Available online at www.sciencedirect.com

ScienceDirect

Publishing Services by Elsevier

International Journal of Naval Architecture and Ocean Engineering 8 (2016) 423–433

http://www.journals.elsevier.com/international-journal-of-naval-architecture-and-ocean-engineering/

Enforcement of opacity security properties for ship information system☆

Bowen Xing [a,*], Jin Dai [b], Sheng Liu [c]

[a] College of Engineering Science and Technology, Shanghai Ocean University, Shanghai, 201306, China

[b] Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA

[c] College of Automation, Harbin Engineering University, Harbin, Heilongjiang, 150001, China

Received 23 November 2015; revised 10 May 2016; accepted 11 May 2016

Available online 21 July 2016

Abstract

In this paper, we consider the cybersecurity issue of ship information system (SIS) from a new perspective which is called opacity. For a SIS, its confidential information (named as "secret") may be leaked through the working behaviors of each Distributed Control Unit (DCU) from an outside observer called an "intruder" which is able to determine ship's mission state by detecting the source of each data flow from the corresponding DCUs in SIS. Therefore we proposed a dual layer mechanism to enforce opacity by activating non-essential DCU during secret mission. This mechanism is calculated by two types of insertion functions: Safety-assured insertion function (f_{IS}) and Admissibility-assured insertion function (f_{IA}). Due to different objectives, f_{IS} is designed to confuse intruder by constructing a non-secret behaviors from a unsafe one, and the division of f_{IA} is to polish the modified output behaviors back to normal. We define the property of "I_2−*Enforceability*" that dual layer insertion functions has the ability to enforce opacity. By a given mission map of SIS and the marked secret missions, we propose an algorithm to select f_{IS} and compute its matchable f_{IA} and then the DCUs which should be activated to release non-essential data flow in each step is calculable.

Keywords: Ship information system; Enforcing opacity; Insertion function

1. Introduction

With the development of ship technology, the ship system tends to be integrated and distributed which leads to a new research area named ship information system (SIS). Although different ships have different functions, all definitions found in literature for a SIS have one key feature in common. As firstly defined by us in Liu et al. (2014), a typical SIS is composed by several independent subnets (sensor networks, display networks, etc.) and a total ship communication network which can exchange information (reference input, plant output, control input, etc.) among subnets and systems. Similar to a networked system, SIS research is categorized into the following two parts which are Information processing and Information transmission. The research on Information processing is mainly focused on service ability such as controllability, observability (Xing et al., Zhi) and reachability (Xing et al., 2015), etc. Meanwhile, the core attention on Information transmission is service quality, such as anonymity (Wang and Wang, 2014; Kumari and Khan, 2014) and secrecy (Rabbachin et al., 2015; Liang et al, 2009), etc. The application of these research results can ward off network intrusion and attacks, prevent the content of data flow from leaking. However, for a

☆ Fully documented templates are available in the elsarticle package on CTAN.

* Corresponding author.

E-mail address: xbwheu@hotmail.com (B. Xing).

Peer review under responsibility of Society of Naval Architects of Korea.

http://dx.doi.org/10.1016/j.ijnaoe.2016.05.012

SIS, if the functions of each Distributed Control Units are confirmable, the on-going mission may also be revealed by detecting the publishing actions of each DCU. In order to find a solution of protecting some important mission states in SIS, a new property of Information Flow named as opacity should be considered in cybersecurity of SIS. Opacity was first introduced in computer science literature (Mazaré, 2004) and later investigated in Discrete Event System (DES) framework (Lin, 2011; Takai and Oka, 2008; Cassez et al., 2012; Wu and Lafortune, 2013; Falcone and Marchand, 2015; Bryans et al., 2008).

Without losing generality, the model of SIS mission state can be also formulated as a DES and SIS is said to be opaque if its " secret" missions can be hidden from an undesirable external observer which is referred as intruder. The intruder is modeled to have full knowledge of the structure of SIS (include the function and characteristic of the data flow from each DCU), but can not obtain the content of each data flow. And the SIS is said to be opaque if for any secret mission, there must exist at least one other non-secret mission that observationally equivalent from the intruder. Due to the specificity of SIS, here we only consider about Current-Mission State Opacity (CMSO) which is similar to Current-State Opacity-SCO in Bryans et al. (2008). For those systems which are not SCO, the mainly research point is ensuring opacity, which is mainly approached as Supervisory Control Theory (SCT) (Lin, 2011; Dubreil et al., 2010; Ben-Kalefa and Lin, 2011) and enforcement (Falcone and Marchand, 2015). As what has been contrasted by Jacob et al. (2015), the difference between SCT and enforcement is the way they preserve secret, SCT constrains the happening of secret by the controller while enforcement does not restrict system's behaviors but modifies its output to hide the reveal of secret. As there may exist multi-information in a single data flow, not only for secret mission but also for normal mission, it is inadvisable to protect secret mission by restricting the publish of data flow. Thus we research on the enforcement of CMSO. There exist three basic implement methods to enforce opacity by modifying the output information to the observer, 1) deleting events, 2) adding events and 3) delaying the output. Among them, addition of events is a total non-intrusive approach and can be used in such system which a secret is not time-independent. This approach named as "insertion functions" is first proposed by Wu and Lafortune in Wu and Lafortune (2012).

As shown in Fig. 1, regarding as a monitoring interface at system's output, the insertion function has the ability to modify the actual output behavior with fictitious factors by inserting additional observable events. The basic idea to design a suitable insertion function selection algorithm which can cheat the intruder to omit the actual secrets meanwhile the intruder could not learn the setting rule by analyzing the modified output observation with system's structure.

In this paper, we follow and expand the basic design rules of insertion functions which has been presented in Wu and Lafortune (2014). Due to different objectives, f_{IS} is designed to confuse intruder by constructing a non-secret behaviors from a unsafe one, and the division of f_{IA} is to polish the modified output behaviors back to normal. We define the property of "I_2–*Enforceability*" for dual layer insertion functions if they have the ability to enforce opacity. By a given mission map of SIS and the marked secret missions, we propose an algorithm to select f_{IS} and compute its matchable f_{IA} and then the DCUs which should be activated to release non-essential data flow in each step is calculable.

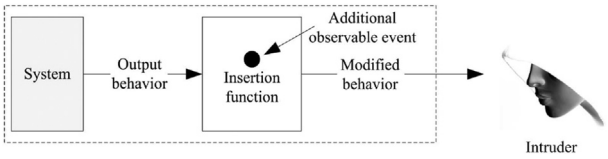

Fig. 1. The insertion mechanism.

To the best of our knowledge, security and opacity issues of ship mission state in SIS have never been addressed so far.

The rest of the paper is organized as follows. Section 2 introduces the typical SIS mission model, and defines the enforcement opacity problem which is introduced in Section 3. Section 4 presents the proposed dual insertion function structure which used in the enforcement of opacity. Section 5 concludes the paper.

2. Structure of SISM

2.1. Basic structure of SIS

As shown in Fig. 2, the structure of SIS we proposed here is similar to Raytheon Companys Total Ship Computing Environment (TSCE) which is one of late-model for USS Zumwalt (DDG-1000). The SIS network is a Double-loop Broadcast Network which connect C2I (Command, Control & Intelligence) system, 3 parallel-hosts monitoring system, Human–Computer Interface (HCI) and dozens of DCUs which are located throughout the ship. And every sensor and actuator which belongs to different systems in the ship are added in this network through remote terminal units (RTUs) with the most nearby DCU. That means a data flow D_m released by DCU_m may include kinds of information that are needed in different systems. As a Broadcast Network in this structure, for each component in SIS, to detect the releasing of data flow is much easier than detecting receiving actions. And according to different sequences of releasing action from each DCU, the on-going mission of the ship is able to be determined.

2.2. SIS mission (SISM) models

If we consider each releasing action as an controllable event, the mission states of SIS can be modeled as deterministic finite state automaton, $G = (X, E, E_{int}, E_{host}, f, f_c, X_0)$, which includes a set of mission states X, a set of release action