Open Issues and Proposals in the IT Security Management of Commercial Ports: The S-PORT National Case

Nineta Polemi, Theodoros Ntouskas

Open issues and proposals in the IT Security Management of commercial ports - The S-PORT national case

Nineta Polemi* and Theodoros Ntouskas

Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 185 34 Piraeus, Greece,
{dpolemi,tdouskas}@unipi.gr

Abstract. Commercial ports are large scale infrastructures which their Information and Telecommunication (PIT) systems offer critical services and host sensitive data. However the current maritime legislation or standardization efforts do not sufficiently cover the IT security of the commercial ports. Identifying these needs we propose a collaborative environment offering security management services including a targeted risk management methodology which will help commercial ports to self manage their security.

Keywords: Security Management, Commercial Ports, Maritime environment, Critical Infrastructures, Collaboration, S-PORT project.

1 Introduction

The tragic accident of Titanic (1912) imposed the new concept of "safety" in the maritime sector and numerous legislations and directives are published since then concentrating in the physical protection of the ships, crew, passengers, cargo and sea. The terrorist events in New York and Washington (2001), Madrid (2004), and London (2005) imposed the concept of "security" in the maritime sector with additional directives and legislation (e.g. IMO / ISPS) in order to avoid such malicious acts. However these new efforts concentrated on the organizational and auditing aspects of physical security of the ships, maritime companies and the commercial ports; they did not consider the IT and cyber security aspects of the maritime environment.

In this paper we will concentrate on the ports and specifically on the security management of Ports' Information and Telecommunication (PIT) systems. The gaps and barriers of the existing security management maritime related legislation, methodologies and tools in the PITs will be presented at this paper. Proposals will be provided that have been partially presented in [3], [19], [15], [18] by the authors.

2 Existing efforts and open issues

The maritime environment is a complex one, as shown in Figure 1, involving and interacting with many entities including ports, ships (with passengers, crew, cargo), port authorities, maritime and insurance companies, customs, ship-industry, banks, ministries, other commercial providers, other critical infrastructures (e.g. railroads, airports) hosting and interacting with complex, heterogeneous Information and Telecommunication (IT) Systems. Commercial ports, are the central entities in the maritime environment and among the transportation critical infrastructures [2] since they are large-scale infra-structures that their degradation, interruption or impairment of their IT Systems has serious consequences on national security, health, safety, economy and welfare of citizens and nations characterized with multiplicity of interdependencies between them and the other entities in the maritime environment.

Fig. 1. Maritime Environment

The Ports Information and Telecommunication (PIT) systems consist (as all IT systems) of the following seven (7) consecutive layers: *Infrastructure* (e.g. buildings, platforms, servers, stationary / mobile terminals, nautilus systems, databases); *Telecom Systems* (e.g. networks equipment, satellites, Geographic Information Systems - GIS); *Software and Manuals* (e.g. identification, maritime, navigation, routing software, Enterprise Resource Planning -ERPs, ticketing); *Information and electronic data* (e.g. marine and coastal data, trade data); *Services* (e.g. invoicing, navigation, luggage/cargo management, logistics, e-health); *Other equipment* (e.g. fire alarm systems, cameras); *Users*: a. internal users (e.g. administrators, personnel), external users (e.g. port authorities, maritime companies, customs, insurance companies, IT and commercial provides), objects (e.g. ships, crew cargo, luggage, vehicles).

However the existing maritime security standards, methodologies and tools concentrate only on the physical security of the ports (safety) especially in the access control of the ports' infrastructures in relation to the safety of the ships. They consider only the first and the last layer of the PIT system and only the

two last components (access control, availability) of security ignoring all its other layers and components making ports as weak security links.

To be more specific, as it has been described in [18] and [15], the various maritime standardization bodies (e.g. IMO, EMSA, EASA, TEN-T EA) do not include in their memorandum IT/cyber security. Similarly, existing risk assessment methodologies for ports (e.g. MSRAM, MARISA, CMA) only detect safety risks and not IT risks.

Furthermore they do not consider the threats rising from the interdependency of the ports with the other ports or other critical infrastructures (e.g. railways) which may cause cascading effects. They do not examine the PIT security independently but with relation to ships' safety. The implementation of the safety directive IMO/ISPS is left at national level i.e. there is not a standard providing the exact procedures and measures that need to be undertaken (e.g. like the ISO27002) in order for a port to become IMO/ISPS compatible. Finally all maritime security management methodologies are not user centric; they consider the user as a passively involved entity that needs to follow the methodology with no interaction or collaboration.

3 Proposals for enhancing maritime IT security management

A proposed solution to better address the PIT security is to combine the IMO / ISPS with common IT security management standards. However the well known security management standards from the standardization bodies NIST [8] and ISO ([4], [5], [6]) will need further modifications in order to adapt to the port IT security so they can address specific sectoral threats, i.e. interdependent threats rising from all entities in the maritime environment (see Fig.1), specific threats (e.g. weather conditions, strikes) and maritime legislation (e.g. IMO/ISPS). Well known security management methodologies (e.g. OCTAVE, CRAMM, MAGERIT, MEHARI, COBIT)[18],[15] which have been successfully applied in various environments (e.g. health, business) they may be useful in ports' environments with appropriate adoptions.

Furthermore we need to consider the fact that ports are critical infrastructures (CIs) and we need to take into account the known legislation, recommendations and standards for CIs. Most of these standards are from the energy sector and more specifically from the U.S. Department of Energy, North American Reliability Corporation (NERC) [9] and the USA national program National Infrastructure Protection Plan [25]. There is not a standardized way in examining the criticality of an infrastructure or/and addressing cyber threats.

Commercial Ports belong in the special category of transportation CIs [24]. The various security management efforts [23], found in this sector-specific, focus on the physical security of the transportation means (targeted to railways), on material transportation and assessment of hazardous material. These security management methodologies for the CIs are at national level and use different impact assessment criteria (e.g. economic, public, health & safety, psychological

/ social / public confidence, complexity, environmental, business, national / territorial security). These methodologies may be used in the ports with appropriate modifications.

A holistic approach to security management of the PIT systems that the authors propose is the creation / enhancement of maritime standard(s) respecting and be com-pliant with: the ISPS code, modified IT and CIs security management standards.

4 S-PORT: a national project

In the national S-PORT project [19], the ports are viewed as CIs and it addresses the following two main security management needs: The development of a targeted security management collaborative methodology for the PIT-systems based on IT security management standards and the ISPS code involving all PIT users; The promotion of collaboration and interaction among PIT users in the security management of the PIT-systems in an automated used friendly approach.

The first need is addressed by S-PORT by applying the STORM-RM collaborative risk management methodology [13], [16] which views risk management as a collaborative decision making problem and combines the Analytic Hierarchy Process (AHP) [22], the security management standards ISO27001 [4] and AS/NZS 4360 [1] and has been modified in order to address the specific needs of PIS and the requirements of the IMO/ISPS directive. In STORM-RM a multicriteria collaborative decision making technique is applied enabling all users (internal and external) to evaluate the impacts depending upon their experience and role in their interaction with the IT system under assessment (where most of the existing risk management methodologies enable only the security team to be involved in the impact evaluation). The STORM-RM has been parameterised for the PIT-systems [14], [20] considering sectoral PIT and cyber threats, setting criteria in the impact evaluation rising from the fact that ports are CIs and assigning roles/ opinion weights according to the ports' users. The basic goal of this parameterised methodology is the collection of knowledge and experience from all port's users (i.e. managers, administrators, security team, local users, cooperate users) in order to evaluate the impacts, sectoral threats, vulnerabilities and risks more accurately.

The second security management need is addressed in S-PORT by developing a collaborative environment [14] (a recent trend in Web services applied in various sectors e.g. e-commerce [10], [11], e-government [7] and e-migration, [17]) using innovative Web2.0 technologies. The S-PORT environment [14], [15] is a parameterisation of the STORM security management environment [12] addressing the specific needs of PIT and involving all PIT users in the security management procedures.

In the S-PORT collaborative environment we embedded the targeted risk management methodology offered as an S-PORT collaborative service to the PIT-users. More specifically, each phase of S-PORT-RM methodology has been

implemented as a distinct module in the S-PORT environment. Additional S-PORT collaborative security management services will be offered thru the S-PORT environment including cartography: graphical representation of the PIT infrastructure and identification of all assets of the PIT-systems; reporting: generation of security documents, e.g. security policies, business continuity plans, disaster recovery plans (as growing documents); collaborative Web2.0 services: forums, chat rooms, questionnaires, for building social interactions in resolving and discussing security issues.

5 Conclusions and Acknowledgments

The fact that commercial ports are critical infrastructures and their Information Systems offer critical services and host sensitive data, makes security management a necessary concern for their business continuity and productivity. In this context, S-PORT environment is expected to become a prototype of the next generation Information Security Managements Systems, being capable of providing high levels of confidentiality, reliability, interactivity and interoperability, for the critical infrastructures of the commercial ports. This work has been performed in the framework of the S-PORT project [21] and the authors would like to thank the GSRT (General Secretariat for Research and Technology Development Department) for funding the S-PORT project and the S-PORT partners.

References

1. AS/NZS 4360: Risk management standards australia. Strathfield (1999)
2. Brunner, E., Suter, M.: International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies. Center for Security Studies, ETH Zurich, Switzerland (2008)
3. ENISA: workshop on cyber security aspects in the maritime sector. available at http://www.enisa.europa.eu/act/res/workshops-1/2011/cyber-security-aspects-in-the-maritime-sector (2011)
4. ISO/IEC 27001: Information technology - security techniques - information security management system - requirements (2005), `http://www.iso.org`
5. ISO/IEC 27002: Information technology - security techniques - code of practice for information security management (2005), `http://www.iso.org`
6. ISO/IEC 27005: Information technology - security techniques - information security risk management (2008), `http://www.iso.org`
7. Karantjias, A., Polemi, N.: An innovative platform architecture for complex secure e/m government services. In: Int. J. Electronic Security and Digital Forensics (IJESDF). vol. 2, pp. 338–354. Inderscience Publishers (2009)
8. National Institute for Standards and Technology: Risk management guide for information technology systems. NIST Special Publication 800-30, available at: http://csrc.nist.gov/publications/PubsSPs.html (Accessed 15 October 2011)
9. North American Reliability Corporation (NERC): available at http://www.nerc.com (Accessed 7 December 2011)

10. Ntouskas, T., Papanikas, D., Polemi, N.: A collaborative system offering security management services for SMEs/mEs. In: R. Bashroush, et al. (ed.) 7th IEEE International Conference in Global Security, Safety and Sustainability (ICGS3-2011). Springer, Thessaloniki, Greece, August 2011 (to appear)
11. Ntouskas, T., Papanikas, D., Polemi, N.: Trusted collaborative services for the IT security management of SMEs/mEs. In: Int. J. Electronic Security and Digital Forensics (IJESDF). Inderscience Publishers (to appear)
12. Ntouskas, T., Pentafronimos, G., Papastergiou, S.: Storm - collaborative security management environment. In: Ardagna, C., Zhou, J. (eds.) WISTP 2011. pp. 320–335. LNCS 6633 (2011)
13. Ntouskas, T., Kotzanikolaou, P., Polemi, N.: Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach. In: 1st International Symposium & 10th Balkan Conference on Operational Research,. Thessaloniki, Greece (to appear)
14. Ntouskas, T., Polemi, N.: A secure, collaborative environment for the security management of port information systems. In: Proceedings of the Fifth International Conference on the Internet and Web Applications and Services, ICIW 2010. pp. 374–379. IEEE Computer Society Digital Library, Barcelona, Spain (2010)
15. Ntouskas, T., Polemi, N.: Collaborative security management services for port information systems. In: International Conference on e-Business, ICE-B 2012. Rome, Italy (submitted)
16. Ntouskas, T., Polemi, N.: STORM-RM: A collaborative and multicriteria risk management methodology. In: Int. J. Multicriteria Decision Making (IJMCDM). Inderscience Publishers (to appear)
17. Pentafronimos, G., Karantjias, A., Polemi, N.: Odysseus: An advanced, collaborative and trusted framework for the provision of migration services. In: Proceedings of the Fifth International Conference on the Internet and Web Applications and Services, ICIW 2010. pp. 531 – 537. IEEE Computer Society Digital Library, Barcelona, Spain (2010)
18. Polemi, N.: Security management of the ports' information systems. ENISA Personal study (to appear)
19. S-PORT Deliverable 1.2: State of the art and user requirements in the Port Information and Telecommunication (PIT) Systems Security. available at http://s-port.unipi.gr/.
20. S-PORT Deliverable 1.4: Port Information and Telecommunication (PIT) Systems Security requirements-A targeted PIT-risk assessment methodology. available at http://s-port.unipi.gr/.
21. S-PORT Project: A secure, collaborative environment for the security management of Port Information Systems, available at http://s-port.unipi.gr/.
22. Saaty, T.L.: Decision making with the analytic hierarchy process. In: Int. J. Service Sciences. vol. 1, pp. 83–98 (2008)
23. Theoharidou, M., Kandias, M., Gritzalis, D.: Securing transportation-critical infrastructures: Trends and perspectives. In: R. Bashroush, et al. (ed.) 7th IEEE International Conference in Global Security, Safety and Sustainability (ICGS3-2011). Springer, Thessaloniki, Greece, August 2011 (to appear)
24. Transportation Security Administration: Critical infrastructure and key resources sector-specifc plan as input to the national infrastructure protection plan. Dept. of Homeland Security, USA (2007)
25. US Dept. of Homeland Security: National Infrastructure Protection Plan 2009. available at http://www.dhs.gov/(accessed December 2010)