Intrusion Tolerant Control for Warship Systems

Chen Yuanbao [1, a], Huang Shuang [1, b], Lv Yunfei [1, c]

[1] Wuhan Second Ship Design and Research Institute, Wuhan, 430064, China

[a]email: 21275017@qq.com, [b]email: 40150730@qq.com, [c]email: 2946572023@qq.com

Keywords: Intrusion Tolerance; Cyber Security; Warship Systems

Abstract. With the adoption of large amount of information communication technology (ICT) and the increasingly frequent cyber-attacks, security issues have gradually become key problems for warship systems. Warship systems, as a special mobile information combat platform, have higher requirements for timeliness and availability. And security accidents in warship systems can cause serious consequences. This means that security protection of warship systems should not only be able to prevent cyber-attack, but also have the ability of intrusion tolerance. This paper proposes an intrusion tolerant control approach that can provide a set of reusable security services as an architectural solution with a close loop control structure. According to the approach, security solution can be implemented by embedding into warship systems with consideration of domain features of warship.

Introduction

Informationized and intelligentized warship is an important developing direction of warship systems. Due to high demand for flexibility, interoperability and easy-managing, information and communication technology (ICT) is widely used in warship systems. However, it also raises concerns about the cyber-security issue of warship systems.

In warship, the internal communication and the external communication gradually achieve interconnection[1]. As a result, warship systems will face the complicated and adverse internet environment directly. Especially, with the putting forward of the Network-Centric Warfare theory[2], information sharing and integration have become more and more important. On the other hand, internal attack is also an important aspect in security threat of warship systems. The internal attacks are probably from misoperation by submariners, or are spiteful attack from disgruntled submariners. In these situations, security protection become an important issue in warship systems.

As a special mobile information device platform, warship systems have quite a lot of difference with traditional information systems. Firstly, warship system is a complex system which contains many complicated business information flows and many physical devices. Information flows affect physical devices and vice versa. Secondly, the types of information involved in business information flows are various and complicated. While the physical devices in warship system directly relate to the warship and human safety of submariners. Once an accident occurs in warship systems, it may damage system equipment and environment, or endanger submariners' safety, even cause the failure of the war. Finally, real-time performance is very important for warship systems. In difficult combat situations, delay of information may result in the failure in war. Thus, security issue of warship systems is quite different from that of traditional information systems.

Hans Liwång et al. analyzed ship security to improve security decision from the angle of risk [3]. Richard G. Bensing et al. developed a template security policy to improve the security of shipboard systems after analyzing the threats and vulnerabilities [4]. SHENG Jin-lu et al. proposed a ship security assessment based on information entropy[5]. These works researched security issue of warship systems from the view of intrusion prevention. But in the real world, no system is ever completely secure. Thus, security protection of warship systems should be resilient, and the running security of warship systems deserve more attention. First of all, Security protection of warship systems should ensure that all critical functions perform well. Meanwhile, security protection should mitigate the effect of security protection on system functions. This is, the aim of security

protection is to control the security risk of warship systems within the acceptable range and keep the overall system secure.

This paper proposes a novel intrusion tolerant control approach based on system theory for warship systems which can balance security and performance of warship systems to minimize the risk when facing intrusion. The intrusion tolerant control approach provides a set of reusable security services as an architectural solution with a close loop control structure. According to the approach, security solution is implemented by embedding into warship systems with consideration of domain features of warship control, and it includes services that: 1) monitor and detect the real-time and security-related measurements from the field control systems being protected, 2) based on system configuration, select appropriate security services according to the detection result, and 3) reallocate tasks and reconfigure communication schedule to tolerate intrusion.

The outline of the paper is as follows. Section 2 analyses the potential attacks and the intention of these attacks, and then constructs the attacker model for warship systems. In section 3, an intrusion tolerant control approach that can provides a set of reusable security services as an architectural solution with a close loop control structure. The concluding remarks are made in Section 4.

Security Issues in Warship Systems

Potential attack

With the development of ICT, the scale of warship systems is more and more large, and system functions become more and more complex. The problem about the cyber security of warship systems is becoming more and more severity. Fig. 1 shows a general hierarchical architecture of warship systems, which is composed of a fiber-optic ring network and some subsystems. Generally, a subsystem consists a data interface unit (DIU) and some intelligent control unit (ICU). The DIU and ICUs in a subsystem are connected via a filed network.

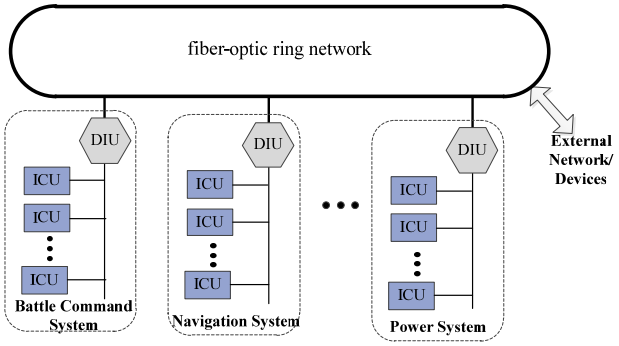

Fig.1 A general hierarchical architecture of warship systems

As shown in Fig.1, external network/devices can access the warship system via the fiber-optic ring network. It also raises concern that warship system is now vulnerable to remote attacks with potential catastrophic consequences. There are many potential attacks for warship systems, and they can be categorized into the following three types.

1) Outside attacks. In the past, a warship system is similar to an information island, and security issues of the whole system is seldom considered[6]. Now, guided by the Network-Centric Warfare theory, external communication of warship systems, communication between warship systems and communication between headquarters and warship systems, become more and more frequent. Consequently it leads to the outside security threats for warship systems.

2) Inside attacks. The inside attack is also a major factor of security threats for warship systems. Warship systems are so complex that misoperations from submariners cannot completely be avoided. Some misoperations can result in serious consequences, which can be regarded as inside attacks for warship systems. On the other hand, submariner who is unsatisfied with government may maliciously attack the systems in warship. In additional, malicious codes injected in the warship systems through removable storage devices can attack system automatically.

3）Future attacks. Besides the above two types of attacks, there may be some new-style attacks

for warship systems with the development of ICT. Furthermore, the emerging concepts of warship, such as intelligent ship, sapiential ship, will broaden the attack surface. An automotive system exhibits multiple access opportunities from outside(e.g., by exploiting security vulnerabilities in wireless communication systems or by encompassing the use of manipulated media discs) or inside the warship.

Due to the special structure and function of warship, the cyber security problem in the systems is not just a security problem but also a safety problem.

Attacker model

As shown in Fig.1, a warship system composes of some subsystems which have similar network structure, thus, we focus on a subsystem in an automobile, shown in Fig.2.

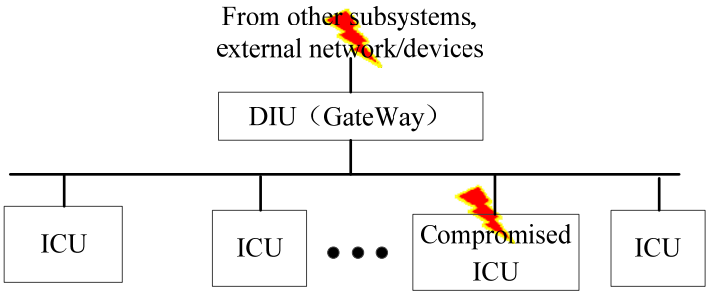

Fig.2 A general subsystem in a warship system.

In our attacker model, we assume that an attacker can access the in-ship network from the Internet, and some hosts may have been compromised. Through the gateway, intrusion from external network/devices or from other compromised subsystems can access to this subsystem. On the other hand, attack can also be launched through compromised node. Thus, as shown in Fig. 2, there are two the attack points where the attacker can attack the subsystem.

A subsystem in warship runs in limited resources environment, and has greater timeliness and availability. And the consequence of security accident may be serious, and even unable to be accepted. So, next section proposes an intrusion tolerant control approach for warship systems which can keep system running normally when intrusion occurs.

Intrusion Tolerant Control for Warship Systems

Fig. 3 shows an example high-level model that takes into account the above system features. This model consists of the following main models: *access control*, *monitor and detection*, *security decision*, *control and recovery*. The *access control* is used to prevent illegal access from external internet or other subsystems. The other three models are responsible for intrusion protection in the subsystem. The *monitor and detection* gathers some measurements from the subsystem. When system anomaly is detected, it will inform *security decision* to select suitable security services. Finally, *control and recovery* is responsible for system reconfiguration and policy adjustment of *access control* according to the selected security services. Through this closed-loop control, security system achieve to tolerate cyber-attacks for warship systems.

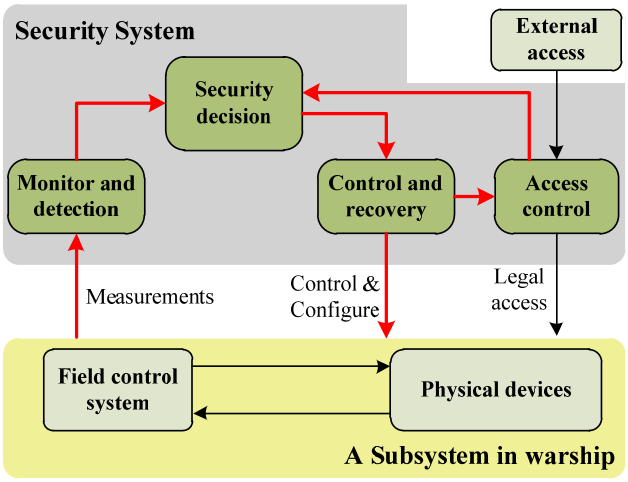

Fig.3 Template Security of a subsystem in warship

Access control at application level

The *access control* is realized through the information flow control at application level. It regulates what a user/device can do and what the programs are allowed to execute on behalf of the user/device[7]. The behavior of accessor can be represented with a quadruple <*subject*, *object*, *signal*, *operation*>. The *subject* is used to characterize the accessor, which can be an IP address, and the *object* is similar to the *subject*. The *signal* is used to represented an action object, and the *operation* is a specific operation actions whoes value can be *create*, *delete*, *read*, or *write*. A data-oriented access control list is used to store the permitted quadruples.

Monitor and detection

The *monitor and detection* acquires measurements from target system and detects systems anomaly. As the security protection cannot effect the target system, so deep packet inspection technology is used to extract measurements in packets from networks.

Intrusion detection technology is usually used to detect systems anomaly, which in general can be classified into two types: signature-based intrusion detection and anomaly based intrusion detection[8]. The field control systems in warship usually have a relatively fixed structure and predictable behaviors, and they also operate in resource constrained environments and achieve real-time/deterministic performance. Thus, anomaly based intrusion detection technology is used to detect systems anomaly in the *monitor and detection*.

In warship systems, there are many redundant information. So, data consistency checking is used to check measurements of redundant information, and the processes of the data consistency checking is shown in Fig. 4. On the other hand, measurements is also checked by critical state detection. The critical state detection calculate the state distance between the real-time state formed by real-time measurements and the corresponding critical states. If the state distance exceeds the corresponding threshold, an anomaly is confirmed.

Security services selection

After a system anomaly is confirmed, security services are selected to insure the system to run normally, which is a decision process. The *security services selection* consists of the following steps.

(1)Decision of abnormal node in external network

The *security services selection* receives anomaly results from the *access control*, and determine the abnormal node in external network, shown in Fig. 4.

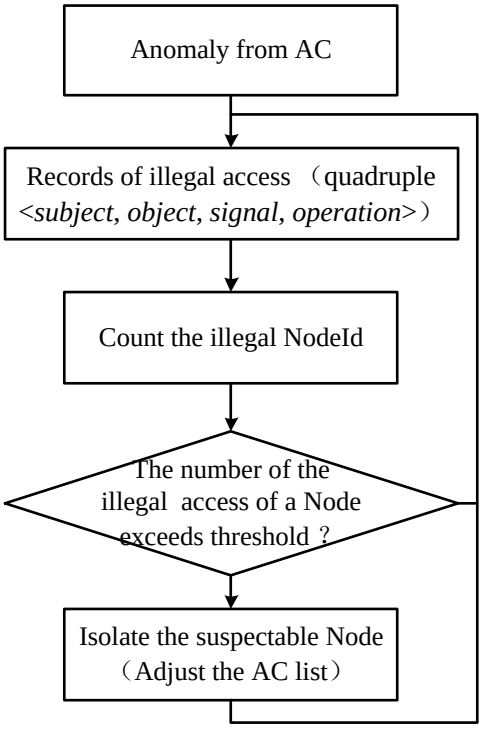

Fig. 4 Decision flow of abnormal node in external network

(2)Encryption algorithm selection

The information flow of warship systems is complex, and there are many messages exchanged in the systems. These messages have different security requirements and availability requirement. Thus, appropriate encryption algorithms should be selected for each message. The encryption flow of meaasge at application level is shown in Fig. 5.

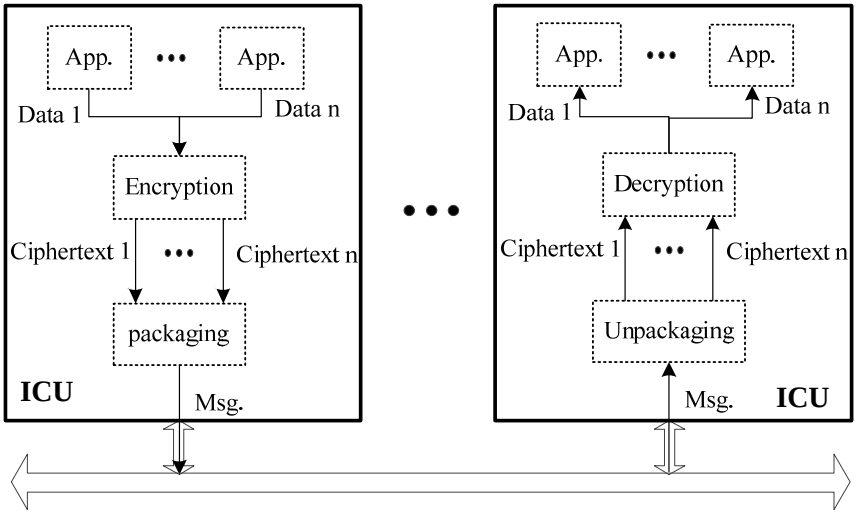

Fig. 5 Encryption flow of meaasge at application level

Encryption algorithms used in encryption flow is determined by their security requirement, real-time requirement and safety degree. The security requirement and real-time requirement are obtained through application specification. The safety degree is determined through safety situation assessment[9] according to the anomaly detection results from the *monitor and detection* and the *access control*.

Recovery and control

After security services are selected, the following steps are carried out to reconfigure and recover the system.

(1)Tuning access permissions

When an abnormal access from external network is confirmed, the access control list should be tuned. Firstly, abnormal nodes are removed from access control list. Then, if abnormal access for some data is continued, a mandatory control to the data is carried out. Table 1 shows the data types,

corresponding security sensitivity and mandatory control in warship systems. For example, the control-related data have *High* security sensitivity, and when it is mandatory controlled, it is not allowed to be accessed.

Table 1 Mandatory control of data

Data type	Security sensitivity	Mandatory control
Control-related data	High	NULL
Command interaction data	Medium	write
Network management data	Low	write /read

(2) Task rescheduling

Generally, tasks in warship systems are scheduled through table driven schedule approach. As shown in Fig. 5, encryption algorithms are real-time changed. So, all tasks should be rescheduled. The parameters of new tasks can be obtained in advance offline.

Conclusion

With the maturing of the Network-Centric Warfare theory, security issue of warship systems has been emerged gradually, and it can reduce operational effectiveness of warship. However, existing researches that focused on warship systems have remained limited and they did not consider the problem from the global perspective. In this paper, from the perspective of system theory, an intrusion tolerant control approach that can provides a set of reusable security services as an architectural solution is proposed after analyzing the security issues of warship systems. According to the approach, security solution can be implemented by embedding into warship systems with consideration of domain features of warship.

References

[1] B. WANG and H.-t. LIN, “Study on security & secrecy demand of ship communication system [j],” Information Security and Communications Privacy, vol. 10, p. 039, 2011.

[2] A. K. Cebrowski and J. J. Garstka, “Network-centric warfare: Its origin and future,” in US Naval Institute Proceedings, vol. 124, no. 1, 1998, pp. 28～35.

[3] H. Liwång, “Risk-based ship security analysis–a decision-support approach,” Ph.D. dissertation, Chalmers University of Technology, 2015.

[4] R. G. Bensing, “An assessment of vulnerabilities for ship-based control systems,” Ph.D. dissertation, Monterey, California. Naval Postgraduate School, 2009.

[5] Ship Security Assessment Based on Information Entropy

[6] Lopez J, Alcaraz C, Roman R. Smart control of operational threats in control substations. Computers & Security, 2013, 38:14～27.

[7] K. Gill, S. H. Yang, W. L. Wang. Secure remote access to home automation networks. IET Information Security, vol. 7, no. 2, pp. 188～125, 2013.

[8] W. Xiong, H. P. Hu, N. X. Xiong, L. T. Yang, W. C. Peng, X. F. Wang, et al. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. Information Sciences, vol. 258, February, pp. 403～415, 2014.

[9] Cárdenas A A, Amin S, Lin Z S, et al. Attacks against process control systems: Risk assessment, detection, and response. in: Proceedings of Proceedings of the 6th International Symposium on Information, Computer and Communications Security (ASIACCS). Hong Kong, China: ACM, 2011. 355～366.