Information fusion for port security decision support

Robert Forsgren, Andreas Horndahl,,
Pontus Svenson,, Edward Tjörnhammar
Swedish Defence Research Agency (FOI)
SE-164 90 Stockholm, Sweden
Contact author email: {ponsve}@foi.se

Ports are examples of complicated infrastructure that today face a wide variety of threats. In order to ensure the security of our ports, many different kinds of sensors are needed. Port security systems must also include appropriate information fusion and information exchange systems, and advanced decision support systems that helps the human operators to achieve situation awareness, i.e., the understanding of current and near-future events and their impacts. Having access to such systems will enable early detection of incidents, thus increasing the time available for proactive interventions to prevent the discovered threats.

Information Fusion combines data from multiple sources with different characteristics and aggregates it to increase the total content of information. One can thus extract information not available from each source individually. One goal of information fusion is that the user should receive a better situation awareness to be able to create their own situation understanding. Another goal is to use the information to support automatic or human decision making.

Information fusion can be either model-based or data-driven. In model-based fusion, data is collected and matched to elements of known models. Data-driven fusion, on the other hand, is similar to data mining in that it tries to automatically construct situation models. The current version of the Impactorium framework mainly supports model-driven analysis, but we are investigating extensions of it to enable data-driven analysis.

In this poster, we describe the Impactorium information fusion platform and its adaptation to critical infrastructure protection, especially port protection. Impactorium is a software tool that allows operators to sort, filter and fuse information from heterogeneous sources, including procedures for automatic and semi-automatic tagging of data from sensors and other information sources. The tool is web-based and uses web services to integrate with different information sources. In Impactorium, threat models, consisting of hypotheses on future events and their associated indicators are used to give decision-makers situation awareness of threats. An indicator is an observable event that to some degree indicates that the threat hypothesis is or is to become true. The combined influence of the indicators can be modelled as a belief network. Given all observed indicators, a prediction of the probabilities of the threat hypotheses can be estimated through Bayesian inference. The joint output of the threat models offers an overview of the current threat level. This can be manually monitored or connected to an automatic alerting system. In order to be adaptable to new threats, it is important that users are able to update and adapt the threat models based on new knowledge about the current situation.

A threat model consists of a threat that is broken down hierarchically into sub threats and activities that depends on or are consequences of the threat. The smallest part that a threat can be broken down to is called an indicator. An indicator is a measurable phenomenon demonstrating, or indicating that a threat is being realized. Indicators are used to simplify the understanding of a complex reality and to predict the development of different situations. There are different types of indicators; structural indicators affect the conditions for collective violence to brake out. They are linked to context, geography, economics, politics etc. where the collective violence occurs, but also include factors such as weather, time of year, celebrations etc. Event restricted indicators are divided into two classes; accelerators (events boosting a process, e.g. absent wages) and triggers (events triggering violence and conflicts, e.g. murder of a president).

Impactorium combines a server architecture with an intuitive user interface that enables you to search, link, fusion and share knowledge and information gained on the battlefield as well as information gained from other sources. The framework is built on existing open source techniques and it is possible to integrate with existing information systems.

Impactorium can be used to monitor several events simultaneously. This is done by using an impact matrix. The impact matrix is a tool that has been used in business and for risk analysis where it is used to help the user to remember the probabilities and impacts of various events. Nodes from the threat models are added to the matrix according their estimated a priori probability with which it will occur and the estimated impact that the event would have if it happened. The probability that a node is satisfied is calculated dynamically and displayed graphically in the matrix. Visualization is an important part of the processing and analyzing information and threats. In Impactorium, threats that needs to be monitored can be visualized in an impact matrix consisting of four quadrants . The threats are placed in different quadrants depending on their a priori probability and their impact on the security.

ACKNOWLEDGEMENT

This work was supported by the FP7 project SUPPORT and by the the FOI research project "Tools for information management and analysis", which is funded by the R&D programme of the Swedish Armed Forces.

978-0-7695-4406-9/11 $26.00 © 2011 IEEE
DOI 10.1109/EISIC.2011.59

IEEE computer society

FOI-S--3802--SE