CERIAS

Whodunnit? - An intrusion analysis system

Sundar Jeyaraman, Mike Atallah

BackTracking Intrusions

- How did the attack happen?
  - What was the exploited vulnerability?
  - Was it the only vulnerability that was exploited?
- Who was the attacker?
  - Insider Vs Outsider

Answerable with acceptable accuracy

Forward Tracking Intrusions

- What did the attacker do?
  - What files did the attacker modify?
  - Were any Backdoors left behind?
  - Was any sensitive information transmitted?
  - Was this system used as a stepping stone in another attack?

Timely and precise answer not available

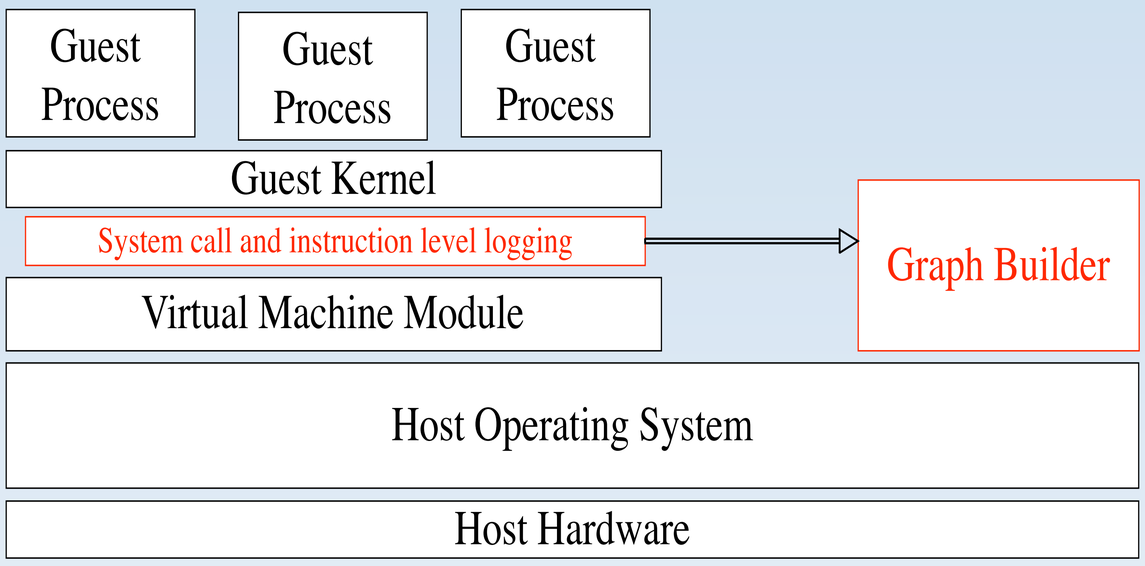
State of the art - Woes

- Manual analysis for the most part
  - Arduous and time consuming
- Effective visualization not available
- No spatio-temporal event correlation
  - False positives
  - False negatives

Whodunnit?

- Key Idea – Capture all the dependencies
- Build a Dependency graph
  - Summary of the system events and the inter-dependence of events
  - Nodes are system objects
  - System calls create dependency edges
  - Anwering queries equivalent to computing dynamic slices
- Enabling technology: Virtual Machine based replay

System Architecture



Whodunnit? - Issues

- Competing goals:
  - Space and Time overhead
  - Precision of the answers
- No “one-size-fits-all”
  - The nature of the queries dictates the parameters

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center