

“Interest”ing Intrusion Detection

Rajeev Gopalakrishna

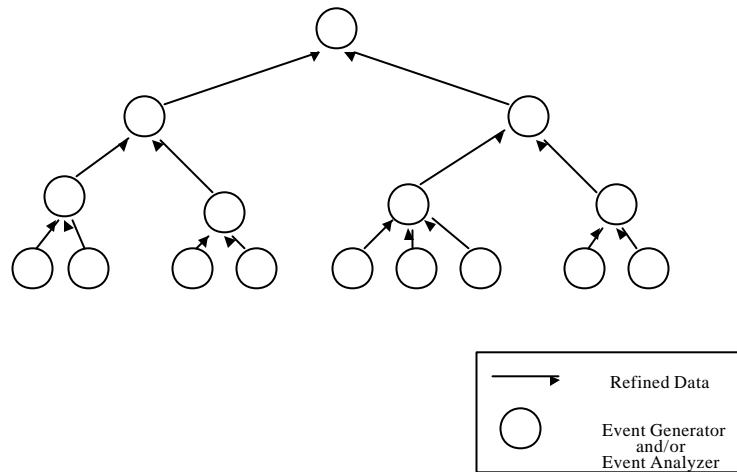
And

Gene Spafford

Motivation

- Concept of agents to perform intrusion detection
- Event-based communication model
- Concept of interest propagation

Generic Hierarchical Intrusion Detection Systems



Drawbacks

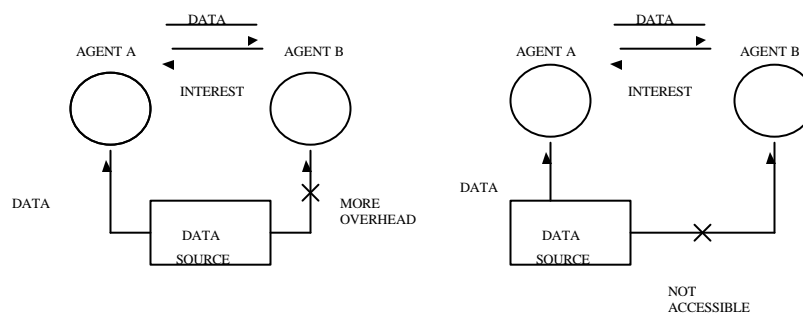
- Analysis hierarchy
- Data refinement
- Bulky modules at all levels of hierarchy
- Passive interaction

Our Approach

- Agents
- No analysis hierarchy
- Intelligent cooperation using the concept of interests
- Interest propagation
- Active communication
- Lightweight modules at all levels of hierarchy

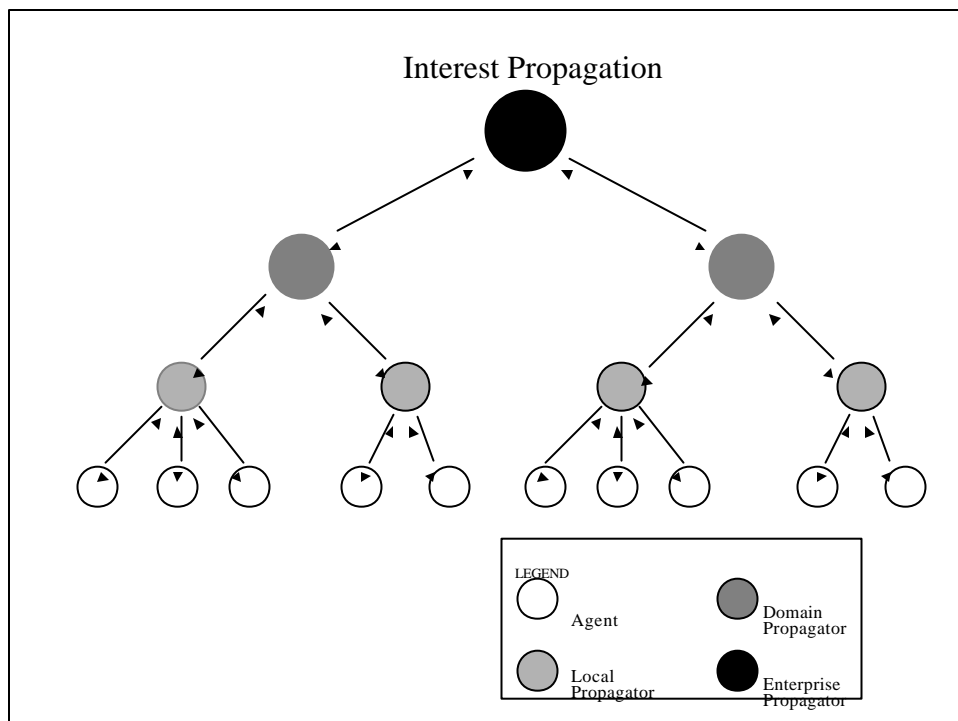
Interest

“a specification of data that an agent is interested in, but is not available to the agent because of the locality of data collection or because the agent was not primarily intended to observe those data”

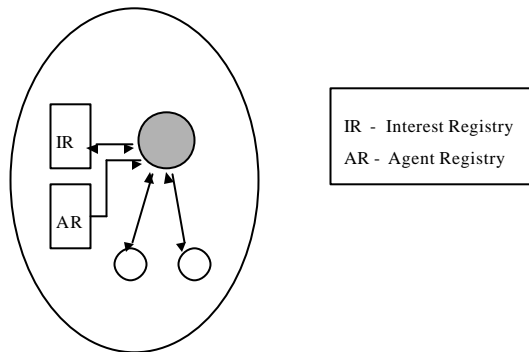


Types of Interests

- Directed or Propagated Interests
- Local, Domain or Enterprise Level Interests
- Permanent or Temporal Interests



Host



Future Work

- Implementation of the framework (Perl)
- Explore alternatives for implementing the interest mechanism