Cyber Fusion Use Case – Template

## General Scenario

We assume that we are responsible for the Cyber Security of a large organization, e.g. in air traffic control (like Eurocontrol).

The system of systems, for which we are responsible, comprises a large amount of workplaces at different sites, which are compositions of computers and software, and the communication systems between the sites.

There are continuously “usual” attacks against elements of our system, e.g. by script kiddies.

We additionally believe that some more sophisticated actors may have interest in attacking our System of Systems, e.g. state actors, large criminal organizations, competitors etc.

## Tasks

We are responsible for the analysis and prediction of the most probable threats as well as for the early detections of dangerous activities of sophisticated attackers (so-called “Advanced persistent threats” APT).

## Holistic Model

The approach is to use a holistic model as described in [1] to assess the probability of different (future) threats and attack vectors and to generate a situational picture concerning the current state of threats and their expected evolution. For the definition of the ACS we restrict the approach to the model of attack, which concentrates on the assessment of prospective attacks. For the demonstration of the approach we defined a user oriented model, which comprised the following elements:



Figure 1: Elements of the Attack Model

The figure shows the structure of the user model of the attack model.

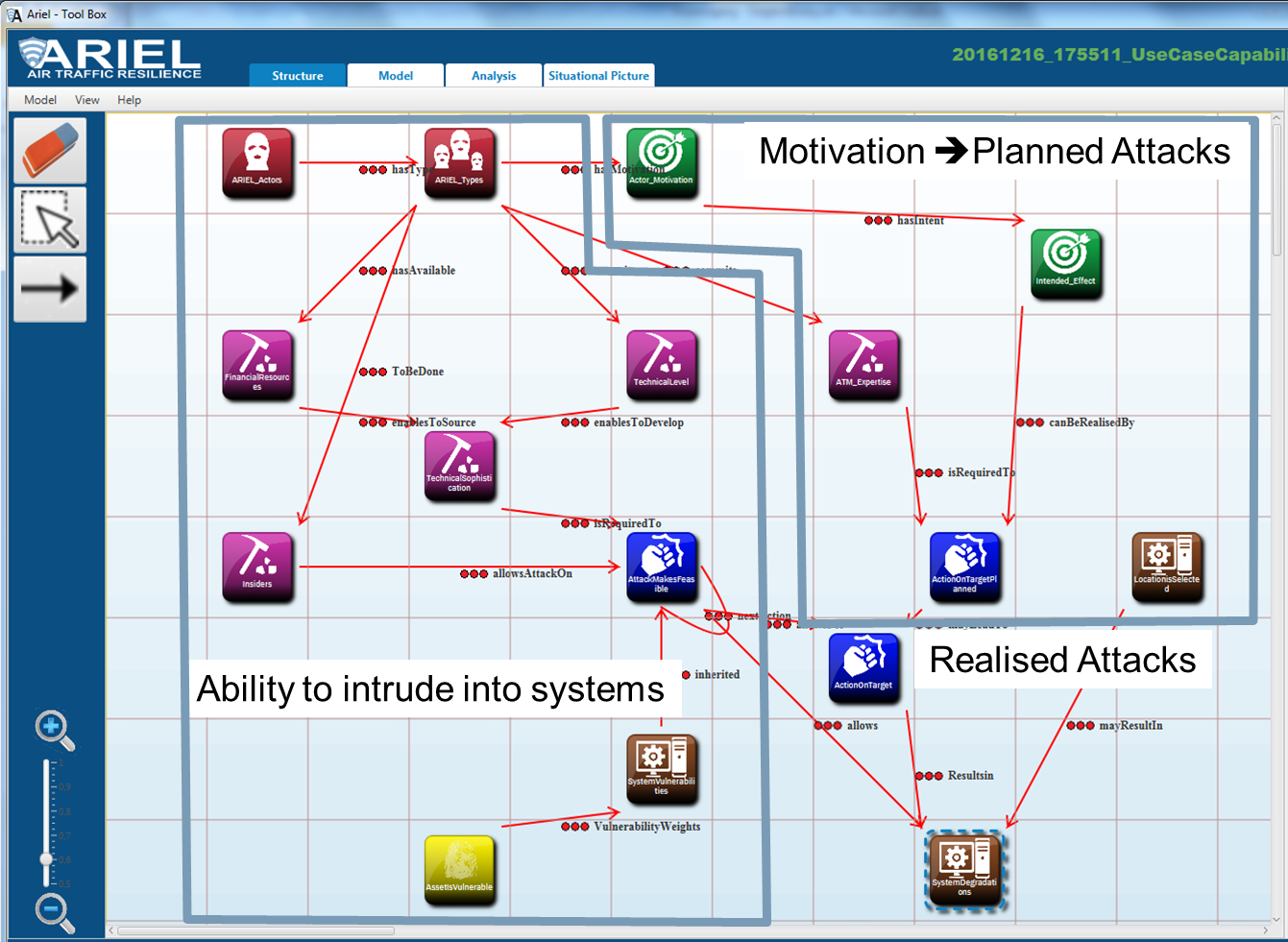


Figure 2: Causality within the User Model

This figure does not contain the indicators, which can be used for the detection of on-going threats. They are

We assumed having three different types of information sources, which can contribute to this task:

* Intelligence Systems comprising Open Source Intelligence to get information e.g. about active actors, dark net activities, current attack tools. These indicators provide information, which can be used to assess the state of active actors, the motivation and intention of these actors and their resources (pink and green part of the attack model).   
  These indicators can also be used to detect pattern of combinations (“IT-derived indicators”), comprising several single attacks, which are correlated with specific intentions.
* Data Exchange between collaborating sites and organizations, which provide information about their current information concerning active threats and actors. These indicators can contribute to the assessment of every element of the model.
* Technical sensors like intrusion detection systems, file watch systems, communication and computer activity surveillance and so on. These indicators contribute to the state of the elements “activity” of the attacker.

The indicators (yellow parts of the model) are associated to the appropriate parts of the user model as exemplarily shown in the next figure.

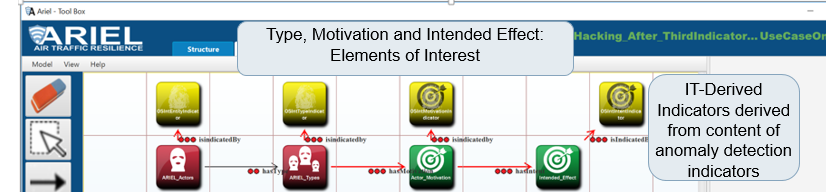


Figure 3: Indicators within the user model

## Generation of the Bayesian Network and CPT Data required for the BN

The user model is not an appropriate Bayesian Network. Most of the nodes comprise states, which might be true parallel (e.g. actions, which might be performed parallel). The dependencies between the nodes of the user model are described by qualitative weights, which can be defined by experienced users; e.g., an expert for cyber attacks can define which actors may have which motivation to perform an attack.

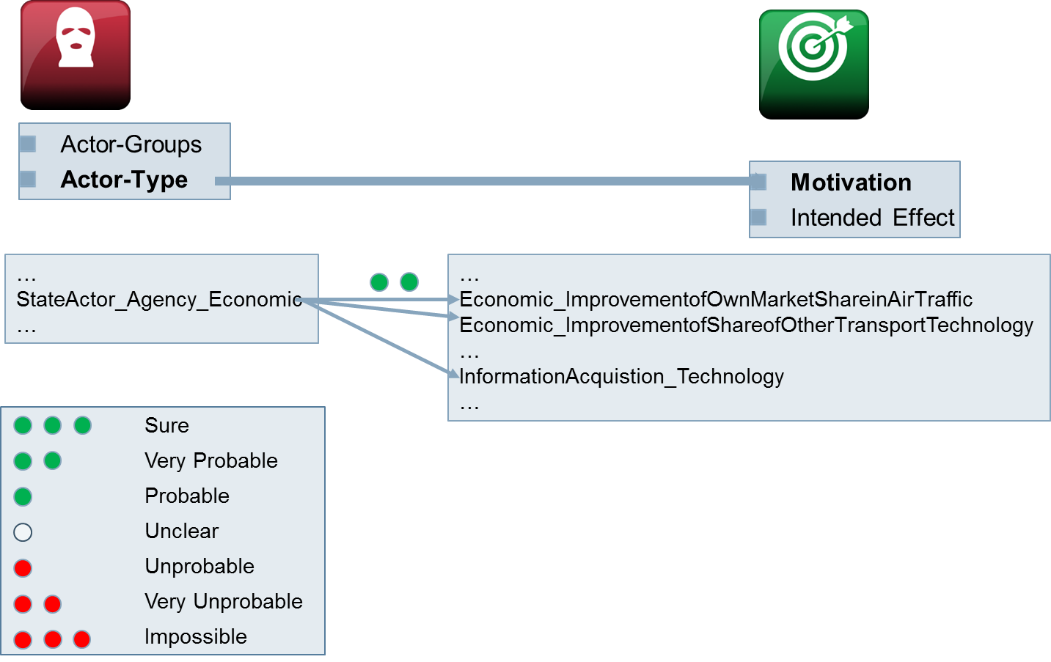


Figure 4: Weighted dependencies between states of the user model

There is the challenge to generate the BN automatically from the user model and from available technical information. There are two parts for the generation of Bayesian Networks, which can be used to the support of the described tasks:

The first part and its solution is already described in [1] and papers referenced there. It describes how to generate a mathematically appropriate Bayesian Network, which is a representation of the holistic attack (user) model. The quality of this part of the model directly depends on the accuracy of the weighted dependencies as defined by the users.  
The BN generated from the user model described above is already relative large, it has 673 nodes, 1456 states and 1222 arcs.

The second part is the determination of the vulnerabilities of the system elements, as they are represented within the “holistic BN”, taking into account the real technical system properties and vulnerabilities of the system components. Within the holistic model, the vulnerability of the system elements is used to derive the chance of success and the probability of attack vectors to access a specific element of the system architecture.

The sub-graph of the network for the system components can be constructed from the system architecture, where every component of the architecture is represented by one node of the graph. The edges of the graph describe which component of the architecture can be accessed from the other ones. The components are described by defining their hardware type, operating system type and application software type.

**First Approach**: The BN and the CPT of the components can be derived from expert assessments (weightings) represented in the user model as for the other parts of the holistic network. This approach was applied for the demonstration of the attack model as described in [1].

**Second approach**: Another more detailed approach to assess the vulnerability of systems is described in [2] (section 2.1). To apply this it is necessary to describe the attack vectors at the level of system processes and their vulnerability values (CVSS AC metric), which can be used to perform one step of an attack vector.

Both methods are candidates for the generation of BN models for large system of systems, if no historical data is available to generate the BN (at least the CPT) from data.

## Small extract of the model to define the ACS (approach 1)

For the definition of a sufficiently small atomic case study, we regard and explain in more detail a small part of the attack model, which comprise the following nodes of the user model:

* Possible attack actions
* Planned attack actions
* Resulting attack actions
* Vulnerability of the systems

The structure of the user model and the resulting BN structure derived by this approach looks e.g. like that:



Figure : User Model of simplified attack vectors in the holistic model

The resulting BN for the systems’ nodes have the following structure:

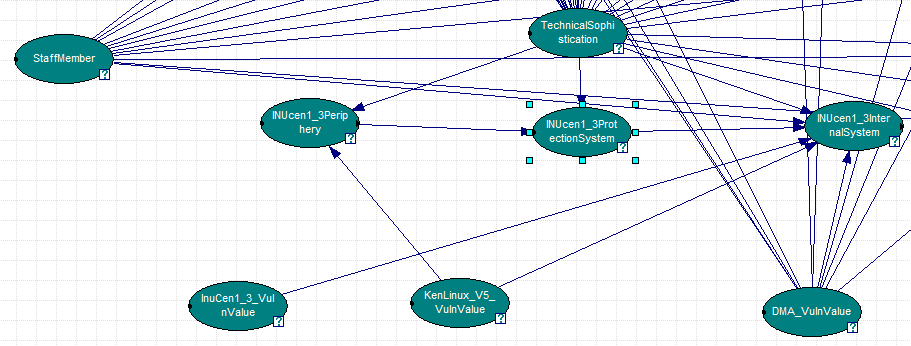


Figure : BN structure of one exemplary internal system node

Note here that DMA\_VulnValue ist the vulnerability of the hardware, KENLinux\_V5\_VulnValue the vulnerability of the operating system and InuCen1\_3\_Vuln\_Value the vulnerability of the application software.

The resulting CPTs look like this:

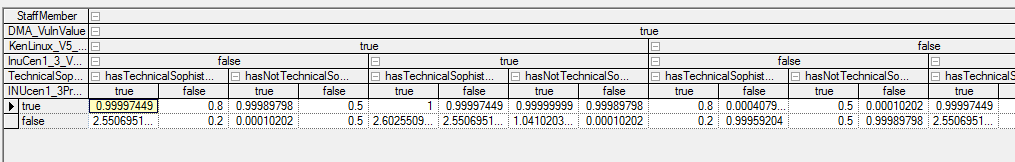


Figure : Part of the CPT of InuCen1\_3\_Internal\_System

## References

1. Tobias Kiesling, Josef Niederl, Jürgen Ziegler: A Model-Based Approach for Aviation Cyber Security Risk Assessment,
2. Using Bayesian Networks for Cyber Security Analysis

Atomic Case Study – Cyber Threats

## Use case

Cyber Fusion Threat Prediction: The URREF ontology shall be used to assess the quality of the knowledge representation (the model data) of the holistic BN as generated by the two approaches. The objective is to generate knowledge representations, which are sufficient to apply the BN for threat analysis and for the generation of situational pictures.

## Type of ACS

TBD

## Solution #1

Basic modelisation + Bayes’ rule

## Question of interest

Assess the quality of knowledge representation

## Evaluation subjects

Approach 1: Experts guess (data) and the method to generate the BN

Approach 2: CVSS data and the method to generate system vulnerabilities at the level of the holistic model.

## Evaluation criteria (from the URREF ontology)

TBD