SECURED AND ENHANCED INFORMATION SECURITY IN THE NIGERIAN MARITIME INDUSTRY

Mughele E.S.
Department of Science & Technology
Computer Science Option
Delta State School of Marine Technology
Burutu. Nigeria
prettysophy77@yahoo.com

ABSTRACT

The Information and Communication Technology (ICT) policy identified ICT as the bedrock of national survival and development in a rapidly changing global environment. The prevalence and rapid development of ICT have transformed human society from the information age to the knowledge age. The Nigerian maritime industry is not an exception. However, securing the critical infrastructure (data/information) of the maritime sector is increasingly becoming worrisome. The data collection method deployed for this research is literature review method by analyzing contents relevant to the domain of discourse. This paper showcases the consequence of low level awareness, inefficient policies and also identifies a solution for secure information communication and transfer in the Nigerian Maritime sector.

Keywords: ICT, Nigeria, Maritime, Information

1. INTRODUCTION

The very definition of the maritime setting is work and life that takes place in or around a watery world (e.g., ships and barges, docks and terminals) (A dessand Ungs, 2011). The maritime industry includes all enterprises engaged in the business of designing, constructing, manufacturing, acquiring, operating, supplying, repairing and/or maintaining vessels, or component parts thereof. The managing and operating of shipping lines, stevedoring and customs brokerage services, shipyards, dry docks, marine railways, marine repair shops, shipping and freight forwarding services and similar enterprises (Ekpo Imoh, 2012). The economic value of natural resources which includes crude oil, natural gas, tin, columbite, iron ore, coal, zinc, limestone, lead, etc, to Nigeria in terms of foreign earnings is directly related to the maritime component of the respective industries. For example, the oil and gas sector as the predominant sector in Nigeria's short sea trade constitute in estimate about 95 percent coastal and inland shipping while fishing trawlers and break bulk carriers make up the remaining 5 percent presenting enormous coastal trade opportunities (Okeke and Aniche, 2012). The maritime activity increasingly relies on Information Communication and Technology (ICT) to optimize its operations, like in all other sectors. ICT is used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc. (ENISA, 2011).

The ICT policy identified ICT as the bedrock of national survival and development in a rapidly changing global environment. ICT is an umbrella term that includes communication devices or application (radio, television, cellular phone, computer hard and software and networking, and satellite system) and services associated with them (Oviawe and Oshio, 2011). The prevalence and rapid development of ICT have transformed human society from the information age to the knowledge age (Galbreath, 2000). The increased dependency towards ICT systems combined with operational complexity and multiple maritime stakeholders involved makes the existing ICT environments particularly vulnerable to attacks, which could result in severe maritime services disruptions. For example, cargo tracking and cargo identification are increasingly subject to security incidents resulting from attacks or system failures. The same applies for the automated systems handling the cargo in ports. Data theft, for criminal purposes, may increase as a direct result of insufficient information security measures or measures not sufficiently matching the complexity of the ICT environment involved.

These last years have also shown that information security threats are a growing menace, spreading in all sectors. Disruption or unavailability of these ICT capabilities might have disastrous consequences - therefore there is an increased need to ensure the ICT robustness against attacks and dependability is a key challenge nationally and globally. Securing the critical infrastructure of the maritime sector is increasingly becoming a priority for the key European stakeholders, including the European Commission, Member State governments and the main actors from the private sector. Critical information infrastructures support vital services and goods such as energy, transport, telecommunications, financial services, etc., that are so essential that their unavailability may adversely affect the well-being of a nation (ENISA, 2011). Maritime information systems provide operational superiority to the armed forces and government agencies by supplying valuable maritime data/information and necessary inputs to the decision maker in near real time (Yılmaz et. al. 2010).

In maritime environments huge amount of maritime data/information 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 Automatic Identification System (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 (Hall and Llinas, 1997). In this study, enforcing data/information security for ICT systems in the Nigerian maritime industry is detailed.

2. THE NIGERIAN MARITIME

The history of Nigeria's maritime industry pre-dates the colonial era. It is on record that before the colonial masters' advent, shipping was going on in Nigeria especially in the riverine areas of the Niger Delta like Bonny, Bayelsa, Opobo, Ijaw, among several others. This explains why even upland, there was serious shipping business, though in its crude form. (www.mydailynewswatchng.com). Nigeria has a coastline of about 870 kilometres, and 3, 000 kilometres in land mass. The country's natural resources waterways, and 913, 075 square include crude oil, natural gas, tin, columbite, iron ore, coal, zinc, limestone, lead, etc, and population of over 150, 000 people in human resources. Nigeria has proven 600 trillion cubic feet reserve of gas, estimated 40 Bitumen (United States Geological Survey) (Okeke and Aniche, 2012). The economic value of these resources to Nigeria in terms of foreign earnings is directly related to the maritime component of the respective industries. For example, the oil and gas sector as the predominant sector in Nigeria's short sea trade constitute in estimate about 95 percent coastal and inland shipping while fishing trawlers and break bulk carriers make up the remaining 5 percent presenting enormous coastal trade opportunities (Okeke and Aniche, 2012).

The amount of sensitive proprietary information circulating within and between Nigerian maritime industries and their counterparties means that information security needs to remain watertight to prevent both industrial espionage and breaches by 'hacktivists' those who hack into computer networks to promote a political or social ideology. Moreover, the need for resource-rich Nigeria to assume control of the information in the maritime sector and to harness the potentials of this most strategic industry in order to generate more value-added among all the stakeholders cannot be overemphasized. For instance, pirates have hijacked tankers as far as 89 nm (nautical miles) offshore, suggesting that they have an awareness of where and when they can find specific tankers in relatively remote locations. Meanwhile, the accounts of hijacked crews have indicated that pirates had prior knowledge of ships' cargoes, while interrogated pirates are reported to have received detailed instructions from their employers regarding which ships to target and their respective cargoes (GRAY PAGE, 2013).

Basically, on 16 July 2011, Leadership news media published articles stating that

"*10 tankers laden with 219,456 metric tons of premium motor spirit popularly known as petrol…are expected at the Lagos ports between July 2 and 24*"***. They go on to state that*** *"seven tankers loaded with 183,000mts of PMS have been awaiting berth at the Atlas Cove Jetty , Bulk Oil Plant, Single Buoy Mooring and the Petroleum Wharf Apapa jetties since June 18. The statistics also showed that among vessels expected at the Lagos Ports District in the month July include seven bearing 47,500mts of AGO, two with 11,000mts of kerosene, two with 15,695mts of base oil.***"**(www.leadership.ng.com). Information of such magnitude is released as a monthly press statement by the Nigerian Port Authority (NPA).

Publishing such information provides criminal syndicates with a list of various cargo parcels to target. Aware of a specific vessel's planned load/discharge date and destination, pirates can track that vessel's movements via its AIS, striking at the optimum moment. Meanwhile, with full knowledge of the vessel's cargo, criminal syndicates can line up buyers for the stolen cargo ahead of the vessel's hijack. Such widespread dissemination of information regarding tanker operations by local parties should serve to re-emphasize the need to ensure that information regarding vessel operations remains guarded. Although local parties (such as agents) will require information regarding tankers' operations, it may be advisable to release this information as late as commercially viable. Additionally, it may be possible to request agents in turn withhold certain information (and thus publication) such as the type of cargo due to be loaded or discharged from a vessel until as late as possible (GRAY PAGE, 2013).

Hence, this has shown that the awareness regarding information security aspects is either at a very low level or even non-existent in the Nigerian maritime sector, this observation being applicable at all layers, including government bodies, port authorities and maritime companies. This overall low awareness represents a concern as there is an increased dependency on ICT of all the key players, processes and activities within the maritime sector. Indicators of this dependency are the increasing number of ICT systems implementations in ports worldwide, and the continuous increase of volume and complexity of information and data been exchanged. However, there is insufficient focus on information security in the mode of operations as it relates to information gathering, dissemination and communication in the Nigerian maritime sector. Most security related regulation only includes provisions relating to safety and physical security concepts (ENISA, 2011).

3. INFORMATION SECURITY

Information security ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability) (ISACA, 2008). It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...). Governments, military, corporations, financial institutions, hospitals, and private businesses as well as the maritime amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, not to mention damage to the company's reputation. Protecting confidential information is a business requirement and also an ethical and legal requirement.

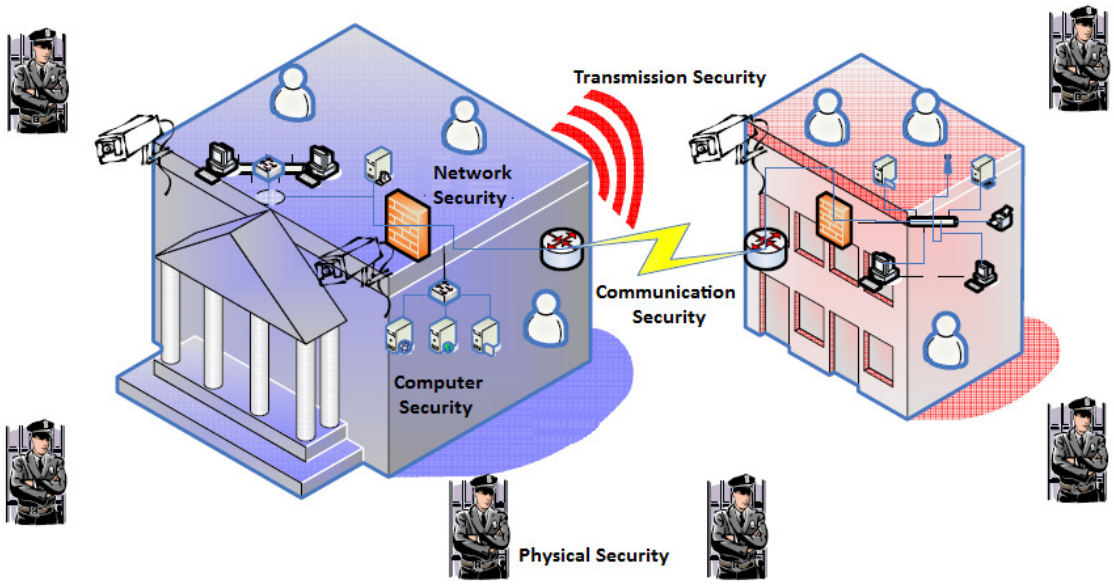

Figure 1: Perspective of Information Security (Vural, 2007)

Figure 1 above illustrates the different perspectives of information security. These are:

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

For establishment of information security, there are many principles that need to be followed and applied thoroughly. The confidentiality, integrity and availability (CIA) is one of the core principles of information security (Perrin, Chad, 2012). There is continuous debate about extending this classic trio (Cherdantseva and Hilton, 2013). In 2013, based on the extensive literature analysis, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-traid. Information security principles are as follows (Yılmaz Vural et. al.):

- **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).

- **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).

- **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.

- **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.

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

- **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.

4. SECURE NIGERIAN INFORMATION CONTENT

The insufficient awareness and focus on information security results in a low sense-of-urgency combined with an inadequate preparedness regarding the risks. Nigeria consider developing focused awareness raising campaigns aimed at the key stakeholders within the maritime sector, in order to highlight the importance of adequate information dissemination and protection means against disruptions targeting assets linked to the maritime sector (ships, ports, communication systems, etc.). Furthermore, it is more appropriate that the initiatives for analysing and further deciding on adequate information security policy measures and (if needed) on regulations with regard to the maritime industry may need to be addressed. Secure Information Exchange among information systems is one of the greatest player in the Nigerian maritime.

The main challenge of Information Exchange is to provide secure communication between maritime information systems (Dimitriou and Krontiris, 2005). For secure information exchange in ICT systems, 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. The two main security threats of information exchange between different classification levels of networks are information leakage from Secure Networks to Unsecure Network and intrusion attempts from Unsecure Network to Secure Network (Yılmaz et. al. 2010)

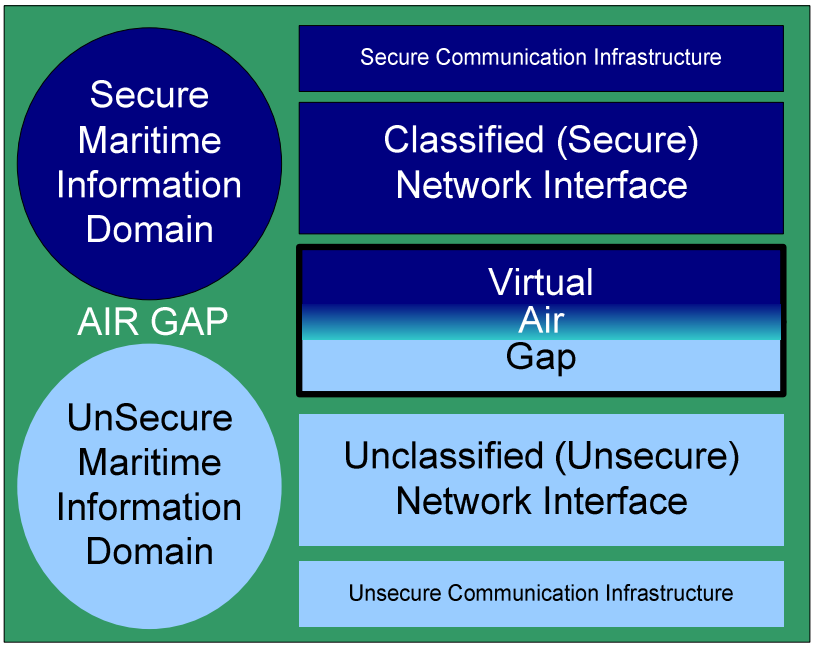

Figure 2: Layers of Secure Network Node (SNN) (Vural, 2007)

According to Vural et. al., the Secure Network Nodes (SNN) for information exchange between secure and insecure networks is proposed (as illustrated in the figure 2 above). 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, along with the network interfaces and communication infrastructures. Virtual air gap also includes IP encryption, firewall and other classical security solutions.

4. CONCLUSION

The inevitability of secured information in the maritime industry in Nigeria has been clearly detailed. Imbibing adequate information dissemination and data protection means against disruptions targeting assets linked to the maritime sector (ships, ports, communication systems, etc.) is being prescribed. It is also essential that appropriate initiatives for analysing and deciding on adequate information security policy measures and regulations should be addressed. For secure information exchange among ICT systems, a convenient and efficient solution should be employed for information transfer. Moreover, the Secure Network Node (SNN) is an effective solution since there are many ongoing projects utilizing it.

REFERENCE

1. Adess Michael and Ungs Timothy J. (2011): Water Transportation and the Maritime Industries. in Water Transport, Byrd, LaMont, Editor, Encyclopedia of Occupational Health and Safety, Jeanne Mager Stellman, Editor-in-Chief. International Labor Organization, Geneva. © 2011.
2. Cherdantseva Y. and Hilton J. (2013): Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing.
3. Dimitriou, T., Krontiris, I. (2005): "A localized, distributed protocol for secure information exchange in sensor networks" Parallel and Distributed Processing Symposium, Proceedings 19th IEEE International
4. Ekpo Imoh Ekpo (2012): Impact of Shipping on Nigerian Economy: Implications for Sustainable Development. ISSN 2239-978X Journal of Educational and Social Research Vol. 2 (7)
5. ENISA (2011): Analysis Of Cyber Security Aspects In The Maritime Sector. European Network and Information Security Agency.
6. GRAY PAGE (2013): Information security at Nigerian ports 02/08/2013
7. Hall, D.L., Llinas, J. (1997): "An introduction to multisensor data fusion" Proceedings of the IEEE Volume: 85 , Issue: 1, Page(s): 6 - 23
8. ISACA. (2008): Glossary of terms, 2008. Retrieved from http://www.isaca.org/Knowledge-Center/ Documents/Glossary/glossary.pdf
9. Jane Itohan Oviawe and L. E. Oshio (2011): Impact of Information and Communication Technology on Teaching and Learning Ability of Education Students in Universities in Edo State, Nigeria. International Review of Social Sciences and Humanities Vol. 2, No.1 (2011), pp. 126-133
10. J. Galbreath, Knowledge management technology in education: An Overview, Education Technology, 40(5) (2000), 28 -33.
11. Leadership, (2013): "95 Ships, 219,465mt PMS, 4,098 Vehicles Hit Lagos Ports", 16 July 2013 (http://leadership.ng/news/160713/95-ships-219465mt-pms-4098-vehicles-hit-lagos-ports)
12. Okeke, V.O.S. and Aniche, E. T. (2012): An Evaluation Of The Effectiveness Of The Cabotage Act 2003 On Nigerian Maritime Administration. pp. 12-28
13. Perrin, Chad (Retrieved 31 May 2012):"The CIA Triad". www.mydailynewswatchng.com/2013/06/04/maritime-good-moves-on-wrong-steps/
14. Vural, Y. (2007), "Kurumsal Bilgi Güvenliği ve Sızma Testleri" Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 40.
15. Yilmaz Vural, Mehmet Emre Ciftcibasi, Serhat Inan: Information Security in Maritime Domain Awareness. STM A.Ş Ankara Teknoloji Geliştirme BölgesiBilkent 5. Cad No:6/A Bilkent Ankara, TURKEY