HOW PORT SECURITY HAS TO EVOLVE TO ADDRESS THE CYBER-PHYSICAL SECURITY THREAT: LESSONS FROM THE SAURON PROJECT

N.P.H. ADAMS[1], R.J. CHISNALL[1], C. PICKERING[1] & S. SCHAUER[2]
[1]InnovaSec Ltd, UK
[2]Austrian Institute of Technology, Austria

ABSTRACT

Ports are organisationally complex critical infrastructures that have to deliver reliable movement of goods and the safe transport of people. The EU is concerned that there is an increasing number of cases where ports have been subject to combined attacks on their IT and physical infrastructure for criminal gain or other malign purposes. The European Commission has funded the SAURON project (Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports) to help protect European ports from a physical, cyber or a combined cyber-physical attack. The aim of this paper is to provide guidance on how port security needs to evolve to respond to the cyber-physical security threat, drawing on concepts developed in SAURON. This paper reviews the current port security approaches and the cyber-physical security threat and then assesses how new systems and technologies under development, including SAURON technologies, may help to reduce port vulnerabilities. For example, to detect combined attacks on port infrastructure in the physical and cyber domains and identify the cascading effects of an incident in both domains to enable effective countermeasures, the SAURON hybrid situational awareness tool incorporates inputs from the physical and cyber domains and analyses their interdependencies. The goal is that once a physical and/or cyber threat is detected, the potential consequences including cascading effects in both planes will be automatically shown to decision-makers in order to give them integrated situational awareness of what is happening and how the situation could evolve, thus supporting decision-making. The benefits of such approaches are described. Security technologies need to be complemented by effective security processes operated by personnel with appropriate training: the paper uses results of a table-top exercise supported by analysis of port user requirements to identify the importance of multidisciplinary training in combatting complex combined cyber-physical security threats.

Keywords: port security, cyber security, physical security, cyber-physical security, situational awareness, training.

1 INTRODUCTION

Ports are organisationally complex critical infrastructure (CI) systems that have to deliver reliable movement of goods and the safe transport of people. The EU is concerned that there is an increasing number of cases where ports have been subject to combined attacks on their IT and physical infrastructure for criminal gain or other malign purposes. These range from the use of malware and key loggers by hackers against cargo-tracking systems in the port of Antwerp from 2011 to 2013 to the Petya and Not Petya ransomware attacks in 2017, which affected 17 shipping container terminals run by Maersk's subsidiary, including two in Rotterdam. In future, this growing threat may include acts of terrorism. An attack on a big EU port (cyber, physical or a combination) could seriously damage the port infrastructure and significantly impact its vicinity. The European Commission has specifically funded the Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports (SAURON) project to protect European ports from a physical, cyber or a combined cyber-physical attack.

During the gathering of user requirements in the SAURON project, ports stated that it would be very helpful to have generic guidance to help ports respond to the combined

ISSN: 2058-8305 (paper format), ISSN: 2058-8313 (online), http://www.witpress.com/journals
DOI: 10.2495/TDI-V4-N1-29-41

cyber-physical security threat. The aim of this paper is to provide guidance to ports on how port security needs to evolve in response to this threat.

The approach of this paper is to review the current port security approaches which follow International Ship and Port Facility Security (ISPS) guidelines (Section 2) and the cyber-physical security threat (Sections 3 and 4), and then to discuss how new systems and technologies under development across Industry and Academia, including SAURON, may be able to help to reduce port vulnerabilities (Section 5). Security technologies need to be complemented by effective security processes operated by personnel with appropriate training: results of a table-top exercise supported by analysis of port user requirements are used to identify the importance of multidisciplinary training in combatting complex combined cyber and physical security threats (Section 6). Finally, conclusions are given and recommendations are proposed (Section 7).

2 CURRENT PORT SECURITY APPROACHES

The ISPS Code of 2003, which was implemented by the International Maritime Organization (IMO) on July 1st 2004, is a set of measures for international security that sets security responsibilities for government authorities, port authorities, shipping companies and seafarers. Cyber security does not explicitly feature in the ISPS code. Although the IMO has produced interim guidance [1] providing high-level recommendations on maritime cyber risk management to safeguard shipping, and given ship-owners and managers until January 2021 to incorporate cyber risk management into safety management on ships [2], there is a need for more comprehensive guidance to ports to respond to the cyber-physical security threat.

According to the ISPS Code, each port facility must carry out, and periodically review and update, a Port Facility Security Assessment (PFSA). The PFSA must include as a minimum the following elements (ISPS Part A 15.5):

1. Identification and evaluation of important assets and infrastructure it is important to protect.
2. Identification of possible threats to the assets and the infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures.
3. Identification, selection and prioritisation of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability.
4. Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

PFSAs are conducted by a Recognized Security Organization (RSO) and approved by the relevant contracting governments. EU Member State port security assessments are structured according to these ISPS requirements. For example, Ireland's Department of Transport, Tourism and Sport (DTTAS) has published its PFSA Template, supported by a checklist, which is used by their representatives to check compliance with ISPS [3]. The Irish PFSA Template headings use the ISPS structure shown above but ask specific questions against each heading that inspectors use to assess port compliance. Port facility security checklists used by Member States to confirm ISPS security compliance all reflect the original ISPS priority of physical security protection and identify the following types of physical assets and infrastructure (taken from the ISPS guidance) to protect:

- Accesses, entrances, approaches and anchorages, manoeuvring and berthing areas.

- Cargo facilities, terminals, storage areas and cargo handling equipment.
- Electrical distribution systems, radio and telecommunication systems and computer systems and networks.
- Port vessel traffic management systems and aids to navigation.
- Power plants, cargo transfer piping and water supplies.
- Bridges, railways and roads.
- Port service vessels, including pilot boats, tugs, lighters, etc.
- Security and surveillance equipment and systems.
- The waters adjacent to the port facility.
- Other:
  - This should include other areas that may, if damaged or used for illicit observation or other hostile activities, pose a risk to persons, property or operations within the port facility. Examples could include external oil and gas-processing facilities adjacent to the port and port waterway.

The business imperative of improving port efficiency and expanding capacity is driving port operators to make increasing use of ICT systems and connectivity to integrate and automate port operations, using intelligent systems aided by advanced communication networks and data analytics in the port environment to improve performance, supported by better data services. Internet of Things sensors and systems and new technologies such as 5G will connect vessels with ports and maintenance services more effectively and decision support tools will reduce inefficiencies across the entire supply chain. However, the new ICT technologies being implemented in ports are also raising concerns about cybersecurity risks and about their impact on the protection of privacy taking into account new regulations on data management and protection such as the General Data Protection Regulation. Cyber-attacks on systems and technologies used for container terminal operations and cargo handling, including inventory and container tracking systems, can cause significant disruptions to such operations. At the same time, maintaining and enhancing security without slowing down commercial operations and port productivity is a key port customer requirement. Interviews with port stakeholders when identifying their user requirements for the SAURON project have stressed that security solutions must support port operations for ports that operate on a 24/7 basis, handling high volumes of mixed cargo, containers and passengers, without imposing constraints on port performance and capacity. The combined cyber-physical security threat is growing significantly as ports become more and more digitised and automated.

3 CYBER-PHYSICAL SECURITY AND THE THREAT TO PORTS

The key issue that SAURON aims to address is the combined use of cyber and physical security attack vectors to compromise port security.

Physical security threat vectors can be used to compromise cybersecurity controls, for example:

- An attacker or inside-actor gains access to a server room, and can then install devices that capture confidential data, insert infected media to compromise security, etc.
- An attacker or inside-actor gains access to a PC belonging to human resources, financial, commercial staff, etc. and gets information on employees or business plans/IPR or carries out illegal financial transactions, etc.

- An attacker or inside-actor plants a key logger on a PC belonging to human resources, financial, or commercial staff and gets information on port or tenant company employees or business plans or carries out illegal financial transactions.
- An inside-actor looks over the shoulder of a port employee as they type administrative credentials into a port IT system.
- An infected USB drive is planted outside or inside the port, which an employee picks up and then loads onto a port network.
- Physical communications links could be cut at strategic points by an attacker or inside-actor.

Similarly, a threat actor may choose to carry out low risk digital reconnaissance and other preparation prior to a physical entry by threat actors (including insiders) into the port. A cyber-attack can be used to compromise physical security controls, for example:

- A PC belonging to port or tenant company staff is compromised using social engineering and phishing techniques and an attacker gets information on employees, assets and infrastructure or third-party goods which enables physical security controls to be overcome.
- An attacker or insider shuts down or manipulates footage from security cameras, allowing illegal entry to a building or facility to go undetected.
- A key-card access system is compromised, allowing an attacker to grant or remove physical access to the building.

An early example of a cyber-physical security attack was an attack, discovered in 2013, on the Port of Antwerp's cargo tracking and release system [4]. The computer system in the port allocates each container a reference number so it can be tracked as it enters the port, its location recorded while it is waiting to be picked up and also records when it is due to be picked up. According to investigators, the criminals probably hired hackers using the 'dark web' to break into the port's computer systems. Cocaine was subsequently discovered, hidden in containers from South America containing bananas and timber. The hackers accessed the system by using spear phishing and malware attacks that targeted port authority workers and shipping companies. When the initial breach was discovered and a firewall installed to prevent further attacks, hackers broke into the premises and fitted key-logging devices on to computers. This allowed them to gain wireless access to key-strokes typed by staff as well as screen grabs from their monitors, giving them passwords and access to the system. The hackers infiltrated the computerised cargo tracking and release system of two container terminals and a harbour company in the port, gaining full remote control and access to the terminal systems [5]. Once the computers were under their control, the group could follow their container and upon arrival, unload it to a location and at a time of their own choosing. The criminals then sent in their own drivers to collect the containers ahead of the scheduled pick-up. When the containers had been picked up, the hackers wiped the containers' details from the system, so when the legitimate drivers turned up there was confusion. The smuggling operation had been ongoing since 2011, and it was the disappearance of containers that alerted the port authorities to the problem and led to a police operation which resulted in the seizure in 2013 of 1,044 kilos of cocaine and 1,099 kilos of heroin [6].

This paper will focus on coordinated attacks across the cyber and physical domains that aim to subvert port security, and how related clusters of security effects can be detected and countered.

4 CYBER-PHYSICAL SECURITY ATTACK TIMELINE

Because cyber-physical systems have an attack surface that is at least as large as the separate cyber and physical systems of which is it comprised, it can be helpful in managing complexity and considering responses, to consider the key stages that an attacker may follow and, more importantly, to which a defender may react. Responses and support systems addressing elements of a typical attack-timeline may then be tailored appropriately to the phase of the attack. We do not assume that a given attack will strictly follow each element in turn; indeed, successful attacks are usually innovative and often contain elements of surprise and novelty. A typical example would be the attack on the Ukrainian electricity supply in December 2015 [7]. In the cyber domain, a zero-day attack would be typical of the unexpected or, in the physical space, an example could be a sea-borne incursion when none had been experienced by the port previously.

Over time, many generic models have been constructed describing attack stages. For example, in defence circles, the Observe Orient Decide Act loop is common. The ICS cyber kill chain [8], based on work by Lockheed Martin, is widely used, and this has been extended and refined by many others (for example Loukas [9]). The main stages are:

1. Initial intent or determination to launch an attack
2. Gaining preliminary understanding of the target through background research
3. (Hostile) reconnaissance
4. Vulnerability determination
5. Intrusion
6. Validation (*in situ* testing)
7. Attack delivery (and defender real-time response)
8. Consequence management (for the defender only)

From the defender's perspective, defence of a cyber-physical system can only really begin when there is something to detect, from steps 3 through to 8, and can be aided by defensive systems, integrated with understood procedures and delivered by skilled and trained staff.

Reconnaissance (step 3), 'testing the boundaries', represents the first element of an attack that may be detected. For example, IT systems typically record all approaches to the external perimeter through firewall logs and physical systems through a variety of means, including access control logs and CCTV recordings. However, identifying important incursions from the general background 'noise' is known to be difficult, and several big data and inference-driven approaches have been used to augment staff skills (for example [10]). In order to minimise nuisance alarms, the sensitivity of such detection methods should be scalable with the perceived threat level. The response to steps 4 and 5 is business-as-usual for security staff who daily minimise/manage the vulnerabilities and detect intrusions. In addition, for cyber-physical systems, the cross-domain impact can and should be used to highlight attacks occurring in one domain which have knock-on consequences on the other and/or the port's operation as a whole.

Once an attack is underway (steps 6 and 7) the defender needs to generate, as rapidly as possible, an holistic situational awareness picture of the nature of the attack. Systems that assist in delivering this picture can also provide decision-support and other tools to manage and mitigate the attack. Finally, consequence management (step 8) commences during the attack but extends beyond its end and covers both real-time and post-incident communication to external stakeholders, the clean-up, restoration to normality and lessons-learned phases.

5 TECHNOLOGIES TO COUNTER THE CYBER-PHYSICAL SECURITY THREAT – LESSONS FROM SAURON

In general, EU ports have well-established physical security measures, mostly arising from the ISPS code or similar frameworks (see Section 2). Perimeter protection, physical access controls, smoke and fire detection sensors and CCTV are just a few of the measures that are commonly found in port infrastructures. The information coming from these sensors is gathered in a physical situational awareness (PSA) system, which allows a security officer to keep track of events and incidents taking place within the port. These systems have often developed incrementally over a long period of time with extensive use of legacy systems, which makes them difficult to maintain and extend.

Due to the increasing digitalisation in port infrastructures with the goal to make processes more efficient (see Section 2), the ICT landscape run by a port has increased significantly in recent years. Port operators have become managers of complex data-processing centres, highly specialised industrial control systems, sophisticated applications and multiple interconnected communication networks. This creates a need to obtain and maintain a consistent overview on what is happening in this cyber environment. Cyber situational awareness (CSA) systems serve that purpose by gathering data from various protective cyber systems running within the port's internal networks, such as firewalls, intrusion detection systems, system log files, etc., and monitoring any suspicious behaviour to identify an attack already in its early stage. Such CSA systems can be implemented within the port itself or can be outsourced to an external security operations centre (SOC). However, although most ports use such protective measures, many do not have either an internal or external SOC.

Overall, EU ports use technically advanced physical security and cyber security systems and processes to resist attacks in the physical and cyber domains. However, if an incident is detected in one domain, none of the PSA and CSA systems currently available is capable of identifying potentially related events and analysing cascading effects across the domains. They concentrate their view on their particular domain and can assess potential damage only therein. Imagine a fire breaking out in one room; this is observed by the smoke detector and indicated to the PSA. The security operator is able to assess the potential damage to the physical assets in that room and to neighbouring rooms and to plan countermeasures for extinguishing the fire. However, if a server rack is located in one of the neighbouring rooms, the security operator cannot know which cyber assets (e.g. servers, applications, processes, etc.) will be affected if the fire spreads to that room and causes the server rack to fail. Such information will be available only in the CSA, which, on the other hand, will not be aware of the fire since this is an event in the physical domain. As a consequence of these isolated views of the cyber and physical domains, complex attacks, such as the one in the port of Antwerp (see Section 3), might not be detected at all by the separate PSA and CSA systems.

The main goal of the SAURON project is to close this gap between the physical and the cyber domain, i.e. between the PSA and the CSA, and interlink the assets in both domains to gain a better overview on the interrelations and the interplay between them. To achieve this, a conceptual framework and methodology for a hybrid situational awareness (HSA) tool has been developed (see Fig. 1) that can determine the potential consequences of any relevant incident detected either by the SAURON PSA or by the CSA system and show the potential cascading effects in both domains [14].

The HSA system consists of two main modules: a threat propagation engine (TPE) and an event correlation engine (ECE). The TPE is responsible for identifying and analysing potential cascading effects. The TPE receives an overview on all physical and cyber assets from

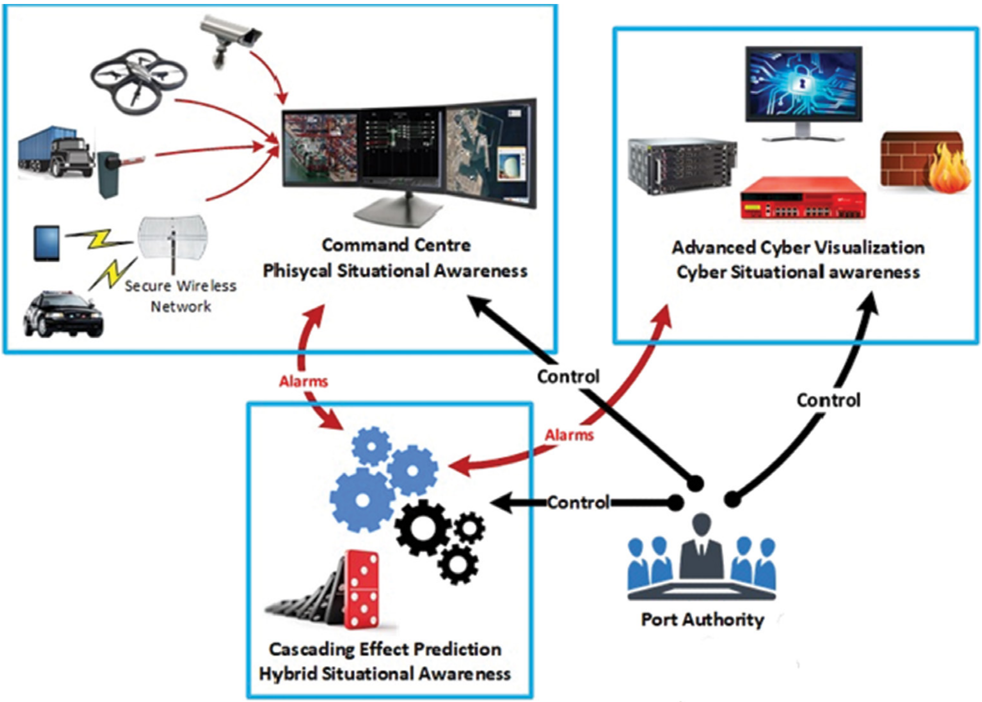

Command Centre
Phisycal Situational Awareness
Secure Wireless Network
Advanced Cyber Visualization
Cyber Situational awareness
Alarms
Control
Alarms
Control
Control
Cascading Effect Prediction
Hybrid Situational Awareness
Port Authority

Figure 1: Conceptual overview on the interaction between PSA, CSA and HSA

the PSA and the CSA, respectively, and interlinks these assets across the two domains, where necessary. For example, if a specific application *A* is running on a server *S*, which itself is installed on the hardware of a server rack *R*, the physical asset ‘*server rack R*’ (and thus also its location within a room) is linked with the cyber asset ‘*server S*’ and the ‘*application A*’ running on that server. In this way, a comprehensive graph of all the interdependent physical and cyber assets within the port is created.

This interdependency graph represents the basis for the mathematical approach used for the computation of the potential cascading effects. This approach comprises two parts [15]: an outer model which consists of the interdependency graph of all physical and cyber assets and an inner model, where each asset is represented by an automaton, which characterises the different operational states an asset can be in (see Fig. 2). In detail, such states can be described textually (e.g. ‘*fully operational*’ or ‘*complete breakdown*’) or represented by numbers (e.g. ranging from 1 to 3) and are usually defined by the port operator itself. A transition from one operational state to another depends on the incident happening to the asset but is not deterministic. Rather, the transition takes place with a specific probability, which better reflects the uncertainty of these complex processes in reality. In other words, a fire might cause a ‘*complete breakdown*’ of an asset with a certain probability by destroying it but with some smaller probability, the assets might just end up with a ‘*reduced capacity*’ but still be operational. Moreover, any change in the operational state of an asset also affects its neighbouring assets due to the interdependencies between them. In this way, any change in the inner model also affects the outer model of the interdependency graph.

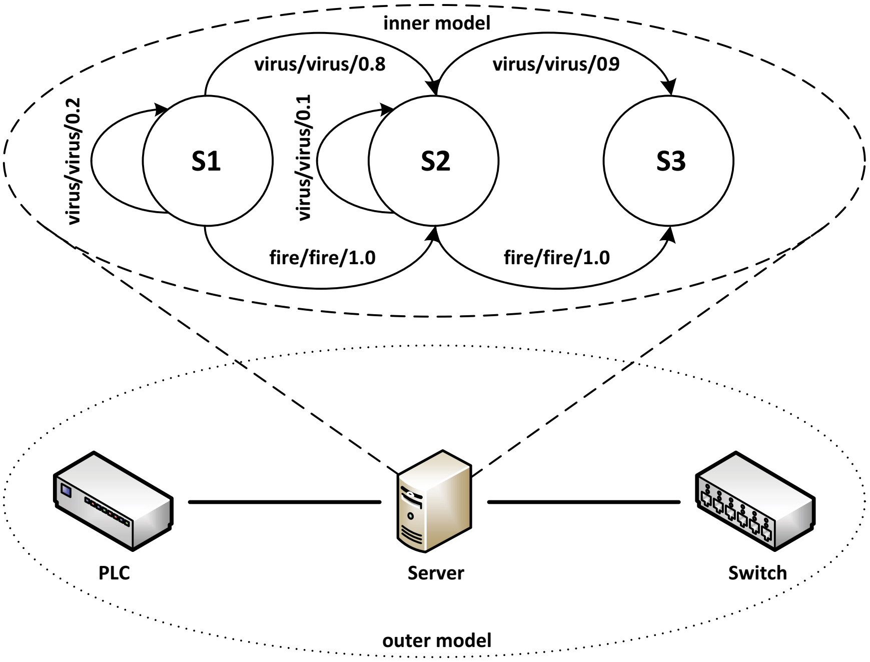


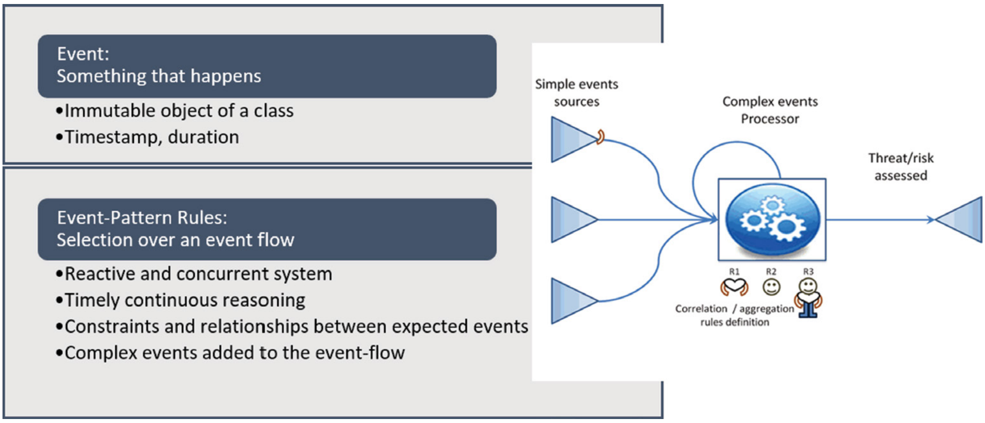
Figure 2: Illustration of the inner and outer model in the threat propagation engine.

Based on this mathematical approach, the TPE is able to simulate an incident happening to one individual asset together with its effects on the entire port infrastructure. In detail, a simulation starts with changing the operational state of one asset (e.g. a room) due to an incident (e.g. a fire). As described above, this also affects the neighbouring assets (e.g. other rooms in that building), changing their operational state with some probability. In this way, the effects propagate through the graph of all assets; at the end of a simulation run, the TPE shows the final state of all assets in the graph. To obtain a statistically reliable result on the operational states of each asset, the TPE performs a large number of simulation runs for a specific incident. These results are then used to make an estimation of the worst-case damage caused by the incident. Thus, the security officer is provided with a comprehensive overview on the full magnitude of the incident's cascading effects. Furthermore, the security measures can be planned according to this overview, e.g. by implementing measures to counter larger indirect effects instead of combating direct effects, to avoid the worst-case scenario.

As an extension to the assessment of cascading effects carried out by the TPE, the ECE aims at identifying complex attack strategies, which cannot be detected by either the PSA or the CSA separately. By collecting information and data about the current situation both in the physical and in the cyber domain, the ECE builds up a comprehensive understanding of the current status of the assets in both domains. This understanding is then used to identify malicious situations and abnormal behaviour, which could indicate an attack on the port, based on predefined rules (e.g. logical and timely sequence) on how events should take place within the port. Such a malicious situation could be the following: imagine an employee who is a database administrator being captured by a video camera in a secure area. Due to facial recognition, he is identified but since he has a clearance for the area, no alarm is raised in the PSA. Nevertheless, the detection event is sent to the ECE. A few seconds later, the user name and password of the database administrator are used to physically log into a computer in the server room. This individual event is detected by the CSA but since the user name and password are correct, this does not raise an alarm; still, the information about the login is sent to the ECE. Due to the very short time frame between the two events, the ECE infers that something is going wrong since the person is not able to get from the location of the facial recognition to the server room in a few seconds. Consequently, the ECE highlights this abnormal situation to the security officer to investigate what is going on.

The ECE operates in real-time to initiate actions arising from events (event-objects) derived from a variety of heterogeneous sources. An event-object, is simply a representation of something that occurs, not necessarily an alarm although alarms are treated as a subset of events. Its semantic representation is characterised by time of occurrence, by location and possibly by duration. The representation is not unique and several event-objects can have the same representation, differentiated by the purposes for which they are used. The implementation of the ECE is based on Drools Fusion [11] and follows its inference rule syntax that uses both combinatorial and temporal logic syntax. Event types can be defined in an hierarchical fashion so that sub-types can use the 'is-a' inheritance relationship to easily inherit rules and reduce the effort need for rule creation. The ECE is stimulated each time a new event satisfies at least one rule (see Figure 3), the rules being latent until stimulated. The rules themselves are derived from a prior risk analysis of the port infrastructure which allows them to be configured for each port uniquely while drawing on rules that correspond to risks that are common to all ports. When one or more rules are triggered, the ECE creates a Hybrid Alert, which is sent to the Threat Propagation Engine and displayed to the security staff.

By combining the capabilities of the TPE and the ECE, the HSA represents an additional benefit for the port operator and its security officers over the individual application of a PSA and a CSA. On the one hand, the HSA provides a concise cyber-physical picture of the entire port infrastructure and thus is able to detect complex, cyber-physical security threats. On the other hand, the HSA simulates the potential cascading effects a single incident can have on the port's entire cyber-physical infrastructure and thus is able to calculate an extensive estimation of the (worst-case) damage caused by that incident.



Event:
Something that happens

- Immutable object of a class
- Timestamp, duration

Event-Pattern Rules:
Selection over an event flow

- Reactive and concurrent system
- Timely continuous reasoning
- Constraints and relationships between expected events
- Complex events added to the event-flow

Figure 3: Illustration of the event correlation engine.

6 PROCESSES AND TRAINING TO COUNTER THE CYBER-PHYSICAL SECURITY THREAT – LESSONS FROM SAURON

A key part of the port security process is the use of inspections (PFSAs) as described in Section 2 together with drills to practice security procedures and processes and training exercises using a range of scenarios. These activities are used to test port security arrangements and identify potential improvements. ISPS guidance [12] specifies that various types of exercises which may include participation of company security officers, port facility security officers, relevant government authorities and ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability and response. These exercises may be:

- Full scale or live;
- Simulations involving selected teams and functions in their operational stations;
- Table-top simulations; or
- Combined with other exercises held such as search and rescue or emergency response exercises.

For emergency response training, simulations such as table-top exercises, drills, and full-scale exercises are particularly valuable for practicing decision-making skills, tactical techniques and communications. In practice, a table-top exercise often provides an excellent opportunity to flexibly and speedily review potential critical incidents and vulnerabilities with key personnel since problem areas can be readily identified and discussed and the plans can then be modified accordingly [13].

To understand the challenges faced by ports in responding to the combined cyber and physical security threat and identify issues that will need to be considered in the SAURON port pilot validation activities in 2020, the SAURON team ran a table-top exercise at the European Association of Airport and Seaport Police (EAASP) Annual Conference on 15 May 2018. The goal was to examine how ports might react to a cyber-physical security incident and what lessons can be learnt for EU port security.

The exercise involved 70 policy makers, airport and seaport police and security representatives, border force personnel and airport and seaport customer security staff from across Europe. The workshop ran for 90 min, with attendees split into three teams acting as if part of an emergency control centre team, for what transpired to be a cruise ship scenario involving a cyber-physical security breach where terrorists used cyber and physical means to set up the conditions for and execute a terrorist attack on a cruise ship. The full attack scenario lasted 6 months from start to finish.

Participants were split into three diverse teams to give an appropriate mix of skills. The table-top exercise followed the scenario, with participants being briefed on the current situation at various stages of the attack and then being asked to decide what they would do based on their security expertise and current procedures. Participants were not told at the start of the exercise about SAURON and that it addresses cyber and physical security challenges to ensure that their reactions were as realistic as possible for the purposes of the workshop. They were asked to consider that they were part of the facility security management and response team in a port emergency control centre that monitors port activities 24/7, 365 days a year, responsible for making decisions about safety and security issues and the management of emergencies. Briefings included descriptions of ship movements, construction activity, expected visits, security updates and other standard port operational matters as well as incidents with potential security implications, simulating a busy port where there are many potential issues for security teams to be aware of.

Key points that emerged from discussions during and after the exercise included:

1. When issues were presented that were potentially consistent with both a cyber security breach and a physical security breach, the teams focused more on the potential physical security breaches rather than potential cyber security issues, which were assigned to responsible staff rather than being explored in a multidisciplinary manner.
2. A combined cyber and physical security attack of this type poses multiple potential security issues that all need to be investigated and resolved quickly which could require significant extra resources.
3. There are many different kinds of port plans for cyber security, e.g. incident response plan (including cyber security), cyber security plan, business continuity plan (including cyber security), etc. which made port responses more difficult. Port cyber security plans are not standardised and concerns were expressed that they might have inconsistencies or gaps which may cause significant challenges if combined cyber and physical security attacks are mounted against ports and different security problems need to be considered together.
4. In the early stages of the simulated attack, which included some initial cyber security breaches 6 months before the final attack, the teams concluded there was not enough information to define the security problems as a major cyber incident (which the NIS Directive requires should be reported), though they would (probably) report it to the appropriate CERT. If there is a cyber security breach (key logger, phishing attack disabling computer and infecting others, etc.), a port may not have the information at this stage to judge if it is a major cyber security incident or not. This becomes very important but that is only apparently 6 months later.
5. Combating a complex cyber-physical attack requires the development of clear plans and procedures that can be practiced (e.g. in table-top exercises) and are easy to use in a rapidly changing situation. Participant responses to potential indications of cyber and physical security problems were uncertain and varied significantly throughout the exercise in contrast to their clear consistent responses to, for example, a simulated physical armed attack, where plans are well developed and regularly rehearsed across member states.
6. All ports carry out similar types of security training exercises as required by ISPS regulations. Participants stated that they found the SAURON exercise very useful and that it had raised interesting issues for them to consider for a combined cyber-physical security attack the table-top exercise had practiced. This type of table-top cyber-physical security exercise could assist some EU ports in their security training and help increase awareness of the cyber-physical threat.

Current operator training in physical security and cyber security is carried out separately: there is no multidisciplinary ‘hybrid threat’ training. Although technology can help operators to better coordinate their responses across the physical and cyber domains, the exercise suggested that an additional ‘social’ dimension needs to be considered. Furthermore, additional training is needed to help operators to respond holistically to combined cyber and physical attacks and to manage cascading effects between one domain and the other. This will be investigated in more detail in the SAURON exploitation activities as it will affect the successful implementation of cyber-physical security measures in ports.

7 CONCLUSIONS

This paper reviews the current port security approaches which follow ISPS guidelines together with the cyber-physical security threat that ports face. Overall, EU ports use technically advanced physical security and cyber security systems and processes to counter attacks in the physical and cyber domains. However, if an incident is detected in one domain, none of the PSA and CSA systems currently available is capable of identifying potentially related events and analysing cascading effects across the domains. To combat the future cyber-physical security threat, ports and other CIs need to develop security systems that link the two domains and can assess the implications of such interrelated cascading effects.

This paper describes how new systems and technologies under development across Industry and Academia may be able to help to reduce port vulnerabilities. One such approach has been developed in the European Commission-funded SAURON project, as described in this paper. The SAURON HSA tool incorporates inputs from the physical and cyber domains and analyses their interdependencies. The goal is that once a physical and/or cyber threat is detected, the potential consequences including cascading effects in both planes will be automatically shown to decision-makers in order to give them integrated situational awareness of what is happening and how the situation could evolve, thus supporting decision-making. The results of a table-top exercise supported by analysis of port user requirements are presented to demonstrate the importance of multidisciplinary training across physical and cyber security domains to combat complex combined cyber and physical security threats. Port and other CI security technologies to combat the combined cyber-physical security threat need to be complemented by effective security processes operated by personnel with appropriate multidisciplinary cyber and physical security training.

ACKNOWLEDGEMENTS

This work was supported in part by the EC SAURON project (http://sauronproject.eu) under grant agreement No. 740477 addressing the topic CIP-01-2016-2017. The authors would like to thank Nicolas Museux of Thales and other SAURON project members for their valuable insights.

REFERENCES

[1] IMO Interim Guidelines on Maritime Cyber Risk Management, MSC.1/Circ. 1526–2016.

[2] IMO resolution MSC.428(98) 2017, Maritime Cyber Risk Management in Safety Management System (SMS).

[3] Irish Government Department of Transport, Tourism and Sport: Maritime Security Ports Publications - Port Facility Security Assessment Checklist, Port Facility Security Assessment Template.

[4] Bell S., Bullguard Blog, Cyber-attacks and underground activities in Port of Antwerp, October 2013.

[5] BBC News, Police warning after drug traffickers' cyber-attack, 16 October 2013.

[6] Europol EC3, Hackers deployed to facilitate drugs smuggling, Intelligence Notification 004-2013, June 2013.

[7] SANS Institute and US Electricity Information Sharing and Analysis Center: Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, March 2016.

[8] Assante, M. & Lee, R.M., The Industrial Control System Cyber Kill Chain, SANS Institute Information Security Reading Room, October 2015.

[9] Loukas, G., *Butterworth-Heinemann, Cyber-Physical Attacks (1st Edition): A Growing Invisible Threat – Chapter 5 Cyber Physical Attack Steps*, June 2015. Paperback ISBN: 9780128012901. eBook ISBN: 9780128014639.

[10] Kantarcioglu, M. & Xi, B., Adversarial data mining: Big data meets cyber security. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (Vienna), pp. 1866–1867, October 2016. DOI: 10.1145/2976749.2976753.

[11] Proctor, M., Drools: A rule engine for complex event processing. *Applications of Graph Transformations with Industrial Relevance. AGTIVE 2011. Lecture Notes in Computer Science*, eds. A. Schürr, D. Varró & G. Varró, vol. 7233. Springer: Berlin, Heidelberg, 2012. DOI: 10.1007/978-3-642-34176-2_2.

[12] ISPS Part A Section 13.7.

[13] Vendrell, E.G. & Watson, S.A., Part of ‘The Professional Protection Officer’, 2010, Elsevier.

[14] Schauer, S., Rainer, B., Museux, N. et al, Conceptual framework for hybrid situational awareness in critical port infrastructures. Critical Information Infrastructures Security. 13th International Conference, CRITIS 2018, Kaunas, Lituania; September 24–26, Revised Selected Papers, 2019, Springer, Cham.

[15] König, S., Rass, S., Rainer, B. & Schauer, S., Hybrid dependencies between cyber and physical systems. Intelligent Computing. Proceedings of the 2019 Computing Conference, vol. 2, 2019, Springer Cham.