Extracting and Visualizing Security Properties using Self-Propelled Instrumentation

Overview
- Inject initial instrumentation into the system at runtime
- The instrumentation inserts more instrumentation ahead of the flow of control

Components
- Injector: forces an application progress to load a shared library
- Agent: a shared library
  - Payload function: contains user-specified code
  - Instrumentation engine

Instrumentation Propagation
- Instrumentation propagates within a process by following control flow
- Instrumentation propagates across thread, process, and host boundaries by following communication flow

Application: Visualization for Security Analysis
- Goal: automate diagram construction for security assessment
  - Data collection
    - Use self-propelled instrumentation
    - Detect system events and security properties
  - Diagram construction from trace data