirmation coefficient. In a perfect biometric system, both error parameters must be zero. Unfortunately, the biometric system is not ideal, so you have to sacrifice something. Typically, the structural parameters are adjusted so that the desired coefficient of error assertions, which determines the corresponding error negation coefficient, is achieved.

Dactylosonic system of biometric authentication

Most biometric systems use fingerprints as an identification parameter (fingerprint authentication system). Such systems are simple and convenient, with high reliability of authentication. The main reason for the prevalence of such systems is the availability of a large database of fingerprints. Such systems are mainly used by the police, various government agencies and some banking institutions around the world.

The dactyloscopic system of authentication works as follows. The user is registered first. Typically, the scanner performs several variants of scanning in different positions of the finger. Naturally, the samples differ slightly from each other, and some kind of generalized sample, a "passport" is required. The results are stored in the authentication database. During authentication, the scanned fingerprint is compared to the "passports" in the database.

Fingerprint scanners. Traditional fingerprint scanners use a small optical camera that captures a characteristic image of the finger as a key element. However, most dactyloscopic device manufacturers are focusing on integrated circuit-based sensor devices. This trend opens up new areas of application based on fingerprint authentication.

Companies that develop such technologies use a variety of tools to obtain fingerprints, including electrical, electromagnetic, and other methods.

One scanner measures the capacitance of parts of the skin to create a fingerprint image. For example, Veridicom's dactyloscopic The device collects information by determining the capacitance using a semiconductor sensor. The principle of operation of the sensor is as follows: the finger inserted into this device acts as one of the capacitor plates (Figure 2). The second plate on the surface of the sensor consists of a 90,000 sensitive plate silicon chip of the capacitor. Sensitive capacitance sensors measure the

change in electric field strength between the ridges and bumps of the finger surface. As a result, the distance to the ridges and depressions is determined and fingerprints are taken.

Figure 22.2. The principle of sensor operation

The method used at AuthenTec in touch control based on integrated circuits allows to further increase the accuracy.

A number of manufacturers combine biometric systems with smart cards and card-keys.

The small size and low cost of integrated circuit fingerprint sensors make them an ideal interface for a security system. They can be mounted on keychains. As a result, the user will have a universal key that provides secure access from the computer to the entrance, the doors of cars and ATMs.

Geometric authentication systems. Claw shape readers create a three-dimensional image of the claw by measuring the length of the fingers, the thickness and the surface of the claw. For example, Recognition Systems products come in more than 90 sizes. The result is a 9-digit sample for further comparison. This result can be stored on an individual fingerprint scanner or in a centralized database. Although handheld scanners are seldom used in a network environment due to their high cost and size, they are suitable for computing environments (including server rooms) with strict security modes and heavy traffic. They have high accuracy and a negation rate, which means a small percentage of denied legitimate users.

Facial structure and voice authentication systems.

These systems are the most user-friendly due to their low cost, as most modern computers have video and audio tools. Systems of this class are used in telecommunication networks to identify a remote user entity. Facial scanning technology is suitable for applications where other biometric technologies are not available. In this case, eye, nose and lip features are used to identify and verify the person. Manufacturers of facial structure detection devices use special mathematical algorithms to identify the user.

It turns out that many organizations do not trust facial scanners. They think the camera takes a picture of them and then displays it on a monitor screen. The quality of the camera may be poor. In addition, facial structure scanning is the only biometric authentication method that does not require verification (can be done using a hidden camera).

It should be noted that the technology of determining the structure of the face requires further improvement. Most facial structure algorithms are sensitive to changes in light as a result of the vibrations of the sun's intensity during the day. Changes in facial expressions also affect the test result. A change in facial position of 450 makes the detection ineffective.

Voice authentication systems

These systems are user friendly due to their low cost. In particular, they can be installed with most standard PCs (such as microphones). Voice authentication systems are based on voice characteristics such as pitch, modulation, and frequency, which are unique to each person. Voice recognition is different from speech recognition. Because speech recognition technology interprets a subscriber's word, voice recognition technology identifies the speaker. There are some restrictions on the identity of the speaker. Different people can speak with similar voices, and each person's voice can change over time depending on their mood, emotional state, and age. In addition, the variety of telephones and the quality of telephone communications make it difficult to identify the speaker. Therefore, it is advisable to use voice detection in conjunction with other biometrics, such as facial expressions or fingerprints.

Authenticity of the retina by the shape of the retina

These systems can be divided into two classes:

- use of eye drops;

- The retina the use of a picture of the vascular bed of the curtain.

The human eyelid is a unique object for authentication. The picture of the blood vessels at the base of the eye is different even in twins. These means of identification are used when a high level of security is required (for example, in the regime zones of military and defense facilities).

The biometric approach simplifies the process of determining who is who. The use of dactyloscopic scanners and voice recognition devices saves employees from remembering complex passwords when accessing the network. A number of companies are integrating biometric capabilities into an enterprise-wide one-time authentication SSO (Single Sign-On). This connection allows network administrators to replace one-time password authentication with biometric technology. One of the first and most common areas of biometric authentication was mobile. The problem is not only computer theft losses, but also information system crashes that can cause great damage. In addition, laptops often use the corporate network through software connections (using passwords stored on mobile computers). Fingerprint sensors that solve these problems are small, inexpensive, and do not require large amounts of energy. These devices allow you to perform four stages of access to information stored on a mobile computer using the appropriate software - registration, exit screen saver, download and authenticate to decrypt files.

User biometric authentication can play an important role in encrypting the use of a private key in the form of a module. This module allows information to be used only by the real private key owner. The key owner can then use his private key to encrypt the information transmitted over private networks or the Internet.

RESULTS

A number of manufacturers combine biometric systems with smart cards and card-keys.

The small size and low cost of integrated circuit fingerprint sensors make them an ideal interface for a security system. They can be mounted on keychains. As a result, the user will have a universal key that provides secure access from the computer to the entrance, the doors of cars and ATMs.

Geometric authentication systems. Claw shape readers create a three-dimensional image of the claw by measuring the length of the fingers, the thickness and the surface of the claw. For example, Recognition Systems products come in more than 90 sizes. The result is a 9-digit sample for further comparison. This result can be stored on an individual fingerprint scanner or in a centralized database. Although handheld scanners are seldom used in a network environment due to their high cost and size, they are suitable for computing environments (including server rooms) with strict security modes and heavy traffic. They have high accuracy and a negation rate, which means a small percentage of denied legitimate users.

Facial structure and voice authentication systems.

These systems are the most user-friendly due to their low cost, as most modern computers have video and audio tools. Systems of this class are used in telecommunication networks to identify a remote user entity. Facial scanning technology is suitable for applications where other biometric technologies are not available. In this case, eye, nose and lip features are used to identify and verify the person. Manufacturers of facial structure detection devices use special mathematical algorithms to identify the user.

It turns out that many organizations do not trust facial scanners. They think the camera takes a picture of them and then displays it on a monitor screen. The quality of the camera may be poor. In addition, facial structure scanning is the only biometric authentication method that does not require verification (can be done using a hidden camera).

It should be noted that the technology of determining the structure of the face requires further improvement. Most facial structure algorithms are sensitive to changes in light as a result of the vibrations of the sun's intensity during the day. Changes in facial expressions also affect the test result. A change in facial position of 450 makes the detection ineffective.

DISCUSSION

The question-and-answer mechanism is as follows. If user A wants to make sure that the message he receives from user B is not false, he adds an unpredictable element - a query X (for example, some random number) - to the message sent by user V. User V must perform a specific operation (for example, calculating a function f (X)) on this operation in response. This cannot be done in advance because user V does not know what random number X will appear in the query. User A, who receives the result of user V action, can be sure that user V is real. The disadvantage of this method is that it is possible to determine the pattern between the request and the answer.

Password-based authentication

One of the most common authentication schemes is simple authentication, which is based on the use of traditional multiple passwords. Network A simple user authentication procedure can be imagined as follows. When a user tries to use the network, he types his ID and password on the computer keyboard. This information is sent to the authentication server for processing. A reference is found in the database for the user ID stored on the authentication server, from which the password is found and compared with the password entered by the user. If they comply, the authentication is considered successful and the user receives legal status and access to the rights and network resources defined for his status through the authorization system.

A simple authentication scheme using a password is shown in Figure 1.

Obviously, the authentication option by transferring 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 through an unprotected channel. To do this, the circuit includes encryption Single and decryption Dk tools.

CONCLUSION

Identification and authentication are interrelated processes of identifying and verifying the authenticity of subjects (users). It is up to the system to allow a particular user or process to use system resources. After identifying and authenticating the subject, authorization will begin.

Authorization is the process of giving a subject certain authority and resources in the system, that is, authorization defines the scope of the subject's actions and the resources it uses. If the system cannot reliably distinguish an authorized person from an unauthorized person, the confidentiality and integrity of the information in that system may be compromised. Authentication and authorization procedures are inextricably linked to user traffic management procedures.

Accounting is the act of recording a user's actions on a network, including his or her attempts to use resources. From the security point of view, the information in this report is very important for the disclosure, analysis and appropriate response to security incidents in the network.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

7 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

8 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

9 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

10 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

11 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

12 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

13 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

14 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

15 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.