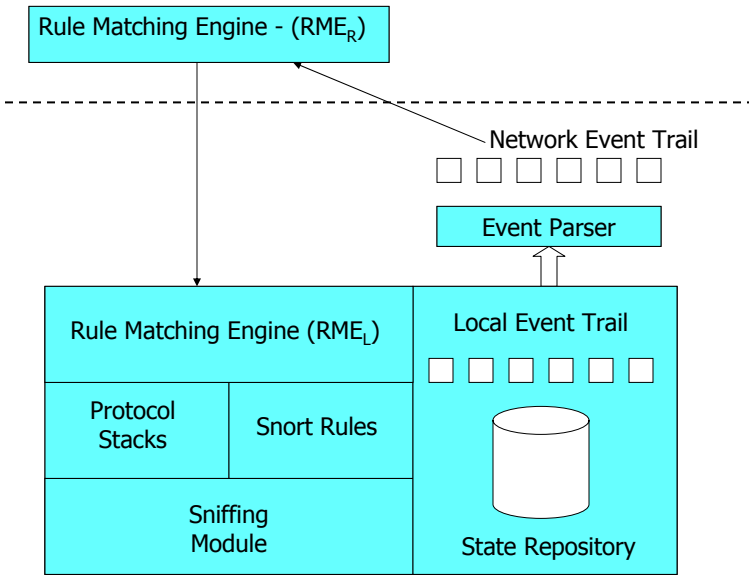
SPACEDIVE: A Distributed Intrusion DetectionSystem for Voice-over-IP Environments

Motivation

- Distributed Intrusion Detection System for VoIP networks - SPACEDIVE
- Why build an IDS just for VoIP?
  - Soft real-time requirements
  - Attack can take place across a session
  - Attack across protocols
- Why distributed detection?
  - Multiple components in a VoIP system
  - One attack may span many components

SPACEDIVE Design Principles

- Integration with Snort
  - Fast pattern matching
  - Widespread use
- Detection at local and remote levels
  - scalability
- Cross-protocol and stateful detection
- Rule language



Low Level Rule Language

- New constructs
  - var – set the value of a state variable
  - event – trigger a local event
  - net_event – trigger a network-level event
  - seqwin (protocol specific - RTP) – specify maximum tolerance for out-of-order packets
  - Connectors: AND/OR/NOT/BEFORE/AFTER

```
alert udp Client_IP any -> Server_IP 5060
(content:"INVITE"; var invite;)

alert udp Server_IP any -> Client_IP any
(content:"sip:OK"; var ok;)

event(ok AFTER invite;) # trigger local event
```


Performance of Rule Matching

- Rule matching overhead
- Defined 4 categories of rules:
  - Type 0: Snort rule matched in Snort
  - Type 1: Snort rule matched in SPACEDIVE
  - Type 2: Use **`var`** construct to set the value of a variable.
  - Type 3: Create local event in the event trail

Performance of Rule-Matching: Results