Data Security in LSST

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
- August 2008 - Release Candidate 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
    - LSST will share a major new data center with NCSA, whose most notable resident will be the NSF supercomputing cluster ?Blue Waters which is expected to come online in 2011.

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

Questions

- How does security policy relate to disaster preparedness?
- How does security relate to measuring and ensuring data integrity?
- How does security, especially authentication, relate to data provenance?

Related Documents

?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)