Selection of a rational authentication method for the remote systems of interaction with the vessels

V V Karetnikov¹, A A Butsanets¹, A V Mitrofanova¹

¹ Admiral Makarov State University of Maritime and Inland Shipping, 5/7 Dvinskaya str., St. Petersburg, 198035, Russia
E-mail: butsanetsaa@gumrf.ru

Abstract. Scientific and technical progress in the development and creation of software and hardware systems has a positive effect on improving the efficiency of water transport operation. The developed systems solve both general and particular tasks. Remote technical condition monitoring systems are used to solve particular problems, for example, to control fuel consumption. The vessels remote control systems are considered as larger ones. Obviously, only wireless means of communication between the remote user (operator) and the vessel are provided in them. The purpose of the paper is to determine a rational approach to ensure the information security for the remote systems of interaction with vessels. The main approaches to ensure the safe use of resources (Password authentication and authentication with one-time passwords, biometric authentication, authentication with a public key, authentication protocols and cryptographic methods) are considered and evaluated by the expert assessments method. Information security threats for the above-mentioned systems of remote interaction with the vessels are highlighted. It has been determined that for remote control systems it is highly expedient to use the cryptography methods with encryption, and for the remote technical condition monitoring such protection is not expedient, but the password authentication (including authentication with one-time password) is sufficient. Further directions of researches will be the elaboration of the specific solutions for selected means of security providing.

1. Introduction

The current level of scientific and technological progress in the development and creation of software and hardware systems has a positive effect on improving the efficiency of water transport operation. Integrated systems for monitoring the technical condition of ship systems and devices, cargo status, and monitoring of fuel and lubricants consumption are gradually being introduced by shipowners on the vessels board of various classes and types. As a rule, such systems are primarily implemented on new marine vessels or private yachts of the premium segment. It should be noted here that over the next ten years a substantial increase in the number of unmanned vessels is foreseen. There are real commercial projects of remotely controlled small-sized (up to 12 meters long) vessels for carrying out the specific tasks of hydrographic, hydrological, environmental or integrated monitoring of water bodies, as well as for using as combat targets for the navy training. The development of the MUNIN project has been underway since 2015 [1]. In December 2018, the sea trials of remote-controlled ferries were conducted by ABB Company in Helsinki and Rolls-Royce in cooperation with Finferries in Turku, Finland. Thus, in addition to the remote technical condition monitoring (RTCM) system for the vessels, a remote control (RC) system has already been created.

The development of remote control systems and the remote technical condition monitoring system are considered all over the world. Theoretical and practical interest is provided by the works in the field...
of intelligent control of voltage quality [2] and control of the vessels power systems stability [3-4], the fuel level monitoring using navigation data [6], modern tracking systems for ship diesel engines wear modes [7-9]. In addition, the developments of hybrid power plants in order to save fuel are known [10]. Organizations are studying the applied issues of designing intelligent vessels control systems in general [11–12]. In the development of such systems, the priority technology is the Internet of things (IOT) [13], which uses the MQTT (message queuing telemetry transport) network protocol in order to save traffic [14]. The problems associated with the reduction of exhaust gases emissions [15-16] can be solved using such systems. Such diversity of ship's intellectual systems requires a rational approach in ensuring the information security. This is a prerequisite for this work.

Ensuring the required level of information security RTCM and RC systems is a complex task, one of the main stages of which is the obligatory to define and formalize the basic principles of providing the security of data transmission to prevent unauthorized access in order to steal the information of the unmanned ships.

It is obvious that only wireless means of communication between the remote user (operator) and the vessel are provided in such systems. Thus, it is necessary to ensure the possibility of recognizing the operator by identifier (identification), carrying out the operator authentication. In addition, the possibility of access to the transmitted information (operator commands and vessel responds) only by the authorized operators (integrity) must be ensured.

Thus, the purpose of this paper is to determine a rational approach to ensure the information security for the systems such as RTCM and RC.

2. Methods and materials

The key terms used in the paper are:

1. Identification. This is the object recognition procedure by its identifier.
2. Authentication. This is the authenticity procedure.
3. Authorization. This is the providing the access to a resource.

Let us consider the basic approaches to ensure the safe use of resources.

Unique Identifiers. Some identifiers are unique, i.e. they can belong to only one subject. ID (Identifier) is the information that can identify the subject. UID — Unique identifier; such identifiers can be generated on the basis of passport data, bar codes, e-mail, etc.

Password authentication is the easiest way based on memorized passwords (the advantage is simplicity, the disadvantage is the low level of protection, it is considered not to provide at least an average level of security).

Biometric authentication. The particular qualities depend on the type of biometric technology, however, despite the undoubted convenience, there may be errors at recognition, and the appropriate additional equipment (scanners) is also required. Besides, if the task of the user (operator) identification in the system will be solved in this way, then the issue of the vessel recognition still remains.

Authentication using one-time passwords. This solution is devoid of the traditional problems of password-protected schemes. The main disadvantage is the need to purchase for users the specialized devices for generating one-time passwords - OTP-tokens.

Authentication with public key. This method has many options for using asymmetric cryptography for authentication, including widespread. For example, the TLS (Transport Layer Security) protocol makes extensive use of digital certificates, and allows you to create a shared secret key for encrypting a communication session between the vessel operator and the server. However, this protocol is focused on providing authentication and secure connection between two subscribers (and the server), and is not suitable for a network where there are subjects and objects, and all of them must be identified and authenticated both in the network and in operation with each other. In general, authentication using parties' public key certificates is one of the most popular directions in modern authentication methods.

Authentication Protocols. Point-to-point (PPP) authentication protocols and their types: PAP, CHAP, EAP (and its variations EAP-TLS, EAP-TTLS, etc.), TACACS + (Terminal Access Controller Access Control System plus), RADIUS (Remote Authentication in Dial-In User Service), etc., have been analyzed. However, all these protocols do not allow the user (operator) and vessel to authenticate with each other after they were authenticated on the network. Even if during the authentication process
the operator receives some key for secure communication with the server, the problem of obtaining the key for secure communication between the user (operator) and the vessel is still not solved.

The ways of ensuring integrity include the various cryptographic methods — encryption, MAC (message authentication code), hashes, electronic signature. At the same time, encryption is the only way to protect against unauthorized access to the transmitted information. Other methods, such as electronic signature, allow us only to detect the fact of changes in the transmitted information, but, in general, do not prevent it. As a result, the following protocols providing encryption are considered: TLS, IPSec (IP Security with its IKE (Internet Key Exchange) standards, ESP Encapsulating Security Payload, ISAKMP (Internet Security Association and Key Management Protocol)). In fact, these protocols are designed to form VPN-solutions.

To solve this problem, the levels of rationality for the use of the above-mentioned access methods with RTCM and RC have to be determined. For this purpose, the method of expert assessments will be used.

Rationality in this case is determined by the following criteria: ease of use, cost, safety level, reliability.

3. Results
Let us consider the applicability of authentication methods to provide the required level of security for RTCM and RC, taking into account the rational use. It should be noted that identification can be carried out using generated or unique identifiers, the first of which are preferable due to their higher level of protection, and the need for their use is determined at the time of a specific project development.

Based on the listed approaches and comparing them with the expected level of security, it is required to analyze the methods of ensuring security for the systems. The results of expert evaluation for each approach are presented in Table 1.

| System  | Type                          | Expert assessment of rationality |
|---------|-------------------------------|----------------------------------|
| RTCM    | Password authentication       | 3.75                             |
|         | Biometric authentication      | 2.75                             |
|         | Authentication using one-time passwords | 3.75 |
|         | Authentication with public key | 3.25                             |
|         | Authentication Protocols      | 3                                |
|         | Cryptographic methods         | 3.25                             |
| RC      | Password authentication       | 2                                |
|         | Biometric authentication      | 2.25                             |
|         | Authentication using one-time passwords | 2.75 |
|         | Authentication with public key | 2.75                             |
|         | Authentication Protocols      | 2.5                              |
|         | Cryptographic methods         | 4.5                              |

The results of the evaluation show that the cryptographic methods are the optimal approach for the remote control systems, and for the remote technical condition monitoring systems, the password authentication (including authentication with one-time password) is sufficient.

This assessment is preliminary and requires more in-depth analysis during the development of a specific project, taking into account the consumed traffic.

4. Discussion
The information security threats are advisable to consider. For remote technical condition monitoring systems the following threats may arise:

1) Information Reading;
2) Information Stealing;
3) Information changing;
4) Disconnection;
5) Substitution of information object (vessel).

When establishing the communication between an operator (user) and a remotely controlled vessel, the following information security threats may arise:
1) Operator spoofing (an attacker impersonate an operator).
2) Spoofing of the remote control vessel (an attacker impersonate the vessel).
3) Unauthorized change of the operator commands.
4) Unauthorized change of the remote control system responds.
5) Unauthorized access to the commands by the attacker (commands reading).
6) Forced disconnection by the attacker.

Since the list of threats for a remote control is broader, the ways to deal with the threats by the example of these systems are considered. With the first two threats, authentication protocols are used, allowing subscribers to be confident in the authenticity of the interlocutor. To deal with unauthorized access and unauthorized changes, as a rule, encryption and message authentication methods (electronic signature, MAC, etc.) are used. The sixth item will not be considered, as it is beyond the scope of this study.

Let us consider the authentication methods that could be applied to solve the specified problems of subscribers spoofing. It should be noted that one-sided authentication methods (when only one of the parties confirms its authenticity to the other) are not considered, since they do not allow us to solve both the threat of operator spoofing and the threat of vessel spoofing. Therefore, only two-sided (mutual) authentication methods, allowing both parties to verify the authenticity of each other, are suitable for remote control.

An additional factor is the mandatory authentication of the operator in the system, which is performed primarily at entering the system and, in case of successful access, will allow him to perform his functions. At the same time, the authenticity of operators is checked by a specialized authentication server. In addition, when an operator attempts to start work with a vessel, it is necessary to check his authority to perform these actions.

To choose one from the existing methods of mutual authentication, the threats of unauthorized access to the transmitted commands or making changes to them have to be also considered. As mentioned above, these problems can be solved by using encryption.

Thus, the following requirements to the systems under consideration can be distinguished:
1) Users (operators) authentication at login.
2) Verification of the user's (operator's) authority to perform the requested actions.
3) The operator authentication in front of the remote control system.
4) The remote control system authentication in front of the operator.
5) Protection against unauthorized access to the communication channel.
6) Protection against unauthorized changes in the information transmitted via the communication channel.

Depending on the additional requirements, the authentication can be based either on the symmetric encryption or on the asymmetric cryptographic protocols (asymmetric encryption or electronic signature).

The symmetric encryption algorithms use the same secret key for encryption and decryption, and all subscribers must keep this key secret. The basis of authentication in this case is the assumption that if only the nominal subscribers A and B know the secret key, then only the subscriber involved into the shared secret, i.e. either subscriber A, or subscriber B, can encrypt some data or decrypt the received cipher text. Time labels, random numbers, numeric sequences, etc. assist to avoid attacks associated, for example, with the attacker's interception of the authentication message and the attacker's subsequent attempt to use the received encrypted data to, for example, embed into the system on behalf of a legitimate user.

In the asymmetric algorithms, one of the key pair is public and can be provided to all engaged parties, and the second one is private, and must be kept secret from everyone. In the asymmetric encryption, having obtained the user's public key available to everyone, anyone can encrypt information on this key.
Only the owner of the second key, the private one, can decrypt the received cipher text. The proof of the subscriber authenticity will be exactly the ability to decrypt the received ciphertext. The electronic signature can be put by the owner of the private key using it, but anyone who takes the available public key can check it. Accordingly, the proof of the subscriber authenticity is precisely the ability to put an electronic signature, which then anyone can verify. When using the asymmetric algorithms to protect against a series of attacks, time labels, random numbers, etc. are also used. Besides, the use of asymmetric cryptography leads to another problem - how to make sure that the uploaded public key belongs to the announced user? One of the most common approaches is to use some independent trusted third party that can guarantee the subscriber’s public key. A certifying center, creating so-called digital certificates, which are in fact the subscriber’s public key, signed with an electronic signature of the certifying center, can be as the third party.

The user's login and reusable password are traditionally used for authentication; however, this scheme has a number of disadvantages, ranging from storage problems to password transfer problems. A more secure approach assumes the use of one-time passwords or authentication based on digital certificates.

The tasks of protecting against unauthorized access to the transmitted information and protecting against making changes to it are primarily solved by encrypting the transmitted information. Encryption is performed by the symmetric encryption algorithm, which requires both subscribers (the vessel and the operator) to know one secret key. The secret key used to encrypt the communication session should change at least from session to session. This imposes requirements on the receipt of this key by both subscribers before the start of the communication session. There are a large number of cryptographic key distribution protocols; however, in order to reduce the amount of the transferred service data and in order to deliver the session keys to both subscribers in time, the authentication protocol combined with the key distribution protocol is of the greatest interest.

5. Conclusion
The conducted research has revealed that the cryptography methods with encryption is very expedient to use for remote control which will allow us to simultaneously solve authentication issues both in the network and in front of each other. Such strong protection does not seem appropriate for remote technical condition monitoring, the password authentication (including authentication with the one-time password) is sufficient. Further research can be directed to a more in-depth study of the schematics solutions for authentication methods using cryptographic protection for the remote control systems and for the password authentication for the remote technical condition monitoring system.

References
[1] Rødseth Ø J and Burmeister H C 2015 Risk assessment for an unmanned merchant ship TransNav 9(3). DOI: 10.12716 / 1001.09.03.08
[2] Gu W, Chen K, Yang Y and Gao S 2018 Design and Realization of Power Quality Monitoring Scheme for Measuring Ship IOP Conference Series: Earth and Environmental Science 170(4) 042158. DOI: 10.1088/1755-1315/170/4/042158
[3] Jin Z, Meng L, Guerrero J M and Han R 2018 Hierarchical control design for a shipboard power system with DC distribution and energy storage aboard future more-electric ships IEEE Transactions on Industrial Informatics 14(2) 703–14. DOI: 10.1109/TII.2017.2772343
[4] Sulligoi G, Vicenzutti A, Arcidiacono V and Khersonsky S 2016 Voltage stability in large marine-integrated electrical and electronic power systems IEEE Transactions on industry applications 52(4) 3584–94. DOI: 10.1109/TIA.2016.2544833
[5] Kanellos F D, Prousalidis J M and Tsekouras G J 2014 Control system for fuel consumption minimization–gas emission limitation of full electric propulsion ship power systems Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment 228(1) 17–28. DOI: 10.1177/1475090212466523
[6] Capezza C, Coleman S, Lepore A, Palumbo B and Vitiello L 2019 Ship fuel consumption monitoring and fault detection via partial least squares and control charts of navigation data
Transportation Research Part D: Transport and Environment 67 375–87. DOI: 10.1016/j.trd.2018.11.009

[7] Yan X, Xu X, Sheng C, Yuan C and Li Z 2017 Intelligent wear mode identification system for marine diesel engines based on multi-level belief rule base methodology Measurement Science and Technology 29(1) 015110. DOI: 10.1088/1361-6501/aa966e

[8] Zhu X, Zhong C and Zhe J 2017 A high sensitivity wear debris sensor using ferrite cores for online oil condition monitoring Measurement Science and Technology 28(7) 075102. DOI: 10.1088/1361-6501/aa6ad8

[9] Meng W and Guo C 2010 Research on speed intelligent control based on neural networks for large marine main diesel engine 8th World Congress on Intelligent Control and Automation 4667–4670. DOI: 10.1109/WCICA.2010.5555893

[10] Kalikatzarakis M, Geertsma R D, Boonen E J, Visser K and Negenborn R R 2018 Ship energy management for hybrid propulsion and power supply with shore charging Control Engineering Practice 76 133–54. DOI: 10.1016/j.conengprac.2018.04.009

[11] Geertsma R D, Negenborn R R, Visser K and Hopman J J 2017 Design and control of hybrid power and propulsion systems for smart ships: A review of developments Applied Energy 194 30–54. DOI: 10.1016/j.apenergy.2017.02.060

[12] Qiu B, Zhang Y, Wei M, Li Y and Wang Y 2018 Hybrid Cloud Based Cyber-enabled Ship Control and Management System IEEE International Conference on Prognostics and Health Management (ICPHM) 1–6. DOI: 10.1109/ICPHM.2018.8448547

[13] Yang S, Shi L, Chen D, Dong Y and Hu Z 2017 Development of ship structure health monitoring system based on IOT technology IOP Conference Series: Earth and Environmental Science 69(1) 012178. DOI: 10.1088/1755-1315/69/1/012178

[14] Atmoko R A, Riantini R and Hasin M K 2017 IoT real time data acquisition using MQTT protocol Journal of Physics: Conference Series 853(1) 012003. DOI: 10.1088/1742-6596/853/1/012003

[15] Raptotasios S I, Sakellaridis N F, Papagiannakis R G and Hountalas D T 2015 Application of a multi-zone combustion model to investigate the NOx reduction potential of two-stroke marine diesel engines using EGR Applied Energy 157 814–23. DOI: 10.1016/j.apenergy.2014.12.041

[16] Jenaru A, Arsenie P and Hanzu-Pazara R 2016 The estimation of the pollutant emissions on-board vessels by means of numerical methods IOP Conference Series: Materials Science and Engineering 145(8) 082016. DOI: 10.1088/1757-899X/145/8/082016