Research in Intrusion Detection
- abstract -

Emilie Lundin
Department of Computer Engineering
Chalmers University of Technology
412 96 Göteborg, Sweden
Tel: +46 31 772 10 00
Fax: +46 31 772 36 63
emilie@ce.chalmers.se

This presentation gives a survey of research done in the field of intrusion detection. The objective of this work is to make it possible to identify the white spots on the research map and to put my own research in a context.

The intrusion detection area consists of a number of research domains. Knowledge from each of these domains must be considered when constructing a functional intrusion detection system. The domains are presented in figure 1.

![Diagram of Intrusion Detection](attachment:diagram.png)

Figure 1: Research areas

Some issues have received a great deal of attention, while others have been almost forgotten. For example, many different detection methods have been used in research prototypes. Everything, from simple pattern matching and statistical methods, to expert systems and genetic programming has been tried.
On the contrary, not many papers have focused on data collection, i.e. what data to use as input to the detection system or how to collect it. Another issue that has been neglected until recently is testing and evaluation of detection systems. It is no good having an efficient detection method, if the input data used are insufficient or faulty. Also, to find out how efficient the detection method really is, we need an evaluation method.

Study of intrusions, intruders and vulnerabilities forms the foundation of this research area. Here, the origin of the problem is studied. Response deals with the issue of how to respond to alarms. For example, it is possible to use active or passive response. Human interaction is also an important issue within this domain. Different detection methods or data collection methods may have different performance characteristics depending on the system they are used in. Therefore, it is important to study different IDS (Intrusion Detection System) environments and architectures. Improving efficiency is always important to make a system useful in practice. Social aspects is an area that is often forgotten in this context, but there are issues like privacy and collection of forensics, that are important for the future use of intrusion detection systems.

The knowledge of what research has been done and what issues remain to be solved, is of help when evaluating prototypes and research projects within the intrusion detection area.