Rethinking transport
27–30 April 2020

TRA 2020 HELSINKI

Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

Advances of Cybersecurity in Maritime Port Operations

Nils Meyer-Larsen[a]*, Rainer Müller[a], Katja Zedel[a]

[a]*ISL Institute of Shipping Economics and Logistics, Barkhausenstrasse 2, 27568 Bremerhaven, Germany*

Abstract

Maritime transport is central to the world economy. More than 90 percent of inter-continental goods are transported by sea. In that way, ports are a key prerequisite for economic success. Consequently, significant disruptions to large ports therefore can negatively impact maritime supply chains and can cause damage to the maritime and trading industries. In today's maritime logistics, cybersecurity is an issue of high importance. A number of incidents such as the NotPetya attack on Maersk in summer 2017 impressively demonstrate that cyber threats impose a high risk of considerable financial and reputational damage for the maritime industry. This paper presents the project SecProPort, co-funded by the German Federal Ministry of Transport and Digital Infrastructure in the IHATEC program, which aims to develop a security architecture for the communications network in maritime port operations.

Keywords: maritime blockchains; maritime cybersecurity; maritime port operations; port communications network; port community system

1. Introduction

According to Bundeslagebild Cybercrime of the German Bundeskriminalamt, 85,960 cases of cybercrime were perpetrated in 2017 in Germany alone. In the area of computer fraud, the damage amounted to € 71.4 million (BKA, 2017). The case of the NotPetya attack on Maersk Shipping Company in 2017, which left several important shipping tradelanes unavailable for several days worldwide, is estimated to have resulted in a loss of approximately $200-300 million (Heise, 2017). These and other facts clearly demonstrate that in current maritime logistics, cybersecurity is a topic of high importance, as cyber threats impose a high risk of considerable financial and reputational damage for companies involved in maritime supply chains. A maritime cybersecurity survey conducted in 2016 among maritime-related businesses resulted in the alarming fact that more than 20% of respondents had been a victim of a successful cyberattack, which caused damage to their IT systems (Safety at Sea, 2016). Consequently, sustained efforts are needed to be prepared for cyberattacks.
This paper presents the project SecProPort, co-funded by the German Federal Ministry of Transport and Digital Infrastructure in the IHATEC program. The aim of the project is to systematically develop a security architecture for the communications network in sea ports and inland ports, based on an in-depth process and threat analysis (Meyer-Larsen, 2019). More information is available on SecProPort (2018).
The paper is structured as follows: After a description of the current status of cybersecurity in maritime transport in section 2, sections 3 and 4 analyze the potentials of methodologies such as forensic investigation and blockchain

* Corresponding author. Tel.: +49-471-309838-53;
E-mail address: meyer-larsen@isl.org

technology, respectively, to support maritime cybersecurity. Section 5 presents an overview of the methodology of the SecProPort project. Section 6 finally gives a conclusion.

2. Current state of cybersecurity in maritime transport

Maritime transport plays a crucial role in the world's economy, as more than 90 percent of worldwide trade is transported by ships and handled by ports (International Chamber of Shipping, 2017). As a result, major disruptions in large ports are likely to affect global maritime supply chains and the transport and trading industries. Furthermore, failure of the port functions would not only result in financial consequences, but could also lead to supply shortages of industry and population.

In modern ports, the entire transhipment system is based on computer systems, and the exchange of data between a large number of partners involved is organised centrally. Consequently, respective information and communication systems are an attractive target for cyber criminals (Meyer-Larsen, 2018). According to Tam (2019), cyber risks and cybercrime are becoming more prevalent in the maritime sector. The difference between conventional physical attacks which were in the major scope of security measures until a few years ago and cyber attacks is that the latter can be executed from a secure distance with relatively little risk. Furthermore, it is by far more difficult to detect cyber attacks, compared to conventional physical attacks. As a matter of fact, ports are particularly challenging objects from the security perspective as they are complex organizations with a high number of involved players and many different functions crossing multiple layers (Baltazar, 2007). Ahokas (2017) comes to the conclusion that, regardless of the growing awareness of the issue of cybersecurity in the maritime domain, "much work needs to be done in order to mitigate the cyberthreats in ports".

Fig. 1. shows typical communication processes in a modern sea port. In a majority of ports, port community systems (PCS), which in fact are centralized information and data hubs, provide data exchange functionality within the port communications network. They possess a large number of technically heterogeneous interfaces to many different partners in the port such as Customs, terminal operators, ship owners, ship brokers, truck operators, rail operators, port railway, inland waterway operators, forwarding agencies, port authorities and other authorities as well as other companies. Furthermore, these centralized communication channels are supplemented by bilateral communication channels that bypass the PCS but are nevertheless highly relevant for overarching security considerations (Meyer-Larsen, 2019).

Fig. 1 Multilateral communication network in port traffic with exemplary bilateral communication processes (Meyer-Larsen, 2019)

Individual measures with respect to cybersecurity of single partners will thus not necessarily lead to a secure overall system. Consequently, even if the individual systems of the port's operators are protected according to the

state of the art, this does not automatically guarantee optimal protection of the entire port communications network with its complex interactions (Meyer-Larsen, 2019). Hence, it is necessary to implement cybersecurity measures which follow a more holistic approach, as DVZ (2019) cites a recent survey which concluded that cybercriminals are in many cases using smaller companies with a relatively low cybersecurity standard as a gateway to get access to larger companies. Furthermore, as the ongoing digitization efforts require open interfaces and communication paths between different companies, conventional IT security measures such as firewalls which restrict external communication are not suitable to provide an adequate level of security. In addition, the system-inherent openness of the port communications network to new, potentially untrustworthy, partners implies additional risks which need to be coped with by appropriate measures.

There are several different motivations for cyberattacks on ports and their systems. Firstly, criminal organizations with financial motivation exist, which seek to obtain information related to the transport of goods through cyberattacks, such as spyware data, to support criminal activities like cargo theft or smuggling. Another means of attack aims at the encryption of data of port systems by utilizing ransomware, requiring the victim to pay a ransom fee to regain access to his productive data and continue operations. Secondly, so-called hacktivists attack IT systems with the goal to simply demonstrate their capabilities by detecting vulnerabilities in IT systems. A third group are foreign governments and competing industrial companies, aiming at espionage and the identification of possible vulnerabilities of foreign port systems, which can be exploited for possible future attacks (Meyer-Larsen, 2019).

Jensen (2015) mentions a study which examined the vulnerability of the maritime industry to various cyber risks and highlighted the lack of adequate defenses. The levels of cybersecurity were found to be insufficient. Furthermore, it was shown that the percentage of incidents which were publically reported was not consistent with the estimated actual amount of criminal activity. This is likely to be caused by the fact that attacked companies are often reluctant to report incidents as they fear reputational damage.

Cyberattacks against ports can be harmful in many ways. The most common scenarios are: 1) overtake control of a ship, 2) shut down the entire port, 3) delete or modify operational data, or 4) access to restricted information (CyberKeel, 2014). It has to be emphasized that the criminals' modi operandi for performing cyberattacks have changed, taking into account the forthcoming interlinking between the different systems within the ports' communication networks. Rather than attacking the systems of individual companies, attackers often seek to become a member of the network, e.g. through manipulated user accounts, which enables him to communicate manipulated messages to other partners or to receive restricted information, in both cases with the goal to facilitate criminal activities. The identification of these manipulated messages can be difficult, as they often at first sight cannot be identified as harmful. Nevertheless, they can potentially lead to undesirable effects such as disturbance of operations and support criminal activity like cargo theft or smuggling. It is even possible that serious safety risks occur in case dangerous cargo information is manipulated and as a consequence dangerous goods are not handled properly.

As explained above, the cybersecurity of the port communications network cannot be guaranteed by individual security measures of single actors alone. In addition, a coordinated holistic concept of security requirements and measures between all relevant partners needs to be implemented. In most ports, the communications infrastructure has evolved over many years of development and adaption to the partners' requirements. Especially in the early years of system development, overarching security concepts were rarely applied. However, increasingly sophisticated cyberattacks require an appropriate cybersecurity architecture to protect the port communications network in an optimal way. Preferably automated verification procedures need to be implemented in order to be able to detect any attacks from outside or inside such as espionage and sabotage in due time and successfully defend them. In addition, effective security mechanisms for the protection against malware attacks have to be implemented, for example, in order to detect malicious software such as viruses, trojans and worms as soon as possible and to disable them. One of the foremost issues in this regard is assessing related forensic needs by understanding the scope and range of cyber risks (Tam, 2018). Furthermore, the cybersecurity architecture should provide resilience strategies in order to limit the effects in case of successful attacks. The working capacity of companies and port operations should be maintained as much as possible in such cases. Regular operating conditions should be re-established as soon as possible after an attack.

3. The role of forensic investigation in maritime cybersecurity

In literature, different definitions with respect to forensic investigation exist. Carrier (2003) defines digital forensic science as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital

sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations". According to the definition proposed in Zatyko (2007), digital forensic science is "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation". In general, the "high-level process of digital forensics includes the acquisition of data from a source, analysis of the data and extraction of evidence, and preservation and presentation of the evidence" (Carrier, 2003).
To further improve the effectiveness of countermeasures against cybercrime, especially in the maritime sector, Tam (2019) propose to apply forensic investigation, which according to the authors is "an essential response strategy following a cyber-related incident". In this regard, forensic readiness is described as the "capability to gather critical digital information and maximize its use as evidence", which is an important factor for the effectiveness of forensic measures and "key to understanding and mitigating cyber-related incidents". Other factors are "quality, and trustworthiness of the data itself" (Tam, 2019).
The major challenges in digital forensic investigation according to Carrier (2003) are twofold: The first one is the so-called Complexity Problem, caused by the fact that "acquired data are typically at the lowest and most raw format, which is often too difficult for humans to understand. It is not necessarily impossible, but often the skill required to do so is great, and it is not efficient to require every forensic analyst to be able to do so" (Carrier, 2003). The second challenge is the so-called Quantity Problem, as "the amount of data to analyze can be very large. It is inefficient to analyze every single piece of it" (Carrier, 2003). The authors propose appropriate measures like translation tools which abstract data until it can be understood and data reduction techniques to overcome these challenges.
With regard to the application of digital forensic investigation, Tam (2019) conclude that, "when compared to other sectors, the maritime sector seems behind". According to them, "there is no capacity or policy to drive cohesive forensic readiness across this sector in order to investigate known, and unknown, risks and concerns". To increase forensic capabilities within the maritime sector, the authors propose "seven steps to enhance and secure digital evidence collection across ships and ports for cyber-informed investigations, and mitigation strategies". These are in particular:

> "Step 1 Define the range of risk scenarios involving ship and port environments […]
>
> Step 2 Identify sources and endpoints, within IT/OT systems, internally and externally for various types of evidence […]
>
> Step 3 Provide secure collection and transfer methods for evidence between established sources and endpoints […]
>
> Step 4 Establish cyber, cyber-physical, policy for accessing, handling, and exchanging digital evidence […]
>
> Step 5 Specify circumstances when investigations should be held internally (e.g., ship-based, organization based) or externally […]
>
> Step 6 Train staff, crew to management, in cyber-incident awareness and secure evidence handling by establishing clear responsibilities […]
>
> Step 7 Establish or modify protocols for evidence-based documentation on cyber-related incidents." (Tam, 2019)

These steps are expected to support the improvement of the current state of forensic readiness within the maritime sector, "to have a better understanding of the scope and scale of cyber-related incidents in their sector, and have the capability to obtain the evidence needed to prevent, prosecute, mitigate, analyse, and recover from incidents" (Tam, 2019).

4. The potential of blockchains to support maritime cybersecurity

According to a publication of the World Economic Forum, the blockchain is one of the disruptive approaches that could fundamentally change the way electronic business communications operate (World Economic Forum, 2017). The blockchain methodology is in fact a kind of distributed audit-proof database, which consists of a linked chain of data blocks which are interlinked in a cryptographically secured way. As a consequence, a subsequent change of a block in the chain either results in an interruption of the chain or requires amendments to all subsequent blocks. In any case, changes of the information contained in the blockchain can be determined. The blockchain data is stored in a peer-to-peer network. The different nodes of the network synchronize with each other according to established rules, such that each of the nodes participating in the blockchain network contains a complete copy of the entire blockchain data, which enabled the verification of the data correctness at any time. The integrity of the blockchain, i.e. protection against manipulation, is guaranteed by the abovementioned built-in cryptographic concatenation, which ensures transaction security in distributed systems (Meyer-Larsen, 2019).
Consequently, blockchains are considered a suitable methodology to protect data exchange related to supply chain operations against manipulation. For example, many research projects in the area of Internet of Things (IoT) and also in the field of transport and logistics are currently developing and evaluating blockchain mechanisms (BASTONET, 2019; Eurotransport, 2019; IBM, 2018) and investigate their compatibility with organizational and legal requirements.
IBM and Maersk have set up a joint venture with the goal of using blockchain technologies in the supply chain, especially in container traffic, and to secure the transactions during communication procedures accompanying the supply chain (Computerwoche, 2018). Nevertheless, it must be taken into account that with regard to the implementation of blockchain technology in port communication systems, long transition times should be expected in which classical EDI-based port communication and new blockchain approaches will coexist. It is important to develop migration strategies, for example for the implementation of converters to communicate between traditional port communication systems and new blockchain-based systems.

5. Project methodology

Due to the reasons mentioned above, an improved understanding of cybersecurity-related mechanisms is required, in particular with reference to the transportation sector (Chiappetta, 2017). The SecProPort project addresses this issue by investigating and further developing the cybersecurity of relevant port processes. The project's aim is to develop a holistic IT security architecture for ports, which will include cryptographic building blocks like encryption, cryptographic hash functions, digital signatures, and public key infrastructures as well as comprehensive role-based authorization concepts and federated identity management. The architecture to be developed will be implemented in demonstrators that relate to a number of specific scenarios and integrated into companies' internal security concepts wherever possible and feasible. In addition, these results will also be made available to other companies in the maritime and port domain and to other industries.
The IT security architecture will consider the following four scenarios, which are subject to a requirements analysis with respect to the security architecture and will be used for the validation of the developed solutions:

1. Dangerous goods registration via the National Single Window
2. Container logistics, including direct communication between ship owner and terminal, bypassing the PCS
3. XXL logistics, involving the transport and shipment of large goods such as wind turbine or aircraft parts
4. Inland port terminal, including respective communication processes in an inland port without PCS functionality.

The identified security requirements will contribute to an industry-specific security standard that will be developed in close cooperation with key stakeholders in IT security such as the German Bundesamt für Sicherheit in der Informationstechnik (BSI) or the European Union Agency for Network and Information Security (ENISA) at European level (Meyer-Larsen, 2019).
The project started in November 2018. At the time of writing of this article, in October 2019, the first project phase was concluded, performing an in-depth analysis of communication infrastructure and related processes of the involved maritime partners. Based on the respective results, a detailed analysis of security requirements and cyber risks will subsequently be carried out, followed by the definition of security concepts which will form the basis for the development of a holistic security architecture covering the entire port communication network.

6. Conclusion

The methods of cybercriminals are constantly changing and evolving. As a matter of fact, the maritime transport industry is crucially dependent on undisturbed worldwide electronic information and communication flows, and consequently needs to be protected against respective attacks now and in the future. Thus, appropriate efforts must be taken on a holistic level, i.e. covering the complete port communication network with its variety of partners, to protect the respective communications processes in terms of confidentiality, integrity and authenticity and to make them resilient to any kind of attack. Appropriate security measures comprise the constant monitoring of communication infrastructure, cryptographic encryption, digital signatures, as well as fast and reliable detection and removal of malware. The application of forensic investigation within the maritime sector should be intensified. The implementation of blockchains can also help to ensure the authenticity or liability of transactions within the port communication network. Certifications and regular security audits, preferably in combination with recognized certification standards such as ISO / IEC 27001, should be introduced to control and document compliance with established cybersecurity measures.

Acknowledgements

SecProPort is co-funded by the German Federal Ministry of Transport and Digital Infrastructure in the IHATEC program.

References

Ahokas, 2017. Ahokas, J., Kiiski, T., Malmsten, J., Ojala, L.: Cybersecurity in ports: a conceptual approach, Published in: Digitalization in Supply Chain Management and Logistics, Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.), Oktober 2017, epubli

Baltazar, 2007. Baltazar, R. and M. R. Brooks: Port Governance, Devolution and the Matching Framework: a Configuration Theory Approach, in: Devolution, Port Governance and Port Performance. Ed. by M. R. Brooks and K. Cullinane. London: Elsevier, pp. 379–403, 2007

BASTONET, 2019. [online] Available at: <https://bastonet.com/> [Accessed 10 May 2019]

BKA, 2017. Bundeslagebild Cybercrime 2017. [online] Available at <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html> [Accessed 10 May 2019]

Carier, 2003. Carrier, B.: Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, in: International Journal of Digital Evidence Winter 2003, Volume 1, Issue 4

Chiappetta, 2017. Chiappetta, A. (2017), Hybrid ports: the role of IoT and Cyber Security in the next decade. Journal of Sustainable Development of Transport and Logistics, 2(2), 47-56. doi:10.14254/jsdtl.2017.2-2.4.

Computerwoche, 2018. IBM baut mit Maersk Blockchain Plattform. [online] Available at <https://www.computerwoche.de/a/ibm-baut-mit-maersk-blockchain-plattform> [Accessed 10 May 2019]

CyberKeel, 2014. Maritime Cyber-Risks, Copenhagen, 2014

DVZ, 2019. DVZ-Brief Nr. 18 vom 02.05.2019 / LOGISTIK, DVV Media Group GmbH

Eurotransport, 2019. Logistik sagt Manipulation den Kampf an. [online] Available at <https://www.eurotransport.de/artikel/ministerium-foerdert-blockchain-projekt-logistik-sagt-manipulation-den-kampf-an-10381602.html> [Accessed 10 May 2019]

Heise, 2017. NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust. [online] Available at <https://www.heise.de/newsticker/meldung/NotPetya-Maersk-erwartet-bis-zu-300-Millionen-Dollar-Verlust-3804688.html> [Accessed 21 March 2019]

IBM, 2018. Transform supply chain transparency with IBM Blockchain. [online] Available at <https://www.ibm.com/downloads/cas/1VBZEPYL> [Accessed on 10 May 2019]

International Chamber of Shipping, 2017. Review of maritime transport. United Nations Conference on Trade and Development, 2017.

Jensen, 2015. Jensen, L.: Challenges in Maritime Cyber-Resilience. Technology Innovation Management Review, 5(4): 35–39. http://timreview.ca/article/889, 2015

Meyer-Larsen, 2018. Meyer-Larsen, N., Müller, R.: Enhancing the Cybersecurity of Port Community Systems, in: Freitag, M., Kotzab, H., & Pannek, J. (2018). Dynamics in Logistics – Proceedings of the 6th International Conference LDIC 2018, Bremen, Germany. Springer, Cham, S. 318-323.

Meyer-Larsen, 2019. Meyer-Larsen, N., Müller, R, Zedel, K., New Concepts for Cybersecurity in Port Communication Networks, Published in: Artificial Intelligence and Digital Transformation in Supply Chain Management, Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.), September 2019, epubli

SecProPort, 2018. [online] Available at <https://www.secproport.de> [Accessed on 29 May 2019]

Safety at Sea, 2016. IHS Fairplay Maritime Cyber-security Survey – the results. [online] Available at <https://safetyatsea.net/news/2016/ihs-fairplay-maritime-cyber-security-survey-the-results/> [Accessed on 9 May 2019]

Tam, 2018. Tam, K., Jones, K.: Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy, Pages 147-164, 2018.

Tam, 2019. Tam, K., Jones, K.: Forensic Readiness within the Maritime Sector. Publisher: CENTRE FOR MULTIDISCIPLIN, 2019. ISBN: 978-0-9932338-4-5, June 2019

World Economic Forum, 2017. Tapscott, D. and Tapscott, A.: Realizing the Potential of Blockchain, White Paper, Cologny/Geneva, 2017

Zatyko, 2007. Zatyko, K.: Commentary: Defining Digital Forensics. [online] Available at https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics [Accessed on 31 October 2019]