Security for Open Science Center for Enabling Technology

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

Security CET
March 7, 2006

Guiding Principles

- Focus on capabilities that are priorities for and are NEEDED by DOE applications and facilities
- Work closely with a few committed applications and facilities to develop capabilities
- Provide development and deployment of security solutions with and in support of DOE applications and facilities
- Deliverables
  - 18 months - Concrete near term goals for deployment activities
  - year 3 and year 5 - Longer term deliverables for deployment and possible research activities
- Will provide extensive deployment support

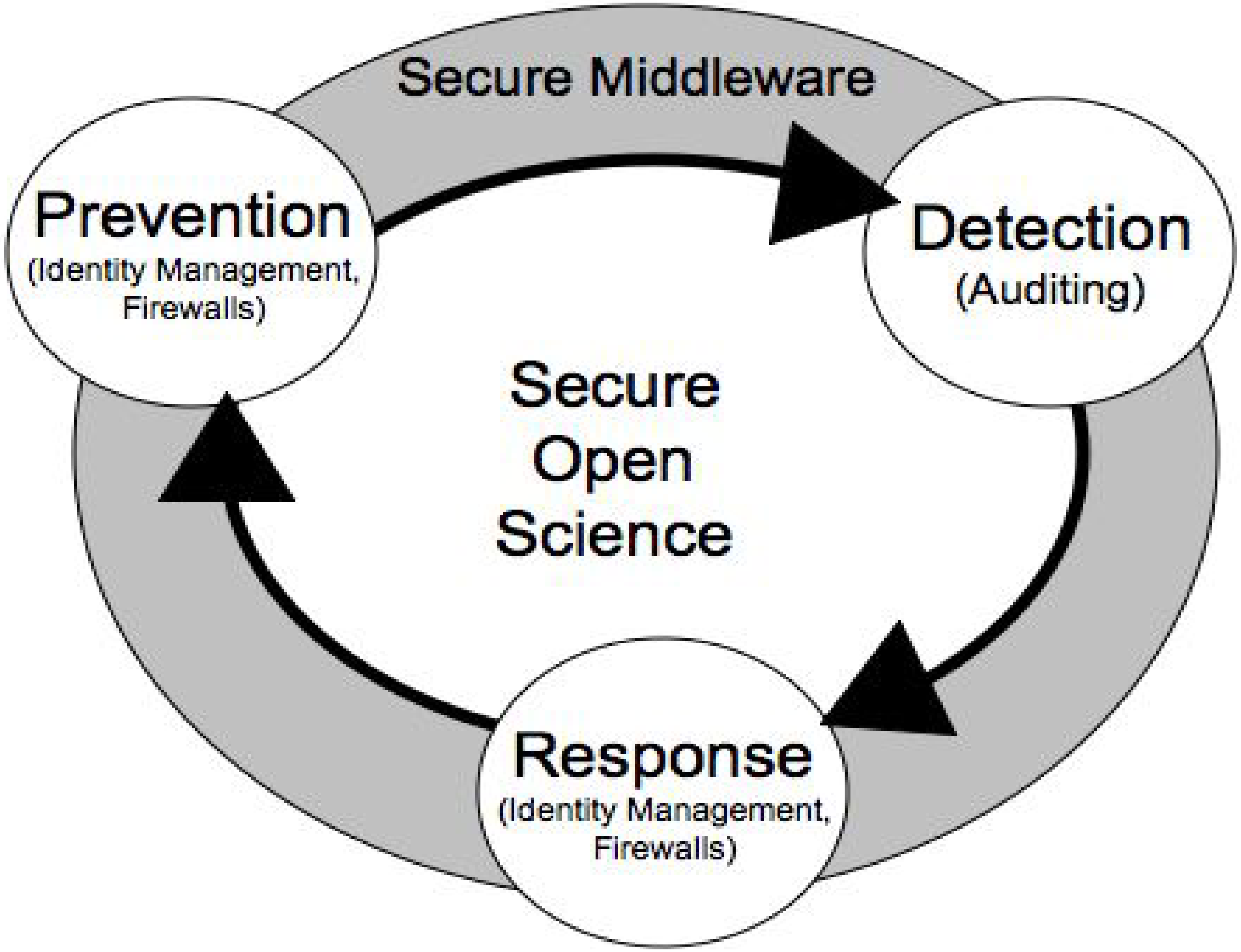
Management Structure

- 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

Distributed Science Security Problem

- Applications and Middleware poorly integrated with site security
- Difficult to track users and usage across sites
- Virtual organizations and sites do not have all the tools needed to manage security
- Forensics in distributed environments is tedious and information is scarce
- Grid middleware poses a potentially inviting hacker target in the future as we deploy these large grids
- Credential revocation is very difficult currently
- Firewalls often limit the application connectivity options

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.

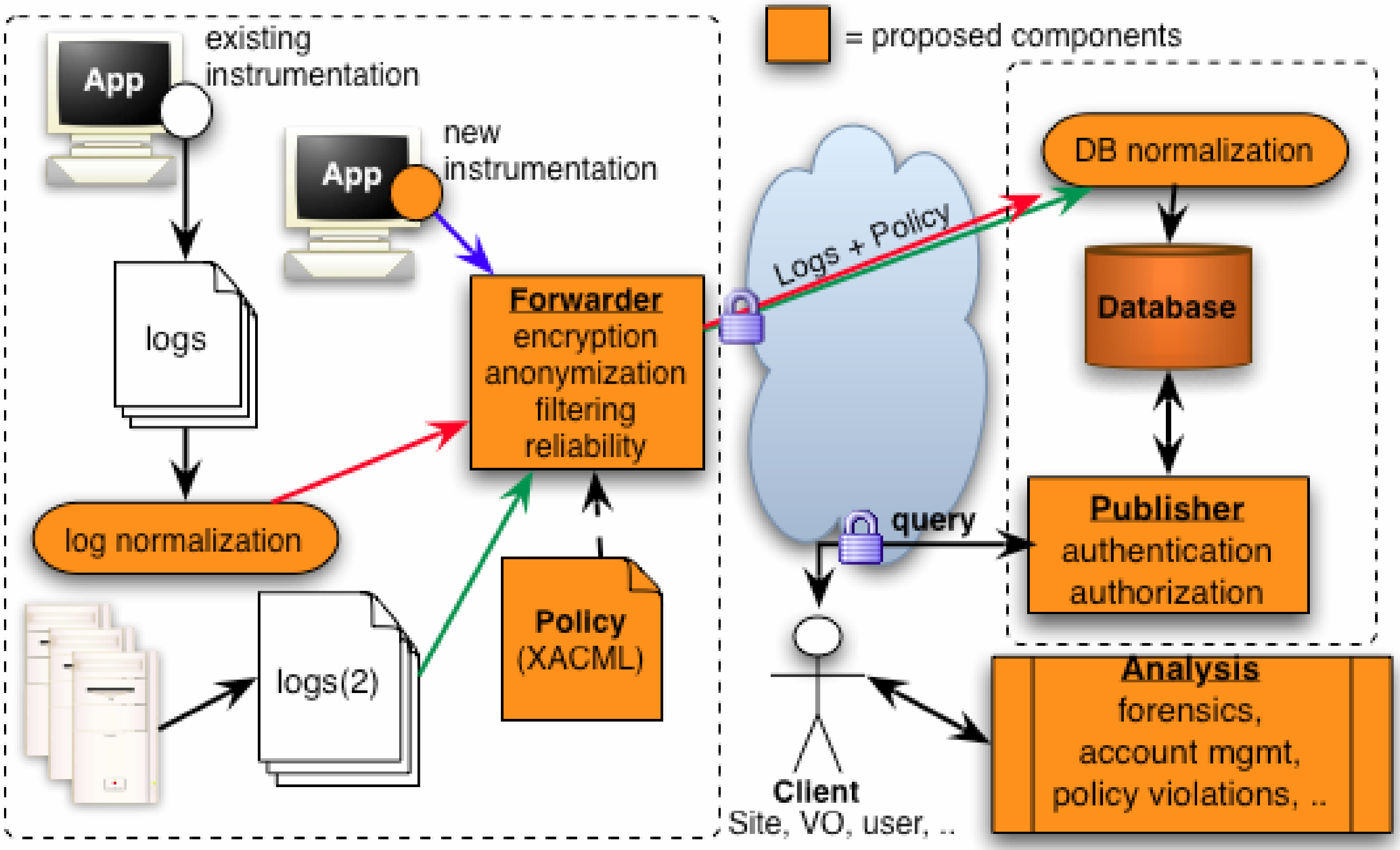
Auditing/Forensic Tools

- 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



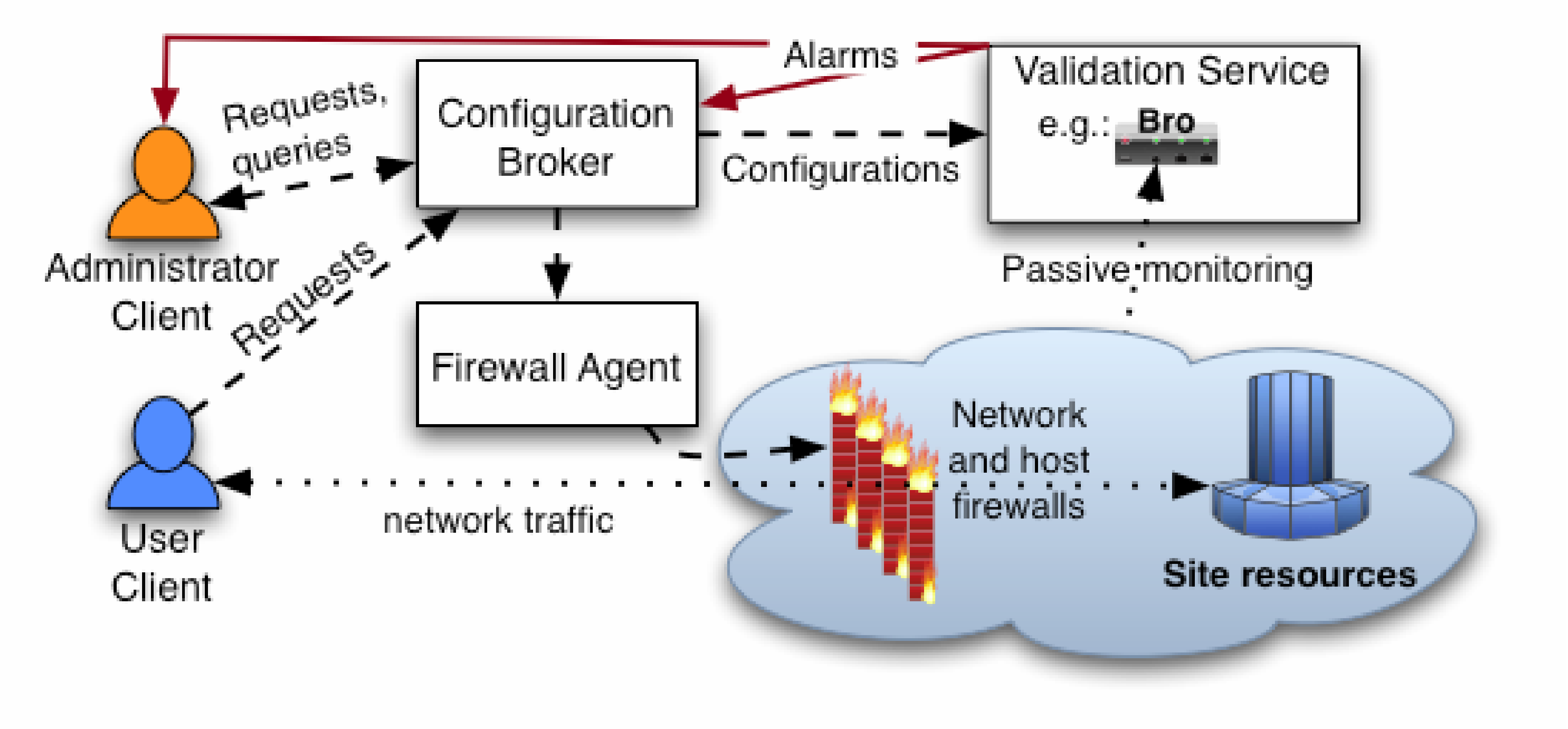
Dynamic Host Firewall Ports

- The Problem:
  - Ports needed by Grid middleware are often blocked by firewalls
    - These firewalls are both host-based and network-based.
    - Dynamically assigned ports are particularly problematic
      - **E.g.: GridFTP data ports**
  - Many sites allow outgoing, but not incoming connections
    - How do a Grid FTP between 2 sites that both only allow outgoing connections?

Dynamic Firewalls, cont.

- High-level Approach:
  - Tools and services to dynamically open and close ports needed by applications and middleware based on authentication and authorization
- Components
  - *Configuration Broker* maintains the overall state of the firewall configuration for the site, validates user credentials, and verifies that requested actions are consistent with site policy restrictions.
  - *Firewall Agent* interacts with the existing site firewall systems, receiving direction from the Configuration Broker.
  - The *Validation Service* receives information about the completed firewall changes and continually analyzes network traffic to insure there are no errors in the firewall configuration.
  - The *Programming API* is the mechanism for software to make requests to the broker.

Dynamic Firewall System



Identity Management

- Problem:
  - Revocation mechanisms are slow and cumbersome
  - Level of integration amongst various solutions incomplete
  - Nagging issues of credential renewal, configuration management, etc.
- Near Term Approach:
  - Build on existing solutions:
    - VOMS, CAS, GUMS, MyProxy, GSI, OCSP
  - Integrate and deploy, e.g.
    - Deploy OCSP service; client support in GT, MyProxy, etc.
    - VOMS support in GridFTP, MyProxy
    - GUMS callout into GT, MyProxy

Identity Management

- Longer term:
  - XKMS support to ease configuration management
  - Integrate data access control policy with work on semantic workflows
  - PKCS 11 support
  - Ubiquitous hooks in middleware for site security integration
    - E.g. Kerberos, auditing,

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

Current Plan for Start

- Funding decision still being made
- Start will be either August or October 2006
- Five year development and implementation plan
- Aggressive schedule and tight funding
- Expect to be able to work closely with and leverage extensively other efforts already underway internationally