Cyber Security of the Autonomous Ship

Sokratis K. Katsikas
Center for Cyber and Information Security
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
P.O. Box 191, Gjøvik N-2802, Norway
+4791138581
sokratis.katsikas@ntnu.no

ABSTRACT
In this keynote talk we give an overview of the state of play of cyber security of the autonomous ship. We discuss the generic system architecture of an autonomous ship, as well as threats, vulnerabilities and risks against such a generic architecture, and we argue for the need to employ a holistic approach to ensuring the cyber security of the autonomous ship.

CCS Concepts
• General and reference~Surveys and overviews

Keywords
Cyber security; autonomous ship; cyber risk.

1. INTRODUCTION
The shipping industry has been a very conservative one. Consequently, it has been slow in adopting technology; Information and communications technology (ICT) on board ships is not an exception to this. However, because the shipping industry is also a very competitive one and because the cost of adopting ICT is very low compared to other types of costs, ICT adoption rates on board ships are increasing at an impressive rate during the past few years. Today's leading manufacturers and ship operators want to innovate using the latest ICT systems, going beyond traditional engineering to create ships with enhanced monitoring, communication and connection capabilities – ships that can be accessed by remote onshore services, anytime and anywhere [1]. As a result, Rolls-Royce envisages a remotely operated local vessel, with reduced crew and remote support and operation of certain functions being the first stage and in operation by 2020 and autonomous unmanned ocean-going ships to be put in operation by 2035 [2].

The concept of an unmanned ship is not new; visions of such ships were reported as early as the 1970's and have continued to appear regularly since [3]. Today's concept of the unmanned ship implies two generic alternatives for an autonomous ship:

- the *remote ship* where the tasks of operating the ship are performed via a remote control mechanism e.g. by a shore based human operator; and
- the *automated ship* where advanced decision support systems on board undertake all the operational decisions independently without intervention of a human operator [4].

The adoption of ICT in any industry has always been accompanied with an enlargement and diversification of the risks that the industry is facing, with existing risks being increased and new risks being introduced. This is mainly due to the fact that whereas traditional operations were designed with no need for cyber security in mind, modern ICT-enabled operations are allowed to be accessed and controlled through the industry's enterprise information system, through interfaces that are rarely adequately secure. As the enterprise system is usually connected to the Internet, the end result is that security-unaware systems, such as e.g. control or navigation systems are made accessible to outsiders. Therefore, it is not surprising that almost all known attacks against industrial control systems have been launched by first compromising the enterprise system and subsequently using it as a stepping stone to attack the control system.

In this keynote talk we give an overview of the state of play of cyber security of the autonomous ship. The remaining of the paper is organized as follows: In Section 2 we discuss the generic system architecture of an autonomous ship. In section 3 we discuss threats, vulnerabilities and risks against such a generic architecture and argue for the need to employ a holistic approach to ensuring the cyber security of the autonomous ship. Section 4 concludes the paper.

2. AUTONOMOUS SHIP: SYSTEM ARCHITECTURE
A system architecture is a conceptual model that defines the structure, behavior, and more views of a system [5]. A system architecture can comprise system components that will work together to implement the overall system. In the case of the autonomous ship these components depend significantly on the level of autonomy that the ship has. Levels of autonomy are often used to describe to what degree the ship can act on its own. A taxonomy of such levels for the general case of machine autonomy is the one described in [6]; ten levels of autonomy are envisaged therein, ranging from Level 1 (The computer offers no assistance, human is in charge of all decisions and actions) to Level 10 (The computer does everything autonomously, ignores human). This taxonomy is used [7] in the context of the Advanced Autonomous Waterborne Applications (AAWA) initiative. Lloyd's have also made available their own autonomy levels and their level assignment procedures and workflow, specific to what they call "cyber ship"; seven levels of autonomy are envisaged therein, ranging from AL0 (Manual – no autonomy function) to AL6 (Fully autonomous) [8]. Within the MUNIN project (www.unmanned-ship.org), a simplified classification scheme has

CPSS'17, April 2, 2017, Abu Dhabi, United Arab Emirates.
ACM ISBN 978-1-4503-4956-7/17/04.
DOI: http://dx.doi.org/10.1145/3055186.3055191

been developed to describe the autonomy of the system as the ship and the shore control center go through different states [9].

The level of autonomy affects the system architecture, which is in turn a central element in the analysis of the cyber security issues involved with autonomous ships. Hence, it is not possible to discuss such issue in detail, without specifying the exact architecture in question. However, it is possible to provide an overview, by considering a generic system architecture, such as the one used in the context of the Smart Ship Application Platform Project (http://www.e-navigation.net/index.php?page=ssap-smart-ship-application-platform). The main elements of the architecture are the ship, which communicates over broadband connections with two data centers on the shore, one in Europe and one in Asia. These in turn communicate with the end users through the service providers' systems. Another architecture has been defined by the MUNIN project [9].

3. THREATS, VULNERABILITIES, RISKS

Regardless of the exact level and form of autonomy, cybersecurity is a serious issue for autonomous ships, because of their increased dependence on ICT for ship control; the increased integration of control systems; the increased connectivity of the ship's control systems to onshore monitoring systems; and the accessibility of such systems to the Internet, through the relevant onshore enterprise information systems. Although the cybersecurity of the autonomous ship has been widely acknowledged as an area of significance [7], [10] the literature is rather poor in such works.

The Guidelines on cyber security onboard ships [11] aim to "offer guidance to shipowners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships." They are basically management guidelines on how to approach the cybersecurity issue in the context of shipping. Interestingly, they include an annex listing onboard target systems, equipment and technologies, and another on shipboard networks; these can be used as input to an asset-driven cyber risk assessment exercise.

Such a risk assessment has been carried out in [12], using the IMO's Formal Safety Analysis method. As its name suggests, this is a scenario-based, safety-oriented method, hence not fully able to grasp cyber security issues that are not necessarily related to safety.

The starting point for developing a framework for securing the autonomous ships of the future is the assessment of the risks that they will face. In doing so, it is important to realize that security, safety and resilience must be examined together, as they constitute attributes of the autonomous ship thought of as a system of systems, particularly cyber physical systems. Even though unified methods for assessing security and safety risks do exist, they have been tailored-made to specific systems (e.g. railways, the smart grid, nuclear power plants, etc.); none exists for the autonomous ship case. Note that the complexity of the ship environment, comprising equipment from different vendors, with long lifecycles, opaque to the user, using proprietary communication protocols, legacy systems with little or no networking capability, etc. does present similarities, from a cyber security viewpoint, to other cases, such as e.g. the industrial Internet of Things, but also calls for custom designed cyber security solutions.

This is because of several reasons, including the limited connectivity of the ship to the shore and to other ships in the area, the inability to perform maintenance operations at any time, the speed and the inertia of a moving ship, the maneuvering capability, etc.

The autonomous ship interacts heavily with its environment and with humans. This means that effective cyber security solutions should come as the result of a holistic approach, encompassing technology, people and processes.

Once again, ICT has found its way in a traditional industry. Once again, it is being introduced with the goal of "getting it to work". Unless new systems are built with security (and privacy) in mind right from their design phase, we will soon be facing cyber security issues in the shipping industry, similar to those that we are experiencing in other industries that have adopted ICT without properly addressing cyber security issues.

4. CONCLUSION

We have provided an overview of cyber security in the context of the autonomous ship concept. Even though this is a concept that is taking up speed very quickly, its cyber security issues have not yet been given the appropriate attention. More research will be required to provide viable solutions to these issues.

5. REFERENCES

[1] Lloyd's Register, "Cyber-enabled ships," 2016.

[2] Rolls-Royce, "Autonomous ships. The next step," 2016.

[3] V. Bertram, "Technologies for low-crew/no-crew," in *Forum Captain Computer IV*, 2002.

[4] "MUNIN - Maritime Unmanned Navigation through Intelligence in Networks," 2016. [Online]. Available: http://www.unmanned-ship.org/munin/about/the-autonomus-ship/. [Accessed 23 02 2017].

[5] H. Jaakkola and B. Thalheim, "Architecture-driven modelling methodologies," in *Information Modelling and Knowledge Bases XXII*, 2011.

[6] R. Parasuraman, T. Sheridan and C. Wickens, "A Model for Types and Levels of Human Interaction with Automation," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* vol. 30, no. 3, pp. 286-297., 2000.

[7] Rolls-Royce, "Remote and Autonomous Ships. The next Steps.," Rolls-Royce Marine, 2016.

[8] Lloyd's Register, "Cyber-enabled ships. ShipRight procedure – autonomous ships," Lloyd's Register, 2016.

[9] Ø. J. Rødseth and Å. Tjora, "A System Architecture for an Unmanned Ship," in *13th International Conference on Computer and IT Applications in the Maritime Industries*, Redworth, 2014.

[10] G. Reilly and J. Jorgensen, "Classification Considerations for Cyber Safety and Security in the Smart Ship Era," in *Smart Ships Technology* , London, 2016.

[11] BIMCO, "The Guidelines on Cyber Security Onboard Ships," BIMCO, Bagsvaerd, 2016.

[12] Ø. Rødseth and H. Burmeister, "Risk Assessment for an Unmanned Merchant Ship," *TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation,* vol. 9, no. 3, pp. 357-364, 2015.