In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

MITIGATE*: An Innovative Cyber-Security Maritime Supply Chain Risk Management System

Armend Duzha[1], Panagiotis Gouvas[2], and Monica Canepa[3]
[1] Maggioli, Santarcangelo di Romagna, Italy
armend.duzha@maggioli.it
[2] SingularLogic, Athens, Greece
pgouvas@gmail.com
[3] Dept. of Naval, Electrical, Electronic and Telecom. Engineering, University of Genoa, Italy
monica.canepa@unige.it

Abstract

Despite the importance of Critical Information Infrastructures (CIIs) and dynamic ICT-based maritime Supply Chains (SCs) for ports operations, state-of-the-art Risk Management (RM) methodologies for maritime environments pay limited attention to cyber-security and do not adequately address security processes for international SCs.

Motivated by these limitations, we have developed and will validate a novel RM system which will empower stakeholders' collaboration for the identification, assessment and mitigation of risks associated with cyber assets and SC processes. This collaborative system will boost transparency in risk handling, while enabling the generation of unique evidence about risk assessment and mitigation. At the heart of this system is an open simulation environment enabling stakeholders to collaboratively simulate risks and evaluate risk mitigation actions. Emphasis is paid on the estimation of cascading effects in SCs, as well as on prediction of future risks.

The system is compliant with prominent security standards and regulations for the maritime sector, i.e. ISPS, ISO 27001, ISO 27005, ISO 28000 etc.

Keywords

Maritime Supply Chain, Critical Information Infrastructure, Cyber-Security, Risk Management, Cloud, BigData.

* The acronym MITIGATE stands for **M**ultidimensional, **I**n**T**egrated, r**I**sk assessment framework and dynamic, collaborative risk mana**G**ement tools for critical information infr**A**struc**T**ur**E**s. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 653212.

1 MITIGATE at a Glance

1.1 System Overview

The objective of MITIGATE is to realise a radical shift in risk management methodologies for the maritime sector towards a collaborative evidence-based Maritime Supply Chain Risk Assessment (MSCRA) approach that alleviates the limitations of the state-of-the-art risk management frameworks. To this end, we have developed and will validate a dynamic, collaborative, standards-based RM system for port's Critical Informative Infrastructures (CIIs), which considers all cyber-threats arising from the international Maritime Supply Chain (MSC), including threats associated with port CIIs interdependencies and associated cascading effects.

The RM system enables port operators to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from the international MSC. In this way, port operators are able to predict potential security incidents, but also mitigate and minimize consequences of divergent security threats and their cascading effects based on evidence associated with simulation scenarios and security assurance models.

MITIGATE emphasizes the collaboration of various stakeholders in the identification, assessment and mitigation of risks associated with the cyber assets and international MSC processes. This collaborative approach will boost transparency in risk handling by the various stakeholders, while at the same time will generate unique evidence about risk assessment and mitigation.

The collaborative approach is empowered by an Open Risk Assessment Simulation Environment (ORASE) which enables the participants in the international MSC to model, design, execute and analyse attack-oriented simulation experiments using novel simulation processes. Particular emphasis is paid on the estimation of the cascading effects, as well as on prediction of future risks (on the basis of common metrics across sectors). Based on evidence-based simulations, port operators, decision makers and other stakeholders are able to select cost effective countermeasures and compile holistic port security policies going beyond the port's CIIs isolated domain, but also to ensure the ports SC security. Furthermore, the system is equipped with real-time decision support systems, which aims at automating the process of estimating risk and enacting risk mitigation measures. MITIGATE integrates also open source intelligence data, including data from social media (e.g. Twitter, Reddit, and RSS feeds) and trusted sources (e.g. NIST National Vulnerability Database), towards enhancing its threat assessment and prediction functionalities.

Special emphasis is put in ensuring MITIGATE risk management framework and the associated collaborative security management tools compliance with existing security standards and regulations (ISPS, ISO27001, ISO27005, ISO28000).

1.2 High Level Architecture

MITIGATE aims to provide a holistic solution regarding risk management in the frame of Maritime Supply Chain Services (MSCSs). To do so, several services have to be provided such as collaborative risk management, advanced simulation and visualization of potential cyber-attacks, open intelligence services etc. In order to archive this, we have formulated a high level architecture that comprises eight coarse grained components that complement each other. These components include:

- an *Asset Modelling and Visualization* component that allows users to declare their cyber assets along with the cyber relationship and serialize this declaration in a strict format. Each organization that participates in the MSC will use it in order to create its own mapping which will be automatically linked to available vulnerabilities and attack-types.

- a *Maritime Supply Chain Service Modelling* component that allows security analysts to model the MSCSs that are performed by their organizations while also allowing to provide the mapping of existing cyber assets with the various processes and sub-processes that are defined in the context of MSCSs.

- a *Simulation and Game Theory* component that is responsible for the discovery of attack paths given a specific asset mapping and the calculations of the best defensive strategy regarding the protection of a specific cyber asset based on the game theoretical principles.

- a *Collaborative Risk Assessment* component that is responsible to guide the security analyst to perform the appropriate steps that are required for the conduction of the risk assessment for a specific MSCS as defined in the MITIGATE Methodology.

- an *Open Intelligence and BigData Analytics* component that is responsible to provide near real-time notifications regarding potential vulnerabilities related to a cyber asset of one organization that participates in the MSC through the text-mining of open sources (e.g. Twitter, Reddit, and RSS Feeds).

- *Notification and Reporting* component that is responsible to provide push notifications to the security analyst regarding any type of messages that are raised from the time-consuming operations such as the conduction of a vulnerability assessment, the calculation of risks, the processing of an open source information etc.

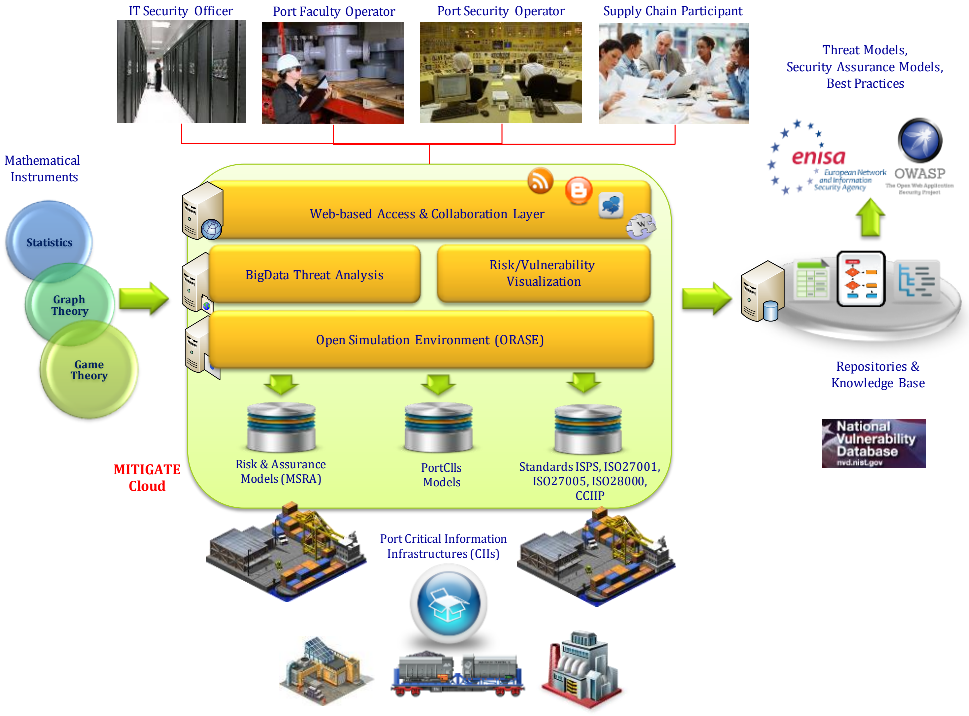
IT Security Officer
Port Faculty Operator
Port Security Operator
Supply Chain Participant
Threat Models,
Security Assurance Models,
Best Practices
enisa
European Network and Information Security Agency
OWASP
The Open Web Application Security Project
Mathematical Instruments
Statistics
Graph Theory
Game Theory
Web-based Access & Collaboration Layer
BigData Threat Analysis
Risk/Vulnerability Visualization
Open Simulation Environment (ORASE)
Risk & Assurance Models (MSRA)
PortCIIs Models
Standards ISPS, ISO27001, ISO27005, ISO28000, CCIIP
MITIGATE Cloud
Repositories & Knowledge Base
National Vulnerability Database
nvd.nist.gov
Port Critical Information Infrastructures (CIIs)

Figure 1: High-level overview of MITIGATE system

- an *Administrative* component that is responsible for the management and the consistency of the various “enumerations” that are required by all other components (e.g. vulnerabilities, attack-types, business partners).
- an *Access Control and Privacy* component that provides security guarantees in a horizontal manner to all other components.

The architecture is completed by a persistency layer and a pub/sub system. The persistency layer consists of two types of databases: one relational DB that is used to store fully structured data and one NoSQL DB that is used to store semi-structured data that change frequently (e.g. vulnerability reports). The pub/sub system is used to decouple the communication of the components, and more specifically, eliminate any blocking communication that may be required.

1.3 Target Audience

The primary target group of interest consists of the cyber-security community (researchers and practitioners) and Maritime Supply Chain participants (e.g. port authorities, maritime ministries, maritime security agencies, cyber-security agencies, maritime logistic and transport companies, insurance companies, customs).

In addition, inter(national) projects and organizations currently engaged in related research areas and standardization bodies, such as IMO, NATO, ENISA, EMSA, DIGIMOVE, DIGIMARE, constitute another important group.

2 Demo description

We will demonstrate realistic cyber-attacks that have been reported, known, assumed or suspected in our pilot sites (ports of Ravenna and Livorno in Italy, Bremen in Germany, Piraeus in Greece, and Valencia in Spain) against four Maritime Supply Chain Services (*Container Cargo Management*, *Vehicle Transport*, *Liquefied Natural Gas (LNG) Transport*, and *Solid Bulk*).

All these MSCSs might be subject of a number of cyber-threats that can be realized by conducting a combination/series of specific cyber-attacks. In this context, malicious users are able to realize complex cyber-attacks for the purpose of disrupting MSCs’ operations or facilitating illegal activities aimed at obtaining financial, political or even ideological gain and benefits. For example, they can destroy a major CII by locally or remotely disrupting, modifying, interfering or gaining access a variety of information/documentation as well as systems. To this end, malicious attackers can launch targeted attacks in order to gain unauthorized access to the ports’ systems and use them as stepping stone to lunch further, more sophisticated, attacks and penetrate deeper into their infrastructure. For example, they can infiltrate the ports’ wireless by obtaining the network identifier or through other network vulnerabilities in order to sniff, modify or inject falsified data to achieve the expected results. In addition, they can perform several phishing attacks by sending a number of emails to the port operators and/or system administrators, trying to convince them either to open a malicious PDF document attachment containing exploit code or to click on a link that will take the user to a fraudulent website that appears legitimate but contains malicious code that exploits vulnerabilities on the web browser (clickjacking attack).

In any case, the attackers can continue to exploit other vulnerabilities in various systems, either in the port network or the SCADA network, to gain unauthorized access. Therefore, they can target the port community system and takes advantage of specific software bugs and flaws that may have. In this way, the attacker can interfere, for example, with the authorization process allowing a vessel carrying illegal or hazardous materials to enter and dock at the port or even to bypass the inspection procedure. Thus, the vehicles can be transferred out of the port without being detected.

3 Lessons Learned

To ensure reliable use of the MITIGATE system in the working environment, pilot users (ports of Bremen in Germany, Piraeus in Greece, Valencia in Spain, Ravenna and Livorno in Italy) were actively engaged from the beginning of the project. Feedback during the beta tests revealed that MITIGATE is promising in addressing their needs. A positive factor specifically mentioned is that the system is fully web accessible and does not require any installation. In addition, visualization and collaborative simulation features are added value.

Further comments and recommendations are expected during the pilot operations starting in January 2017 when the first integrated and stable version of the MITIGATE system will be released. For each pilot site, the system will be localized and adopted to organizational structures and stakeholders' role.

Acknowledgments

The authors are grateful to the European Commission, Programme "*H2020-EU.3.7. – Secure societies – Protecting freedom and security of Europe and its citizens*" for the support in funding the MITIGATE project. In addition, we would like to thank all partners in this project for their contributions and efforts.

References

MITIGATE (2015) http://www.mitigateproject.eu/