Research on Secure Method Oriented Digital Ocean System

Yu Zhang[1, a], Zhiqiang Wei[2, b] and Hao Liu[2, c, *]

*Corresponding author: Hao Liu

[1]School of Ocean University of China, Qingdao 266100, China;

[a]yuzhangouc@163.com, [b] weizhiqiang@ouc.edu.cn, [c] liu.hao@ouc.edu.cn

Keywords: Digital Ocean, Marine Data, Multi-level security, BLP model, Biba model.

Abstract. According to the status of security work in marine-related fields, we analyze the risks faced by Digital Ocean system. We collect the specific characteristics of marine data and propose a secure method oriented digital ocean system. We adopt multi-level security mechanism that marine data is ordered by level of importance and we propose a security model that is a combination of BLP model and Biba model. The security model ensures confidentiality and integrity in Digital Ocean system, which provides effective experience for the construction of secure methods in marine-related fields.

1. Introduction

The 21st century is an information age. Marine informatization is a part of the national informatization strategy and Digital Ocean is an infrastructure project of marine informatization development strategy. The data in Digital Ocean contains marine remote sensing data, ARGO buoy data, marine geological and geophysical data, marine dynamic environmental data and marine biological and ecological data and so on. These marine data are not only closely related to comprehensive marine management, but also closely related to national security and marine strategic interests. However, there are a lot of risks such as sensitive marine information leakage, marine data missing, viewing marine data beyond the access permissions and marine data tampering in the process of mining and analyzing marine data. So, construction security system and methods in marine-related fields has received highly attention from the government.

2. The analysis of digital ocean system

2.1 The characteristics of marine data.

2.1.1 The diversity of marine data.

There many kind of marine data in Digital Ocean, such as basic marine environment data, marine satellite remote sensing data, marine economic statistical data, marine mode data and marine instruments survey data and so on. Basic marine environment data contains hydrology, surface meteorology, ocean current, temperature, salinity, biology, chemistry, environmental quality, geology and so on [1]. These data are related to the scientific data of each subject in the ocean.

2.1.2 The multiple sources of marine data.

The sources of marine data are complex. It is because the ways of acquiring marine data are various. The ways of acquiring marine data are not only navigation monitoring, position monitoring, aerospace remote sensing observation, such as buoy, Nathan station, CODAS, CTD, ADCP, observation vessels, but also through the activities of national cooperation [2]. While, the multiple sources of marine data can lead to the precision, form and structure of marine data becoming complex.

2.1.3 The polymorphism of marine data.

The polymorphisms of marine data are different manifestations of marine data. Such as graphics, images, sound, text, database tables, etc. Marine data in different manifestations need different methods of data memory and processing.

2.1.4 The large amount of marine data.

The marine data are updated constantly such as basic marine environment data. These marine data are time series data that increase at an explosive speed [3].

2.1.5 The heterogeneity of marine data.

The data storage modes of different type's marine data are flexible. Diverse original observation data are stored in different storage media. The digital marine data stored in Word documents, text files or a database tables and so on.

2.2 The risks to Digital Ocean.

In the process of obtaining the marine data, there are some risks such as untrustworthy information sources, sensitive marine information leakage and so on. There are different sensitivity and importance in marine data. But, in the process of storing the marine data, the marine data security management scheme is unable to meet the requirements of classified protection. In the Digital Ocean system, marine data owners and users have different operation permissions. But the illegal users can access sensitive marine data in an indirect way, such as using the historical access, exchanging of information or using inference channels [4].

3. A Secure Method Oriented Digital Ocean System

The confidentiality of marine data refers to preventing the leakage of marine data. The integrity of marine data is protecting marine data from unauthorized tampering and deletion. The availability of marine data is to ensure authorized user can access marine data.

3.1 The security model oriented Digital Ocean System

We adopt multilevel security mechanism that marine data is ordered by level of importance. The typical multilevel security models include BLP model [5], Biba model [6] and Clark-Wilson [7] model and so on. BLP model is mainly to ensure the confidentiality of data. BLP model allows lower confidentiality security level information to flow to high confidentiality security level users [8]. The information flow in BLP model as shown in Fig. 1

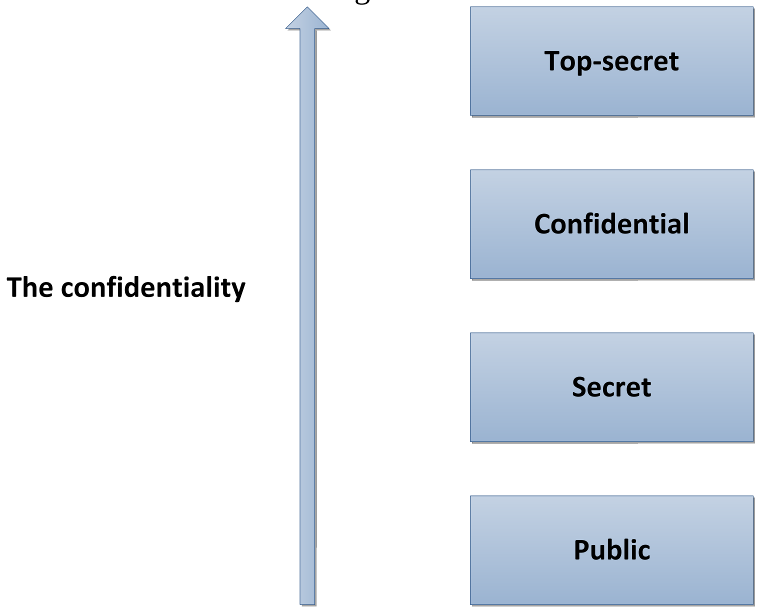

Fig. 1 The information flow in BLP model

Biba model is mainly to ensure the integrity of data. Biba model allows lower integrity security level information to flow to high integrity security level user [9]. The information flow in Biba model as shown in Fig. 2

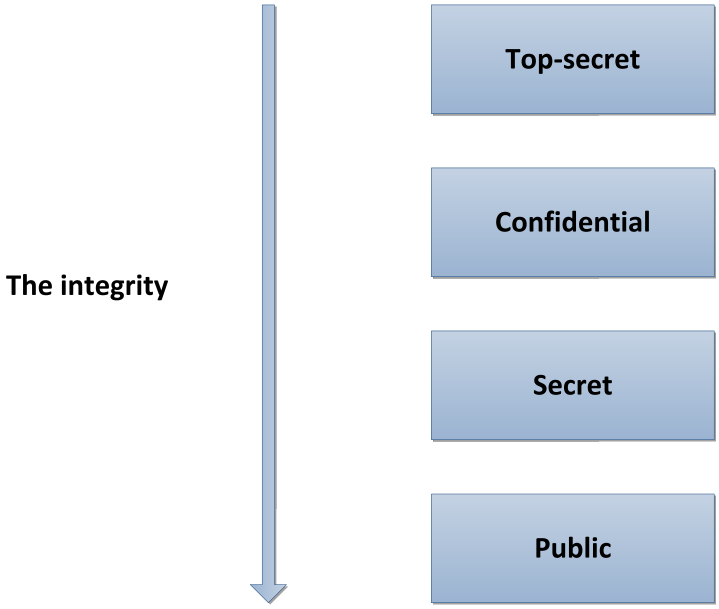

Fig. 2 The information flow in Biba model

To ensure the confidentiality and integrity of marine data, the security model of combination of BLP and Biba is proposed in this paper. F Pub pointed out that the confidentiality level of data, the integrity level of data and the availability level of data are not entirely consistent [10]. In this paper, we propose the security model oriented Digital Ocean system and we assume that the confidentiality and integrity of the user and the marine data are independent of each other. The information flow in unified security model as shown in Fig. 3

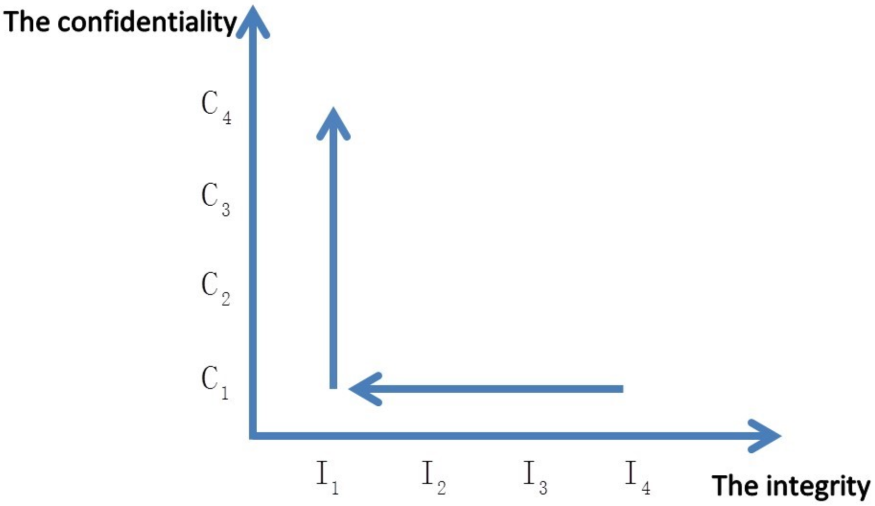

Fig. 3 The information flow in unified security model

We introduce marine data security categories that contain confidentiality category and integrity category. Security categories values are LOW, MODERATE and HIGH, and HIGH > MODERATE > LOW.

Users can view marine data when the security levels of users and marine data meet one of the following three conditions:

(1) The confidentiality security level of users is greater than or equal to marine data and the integrity security level of users is no greater than marine data;

(2) Users can access data if the confidentiality security level meet the condition of the first and the integrity security level of users is greater than marine data, meanwhile the confidentiality category of marine data is higher than its integrity category and the minimum integrity security level of users is less than or equal marine data;

(3) For users, the confidentiality security level is less than marine data and the integrity security level is less than or equal to marine data, and for marine data, the integrity category is higher than its confidentiality category and the maximum confidentiality security level of users is greater than or equal to marine data.

Users can alter marine data when the security levels of users and marine data meet one of the following three conditions:

(1) The confidentiality security level of users is no more than marine data and the integrity security level is greater than or equal to marine data;

(2) The confidentiality security level of users is less than or equal to marine data and the integrity security level is less than marine data, but the confidentiality category of marine data is higher than its integrity category and the maximum integrity security level of users is greater than or equal to the integrity security level of marine data;

(3) The confidentiality security level of users is greater than marine data and the integrity security level of users is greater than or equal to marine data, but the integrity category of marine data is higher than its confidentiality category and the minimum confidentiality security level of users is less than or equal to the confidentiality security level of marine data.

3.2 The adjustment principle of user security level

If we combine the BLP model with the Biba model directly, marine data cannot flow into different security levels completely, because confidentiality protection strategy and integrity protection strategy are independent of each other. But, we can adjust security level of users or marine data dynamically in some way. When the security levels of users and marine data satisfy certain conditions, we adjust security level of users according to the security attributes of marine data to make sure confidentiality and integrity.

(1) When the security labels of users and marine data meet both BLP model and Biba model, we needn’t adjust security level of users.

(2) The security labels of users and marine data only meet BLP model:

a. The confidentiality category of marine data is higher than its integrity category. It’s meaning the confidentiality of marine data is superior to its integrity. So, we can only adjust the integrity level of users.

b. On the contrary, if the integrity category of marine data is higher than its confidentiality category, that is to say, the integrity of marine data has more superior than confidentiality. Therefore, we cannot adjust the integrity security level of users. Adjusting the confidentiality security level of users is no practical meaning because users and marine data don't meet Biba model and we cannot adjust the integrity security level of users. So, we don't need adjust confidentiality security level of users.

(3) The security labels of users and marine data only meet Biba model:

a. The integrity category of marine data is higher than its confidentiality category, that is to say, the integrity of marine data is superior to its confidentiality. So, we can’t adjust the integrity security level of users, but we can adjust the confidentiality level.

b. The confidentiality category of marine data is higher than its integrity category and the confidentiality of marine data have more priority than its integrity. So, we cannot adjust the confidentiality security level of users. Adjusting the integrity security level of users is no practical meaning because users and marine data don't meet BLP model and we cannot adjust the confidentiality security level of users. So, we don't need adjust integrity security level of users.

(4) When the security labels of users and marine data meet neither BLP model nor Biba model, we don't need adjust security level of users.

3.3 Security analysis

The aim of security analysis is to know how to utilize the model to protect marine data. The law of the model is introduced below.

If the security labels of users and marine data meet both BLP model and Biba model, the model don't destroy the confidentiality and integrity of Digital Ocean system.

When the security labels of users and marine data accord with BLP model but don't meet Biba model, the model don't destroy the confidentiality of Digital Ocean system; In the situation that the confidentiality category of marine data is higher than its integrity category, users can adjust integrity category, not restricted by Biba model, within the scope of authority. Thus, we can draw the conclusion that the model doesn’t destroy the integrity of Digital Ocean system.

The model doesn’t destroy the integrity of Digital Ocean system when the security labels of users and marine data only meet Biba model; If the integrity category of marine data is higher than its confidentiality category, users can adjust confidentiality category, not restricted by BLP model, within the scope of authority. Therefore, we can conclude that the model doesn’t destroy the confidentiality of Digital Ocean system.

3.4 The advantages of the security model oriented Digital Ocean System

BLP model is the representative confidentiality model and Biba model is the representative integrity model, but the direct combination of BLP model and Biba model hinders the flow of information. Therefore, we introduce marine data security categories and adjust the confidentiality level and the integrity of users according to the importance level of confidentiality and integrity in marine data. The security model ensures the confidentiality and the integrity of marine data.

4. Conclusions

According to the specific characteristics of marine data and the risks faced by Digital Ocean system, we propose a secure method oriented digital ocean system and security model to protect marine data. We introduce marine data security categories and adjust the confidentiality level and the integrity of users according to the importance level of confidentiality and integrity in marine data. The security model protects the confidentiality and the integrity of marine data and ensures multi-level security of the Oriented Digital Ocean System. Certainly, there are other secure methods, such as, inference control of marine data or design the database that statistics query and don’t leak sensitive information. So, we can ensure multilateral security of the Digital Ocean System.

5. Acknowledgments

This research is supported by National Secrecy Science Research Program (BMKY2015BT03) and Qingdao People's Livelihood Science and Technology Program (14-2-3-62-nsh)

6. References

[1]. ZHANG F, SHI S X, YIN R G, et al. A study of data architecture in digital ocean [J]. Marine Science Bulletin. Vol. 28 (2009) No. 4, p. 1-8.

[2]. XIA D, SHI S, WANG D, et al. Study on the techniques of Marine data warehouse and data mining[J]. Marine Science Bulletin. Vol. 24 (2005) No. 3, p. 60-65.

[3]. ZHANG M H, HUANG D M, XIONG Z M, et al. Construction of an integrated management platform for multi-dimension heterogeneous and massive ocean data[J]. Marine Sciences. Vol. 36 (2012) No. 2, p. 110-115.

[4]. YAN H P, WANG W, SHI B L. Inference control in secure database [J]. Journal of Software. Vol. 17 (2006) No. 4, p. 750-758.

[5]. BELL D E, BELL D E, LAPADULA L J, et al. Secure computer systems: mathematical foundations Mtr-2547[J]. Secure Computer Systems Mathematical Foundations. (1973)

[6]. BIBA K J. Integrity considerations for secure computer systems [J]. Electronic Systems DIV Air Force Hanscom AFB. (1977)

[7]. CLARK D D, LSON D R. A comparison of commercial and military computer security policies [J]. (1987) p. 184-184.

[8]. XUE H, ZHANG Y, GUO Z, et al. A multilevel security model for private cloud [J]. Chinese Journal of Electronics. (2014) No. 2, p. 232-235.

[9]. GUO R C, LIU W Q, NING X U, et al. Application of Improved Biba Model in Security Operating System[J]. Computer Engineering. Vol. 38 (2012) No. 13, p. 96-98.

[10]. PUB F. Standards for security categorization of federal information and information systems [J]. NIST FIPS – 199. (2004).