**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*

**System Architecture**

```
    Guest Process          Guest Process          Guest Process
    ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓
    |           |           |           |
    | System call and instruction level logging |
    | Virtual Machine Module                  |
    ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛
    ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓
    |           |           |           |
    | Guest Kernel                         |
    ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛
    ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓
    |           |           |           |
    | Host Operating System                 |
    ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛
    ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓           ┏━━━━━━━━━━┓
    |           |           |           |
    | Host Hardware                          |
    ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛           ┗━━━━━━━━━━┛
```

**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