

**2nd International Conference on Hybrid Intelligent Systems (HIS'02)  
Special Session on Hybrid Intelligent Systems for Intrusion Detection**

**Session Chairs**

Fabio Abbattista, Pasquale Lops, Giovanni Semeraro  
[fabio@di.uniba.it](mailto:fabio@di.uniba.it), [lops@di.uniba.it](mailto:lops@di.uniba.it), [semeraro@di.uniba.it](mailto:semeraro@di.uniba.it)

**Aim and Topics**

Security of network systems is becoming increasingly important as more and more sensitive information is being stored and manipulated online. Intrusion Detection Systems (IDSs) have thus become a critical technology to help protect our systems.

Broadly speaking, there are two classes of intrusion detection techniques available: recognition of intrusion patterns (signature based approaches) and anomaly detection.

Most IDSs are based on handcrafted signatures that are developed by manual encoding of expert knowledge. These systems match activity on the system being monitored to known signatures of attacks. The major problem with this approach is that the system cannot generalize to detect new attacks.

On the contrary, anomaly detection systems, try to determine whether deviations from an established normal behaviour profile can be identified as intrusions. Profiles can be updated periodically (aged) so that shifts of normal behaviour are accounted for. The key advantages of anomaly detection systems are that they can detect unknown intrusions since they require no a priori knowledge. However, defining and maintaining "normal" profiles is a nontrivial and error prone task.

Users' behaviour has been widely investigated in the user modelling area, where the focus is mostly placed on the acquisition of information about typical action sequences performed by people. In this case the final goal is assisting users during the execution of their activities. Learning techniques are exploited to automatically synthesize action sequences from log files; then, the individual user's behaviour is matched against such sequences to understand what s/he is doing and possibly help her/him at the execution of the task. The interesting aspect of such research is that it aims at constructing usage models, related to the possible classes of system users.

A system is typically used by heterogeneous users, who can be more or less expert, or may cover different roles, determining different sets of activities on the system (e.g., compare the tasks performed by a system administrator with those of a end-user). The final goal is therefore to automatically synthesize behaviour patterns reflecting the behaviour of one or more classes of users.

Topics of interest for the session include, but are not restricted to, the application of Intelligent Systems technologies to:

- Intelligent systems for dynamical user behaviour modelling
- Intelligent systems for log data analysis and filtering
- Intelligent systems for knowledge discovery from log data
- Intelligent systems for anomaly detection in network systems
- Intelligent systems for network systems defence

**Important dates**

July, 25th 2002: Full Paper Submission  
August, 7th 2002: Notification of acceptance  
August, 25th 2002: Camera Ready Submission

**Submission Details**

Please submit a full paper of 8 to 10 pages (Letter or A4 paper) for oral presentation. The proceedings of the Conference will be published by IOS Press, Netherlands. A selected number of papers will also be considered for a special issue of the Elsevier Science Journal "Applied Soft Computing" and for a special issue of the IOS Press Journal-Intelligent Data Analysis. Please follow the author's guidelines given by IOS Press for more information on submission. Author's guidelines can be downloaded from the conference web page (<http://his02.hybridsystem.com/>).

Submissions should be sent, by e-mail, to the following address:

Fabio Abbattista  
[fabio@di.uniba.it](mailto:fabio@di.uniba.it)