Integrity of Integrated Navigation Systems

Mass Soldal Lund*, Jørgen Emil Gulland†, Odd Sveinung Hareide‡§, Øyvind Jøsok*¶, Karl Olav Carlsson Weum†
*Norwegian Defence University College, Cyber Academy
†Norwegian Defence University College, Royal Norwegian Naval Academy
‡Royal Norwegian Navy, Navigation Competence Center
§Norwegian University of Science and Technology, Joint Research Program in Nautical Operations
¶Inland Norway University of Applied Sciences, Faculty of Social and Health Sciences

***Abstract*—Computerized systems are revolutionizing modern ships' bridges and maritime operations. Central components in this are Integrated Navigation Systems (INS) and Electronic Chart Display and Information Systems (ECDIS) which provide the maritime navigator with the ship's position and displays it in electronic charts. The integrity of these systems if of great importance for the safety and security of maritime operations, but is a little studied topic. In this paper we investigate the integrity of navigation systems, though a survey of INS's on the market (n=22), a survey of known cyber incidents and attacks targeting the integrity of navigation systems, and a discussion of cryptographical measures to ensure the integrity of navigation data in INS's.**

I. Introduction

Modern ships are equipped with Integrated Bridge Systems (IBS). An IBS is "a combination of systems which are interconnected in order to allow centralized access to sensor information or command/control from workstations, with the aim of increasing safe and efficient ship's management by suitably qualified personnel" [1]. In other words, an IBS is an integration of systems that enables monitoring and control of a ship and its operation from the bridge. The systems integrated usually include navigation systems, communication systems and engine control systems, but may also be surveillance systems (CCTV), entertainment systems, and in the case of naval ships, damage control systems and weapon systems. These computerized ship's bridges represent a technological revolution for the maritime navigation. Historically, the main task for the navigator was to *find and fix* the position of the vessel, while today's navigator *monitors* the vessel's position obtained by navigation sensors and presented by navigation software [2].

This paper concentrates on navigation systems. Maritime navigation systems connected through onboard networks are referred to as Integrated Navigation Systems (INS) [3]. In an INS, sensors used in navigation such as GPS, gyroscope, depth sensors, etc. are connected to workstations equipped with software for displaying electronic charts, known as Electronic Chart Display and Information Systems (ECDIS) [4]. The ECDIS software shows the position of the vessel in the chart using data from the navigation sensors, as well as the positions of nearby vessels based on data received through the Automatic Identification System (AIS) [5]. In addition, ECDIS software has functionality for route planning and route monitoring.

It seems obvious that the integrity of INS's is of great importance for safe and secure operations in the maritime domain [2], [6], [7]. Still, little concrete is said about this in the emerging literature on maritime cyber security. Much of what is written is on a general level, e.g. applying general cyber security considerations to maritime systems, or focusing mainly on policy (see e.g. [8] or [9] for several examples of both categories). In particular, references to reported incidents, attacks and vulnerabilities are scarce and the same few examples are cited again and again.

In this paper we present a survey of the security of INS's, with an emphasis on integrity. We start by surveying INS's available on the market (n=22) in Section II. Based on the findings we describe a prototypical INS. Then, in Section III we survey reported attacks and incidents targeting the integrity of INS's, while in Section IV we discuss cryptographic countermeasures. Finally, in Section V we provide conclusions.

II. Integrated Navigation Systems (INS)

An INS is an integration of navigation sensors with workstations equipped with ECDIS. This section documents a survey into INS's. We start by describing the method of the survey before we go on to present the findings. Finally, the findings are used to define a prototypical INS.

A. Method

One INS was studied in detail as part of the development of a maritime cyber security demonstration (see Section III). For this INS we had access to an installation of the system, experts on the system, technical documentation, and capture of internal network traffic (see [2], [10] for details). Through Internet searches we identified further 34 providers of navigation and bridge systems and gathered as much information of their systems as possible. This resulted in a catalog of mostly brochures, but in some instances also quite detailed technical documentation. These brochures and other documents were analyzed to extract information on a number of topics (identical to the sub-sections of Section II-B).

Among the 35 providers there is a wide range in what is offered, from full ship integration to navigation sub-systems. In theory it makes sense to view an IBS as a system of systems with the INS as one of its systems. I practice, however, not all providers make a clear distinction between an INS and an IBS – perhaps because navigation is such an integral part of the daily work on a bridge. In order to have a criterion for the inclusion or exclusion of any given provider's system (henceforth referred to as a "solution") in the study, we decided that the minimum requirement to be included was that a solution provide at least navigation hardware (e.g. workstations and sensors) and navigation software (e.g. ECDIS). This can be seen as a working definition of INS's for the purpose of this study, even though it may differ from definitions given by the International Maritime Organization (IMO) [3].

Of the initial 35 solution we excluded one providing maritime computers but no navigation system as such (e.g. no navigation software), one providing ship integration systems but no navigation system, and one providing navigation software but no hardware. Of the remaining 32 solutions, we judged that for ten of them the information we were able to find was too scarce to provide useful answers. These ten solutions were therefore excluded from the study, and we ended up with a selection of 22 solutions. A list of the providers of the included solutions is given in the Appendix.

B. *Findings*

In the following the findings of the survey are presented, divided into six topics: Workstations, sensor integration, network, radar, autopilot, and Internet connection.

1) Workstations: All 22 solutions provide workstations for the crew of the bridge. These are invariably standalone computers running software locally, i.e. what we would think of as thick clients. In five of the solutions these workstations are ECDIS consoles, i.e. workstations used for chart display only, while 15 of the solutions provide multi function workstations (MFW). MFW's, often also called multi function displays (MFD), are workstations which allow the operator to switch between ECDIS display, radar display and conning display. For the remaining two solutions it is unknown whether the workstations are ECDIS consoles or MFW's. Some of the solutions are bridge systems that integrate other systems in addition to navigation systems, but it seems that in most cases MFW's are still navigation workstations providing ECDIS, radar and conning displays, while other functions such as engine control or CCTV have separate workstations/consoles.

In eleven of the solutions, the operating system of the workstations is specified as Microsoft Windows, nine as Windows XP, Windows Vista and/or Windows 7, two as just Windows. While it must be take into account that many of the documents collected in the survey are several years old, this finding is consistent with reports that Windows XP is often encountered on operating ships [7], [11]. For one of the solutions, the operating systems is specified as Linux, while for the remaining ten, the operating system cannot be determined from the available information.

2) Sensor integration: A main feature of an INS is the integration, interpretation and presentation of sensory input in navigation software such as ECDIS. By sensor integration we understand the means by which data from sensors such as GPS, gyroscope, echo sounder or AIS receiver are provided to the workstations. These sensors have serial output, usually conforming to the IEC 61162-1/NMEA 0183 standard for maritime navigation devices [12]. The large majority (18) of the solutions in the study provide some kind of sensor integration unit, though given different names such as Data Distribution Unit, Data Acquisition Unit, Data Collection Unit, Sensor Concentration Unit, etc. Common for these units is that they receive data from the navigation sensors though serial interfaces and provide a single source of sensory data for the workstations. Three of the solutions do not provide sensor integrator units and thus the sensors have direct serial connections to the workstations.

3) Network: One of the solutions is a standalone ECDIS workstation with sensors connected to serial ports. However, any solution more complex than this will need various components communicating somehow; thus the rest of the solutions are networked in one way or another. Their networks connect sensor integration units to the workstations, they interconnect workstations for exchange of data (e.g. sensor data, routes and chart updates), and they connect the INS to other onboard systems such as the ship's communication system. The exact configuration varies, but in 19 of the solutions the network is some sort of IP-based Ethernet LAN. Also in the standalone solution, the workstation is fitted with Ethernet ports enabling IP-based networking. That IP-based Ethernets are the dominating networking technology in navigation networks is also confirmed by [13]. One solution employs a CAN-bus network, a multi-master serial bus system originally developed by the automotive industry for use in cars [14]. In the remaining solution the network protocol is unknown. In nine of the solutions, the networks connecting sensor integration units to workstations are described as dual or redundant.

Which communication protocols utilized in the navigation networks are to a large extent unspecified in the information collected, but TCP is used in at least three solution and UDP in at least six solutions, including two which claim to adhere to the IEC 61162-450 "Lightweight Ethernet (LWE)" standard for shipboard networks. LWE is based on a single switched Ethernet and UDP multicast [12], [13].

4) Radar: In 16 of the solutions, integration of radar is described. A radar is different from the other kinds of sensors in an INS in that its data is in the form of pictures, while the other sensors transmit numerical and textual data. For this reason radars are treated differently than other sensors, and only one of the solutions has radar connected to the sensor integration unit. Of the remaining 15, twelve have radars connected to the workstations through a network – either a separate network or the same network as the sensor integration units – while in three of the solutions radar is connected directly to workstations by some other means.

5) Autopilot: A feature described in several (eight) of the solutions is the integration of an autopilot with the route planning functionality of the ECDIS software, i.e. the possibility of having the autopilot steer the ship to follow a route defined in

TABLE I
Summary of Findings

Workstations	Multi function	ECDIS	Unknown
	15	5	2
Operating system	Windows	Linux	Unknown
	11	1	10
Sensor integration	Yes	No	Unknown
	18	3	1
Networking	Ethernet	CAN-bus	Unknown
	20	1	1
Radar	Networked	Direct	Unknown
	13	3	6
ECDIS controlled autopilot	Yes		Unknown
	8		14
Internet connection	Yes		Unknown
	12		10

the ECDIS. This obviously means that the autopilot unit has to receive commands from a workstation, and for a couple of the solutions these commands are described as being transmitted over the network. Unfortunately, the information collected is too sparse say anything more concrete on this topic.

6) Internet connection: Navigation charts are updated on a regular basis; navigation systems therefore need to receive regular chart updates. Furthermore, third party software such as the Windows operating system, is also in need of regular updates and patching. It has been common to install updates using physical media such as CDs or USB flash drives. However, ships are now increasingly being equipped with Internet connections over satellite and/or 4G broadband (for use when sailing close to shore) [11], [15], [16]. Of the solutions in the study, twelve report the possibility of providing the INS with an Internet connection for online chart updates, in most cases by providing a gateway from the network of the INS to the communication system of the ship. In five of the cases it is specified that this gateway is also a firewall.

C. Summary

The findings are summarized in Table I. While there clearly are variations in the concrete configurations of the different INS's, it is also possible to identify a number of typical traits. We use these to describe a prototypical INS, illustrated in Fig. 1. The typical situation is that one or more Ethernets are employed to connect the various components of the INS. The most central of these components are (multi function) workstations and a sensor integration unit (or sometimes two for redundancy), but also radar and autopilot may be connected to the network. In addition there may be a gateway to other systems on the ship, which may also include an Internet connection.

III. Attacks and Incidents

The largest concern with navigation systems has so far been the threat of GPS spoofing, i.e. attacks where navigation systems are fooled by the transmission of false GPS signals [17], [18], [19]. While GPS spoofing can pose a threat toward the integrity of the GPS position calculated by the vessel's GPS receiver and thus a threat toward the integrity of the position displayed in the electronic charts of the vessel, it is not a threat toward the integrity of an INS itself.

However, there also exist examples of threats to the integrity of navigation systems. Electronic charts are often updated using USB flash drives. E.g. [15] reports of a case in which an ECDIS console on board a large tanker was infected by malware when charts were updated in such a way. As we have seen, INS's are increasingly often connected to the Internet for online chart updates. In [11], it is demonstrated how this can be exploited to launch an attack on navigation software.

In a maritime cyber security demonstration conducted in August 2017, we infected a workstation of an INS using a USB device simulating mouse and keyboard. The malware installed could intercept and manipulate GPS coordinates transmitted to the workstation from the sensor integration unit through the network. Thus, the malware could alter the position that appeared in the ECDIS software (see [2], [10] for details). A demonstration similar to ours, though using an Internet connection for delivery, was reported in December 2017 [20].

During our demonstration we also experimented with connecting a small computer (Raspberry Pi) to a switch in the network of the INS. By sending GPS coordinates to the network we showed that the workstations were not able to distinguish these coordinates from GPS coordinates sent by the sensor integration unit. Furthermore, by increasing the frequency of the transmissions we were in effect able to override the sensor integration unit.

IV. Cryptographic countermeasures

The performance standards for INS's from the IMO requires that the systems implement "integrity monitoring" in the form of comparison between redundant sources of navigation data [3]. While this may be sufficient to safeguard against malfunctioning devices, it seems insufficient for protection against cyber attacks; if an INS is compromised there is no reason while data from several sources cannot be manipulated.

In the following we discuss potential crypographic means to protect the integrity of data in an INS. We restrict the discussion to data sent from the sensor integration unit to the workstations, though similar challenges will apply to data sent from radar to workstations, between workstations, or from workstations to the autopilot. Based on the prototypical INS described in Section II-C and the threats implied by Section III, certain requirements for the cryptographic countermeasures can be derived: (1) It seems reasonable to assume that data is distributed by multicast; thus the countermeasures should be suited for multicasts. (2) Although we have documented that Internet connections are increasingly common, this cannot always be assumed; we therefore want the countermeasures to work also for offline/air-gapped systems. (3) The countermeasures should protect against man-in-the-middle attacks (manipulation or fabrication of navigation data). (4) The countermeasures also should protect against

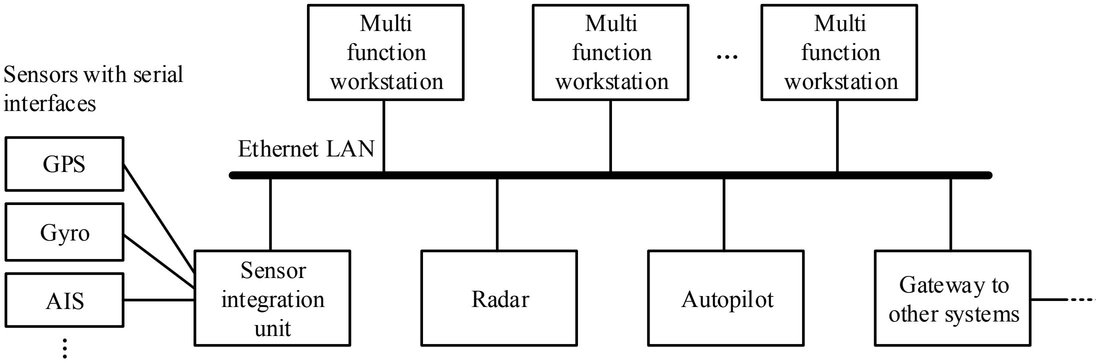
Multi function workstation
Multi function workstation
...
Multi function workstation
Sensors with serial interfaces
GPS
Gyro
AIS
Ethernet LAN
Sensor integration unit
Radar
Autopilot
Gateway to other systems

Fig. 1. Prototypical Integrated Navigation System

replay attacks (navigation data captured and retransmitted at a later point in time). (5) While the sensor integration unit may be assumed to be a hardware device, workstations must be assumed to be regular computers running (potentially old and unpatched) Windows installations; we therefore want the countermeasures to provide protection even when workstations are compromised.

Requirements (1) and (3) point toward a solution using public key cryptography. The sender (i.e. the sensor integration unit) cryptographically signs the messages with a private key while the multiple receivers (workstations) verify the signatures using a copy of the corresponding public key. Requirement (4) can be obtained by including a sequence number or time stamp in the signed messages. Requirement (2) will rule out a standard PKI solution relying on an online Certificate Authority (CA). Drawing on insights from wireless sensor networks (WSN) there seem to be two main options: (A) A simplified PKI solution with a single root CA, or (B) an identity-based signature scheme [21].

In option (A), a key-pair of a secure key sk and a public key pk is generated and installed in the sensor integration unit. pk is signed by the secure key sk_{CA} of an offline root CA (e.g. the INS provider or the shipowner) to produce a certificate C for the sensor integration unit. C is installed in the sensor integration unit and distributed to the workstations through the network. The certificate C_{CA} of the CA is installed in the workstations, which use C_{CA} to verify C and C to verify messages from the sensor integration unit.

Option (B) is an identity-based signature scheme [22]. In this scheme the secret key sk is generated by a offline key generator center (again, the INS provider or shipowner) from a random seed known only to the center, and the identity i of the sensor integration unit (e.g. a serial number or MAC address). As in (A), pk is installed in the sensor integration unit, which uses it to sign messages. In difference from (A), the identity i is in itself the public key; no certificate is needed as its authenticity can be assured by inspection. i is installed in the workstations and used to verify the messages of the sensor integration unit.

One challenge remains. In both cases the integrity of the means of verification (C_{CA} is case of (A) and i in the case of (B)) must be ensured once installed in the workstations, but requirement (5) prevents us from relying on their operating system for this. We suggest the solution may be to store these values in tamper proof Hardware Security Modules (HSM) [23] from which the ECDIS software can retrieve them (or possibly perform the verification in a secure environment). Application of removable HSM's may also ease the distribution and installation of the certificates or identities.

Clearly, none of the options provide a 100 % guarantee for the integrity of the navigation data. Under the assumption that the workstations may be compromised, no such guarantees are possible. If an adversary can manipulate the operating system of the workstations, then he/she can potentially also manipulate the navigation software. However, we still hold that the suggested cryptographic countermeasures will add a layer of security, as we can reasonably assume that the manipulation of an proprietary ECDIS application will be harder than the manipulation of an insufficiently protected Windows installation.

V. Conclusions

As Integrated Navigation Systems (INS) and Electronic Chart Display and Information Systems (ECDIS) become the standard on modern seagoing vessels replacing the traditional paper chars, the integrity of these systems become increasingly important for the safety and security of maritime operations. This paper has made an investigation into the integrity of currently available INS's. This investigation has taken the form of a survey into 22 INS's available on the market, as well as a survey of known cyber incidents and attacks with consequences for the integrity of navigation systems. These surveys show that in general, the integrity of INS's is not sufficiently protected.

Based on the survey of INS's we described a prototypical INS. This prototypical INS was used as the basis for a discussion of cryptographical measures to improve the protection of the integrity of navigation data in INS's. This discussion provided a set of requirements, and two possible option for their fulfillment: A simplified PKI solution and an identity-based solution, both combined with the use of Hardware Security Modules (HSM). While guaranteed security is unobtainable, we believe cryptographic countermeasures as we have sketched represent a potential for improving the integrity of INS's.

Appendix

Navigation system providers included in the study:

Astronautics
Böning
Consilium
Danelec Marine
Furuno
GEM
iXblue
Kelvin Hughes
Kongsberg
L3 MAPPS
Larsen & Toubro
Marine Technologies
Northrop Gruman Sperry Marine
OSI Maritime Systems
Praxis
Raytheon Anchütz
Rolls-Royce
SIMRAD
Tokyo Keiki
Transas
Wärtsilä Valmarine
YALTES

Acknowledgments

The work on which this paper reports was partially funded by the Norwegian Armed Forces CD&E grant EP1710 and partially by the Royal Norwegian Naval Academy R&D grant.

References

[1] *Resolution MSC.64(67): Adaption of new and amended performance standars*, International Maritime Organization (IMO), 1996.

[2] O. S. Hareide, Ø. Jøsok, M. S. Lund, K. Helkala, and R. Ostnes, "Enhancing navigator competence by demonstrating maritime cyber security," *Journal of Navigation*, 2018, to appear.

[3] *Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS)*, International Maritime Organization (IMO), 2007.

[4] *Resolution MSC.232(82): Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS)*, International Maritime Organization (IMO), 2006.

[5] A. Norris, *Integrated Bridge Systems Vol 1: Radar and AIS*. The Nautical Institute, 2008.

[6] C. Demchak, K. Patton, and S. J. Tangredi, "Why are our ships crashing? Competence, overload, and cyber considerations," *Center for International Maritime Security*, Aug. 25, 2017. [Online]. Available: http://cimsec.org/ships-crashing-competence-overload-cyber-considerations

[7] K. D. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," *Engineering & Technology Reference*, Apr. 22, 2016.

[8] *Proceedings of the Marine Safety & Security Council, the Coast Guard Journal of Safety & Security at Sea. Special Issue on Cybersecurity*, vol. 71, no. 4, U. S. Coast Guard, Winter 2014–2015.

[9] J. Direnzo, III, N. K. Drumiller, and F. S. Roberts, Eds., *Issues in Maritime Cyber Security*. Westphalia Press, 2017.

[10] M. S. Lund, O. S. Hareide, and Ø. Jøsok, "An attack on an Integrated Navigation System," in review, 2018.

[11] Y. Dyryavyy, *Preparing for Cyber Battleships – Electronic Chart Display and Information Systems Security*, NCC Group, 2014.

[12] Ø. J. Rødseth, M. J. Christensen, and K. Lee, "Design challenges and decisions for a new ship data network," in *Proc. International Symposium Information on Ships (ISIS 2011)*. Deutsche Gesellschaft für Ortung und Navigation e.V., 2011, pp. 149–168.

[13] M. J. Christensen and Ø. J. Rødseth, "Lightweight Ethernet – a new standard for shipboard networks," *Digital Ships*, Dec. 2010.

[14] CAN in Automation (CiA). CAN knowledge. [Online]. Available: https://www.can-cia.org/can-knowledge/

[15] C. Baraniuk, "How hackers are targeting the shipping industry," *BBC News*, Aug. 18, 2017. [Online]. Available: http://www.bbc.com/news/technology-40685821

[16] *Maritime cyber-risks: Virtual pirates at large on the cyber seas*, Whitepaper, CyberKeel, 2014.

[17] D. Goward, "Mass GPS spoofing attack in Black Sea?" *The Maritime Executive*, Jul. 11, 2017. [Online]. Available: http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

[18] L. Kugler, "Why GPS spoofing is a threat to companies, countries," *Commun. ACM*, vol. 60, no. 9, pp. 18–19, 2017.

[19] M. L. Psiaki and T. E. Humphreys, "GPS lies," *IEEE Spectr.*, vol. 58, no. 8, pp. 26–32, 52–53, 2016.

[20] V. Wee, "Naval Dome exposes vessel vulnerabilities to cyber attack," *Seatrade Maritime News*, Dec. 22, 2017. [Online]. Available: http://www.seatrade-maritime.com/news/europe/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html

[21] K.-A. Shim, "A survey of public-key cryptogtaphic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 2016.

[22] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Advances in Cryptology (CRYPTO'84)*, ser. Lecture Notes in Computer Science, no. 196. Springer, 1985, pp. 47–53.

[23] L. Sustek, "Hardware Security Module," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 535–538.