

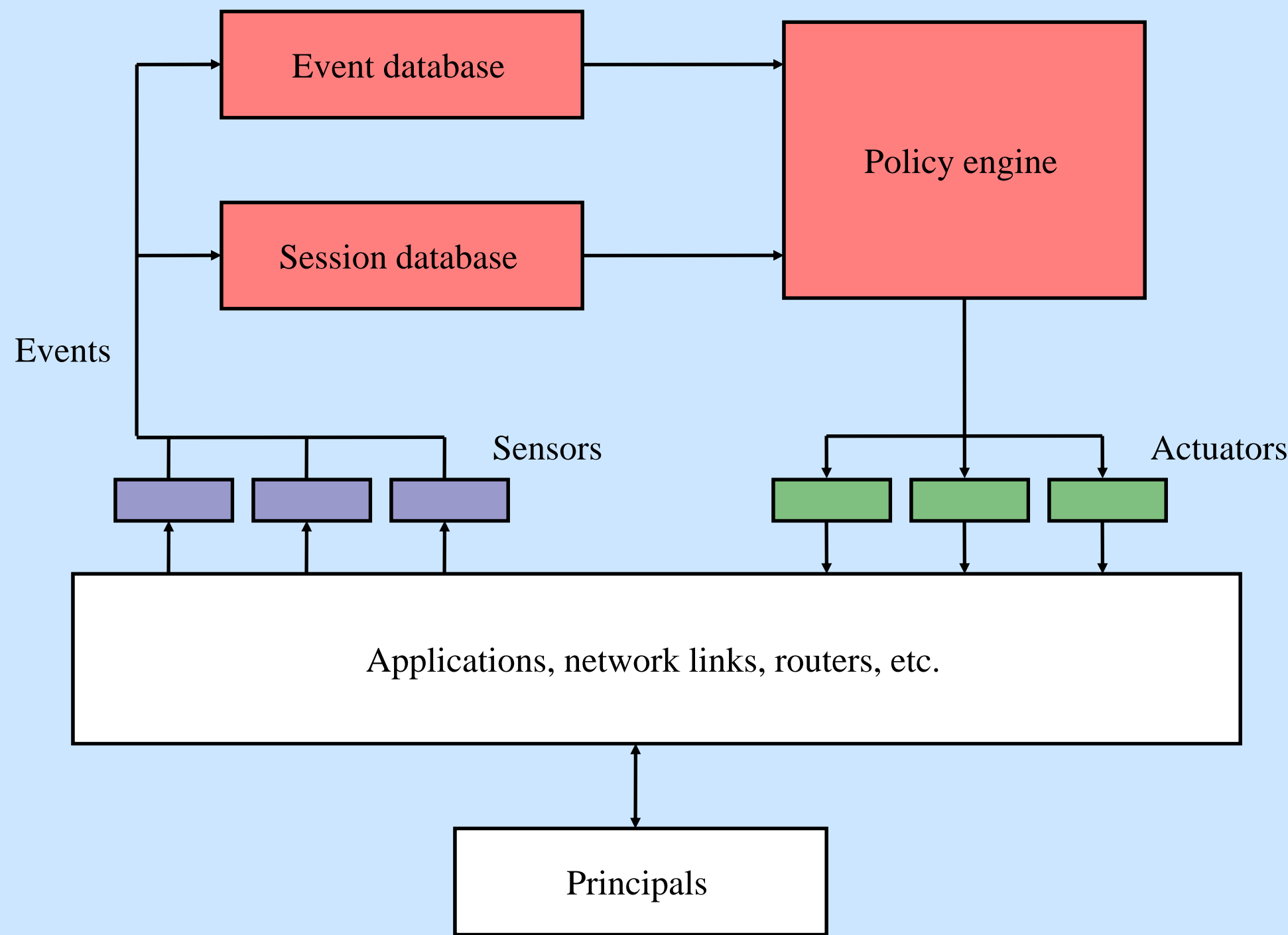
Arachne: Integrated Enterprise Security Management (5-24402)

Matthew Burnside, Angelos D. Keromytis

<http://arachne.cs.columbia.edu>

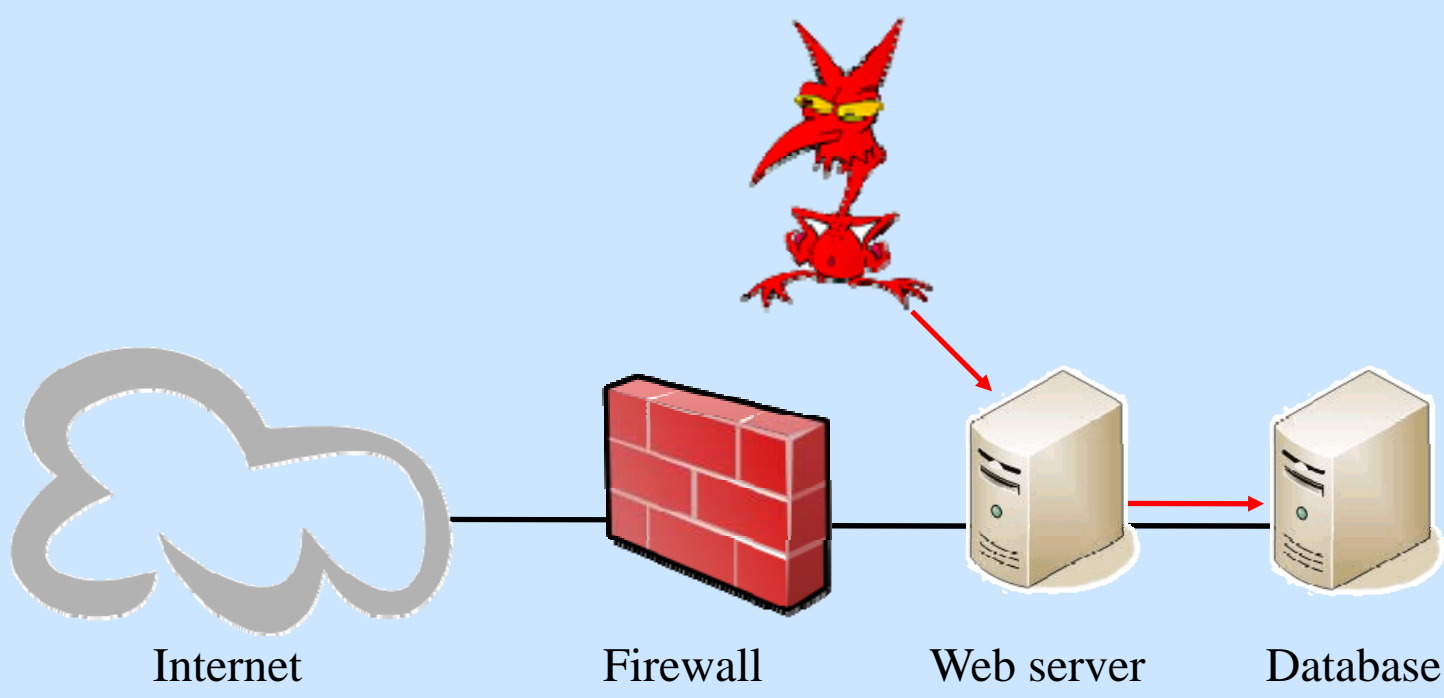


Arachne architecture

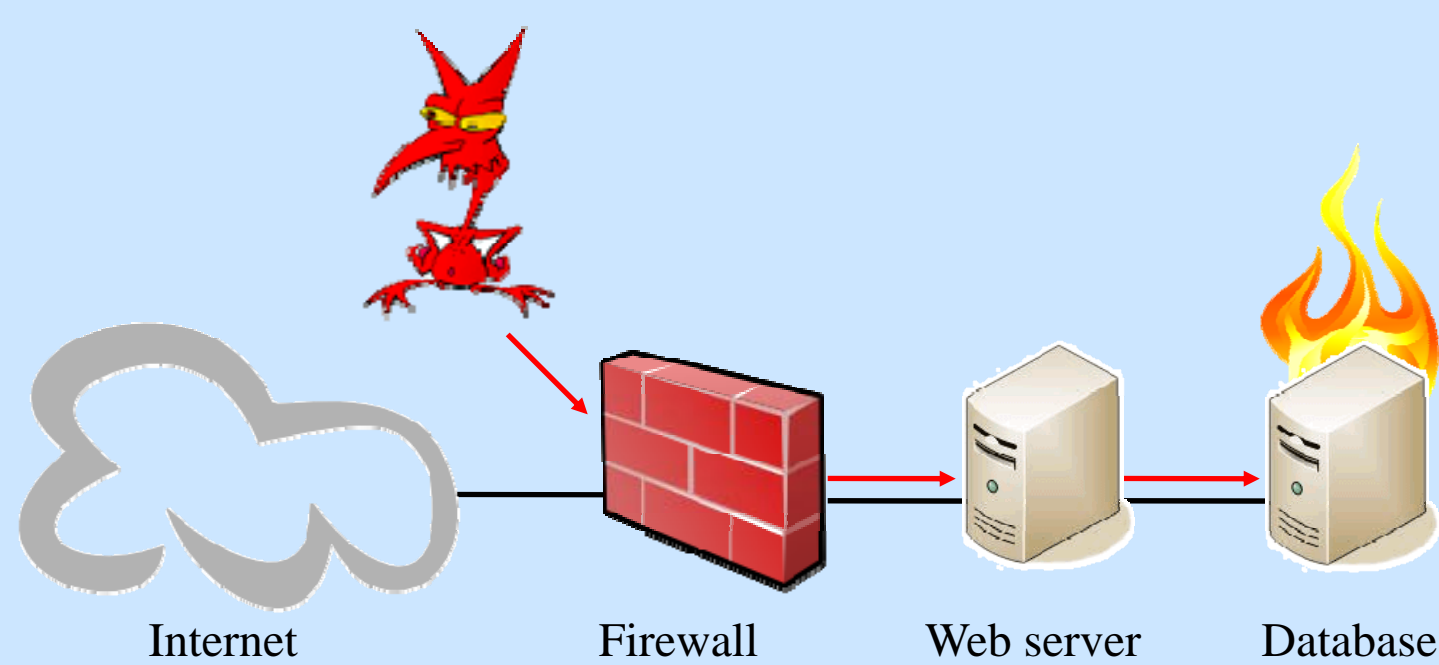


Access control challenges:

- Prone to locally correct but globally incorrect decisions.
- Evaluation is synchronous but adversary's behavior is not.
- Limited available responses.



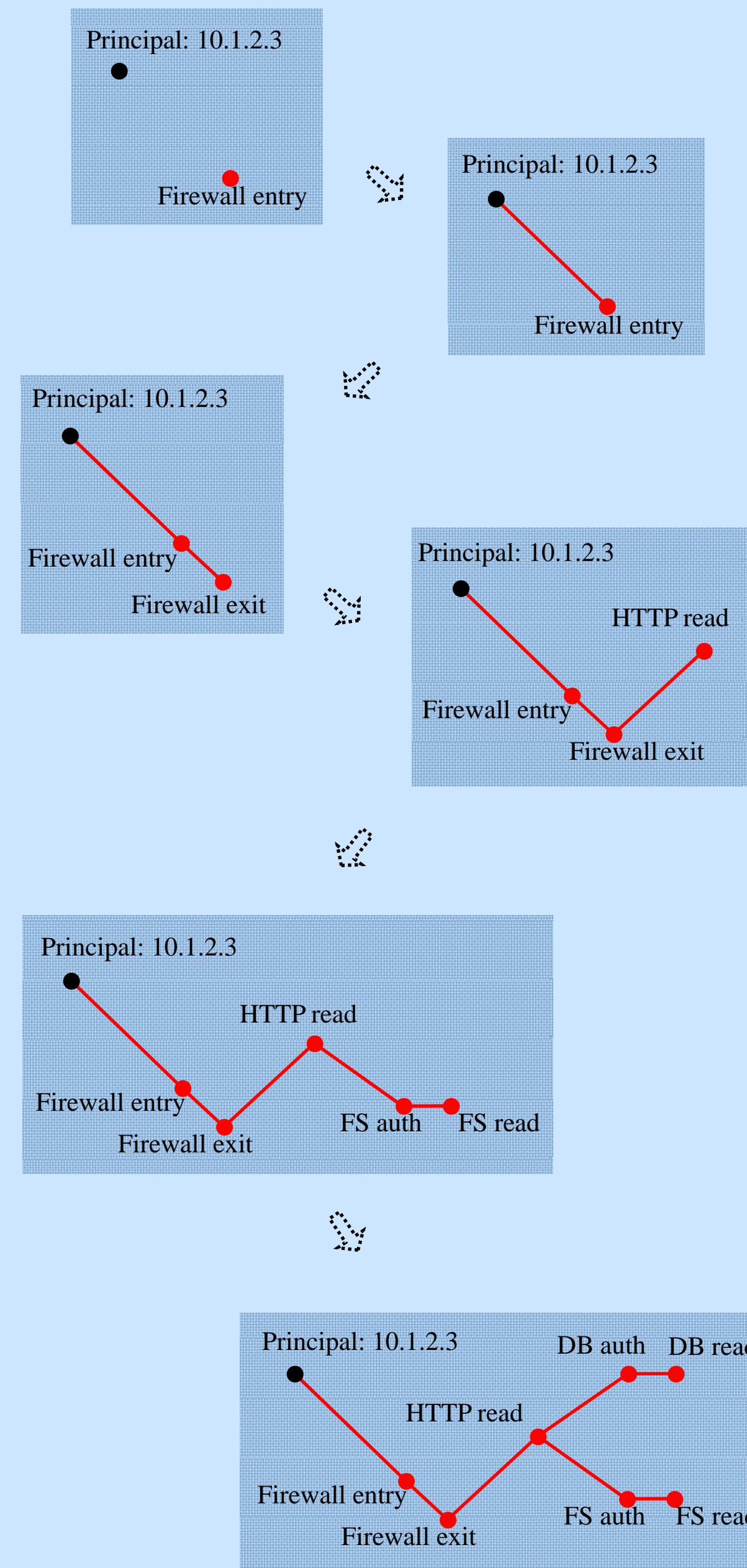
Locally correct, globally incorrect.



Decisions must be revisited asynchronously.

Desirable responses

- Raise log level.
- Redirect to a honeypot.
- Redirect to an instrumented network.
- System revert.



Sensors

- Customized for the specific application or network link being observed.
- A sensor knows which events are important.

Typical case: parse the log files.

Principals

- Different meanings for different parts of the network!
- Network layer: IP address
- Application 1: <username, password>
- Application 2: public/private key pair
- Arachne is principal agnostic.
- Each sensor is customized to recognize the principal-type for its specific application.

Event database

- MySQL
- Archives events at least until they are removed from the session database.

Session database

- A session is a graph where the vertices are events and the edges are causality links between them.
- No general method for determining causality, but we can use sensors to get a close approximation.