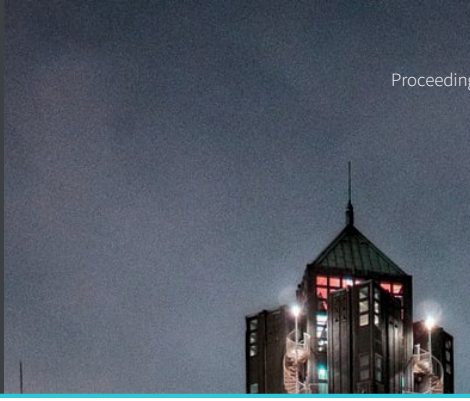
Proceedings of the Hamburg International Conference of Logistics (HICL) – 27



Nils Meyer-Larsen, Rainer Müller and Katja Zedel

New Concepts for Cybersecurity in Port Communication Networks

HICL

Published in: Artificial Intelligence and Digital Transformation in Supply Chain Management
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
September 2019, epubli

New Concepts for Cybersecurity in Port Communication Networks

Nils Meyer-Larsen[1], Rainer Müller[1] and Katja Zedel[1]

1 – ISL Institute of Shipping Economics and Logistics

Purpose: Seaports are to a growing extent controlled by IT systems. Smooth information exchange is crucial for business. Downtimes give rise to substantial financial losses and supply bottlenecks, due to the interconnections in a complex alliance of port stakeholders' systems. Hence, Cyber security in an important aspect in Port Communication Systems.

Methodology: The project SecProPort will develop a holistic IT security architecture for port communication networks, which will support the security requirements of the stakeholders' operating procedures, protect them against sabotage, and prevent third parties from illicitly gathering sensitive data or getting unauthorized access to the communications network.

Findings: The desired architecture is to be implemented by first analyzing typical attack scenarios targeted at the data processed in the port communication alliance. The next step entails designing the actual security architecture for the alliance and installing a prototype in collaboration with the application partners.

Originality: SecProPort aims at a holistic approach with respect to secure port communications networks, rather than addressing individual stakeholders. The architecture will also provide resilience measures for minimizing the impact on other actors in the alliance in case of an incident, and returning to normal operation in a controlled manner.

Keywords: Port Communication Network, Maritime Cybersecurity, Port Community System, Maritime Blockchain

First received: 10.May.2019 **Revised:** 22.May.2019 **Accepted:** 02.June.2019

1 Introduction

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. In 2016, the first maritime cyber-security survey conducted by IHS Markit in association with BIMCO among maritime-related businesses concluded that more than 20% of respondents had been a victim of a successful cyberattack, causing damage to their IT systems (Safety at Sea, 2016). Consequently, sustained efforts are needed to be prepared for cyberattacks. This paper presents the recently started project SecProPort (SecProPort, 2018), 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.

2 Current Status of Cybersecurity in Maritime Transport

Maritime transport is central to the world economy. More than 90 percent of intercontinental 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. One possible target of attacks is information and communication technologies, as in

modern ports, the entire cargo handling system today is based on IT systems and the data exchange between a large number of involved partners is centrally organized. Port community systems (PCS), centralized information and data hubs, which provide data exchange within the port communications network in many ports, play an important role here. They by definition have a large number of interfaces to many different partners: 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. The interfaces are technically heterogeneous: UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce and Transport), XML (Extensible Markup Language), RPC (Remote Procedure Call), SOAP (Simple Object Access Protocol), and other protocols, but also e-mail. In addition, there are bilateral communication channels that bypass the PCS but are nevertheless relevant for overarching security considerations (Figure 1). Securing the PCS or individual partners alone against cyberattacks therefore does not necessarily lead to a secure overall system. According to (DVZ, 2019), a recent survey concluded that cybercriminals are often using smaller companies which possess a limited cybersecurity standard as a gateway to get access to larger companies. Conventional IT security measures such as firewalls only provide limited security, because in the course of digitization the different systems in question are supposed to communicate with each other. Consequently, deliberately open access paths through firewalls must be created in order to facilitate the automation of port processes.

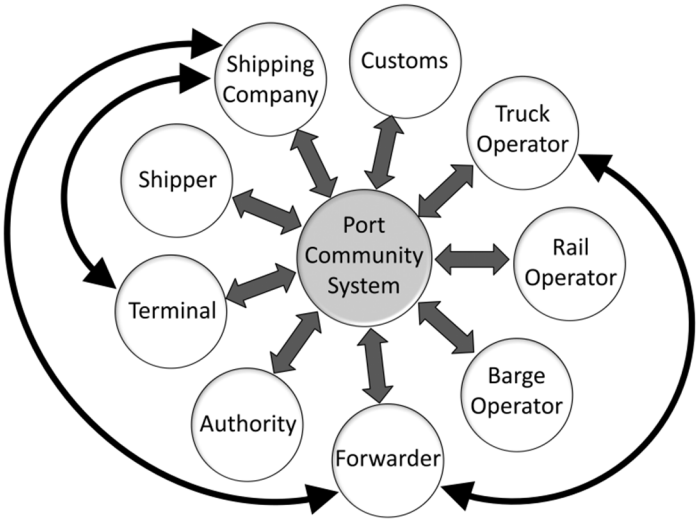


Figure 1: Multilateral communication network in port traffic with exemplary bilateral communication processes (ISL, 2019)

Cyber attacks nowadays are a high risk, as attacks can be executed from a secure distance with relatively little risk, unlike traditional physical attacks (Sensiguard, 2017). Systems can be observed over a longer time, and the discovered weaknesses can later be exploited for a large-scale cyber attack. Another problem with the continuing lack of cyber-security awareness is that attacked companies are often reluctant to report incidents "as they fear reputational damage" (Meyer-Larsen, 2018).

According to the German Bundeskriminalamt, 85,960 cases of cybercrime were perpetrated in 2017 in Germany alone, an increase of 4% compared to

2016. In the area of computer fraud alone, the damage amounted to € 71.4 million (BKA, 2017). The number of unreported cases is estimated to be very high. 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). During the attack, malicious software infiltrated a large number of computers from various companies and caused, among other things, loading and unloading processes of container vessels to stop. According to various experts, NotPetya was a Wiper Trojan of Russian origin, with the primary goal to disrupt operations and cause financial damage.

An important fact is that, due to the increasing interlinking between the various systems of each port operator, the attackers' modi operandi have changed. If an attacker succeeds in becoming a member of the network - be it through an external attack on the IT system of a participant or as an innate perpetrator - he can try to import manipulated messages into the communication network. Although these cannot at first sight be identified as harmful, they can potentially lead to undesirable effects, disturb operations, and support criminal activity. 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.

Failure of the port suprastructures would not only result in financial consequences, but could also lead to supply shortages of industry and population. Confidential data may be tapped via manipulated user accounts to en-

able or support criminal acts, e.g. drug smuggling. Last but not least, serious safety risks can arise if dangerous goods are not handled and monitored properly as a consequence of data manipulation.

There are a number of different motivations for cyber attacks on ports and their systems, as already outlined in earlier articles. First, there are criminal groups with financial or ideological motivation. In general, criminal organizations seek to obtain information through cyber attacks, such as spyware data, to facilitate cargo theft, smuggling, or even terrorism. Another variant of attack results in the encryption of data of the port systems by utilizing ransomware, requiring the victim to pay a ransom fee to regain access to his productive data. A second group is commonly referred to as hacktivists, whose main motivation is to demonstrate their capabilities by detecting weaknesses in IT systems and conducting cyber attacks, which, in the case of ports, can cause significant disruption of port operations with the above-mentioned consequences. The third group are foreign governments and competing industrial companies. Their goals are "espionage and the identification of possible vulnerabilities of foreign port systems", which can be exploited for subsequent attacks (Meyer-Larsen, 2018).

As already explained above, the IT security of a port communications network can not be guaranteed solely by individual security measures of single actors - rather, an overarching coordinated concept of security requirements and guarantees between the actors involved is necessary. The communications network in the port is usually a structure that has evolved over decades, which has been expanded and adapted over the years according to the requirements of the involved actors. Overarching security concepts were rarely used. However, an appropriate IT security architecture is man-

datory if port applications are to be protected against increasingly sophisticated cyberattacks. The system-inherent openness of the port communications network to new, potentially untrustworthy, actors requires the introduction of preferably automated verification procedures in order to be able to detect any (insider) attacks such as espionage and sabotage in due time and successfully defend them. Furthermore, the IT security architecture should implement resilience strategies in order to limit the effects of successful attacks and to maintain the working capacity of companies and port operations as much as possible. Regular operating conditions should be re-established as soon as possible after an attack. In addition, effective security mechanisms for the defense against external attacks have to be implemented, for example, in order to detect malicious software such as viruses, trojans and worms in a timely manner and to disable them.

The security of the entire communications network appears in an interplay of security requirements, measures of the involved actors, and the network infrastructure itself. The described security architecture thus places demands on the internal security mechanisms of the individual communication partners with their specific roles in the network and requires the willingness to cooperate of all involved parties. Since in many cases the involved communication partners are competitors in their businesses, a major challenge in building a security architecture is ensuring the confidentiality of information while maximizing transparency.

3 Methodology

Especially with reference to the transportation sector, an improved understanding of cybersecurity-related mechanisms is required (Chiappetta, 2017). Thus, the SecProPort project aims to investigate and further develop the IT security of relevant port processes by developing an IT security architecture for the various processes in cooperation with individual port operators. The further development of IT security in the port domain is facilitated by developing adequate migration plans and supporting software tools. A preventive approach is pursued by addressing current weaknesses in the port processes, thereby reducing the likelihood of cyber attacks on the port processes and their supporting systems in the future. Furthermore, the process-oriented approach to IT security allows a synergistic optimization of the existing work processes in ports.

As explained above, SecProPort will define an IT security architecture for the port communication network. It will be implemented in demonstrators that relate to specific scenarios. The IT security architecture will include cryptographic building blocks (encryption, cryptographic hash functions, digital signatures, public key infrastructures) as well as comprehensive role-based authorization concepts and federated identity management. Other aspects are related to information flow control, which involves intelligent monitoring of IT components within the port communications network together with attack detection in the form of intrusion detection systems and intrusion prevention systems (IDS/IPS).

The goal of SecProPort is to implement the project results into companies' internal security concepts wherever possible and feasible. The partners

represented in the project will examine to what extent the developed solutions and concepts can be integrated into the companies' internal security policies. In particular, this concerns the results of the work on the security architecture and corresponding mechanisms, on incident response management, and on migration strategies. In addition, these results will also be made available to other companies in the port environment and to other industries.

The IT security architecture to be developed is based on the following four scenarios, which are subject to a requirements analysis with regard to the architecture and later will be utilized for the evaluation of the solutions developed in the project:

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.

These scenarios in particular imply the following communication framework to be investigated within the port communication network. A bilateral communication between ship owner and terminal operator, communication via the PCS from a forwarding agent or a logistics provider and a shipowner's dangerous goods declaration via the PCS are considered. The inland port scenario considers a fully distributed communication of the partners involved.

Furthermore, the identified security requirements will contribute to an industry-specific security standard that will be developed in 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.

4 The Potential of Blockchains to Solve Cybersecurity Issues

Blockchain technology is one of the disruptive approaches that could fundamentally change the way electronic business communications operate, as the World Economic Forum writes in a publication on the potential of blockchain technology (World Economic Forum, 2017). The blockchain methodology can be understood as a distributed audit-proof database, which consists of a linked list of data blocks. In the respective next block, the predecessor block is linked in a cryptographically secured way, so that a subsequent change of a block in the chain either causes 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 network consists of a set of peer-to-peer networks that synchronize with each other according to established rules in order to verify the data contained. Each of the nodes participating in the blockchain network holds a complete copy of the entire blockchain. Compared to conventional centralized systems, the decentralized blockchain therefore has a higher reliability and an improved availability.

In addition, the integrity of a blockchain, i.e. protection against subsequent manipulation, is ensured by built-in cryptographic concatenation, which improves and simplifies transaction security in distributed systems

(Pilkington, 2016; Prinz, 2017). The important security aspects of blockchain technology include:

- manipulation and auditing security
- resilience and optimized availability
- the security of users' cryptographic identities

As explained above, the blockchain's predecessor block is linked to the next block in a cryptographically secured way. Each subsequent modification of a block alters the cryptographic key value of the block. Since this key is contained in the following block, this change is clearly recognizable and would immediately lead to discarding the changed blocks.

Blockchain mechanisms are ideal for securing transactions in distributed systems. In that way, blockchain methodology is considered suitable 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). Nevertheless, their compatibility with organizational and legal requirements must still be investigated. Technical issues in this area include crypto procedures, audit security, reliability, availability, vulnerability and tamper resistance of blockchain-based systems.

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). Even with medium to long-term penetration of blockchain technology, however, long transition times must be expected in which classical EDI-based port communication and

new blockchain approaches coexist, e.g. in the communication of mandatory reports with authorities. In this respect, the use of converters to communicate between "old" and "new" world is an important aspect.
Migration strategies are required. Dobrovnik (2018) suggests single-use cases as first steps with regard to the implementation of blockchain technology in logistics in order to minimize the risk of failure, because appropriate implementations can be based on existing conventional applications and thus support a smooth transition to the new technology. A respective approach will allow involved parties to gain experience and skills required for more advanced applications (Iansiti, 2017). SecProPort will follow this approach by investigating aspects of the implementation of blockchain technology in restricted scenarios.

5 Conclusion

The methods of cybercriminals are constantly evolving. In order to ensure that the maritime transport industry, with its dependence on electronic information and communication flows, is protected against respective attacks in the future, appropriate efforts must be taken to safeguard the respective communications processes in terms of confidentiality, integrity and authenticity and to make them resilient to attacks. These security mechanisms include the constant monitoring of the communication infrastructure, cryptographic encryption, as well as reliable detection and removal of malware. Certifications and regular safety audits can be used to check and document adherence to the security measures introduced. Corresponding regulations should be combined with recognized certification standards such as ISO / IEC 27001.

Furthermore, improved methods for authenticating the various involved partners, such as digital signatures, are needed in order to prove the identity of the respective communication partners beyond doubt. In this context, the implementation of blockchains can also help to ensure the authenticity or liability of transactions within the port communication network. With regard to the application of blockchains in maritime logistics, however, many legal and organisational issues remain open. The decentralized structure as well as transparency and immutability raise numerous problems and questions in legal terms, especially with respect to liability and data protection. Nevertheless, blockchains are expected to facilitate the digitization of supply chains, improve transaction visibility, and provide improved security against criminal activity. The use of blockchain technologies seems particularly useful in scenarios that are decentrally organized, such as in inland ports, which, unlike seaports, operate without a central PCS. Various current research projects are currently investigating these aspects. In the medium term, respective results can be expected, which will form a basis for further developments.

SecProPort contributes to respective efforts by investigating aspects of the implementation of blockchain technology and other IT security technologies in restricted scenarios. In the first project phase, a detailed analysis of relevant business processes in different scenarios was performed, which will form the basis for a requirements analysis with respect to the security architecture to be defined, followed by the development of respective concepts and tools. In the final project phase, the developed tools and methodologies will be validated and implemented within the SecProPort scenarios. Furthermore, the identified security requirements will contribute to an

industry-specific security standard that will be developed in cooperation with key stakeholders in IT security.

Financial Disclosure

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

References

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]

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]

Dobrovnik, 2018. Dobrovnik, M., Herold, D.M., Fürst, E., Kummer, S., Blockchain for and in Logistics: What to Adopt and Where to Start, Logistics 2018, 2(3), 18, 2018

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]

Iansiti, 2017. Iansiti, M., Lakhani, K.R., The truth about blockchain. Harvard Business Review. 2017. [online] Available at https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf> [Accessed on 1 June 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]

ISL, 2019. Meyer-Larsen, N., own illustration, 2019

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.

Pilkington, 2016. M.Pilkington: Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016

Prinz, 2017. W.Prinz, A.Schulte, Blockchain – Technologien, Forschungsfragen und Anwendungen, Blockchain Positionspapier, https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/FhG-Positionspapier-Blockchain.pdf, 2017

SecProPort, 2018. [online] Available at <https://www.isl.org/en/projects/secproport> [Accessed on 9 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]

Sensiguard, 2017. SensiGuard Supply Chain Intelligence Center, Global Intelligence Note 6, October 2017

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