VIENNA 2018 TRA
TRANSPORT RESEARCH ARENA
A digital era for transport
solutions for society, economy and environment

Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Cybersecurity in Maritime Logistics

Dr. Nils Meyer-Larsen a, Rainer Müller b*

[a]*Institute of Shipping Economics and Logistics, 28359 Bremen, Germany*
[b]*Institute of Shipping Economics and Logistics, 28359 Bremen, Germany*

Abstract

Major disturbances of large ports could lead to tremendous negative effects to maritime supply chains and the whole economy. Beside physical threats, ports are also vulnerable to cyber attacks due to their dependency on information and communications technology. Port Community Systems (PCSs) are information hubs for ports integrating information from various sources for global supply chains, connecting systems of terminal operators, carriers, freight forwarders and authorities. These systems are critical infrastructures – successful cyber attacks can lead to significant transport disturbances and severe consequences for the whole economy. This paper presents ongoing work within the research project PortSec, aiming at improved resilience of PCSs with respect to cyber attacks.

Keywords: Cyber Security; Maritime Logistics; PCS; Port Community System

* Corresponding author. Tel.: +49-471-309838-65.
E-mail address: rmueller@isl.org

1. Introduction

Maritime transport is of central importance for the German economy. In order to ensure the smooth flow of cargo through the seaports, electronic data transmission systems for ports, commonly known as Port Community Systems (PCS), are used. PCSs can be seen as centralized information and data hubs for ports integrating and distributing information from various sources for global supply chains. They connect companies and authorities involved in maritime transport, such as shipowners, freight forwarders, terminal operators, carriers (ocean, road, rail, and inland waterway) and authorities like Customs, in particular by providing interfaces to their systems.
Major disturbances of large ports could lead to tremendous negative effects to maritime supply chains and the economy. Beside physical threats, ports are also vulnerable to cyber attacks due to their dependency on information and communication technology. In that way, PCSs are critical infrastructure – successful cyber attacks can lead to significant transport delays and severe consequences for the whole economy.
As part of the Critical Infrastructure in traffic and transport, failures or disturbances of respective systems can lead to massive problems in port operation, in extreme cases even to a standstill. Cyber attacks on PCSs can – depending on the duration – even lead to bottlenecks in the supply of industries and population.
Confidential data could be tapped using manipulated user accounts in order to prepare for criminal acts like cargo theft or smuggling of drugs. Manipulation of data, for example in case of containers loaded with dangerous goods, could lead to storage without obtaining the legally required separation instructions. This may result in chemical reactions of hazardous substances and eventually lead to fire or explosion.
This paper describes first insights into intermediate results of the research project PortSec (PortSec, 2017). This project uses a software-centric approach in order to detect possible vulnerabilities in the field of cyber security for PCSs. The objective of the PortSec project is to develop a systematic and comprehensive IT risk management in port telematics, taking into account the underlying software architecture and including legal and economic security requirements. The software-based approach focuses on the prevention of attacks rather than their detection and defence. This approach is particularly innovative and has not yet been applied in existing procedural models and standards for the establishment of information security management systems (ISMS). One goal of the project is to develop an industry-specific security standard to prevent cyber attacks. This standard includes a certification scheme for PCSs.

2. Methodology

In order to create a catalogue of cyber security risks for PCSs, a structure to systemize these risks was created. In detail, each risk consists of the following items: a risk scenario, an asset and the motivation. The risk scenario describes the purpose of an attack on a PCS, e.g. a smuggler intends to create a Customs release for a container in order to receive the smuggled goods. An asset defines a system or a message which has to be modified, deleted or diverted in order to fulfil the attack. The motivation specifies the goal of the attack, e.g. the goal of a smuggler is to pick up a container with drugs without any Customs or other authorities' intervention.
In order to create the catalogue, the following steps have to be carried out:

(i) literature review on former cyber attacks on PCSs,
(ii) an analysis of business processes of a PCS,
(iii) brainstorming sessions on possible risk scenarios,
(iv) an analysis of the system and network structure of the PCS and
(v) an analysis of the vulnerability of the PCS software. By now, the first three steps have been carried out. The last two steps are in progress.

(i) In order to create a comprehensive overview on former cyber attacks on PCSs, a narrative literature review was carried out. Due to the fact that scientific literature for cyber attacks on PCSs is limited the literature review also includes magazines in the field of maritime logistics.
(ii) The business processes of the PCS were analysed. In detail, in several workshops with one PCS operator the business processes were analysed and modelled using BPMN (Business Process Model and Notation). Therefore, the systems, interfaces and encryption of the different software components methods were documented.
(iii) The BPMN diagrams including the technical attributes for the systems and interfaces were analysed in order to detect possible risk scenarios. Later, during several brainstorming sessions, additional risk scenarios were identified.
(iv) Next planned step is the analysis of the system and network structure of the PCS.

(v) Software components of the PCS will be analysed in order to detect possible vulnerabilities.

3. Threat Analysis

With regard to the analysis of potential threats, scenarios are developed describing possible cyber attacks on PCSs. For this purpose, the domain-specific business processes in the area of port communication are analyzed. The security requirements of the processes and the processed data are assessed as well. The analysis is designed to identify possible weaknesses, primarily related to interfaces used for communication via the Internet. In addition, the systems are examined regarding protection factors like availability, confidentiality, and integrity.
Based on the results of the threat analysis, relevant attack scenarios will be defined, and associated economic and business risks will be evaluated with regard to potential damage. For this purpose, each individual scenario will be assessed with regard to the probability of occurrence, vulnerability and consequences in order to evaluate the effects and resulting damage of possible attacks on the PCS operator, the port industry, and downstream logistics processes. The impact of attacks and resulting effects on the economy will be examined as well. Previous similar attacks will be analyzed in order to complete the picture of the threat scenarios.
A further objective of the project is the development of a method by which domain knowledge can be transferred in a formal way into the knowledge database to be developed. A respective concept will be developed followed by the implementation of a procedure which facilitates the input of domain knowledge in an automated and formalized manner. Finally, the domain knowledge about the dangers and the resulting risks will be transferred to the knowledge database. In that way, the knowledge can later be used for testing procedures.

4. Literature Review

The literature review on the current situation on cyber security in ports shows that in the past ports were mainly concerned about physical security. However, nowadays the highest risk lies in cyber attacks, which can be executed from computers thousands of miles away (Ports&Harbours, 2016). Unlike conventional attacks, cyber attacks can be performed while the attackers act from a safe distance. Attackers can monitor systems and collect information in order to detect vulnerabilities before performing an attack which could lead to major disruptions (Ports&Harbours, 2015). In contrast to physical attacks, the detection of a cyber breach is more difficult. In addition, normal insurance policies do not cover cyber attacks (Portstrategy, 2015a).
According to a study in 2013 published by the Brookings Institution, there is a relatively low level of cyber security awareness and culture in U.S. ports. Only one of the six involved ports has a cyber vulnerability assessment. None has a cyber incident response plan (DHS, 2017a). Another problem concerning lacking cyber security awareness is the fact that attacked companies, like ports, refrain from reporting attacks, as they fear reputational damages. A better mindset in reporting cyber attacks could help other ports to be prepared (Portstrategy, 2015a).
Different groups might target ports. The first group are criminals aiming on making money out of their cyber attacks. In general, criminal organisations are increasingly using cybercrime to facilitate cargo theft (Portstrategy 2015b). Thieves could try to retrieve data on the content of a container using a PCS in order to steal goods out of a container later. Besides information on the containers' contents, criminals are also interested in truck drivers' habits like regular routes and usual truck stops. Criminal organisations are able to use this information to identify the most vulnerable point in the supply chain which increases the effectiveness on their physical attacks (Portstrategy, 2015b). Next, criminals could also encrypt the data of all containers in the port. In this case the port would have to pay a ransom fee in order to get access to its productive data again. The second group is commonly known as hacktivists. They are mainly interested in proving their abilities by detecting vulnerabilities in the systems of the port which could lead to major disturbances in port operations. The third group is Governments. Their objectives are espionage and the identification of possible vulnerabilities of foreign port systems which could be used for possible future attacks (Portstrategy, 2015a).
Some attacks in the field of cyber security on ports and PCSs were reported. The most famous incident happened in Antwerp between 2011 and 2013. Hackers were recruited by an organized crime group. The group hid narcotics in containers used by legal shippers. In order to get access to the drugs later, the recruited hackers accessed the PCS of Port of Antwerp to retrieve the locations and security details of these containers. This enabled the criminals to send own drivers to pick up the containers before the legitimate owner arrived. At the beginning, the hackers used malware in order to access the IT systems. After the discovery of the malware they broke into the port premises and installed key-logging devices onto computers of the port (DHS, 2017b).
In 2012, a cargo system operated by the Australian Customs and Border Protection was penetrated by a crime syndicate. This syndicate also used legal transports by other shippers for their drug smuggling. Due to the

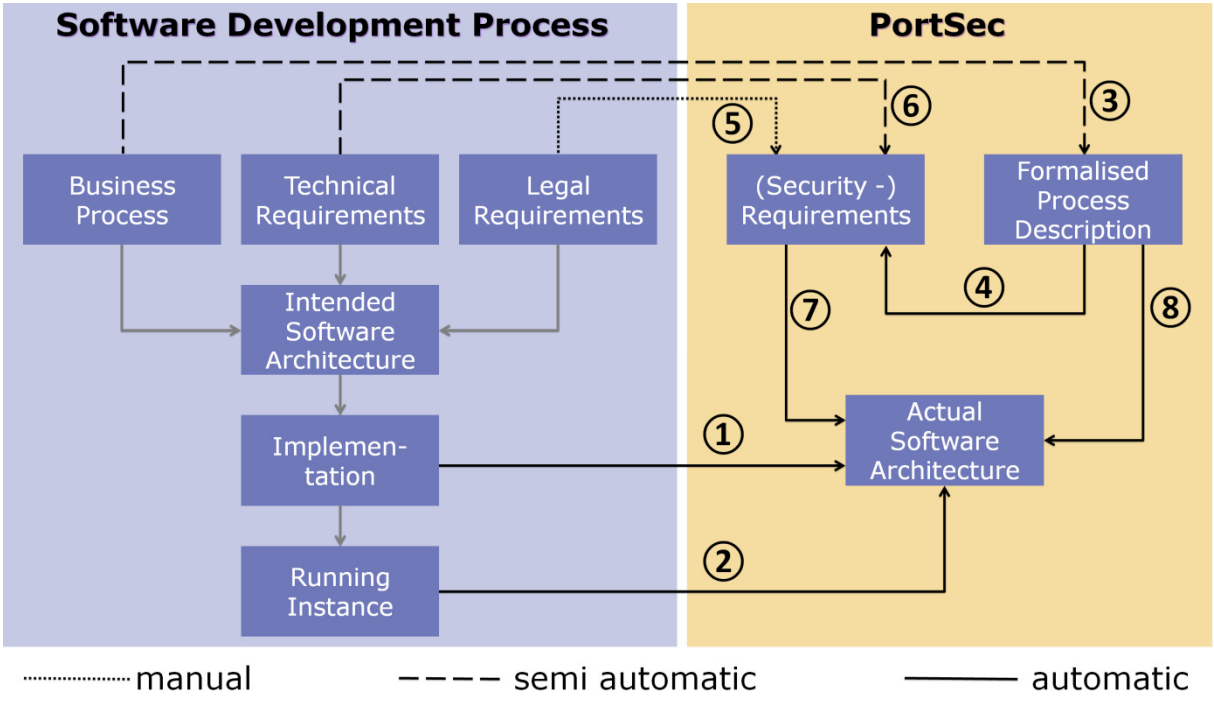

Fig. 1 Individual steps of the PortSec approach.

penetration of the system the criminals were able to check whether these containers were classified as suspicious by police or customs authorities. The crime syndicate abandoned containers which were classified as suspicious (Kochetkowa, 2015).
In March 2017, the Port of Vancouver (Canada) was subject to a Denial-of-Service attack. According to the port's spokesman, the port regularly experiences this type of attack. In contrast to previous incidents, this attack was initiated from inside of the port by a virus which infected a computer of the port's network (CT, 2017).

5. Automated testing of software

A comprehensive review of the IT security risks related to software has to identify basic security issues, e.g. with respect to software architecture (e.g., lack of encryption, incorrect authorization testing, and unprotected entry points). In particular, the architectural risk analysis must be based on the actual software implementation and not only on abstract descriptions, which are often incomplete. Since manual architectural analysis is often very complex and requires considerable expertise, this step should be supported by tools. Therefore, the PortSec project is based on a software-centric approach in which IT security risks are derived from the implemented software architecture in an automated way. Fig. 1 presents the individual steps of the planned approach.
First, the implemented software architecture is automatically extracted from the source code of the PCS, employing static and dynamic program analyses (1). This step is necessary, since PCSs in general consist of legacy software, which often lacks exact and up-to-date architectural descriptions. The software architecture analysis enables the identification of fundamental security risks of the software with regard to possible cyber attacks. The redesigned software architecture is then supplemented by descriptions of the network in which the PCS is operated (2). The network infrastructure is thereby detected automatically. Here, we can refer to preparatory work in which information about the IT infrastructure (assets) is managed with the aid of ontologies.
To consider specific security requirements for PCSs, the business processes and corresponding legal and business requirements are formally represented (3). As a result, a security evaluator can uncover situations in which unauthorized access to restricted business processes is possible and organizational control rules are circumvented (such as the task separation or the four-eye principle). This step ensures that the security requirements are in accordance with the legal and organizational requirements applicable to the operation and utilization of PCSs. The security requirements to be tested are derived from the formal descriptions of business processes (4), legal / economic requirements (5) as well as technical requirements (6).

In the next step, the actually implemented system and software architecture is evaluated with respect to the security requirements and the actual business process descriptions. This step leads to the identification of specific risks for port telematics (e.g., is it possible that an employee without authorization changes the declaration of dangerous goods containers due to excessive access rights?). At the same time, more general technical security risks are identified, e.g. insecure use of software frameworks or incorrect encryption.

6. Industry-specific security standard

The German law for the security enhancement of information technology systems (IT security law), in force since July 2015, represents the consistent development of the German Federal Government's efforts to enable IT systems and digital infrastructures in Germany to be the safest and most secure in the world. Especially in the area of critical infrastructures (KRITIS), a failure or impairment of the provision of services could result in dramatic consequences for the economy, the state, and the society in Germany and other countries. The availability and security of IT systems plays an important and central role, especially in the field of critical infrastructures.

The IT security law allows operators of critical infrastructures and their associated industries to define branch-specific security standards together with the German Federal Office for Information Security (BSI). Building on the results of the PortSec research project, a sector-specific security standard for PCSs is developed supporting the IT security law and ensuring compatibility with comparable and supplementary standards. The development of normative controls, which - similar to Annex A of ISO / IEC 27019 - must be considered as an addition to an existing ISO / IEC 27001 certification - is planned. The security standard to be developed is discussed and coordinated with relevant stakeholders in the field and the German Federal Office for Information Security as the responsible agency in accordance with the IT Security Act. Furthermore, relevant industry associations will be involved in the activities.

The industry-specific security standard to be developed consists, on the one hand, of an audit scheme which defines the scope, depth and methods of testing. On the other hand, the security standard includes a certification scheme which specifies the processes for a multi-stage certification process and defines the life cycle of certificates, auditors and test bodies. This is particularly important as the IT Security Act requires all critical infrastructure operators to provide a proof of compliance with all requirements, explicitly calling for security audits and certifications. Within the framework of PortSec, an audit and certification concept will be developed, considering PortSec results, which can be used by all operators of critical infrastructures in the area of maritime transport and traffic.

Acknowledgements

PortSec is funded by the German Federal Ministry of Education and Research (BMBF).

References

CT, 2017, Port of Vancouver meeting hindered by cyberattack, in ‘CT Report March 11, 2017, http://www.customstoday.com.pk/port-of-vancouver-meeting-hindered-by-cyberattack/, accessed 28 April 2017

DHS, 2017a, Consequences at Seaport Operations from Malicious Cyber Activity, Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA), https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf, p. 6, accessed 28 April 2017

DHS, 2017b, Consequences at Seaport Operations from Malicious Cyber Activity, Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA), https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf, p. 9, accessed 28 April 2017

Kochetkova, 2015, Maritime industry is easy meat for cyber criminals, Kaspersky Labs, May 22, 2015, https://blog.kaspersky.com/maritime-cyber-security/8796/, accessed 8 September 2015.

Ports&Harbours, 2015, Port could be falling short on cyber attack protection, in: Ports&Harbours May/June 2015, p.42

Ports&Harbours, 2016, Secure for Sea, in: Ports&Harbours November/December 2016, p.16f

PortSec, 2017, www.portsec.de, accessed 2 October 2017

Portstrategy, 2015a, Data overdrive, in: portstrategy June 2015, http://www.portstrategy.com/news101/port-operations/safety-and-security/data-overdrive, accessed 2 October 2017

Portstrategy 2015b, Who stole my container, in: portstrategy September 2015, http://www.portstrategy.com/news101/insight-and-opinion/port-talk/who-stole-my-container, accessed 2 October 2017