CERIAS

Causality-Based Intrusion Analysis

Sundar Jeyaraman, Mike Atallah

Questions

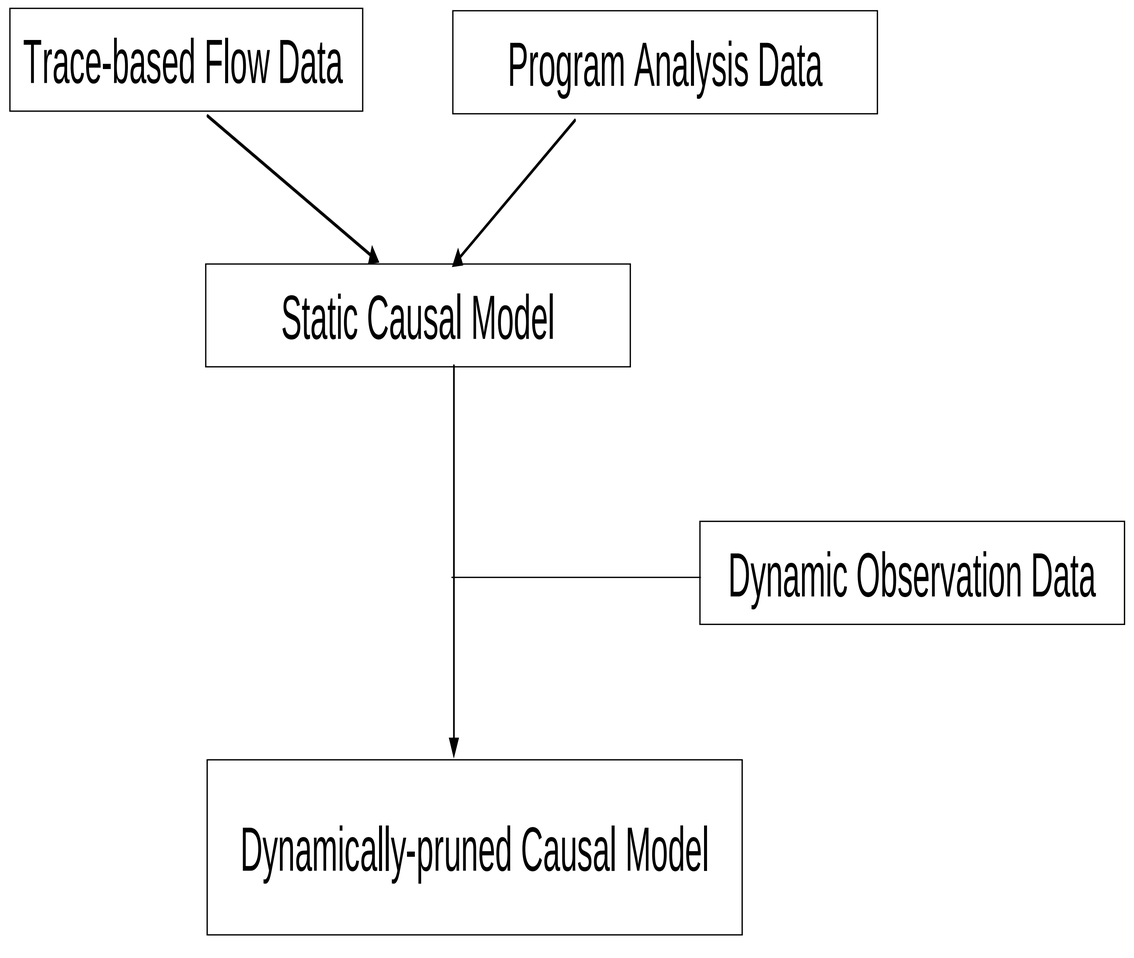
- How did the intruder gain access?
- Who was the intruder?
- What was the damage inflicted?
  - Modified Files
  - Backdoors (Access For Sale)
  - Sensitive Information Transmitted
  - Stepping Stone for other attacks

State of the art – Limitations

- Manual Analysis for the most part
- Cramped by Incomplete IInformation
  - System Logs
  - Disk Image
  - Network Logs

MISSING: Causal Relationships between events

System Architecture



Simple Causality

- Did event ‘A’ influence ‘B’?
- A simple boolean Yes/No solution
- Answered by observing Control/Data flow

Causal Strength

- How much of an influence did ‘A’ have over ‘B’?
- Measure of “Necessity”
- Measure of “Sufficiency”
- Probabilistic answers from controlled experiments and dynamic monitoring