WG Early Warning Systems

Joachim Biskup, Bernhard Hämmerli, Michael Meier (chair), Sebastian Schmerl, Jens Tölle, Michael Vogel

Definitions

Early Warning Systems aim at detecting unclassified but potentially harmful system behavior based on preliminary indications and are complementary to Intrusion Detection Systems. Both kinds of systems try to detect, identify and react before possible damage occurs and contribute to an integrated and aggregated situation report (big picture).

A particular emphasis of Early Warning Systems is to establish hypotheses and predictions as well as to generate advises in still not completely understood situations. Thus the term early has two meanings, a) to start early in time aiming to minimize damage, and b) to process uncertain and incomplete information.

Challenges

We see an Early Warning System consisting of the following process chain:

1. observation of system behavior,
2. pre-classification in order to concentrate on relevant observations,
3. learning a suitable classification framework,
4. applying the learned classification framework on actual observations and evaluation of current system behavior, and
5. reaction.

This process chain is meant as a continuously working pipeline with feedback to adjust preceding steps.

In order to implement this process a number of challenges have to be addressed. An Early Warning System has to deal with yet unclassified not well-understood but potentially harmful system behavior. Further, a set of countermeasures must be defined which have to be appropriately customized and initiated to a detected and prevent a threat. Since effective Early Warning can only be realized by a cooperative approach, the different interests of all involved parties have to be considered. Moreover, non-technical challenges include the establishment of trust relations among parties participating in the Early Warning System as well as compliance with legislation. How to motivate parties to contribute to an Early Warning System and what are suitable business models to operate and maintain such a system are additional open questions.

Dagstuhl Seminar Proceedings 08102
Perspectives Workshop: Network Attack Detection and Defense
http://drops.dagstuhl.de/opus/volltexte/2008/1493

Assessment of the State of the Art

For each step of the process, first proposals are known to the community. But a composition of these steps into an integrated process has not yet been studied and needs future research.

Recommendations/Conclusions

Our recommendation is to bring together the communities of network measurement, machine learning, intrusion detection and information engineering and integration to address the challenges of Early Warning Systems.