Situation monitoring and threat reasoning for infrastructure protection

Pontus Svenson
FOI Swedish Defence Research Agency, SE 164 90 Stockholm, Sweden

***Abstract*—We briefly discuss how the Impactorium framework can be used for situation monitoring and how it will in the future be extended to include threat reasoning capabilities..**

I. Introduction

An essential component of any security or crisis management system is support tools, computer-based or manual, to help operators increase their situational awareness. This can be helped by fusing data from sensors and other information sources to enable detection of abnormal or dangerous behaviors. Information fusion combines information from different sources and the result can be used to create decision support systems that help users increase their situational awareness. Situational awareness is to be aware of relevant elements in a region of space-time, their relations and meanings, as well as their near future evolution.

We present the Impactorium information fusion and decision support research platform [1,2] and discuss planned extensions for civil security applications that will be implemented in FP7 projects. Impactorium is a system for fusing information from heterogeneous sources in order to do risk-assessment and threat analysis as well as situation monitoring by filtering and sorting information. A crucial component of a decision support system is the capability to allow users to pose and reason about hypotheses about the near-time evolution of the current situation. Plans for extending Impactorium with such functionality are presented.

The need to monitor situations and reason about threats arises in several different security applications, ranging from back-office intelligence analysis [3] to on-the-spot first response work. In this presentation, the focus is on critical infrastructure protection and supply chain infrastructure protection, but possible applications for cyber defense will also be discussed.

II. Results

Impactorium has three components: a modeling tool where the user constructs a network (Bayesian belief network or more generally semantic network) corresponding to events of interests and their indicators; a structuring and fusion component, where reports are associated with indicators and network nodes; and a visualization component, where probabilities of different events are shown and the user can sort and filter the available reports based on what events they are associated with.

The tool is based on information structuring with the help of *semantic networks*. Reports from heterogeneous sources are tagged with relevant terms selected from a previously defined set. Leaf nodes in the network are associated with lists of reports or dynamic searches of the information sources. Based on the information contained in the reports associated to a node, the node is given an indicator value. For non-leaf nodes, a value is calculated based on the values of the neighboring nodes. Non-leaf nodes can also be associated directly with information searches. Node value updating can be done in several different ways. Originally, only Bayesian belief network updating was used, but later versions of the tool also include max, mean, min functions. It is also possible for the user to override calculations and manually insert a node value.

A threat model for a specific threat is a network that relates the threat or event of interest to other nodes and provides calculation functions for each node. By monitoring the values of threat nodes, it is possible for the user to be alerted to imminent threats.

The list of future events/threats and calculated likelihoods can also be used as input to a threat reasoning system. This component will enable users to define management strategies for each different future chain of events. These pre-defined crisis management strategies will then be combined using the likelihoods of different threats, allowing the user to select the most appropriate management strategy based on the entire ensemble of possible future chains of events. In this way, actions that mitigate as many as possible of the likely threats can be chosen.

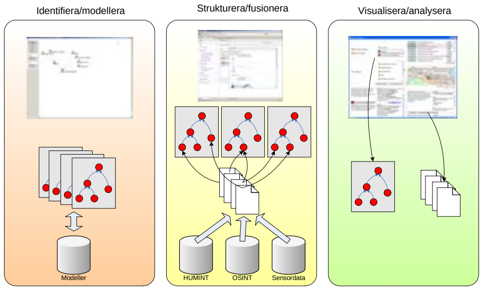

Figure 1: Conceptual overview of the Impactorium tools.

The new crisis management functionalities of Impactorium will be tested in demonstrations for harbor security and supply chain security. They could also prove useful for high-level reasoning about cyber threats.

References

[1] P. Svenson, T. Berg., P. Hörling, M. Malm, C. Mårtenson, "Using the impact matrix for predictive situational awareness", In Proceedings of the 10th International Conference on Information Fusion (FUSION 2007), 2007

[2] R. Forsgren, L. Kaati, C. Mårtenson,P. Svenson, E. Tjörnhammar, "An Overview of the Impactorium Tools 2008", In Proceedings of the Second Skövde Workshop on Information Fusion Topics (SWIFT 2008) (2008).

[3] P. Svenson, R. Forsgren, B. Kylesten, P. Berggren, W. Rong Fah, M. S. Choo, J. K. Yew Hann, "Swedish-Singapore studies of Bayesian Modelling techniques for tactical Intelligence analysis", In Proceedings of the 13th International Conference on Information Fusion (FUSION 2010)