Information Security in Maritime Domain Awareness

Yılmaz VURAL, Mehmet Emre CIFTCIBASI, Serhat INAN
STM A.Ş Ankara Teknoloji Geliştirme Bölgesi
Bilkent 5. Cad No:6/A Bilkent Ankara
TURKEY

yilmazvural@gmail.com / eciftcibasi@stm.com.tr / sinan@stm.com.tr

ABSTRACT

Maritime Domain Awareness (MDA) is achieved by interoperability of maritime information systems. Maritime information systems consist of platform centric heterogeneous systems. Interoperability has to be achieved by evolution to net centricity from platform centricity by qualified information exchange. There are many challenges on the exchange of the qualified information. Information security is the main challenge for maritime interoperability. Besides traditional information security techniques, new generation solutions are used for maritime interoperability and data sharing. In this paper, MDA environments are briefly defined and challenges on information security are examined in detail. Afterwards, new generation methods for secure exchange of qualified information are analyzed.

1.0 INTRODUCTION

Information systems consist of not only hardware, software and interfaces but also people as a result of the cyber world dynamics. Many information systems are used in different areas such as defense, finance, health, logistics, food and energy. Among those systems that propose a quantitative and qualitative enrichment of information [1], Command control information systems (C2IS), geographical information systems and mission support systems are commonly referred as defense information systems.

In platforms, consisting of information systems in naval environments, the defense technologies and information systems merge into maritime information systems where a platform can be defined as any system (autonomous or networked) that performs a mission with or without operators, has one or more application functions, and contains one or more resources [2].

Maritime information systems provide operational superiority to the armed forces and government agencies by supplying valuable maritime data and necessary inputs to the decision maker in near real time. Accordingly MDA is the concept of achieving the information superiority in maritime activities by enabling the decision maker to plan maritime activities. The main aim of MDA is to establish the common understanding of maritime situation.

Currently most of the maritime information systems are platform centric heterogeneous systems. Although these heterogeneous systems need to share information between each other in order to increase the awareness of local and global authorities/decision makers, their platforms are not loosely coupled [3]. On the other hand in the net centric architectures; the systems should take part in the full bidirectional integration that is often referred to as qualified information exchange rather than the traditional integration that required one way data transport.

Interoperability opens the pathway to the information exchange in maritime environments where heterogeneous systems exist. In maritime systems consisting of heterogeneous sub-systems, the information exchange shall be modeled in such a way that the data protocols and interfaces are well defined. Heterogeneous systems are mostly classified in different security levels depending on the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Security in Maritime Domain Awareness	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **STM A.ª Ankara Teknoloji Geliºtirme Bölgesi Bilkent 5. Cad No:6/A Bilkent Ankara TURKEY**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
Maritime Domain Awareness (MDA) is achieved by interoperability of maritime information systems. Maritime information systems consist of platform centric heterogeneous systems. Interoperability has to be achieved by evolution to net centricity from platform centricity by qualified information exchange. There are many challenges on the exchange of the qualified information. Information security is the main challenge for maritime interoperability. Besides traditional information security techniques, new generation solutions are used for maritime interoperability and data sharing. In this paper, MDA environments are briefly defined and challenges on information security are examined in detail. Afterwards, new generation methods for secure exchange of qualified information are analyzed.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**8**	

information they process. Establishing the information security is a major challenge in the maritime information sub-systems, as data exchange is required between the different security levels.

In this study, qualified information exchange between different security levels and sub-systems is detailed. Solutions for qualified and secure information exchange, including data diode, virtual air gap and Secure Network Node are proposed.

2.0 MARITIME DOMAIN AWARENESS

MDA is a net centric capability model which enables the interoperability of military and civilian organizations that are directly or indirectly responsible for maritime activities that need information superiority for effectively performing their operations. In the research of this study, several definitions of MDA are found in literature, such defining MDA as effective understanding of anything associated with the global maritime environment that could affect the security, safety, economy, or environment [4].

The most recognized definition for MDA is the NATO definition that follows as “Maritime Domain Awareness is an enabling capability which seeks to deliver the required Information Superiority in the maritime environment in order to achieve a common understanding of the maritime situation in order to increase effectiveness in the planning and conduct of operations.” In addition to that, the NATO definition of maritime environment is "The maritime environment comprises the oceans, seas, bays, estuaries, waterways, coastal regions and ports" [5].

In maritime environments huge amount of maritime data is needed to be gathered by government authorities and merchant agencies in order to achieve maritime situational awareness. The maritime data includes all commercial and military maritime vessel information and port records which are composed of ship, cargo and passenger. Maritime data is collected by different sensors such as AIS, radar, electro-optical, RDF, meteorological and hydrological transceivers. These sensors are used by different platform centric systems and each system is an autonomous system [6].

Different autonomous systems are established for similar purposes that cause reiterated investments and reiterated data. These systems cause information repetition and waste of resources. When the maritime systems are observed, many reiterated systems occur as each government agency establishes a similar sensor suite for its own requirements. Establishment of Common Operational Picture (COP) using qualified information collected from heterogeneous systems is one of the best examples that needs interoperability in MDA environments. Information Technology (IT) solutions, such as Service Oriented Architecture (SOA), shall maintain this interoperability that provide the decision support to MDA by contributing to the formation of common operational picture [7].

These autonomous systems are integrated by platform centric approaches and this traditional integration approach supports only one way data transport, not the full bidirectional processable data sharing, which will be abbreviated as “qualified information exchange”. With qualified information sharing and analyses between the related parties Maritime Safety, Maritime Cruise Security, Maritime Economic Activities Safety and Protection of Natural Resources shall be reached as the ultimate goals of MDA.

In order to reach the MDA goals, there are many problems to be solved in the integration of platform centric heterogeneous systems and net centric systems which are deployed for different purposes and occasionally reiterated. The main problem is the interoperability of these systems that are aimed to serve for the same goals. The reiteration of systems will be minimized when the maritime interoperability is established.

The challenges on the pathway of establishment successful maritime interoperability are information security, process standardization, and resistance of governmental agencies for interoperability. As the

interoperability problem is worked on, many other problems are determined underside. The major one of the sub problems of interoperability is the lack of high level information security in MDA circumstances.

3.0 INFORMATION SECURITY

Information security is composed of many different perspectives that are illustrated in Figure 1: Perspectives of Information Security, as stated below: [8-10]

- Physical security in order to protect information assets,
- Transmission security (TRANSEC) for protection of private data from unintended electromagnetic emissions,
- Communication security (COMSEC) for protection of data on communication media,
- Network security (NETSEC) for protection of data flow in a network domain,
- Access and authentication security (COMPUSEC) for protection of unauthorized access to computers.

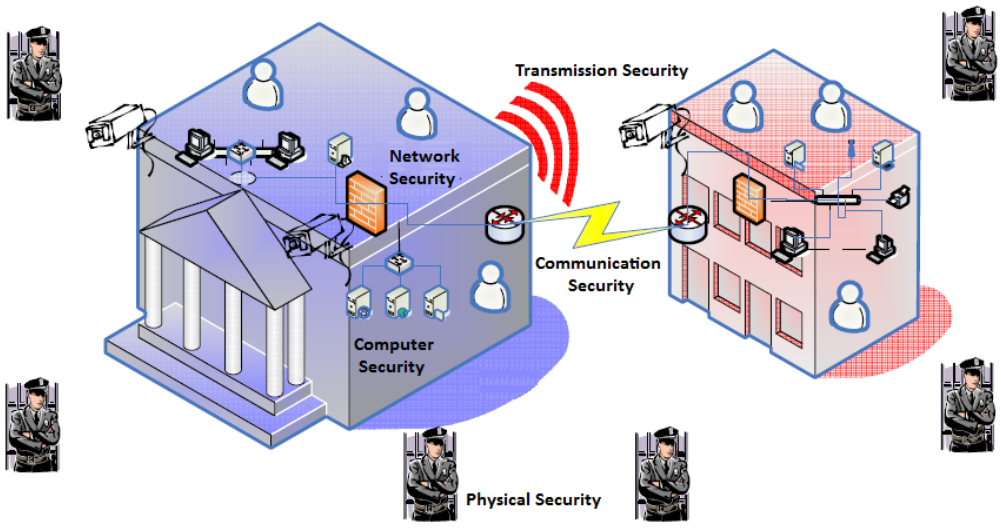

Figure 1: Perspectives of Information Security [11]

For establishment of information security, there are many principles that need to be followed and applied thoroughly. The main three principles are confidentiality, integrity and availability. Among - these three main principles, there are many rules such as access control, safety, non repudiation, reliability, log management, authentication and authorization.

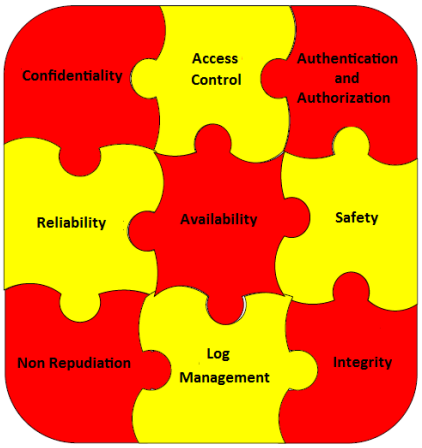

Figure 2: Information Security Principles

The principles of information security that need to be followed for establishment of high level information security are illustrated in Figure 2: Information Security Principles and are briefly explained in the following paragraphs:

- Confidentiality: The protection of information in electronic media from unauthorized people and processes via methods such as encryption, even if data is captured by unintended parties. In maritime information systems, confidentiality is achieved by the usage of IP and lower level encryption devices.

- Integrity: The method that assures the reception of data by receiver, as provided to the communication medium by sender. In maritime information systems integrity is achieved by usual hash algorithms.

- Availability: The precautions that enable the authorized access to required information, by users at all times as necessary. In maritime information systems, availability is achieved by the uninterrupted operation and replication of information systems. The systems have to be constructed robustly and protected by classical security solutions via proper security regulations. Availability is one of the major challenges in Maritime Information Security. The challenge in availability is the differentiation of malicious behaviors (eg: Denial of Service (DoS) attacks).

- Log Management: The storage of all electronic incidents in a network for future analyses. In maritime information systems, log management is achieved by system management tools for anomaly detection and correlation algorithms.

- Authentication and authorization: The proper validation and rights management of the user for accessing the resources of a network. In maritime information systems, authentication and authorization is achieved by password security mechanisms such as One Time Password (OTP).

- Reliability: The consistency of expected behaviors and real life outcomes of network services. In maritime information systems reliability is achieved by system design principles.

- Non Repudiation: The necessary precautions that need to be taken for the non repudiation of the communication between sender and receiver. In maritime information systems, non repudiation is achieved by digital signatures.

- Access Control: The granting of access rights to network services in an information system. In maritime information systems, access control is achieved by physical security and properly regulated authority such as MAC and IP filtering.

- Safety: The physical and technical solutions that need to be taken in order to protect information systems. In maritime information systems, safety is achieved by regulation of human factors.

While all information security principles are always important for every information system, for heterogeneous MDA IS, each system requires different levels of information security principles. In environments such as naval military technologies, confidentiality and access control steps forward, while in civilian merchant agencies availability and safety come into effect.

All these information security principles are termed as parts of traditional information security techniques. Traditional security solutions are generally the software and hardware solutions that are used to maintain the required level of security among the civilian systems that are deployed at equivalent security levels. These solutions are used to provide the required level of security from the physical level up to application level in civilian systems. Some examples of the classical security solutions are encryption solutions at the communication level; firewall, IDS/IPS, VPN solutions at the network level; application firewall, application IDS, anti virus, anti spam solutions at the application level. These solutions are not satisfactory for qualified secure information exchange between the civilian and military information systems in MDA that are deployed at different security levels.

4.0 SECURE INFORMATION EXCHANGE

Secure Information Exchange among heterogeneous systems is one of the greatest objectives in MDA. The main challenge of Information Exchange is to provide secure communication between maritime information systems [12]. Heterogeneous systems consist of various military and civilian information systems where such system has its own security principles and shall be classified accordingly. The balanced trade-off between flexibility and security has to be maintained among these systems.

For secure information exchange, firstly the necessary information is to be filtered, classified and transformed to common format. The qualified information that is transformed to common format is to be shared with the stakeholders via the communities of interest. Traditional and new generation security solutions are needed that enable the sharing of this qualified information via the communities of interest. The traditional and new generation information security techniques for sharing secure information are briefly explained in the following paragraphs.

The traditional solution that is widely used for information exchange among information systems that are deployed at different security levels is the air gap method. In the scope of air gap method there is no physical contact between the networks that host the high level security information systems and the other networks with low level security. The information exchange is performed offline in this solution. The price for these security solutions is high: Separate backbones, separate workstations, separate applications, and very high total cost of ownership (TCO). This solution brings some problems together like cost, integration, performance, and so on.

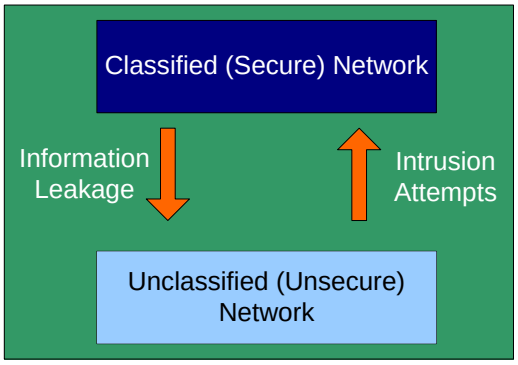

Figure 3: Main Security Threats of Information Exchange

The two main security threats of information exchange between different classification levels of networks are information leakage from Secure Networks to Unsecure Network (Case 1) and intrusion attempts from Unsecure Network to Secure Network (Case 2), as illustrated in Figure 3: Main Security Threats of Information Exchange. Case 2 security problems such as cyber attacks can be handled with current security solutions; however, Case 1 is much harder to maintain due to limitations in classical security infrastructures. "Air Gap" has to be formed to prevent these security problems, but NATO Network Enabled Capability (NNEC) Feasibility Study report reveals that the air gap solutions are not capable of handling future information technology objectives. [13]

In MDA, the networks that have different security levels, for transferring the information in different formats and content generated by military and civilian resources, are to be communicated securely. Secure communication requires both high (military) and low (civilian) security principles to merge in the higher security side. The higher security network always imposes its principles to the lower security network. In classified zone compromise from flexibility is necessary, while in unclassified zone, standardization and flexibility are of the utmost priorities. Considering these facts, the importance of information security in MDA environments arise, namely secure information exchange [14].

For minimizing the risk of information leakage, the primarily taken precaution is the data diode that enables the one-way communication. Data diodes are the solutions among the other new generation security solutions that are used to minimize the risk of threats caused by the information leakage. But data diodes are one-way solutions and do not allow data transfer from secure network to unsecure network. For overcoming all these problems, new generation security solutions are developed that is named as "Virtual Air Gap" solution.

"Virtual Air Gap" technology is constituted from an underlying host operating system, virtual machine monitor, virtual network hubs, network encryptors, and a filtering router that allows multiple machine environments to run simultaneously and to access multiple networks all from the same physical platform. The benefit of the Virtual Air Gap architecture is that it removes security functionality from the control of the end-user OS and applications. Important security functions such as communications encryption can be placed in a separate protected environment that cannot be influenced by user software. Similarly, an isolated filtering router function is used to provide protection from rudimentary network attacks.

In this study, we propose the Secure Network Nodes (SNN) for information exchange between secure and insecure networks. The components of SNN are illustrated in the following figure.

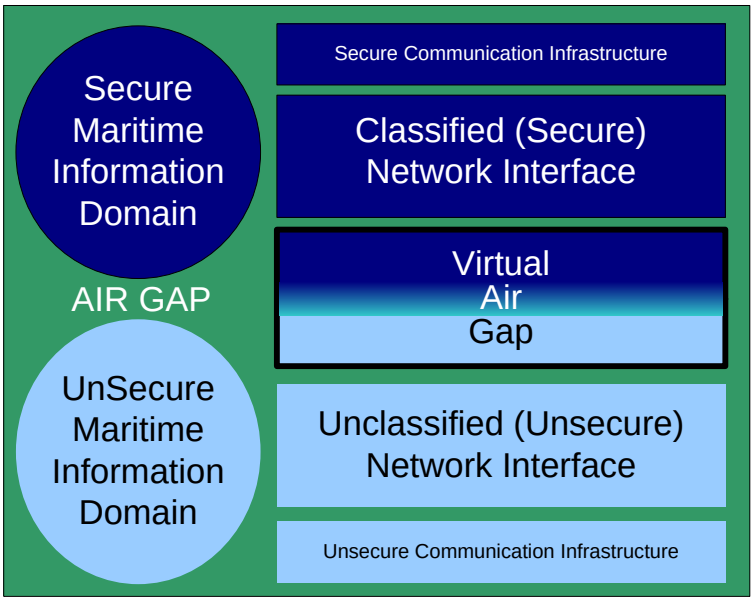

Figure 4: Layers of Secure Network Node

Secure Network Nodes have two, so called, "sides". First side, named unsecure maritime information domain, is connected to an unsecure "red" network, while the second side is connected to secure "black" network, the secure maritime information domain. The SNNs include a virtual air gap which can be understood as the third "side" that merges these two sides together as one layer, among with the network interfaces and communication infrastructures. Virtual air gap also includes IP encryption, firewall and other classical security solutions.

Communication infrastructures and network interfaces include necessary hardware and software for connecting the two networks having different transmission media and custom user configurations. Each SNN needs to be customized for its own regional location and enterprise communication requirements. And each SNN has to be remotely configured and remotely programmable for 7x24 operations. The physical security requirements of SNNs inherit that, the location of SNNs have to be within the secure network's geographical location as they need tightly bound connection to secure network interfaces.

5.0 CONCLUSION

In conclusion, online information exchange is inevitable among information systems that have different security levels for reaching the ultimate MDA goals. For performing the secure online information exchange, the classical and new generation security solutions shall be used together. In this study, the classical and new generation solutions for obtaining high level information security in MDA circumstances are analyzed in detail. As a result, in addition to the classical security solutions, the "Virtual Air Gap" solution is more convenient than data diode solution that enables only one way information transfer.

There are many ongoing projects utilizing SNNs, within NATO region. By the time the potential of SNNs will be better understood. NATO members need to employ SNNs, in order to connect NATO network to member nation's information networks. NATO MDA will be greatly achieved by employing SNNs, so that NATO wide information systems can be constructed with bi-directional and secure information exchange between member nations. SNN approach will add considerable benefits to NATO information systems.

6.0 REFERENCES

[1] Despriee, M., Tanguy, P., Therier, L., "Maritime crisis management aided by information and communication technologies: the POLLUCOM system", **Oceans 2005 – Europe**, Page(s): 1260 - 1263 Vol. 2, (2005).

[2] Walden, D.D., "A platform-centric functional hierarchy" **Proceedings of International Conference and Workshop on Engineering of Computer-Based Systems**, Page(s): 397 – 404 (1997).

[3] Stotz, Adam; Sudirt, Moises,"Intelligence Exchange (IntellEx)" Military Communications Conference, **MILCOM-2007 IEEE**, Page(s): 1 - 6 (2007).

[4] Tetreault, B.J., "Use of the Automatic Identification System (AIS) for Maritime Domain Awareness (MDA)", **Proceedings of MTS/IEEE**, Page(s): 1590 - 1594 Vol. 2, (2005).

[5] Internet: Tidepedia "Maritime Situational Awareness" (09.03.2010)

http://tide.act.nato.int/tidepedia/index.php?title=Maritime_Situational_Awareness_(MSA)

[6] Hall, D.L., Llinas, J., "An introduction to multisensor data fusion" **Proceedings of the IEEE** Volume: 85 , Issue: 1, Page(s): 6 - 23 (1997)

[7] Giompapa, S., Gini, F., Farina, A., Graziano, A., Stefano, R., "Maritime border control computer simulation", **Aerospace and Electronic Systems Magazine, IEEE** 23(11), Page(s): 39 - 45 (2008).

[8] Internet: Wikipedia "Kriptografi" http://tr.wikipedia.org/wiki/Kriptografi (09.03.2010).

[9] Internet: Wikipedia "Steganografi" http://tr.wikipedia.org/wiki/Steganografi (09.03.2010).

[10] Sharp, E. D., "Information Security in the Enterprise", **Information Security Management Handbook Fifth Edition**, Tipton, F. H., Krause, M., Auerbach Publications, New York, 1199-1200, (2004).

[11] Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri" Yüksek Lisans Tezi, **Gazi Üniversitesi Fen Bilimleri Enstitüsü**, 40, (2007).

[12] Dimitriou, T., Krontiris, I., "A localized, distributed protocol for secure information exchange in sensor networks" Parallel and Distributed Processing Symposium, Proceedings 19th IEEE International (2005)

[13] Internet: NNEC Feasibility Study, https://transnet.act.nato.int/WISE/Informatio (05 Jan 2006)

[14] Rao Perka, V., Mishra, P., "Secure Information Exchange - A Security Quantification Approach" Electro/information Technology, Page(s): 448 – 453 IEEE International Conference (2006)