SECURE PAYLOAD ACCESS TO THE INTERNATIONAL SPACE STATION

Author:
R. Lee Pitts
E-mail: lee.pitts@msfc.nasa.gov

Technical Contributor:
Chris Reid
E-mail: chris.reid@msfc.nasa.gov

Lockheed Martin Space Operations
Utilization and Mission Support

Marshall Space Flight Center

SECURE PAYLOAD ACCESS TO THE INTERNATIONAL SPACE STATION

Abstract

The ISS finally reached an operational state and exists for local and remote users. Onboard payload systems are managed by the Huntsville Operations Support Center (HOSC). Users access HOSC systems by internet protocols in support of daily operations, preflight simulation, and test. In support of this diverse user community, a modern security architecture has been implemented. The architecture has evolved over time from an isolated but open system to a system which supports local and remote access to the ISS over broad geographic regions. This has been accomplished through the use of an evolved security strategy, PKI, and custom design.

Through this paper, descriptions of the migration process and the lessons learned are presented. This will include product decision criteria, rationale, and the use of commodity products in the end architecture. This paper will also stress the need for interoperability of various products and the effects of seemingly insignificant details.

SECURE PAYLOAD ACCESS TO THE INTERNATIONAL SPACE STATION

HOSC Early Security Architecture

From the early 1980's until the mid 1990's, the Huntsville Operations Support Center (HOSC) was essentially a standalone telemetry and command system. The HOSC supported a myriad of users including Shuttle Main Engine Group (STS SSME), ET, and Solid Rocket Booster (SRB) Real-time Engineering analysis teams, Hubble Space Telescope (HST) Orbital Verification, and Spacelab Payload Operations.

The security model for that period was dictated by several factors, but foremost was the limitations of existing network technologies. The Spacelab missions that the HOSC supported carried on many types of onboard experiments developed by teams across the country and with our partners from European Space Agency (ESA) and National Space Development Agency (NASDA). One of the major drawbacks at that time was that in order for the various experimenters, known as Principal Investigators (PI), to process real-time telemetry and ground command to their experiment, it was necessary for the PI teams to be physically located at our facility. There were several factors that led to this mode of operations. Security mechanisms in the early 1980's were leveraged on the existing technologies of the day. The HOSC was a shared media network composed mainly of 10 MB and 100 MB Ethernet and later limited Fiber Distributed Data Interface (FDDI) controlled by primarily routers and bridges. High long line circuit costs coupled with the inability to secure the data and provide a two way interface dictated that the majority of PI teams would have to bring all their Ground Support Equipment to the HOSC and connect to our networks while their Payload was in orbit. This model, while effectively controlling the user community's physical as well as network access, carried with it a high cost to the remote user teams who had to reallocate to our facility, and also limited them in what and how much equipment could be brought to support their on-orbit operations.

The HOSC internal network was divided into several different LANs with names derived from the domain we intended on protecting; STS, DEV/VAL, SOA, PLD, and MSS. The goal was to isolate and control the flow of telemetry and command data from the user's workstation to our central processing and commanding subsystems during real-time operations while being able to simultaneously support software development and verification activities, user product development, and impending Space Shuttle activities. This was accomplished by isolating the traffic on LAN segments using existing bridging and routing technology coupled with a schema for assigning addresses controlled by the Operational Support Team (OST). The HOSC software developed at that time was used to support telemetry and command processing using a different security model. Data support from a user workstation was only initiated by the central processing and commanding systems after ensuring the end user workstation was an approved member of the support. This was based on a predefined list that was stored on the central processor. The end user workstation had to establish this two-way communication verification loop before any data or commanding could be accomplished.

User workstations not defined in the support list were denied any services. Security for the PI teams who brought their own unique data processing equipment was accomplished by only allowing one way traffic through RS-232 and RS-422 serial connections controlled by a data distribution system. The OST controlled all user interfaces. Commanding in the facility could only be initiated through a HOSC provided workstation with the proper user identification and workstation authorization. No interfaces were provided so that a PI team could connect to our network and potentially command to an on-board experiment.

Secure Payload Operational Security Model

Characteristic users

Today the HOSC is continuing to evolve after going operational in support of the ISS. Access is restricted, allowed, and defined by security layers, both physical and logical. These layers can be viewed as moats or regimens around the HOSC services. As stated earlier, HOSC provided services are exclusively IP based (minus video). Additionally, nearly all sources of data (minus voice and video) are provided over IP networks.

The HOSC user base is quite diverse; geographically, technically, and culturally. As might be imagined, it is composed of highly educated individuals in a large number of scientific disciplines. With **Increment 5** as shown in figure 1, three TeleScience Centers (TSC) and seven independent Payload Investigators (PI) as well as the Russian Space Agency (RSA) are supporting science on the ISS. Except for the RSA, all are within the confines of North America. These include experiments in materials science, power, propulsion, combustion, fluid physics, plasma physics, human life sciences, space product development, and education. Each experimenter is using one to many of the services provided by the Payload Operations Integration Center (POIC) at the HOSC.

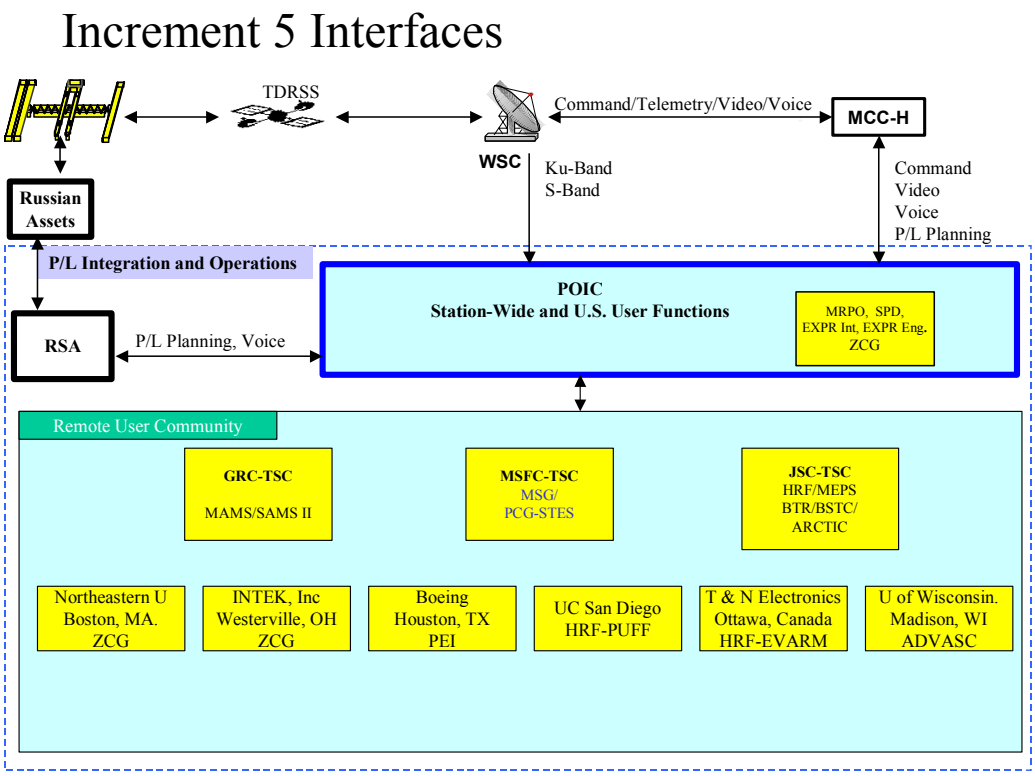

Figure 1 - Increment 5 Interfaces

Extensive interfaces are being defined with users worldwide including ESA, NASDA, Russian Space Agency (RSA), and Agenzia Spaziale Italiana (ASI). When these and other International Partners (IP) are fully utilized, the ISS will encompass work and components from sixteen countries across five continents.

Security model concept of operations

A model was established to enable users to gain access to POIC services. This model is based on five (5) regimens as shown in figure 2. These regimens provided for a layered approach to not only managing security but to managing access. Response can be dictated by the threat in relation to the regimen. The response can be choreographed accordingly and evaluated independently. These five regimens are maintained locally and remotely. Local maintenance at the HOSC ensures the protection and security of POIC services. Remote maintenance of the security model is partially in the control of the POIC and partially in the control of the remote facility. Following are discussions of each regimen and salient features of each. A complete discussion of each regimen will not be covered as they will be unique to each situation.

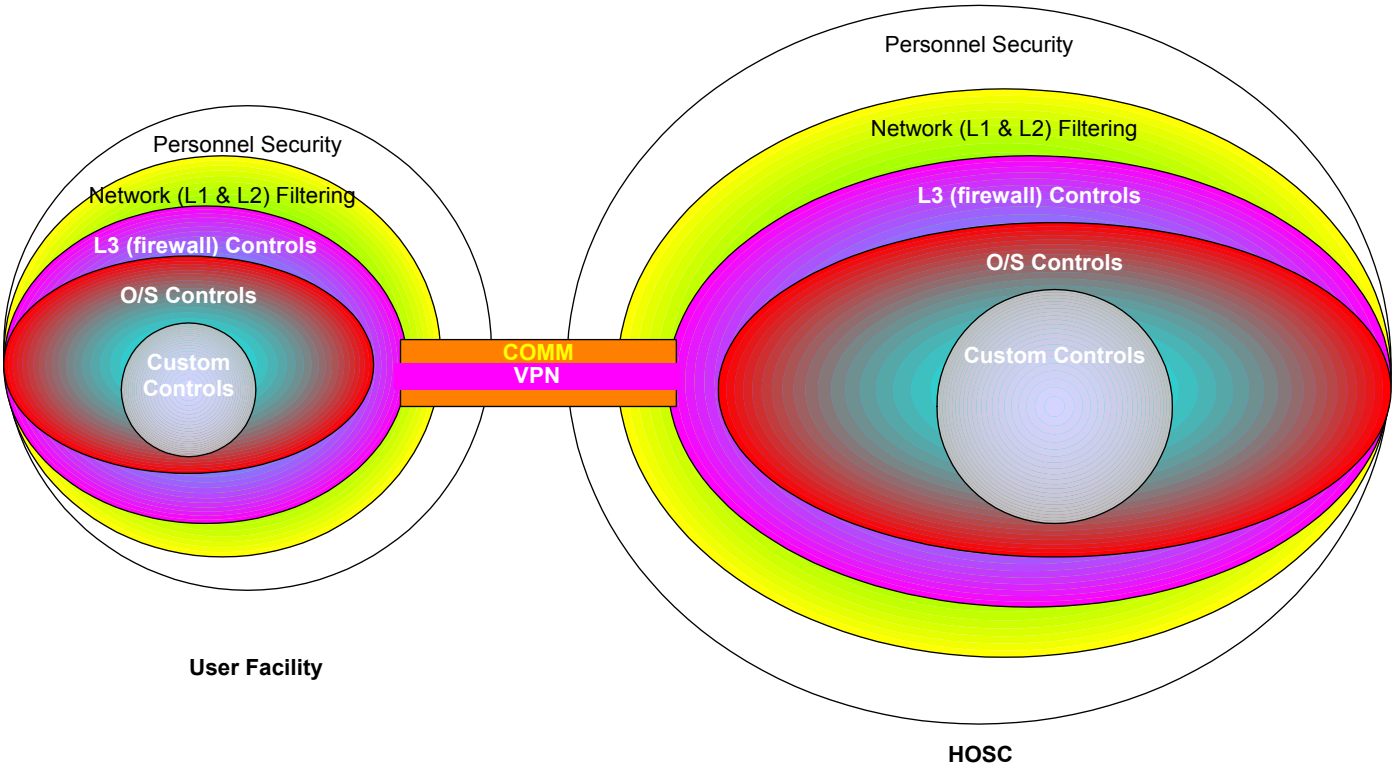

Figure 2 - HOSC Security Model

Regimen 1. The outer and perhaps most basic layer is the personnel security regimen shown in figure 2. This includes physical security as well as personnel screening. Under this regimen is the very real threat of ***Social Engineering.*** Most threats in this area are the most obvious and most commonly lead to compromise.

The actual physical facility should provide access to only those with the knowledge and need for access. The core components need to be locked up. It is preferable that this be accomplished with a keycard or other access method allowing authorized users easy access but prohibiting others. The computer center should not be a pass-thru area where people are granted access for convenience. Non-essential services should be kept out. All system consoles should be protected as well. Access points should not be left unsecure.

Personnel screening is an area which has become more and more acceptable. When working at or with a government facility, screening is mandatory. For the POIC and the ISS program all users

must have a minimal level of screening subject to capability access to be granted. This is required locally and remotely of all users without regard to citizenship; the assumption of risk is ever present. As a result, the Computer Security Office reserves the right to audit any facility or deny access to any user.

For the POIC, all users have a vested interest in the project. Most of the payload investigators have their reputations, large quantities of money, and time invested in their experiments. No one wants to compromise security and risk everything. Most lapses are the result of expediency or implied risks to experiments.

Finally, a moment on "social engineering". This threat is possibly the most pernicious. Often people are induced to compromise themselves and do it for the most noble of reasons: helping someone out! There are a number of definitions which are thrown around but The Jargon Dictionary sums it up admirably.

"Term used among crackers and samurai for cracking techniques that rely on weaknesses in the wetware rather than software. The aim is to trick people into revealing passwords or other information that compromises a target systems security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or an employee with an urgent access problem"

Unknown Author. " Social Engineering". The Jargon Dictionary

There are many scams using guile or persuasion to pry information from users or systems managers. Local HOSC users make up a relatively small percentage of the total users. The largest percentage of users is remote, and that percentage is growing with each increment. This is made worse by constantly rotating shifts which have different schedules at each facility. Continually we receive requests by "supposed users" from various facilities (including the HOSC) for help in accessing computer resources. Therefore, to verify the validity of a request, the requestor must provide a passcode to identify the user uniquely. Records are consulted and the level of proper access is ascertained before special privileges are allowed, password reset, or access to an alternate asset is allowed. ***No exceptions are permitted!***

Once established, one of the best means of maintaining the personnel security regimen is through education or training based on a well defined security policy. This has to apply to everyone; managers, operators, and "*important users*". It should include specific responsibilities relating to physical security, limiting revealing data, and procedure awareness. General responsibilities should include a threats assessment and making the user aware of the impact of data leakage.

Regimen 2. The second basic layer is network security, particularly Open Systems Interconnection (OSI) layer 1 and 2 filtering of figure 2. As stated earlier, the HOSC was a traditional shared media network composed of FDDI and ether technology. The routing was accomplished via Cisco multiport routers at layer 3, with various gateways provided between public, common, and private networks. As initially conceived, this was a shared media network.

As technology moved forward, so did the HOSC. Shared media has been bridged to switched IP and as hardware becomes obsolete, shared media is being completely supplanted by switched devices at lower cost. An added benefit of IP switching is enhanced security on the networks by eliminating opportunities for promiscuous access.

Since these switches are layer 2 devices, they build an Address Resolution Protocol (ARP) table of the Media Access Control (MAC) addresses and the physical ports those MAC addresses are being received on. For efficiency and speed, packets are forwarded to the addresses in the ARP table. The number of packet collisions vanishes for these resolved transactions. Broadcast and yet-to-be-resolved addresses can still collide. The security benefit of the switch is that it is not a shared media device and it only receives data on a port that is destined for that port. Within the HOSC security domain, a rogue sniffer is no longer able to capture traffic not specifically destined for them. All the boundary devices of Figure 3 are IP switches. The IP switch interface with public networks is the demarcation point between external systems and the HOSC controlled resources. An IP switch protects access to the firewall and common use items such as web and DNS servers. Past the firewall, an IP switch is utilized as the mission systems networks backbone. Layer 2 switches are also being used to replace all hubs on the "Common" and "Mission Systems" networks.

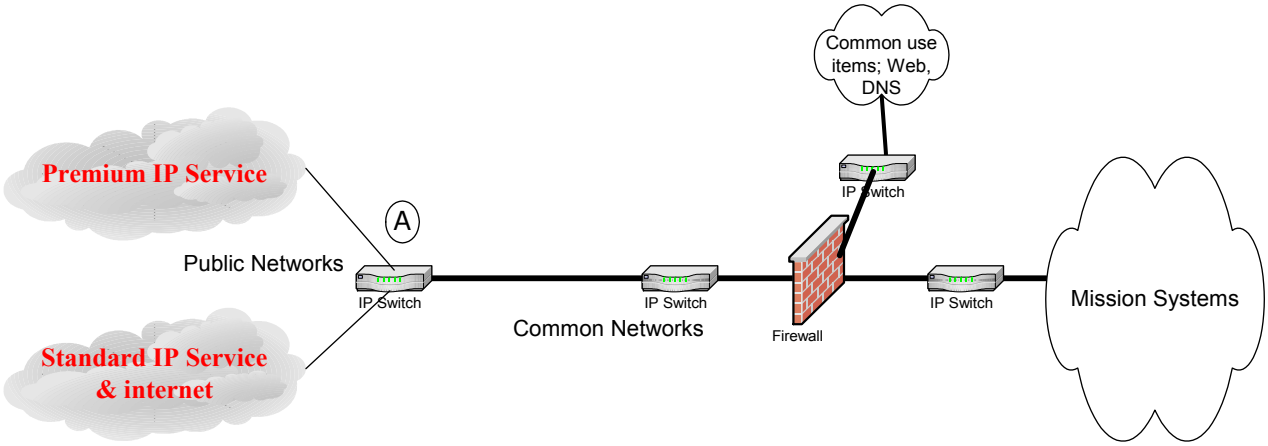

Figure 3 – Network Layout

Additionally, since each of the switches in figure 3 support routed protocols, extraneous protocols are not allowed in. Each protocol must be specifically identified for a service. One final note on the switched network which applies to all core services: this is not an area to cut corners. The use of high quality equipment and expertise is essential, but so is reliable and responsive support. These services should be maintained with updates and patches applied as they are identified. If the vendor does not provide adequate levels of support, drop them and find one that does.

3. The third layer of support is at the firewall as shown in figure 2. This regimen is where a high degree of affinity with the remote user must exist; common Reguest For Comments (RFCs), ISS protocols, and standards must be observerd. The HOSC is a facility with a diverse set of services for its users, both remote and local. When selecting the firewall and supporting products, it is important to decide on products which supports your security model, are widely available (to include exportable capabilities), has exceptional support, continues to evolve, and can be managed on a day-to-day basis by onsite personnel. Following are some examples of these axioms.

As the HOSC went from an isolated to international facility, the firewall we originally selected had some serious drawbacks. First, it primarily acted as an IP filter and only operated through the

use of Network Address Translation (NAT). This constrained our applications for remote users and made each configuration for operations, simulation, and test unique. What we needed was a firewall which allowed a peek only at those systems designated for remote use. Also, the firewall needed to support packet filtering based on the state of the previous packet, e.g. stateful inspection. Second, we looked for support that was complete, reliable, and timely. Unfortunately, our first firewall was the victim of the TELCO wars. As such, the firewall company was swallowed up and support was curtailed soon thereafter. Third, many groups follow our lead when selecting products and must follow our lead on standards. We had selected a firewall which represented a sunset solution. Our secure communications solution was based on two standards; Secure Socket Layer v3 (SSL) and Secure Shell (SSH). This required at least three (3) products so we looked for an integrated product that supported widely available standards. Fourth, our users and our requirements are constantly evolving and our facility is constantly requested to accommodate new users and endeavors. Since we are international in scope, we expect to be a target and require expeditious and reliable support. Finally, our support personnel must manage our firewall on a daily basis. In the current budgetary environment this doesn't mean cut corners, quite the opposite. The user interface for configuration and management must be lucid with adequate training to support.

Based on these five discussion points, it was decided to procure an integrated firewall and Virtual Private Network (VPN) solution. This solution relies on an IPSec 1.0b compliant VPN to encapsulate TCP traffic. This includes approximately two dozen services. The service types include http, https, ftp, x-windows, and SQLNet. Also included are ISS unique protocols for ISS data delivery. What is not included in the VPN traffic are UDP services to include multi-cast and DNS. Figure 4 below defines the types of user who may access the HOSC under this regimen.

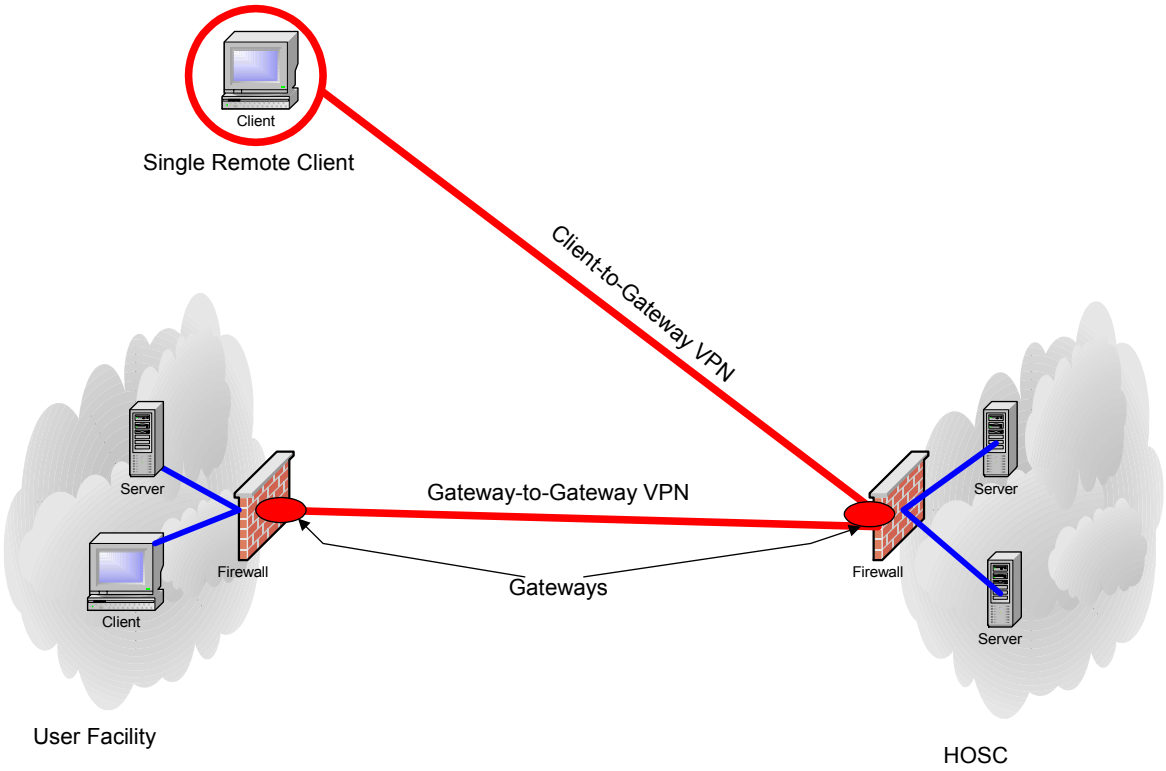

Figure 4 – User VPN Access

For the remote user or facility, two access methods are supported. First an individual user can access the HOSC services as a VPN client of the HOSC VPN gateway. The VPN client is a no cost option but must be downloaded from the HOSC VPN gateway vendor. The second option allows systems behind an IPSec 1.0b compliant VPN gateway to access the HOSC VPN gateway.

As stated earlier in regards to the network filtering regimen, this is not an area to cut corners. The use of high quality products which are supported by reliable and responsive vendors is a must. These services should be maintained with updates and patches applied as they are identified. If a vendor does not provide adequate levels of support, drop them and find somebody else.

4. The Operating system (O/S) represents the fourth regimen of figure 2 which supports the HOSC security model. The HOSC is composed of heterogeneous computing platforms even though we have worked to limit the diversity. Currently the HOSC platform suite includes six platforms with various versions or operating systems on each platform type. The number of platform types at the HOSC is primarily dependent on the number of entities using HOSC facilities. However this is a continuous resource drain and security crisis keeping all systems at an appropriate O/S level, acerbated by being in 24x7 operations. Therefore we are proceeding down the path of developing images of the most numerous systems based on application version level, COTS version, O/S release, and current security alerts.

These images must follow the normal rules of an O/S to be deployed. The use of these images ensures that everyone's "lessons learned" are applied evenly and thoroughly. For instance, turn off services that are not used. Get rid of default accounts, install the same COTS on all platforms, install all applicable security and O/S patches, test the image prior to deployment, and don't put anything outside your firewall you are not willing to lose.

5. The fifth and final regimen as shown in figure 2 is the custom controls regimen that each site develops to meet its own needs. Generally these are unique to each site or type of installation and may have heavy architectural overtones, but one thing is usually common. The custom controls are usually designed to protect the core mission critical systems.

The HOSC is no different. To protect the HOSC users and the core systems, a three-tier architecture has been developed. Figure 5 details the tiers of client systems, interface servers, and application servers. Each tier fills a unique role.

Client systems can be found internally or remote to the HOSC. External systems must have communications by VPN and be isolated from promiscuous access. Internal clients are located on switched networks and are rigorously managed. A client may host web, x-server, or native applications which provide a complete ground system solution for ISS payload users. Users are allowed access to the second-tier systems but are not allowed on the third tier.

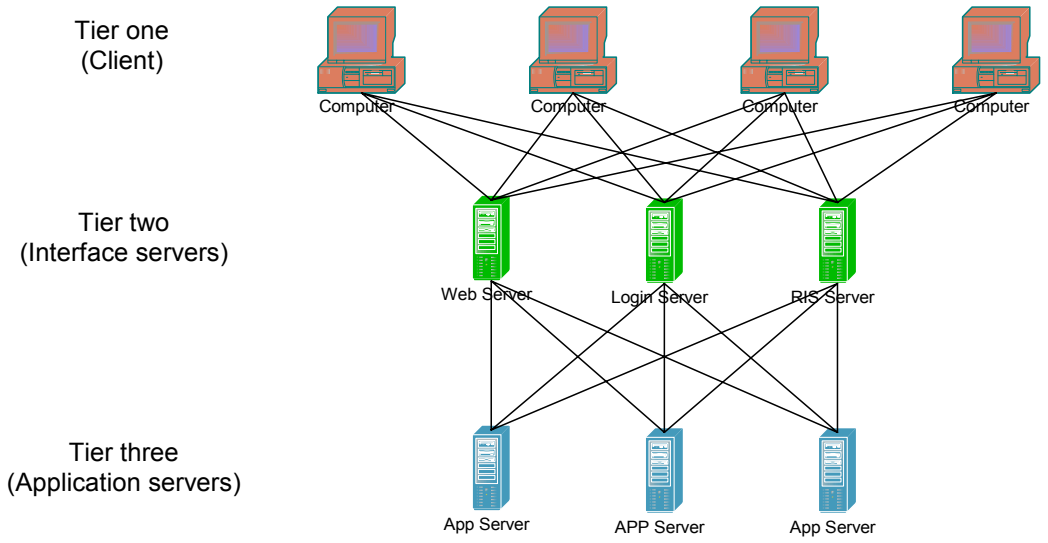

Figure 5 – Three-Tier Architecture

Interface servers are composed of three types. Web servers provide payload service to local and remote users. These servers are outside of the mission systems networks but behind one side of a mutli-sided firewall. The web servers are viewed as sacrificial and no persistent data are stored on them. Additionally, client passwords and privileges are stored on mission systems and request for access is relayed to the mission systems application servers. Web users are restricted to web servers based on the users' IP address, either internal or external. The second type of interface server is the Gateway or Login server. These servers act as the gateways of the clients for non-web based services which require user authentication and privacy. These platforms provide processed data or X-client services to authenticated clients. Like web servers, gateway servers are viewed as sacrificial and no persistent data are stored on them. Gateway users are restricted based on the users' IP address, either internal or external. The final interface server type is the Remote Interface System (RIS) server. This server provides data to multiple remote users with the requesting remote user authenticated. Like web servers, RIS servers are viewed as sacrificial and no persistent data are stored on them.

The application servers are mission critical devices. They encompass a broad range of services to include ISS drop boxes, telemetry archive, project database, telemetry and science data distribution, long and short term plan activities, exception monitoring, and an advanced information management system. These systems are considered inviolate and protected at all cost, not only for the data they manage but for the interfaces they manage.

Throughout this system a number of checks have been implemented to insure that a user is valid and authorized for a privilege or service. Users and their privileges are created through the normal account process. This is where each user is characterized and a profile is built. Whenever a user requests a service, the request is compared to this profile. The request can be from a device local to the HOSC or remote. Most requests are generated by HOSC created clients. However if any software client is modified maliciously to request an unauthorized privilege, the request will be denied when the profile is interrogated. From database to digital certificates to password authentication, the HOSC validates each user's level of access and purpose to ensure that each user receives every service required to support operations aboard the ISS.

Evaluating HOSC systems for malicious action is pervasive and includes many areas. Custom controls also include the incorporation of COTS products into the HOSC environment. This includes virus scans and other proactive defense measures at multiple tiers within the HOSC architecture. Quite often these defenses overlap to prevent singularities in products from compromising operations.

Summary

Payload operations at the HOSC originally were executed in an isolated environment with Payload Investigators onsite. For the ISS, payload operations are conducted remotely across wide area networks which will shortly include international participation. To support this level of access, a new security model was implemented.

The HOSC security model is based on five (5) hierarchal regimens. This security model supports remote user access to the International Space Station's hosted experiments by the United States and International scientific community. The security model is hierarchically implemented:

Regimen 1:	Personnel security
Regimen 2:	Network security
Regimen 3:	Level 3 Firewall security
Regimen 4:	Operating System controls
Regimen 5:	Custom controls

Independently, each regimen is incapable of protecting the mission systems at the HOSC. When combined, the regimens overlap to provide comprehensive security. This allows confidence in the ability to conduct payload operations by investigators anywhere in the world.