INSERTING INFORMATION SECURITY TO THE SYSTEM OF CONTINUING EDUCATION AND PROTECT DATA DURING THE PERIOD OF EDUCATION

ERKAYEV HUSAN AHMADALIYEVICH
Teacher of the Department of Information Technology of TSPU Tashkent city

ABSTRACT

This article discusses the concept of information security in the system of continuing education, discloses methods of information protection in pedagogical activity.

Keywords: Education, information technology, modern technology, computer games, communication, independent movement, speech culture, the Internet, electronic information, hash function, symmetric and asymmetric cipher algorithms cryptanalysis, cryptography, tolerance level, keys.

Nowadays, in the developing technologic world, all attention is paid for the protection of information; most people are getting aware of the importance of information protection. Whether one is a doctor, a teacher, a businessman or a lawyer, they all have their own secrets which should not be exposed. They are called ***service secrets.***

To be proved as information, a material should contain 3 characters:

- Data must be full;
- Data must be reliable;
- Data must be valuable.

If data have these points, they can be called information. By keeping and usage the information can be divided into two groups: open source and private source.

Open-source information can be obtained from mass-media or from internet, for instance, from sources which have not any barriers for the users to get the information. Private-source has its own users and can be defined by the risk of damage if they get revealed. They can be several types: government secrets, military secrets, secrets of scientific researches, service secrets.

As to be kept in the safety the information is protected. Methods of protection can be: physic protection, right protection, mechanic-apparatus protection, device-soft protection, cryptographic protection.

Today we have got all conditions to use these kinds of protections. For instance, the information can be kept in the safe and decrease the number of persons who has access to the information or to put it in strictly protected buildings. Although, these methods have advantages, they even have disadvantages which can be seen in the process of changing information. Above all, these means can be also be added to the list of information protection:

- To protect the channel where the information is sent
- Private-source information which is being sent in the open-source channel must be covered(mixed) with information (to use stenographic method).
- To send open source-information that holds private data in its origin.

But in the cryptography sending information is not seen a private data, it`s only modified that can be read only by cryptologist. Modern cryptology check out the features of the data given below:

- Privacy (provide with confidence)
- Completeness (define modified data)
- Authentication (define user`s verity)

- To provide with the confess of the copyright rules to both sides beforehand
- To provide creation, expansion and management of the keys.

Privacy – to provide with safety of the information from the sides who have no access to the data.

Completeness – provide with the guarantee that the information cannot be edited without the permission of the author.

Authentication – provide with the detailed data of the information changing sides.

To provide with the copyright rules to both sides beforehand – make subjects admit the action they have done recently.

Above we have viewed just few of the features and they are not the all we wanted to express, yet we have to conclude and end our article with the fact that the information protection is still remaining as a main issue of the rapidly developing world.

The first requirement is to oppose the creation of one key with counterfeit keys, and the second requirement is to counter the modification of transmitted data. Generally, the concept of authentication applies to all aspects of the data-driven processes. Examples: communication session, parties, data being transmitted, and more. Authentication for all parts of the data process is an important part of providing reliable data transmitted. This is especially true in the exchange of information between conflicting parties. Because it is not only the cryptocurrency that is the basis for the threat of information sharing, but also the wrong actions of both parties.

Authentication for a communication session means full connection, timely transfer of data, and prevention of repeated data transfer by a cryptographic analyst.

Additional parameters are used to provide authentication for the communication session. For example: the data to be transmitted is a cryptographic algorithm, including timestamps, random numbers, and serial numbers.

Interoperability Authentication - Verify that any party you want to interact with is actually sharing information with the other party. In most cases, the parties are also referred to as the parties 'authentication and respectively the parties' identification. This is a formal explanation, which means identification of the parties, usually the procedure for the identification of the parties to distinguish them from other users. In this case, the process of identifying these names is to display or give these names. Therefore, authentication can be called validation of authentication.

Description. The sequence of tasks assumed by two or more parties to solve a practical problem is called a protocol. The authentication tool is an authentication protocol that provides for the identification (authentication) of trustees.

Identity protocols are of two types:

• One-way authentication protocols.

• Mutual identification protocols.

As a result of the authentication protocol, both parties do not disclose their private key and answer each question (request).

Authentication of the data itself is true of the fact that the information transmitted over the communication network is true, that is, the accuracy of the data transmitted, the time of its preparation and the parameters of the judgment. If both parties trust each other, this can be done using an encryption algorithm with a public key.

However, if the parties express a lack of confidence in each other, then it is necessary to develop a mechanism for resolving the issue. This mechanism is called Digital Signature (EDS), and we will give some comments below.

From experience, it is clear that some people may deny that they have not done anything for their own purpose or behavior (for example, a document) for a long time. The only way to clarify such controversial issues is through digital signature.

Any standard digital signature algorithm available today consists of two parts:

1. Signature Counting section.

2. Signature verification section.

According to the EDS algorithm, only the data owner can sign the data with a private key. All users can check EDS authenticity.

Digital signature scheme: can be implemented using both symmetric and asymmetric encryption algorithms. In the digital signature scheme based on the symmetric encryption algorithm, the signature data is a secret encrypted form.

However, the disadvantage of this signature is that the private key is kept secret. This can cause a number of inconveniences, such as always having to choose a new key when signing and only using it once.

There are two types of digital signature generation using asymmetric encryption algorithms:

1. The information provided is fully encrypted with the owner's private key. The signator can verify the signature with the public key.

2. Signature counting is a digital transformation of signature data, and the signature counting algorithm depends on the private key.

This is why it is important that the signer be signed only by the owner and anyone can verify it. This is why the signature verification part is compiled by the owner's public key.

It should be noted that if the length of the signature in the first round is determined by the length of the given data, then in the second round, the length of the signature is determined regardless of the length of the data. When calculating digital signatures in relation to a given data, it is most convenient when the data is first calculated as a hash value and then the sequence of actions specified in the algorithm (EDS). The hash value is calculated using the hash function algorithms, respectively.

LIST OF REFERENCE

1. Moldavian A. A., Moldovyan - N. And. Restricting the use of tobacco products from primitives and it does not mean that in the body algorithm and statesman of the country. In Saint Petersburg "BHV-Petersburg» In 2014. 448 p.
2. Rostovtsev A. G., MakhovenkoOr. N., Theoretical restrictions on the use of tobacco products. NGO " Professional», In Saint Petersburg. In 2014. - 478 pages.
3. Strings V. "the restriction of the use of tobacco products and protection of networks. Principle and practice". Moscow - Saint Petersburg - Kiev. From them. bait «Williams». 2-or publication. 2017. – 669.
4. Schneider B. " Applied restriction of the use of tobacco products" Moscow " Publishing House TRIUMPH " in 2012 815 pages.

5. Comparison of the effect of multimedia and booklet methods on quality of life of kidney transplant patients: A randomized clinical trial study Mansouri P., Sayari R., Dehghani Z., Hosseini F.N. (2020) International Journal of Community Based Nursing and Midwifery, (1) , pp. 12-22.
6. ErkayevHusanAhmadaliyevich&PrimkulovaAlimaAsetovna, European Journal of Research and Reflection in Educational Sciences Vol. 7 No. 12, 2019 ISSN 2056-585