SECURE REMOTE ACCESS TO TELEMETRY: A STUDY IN HOW TO ALLOW REMOTE ACCESS TO SATELLITE TELEMETRY DATA

Arthur T. McClinton Jr.
Noblis, Inc[1].
Falls Church, VA
Art.McClinton@Noblis.org

ABSTRACT

The need to allow remote access to telemetry data from closed networks has long existed. To ensure the correct engineers are available for anomaly resolution, NOAA developed the Secure Remote Access Server (SRAS) to allow transfer of satellite telemetry to an external secure server. SRAS uses one-way links to protect the ground system and secure communications for all communications with the user. After the SRAS was developed, a similar system was developed to support file transfers. This paper provides an overview of these systems and lessons learned in the development of one-way fiber systems.

Keywords: secure remote access, one-way link, OWL

BACKGROUND

Early in the morning of August 21, 1993, NOAA 13 started what was expected to be a normal acquisition pass at the station in Fairbanks, Alaska. The Polar-Orbiting Operational Environmental Satellites (POES) are the backbone of the remote sensing system used by the National Weather Service (NWS) to collect the information needed to generate the long-range global weather forecasts for public and governmental uses. Soon, the operator workstations in the NOAA SOCC started beeping, indicating that something could be wrong with the satellite. Since the spacecraft had passed its initial checkout and this event occurred outside of regular working hours, the only people present were the spacecraft controller and an aerospace engineering technologist. After quick consultation it was determined that a problem appeared to exist in the power subsystem, so the power subsystem engineer was called at home. Although he was very concerned, he decided to wait until the next satellite contact to see what additional data he could collect before making the drive to the office. Therefore, it was 104 minutes later that it became apparent to everyone that this was an emergency that needed to be addressed to try to save the 13-day-old spacecraft. Unfortunately by the time the engineer arrived at the SOCC and the next spacecraft contact was possible, no signal was received.

Although the subsequent National Aeronautics and Space Administration (NASA) / NOAA review team experts agreed that nothing could have saved NOAA 13, it was determined in many cases that quick reaction from the subsystem engineers could extend the life of the orbiting NOAA environmental satellites. SRAS development and installation led to a significant difference when GOES 12 suffered a propulsion leak in early December 2006. The GOES Ground system engineer was on business travel at the time he was notified of the leak. He pulled out his laptop and connected to the SRAS where he was able to monitor the activities to perform the emergency momentum unloads and other associated activities to save the satellite.

The failure of the NOAA 13 led to Mitretek Systems[2] developing the Engineering Network Prototype (ENP) to show how web access could be used to distribute satellite data from the closed SOCC Local Area Network (LAN) to allow engineers to examine data from home. The results of this prototype led to the development of requirements and potential architectures for the development of the SRAS. The SRAS design and development was performed by Pragmatics Inc[3]. It has been available to NOAA engineers since 2003.

With the advent of the USB drive, NOAA engineers wanted to use a USB to extract data from the closed satellite ground system network while the NOAA IT Security Officer wanted to ban USB usage. NOAA decided to use part of the SRAS technology to develop an External Analysis Transfer System (EATS) which would allow an engineer to export satellite data without the need to use USB technology.

This paper describes the ENP, the SRAS, the EATS and the lessons learned while developing and operating them.

ENGINEERING NETWORK PROTOTYPE

The first step of the process, showing NOAA that such a system was feasible, was accomplished during a year-long Engineering Network Prototype (ENP) task jointly sponsored with Mitretek Systems Sponsored Research funds and NOAA Office of System Development funds. The ENP exported NOAA 14 data and made it available for the engineers to view using a simple network browser. The prototype was rapidly accepted by the user community and served as the test bed for developing the requirements used in the fielding of a formal system to support all of the SOCC controlled satellites.

The ENP[4] provided a test bed for developing scenarios for extracting data and making it available to an engineer at home. Figure 1 illustrates the ENP architecture[5]. To enable quick development, the NOAA 14 segment files were automatically fed into the ENP front-end processor that executed the POES Acquisition and Control Sub-system (PACS) operational decomutation software. The results were sent to the ENP Server. The data was stored using a MYSQL database. The spacecraft engineer retrieved data while using a standard web browser. Plotting and analysis was performed using helper applications of EXCEL or PV-WAVE.

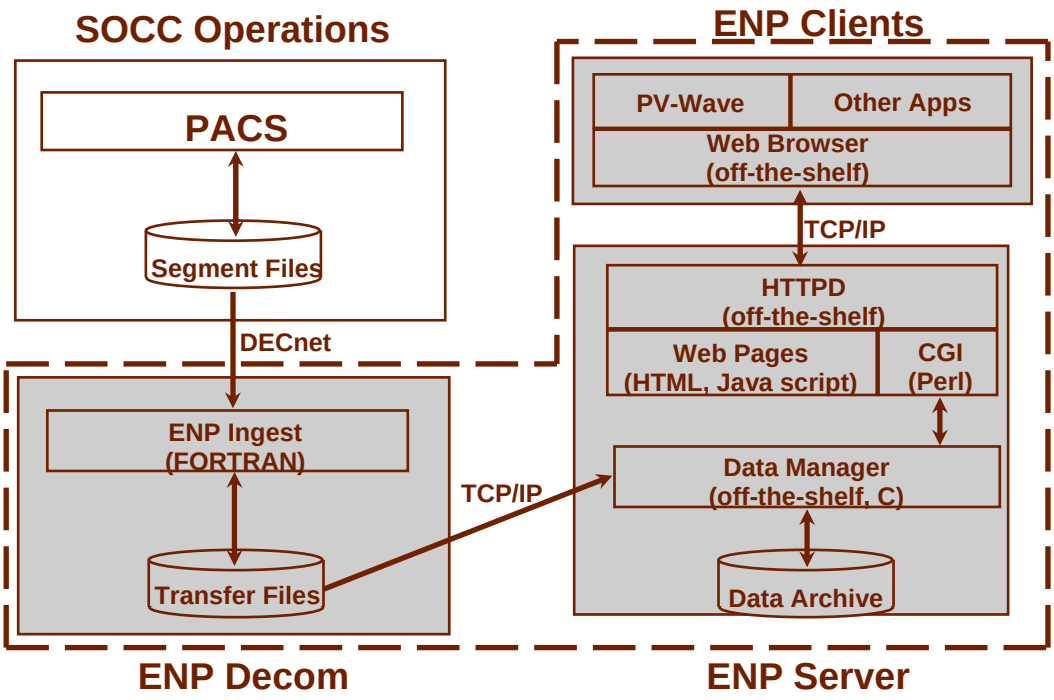

Figure 1. Engineering Network Overview

Although the ENP was highly praised by the NOAA engineers, several features were purposefully overlooked during the rapid development of the prototype. The main goal of the prototype was to determine if the users would accept a web interface. This prototype led to the development of requirements for both the follow on SRAS system and the SOCC workstation replacement contract[6].

REQUIREMENTS AND ARCHITECTURE DEVELOPMENT

During the development phase, NOAA collected another set of user developed requirements. The independent cost estimate showed that users had specified requirements that would double the SRAS costs. Many of these new requirements resulted from new engineers who had not been part of the prototype. Mitretek Systems was tasked to provide an evaluation of possible architectures for the system. These architectures showed the impact of some of the more costly new requirements. Presented with the various concepts of operations, the costs of the various requests, and the optional system architectures, the users chose the architecture shown in Figure 2. This architecture provided a system that is external to the SOCC. Its only connection to the SOCC uses one-way fiber links where the data is pushed from the existing telemetry and command (T&C) systems to the SRAS server. Once received by the SRAS it is stored in a database for retrieval by users[7].

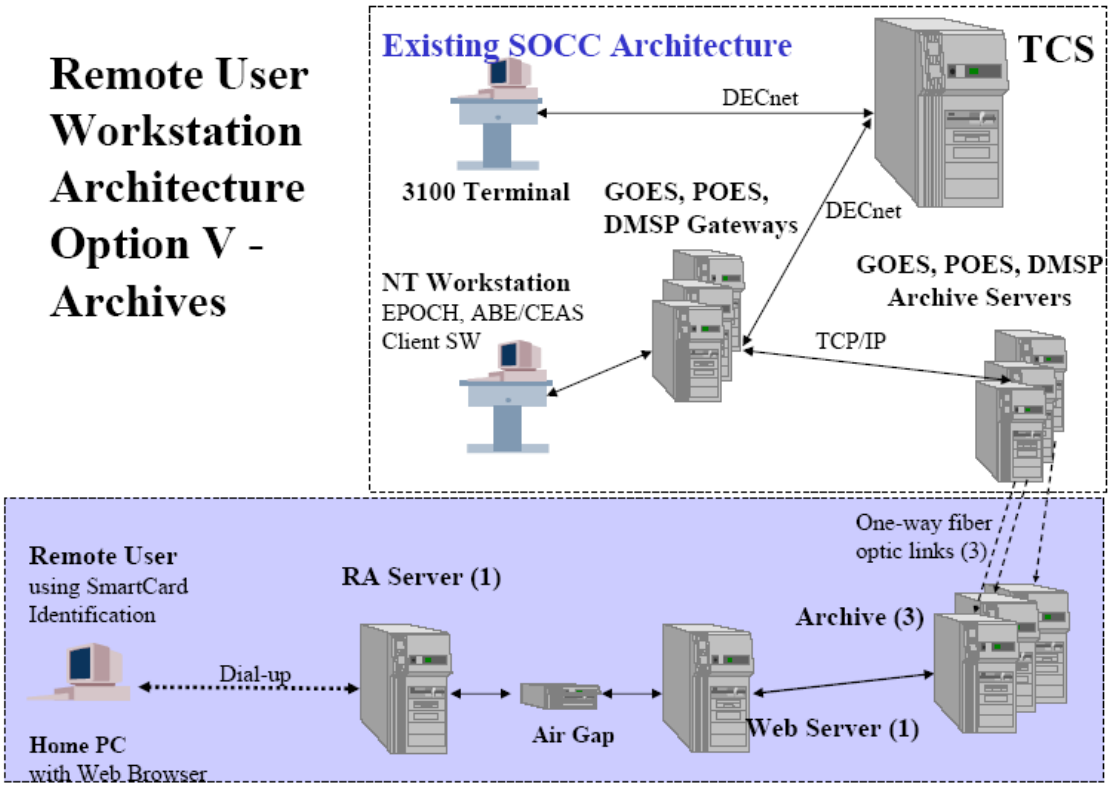

Figure 2. Selected Architecture for Remote User Workstation

SECURE REMOTE ACCESS SERVER

Figure 3 shows a data flow through from the POES T&C system through the SRAS to a external user. The data is sent from the POES archive storage on the closed LAN to the "Blue OWL" where it is forwarded to the "Red OWL" which is located on the SRAS network. The OWL[8] pairs collect health and safety data from the existing T&C systems. Next the data is ingested into the SQL database via the Braxton Technologies[9] WebTLM ingest scripts. During this process the user is notified of any anomalous conditions specifically requested. Once the data is stored in the database, the user can make specific requests from the SRAS Web Application which runs the Braxton Technologies WebTLM package. For a more complete description of the SRAS with screen shots of the data please see one or more of the following references[10,11].

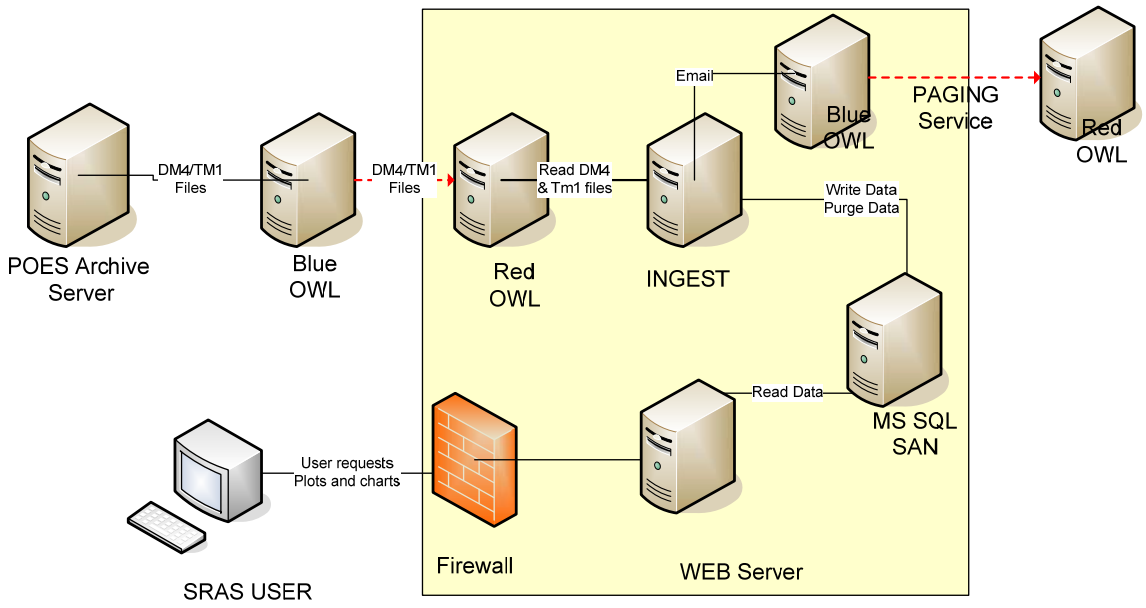

Figure 3. Major Components of SRAS Application

A separate series of machines is used for each of the four (POES, DMSP, GOES I-M and GOES NOP) satellite series that are monitored by NOAA.

The SRAS security suite is designed to protect the SRAS while making it easy for the user to access the system. What the user sees is a certificate that is placed on a smart card. This certificate not only indentifies the user but protects the data sent to the user. In addition to a firewall, an Intrusion Detection System (IDS) monitors all traffic on the SRAS network.

The SRAS has been available for use by NOAA engineers since April 2003. During this timeframe, some SRAS tuning and sizing has taken place. In 2007 a full refresh was made to upgrade to blade technology and latest operating systems. At the present time, an engineer can request a plot or chart of data from any of the GOES, POES, and DMSP operational satellites. Each of the satellites produces from 50–100 million points of data per day. This data is stored in the MS SQL database for retrieval by the engineers and the data is deleted after 24 or 48 hours.

EXTERNAL ANALYSIS TRANSFER SYSTEM

With the development of a common windows based workstation for use on all of the NOAA T&C systems and the spread of the USB disk drives with capacities exceeding 4 GB, the users started requesting access to the USB ports on the workstations. This obviously has security implications. It was determined that a method was needed to allow the user to export data from the closed T&C network to the user Administrative network used in the offices. The decision was made to use the OWL computers in a fashion similar to that used within SRAS. Users would copy or ftp files to the Blue OWL where

they were automatically copied to the Red OWL (and deleted from the Blue OWL). Files remain on the Red OWL for a period of time (nominally 10 days) since they are owned by the system and not the original user.

The EATS software was an enhancement to the SRAS system. The software did not require the special signal files used within SRAS and it had a heart beat to verify that everything was working correctly. After writing the telemetry file, SRAS would then write a zero length signal file to indicate the first file was ready for transfer. EATS was programmed to monitor the increasing file size to determine when it had been fully written. This removed the need for signal files. The other problem observed in SRAS was the link from Blue to Red would stop operating for various reasons. Thus EATS was modified to include sending a temporary file every minute if no normal traffic had been sent. On the Red side an email message was sent to the administrator if no file had been received (normal or temporary) within a 2 minute period.

During the development of EATS a user came with a request for EATS to have an option to not overwrite files with identical names. Thus we allowed special characters to the file name which were used by the Red side to change the file name by adding the current date or current time to the file name stored on the Red machine.

LESSONS LEARNED

The development of the ability to allow engineers to access remote telemetry data to monitor the operations of NOAA spacecraft has provided several lessons. Most of these lessons are obvious in hindsight but originally were not considered when developing the SRAS and the EATS.

Prototyping only answers the questions you ask - The ENP was based upon stovepipe architecture. It did not consider Security or COTS products. While it did provide a basis for the generation of requirements, it did not provide the architecture alternatives that were later considered in the possibility of various COTS products.

Requirements need to be considered within possible architectures - The use of an architecture study following the requirements development led to a rational manner to modify the costly requirements. The selected architecture led to new requirements based upon that architecture. We found when the users understand the architecture and cost impacts of specific requirements they are more able to participate in the design of the system.

One-way communications needs a back channel - The OWL one-way fiber implementation used the Secure Directory File Transfer System (DFTS) COTS product. Although this product will guarantee the reliable delivery of the file from the Blue to the Red OWL by sending a file twice and then comparing, it has no back channel and hence no way to identify that a file did not make it from Blue to Red. We did find that the normal reason for a failure was caused by the application software. What the EATS

programming accomplished was to add robustness to this transfer. The first improvement was to handle exceptions that would cause the original file to fail and the second was to provide a heart beat file. A small file was transferred on a regular basis (once a minute), if no user data files were available for transfer. Then on the Red OWL side, the receive program would issue an email message to the administrator if no file was received within the expected period of time.

Monitor operations at the appropriate level - Within the SRAS, the data is stored in the MS SQL database for retrieval by the users. If the data flow stops for any reason, the first to know were the users that had logged into the system to access data. The second version of the SRAS added the capability to page the SRAS administrator if no data was received for each specific satellite within the defined period of time. Thus for a GOES satellite, which is constantly sending data, it might be set for 30 minutes. On the POES low earth orbiting satellite it might be set at a longer period of time to exceed the expected largest data gap. This approach allowed the administrator to be the first to know of an outage instead of a user.

Long lasting COTS systems need flexible architectures – NOAA had been accustomed to building a stovepipe system on a platform and running it for a decade or more. They still have 20-year-old VAX computers running portions of the ground system. SRAS on the other hand is interfacing to users running Windows and Internet Explorer. Even though the requirements specified IE 5.0 and up, the new security requirements within later versions of IE resulted in needing to make changes to the SRAS. SRAS was originally developed to support users running Windows 98/2000, Internet Explorer 4/5 and dial up lines. During the development and refresh cycle all users have upgraded to XP, IE 7 and internet connections. The SRAS refresh has improved the ability to handle expected future changes.

Recognize and plan for rapidly changing technologies - The smart card technology used for maintaining the certificates has changed at such a rapid pace that we have found that we need to buy sufficient cards to support needs of all users. The first SRAS was developed for a specific smart card. When SRAS was fielded these cards were not available and an upgrade was needed to have sufficient cards for the user community. SRAS was originally designed to meet the Federal Bridge standard but availability of products resulted in changing to certificates on smart cards. When USB smart cards replaced smart cards and smart card readers, SRAS was once again changed to meet the new standard. The eventual implementation of HSPD12 standards will result in additional changes to the system to support this form of authentication.

REFERENCES

[1] Noblis, Inc is an independent, non-profit, science, technology and strategy company working in the public interest. For further information see www.Noblis.org

[2] Mitretek Systems was the corporate name for Noblis prior to February 2007

[3] Pragmatics Inc. was the prime SRAS contractor, more information can be found about Pragmatics at http://pragmatics.com/.

[4] Small, B., “Engineering Network Prototype Final Report,” Mitretek Systems, 1998.

[5] McClinton, A. T. Jr., "NOAA POES Engineering Network Prototype Status," Grounds Systems Architecture Workshop, Aerospace Corporation, 1998.
[6] "Common Engineering Analysis System Requirements Specification," Mitretek Systems, 1998.
[7] McKenzie, K. and the SRAS Team, "Secure Remote Access Server Architecture," NOAATECH2002, *www.noaatech2002.noaa.gov*.
[8] OWL is the trademark and product of OWL Computing Technologies Inc. It is a secure one-way link using data diode technology. More information is available at *www.owlcti.com*.
[9] Braxton Technologies produces several COTS ground system products including the WebTLM product chosen for SRAS. More information can be found at http://www.braxtontech.com/.
[10] McClinton, A.T. Jr, "Secure Access to Telemetry Data", Grounds Systems Architecture Workshop, Aerospace Corporation, 2005, http://csse.usc.edu/gsaw/gsaw2005/s4/mcclinton.pdf
[11] McClinton, A.T. Jr, "SRAS Overview", Presented to the SOCC Lunchtime Seminar, 2008, http://www.oso.noaa.gov/seminars/docs/SRAS_Overview.pdf