Data exchange technology based on handshake protocol for industrial automation system

To cite this article: A V Astafiev and T O Shardin 2018 J. Phys.: Conf. Ser. 1015 042002

View the article online for updates and enhancements.

Related content

- Building automation system of payment platform weight component for large spacecraft reflector
  I V Kovalev and J O Badanina

- DEVICES FOR OBSERVATORY AUTOMATION
  R. K. Honeycutt, B. R. Adams, D. J. Swearingen et al.

- Problems in modernization of automation systems at coal preparation plants
  L P Myshlyaev, M V Lyakhovets, K G Venger et al.
Data exchange technology based on handshake protocol for industrial automation system

A V Astafiev, T O Shardin

Murom institute (branch) of Vladimir state university, 23a, Orlovskaya Str., Murom, 602264, Russia

E-mail: Alexandr.Astafiev@mail.ru

Abstract. In the article, questions of data exchange technology based on the handshake protocol for industrial automation system are considered. The methods of organizing the technology in client-server applications are analyzed. In the process of work, the main threats of client-server applications that arise during the information interaction of users are indicated. Also, a comparative analysis of analogue systems was carried out, as a result of which the most suitable option was chosen for further use. The basic schemes for the operation of the handshake protocol are shown, as well as the general scheme of the implemented application, which describes the entire process of interaction between the client and the server.

1. Introduction

Currently, most large enterprises face significant difficulties in improving the manageability of the company. The reduction of the task-performance time and the ability of subsequent monitoring are among the key factors that influence the quality of execution of electronic document management processes. One of the ways to accomplish these objectives is to implement an automated system that performs the above mentioned functions. However, the attempt to solve the problem of implementing such system encounters significant difficulties connected with the lack of an adequate supply in the market, or this offer is not profitable for the company for one reason or another.

It should be taken into account that the Internet is an open information environment and, for technical reasons, most traffic is transmitted in an open way, which allows an attacker to gain access to confidential data. Therefore, the information transmitted through this system to the enterprise should not be available to third parties. This criterion is one of the main, therefore to find the optimal solution among the available ones is impossible in some cases.

This technology will allow the employees of the industrial enterprise to ensure fast synchronization of data. In the course of information interaction, it is necessary to use protection in the transmission of data using a secure communication channel in order to prevent the interception of information by an attacker, which he can later modify and thereby damage, which entails significant material losses.

2. Threats of client-server applications

At the analysis stage of client-server applications in accordance with GOST-53114-2008 [1], the main threats were identified, according to which it is possible to intercept confidential data during the information interaction between the client and the server. The main threats and measures to prevent them are presented in Table 1:
Table 1. Main threats of client-server applications

| The main parts of the client-server application | Threats                                      | Countermeasures                                      |
|-----------------------------------------------|----------------------------------------------|------------------------------------------------------|
| Server software part                          | Access to administrative partitions from outside | Control of IP addresses                              |
|                                               | Identify weak passwords                      | Protection of the administrative section from third parties |
|                                               | Inadequate session security (no timeout)     | Maintaining password rules and changing them         |
| Client software part                          |                                               |                                                      |
|                                               | Identify weak passwords                      | Session time limit                                    |
| Client-Server Interaction                     | Invasion of third parties in information exchange (interception of information) | Using secure communication protocols |
of the site with 1C

| Free CMS | The implementation of a handshake protocol for secure data exchange is required |
|------------------------|------------------------------------------------------------------|
| Free WooCommerce plugi | Ready-made integration solutions implemented under older versions of 1C or not supported |
| There are ready-made solutions for the integration of the site with 1C | |
| This bundle of modules is already used on the customer's website | |

As a result of the comparative analysis, it was decided to use the last version of integration. With its merits, it was the one that suited most, since it was already used at the enterprise.

4. **Using the handshake protocol as a means of protecting information**

In practice, the process of transferring information over a secure communication channel is often associated with the use of protocols based on various cryptosystems. During the implementation of the application, the following method was taken as a basis:

The handshake protocol [4] is a cryptographic protocol based on the symmetrical mutual exchange of information between the participants of the information interaction according to the request-response scheme (Figure 1).

![Diagram of the handshake protocol in the application](image.png)

**Figure 1.** A diagram of the handshake protocol in the application

Using the RSA cryptosystem in this protocol allows exchange participants to initially use the necessary parameters for the safe transfer of information.

It is worth noting that the handshake protocol has analogues: an SSL certificate and an electronic signature [5]. To identify the merits and demerits of each analogue, an analysis of these algorithms was performed using the RSA cryptosystem according to the following criteria:

1. The least material costs criterion allow one to estimate profitability of application development, and material costs for maintenance of the algorithm are required.
2. Using the Certification Center allows one to assess whether additional authentication of keys is required using an electronic signature.

3. The cryptographic strength of the encryption algorithm used in the protocol allows us to assess whether this encryption algorithm has sufficient ability to withstand cryptanalysis. This is one of the important criteria, since with insufficient or low cryptographic strength, the use of an algorithm to protect information between exchange participants is not appropriate.

4. Difficulty level of using the method in applications allows one to assess whether the work for the user working with the interface of the algorithm used is understandable.

The results of the analysis are summarized in Table 3:

| Type                | The least material costs criterion | Using the Certification Center | The cryptographic strength of the encryption algorithm used in the protocol | Difficulty level of using the method in applications |
|---------------------|------------------------------------|-------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------|
| Handshake protocol  | Material costs are not required     | Certification centers are not required | The algorithm has a high cryptographic strength | Easy to use in applications                          |
| SSL certificate     | Material costs are required         | Certification centers are required | The algorithm has a high cryptographic strength | Additional software is required                       |
| Electronic signature| Material costs are required         | Certification centers are required | The algorithm has a high cryptographic strength | Easy to use in applications                          |

As a result, it can be seen that the handshake protocol is safe to protect information when it is used as a secure data exchange technology. The method has a number of advantages, namely: it is economically advantageous (costs are minimal or none at all), does not require certification centres, which makes it possible for any person to use it, and is also easy to use with high cryptographic stability. The mathematical model of this algorithm is shown below in Figure 2:

![Figure 2. A mathematical model of the RSA algorithm used in the handshake protocol](image-url)
The scheme of the developed system is shown in Figure 3.

The secure communication channel used in the client-server application

![Diagram of the developed system](image)

**Figure 3.** A scheme of the developed system, using the implemented technology for secure data exchange

The system represents two interconnected modules:

1. The client part is a plug-in on the site running CMS Wordpress. Communication with the server occurs via the SOAP protocol.

2. A server part is a system of key generation and additions for the created 1C enterprise database (web service). It is located on the computer of the organization.

As a result of the work done, this development proved its effective use in practice. The development is confirmed by the certificates on registration of computer program No. 2017617564, No. 2017661972, and also implemented at the enterprise for the production of furniture products.

5. **Conclusion**

As a result of the work done, this development proved its effective use in practice. The development is confirmed by the certificates on registration of computer program No. 2017617564, No. 2017661972, and also implemented at the enterprise for the production of furniture products.

**References**

[1] GOST R 53114-2008 Information security, Ensuring information security in the organization. Basic terms and definitions

[2] Astafiev A 2015 Development of Methods for Determining the Locations of Large Industrial Goods During Transportation on the Basis of RFID *Procedia Engineering* **129** 1005-1009

[3] Astafiev A.V 2016 Development of the automatic marking identification system based on two-stage visual recognition of metal-rolling billets *Dynamics of Systems, Mechanisms and Machines, Dynamics*

[4] Moldovyan A A, Moldovyan D N, Levina A B 2016 *AUTHENTICATION PROTOCOLS WITH ZERO SECRET DISCLOSURE* (St. Petersburg: ITMO University)

[5] Vodolazsky V 1992 *Commercial encryption systems: the main algorithms and their implementation. Part 1* (Monitor)
[6] Rongxing L, Zhenfu C, Xiaolei D, Chao S, Congkai S 2006 Password-based group key agreement protocol for client-server application Wuhan University Journal of Natural Sciences 6 1701-1703
[7] Clark A 2011 HTTP Session Security Encyclopedia of Cryptography and Security 2 567-569
[8] Gunawan I, Haryadi D S, Noertjahyana A, Hermawan Y 2015 Securing Client-Server Application Design for Information System Inventory, Proceedings of Second International Conference on Electrical Systems (Technology and Information 2015) pp 573-580
[9] Morrissey P, Smart N P, Warinschi B 2010 The TLS Handshake Protocol: A Modular Analysis Journal of Cryptology 2 187-223
[10] Morrissey P, Smart N P, Warinschi B 2008 A Modular Security Analysis of the TLS Handshake Protocol International Conference on the Theory and Application of Cryptology and Information Security Advances in Cryptology ed J Pieprzyk (Melbourne: ASIACRYPT’08) pp 55-73
[11] Rhodes B, Goerzen J 2014 Foundations of Python Network Programming (New York: Apress)
[12] Jonsson J, Kaliski Jr, Burton S 2002 On the Security of RSA Encryption in TLS Advances in Cryptology vol 2442 ed M Yung (Heidelberg: Springer) pp 127-142