Improving the security level of the information system using the SSL protocol

Olga Purchina[1], *Anna* Poluyan[1], and *Dmitry* Fugarov[1*]

[1]Don State Technical University, Gagarin square 1, 344000 Rostov-on-Don, Russia

Abstract. An important role in the organization of production sites is played by the security of information for the process of planning the management of the production site. Information security is a very important component of any information system used on the production site. Improving the quality of information system security can be achieved only by a set of data protection measures. The results of the implementation of these measures should provide a clear picture of the information system used, about users, about the separation of powers, etc., which will allow making the right management decisions in the event of an intrusion into the system. Improving the security of information systems, taking into account modern requirements of information security policies, involves the development of data protection concepts and the introduction of the latest encryption methods into the information system. The paper presents the concept of building an information system using data encryption based on SSL encryption. SSL — Secure Socket Layer, the level of secure sockets. SSL encryption is characterized by the creation of a cipher with a public key. This allows you to authenticate the user and the server by resorting to digital signature technology. In addition, this is how the session key is generated to develop a fast symmetric cipher algorithm, which allows you to encrypt a large mass of information.

1 Introduction

An important role in the organization is played by the security of information in the production process. Improving the quality of information system security can be achieved only by a set of data protection measures. The result of the work of the information system should be a clear idea of the production, allowing to make management decisions, as well as to ensure the security of the transmitted information [1].

SSL or from English Secure Sockets Layer is a protocol in the field of cryptography, which should be understood as the most secure communication layer. It is used to verify the authenticity of the exchange key through asymmetric cryptography [2]. A symmetric cipher is also being created to ensure the confidentiality of information, data verification codes for the integrity of messages. This protocol has been widely used in the field of instant information exchange and for the transmission of voice messages via VoIP in e-mail [3].

* Corresponding author: ddf_1@mail.ru

This protocol protects the exchange of information through encryption and authentication. For the operation of the protocol, asymmetric cryptography is used, with the help of which the authenticity of the data exchange key is verified. Symmetric encryption is also being created to preserve the confidentiality of data, and a code is being developed to verify the authenticity of information for the integrity of messages [4]. We can say that we are talking about a secure communication channel, characterized by the following properties:

1. This is a private channel. In it, an encryption is created for each message at the end of the dialog, which allows you to determine the secret key.
2. Channel authentication. Each participant of the dialog is subject to authentication.
3. Channel reliability. Data is transmitted only after a complete integrity check.

Among the advantages of this protocol is its independence from the protocol of an applied nature. HTTP, FTP, TELNET can be superimposed on top of the protocol in question [5]. At the same time, the transparency of the system will be preserved, in other words, this protocol will coordinate the encryption algorithm and the key, perform authentication of the server before transmitting or accepting the first byte of information [6]. There are 2 main methods of creating an information cipher. It is a symmetric cipher based on a single secret key and an asymmetric cipher based on multiple public or private keys. SSL uses both options. An asymmetric cipher is based on the use of a key pair. Moreover, one key will be open. It can be found in the owner's certificate. The other key is private. It is not published in the owner's certificate. In this case, all keys are used only in pairs. The information is encrypted using the public key. And with the help of a private key, the data is decrypted [7]. In this relationship, you can do the following:

1. Each user has the right to receive a public key and use it to create an information cipher. At the same time, only the person who has access to the private key will be able to decrypt the data.
2. If a user who has a key pair creates a data cipher with his own private key, then other users will be able to see that this information was transmitted with a specific private key. At the same time, no changes were made to the information by a third party. Actually, this is the essence of creating a digital signature.

When encrypting with a public key, two keys are used, public and secret, and either of them can be used to encrypt a message [8]. If a public key was used to encrypt a message, then a secret key should be used to decrypt it, and vice versa. In such a situation, there are two possible ways to use keys. Firstly, the party keeping the secret key secret and publishing the public one can receive messages encrypted with the public key from the opposite party, which no one can read except her (after all, decryption requires a secret key known only to her) [9].

2 The main part

The SSL protocol has been implemented into the proposed information system, which supported the development of ciphers. The information that comes through the HTTPS protocol is converted into cryptographic data of the TLS or SSL protocols. Thus, it is possible to ensure the safety and confidentiality of information [10]. Thanks to this method of protection, various Internet applications are under reliable protection today, as well as secure connections in bank payment systems are protected. The protocol works with any browser. HTTPS functions with TCP port 443, unlike the HTTP protocol. Virtual Private Networks (VPNs) that used SSL were created as an alternative to remote access based on IPsec VPN. Despite this, due to the affordability and high reliability, this technology has become the most attractive for VPN [11]. SSL is widely used in e-mail when exchanging data (Figure 1).

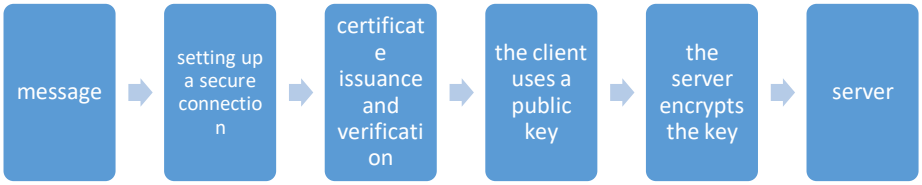

Fig. 1. Sending a message using an SSL certificate.

Protocol tasks by priority:

1. Security at the cryptographic level. SSL provides secure communication between participants in the data exchange process.

2. Compatibility. Specialists in the field of programming create applications based on SSL, which as a result will be able to effectively exchange cryptographic information without special recognition of the cipher of other programs.

3. Extensibility. SSL allows you to get a working environment for the necessary inclusion of public keys and more time-consuming processes of creating ciphers.

4. Relative productivity. For the SSL-based protocol to function, high CPU speeds are required. The same goes for using the public key. As a result, SSL enters the auxiliary caching stage to reduce the number of connections, which requires setup from scratch. Activity within the network is also reduced.

The protocol works with three authenticity checks [12]:

- Authentication of the server with an unidentified user.
- Complete anonymity.
- Authentication of all participants in the data exchange process (server—user).

This protocol handles all errors quite simply. When they are detected, the relevant information is sent to another private owner of the system. An error that cannot be eliminated requires termination of communication by the user or the server [13].

SSL is affected by different cryptographic values. Different cryptography algorithms can be used for encryption. So, when implementing a successful attack on such an algorithm, the protocol will not be able to provide a secure connection. An attack on a specific communication network is carried out through a session recording. It is necessary to distinguish the attacks that are committed against SSL. It should be taken into account that the SSL protocol is able to withstand these attacks if the client uses only a verified server for data processing [14].

The most common MitM attack. There are three parties involved in it: the attacker is between the user and the server. In such circumstances, the criminal intercepts the data that is sent in both directions and performs their substitution [15]. For the user, the attacker is represented on behalf of the server, and vice versa. With Diffie—Hellman key exchange, such attacks are most successful due to the integrity of the data and the impossibility of their authentication. At the same time, such attacks are not carried out within SSL due to the mandatory authentication of the information source.

With this type of attack, some large companies get the necessary data using Forefront TMG. In this situation, the criminal changes the original certificate to his own. Such an attack is successful by specifying Forefront TMG as a trusted certification authority. As a rule, such an operation remains unnoticed by the client due to the activities of corporate users within Active Directory. This control tool can be used to obtain data, steal personal information that is transmitted over a secure HTTPS connection.

The problem of sufficient awareness of customers about the likely interception of information remains relevant [16]. The fact is that when the original certificate is substituted, the corresponding security messages are not displayed. Therefore, the client believes that the data transfer is protected. Using Forefront TMG, it is possible to carry out a second MitM attack on the Internet. In this case, the certificate is not received by the client. To protect data from such an attack, it is required to stop working with web resources whose certificates contain certain errors [17].

Response attack. The criminal records the communication connection between the user and the server. Next, the attacker connects to the server to reproduce the recorded client data. However, SSL prevents this attack through connection identification. Of course, it is impossible to warn the connection ID only by theory, since it includes random events. If an attacker has significant funds, then he can record numerous sessions to select the optimal one based on the nonce cipher. However, such codes differ in 128—bit length. This means that in order to be able to predict 50%, the criminal must keep a record of nonce codes [18].

Algorithms used in SSL:

- PSK, SRP, ECDH, RSA to exchange keys and implement authentication.
- For ECDSA, DSA, RSA authentication.
- To create a symmetric cipher: Camellia, AES, DAS, IDEA, RC4, RC2, Triple DES.
- MD2, MD4, MD5, SHA for hash functions.

The concept of information system protection. Based on the analysis of the company's information security policy, the SSL encryption algorithm and the software used in the organization, changes were implemented to achieve the necessary IP security [19]. These measures will allow achieving the desired level of security of the information system for production sites [20].

1. Complete centralization of the application implies moving away from local databases located on servers in branches, writing instructions for support functions, transferring application support to the Help Desk and infrastructure functions.

2. Publishing the application on the company's intranet will allow accounting and filtering of users. Also implement additional group access rights to open this application.

3. Placing the database in the data center will increase the overall availability time of the application. It will ensure the correct allocation of equipment resources, fast and high-quality application of updates for the entire program at once. And most importantly, reliable backup, because the backup will be taken from the entire server and in the event of a hardware failure or a critical failure of the application, it will always be possible to deploy a fully working version of the application on other equipment that can be installed as in the company's data center.

4. Protection of client stations is a mandatory point of the concept because it is from them that the main threat comes. The antivirus must be network-controlled to quickly localize the threats that have arisen. Also, the user should not be able to disable the antivirus or weaken its protection.

5. The most basic threat to information security comes from users because the information system can be perfectly protected, but the user can launch a virus at his station, which will not only lead to the loss of information at his station, but also possible loss of information on the server and the spread of this virus over the network.

6. It is possible to get into the system only from the domain structure. Employees dismissed or blocked for other reasons should not have access to more than one information system: files on local stations, e-mail and other information systems of the company. Also, changing the password after the expiration of its statute of limitations and the introduction of requirements for the complexity of the password.

7. Encryption of the transmitted data between the server and the client.

3 Conclusion

The concept of the constructed information system, unlike the existing ones, has security that meets the modern requirements of companies. According to the developed concept, an information system was created to track transport at the production site using SSL encryption. The system has the ability to implement additional monitoring points, uniformity.

References

1. D.D. Fugarov, et al., *Methods for Revealing Hidden Failures of Automation System for Technological Processes in Oil and Gas Sector.* J. Phys. Conf. Ser. **1118,** 012055 (2018)
2. A.Y. Poluyan, et al., *Adaptive algorithm of selecting optimal variant of errors detection system for digital means of automation facility of oil and gas complex.* J. Phys. Conf. Ser. **1015,** 022013 (2018)
3. N.N. Ventsov, et al., *Studying the effect of paralleling settings on the functioning of a barcode recognition app,* International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017, 8076476 (2017)
4. Y.O. Chernyshev, et al., *Swarm-intelligence-based algorithm of connections permutation between pins.* J. of Theor. and Applied Inf. Tech. **80(1),** 13-20 (2015)
5. O. Purchina, et al., *The algorithm development based on the immune search for solving unclear problems to detect the optical flow with minimal cost*. E3S Web of Conf. **258,** 06052 (2021)
6. Y. Gerasimenko, et al., *Mathematical modeling and synthesis of an electrical equivalent circuit of an electrochemical device*, Advances in Intelligent Systems and Computing **1259,** 471-480 (2021)
7. M. Ganzhur, et al., *Modeling of storage processes using Petri nets*, E3S Web of Conf. **175,** 05038 (2020)
8. D. Fugarov, *Development and Mathematical Modeling of the AC Sensor for Refinery Automation Systems*, Smart Innovation, Systems and Technologies **247,** 271–281 (2022)
9. O. Agibalov, On the issue of using intuitionistic fuzzy sets for describing the expediency of solving optimization problems by genetic algorithms with given parameters, E3S Web of Conferences, 224, 01008 (2020)
10. A.I. Kozinkina, et al., *A Magneto Dielectric AC Measuring Transducer for Refinery Automation Systems.* J. of Machinery Manufacture and Reliability **49(11),** 963-970 (2020)
11. D. Onyshko, et al., *Synchronization system in wireless sensor networks of oil and gas complex,* E3S Web of Conf. **164,** 03030 (2020)
12. A.Yu. Poluyan, et al., *Solution of task on the minimum cost data flow based on bionic algorithm,* J. Phys. Conf. Ser. **1333**, 032056 (2019).
13. A. Gazizov, et al., *Theoretical aspects of the protection of personal data of employees of the enterprise by the method of pseudonymization*, E3S Web of Conf. **210,** 11001 (2020)
14. A.Yu. Poluyan, et al., *Application of bionic and immune algorithms for the solution of ambiguous problems of transportation routing*, J. Phys. Conf. Ser. **1333,** 032057 (2019)

15. D.D. Fugarov, et al., *Magnetodielectric AC measuring transducer for automation systems in oil refineries.* J. of Phys.: Conf. Ser. **1333(6),** 062020 (2019)
16. K.Yu. Solomentsev, et al., *Interference elimination in digital controllers of automation systems of oil and gas complex.* J. Phys. Conf. Ser. **1015,** 032179 (2018)
17. A.I. Sukhinov, et al., *Accounting method of filling cells for the solution of hydrodynamics problems with a complex geometry of the computational domain,* Mathematical Models and Computer Simulations **12(2),** 232-245 (2020)
18. Y.O. Chernyshev, et al., *Swarm-intelligence-based algorithm of connections permutation between pins,* J. of Theor. and Appl. Inf. Tech. **80(1),** 466-473 (2015)
19. D. Fugarov, *Technological Control of the Granulometric Composition of Active Materials of Chemical Current Sources*, Lecture Notes in Networks and Systems **510**, 1417–1423 (2023)
20. O. Purchina, et al., *Securing an Information System via the SSL Protocol*, International Journal of Safety and Security Engineering **12(5)**, 563–568 (2022)