Security

Overview

LSST has two apparently conflicting goals:

- **Openness** - generous access to data by scientists and the public
- **Security** - reliable infrastructure and long-term data integrity

As a large and publicly exciting project, LSST can expect to attract many kinds of interest, ranging from scientific curiosity to active attacks. We must ensure that we:

- Encourage engagement by providing access to data
- Prepare for both attacks and disasters
- Ensure the functioning of our essential data-collection pipeline
- Protect the long-term integrity of our data

Important Dates

- May 15 - Annotated Outline (for All Hands Mtg)
- August 2008 - Review draft for inclusion in NSF PDR
- October 2008 - NSF PDR due

Types of Security

1. Physical Security -- buildings, networks, cables, electric power, physical machines
2. System-level Security -- operating systems, processes, file systems, local user accounts & root access
3. Applications -- services, registries, trust networks, bandwidth management
4. User Access -- personal workspaces, job management, user interfaces

Sites

See also a table of LSST security realms.

- Mountaintop
    - Network access *strictly through base facility*
    - Important roles: Buffering, Network transfer to Base Facility
- Base facility (at La Serena)
    - [Who *can* access?]
    - *No public access* (all through collocated Data Access Center)
    - Nightly processing (real-time)
    - Data transferred to Archive Center
- Archive Center (at NCSA)
    - [Who *can* access?]
    - Data Archive
    - Primary data processing
- Data access Centers
    - Operated by LSST

1. Collocated with the Archive Center (NCSA)
2. Collocated with Base Facility (La Serena)
3. San Diego
4. Education and Public Outreach (EPO)

- Possibly others, independently funded

Shared Facilities

Where LSST shares a site, we can expect to collaborate with other organizations on security, especially physical security.

- NCSA
  - The LSST Archive Center will be housed in NCSA's ?Petascale Computing Facility, which will also house the NSF supercomputing cluster ?Blue Waters, expected to come online in 2011.
  - NCSA's security policy document is linked below.

[Needed: list of other organizations whose facilities we will share]

Threats

What threats does LSST need to guard against?

[To be filled in & organized -- this is really just a placeholder]

- Data deletion, both accidental & malicious
- DOS, both accidental & malicious
- Loss of connectivity (is this a security issue, an operations issue, or both?)
  - Between mountaintop & base station
  - Between base station & archive center

Are these threats too abstract? Should we focus on things like "cable cut" instead of "loss of connectivity"? Both the cause & the symptom are important.

Questions

How does security policy relate to:

- Disaster preparedness? For example, cable cuts on the mountain?
- Application performance? In particular, denial-of-service that exploits expensive computations?
- Measuring and ensuring data integrity?
- Data provenance (especially the relationship between authentication and data provenance)?

Related Documents

Institutions

?NCSA Security Policies

?NOAO Security Policies

- ?Cybersecurity and Acceptable Use (html)
- ?Acceptable Encryption Use Policy (pdf)
- ?Network Audit Policy (pdf)
- ?Backup Policy (pdf)
- ?Information Sensitivity Policy (pdf)
- ?Laptop Security Tips (pdf)
- ?Guidelines for Choosing a Good Password (pdf)
- ?Privileged Account Access Policy (pdf)
- ?Remote Access Policy (pdf)
- ?Server Security Policy (pdf)
- ?Wireless Access Policy (pdf)

Guides and Handbooks

- ?Guide to NIST security documents (pdf, March 2007, 36 pages)
- ?NIST Security Handbook for Managers (pdf, October 2006, 178 pages)
- ?NIST Security Handbook (pdf, 1995, 290 pages)
- ?RFC 2196 - Site Security Handbook (html, 1997)

Document Template Collections

- ?SANS
- ?NIST archive
- ?Templates from Ephibian (attached below)