Framework Applications

The semantic framework can be applied to many areas of networked data analysis. As for now, the framework is restricted to offline (non real-time) scenarios along with a few other #limitations limitations]. We discuss the following examples, some of which (marked with '*') are also discussed in our NSDI'11 paper.

Modeling hypotheses*

This example discusses a scenario where DoS detection heuristics from a publication are formulated as a model and are validated over packet traces.

Modeling experiment behavior*

This example discusses a scenario where an entire experiment behavior - in the case the DNS Kaminsky cache poisoning experiment - is formulated as a model and applied over packet traces collected from a complete experiment run.

Modeling a security threat* (*page under construction*)

This is an example of modeling a simple worm spread over IDS logs.

Modeling dynamic change* (*page under construction*)

This example models changes in traffic rate due to attack.