Security of Rubin Observatory data

William O'Mullane

2021-05-13

1 Introduction

There is a perceived risk that LSST images may be snooped during transmission from the telescope. This concerns the images used for alert processing which are transmitted within a minute and provide a valuable resource for identifying moving objects including satellites. Though our processing will ignore satellites other parties may be interested in this information.

There have been several communications concerning encryption on the wire, and this is covered in some detail in DMTN-163.

In Section 2 an attempt is made to list new requirements based on the current discussions. An LCR needs to be raised to bring these costed and bought into the construction baseline.

1.1 Baseline

The Rubin Observatory construction project has been built with academic level security in mind. The Information classification policy LPM-122 classifies data as "User Protected". The DM Information Security plan LDM-324 states the "majority of network traffic will not require confidentiality"

Since our astronomy data is research data with no intrinsic value no great efforts have been made to secure the data nor the network it is traveling on. The network has been designed, and now largely implemented, for high throughput not for high security.

The baseline is for encryption of controls but not data i.e. authentication is encrypted, data transmission is not.

We assume the security rating of LSST data (or subsets of it) as per NIST [NIST.800-60]. This is also one of the first steps in [NIST.FIPS.200] called out in [NIST.SP.800-171]. We define

the security objective to be *Availability*, the potential impact is *low* for confidentiality, availability and integrity. Hence the Security Category (SC) is {low,low,low} in NIST terms.

2 New requirements

This is a list of new requirements which will require an LCR and costing.

NR-1 The operations team with LLNL shall design and implement an Alert Vetting System(AVS)..
Data Production shall send a subset of potential alerts to LLNL for processing via the AVS, which will run at that separate facility. LLNL will check those alerts against their catalog of assets and flag alerts that should not be issued before the embargo time expires. Rubin should send the alert packets as generated; a list of all the alert packet IDs with a Boolean hold flag should be returned to DP. At a later stage (end of night) a list of images to be embargoed for a longer period should also be returned. (See page 4.)

NR-2 DM shall implement a delayed data store. .
The delayed data store will need to hold AVS embargoed images on encrypted disks for a period of between 1 and 30 days. (See page 4.)

NR-3 IT shall purchase routers capable of performing AESStandards (2001) IPSec in between Chile and SLAC..
At lease two routers will be needed and we may need four for failover. This is a multi million dollar commitment. (See page 5.)

NR-4 IT shall increase physical security in Chile and SLAC..
Physical measures shall include :

- Locks on server racks.
- Sensors and cameras to record the opening of cabinets.

- Out of band channel for physical security alerts if main network is disabled.
- Access control devices to server rooms that record entry/exit by personnel.
- Auditable processes to handle on-boarding, off-boarding, maintenance work, removable media, etc.
- For the secure delayed store :
  - Controls to prevent booting from USB devices or copying to external media.
  - Full disk encryption to protect against theft or returns of hardware.

(See page 5.)

3 Which data is sensitive ?

In communications thus far and in the security summit held on 6^{th} April 2020 all data has been considered.

Since then the idea of an Alert Vetting System (AVS) to be implemented by LLNL has been raised. A certain set of of potential alerts would be sent to and evaluated by the AVS. These would include all streaks unattributable to known asteroids that

1. correspond to objects moving faster than vMax=30 deg/day, or
2. whose velocity cannot be determined (e.g., due to overlaps with chip boundary).

Streaks not forwarded to the AVS would be published as per current baseline. Forwarded streaks will be vetted. If a streak is determined to be astrophysical by the AVS, it will be included in the prompt product data base and shipped to the Minor Planet Center (MPC) with all other natural streaks. If it is not natural, it will not be returned by the AVS and hence eliminated fro the prompt products database and not sent to the MPC.

NR-1 The operations team with LLNL shall design and implement an Alert Vetting System(AVS)..

Data Production shall send a subset of potential alerts to LLNL for processing via the AVS, which will run at that separate facility. LLNL will check those alerts against their catalog of assets and flag alerts that should not be issued before the embargo time expires. Rubin should send the alert packets as generated; a list of all the alert packet IDs with a Boolean hold flag should be returned to DP. At a later stage (end of night) a list of images to be embargoed for a longer period should also be returned.

3.1 Delaying focal plane data

We believe the vast majority of the 20TB of nightly images are not of a sensitive nature however we understand the wish is to hold all images in an encrypted store for at least 1 to 3 days. We understand AVS may embargo some images for up to 30 days based on the streaks found in them.

NR-2 DM shall implement a delayed data store. .

The delayed data store will need to hold AVS embargoed images on encrypted disks for a period of between 1 and 30 days.

4 Network security

The transfers from Summit to Base and Base to NCSA go over private networks that are not part of the public Internet. We have our own dedicated fibers running from the mountain to the base [LSE-78], intercepting transfers would require physical access to the fibers - tapping those would probably disrupt our network at least temporarily.

We understand there is a concern for the transmission of the images for alert processing and DMTN-163 covers this in detail.

NR-3 IT shall purchase routers capable of performing AESStandards (2001) IPSec in between Chile and SLAC..

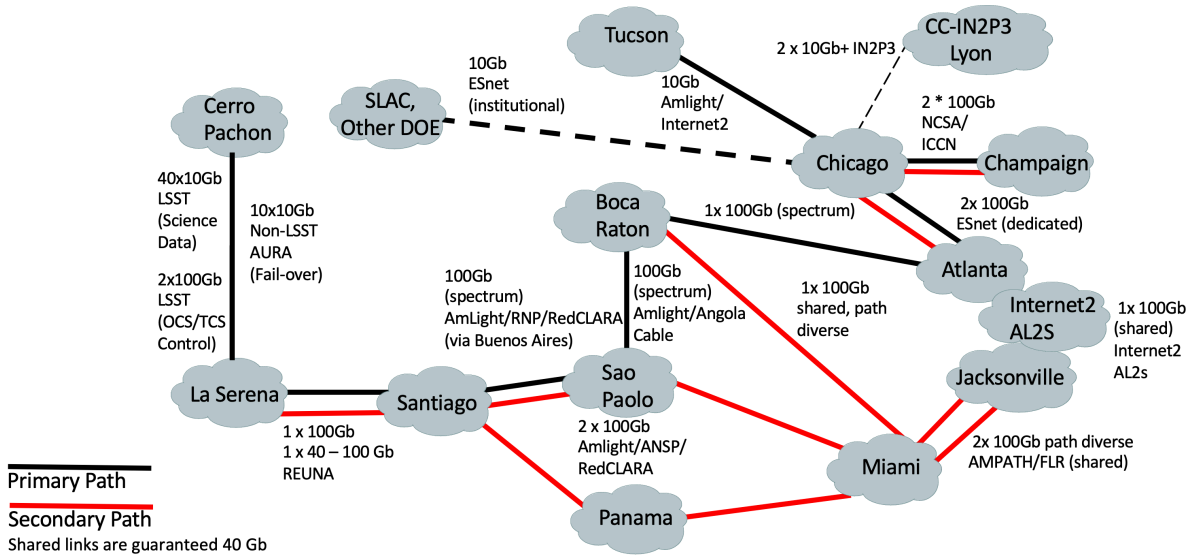

FIGURE 1: Rubin Observatory Network topology for FY22, the primary route is on dedicated lines, the back route is on shared equipment. Securing this beyond the level of the provider will be close to impossible.

At lease two routers will be needed and we may need four for failover. This is a multi million dollar commitment.

If we do not transfer embargoed images to France or UK we understand encryption on the international links should not be needed.

5 Physical Security

On the mountain and in the base facility Rubin networks and computers are in rooms requiring ID card access and the compounds have 24/7 security staff. We can increase physical security in Chile and SLAC. Access from outside the site is only via VPN. This also implies limiting the Rubin personnel who have access to the files during the night.

NR-4 IT shall increase physical security in Chile and SLAC..

Physical measures shall include :

- Locks on server racks.
- Sensors and cameras to record the opening of cabinets.
- Out of band channel for physical security alerts if main network is disabled.
- Access control devices to server rooms that record entry/exit by personnel.
- Auditable processes to handle on-boarding, off-boarding, maintenance work, removable media, etc.
- For the secure delayed store :
  - Controls to prevent booting from USB devices or copying to external media.
  - Full disk encryption to protect against theft or returns of hardware.

5.1 Chile physical security

The summit computer room is used exclusively by Rubin Observatory, however, the computer room at the base is shared with other NOIRLab programs.

The administration of the base computer room belongs to NOIRLab.

Rubin's computer rooms in Chile have the following security controls:

- Access to the computer room is controled by card readers. The system is administered by NOIRLab.
- Video surveillance of Rubin's computer racks. The surveillance platform is administered by Rubin.
- Computer racks are maintained always locked, both front and back door.
- Water and temperature sensors are located in several locations of the computer rooms.
- Door locking sensors are located in racks with critical networking equipment.

6 High level summary

Though the reason behind the call for security and the level required remain totally unclear NSF and DOE asked for a brief summary of possibilities. One should also consider which data we are talking about see Section 3. Items here are not costed but an indication is given in terms of low (possibly within cost), moderate (some $100Ks), high (>$1M) Any change should be properly costed.

Security idea	Rough cost level
Delay/degrade image info. If the precise position of small objects is the driver then not providing accurate shutter times would make precise positions inaccessible	Low to Moderate.
Delay some or all images. Depending on how secure this needs to be and where it is done the cost scales.	Low to Moderate.
Do alerts in Chile. If we want to control image access for a longer period we could consider alert production in Chile. The hardware budget would remain the same but we may require extra support in Chile.	Low to Moderate.
Encrypt all images. This would have to be done on the summit or in la Serena before hitting the long haul network. Possibly no new hardware needed but a change in software.	Can be Low
Transmission Layer Encryption. Network encryption would probably require new hardware.	Moderate
Physically securing the network. This will be next to impossible and would probably require new network agreements. This however would be the only way to ensure no packet snooping.	Very high
Avoid certain time coordinates. This would require changing the scheduler to provide more constraints on pointing.	Moderate

A References

[DMTN-163], Allbery, R., 2020, *Encryption of Rubin Observatory data*, DMTN-163, URL `https://dmtn-163.lsst.io`,
LSST Data Management Technical Note

[NIST.FIPS.200], Division, C.S., 2006, Publication 200, minimum security requirements for federal information and information systems, URL `https://doi.org/10.6028/NIST.FIPS.200`

[LDM-324], Kantor, J., 2016, *Data Management Information Security Plan*, LDM-324, URL https://ls.st/LDM-324

[LSE-78], Lambert, R., Kantor, J., Huffer, M., et al., 2017, *LSST Observatory Network Design*, LSE-78, URL https://ls.st/LSE-78

[LPM-122], Petravick, D., 2015, *LSST Information Classification Policy*, LPM-122, URL https://ls.st/LPM-122

[NIST.SP.800-171], ROSS, R., VISCUSO, P., GUISSANIE, G., DEMPSEY, K., RIDDLE, M., 2020, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Standards, F.I.P., 2001, Announcing the advanced encryption standard (aes), URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[NIST.800-60], Stine, K., Kissel, R., Barker, W.C., Fahlsing, J., Gulick, J., 2008, INFORMATION SECURITY, 31, URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

B Acronyms used in this document

Acronym	Description
AES	Advanced Encryption Service
AVS	Alert Vetting System
DM	Data Management
DMTN	DM Technical Note
DOE	Department of Energy
DP	Data Production
IT	Information Technology
LCR	LSST Change Request
LDM	LSST Data Management (Document Handle)
LLNL	Lawrence Livermore National Laboratory
LPM	LSST Project Management (Document Handle)
LSE	LSST Systems Engineering (Document Handle)

LSST	Legacy Survey of Space and Time (formerly Large Synoptic Survey Telescope)
MPC	Minor Planet Center
NCSA	National Center for Supercomputing Applications
NIST	National Institute of Standards and Technology (USA)
NSF	National Science Foundation
OPS	Operations
SC	Science Collaboration
SLAC	SLAC National Accelerator Laboratory
SP	Survey Performance
UK	United Kingdom
VPN	virtual private network
deg	degree; unit of angle