Collaborative Security Management Services for Port Information Systems

Theodoros Ntouskas and Nineta Polemi
Department of Informatics, University of Piraeus, Karaoli & Dimitriou str 80, 18534 Piraeus, Greece

Keywords: Security Management, Commercial Ports, Critical Infrastructures, Collaboration, S-Port project.

Abstract: Ports Information and Communication Technology (PICT) systems offer critical services and host sensitive data. However the current maritime legislation, standardization and technological efforts do not sufficiently cover the PICT security. Identifying these needs, we propose the collaborative environment S-Port offering security management services.

1 INTRODUCTION

Commercial ports play an important role in the European trade and economy, since 52% of the European Union (EU) goods traffic in 2010 was carried by maritime transport and the 90% of EU external trade take place through maritime sector (ENISA, 2011). Additionally, they are among the transportation critical infrastructures (Transportation Security Administration, 2007), (Brunner and Suter, 2008) since they are large-scale infrastructures that their degradation, interruption or impairment of their ICT 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.

The normal functionality of any critical infrastructure such as the commercial ports depends largely on the proper operation of their ICT systems. The large amount of critical and sensitive data, the information and services that are managed on a daily basis, the large number of entities called to be served, and the interdependencies with the other infrastructures require effective security management.

However the current maritime legislation or standardization efforts do not sufficiently cover the ICT security of the commercial ports. In particular the commercial ports are not treated as independent critical infrastructures hosting critical ICT systems interacting with many entities and their security is not assessed or managed in a holistic, effective manner. The fact that ports are critical infrastructures raises specific threats (e.g. strikes, terrorist attacks, weather conditions etc), that their identifications and impacts (e.g. in national economy, national security, disruption of public order) are ignored yielding to inaccurate risk evaluations.

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. For example: the International Maritime Organization (IMO) (International Maritime Organization, 2011) has published a series of directives that fall in two categories: SOLAS and MARPOL. The SOLAS directives for the safety of the ships, passengers and cargo and the MARPOL directives for the environmental (sea) protection. The 2002 IMO directive ISPS (International Ships and Port Facilities Security Code) that all commercial ports need to be complied with, address mostly safety requirements for the ports including: Secure access, Audit, Secure handling of cargo, Availability of telecommunication infrastructure, Incident reporting, Creation of security team Risk Assessment and Training. ISPS does not address either cyber threats or security measures for the PICT systems.

Targeted methodologies for risk assessment of ports like MSRAM (Maritime Security Risk Analysis Model) (U.S. Department of Energy, 2002), (Adler and Fuller, 2007) address only physical security and they are compatible with the ISPS. Similarly the available maritime risk assessment systems like MARISA (Balmat et al., 2009) concentrate on the safe navigation of ships during their presence in the port. The risk assessment system CMA (Kang et al., 2009) detects abnormal behavior of ships and identifies respecting

Ntouskas T. and Polemi N..
Collaborative Security Management Services for Port Information Systems.
DOI: 10.5220/0004076503050308
In *Proceedings of the International Conference on Data Communication Networking, e-Business and Optical Communication Systems* (ICE-B-2012), pages 305-308
ISBN: 978-989-8565-23-5

threats.

To conclude, the available maritime security management directives, methodologies and systems only consider safety (physical security) and not security.

A holistic approach to security management of the Ports Information and Communication Technology (PICT) systems that the authors propose is the creation/enhancement of maritime targeted security management methodologies which are compliant with the: ISPS code, modified ICT and CCIP security management standards.

2 S- PORT: A NATIONAL PROJECT

In the national S-PORT project (S-PORT Project, 2011) we have identified the above mentioned issues, searched the previously mentioned efforts, identified the PICT-security management needs with the guidance of the involved national ports (Piraeus Port Authority, Thessaloniki Port Authority, Municipal Port Fund of Mykonos). S-PORT views the ports as critical infrastructures and addresses the following two main security management needs: The development of a targeted security management collaborative methodology for the PICT-systems based on IT security management standards and the ISPS code involving all PICT users viewing the port infrastructures as critical infrastructures; The promotion of collaboration and interaction among PICT users in the security management of the PICT-systems in an automated used friendly approach.

2.1 S-PORT Risk Management Methodology for the PICT Systems

S-PORT-RM is the proposed Risk Management methodology which is based on STORM-RM (Ntouskas and Polemi, 2012), (Ntouskas et al., 2011a). STORM-RM combines the Analytic Hierarchy Process (AHP) (Saaty, 2008) and security management standards ISO27001 (ISO/IEC 27001, 2005) and AS/NZS 4360 (AS/NZS 4360, 1999) and has been modified in order to address the specific needs of PICT and the requirements of the ISPS code. The basic goal of S-PORT-RM 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, threats, vulnerabilities and risks more accurately.

In order to have the S-PORT-RM methodology as service that will be provided by the S-PORT collaborative environment, each Phase of S-PORT-RM methodology has been implemented as a distinct module in the S-PORT environment.

2.2 S-PORT Collaborative Security Management Environment

S-PORT environment is a parameterization of the STORM security management environment (Ntouskas et al., 2011b) addressing the specific needs of PICT and involving all PICT users in the security management procedures.

The overall architecture of the S-PORT collaborative environment is depicted in the above figure (Fig. 1) and consists of four (4) main entities: the *S-PORT main Platform*, the *Middleware System*, the *Identity & Access Management System (IAM)* and the *Business Process Management System (BPM)*. The S-PORT entities and their functionalities are described in detail in the following paragraphs.

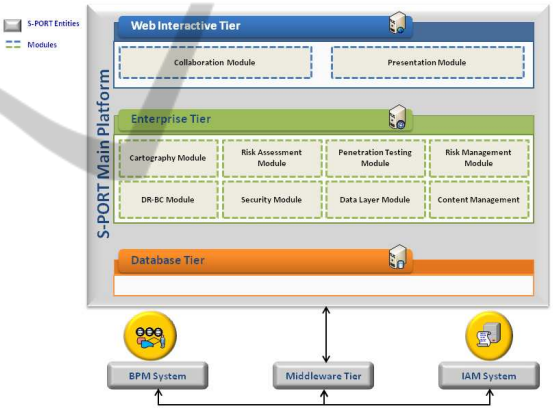

Figure 1: S-PORT collaborative environment - architecture.

More specifically, the *S-PORT main Platform* consists of:

- The **Web Interactive Tier** which is based on Web 2.0 technologies and open source solutions (i.e. Ajax forms, popup help menus, charts etc.), is responsible for the graphical and user-friendly representation and also the provision of collaboration among the S-PORT users. It is enriched with the Collaboration Module (enhanced with Forum, Wiki, Blog and Chat room) in order to achieve the communication between all users and also with the Presentation Module responsible for the collection and representation of the assets and the results of S-PORT-RM procedures with user-friendly manner.

- The **Enterprise Tier** which is composed by eight (8) modules, is responsible for creating and handling all S-PORT primary assets (e.g. cartography assets, risk assessment assets, risk management assets, S-PORT growing documents). The first module is the Content Management Module which is responsible for creating, edit-ing, updating and publishing all S-PORT primary and processed content in a consistent and structured way. The main modules (Cartography, Risk Assessment, Penetration Testing and Risk Management modules) are responsible for the implementation of the S-PORT-RM methodology and they handle and calculate all the basic entities and results of risk management procedures (i.e. impact / threat / vulnerability/risk values of all ICT assets). The DR-BC Module communicates with Risk Assessment and Risk Management modules in order to provide the required functionality for the design, creation and maintenance of Business Continuity (BC) and Disaster Recovery (DR) plans, according to the SPORT-RM results. The Security Module provides the essential communication between the S-PORT main Platform and the Middleware System in order to ensure the secure access of the S-PORT content. Finally the Data Layer Module contains all the necessary functionalities and required mechanisms in order to achieve the communication and inter-connection among all the modules of the Enterprise Tier with the Database Tier.
- the **Database Tier** hosts all S-PORT assets (such as ICT assets, impact categories, possible threats, vulnerabilities etc.) with their attributes and specific characteristics.

The second S-PORT entity is the *Business Process Management System (BPMS)*, which undertakes the accountability to identify and depict the business procedures of critical e-services of PICT, in order to have graphical representation of them and their primary assets. BPMS communicates through Middleware System with the Cartography module in order to have the asset identification and asset interconnections reporting.

The *IAM System* is responsible for the identity and access management, incorporates security mechanisms and policies that enhance the S-PORT environment with proper authentication and authorization properties enclosing end-user's preferences and requirements. Based on the above security procedures, different S-PORT user roles (i.e. administrators, managers, security team, internal, external users of ports) have access to specific S-PORT services according to their business role and requirements.

The final S-PORT entity is the *Middleware System* (an enterprise service bus - ESB) which is a lightweight messaging framework, ensuring that the different S-PORT entities, Main Platform, IAM System and BPM System, communicate through a common channel and the information exchanged is accurate and in standardised format. Additionally, the use of the Middleware System enables upgrading / expansion or interconnection to any external entity (service or system) if deemed necessary by future upgrades of the environment S-PORT.

S-PORT environment offers a bundle of targeted services to the PICT users in order to guide them to securely manage their PICT, according to the PDCA model (i.e. Plan -establish the ISMS, Do - implement and operate the ISMS, Check - monitor and review the ISMS, Act - maintain and improve the ISMS) of the ISO27001 security standard for the design, implementation and monitoring an Information Security Management System (ISMS).

Specifically the *Risk Assessment Services* which consist of the S-PORT-RM Phases responsible for the Risk Assessment (i.e. Cartography, Impact Assessment, Threat Assessment, Vulnerability Assessment, Risk Evaluation Phases) will help PICT users to identify and evaluate the impacts, threats and vulnerabilities of their IT assets. Each of the above Risk Assessment service are conformed with the ISO27001and guide PICT users to: identify the values of assets and their owners, identify users and responsibilities, identify the threats and vulnerabilities to the IT assets, evaluate business impacts taking into account the consequences in case of loss of Confidentiality, Integrity or Availability, estimate the risk level, assess the likelihood of a threat, esti-mate the risks level of each It asset, define the criteria accepting risks.

In addition with these services the *Practical Vulnerability Assessment Service* will help them to identify the practical vulnerabilities with the use of appropriate tools. There exists a pool of different penetration testing tools appropriate for each asset in order to find their vulnerabilities.

Furthermore the PICT users will be able to select the appropriate control / countermeasure according to the S-PORT-RM algorithm in order to protect their IT assets (with the use of the *Risk Management Service*) ensuring that all security requirements are met.

More specifically with the use of the *Security Policy / BCP Service*, the PICT users will be able to design and keep updated the security policy, business continuity plan and all the necessary documented procedures (i.e. control of documents, control of records, internal audits, corrective actions, preventive actions) of their Information System.

Finally, the *Collaborative Services* (Forum, wiki, Chat Rooms, Blog, Document Library) are responsible for the communication of the users in order to find details about the risk assessment/management procedures, discuss about security issues, find solutions about daily IT problems, report a security incident, provide training and awareness programmes in order to all PICT user are aware of the Security policy and procedures.

3 CONCLUSIONS

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. A holistic approach to security management of the PICT systems that the authors propose is the creation/enhancement of maritime targeted security management methodologies, compliant with the: ISPS code, modified ICT and CCIP security management standards.

In this context, S-Port environment is expected to become a prototype of the next generation, collaborative, Security Managements Systems, being capable of providing high levels of confidentiality, reliability, interactivity and interoperability, for the critical infrastructures of the commercial ports implementing a targeted security management methodology compliant with the ISPS and ISO27001. In addition, S-Port services hosted in the S-PORT environment guide PICT users to identify impacts, threats and vulnerabilities, find the appropriate countermeasures and maximize ports' operations efficiency and productivity.

ACKNOWLEDGEMENTS

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 for their contribution. Also the authors would like to thank ENISA for organising the Workshop on Cyber Security Aspects in the Maritime Sector.

REFERENCES

Adler, R. and Fuller, J. (2007). An integrated framework for assessing and mitigating risks to maritime critical infrastructure. In *IEEE Conference on Technologies for Homeland Security*, pages 252–257.

AS/NZS 4360 (1999). Risk management standards australia.

Balmat, J., Lafont, F., Maifret, R., and Pessel, N. (2009). MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor. In *Ocean Engineering*, volume 36, pages 1278–1286.

Brunner, E. and Suter, M. (2008). International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies. Technical report, Center for Security Studies, ETH Zurich, Switzerland.

ENISA (2011). 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.

International Maritime Organization (Accessed at 7 December 2011). available at http://www.imo.org/Pages/home.aspx.

ISO/IEC 27001 (2005). Information technology - security techniques - information security management system - requirements. http://www.iso.org.

Kang, M., Li, M., Montrose, B., Khashnobish, A., Elliott, S., Bell, M., and Pieper, S. (2009). Overview of the security architecture of the comprehensive maritime awareness system. In *Military Communications Conference (MILCOM 2009)*, pages 1–7. IEEE.

Ntouskas, T., Kotzanikolaou, P., and Polemi, N. (2011a). Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach. In *1st International Symposium & 10th Balkan Conference on Operational Research (to appear)*, Thessaloniki, Greece.

Ntouskas, T., Pentafronimos, G., and Papastergiou, S. (2011b). Storm - collaborative security management environment. In Ardagna, C. and Zhou, J., editors, *WISTP 2011*, pages 320–335. LNCS 6633.

Ntouskas, T. and Polemi, N. (2012). STORM-RM: A collaborative and multicriteria risk management methodology. In *Int. J. Multicriteria Decision Making (IJMCDM)*. Inderscience Publishers (to appear).

S-PORT Project (2011). available at http://s-port.unipi.gr/.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. In *Int. J. Service Sciences*, volume 1, pages 83–98.

Transportation Security Administration (2007). Critical infrastructure and key resources sector-specifc plan as input to the national infrastructure protection plan. Technical report, Dept. of Homeland Security, USA.

U.S. Department of Energy (2002). Resource Handbook on DOE Transportation Risk Assessment. Report DOE/EM/NTP/HB-01. Technical report, National Transportation Program, Office of Environmental Management, USA.