Outcome WG Situational Awareness

Richard Kemmerer (chair), Roland Bueschkes (vice chair), Ali Fessi (note taker), Hartmut Koenig, Peter Herrmann, Stephen Wolthusen, Marko Jahnke, Hervé Debar, Ralph Holz, Tanja Zseby, Dirk Haage

Definition

Situation awareness (SA) has been defined as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988, 1995b, 2000).

In terms of computer network security and defence, situation awareness refers to the operational picture that consolidates all available information that is actually needed for identifying attacks and for selecting and applying appropriate countermeasures (sometimes referred to as ‘course of action’). The term situation awareness refers not only to making human beings ‘situation-aware’ (e.g. in order to support decisions), but also systems and their implementations.

It has been agreed that the consolidation of the information needs to be performed in an appropriate model that is comprised of resources (or assets), actors, and their inter-dependencies. This model needs to be aligned to the actual mission or high-level objectives of running the computer network and to support different layers of granularity (e.g. from the business process layer over network operation centers’ point-of-view down to low-layer configuration information).

The longer-term (or in some ways ‘static’) information that is to be projected in that model may include

- business processes,
- service level agreements,
- network architecture,
- security architecture,
- network access paths,
- network topology and configurations,
- system configurations, and
- actual vulnerabilities.

The short-term information that contributes to a current picture of the actual situation in the network includes

- system logs,
- network logs,
- performance measurements,
- internal alerts, and
- external alerts (from 3rd parties, early warning systems etc.).

Dagstuhl Seminar Proceedings 08102
Perspectives Workshop: Network Attack Detection and Defense
http://drops.dagstuhl.de/opus/volltexte/2008/1494

 Richard Kemmerer (chair), Roland Bueschkes (vice chair), Ali Fessi (note taker), Hartmut Koenig, Peter Herrmann, Stephen Wolthusen, Marko Jahnke, Hervé Debar, Ralph Holz, Tanja Zseby, Dirk Haage

Challenges

It is a common understanding that the information consolidating model is one of the biggest challenges in research and deployment. There are several unsolved questions on how to model assets, actors, and their dependencies, honouring the network's objectives on different abstraction levels.

Obviously, even more challenges arise as soon as the necessary information for creating and updating the situation model is

- not available (e.g., due to missing ability or willingness to share), or
- incorrect (e.g., due to malfunctions, misconfiguration, or forgery).

Non-available or incorrect information may not only lead to an incomplete operational picture, but also to contradictions, which need to be resolved. In general, forging information for the model enlarges the attack surface. Thus, the process of consolidating information and resolving conflicts needs to have a minimum degree of robustness.

Since the definition of SA also includes a projection of the state of the model components to the near-term future (e.g. in order to suggest courses of actions or to provide decision support), there have been many challenges identified concerning how to formulate hypotheses or predictions about detected phenomena and their update (support, rejection) in an iterative process. It was commonly understood that including potential adversaries will introduce multiple magnitudes of complexity to the SA model.

State-of-the-Art

From the IT security community's point-of-view, there have been many different substantial contributions to obtaining common operational pictures of computer networks. Examples include

- vulnerability management,
- intrusion detection,
- security information & event management, and
- intrusion response modelling and selection metrics.

But there has been many related work identified also in other areas of interest and other research communities:

- system & network management,
- IT service management,
- multi-sensor data fusion,
- trust modelling,
- belief modelling and propagation,
- modelling of military strategies and business processes,

- game theory.

The current state-of-the art in these areas needs to be further evaluated in order to estimate synergy benefits that can be expected.

Future Directions

As future directions in that area, the following non-exhaustive list has been identified

- system modelling,
- event correlation and fusion,
- decision support based on uncertain information,
- attacker modelling, and
- root cause analysis.

Finally, if it becomes feasible to obtain a comprehensive operational picture and reasonably verified hypotheses about adversaries and their intentions, several new challenges are expected to arise concerning how to actually implement situation awareness in tools and systems (e.g., situation-aware intrusion detection and prevention systems).