

Security of prompt imaging on LSST

William O'Mullane

2019-02-25

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.

2 Network security

On the mountain and in the base facility LSST networks and computers are in rooms requiring ID card access. We could increase security but it would be costly and probably not very popular with staff i.e it would require raising the security level of the entire facility to something like FSL¹ 2 .

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 disrupt our network at least temporarily i.e. we would at least know something was up. Though technically feasible by perhaps bribing or coercing staff somewhere this seems unlikely - a physical tap should also be noticed during fiber inspections. The image as transferred over this line is also in an obscure format (though could be put together with some effort).

3 Transmission security

As we understand it, holding data for 12 to 24 hours before releasing to the collaboration is an acceptable approach to securing the images - this can be ensured by limiting the LSST personnel who have access to the files during the night. We would transmit images for alert

¹<https://emilms.fema.gov/IS1172/groups/85.html>

processing in near realtime to NCSA.

Currently alert images from the base are to be transmitted using BBCP². The control channel is encrypted but the data channel is open - this is considered secure in the scientific world (Hanushevsky et al., 2001). Hence theoretically packets could be snooped on the their way to Illinois could be extracted and processed.

We could encrypt the data channel. This would cost us in compute, potentially doubling or more the number of cores needed for transfer. We would also have some software modification and setup. There are also examples of hardware solutions for this which would probably be affordable, INRIA in Muehlberghuber et al. (2013) have build a FPGA based AESStandards (2001) implementation which gives 100Gbit/s network rates with μs additional latency. Table 3 of Muehlberghuber et al. (2013) lists the hardware which looks modest enough - we work with INRIA already. There is no price given in the document, but considering the cost of components and a contract to put it together one *might* consider it to be under \$1M, but we would need to get a quote.

We could encrypt the images themselves before transmission or even on the FPGA of the camera data acquisition (DAQ) system. The DAQ is complex construction prone to delays so we would rather not jeopardize the project by introducing changes there. Encrypting the files outside would mean more CPU and I/O - it would add a delay in the alerts processing - it may take as much as 20% of the alerts time budget (1 minute). This would not be very welcome in the science community. This would require some effort on our side to add encryption to the processing chain but this should be order some hundreds \$K depending on how *secure* it is required to be.

3.1 Keeping it in Chile

The original baseline was to do alert processing in Chile in the base facility. Some years ago support for computing in Chile was sub optimal but has improved significantly - there is space in the base facility to hold machines for this. If we agree the base/summit are secure we could avoid on the wire snooping by doing alert processing in the base facility. We would also then have to hold images there for the appointed embargo time (12 or 24 hours) before releasing them to the community. We would need to do some work on the cost impacts of this but they should not be insurmountable.

²BBCP is an alternative to Gridftp when transferring large amounts of data

A References

References

Hanushevsky, A., Trunov, A., Cottrell, L., 2001, In: In Proc. of the 2001 Int. Conf. on Computing in High Energy and Nuclear Physics (CHEP 2001), Beijing, URL <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.2288&rep=rep1>

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

Muehlberghuber, M., Keller, C., Gürkaynak, F.K., Felber, N., 2013, In: Burg, A., Coşkun, A., Guthaus, M., Katkooori, S., Reis, R. (eds.) *VLSI-SoC: From Algorithms to Circuits and System-on-Chip Design*, 1–20, Springer Berlin Heidelberg, Berlin, Heidelberg

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

B Acronyms used in this document

Acronym	Description
AES	Advanced Encryption Service
BBCP	BaBar Copy Program
CPU	Central Processing Unit
DAQ	Data Acquisition System
DM	Data Management
DMTN	DM Technical Note
FPGA	Field-Programmable Gate Array
FSL	Facility Security Level
INRIA	French National Institute for computer science and applied mathematics
LSE	LSST Systems Engineering (Document Handle)
LSST	Large Synoptic Survey Telescope
NCSA	National Center for Supercomputing Applications