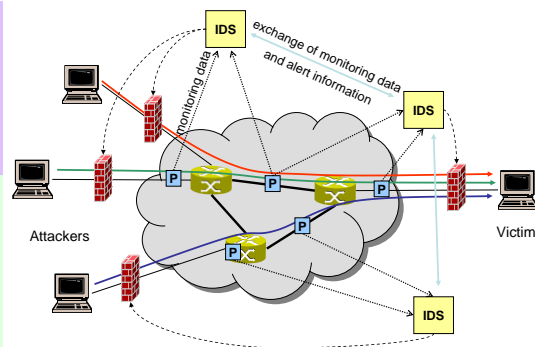
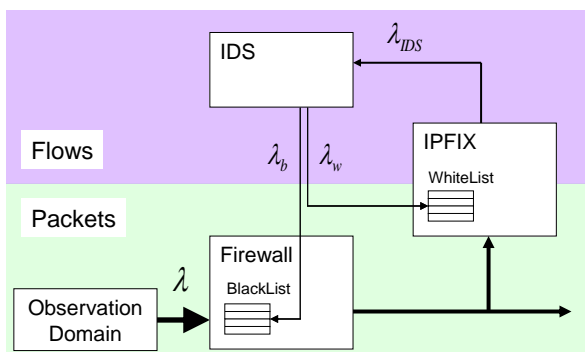
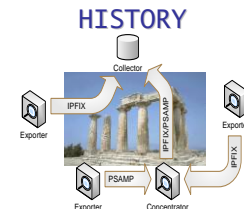


Master's Thesis

Self-Organizing Security Environments – Monitoring and IDS

Description:

Automated self-organizing security environments are becoming a major requirement for future network architectures because the number and effectiveness of threats such as security attacks, worms and viruses are increasing. In the early beginnings, simple firewall solutions have been used to prevent attacks. Nowadays, more sophisticated and – most importantly – distributed solutions are demanded. Modern security solutions apply monitoring techniques able to cope with high speed computer networks, different kinds of detection algorithms such as pattern matching or anomaly detection solutions, and complex distributed firewall and proxy installations. Recently, we developed a simple model (shown below) to analyze the properties of monitoring/detection/reaction scenarios with respect to load adaptation according to the current state of the network.



Problem definition:

In this master's thesis, our simple model needs to be extended to cover the complex interactions between the many entities in a network security environment. Thus, a major part of this thesis is to study distributed security solutions and to identify the relationships, possible bottlenecks and adaptable parameters. In a second step, a model needs to be developed (either analytically or a simulation model), that allows to analyze the load of the systems with respect to the current network traffic and/or attacks.

Requirements:

Basic knowledge about computer networks

Keywords:

Monitoring, Attack detection, Simulation, Self-organization

Contact:

Dr. Falko Dressler

dressler@informatik.uni-erlangen.de – <http://www7.informatik.uni-erlangen.de/~dressler/>