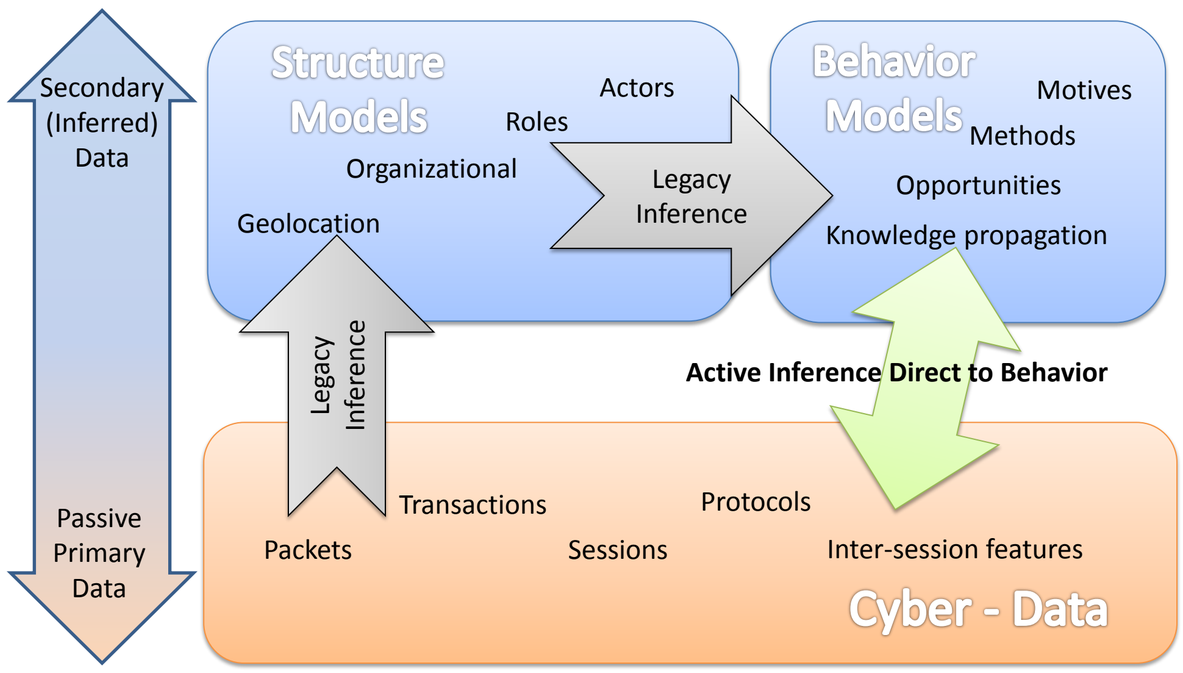
SAILBOAT

ManTech International Corporation

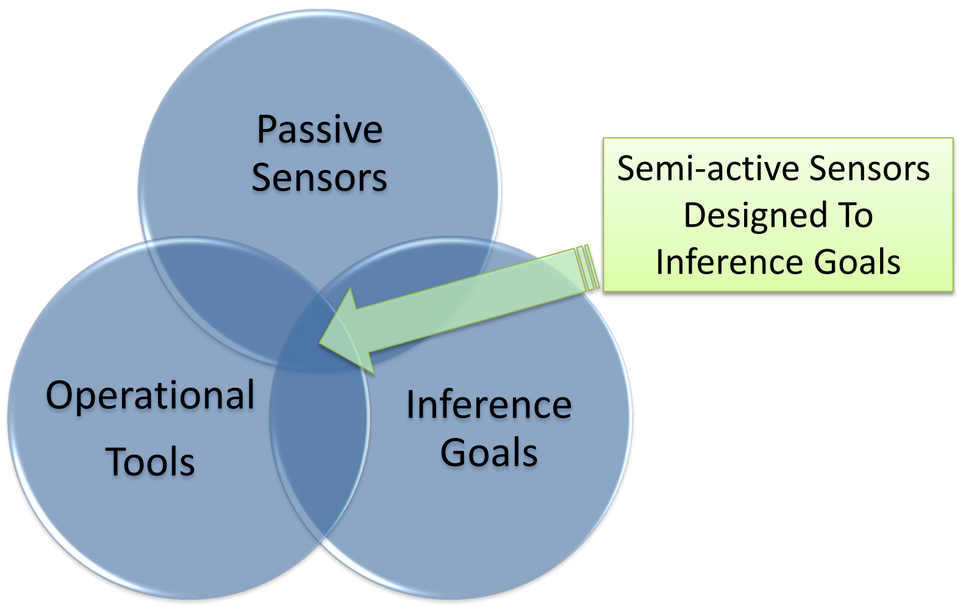
SAILBOAT Overview

Opportunistic, passive cyber data generally drives inferencing into models for Actors, Roles, Locations, Organizations and thence to predictive behavior models such as Motives, Methods, and Opportunities, but may result in sparse, low confidence data. Adding active sensor components specifically to produce behavioral evidence, we infer more directly to the predictive models, and prioritize efforts where resulting inferences are most valuable.

Active Inference to Behavior Model



Semi-Active Inference-Level Behavior-Observing Automated Telemetry



Atypical Semi-Active Sensor Techniques

Knowledge/Belief Injection & Propagation Sensors

Example: Certificate compromise rumor injection, followed by semi-active detection of certificate rejection by candidate actors.

Watering- Hole Techniques

Computer service behavior deviations based on triggering events or identifying client behavior / attributes.

Spear-Flushing

I.E. Reverse spear-fishing: induction of secondary behavior based on targeted content.

Canary Content Placement & Exfiltration Sensors

I.E. decoy content with active or semi-active monitoring of sharing and leak sites.

Example Narrative

Actor A is high-knowledge and motivated, and has similar attributes with actor B, who is known to have opportunity to access a sensitive asset, but there is no correlating primary evidence that A and B are connected. Through canary or watering hole techniques, an Actor A session is presented with evidence of a compromise of a particular root certificate. The semi-active sensor then uses watering-hole techniques to test when and if Actor B has reconfigured to reject certificates signed by the rumored compromised root certificate. Timing and other data (searches, chatter) may clearly indicate actor models A and B may be merged, or indicate direct-knowledge transfer that indicates close knowledge transfer graph adjacency. A merger of A and B further completes the Motive, Method, and Opportunity characteristics of the Actor model, and indicates probable attack on the accessible asset.

Potential Advantages

Increased Yield of Critical Inferences

- Design target of what knowledge is needed rather than what is easily collected

Operational yields with automated effort

- Opportunistic sensors combine with automated operational capabilities.

Reusable components and techniques

- Watering hole infrastructure can be tasked with multiple sensors and goals
- Knowledge propagation sensor pattern can be realized in several technologies.

Risk Mitigation

Risks include the leaking of data state of the model.
Mitigations:

- Probabilistic sensor behavior dithering.
- Hard limits on state-driven sensor action exposures.