SECURITY FOR MULTIMEDIA SPACE DATA DISTRIBUTION OVER THE INTERNET

Thom Stone [†] and Lou Picinich [††]

NASA Ames Research Center
MS 244-19
Moffett Field, CA 94087, USA
FAX: 415-604-0673, [†] E-mail: tstone@mail.arc.nasa.gov
[††] E-mail: lpicinich@mail.arc.nasa.gov

ABSTRACT

Distribution of interactive multimedia to remote investigators will be required for high quality science on the International Space Station (ISS). The Internet with the World Wide Web (WWW) and the JAVA environment are a good match for distribution of data, video and voice to remote science centers. Utilizing the "open" Internet in a secure manner is the major hurdle in making use of this cost effective, off-the-shelf, universal resource.

This paper examines the major security threats to an Internet distribution system for payload data and the mitigation of these threats. A proposed security environment for the Space Station Biological Research Facility (SSBRP) is presented with a short description of the tools that have been implemented or planned. Formulating and implementing a security policy, firewalls, host hardware and software security are also discussed in this paper.

Security is a vast topic and this paper can only give an overview of important issues. The paper postulates that a structured approach is required and stresses that security must be built into a network from the start. Ignoring security issues or putting them off until late in the development cycle can be disastrous.

INTRODUCTION

The Internet is ubiquitous, feature rich, cost effective, and ever evolving to take advantage of new technological paradigms. The openness that allows all of these technological riches also creates possibilities for security problems of cosmological proportions. One only has to read the popular press to hear of some breach that caused major problems for a prominent institution. Even a benign breach of a network can cause major outages while systems are cleansed of security holes, and the veracity of any science data residing on a despoiled computer could be considered suspect. Costs of building ones' own secure science distribution network for a project of such diversity and time duration as a Space Station Payload makes the Internet the only practical method to perform science in the 21st Century. It is the purpose of this paper to explore the methodology to use the power of the Internet while providing a secure infrastructure for managing a payload on a manned space vehicle.

SSBRP includes major elements on the ISS consisting of multiple habitat holding racks, a glovebox, and centrifuge. The User Operations Facility (UOF) will be at Ames Research Center (ARC) where the payload will be controlled and monitored, and data will be stored and distributed to remote science workers. Science will require that Investigators at distant institutions be able to communicate with the UOF and receive both near real-time and stored data. Data will include multiple video streams, audio, as well as real-time and stored data in many formats. Video conferences between the Principle Investigator (PI) and the UOF must be supported. There is also a requirement to distribute project information (which could include real data and video) to the general public via the World Wide Web (WWW). In addition the UOF will be required to access the public Internet to get NASA ISS data and for vendor information.

The Communication and Data System (CDS) team is responsible for development of the ground systems including operations and data distribution. CDS team has chosen a Web / JAVA paradigm to operate the payload and distribute science data. The Internet (or the new high speed research Internet now being built) will provide the transport media for remote communications. JAVA provides for platform independent software development and deployment, and, the ability to change and add software with minimal user interaction.

PART 1 - SECURITY PLANNING AND SSBRP

Security has been a concern since CDS was first specified. It was realized that security must be an integral part of a system and cannot be added later as an afterthought. Recently SSBRP network security planning was formalized with the production of several documents starting with a Security White Paper. This SpaceOps 98 paper is derived from these documents and the process used to develop them. Part 1 of this paper will describe the process of developing a path to a secure multimedia network, and part 2 will describe actual security measures considered.

There is an interminable war simmering between an array of people ready to compromise computer resources for one purpose or another and those that need to protect them. The threat is not limited to those systems connected to the Internet, although this point of entry is the most visible in the public eye. So called isolated, non standard systems are even more vulnerable than standard systems since current countermeasures have concentrated on the Internet Protocol (IP) world.

Contrary to claims made in the trade press advertisements, there is no single device to secure and IP network. Firewalls, encryption devices and software all play a part in keeping a network functioning, but provide total security in an increasingly dangerous cyberworld. Security must be viewed as an ongoing process and the treats that besiege a network must be dealt with in a structured and methodical manner.

WHY A PLAN?

The development of a comprehensive security plan is basic to protecting information systems of any kind. The main purposes of preparing formal security analysis documents are:

- Educate the project to the risks.
- Formalize a plan to counter the threats.
- Apprise management of the risks and costs that will be required. [Management buy-in is a necessity if security planning is to succeed]

THE STEPS TO DEVELOPING A SECURITY PLAN

The first necessity in developing a security plan is an understanding of the underlying system and it's interfaces. Data requirements, including bandwidth and protocols must be documented and understood. The CDS team established, for all external network connections, the data protocols required, estimated the volume of data expected, and examined other critical factors that influence security. Internal connectivity needs were also charted to insure that holes in the system do not propagate throughout the Intranet.

The next item that must be produced is list of the goals for the security plan. Security goals should be high level and express the scope of the security task. Table 1 contains the list developed for CDS.

TABLE 1: CDS HIGH LEVEL SECURITY GOALS

SSBRP SECURITY GOAL	COMMENTS
Protect ISS Core from harm	Although the primary responsibility for this rests with Core operations, SSBRP must take an active part in protecting the Station.
Protect SSBRP onboard hardware/systems	A minor breach could jeopardize the science program.
Protect ground hardware/software	Includes physical as well as software protection providing acceptable availability
Protect sensitive data from unauthorized access	Some life science data are proprietary or restricted.
Protect access to auxiliary ISS/NASA systems	Payload planning system, payload data library etc.
Meet or exceed all NASA security requirements	NASA Policy.

Next there is a more daunting task: a risk assessment must be undertaken. This should be definitive since all security planning will be derived from the risks documented. The CDS team found that some of the risks were generic to any critical, high profile, system with interface to the open Internet but that there were some threats that were particular to the CDS environment. Here is an abridged list of the risks:

- Physical security issues.
- Exporting encrypted or sensitive data or computer programs to foreign locations.
- Unauthorized Commands.
- Protecting data while being transmitted on the Internet.
- Unauthorized access to the Intranet (a very large issue).
- Protecting proprietary science data for Principal Investigators.
- Denial of service attacks.
- Utilizing Internet and WWW services without compromising the mission.
- Outside tampering with SSBRP public home page.

As in any computer security analysis a complete threat matrix should be devised.

FORMAL POLICY DOCUMENT

CDS team members decided that the vehicle for the security planning document would be a detailed security management policy statement. Most security policy documents are terse, very high level without technical detail, and as general as possible. The CDS team has chosen to take an opposite position. Managers and other parts of the CDS team will regularly perform critical analysis of requirements documents. Formal NASA requirements insure that there will be someone who is responsible to see that that the requirement is met thought out the lifecycle of the project and that there will be traceability of the tasks involved. The SSBRP Network Security Policy was written in the manner of a requirements document with great detail, using "shalls" for those policies that will dictate the security of the payload.

LOGICAL STRUCTURE OF THE POLICY DOCUMENT

The document was divided into sections. Each section covers one of the major network security risks. Four topics were presented pertaining to each risk.

- Policy Statements
- Security Risk

- Technical Mitigation
- Security Overhead

First, each section began with a list of policies that related to that threat (risk).

Some examples of policy statements:

> *"All SSBRP systems shall meet or exceed all security standards from ISS, NISN, NASA HQ and NASA ARC. CDS shall maintain adequate staffing to ensure that these standards are implemented and enforced throughout the mission. Periodic reviews shall be scheduled to test compliance."*
>
> *"CDS shall support UNIX system administration at a level such that security features can be properly maintained."*
>
> *"CDS support staff shall maintain a close relationship with the ARC security group, and NASA Automated Systems Incident Response Capability (NASIRC) teams, and the Computer Emergency Response Team (CERT)."*
>
> *"One time passwords shall be used to access to all hosts within the core network."*

The SSBRP Security Policy has too many policy statements to list here and some are very specific to our payload. Each is directly associated with a documented risk and most can be tested to insure compliance.

Second, the policy section is followed by a detailed statement of the risk and the ramification of the threat. For example:

> *"The SSBRP system is subject to a flood attack. A single user or group of users can deny services from our system by sending requests, even invalid requests, at such a high rate as to keep valid requests from being processed. This could shut down critical experiments on station."*

Third, a discussion of technical mitigation is given. This section contains possible counters to the threats and is very detailed. Specific hardware and software options are presented. Since security has been incorporated in the CDS design process many of the items have already been accomplished or planned. An example of the type of material presented in this section:

> *"CDS will close services such as PING and FINGER to limit the impact of the requests. The filters in the Firewall will also limit the impact of request from unauthorized IP addresses. Firewalls can limit the impact of these attacks but this in turn takes resources from the Firewall. Crudely the CDS operations staff will have to be able to shut access off from parts of the Internet where the attacks are originating. This will have to be done at the BGP (Border Gateway Protocol) or router port level at the ISP of choice. The problem could be mitigated with a request "director", hardware that distributes WWW requests across servers. Since these devices handle only requests, they are fast enough to reject messages and distribute valid requests across a range of servers."*

Protecting against unauthorized access is a most important topic and is treated with much depth in the SSBRP Security Plan. There are separate sections outlining the four steps to mitigation:

- Prevention
- Detecting when the network is compromised and reporting the incident
- Limiting the damage
- Recovery

Fourth, the overhead that will be required to mitigate each threat is outlined. These overhead items include non-tangible things such as the hassle of entering and remembering passwords or operators not being able to surf the WWW while on shift. The SSBRP Security Policy Document produced did not include actual dollar cost at this point but these will be accounted for during the next (detailed security design) phase. An example of overhead that security will levy:

> *"Minimum approach will require a second Firewall which will need to be configured and maintained."*

The Security document will need to have a thorough review by management and the technical staff (the reason it should be structured like a requirement document). After all comments have been assimilated and presentations have been given and the management signs the document, a formal network design (with costs) can be produced. This should be trivial after the technical analysis phase of the policy document.

PART 2 - SECURING THE NETWORK

The process above resulted in proposing concrete steps to be taken to protect the network. These steps addressed all of the threats documented and can be justified by being tied directly to a documented security risk. The overhead involved in the security effort is also defined so the project management knows what the security is costing.

The most important security efforts are non "mechanical". No amount of technology thrown at the security effort will be effective if the following is not done:

- Document the requirements and the network.
- Document procedures for dealing with security problems.
- Build security awareness on the part of the staff and the remote users.
- Have good systems administrative support.
- Perform backups regularly and track and install security patches from vendors as quickly as possible. The network is only as secure as the weakest system.
- "Harden" computers against intrusion. Tune the system software to provide maximum security,
- Turn off network services that are not required.
- Turn on and monitor logs and other system information regularly.
- Team with the local security organization. Get on the list for security alerts.
- Keep the public access Web pages outside of the firewall and away from the production network. Data should be moved from the live system to the public system using a secure method.

TECHNICAL SOLUTIONS

On the technical level SSBRP Security Plan calls for a system of "walls" against the various security threats. Space does not allow for a discussion of all of the technical solutions CDS intends to deploy. It would also not be discreet to publish too much detail.

Two attributes of multimedia complicate the security solution, high bandwidth demand and the fact that realtime data and video distribution use protocols which do not acknowledge bad data. The volume of data involved makes mitigation through encryption, and packet inspections more problematic.

The following are some solutions that deserve general consideration:

- Smart card deployment for one time passwords.
- Using non-routing addressing on Intranets.
- Router level security (IP filters, protocol masking)
- Firewalls: devices for filtering traffic to insure packets actually come from authorized users doing valid work.
- Connectivity to the Internet though bastion hosts with two network ports to limit interfaces with the outside world.

- Encryption devices to code sensitive data so that it can not be intercepted (read or changed) on the open Internet.

PASSWORDS

The old adage is that if users are forced to choose passwords that are "unguessable" they will have them pasted up in big letters on their monitor. All the "biometric" identification systems and password encryptors have a gaping hole as they can be "sniffed" (recorded off of the network) and played back to gain illicit entry. Single use passwords are one of the best and least expensive ways to protect a network. Usually a "smart" card is issued to users. The smart card generates and displays a new number every minute. A task running on a server uses the same algorithm to generate the same number. The user is asked to enter the number which is matched against the algorithm generated number (each user gets a different sequence). Once a number is used it can not be reused. This guarantees that only the person holding the card can get into the computer using a specific usercode. To implement these "smart cards" a server must be set up, and card distribution and control must be undertaken. This can be a daunting task if there are many far flung users, however, a single card can be used to log on to many resources. Every resource on a network including routers and smart hubs should be protected with one time password cards.

INTRANET

One way to keep outsiders from being able to probe production networks or pass rogue packets onto the LAN is to build an "Intranet" using RFC 1918 addresses. These are IP addresses that have been designated as "not routeable" over the wide area. Routers will not pass these addresses to the next hop router except within the local area. Packets from the outside will not get to hosts on the Intranet except to hosts with two IP addresses, real addresses and RFC 1918 addresses. Sites should avoid selecting random Intranet addresses with the hope that they will not be guessed. Chances are that they will be guessed and be used to break into the systems on the Intranet

ACCESS CONTROL

Router filters, bastion hosts (AKA Proxy servers), and firewalls are all embodiments of access control (determining who gets to communicate with your systems to do what). This type of security is transparent to valid users since it operates at the Packet level and only comes into play when someone who is not a valid user sends packets or a valid user requests a service they are not authorized to use. These three means of access control are not exclusive of one another. They can and should be used together to create a series of "walls" so that if one is mis-configured, or breached by hackers, via some unplanned weakness, the others will continue to protect. This may also slow penetration into the "core" giving time to discover the breach or creating enough hassle for the intruder to give up. The following is a description of the three and some caveats for each.

ROUTER FILTERS

Routers are the first device packets hit when they come from the Internet, and therefore are a logical choice of where to filter out unwanted traffic before it gets too far into an Intranet. Filters would be used to limit which services and protocols are allowed to be forwarded. Router filters are configured/programmed into the running code on a router.

ROUTER FILTER CONCERNS

Mistyped or badly constructed router filters can bring down an entire network or cause strange network problems. They can also slow network responses considerably.

Filters take processor time away from routing functions on busy networks. More involved filters that go further down in the protocol stack cause even more overhead and can bring network response time to unacceptable levels.

Simple router filters deal with one packet at a time and can not keep information about related streams of packets. State driven access control based on complex sequences of IP data can not be implemented with simple router filters.

After router filters are configured, most router filters can still be defeated by "spoofing". Address spoofing is substituting an approved address for an non approved actual address.

Router filters can also be inadvertently disabled when routers are reconfigured for any number of unrelated reasons.

BASTION HOSTS / PROXY SERVERS

These are applications that sit on hosts that are dual attached to the Intranet and to the Internet (or firewall). When a user in the local net wants to use a service to the outside they must first access to the bastion host. Sometimes applications use the software on a bastion host without the user being aware of where the software is actually running. This is also called a proxy server. Bastion hosts or proxy servers keep unwanted visitors from accessing most of the network and allow concentration of security measures onto a small group of hosts. In case of a serious attack the bastion host can be bought down while the rest of the network continues to operate.

PROXY CONCERNS

- Proxy servers can become a serious bottleneck in providing network services.
- Proxy servers do not always provide services as well as those running on the original systems. Functionality can be limited.
- These servers can create a false sense of security so hardening other hosts on the Intranet may be neglected.

FIREWALLS

Firewalls are becoming a standard feature for networks with Internet attachments and with good reason. Firewalls include several security features:

- Packet discrimination. This is usually of finer grain then can be obtained via router filters. A firewall can use state table driven intelligence to control IP conversations. This is known as stateful inspections.
- Event logging is an important and usually overlooked features of firewalls. One can find both successful and unsuccessful penetration attempts on the system from the advanced logs available on most commercial firewalls.
- Address translation (proxy service) is where a firewall translates incoming IP numbers to the non routeable Intranet addresses. This can prevent malefactors from gaining information about your network and insuring that "stray" packets do not reach a host that must be protected.
- Password checking.
- Some firewalls perform encryption services.
- Provide vendor support and upgrades to meet ever evolving network threats.

FIREWALL CONCERNS

- Firewalls are complex computers. They do not come with a switch saying "Hacker", "No Hacker". Configuration takes expertise and experience.

- Firewalls must be based on very concrete policies to determine what may be done on the network. These policies can be difficult to determine and implement. These technical policies should be derived from the management policy document.
- Firewalls add one more layer of complexity, one more single point of failure, and one more point of overhead to slow the responsiveness of the network.
- Firewalls need to have frequent software releases to be able to handle newly discovered threats, and to handle new network services such as multicast and streaming video.

ENCRYPTION

Encryption passes data through an algorithm with a specific key. The data become unintelligible to anyone intercepting it. The valid reader passes the data through the same algorithm using the same (or a compatible) key to reconstitute the data. The main issues with encryption is the processing required to "code" and "uncode" the data stream and the distribution and control of keys. It is not secure to have the same key for all outside users (If one system is compromised they all are) and other key distribution systems such as "private key" / "public key", key servers, and certificate servers are complex. While not the security panacea some claim, encryption is an important tool in protecting sensitive data. SSBRP plans to encrypt some sensitive data and video as well as Internet voice. Passwords should always be encrypted as well as sensitive mail that could contain planning and schedule information. Multimedia data, because of the volume must be encrypted in hardware. Encryption protects data from being intercepted or changed while it travels on the public network. It also protects from "spoofing" or password stealing.

ENCRYPTION CONCERNS

- High rate multimedia data will require hardware encryption yet another possible single point of failure.
- Key distribution requires much effort.
- Encryption makes trouble shooting communications problems difficult.
- Sending encrypted data to foreign locations is subject to US export controls and the laws of other nations.
- Does not protect against "denial of service" attacks.
- Does not protect entry from unencrypted links (dial up, console port etc.).
- Does not protect entry due to weakness in system software such as Sendmail weaknesses or Operating System holes.
- If partner systems are violated encryption no longer protects the data.
- Multicast data presents unique encryption key distribution problems that have yet to be solved.

CONCLUSION

Security of networks attached to the Internet is not trivial, but the consequence of ignoring this issue is catastrophic. Critical, high data rate multimedia applications such as Space Station payloads are a special challenge.

Good planning, analysis, and design however, can produce a shield adequate for protecting a Space project if started early enough in the life cycle. The four work horses of security: Prevention, Detection / reporting, limiting the damage, and recovery are the key. Producing a risk analysis, management policy document and a detailed security plan is essential.

There are many tools to protect IP networks. Some of them are very effective when used correctly. The challenge is to find which tools will meet the security criteria of a particular network.