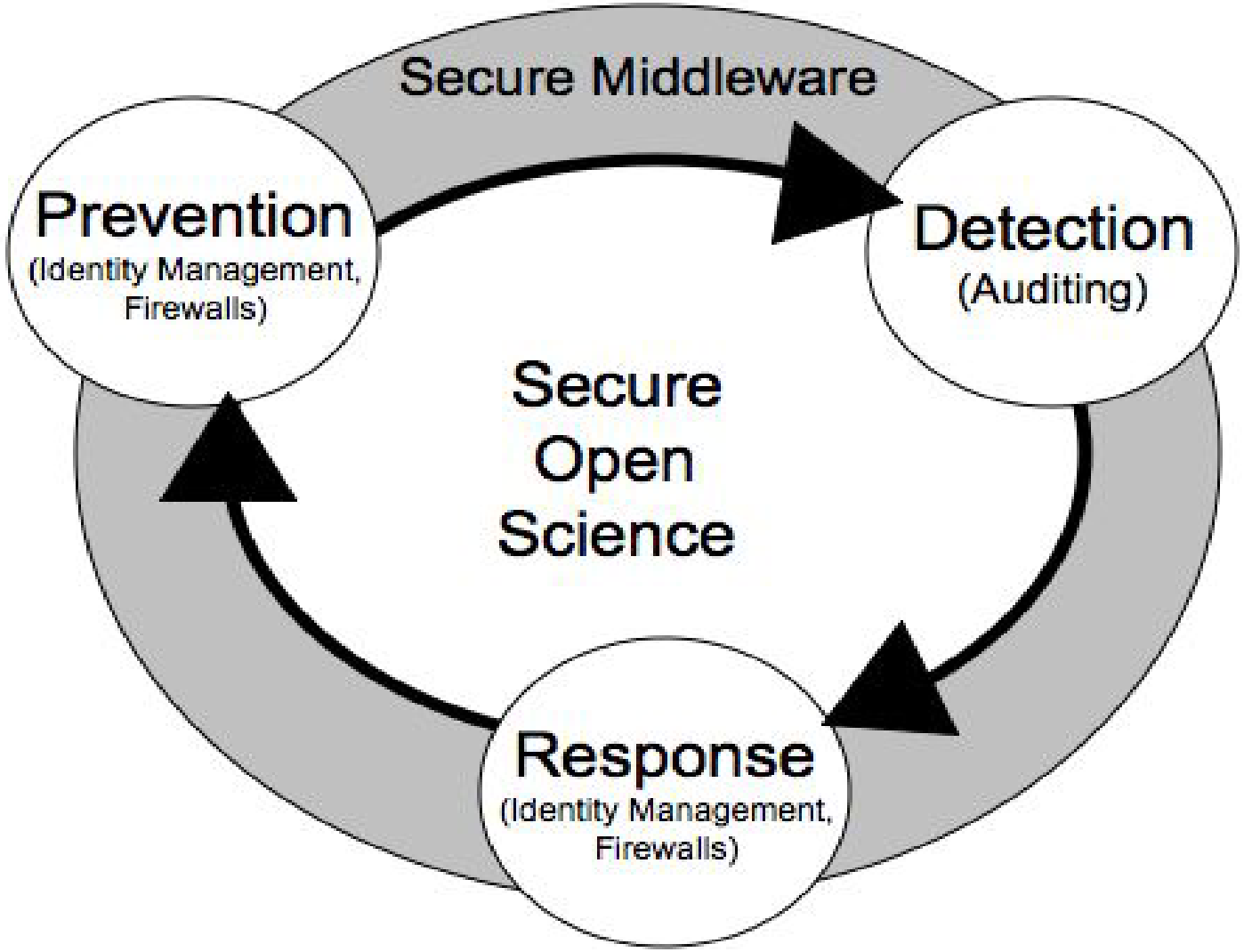
Security for Open Science Project

Lead PI - Deb Agarwal, Lawrence Berkeley National Laboratory
-
Lawrence Berkeley National Laboratory - Brian Tierney, Mary Thompson
Argonne National Laboratory - Frank Siebenlist, Ian Foster
Pacific Northwest National Laboratory - Jeff Mauth, Deb Frincke
University of Illinois, NCSA - Von Welch, Jim Basney
University of Virginia - Marty Humphrey
University of Wisconsin - Miron Livny, Bart Miller
National Energy Research Scientific Computing Center - Howard Walter
Energy Science Network - Michael Helm
University of Delaware – Martin Swany

Management Structure

- Project Lead – Deb Agarwal
- Participating Organizations:
  - LBNL, ANL, PNNL, NCSA, Univ. Wisconsin, Univ. Virginia, ESnet, NERSC, Univ. Delaware
- Currently Planned application Partnerships
  - OSG, Fusion, Astronomy (LANL), ESG, etc
- Currently Planned Facilities Partnerships
  - NERSC, NCSA, ESnet, NLCF, etc

Strategy - Prevent, Detect, and Respond



Interrelated Topic Areas

- Auditing and forensics
  - Services to enable sites, communities, and application scientists to determine precisely *who* did *what, where* and *when*.
- Dynamic ports in firewalls
  - Services to open and close ports dynamically for applications while enforcing site policy.
- Identity management
  - Services to seamlessly manage identity and access control across sites and collaborations, and to allow for rapid response to security incidents.
- Secure middleware
  - Services to proactively find and fix software vulnerabilities and guarantee deployed security software is current and correctly configured.

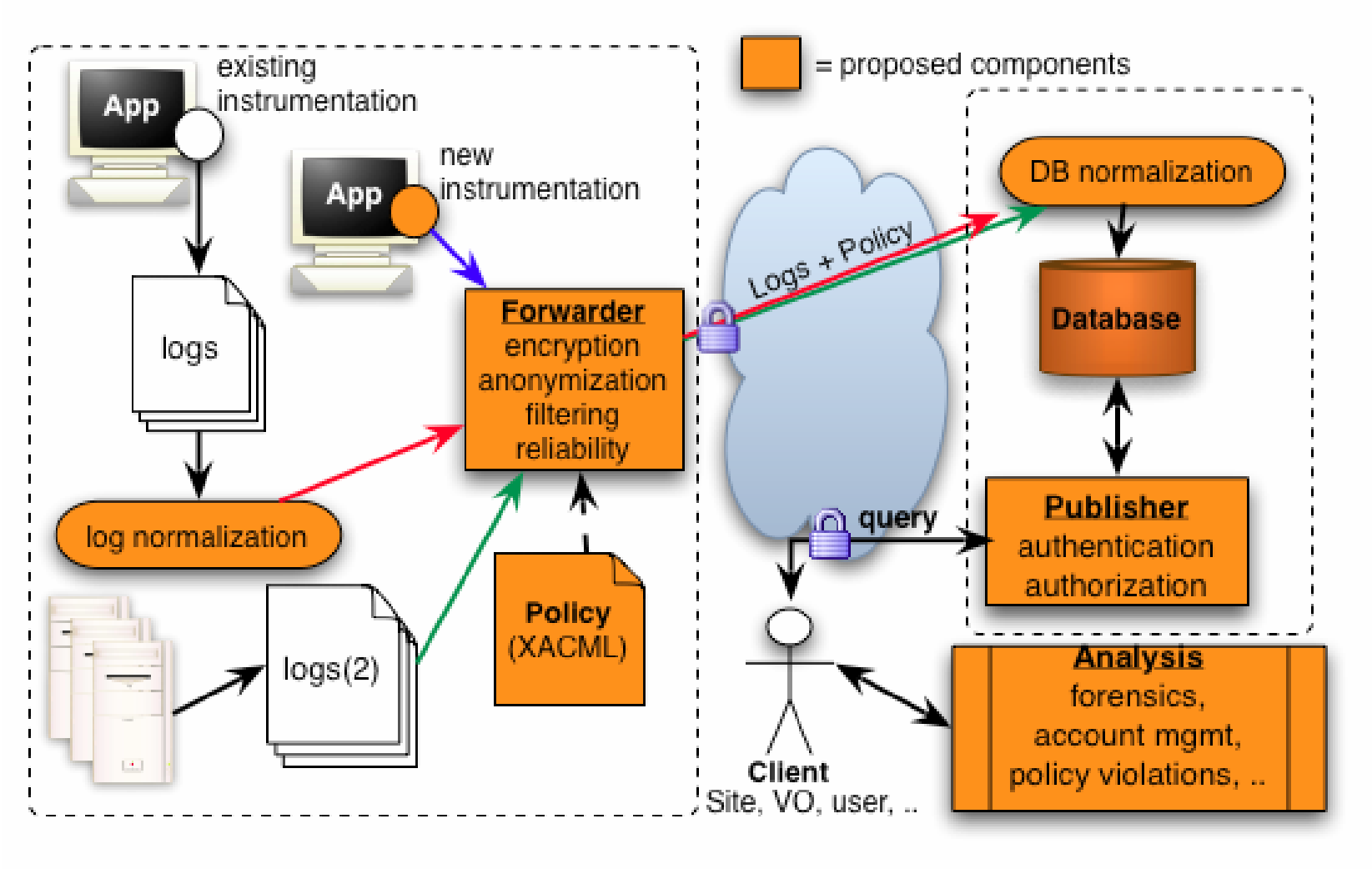
Auditing/Forensic Tools

- The Problem:
  - Multi-institutional collaborations with extensive remote access
  - Virtual organizations need to be able to track resource usage, credential usage, data access, etc
  - Difficult to get consistent audit information across sites
  - Different groups need different audit information
  - Sample questions that are currently hard to answer:
    - Give me a list of all data files opened by User X in the last week
    - What are the list of sites that user X accessed in the past week?
    - How much CPU did VO X use at site Y in the past month?
    - Give me a list of all users who used shared account X on resource Y yesterday.
    - Who made requests to the dynamic firewall service yesterday?
    - Did the IDS see any traffic on ports that where supposed to be closed, based on auditing information from the dynamic firewall service?

Auditing/Forensic Tools cont.

- High-Level Approach:
  - An end-to-end auditing infrastructure which uses a policy language to allow resource (both systems and data) owners specify where auditing information may be published and who may access the audit logs.
- Components
  - Logging software (instrumentation) - Applications call easy-to-use libraries to log events with detailed information.
  - Normalizers– Agents transform existing logs so that they can be incorporated into the common schema of the audit system.
  - Collection sub-system (forwarder) – Audit logs are collected by a dependable, secure collection system.
  - Repository (database, publisher) – Audit logs are sent over the network, normalized, and archived. Then they are made available through a query interface.
  - Forensic tools (analysis) – Forensic tools query and process the audit data to find problems and answer questions.

End-to-End Auditing System



Secure Middleware

- Problem
  - Grid middleware has become an essential part of the science infrastructure security of this infrastructure is an essential consideration
- Approach - steps
  - *Architectural analysis* to understand the system level view of a middleware component and its external interactions
  - *Identify trust boundaries/threat model* to understand the dependencies and areas of concern
  - *Component and system analysis* of the particular software to understand vulnerabilities
  - *Disclosure of results* process is handled carefully to allow time for mitigation efforts
  - *Mitigation mechanisms* to provide means of patching or mitigating the potential security vulnerability