Generating data sets as inputs of reference for cyber security issues and industrial control systems

Thomas Becmeur, Xavier Boudvin, David Brosset, Gaël Héno, Benjamin Coste, Yvon Kermarrec, Pedro Merino Laso

Generating data sets as inputs of reference for cyber security issues and industrial control systems

Thomas Becmeur*, Xavier Boudvin*, David Brosset*
Gaël Héno*
* Ecole Navale - 29460 Lanveoc, France
David.Brosset@ecole-navale.fr

Benjamin Costé* †, Yvon Kermarrec*†,
Pedro Merino Laso *†
IMT Atlantique - 29238 Brest, France
Yvon.Kermarrec@telecom-bretagne.eu

***Abstract*—In this paper, we present a platform we have designed and built in order to generate data and scenario traces that can serve as inputs and references when evaluating our algorithms for detecting cyber security intrusions. Our context is related to civilian and military ships and our research is performed within a strong partnership with industry and academy. As obtaining actual and accurate data sets are not straightforward, we have chosen do generate realistic datasets with a platform we have designed and built.**

***Keywords*—security of ICS - SCADA - ship simulation .**

I. Introduction

Both civilian and military ships are present on the various seas and oceans and handle a large extent in the exchange of goods in international trade. Ships also ensure to a large extent to travelers' mobility by ferry and giant cruise vessels. There is a huge diversity of both mission and functionality provided by a ship which must assemble numerous systems (mechanical, computer- and electronic- based, engines and propulsion, etc.) to support them. These make it possible to build larger, faster and more powerful ships.

Security has always been a concern in the ship industry, because of the crew, of the values of conveyed goods, and the impact of wreckage on the maritime environment. Ship piracy has also evolved with the information and communication technologies. New forms of threats arise due to the ubiquitous internet on board the vessels: a 'remote' pirate can gain control and operate a ship as what we have seen with cars on highways; a pirate can also forge and send false signals (e.g.; GPS) or alter electronic navigation maps.In this context, 2 French academic institutions and 2 major industries have joined their forces in order to investigate new approaches for detecting and preventing cyber attacks in the maritime context and to raise awareness.

In this paper, we present a platform that we have designed and built so that we can evaluate the approaches and algorithms we propose and compare their benefits. For this purpose, we need data sets of reference which can present various situations that can then be served as inputs for our algorithms. In the first section of this paper, we present the rationale and our motivation for building our platform. In the second section, we describe its components and organization. In the third section, we highlight a specific extension of our generic platform that has been performed to detect anomalies and possible attacks. In the final section, we conclude with a synthesis of our ongoing activities and the future plans we have as perspectives to improve our platform.

II. Our design criteria for a platform

As indicated, our aim is dual when designing our platform: it should have an educational concern since it will be used to raise awareness on cyber security in the maritime context. It should also allow us to implement and evaluate new algorithms and approaches to detect anomalies and attacks that can put a ship in jeopardy or destroy it. Our design criteria and requirements are as follows:

- Similarity to existing ships and naval systems: this constitutes our major criterion as we need to raise attention and awareness within the naval community. A ship is, of course, a large and complex system made of thousands of hardware and software components that interact to ensure the different missions of a ship.
  We need a demonstrator so that maritime stakeholders (and also industrialists) can understand what is involved and how to deal with a cyber crisis.
- Integration of Industrial control system and SCADA.
  A ship integrates several ICS (for operating the anchor, for opening valves in pipes, etc.) and appears in a way to a classic factory, except that it is located on the sea and moving. Vulnerabilities in ICS have been *de facto* imported by ship and we wanted to raise attention on them as they do and control critical functions on a ship.
- Modularity : the platform is to be used in a research context and therefore we expect it will evolve.
- Usability in an education context. We intend to schedule labs and involve students in projects, so that they can experiment and investigate security issues by using our platform. This requires debugging and visualization tools so that their software development can be successful.

III. Our platform

To meet these requirements we have selected 2 subsystems that we can find on any ship and which provide critical functions for sailors:

978-1-5090-5476-3/17/$31.00

- The propulsion and the engine control. A propeller is the key component of this subsystem inside a boat. In our platform, we have duplicated the component so as to simulate a large boat with two distinct and autonomous engines. Because of cost constraints, we have replaced the propeller with a computer fan (and even if their destination is quite different, the similarities between both devices are numerous and explicit in the context of demonstrations). The engine and the propeller are characterized by their status (on or off) and also their speed (expressed in rotations per minute) and we may include additional characteristics (*e.g.*; temperature, vibrations).
- The navigation subsystem, and the rudder in particular, make it possible to change the direction of the ship. On a traditional boat, the governor control lever consists of a helm.Here also we have duplicated the rudder and the lever so as to have a similarity with a large boat (*e.g.*; a tanker or a container ship).

We have selected them because both sub systems are critical when at sea or in the harbor. Every sailor knows the impact of the unavailability or alteration of one element on the ship. Moreover, these 2 subsystems constitute an interesting domain as we can build scenarios in which one of the sub-systems is made unavailable or not responding to commands properly (*e.g.*, at sea, when a ship navigates we can set the speed of a regime that goes beyond the engine limits or ignore warning on temperature elevation), and scenarios where an attack on both sub systems can impact the ship seriously (*e.g.*, in a harbor, in the landing operation to reactivate the engines and to set the rudder to the opposite angle with respects to the docks).

A. Architecture and hardware issues

As indicated earlier, we have chosen to focus on ICS and SCADA. For our platform, we have installed 2 automata and each of them is responsible for one of the sub systems: one for controlling the ship direction and the 2nd one for controlling the engine and its speed in particular. Each automaton integrates a CPU (*e.g.*; in order to execute the application control code) and a communication processor which provides industrial protocol features (*e.g.*; in order to exchange data between the automaton and its environment, with ModBus, DNP3, S7).

We have also configured and installed a central coordinator (a Raspberry PI) which ensures the communication between the automata and also conveys commands and requests to/from the SCADA system. The central controller appears as an intermediate between the SCADA and the automata and therefore plays a central role in the overall architecture. The Raspberry PI provides a low-cost processor and a data flow orientation that fits our needs and requirements. Even though, we are in a prototype context, the communication bandwidth and speed make it possible to address various kinds of data flow density and to perform various controls and actions on the messages that are received or sent.

Both hardware elements (the central coordinator and the CPUs of the automata) are fully programmable. Both are equipped with software environments and specific programming paradigms that make it possible to implement various controls, to execute code and to raise alarms if needed. In this paper, we present in the next section one example of such a control which can ensure consistency between both sub systems and a global property for our ship demonstrator.

a) : A ship operates in a complex environment that is composed of numerous sensors and effectors: a sensor can measure the temperature of the engine parts that is then fed into a controller to ensure the safe operation of the engine, a GPS chip can also acquire the ship position and can relate it on electronic maps,... All of these sensors and effectors are complex by themselves and we chose to exclude them from our platform, as their integration would go beyond the scope of our project and its timeline. Nevertheless to have a higher similarity with a real ship, we have decided to simulate them. For this purpose, we have configured and programed Arduinos and they can provide (at low cost) input/output data to our platform components. They can also be programed easily and provide various schemes to manage and contribute to various scenarios.

IV. CONCLUSIONS

In this paper, we have presented the platform we have designed and developed with emphasis on cyber security awareness in the context of a maritime environment. SCADA systems are numerous on board and ensure critical functions when a ship is at sea or landing in a harbor. Our major achievement is to have designed a realistic and ICS with high similarities to what is available on ships. Based on the early feedback we have received during demonstrations of the scenarios we presented, we believe that we have been able build a realistic environment and the data that are generated by the platform appear usable.

In our team, PhD students investigate new algorithms and innovative approaches for detecting cyber attacks more precisely and as early as possible. Data are highly critical when comparing and evaluating new methods and processes but we have a severe shortage of data sets (linked to proprietary data or to security concerns from the industrialists). We plan to extend our platform so that we can collect data messages, commands and other related outputs through probes. These data sets could then be indexed with the scenario and constitute a rich data reference.

In the near future, we plan to extend this early prototype and to continue collecting data and network messages from a real and operational vessel in various configurations and contexts. They will be used to tune and modify, if needed, our current models.

REFERENCES

[1] Stouffer, Pillitteri, Lightman, Abrams, Hahn, Guide to industrial control systems (ICS) security, in NIST special publication, vol=800, num=82

[2] Industrial Control Systems Assessment Summary Report, url http://www.ics-shipping.org/shipping-facts/shipping-facts

[3] 2015 IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28-30, 2015

[4] Johannes Klick and al, Internet-facing PLCs as a network backdoor, IEEE Conference on Communications and Network Security, CNS 2015, Florence, pp:524–532