6-2008

A Survey of Satellite Communications System Vulnerabilities

Jessica A. Steinberger

A SURVEY OF SATELLITE COMMUNICATIONS SYSTEM VULNERABILITIES

THESIS

Jessica A. Steinberger
AFIT/GA/ENG/08-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GA/ENG/08-01

A SURVEY OF SATELLITE COMMUNICATIONS SYSTEM VULNERABILITIES

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Astronautical Engineering

Jessica A. Steinberger, BS

June 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GA/ENG/08-01

A SURVEY OF SATELLITE COMMUNICATIONS SYSTEM VULNERABILITIES

Jessica A. Steinberger, BS

Approved:

Dr. Richard A. Raines (Chairman)	date
Dr. Robert F. Mills (Member)	date
Dr. Michael A. Temple (Member)	date

AFIT/GA/ENG/08-01

Abstract

The U.S. military's increasing reliance on commercial and military communications satellites to enable widely-dispersed, mobile forces to communicate makes these space assets increasingly vulnerable to attack by adversaries. Attacks on these satellites could cause military communications to become unavailable at critical moments during a conflict. This research dissected a typical satellite communications system in order to provide an understanding of the possible attacker entry points into the system, to determine the vulnerabilities associated with each of these access points, and to analyze the possible impacts of these vulnerabilities to U.S. military operations. By understanding these vulnerabilities of U.S. communications satellite systems, methods can be developed to mitigate these threats and protect future systems.

This research concluded that the satellite antenna is the most vulnerable component of the satellite communications system's space segment. The antenna makes the satellite vulnerable to intentional attacks such as: RF jamming, spoofing, meaconing, and deliberate physical attack. The most vulnerable Earth segment component was found to be the Earth station network, which incorporates both Earth station and NOC vulnerabilities. Earth segment vulnerabilities include RF jamming, deliberate physical attack, and Internet connection vulnerabilities. The most vulnerable user segment components were found to be the SSPs and PoPs. SSPs are subject to the vulnerabilities of the services offered, the vulnerabilities of Internet connectivity, and the vulnerabilities associated with operating the VSAT central hub. PoPs are susceptible to the vulnerabilities of the PoP routers, the vulnerabilities of Internet and Intranet connectivity, and the vulnerabilities associated with cellular network access.

Acknowledgments

I would like to sincerely thank my thesis advisor, Dr. Richard Raines, for his guidance and support throughout my thesis research effort. Thank you for your patience as I struggled my way through the process. Also, I truly appreciated your willingness to accommodate my work schedule when I started at AFIT as a part-time student. In addition, I would like to thank Major Paul Harmer from the USSTRATCOM, Joint Information Operations Warfare Command, Joint Electronic Warfare Center, Vulnerability Assessment Branch for helping me to narrow the focus of my project and providing some very useful sources of information. I would also like to express my sincere gratitude to Mr. Scott Anderson from SEAKR Engineering for his help and willingness to provide me with information on the IRIS project.

I owe a sincere debt of gratitude to the folks at NASIC who enabled me to come to AFIT as a full-time student through the LTFT program. Thank you for this opportunity. I would also like to thank my friends and family for their support throughout this endeavor. I appreciate you pushing me to finish my thesis on time to graduate. It would be a difficult feat to accomplish while working full-time.

Table of Contents

Page

List of Figures

Figure Page

List of Tables

Table Page

List of Acronyms

Acronym	Definition
ABM	Asynchronous Balanced Mode
ACK	Acknowledgement
A/D	Analog-to-Digital
ADCCP	Advanced Data Communication Control Procedures
AGC	Automatic Gain Controller
ANSI	American National Standards Institute
AOR	Atlantic Ocean Region
AP	Access Point
ARABSAT	Arab Satellite Communications Organization
ARP	Address Resolution Protocol
ATM	Automatic Teller Machine
BGP	Border Gateway Protocol
BPSK	Binary Phase Shift Keying
BVSAT	Broadband VSAT
CCTV	China Central TV
CDMA	Code Division Multiple Access
Centrex	Central Office Exchange
CFDAMA	Combined Free DAMA
CFDM	Companded FDM
CFM	Companded Frequency Modulation
CME	Coronal Mass Ejection
COMSAT	Communications Satellite
COTS	Commercial-off-the-Shelf
CSC	Common Signaling Channel
CSMA/CD	Carrier-Sense-Multiple Access/Collision Detection
CSRF	Cross-Site Request Forgery
DAMA	Demand Assignment Multiple Access
DDoS	Distributed DoS
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EIGRP	Enhanced Interior Gateway Routing Protocol
EM	Electromagnetic
EMP	EM Pulse
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FDOA	Frequency Difference of Arrival
FEC	Forward Error Correction
FM	Frequency Modulation

FSS	Fixed Satellite Service
FTP	File Transfer Protocol
GEO	Geostationary Earth Orbit
GIG	Global Information Grid
GPRS	General Packet Radio Service
GPS	Global Positioning System
HDLC	High-Level Data Link Control
HPA	High Power Amplifier
HTML	Hypertext Markup Language
IBS	INTELSAT Business Services
ICMP	Internet Control Message Protocol
IDR	Intermediate Data Rate
IF	Intermediate Frequency
IFRB	International Frequency Registration Board
IM	Intermodulation Product
IP	Internet Protocol
IPsec	IP Security
IRIS	Internet Routing in Space
IS	INTELSAT
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
ISS	International Space Station
ITU	International Telecommunications Union
ITSP	Internet Telephony Service Provider
JCTD	Joint Capability Technology Demonstration
JIIM	Joint, Inter-Agency, Inter-Governmental, and Multi-National
JSC	Johnson Space Center
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LEO	Low Earth Orbit
LFSR	Linear Feedback Shift Register
LNA	Low Noise Amplifier
LOP	Line of Position
LSA	Link State Advertisement
LTTE	Liberation Tigers of Tamil Eelam
MAC	Media Access Control
MCPC	Multiple Channels per Carrier
MEO	Medium Earth Orbit
MF	Multi-Frequency
MIB	Management Information Base
MMS	Multimedia Messaging Service
NAK	Negative ACK
NAP	Network Access Point
NCC	Network Control Center
NMS	Network Management System

NOC	Network Operations Center
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PC	Personal Computing
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PDP	Packet Data Protocol
PoP	Point-of-Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PRNG	Pseudorandom Number Generator
PSTN	Public Switched Telephony Network
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RIP	Routing Information Protocol
RMP	Reliable Multicast Protocol
SCPC	Single Channel per Carrier
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SPADE	SCPC PCM Multiple Access Demand Assignment Equipment
SRMP	Scalable RMP
SSES	Single Satellite Ephemeris Solution
SSH	Secure Shell
SSID	Service Set Identifier
SS/L	Space Systems/Loral
SSP	Satellite Service Provider
SSPA	Solid State Power Amplifier
SS/TDMA	Satellite-Switched/TDMA
TCM	Trellis-Coded Modulation
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDOA	Time Difference of Arrival
TLS	Transmitter Location Systems
TT&C	Telemetry, Tracking, and Control
TTL	Time to Live
TV	Television
TWTA	Traveling Wave Tube Amplifier
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal

WAN	Wide Area Network
WEP	Wireless Encryption Protocol
WLAN	Wireless LAN
WNA	Wireless Network Adapter
WPA	Wi-Fi Protected Access
XSS	Cross-Site Scripting

A SURVEY OF SATELLITE COMMUNICATIONS SYSTEM VULNERABILITIES

I: Introduction

The use of satellite communications, both commercial and military, has been increasing steadily over the past several years, both in the U.S. and in other countries. Additionally, since satellite communications technology advances have allowed these satellites to decrease in size while maintaining capabilities, the cost of launching and using communications satellites has decreased. Many of these satellites utilize commercial-off-the-shelf (COTS) components, enabling further cost reductions. These cost decreases have enabled other (less advanced) countries to obtain space assets, including those that could serve as anti-satellite payloads. Many countries, if not purchasing their own satellites, are leasing transponders on-board commercial communications satellites, such as the INTELSAT satellites [4].

Satellite communications are the “backbone” of net-centric warfare. They are important for sending information to widely-dispersed, mobile forces. There are not enough military-dedicated satellites on-orbit to provide the bandwidth required to transmit these volumes of information. Therefore, the U.S. military relies on both military and commercial satellites to provide these communications. This reliance on commercial space systems for military operations makes these assets vulnerable to attacks by adversaries. As Robert Ackerman’s article entitled *Space Vulnerabilities*

Threaten U.S. Edge in Battle states, “the disruption, denial, degradation, or destruction of space systems or services could seriously affect U.S. war fighting capabilities” [4]. As of April 2006, the percentage of communications being provided by commercial communications satellites for Operation Iraqi Freedom was an astounding eighty-four percent, according to Hank Rausch’s *Jamming Commercial Satellite Communications during Wartime: an Empirical Study*. Much of these commercial satellite communications were being supplied via leased transponders on-board INTELSAT and EUTELSAT satellites. Unfortunately, these commercial communications satellites are not built with the capabilities to protect themselves from potential attacks, such as jamming [130]. Such attacks could cause military communications to become unavailable at critical moments during a conflict.

The criticality of satellite communications to U.S. military operations makes the understanding of the vulnerabilities in satellite communications systems highly important in order to be able to thwart possible future attacks of these systems. This research aims to dissect typical satellite communications systems (which include a space segment, an Earth segment, and a user segment) to: 1) provide a better understanding of possible attacker entry points into the systems, 2) provide a better understanding of satellite communications systems vulnerabilities, and 3) examine the possible impacts of these vulnerabilities to U.S. military operations.

The remainder of this document is divided into four chapters. Chapter two contains background information on communications satellite systems, particularly the INTELSAT system. It includes information on the INTELSAT space segment (i.e. the satellites), the INTELSAT Earth segment including both INTELSAT standard Earth stations and very small aperture terminals (VSATs), and multiple access schemes utilized in communications satellite systems. This information all ties into the determination of all the possible entry points into a communications satellite system that is presented in the third chapter. In addition, a discussion of some emerging and proposed satellite systems is presented in order that any new access points and vulnerabilities that arise due to these systems may be analyzed. Finally, several examples of attacks on communications satellite systems that have taken place in the past are provided as evidence that these types of attacks are possible and that the threat of attacks on U.S. space assets is real.

Chapter three presents a breakdown for each segment of a communications satellite system, down to the component-level. From this level it is possible to identify the possible access points in each segment that may allow an attacker access to the communications satellite system. Once all of the access points are determined, it is then possible to analyze each access point and determine the vulnerabilities that each poses to the overall communications satellite system architecture. The results of this analysis are presented in the fourth chapter.

In addition to the vulnerabilities of each access point, chapter four also discusses which access point is most vulnerable within each satellite communications system segment. An example of the impact these vulnerabilities can have on a particular satellite system, namely INTELSAT 14 which is the satellite planned to carry the Internet routing in space (IRIS) payload, is also presented in this chapter.

Chapter five provides a summary of research findings. Also, some ideas for future work in this area are presented

II: Background

2.1 Introduction

The U.S. continues to dominate the military space arena, as it has since the end of the Cold War, owning over half of all the military satellites currently in orbit. In the recent past, the U.S. military has come to rely more heavily on commercial space systems to provide communications. In fact, during the Gulf War, INTELSAT provided the majority of long haul communications. The *2001 Report of the Commission to Assess United States National Security Space Management and Organization* cautioned that the U.S. may be making itself vulnerable to a "space Pearl Harbor" because of its strong dependence on space systems. The report recommended that the U.S. develop ways to protect its space assets [146].

Earth stations and communications links are the most vulnerable space systems elements and may be susceptible to attack by any of the following means: conventional military means, computer hacking, and electronic jamming. Several mitigation methods, such as shielding, directional antennas, and burst transmissions, can help to protect the communications links. However, these methods cannot completely protect the links, leaving them still vulnerable to some attacks. The Earth stations, on the other hand, are susceptible to physical attacks which could potentially wipe out communications across the space system, especially since most commercial space systems have only one network operations center (NOC) and one Earth station. For this reason, countries may need to protect their satellite Earth stations by means of basic military force [146].

2.2 History of INTELSAT and INTELSAT Satellite Capacity

In August 1964, the international organization INTELSAT was created to produce, own, and operate a global communications satellite system. INTELSAT was a treaty-based organization made up of nearly 150 member nations. In 2000, the member nations agreed to INTELSAT becoming a private company, forming INTELSAT Ltd. INTELSAT Ltd is based in Bermuda [45, 150]. Today, INTELSAT is the world's leading provider of GEO satellite services, owning and operating more than fifty communications satellites (COMSATs) [51]. INTELSAT satellites offer a variety of services, including: telephony, data transfer, fax, television (TV) broadcasting, and teleconferencing. INTELSAT offers a wide range of Earth terminals that can be used to access its satellites. These terminals range from 0.5 meters (m) to 30 m and can be operated in both the C- and Ku- bands. Note that C-band operating frequencies are nominally 6 gigahertz (GHz) for the uplink and 4 GHz for the downlink, and in the Ku-band, operating frequencies are typically 14 GHz for the uplink and 11 to 12 GHz for the downlink [45].

INTELSAT's first COMSAT, INTELSAT I (also known as Early Bird), was launched on April 6, 1965. INTELSAT I was the first commercial COMSAT and it was used to provide telecommunications services between the United States and Europe. INTELSAT I carried 240 two-way voice circuits or one TV channel. Only two earth stations (one in the U.S. and one in Europe) could access INTELSAT I at any one time, creating only one point-to-point trunk [8, 143]. INTELSAT launched its second series of satellites, the INTELSAT II satellites, in 1967. The INTELSAT II satellites offered coverage of the Atlantic and Pacific regions [83]. Like INTELSAT I, the INTELSAT II satellites also carried 240 two-way voice circuits [108]. In contrast to the INTELSAT I satellite, the INTELSAT II satellites could provide TV and phone services simultaneously [8]. On the INTELSAT III series satellites, launched between 1968 and 1970, there was a significant increase in capacity per satellite over the INTELSAT I and INTELSAT II satellites. Each INTELSAT III satellite carried 1200 to 1500 two-way voice circuits or four TV channels [83, 108]. INTELSAT began launching its INTELSAT IV series satellites in 1971. The INTELSAT IV series satellites carried between 3,000 and 9,000 two-way voice circuits or twelve TV channels (that is, one color TV channel per repeater) [83, 108]. Due to demands for more capacity, in 1975 INTELSAT began launching its INTELSAT IV-A series satellites. The nominal INTELSAT IV-A capacity was 6,000 two-way voice circuits plus two TV channels, with their capacity capable of reaching a maximum of 15,000 two-way voice circuits. The INTELSAT V satellites, launched from 1980 to 1984, had a nominal capacity of 12,000 two-way voice circuits plus two TV channels. An additional maritime communications subsystem was incorporated into INTELSAT 505, 506, 507, 508, and 509. The maritime communications subsystem consisted of thirty voice circuits for high-power mode and fifteen voice circuits for low-power mode. To maintain the necessary amount of capacity in the Atlantic region, INTELSAT modified the INTELSAT V satellites, creating the INTELSAT V-A series. The INTELSAT V-A series was launched from 1985 to 1989 and each satellite in the series has a capacity of 15,000 two-way voice circuits plus two TV channels. The INTELSAT VI series satellites, launched from 1989 to 1991, each has a nominal capacity of 24,000 two-way voice circuits plus three TV channels, while the INTELSAT VII series satellites carry a nominal capacity of 18,000 two-way voice circuits plus three TV channels [108]. The INTELSAT VI communications payload included a static and dynamic switching network. The static network allowed transponder interconnections, while the dynamic network made possible satellite switched time division multiple access (SS/TDMA). SS/TDMA will be discussed further in the section on multiple access schemes [8]. The INTELSAT VII satellites, which replaced the INTELSAT V and INTELSAT V-A satellites in the Pacific region, were launched between 1993 and 1996. The INTELSAT VII series satellites are smaller than the INTELSAT VI series satellites, a change from the current trend of increased size and capacity with each additional satellite series. The INTELSAT VII series satellites are smaller due to a requirement for more flexibility, which was accomplished by the use of many switches to interconnect INTELSAT VII's increased number of antenna beams. INTELSAT VII-A satellites, a "growth version" of INTELSAT VII, have nominal capacities of 22,500 two-way voice circuits and three TV channels. The INTELSAT VIII series satellites, which began launching in 1997, also have a capacity of 22,500 two-way voice circuits and three TV channels [108]. The INTELSAT VIII-A satellites, INTELSAT 805 and 806 which were launched in 1998, have approximately the same capacity as the INTELSAT VIII series satellites [108, 150]. The difference between the INTELSAT VIII and INTELSAT VIII-A series satellites is a major restructuring of the communications payload. The INTELSAT IX series satellites, launched from 2001 to 2003, were intended to replace the INTELSAT VI satellites [108]. The INTELSAT IX satellites each carry approximately 600,000 two-way voice circuits or 600 TV channels, a dramatic increase over the early series INTELSATs [83]. A summary of the evolution of INTELSAT capacity for Series I through Series IX can be seen in Table 1 below.

Table 1. Evolution of INTELSAT Satellite Capacity (INTELSATs I-IX) [8, 83, 108, 143]

Satellite	Capacity
INTELSAT I	240 two-way voice circuits or 1 TV channel
INTELSAT II	240 two-way voice circuits or 1 TV channel
INTELSAT III	1200-1500 two-way voice circuits or 4 TV channels
INTELSAT IV	3000-9000 two-way voice circuits or 12 TV channels
INTELSAT IV-A	6000 two way-voice circuits plus 2 TV channels or 15,000 two-way voice circuits
INTELSAT V	12,000 two-way voice circuits plus 2 TV channels and 15 (low power mode) or 30 (high power mode) two-way voice circuits for maritime communications subsystem
INTELSAT V-A	15,000 two-way voice circuits plus 2 TV channels
INTELSAT VI	24,000 two-way voice circuits plus 3 TV channels
INTELSAT VII	18,000 two-way voice circuits plus 3 TV channels
INTELSAT VII-A	22,500 two-way voice circuits plus 3 TV channels
INTELSAT VIII	22,500 two-way voice circuits plus 3 TV channels
INTELSAT VIII-A	22,500 two-way voice circuits plus 3 TV channels
INTELSAT IX	600,000 two-way voice circuits or 600 TV channels

In 2004 INTELSAT continued with its trend of launching large, high capacity satellites with the launch of INTELSAT 10-02. INTELSAT 10-02 is the replacement for an INTELSAT VII series satellite, INTELSAT 707. INTELSAT 10-02 carries up to 70 C-band and 36 Ku-band 36-megahertz (MHz) equivalent transponder units. This capacity compares to the INTELSAT IX series satellites with INTELSAT 907 carrying 76 C-band and 22 Ku-band 36-MHz equivalent transponder units [90].

INTELSAT launched another satellite, INTELSAT 11, in late 2007. INTELSAT 11 is intended to replace INTELSAT 6B and INTELSAT 3R, which were formerly named PAS-6B and PAS-3R and were owned by PanAmSat. PanAmSat and its satellites were acquired by INTELSAT in 2006. INTELSAT 11 has a communications payload which consists of 25 C-band and 18 Ku-band transponders [90].

2.3 Satellite Access Points

INTELSAT standard Earth stations (Standards A, B, C, D (no longer in use), E, F, G, H, and K) provide access to the INTELSAT satellites. Access to the satellites requires a choice of modulation and multiple access techniques. In addition, cross-strapping allows interconnections between C-band and Ku-band earth stations. This is possible starting with the INTELSAT V series satellites [2, 9, 108].

2.3.1 INTELSAT Standard A

The INTELSAT Standard A terminal operates in the C-band and it has been used for all INTELSAT series satellites (I to IX). A smaller Standard A antenna size, which can be used with INTELSAT satellite series beginning with INTELSAT V, was introduced in 1986. Antennas sizes were reduced from 29-32 m to 15-18 m. The smaller antenna size caused the Standard A gain requirements to be reduced. The modulation and multiple access formats that are compatible with Standard A terminals include: frequency division multiplexing/frequency modulation (FDM/FM), companded FDM/FM (CFDM/FM), single channel per carrier/quadrature phase shift keying (SCPC/QPSK), TV/FM (TV transmissions using FM), time division multiple access (TDMA), QPSK/intermediate data rate (IDR), INTELSAT Business Services (IBS), Trellis-coded modulation (TCM)/IDR, and demand assigned multiple access (DAMA). Trellis-coded modulation is a modulation scheme which allows highly efficient transmission of information over band-limited channels (for example, telephone lines). All of the aforementioned multiple access formats will be discussed in more detail later in this section [108].

2.3.2 INTELSAT Standard B

INTELSAT's Standard B terminal also operates in the C-band. Its use began with the INTELSAT IV series satellites. The Standard B terminals differ from the Standard A terminals in their use of smaller antenna sizes, ranging from approximately 11 to 13 m. The smaller antenna size again means a decrease in antenna gain, and therefore a higher per-circuit satellite usage charge. The higher per-circuit usage charge is the reason why Standard A terminals are still more widely used than Standard B terminals today, despite the goal of the Standard B terminals to provide a lower-cost terminal for nations with modest communications traffic requirements (less than twenty-four voice circuits). The modulation and multiple access formats used with Standard B terminals include: CFDM/FM (companding helps offset the lower antenna gain), SCPC/QPSK, TV/FM (transitioning away from TV/FM to digital TV transmission), QPSK/IDR, IBS, TCM/IDR, DAMA, and low-cost TDMA [108].

2.3.3 INTELSAT Standard C

INTELSAT's Standard C terminal's use began with the INTELSAT V satellites. The Standard C terminal operates in the Ku-band. Standard C terminals can incorporate two antennas separated by approximately 10 to 20 miles in order to overcome attenuation due to rain via spatial diversity. The Standard C terminals are generally utilized by nations with major communications requirements, as are the Standard A terminals, but these countries usually already have at least one Standard A terminal. The modulation and multiple access formats that are compatible with the INTELSAT Standard C terminals include: FDM/FM, CFDM/FM, QPSK/IDR, IBS, and TCM/IDR [108].

2.3.4 INTELSAT Standard D

INTELSAT's Standard D terminal, decommissioned in 1998, operated in the C-band. Standard D terminals were intended for use in places with very low satellite communications requirements, only about one to two voice circuits per terminal. In general, Standard D terminals, which were lower-cost than Standard B terminals, were used by small islands in the Pacific and some African nations for communications between the rural areas and the countries' capitals. The only modulation and multiple access format used with the Standard D terminals was SCPC/companded frequency modulation (CFM) [108].

2.3.5 INTELSAT Standards E and F

INTELSAT's Standard E and F terminals began use in the mid-1980s. They only differ by frequency band, Standard E operating in the Ku-band and Standard F operating in the C-band. These two terminals are used particularly with IBS. Instead of serving entire nations, Standards E and F are used to serve specific customer locations or multiple customers in small regions, for example a big city. The modulation and multiple access formats compatible with Standard E terminals include: QPSK/IDR, IBS, and

TCM/IDR. The Standard F compatible modulation and multiple access formats are CFDM/FM, QPSK/IDR, IBS, TCM/IDR, and DAMA [108].

2.3.6 INTELSAT Standard G

The INTELSAT Standard G terminals can be used in either the C-band or the Ku-band. Standard G terminals are used for services offered by countries that lease or purchase INTELSAT capacity. In the case of Standard G terminals, the network operator has the freedom to choose most system characteristics. The terminal must simply abide by the rule that it cannot interfere with other satellite users. This freedom to choose the terminal design characteristics means that all modulation and multiple access formats are acceptable, as long as INTELSAT agrees [108].

2.3.7 INTELSAT Standards H and K

INTELSAT Standards H and K are like Standards E and F in that they only differ in frequency. Standard H operates in the C-band and Standard K operates in the Ku-band. Standards H and K were implemented in the late 1990s. Standards H and K employ even smaller antennas than Standards E and F. The modulation and multiple access formats compatible with Standard H terminals include both IBS and DAMA. For the Standard K terminals only IBS is compatible [108].

2.3.8 INTELSAT Services

IDR services, introduced in 1984, provide digital communications to international public switched telephony networks (PSTNs) and are available on nearly all INTELSAT satellites. IDR utilizes QPSK modulation and shares transponders via frequency division multiple access (FDMA). IDR is employed by INTELSAT Standards A, B, C, E, and F terminals. It is the digital counterpart to the analog FM/FDMA carriers [2, 8, 108].

IBS was also launched in 1984 and has the same transmission characteristics as IDR, except for a different data rate. IBS is used for private communications via Earth terminals located at specific customer sites or in nearby cities. Standards E, F, H, and K are used primarily for IBS [108]. Video conferencing is offered via occasional use IBS [2].

Intelnet was set up in the mid-1980s and supports low rate transmission services to/from small terminals (2-8 feet in diameter). These small terminals then communicate with larger hubs. The multiple access formats and modulation techniques that can be used for Intelnet are FDMA or code division multiple access (CDMA) and binary phase shift keying (BPSK), QPSK, or spread spectrum [2, 108]. The Intelnet service is used to gather and disperse data between hubs and very small aperture terminals (VSATs) [2]. For Intelnet leases, Earth stations are expected to meet the Standard G terminal specifications. However, INTELSAT may approve terminals not meeting these specifications as “non-standard” terminals [10].

2.3.9 Very Small Aperture Terminals (VSATs)

VSAT networks are in many cases used to connect and provide Internet protocol (IP)-based multimedia services to companies whose corporate offices and manufacturing, supply, and distribution centers are widely dispersed. Each INTELSAT VSAT terminal is interconnected via a large central hub which is located at a gateway Earth station. VSAT terminals, because they are small, are fairly inexpensive [2].

The INTELSAT system features several different types of VSAT networks, including: data transaction-type networks; circuit-switched-type networks; video, audio, and data distribution-type networks; and micro-terminal-type networks [10].

Data transaction networks are the most frequently used type of INTELSAT VSAT network. Two-way data transmission is the major function of this type of VSAT network. Data transaction networks have a star configuration (see Figure 1). In this type of configuration a central hub functions as both a network control center (NCC) and a traffic gateway.

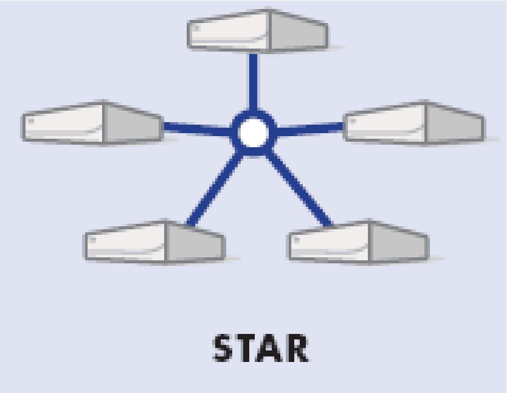


Figure 1. VSAT Network - Star Configuration

Central hubs in this type of network serve to: monitor links at the VSATs, configure the network, enable and disable VSATs, download software, collect network statistics, assign satellite capacity, and in some cases may also operate as a packet switch [10].

Circuit-switched VSAT networks have a both pre-assigned circuits and demand-assigned circuits, with demand assignment used only for voice circuits. Mesh or star topologies are commonly used for this type of network (See Figure 2) [10]. In the case of a mesh configuration with demand assigned circuits, a VSAT uses a common signaling channel (CSC) to send a request to the hub Earth station that a link is set up between the requesting VSAT and another VSAT. The hub Earth station informs the called VSAT that there has been a link request and then the hub assigns two channels to link the two VSATs. When the call has ended, the channels are free to be used when another request is made. In a mesh configuration with pre-assigned circuits, all networked VSATs use the same channel to receive and transmit, usually via a TDMA multiple access scheme [48].

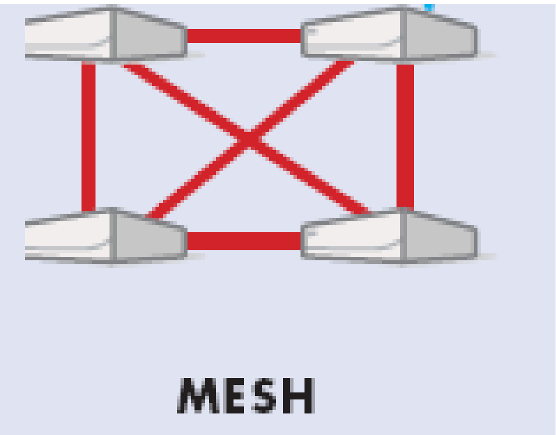


Figure 2. VSAT Network - Mesh Configuration

Voice transmission is the main role of circuit-switched VSAT networks, with data transmission coming in second. Video conferencing may also be available through these networks. Assignment of voice circuits is done either from an NCC or via a distributed control procedure. The NCC also performs monitoring and control of network traffic, network configuration, generation of call records, software downloads, and data recording [10].

Video, audio, and data distribution VSAT networks typically have a star topology. In actuality, the network management systems for this type of VSAT network can operate with several traffic gateways (in a multi-star configuration). Digital audio and data distribution networks often use a TDM carrier. CDMA cannot be used for these networks [10].

Micro-terminal VSAT networks, which are used for portable communications, employ CDMA to alleviate interference problems caused by large antenna beamwidths. In particular, direct sequence spread spectrum (DSSS) CDMA is used. As in the case of circuit-switched VSAT networks, voice transmission is the main function of these micro-terminal networks. Data and low-rate imagery applications can also be supported. Micro-terminal networks typically operate in a star configuration. Operation in a multi-star configuration is also possible [10].

In addition to the aforementioned multiple access schemes, there are also contention-based random access schemes such as Aloha and its variations that are generally used with VSATs. In the case of unslotted Aloha, any user can transmit at any time. If the information is received correctly, the receiving hub station sends an acknowledgement. If no acknowledgement is received by the user, the information is retransmitted after waiting for a period of time. With slotted Aloha, the packets are transmitted in time slots [84, 98].

In addition to the previously mentioned Intelnet services, INTELSAT offers VSAT networks for domestic or international lease as part of INTELSAT's multi-use transponder services offering. For leases within the multi-use transponder services, Earth stations are expected to meet Standard G terminal specifications [10].

INTELSAT also offers a service called Broadband VSAT (BVSAT), which is a bandwidth-on-demand service. The BVSAT network offers high speed networking for data, voice, video, and Internet traffic. As part of the BVSAT network, INTELSAT has located gateways in four major regions: Europe and the Middle East, Africa, the Americas, and the Asia-Pacific region. BVSAT employs LINKWAY Infrastructure VSATs from Comsat Laboratories, a division of ViaSat [157].

LINKWAY is a "hubless" VSAT system which allows each terminal to use a range of bandwidth over multiple transponders. LINKWAY offers two VSAT system options: LINKWAY 2100 and linkway.ip. Both of these terminal types are interoperable over C- and Ku- band fixed satellite service (FSS) satellites, such as the INTELSAT COMSATs. LINKWAY 2100 BVSAT networks can employ a mesh, star, or hybrid topology, which allows terminal to be capable of accessing all channels in the network (see Figure 3). Therefore, each aforementioned network topology is available from a single platform.

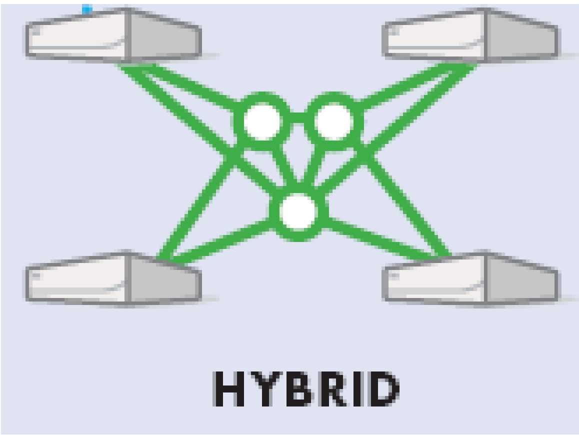


Figure 3. VSAT Network - Hybrid Configuration

Linkway.ip specifically handles IP applications. Some applications for which linkway.ip is ideal include: Internet Service Provider (ISP) point of presence (PoP) connections, voice over IP (VoIP), and data and video multicasting [157].

INTELSAT's VSAT network also offers services such as: interoffice connectivity, point-of-sale transactions, virtual private networks (VPNs), local area networking (LAN) and wide area networking (WAN), Internet and Intranet, video conferencing, remote site networking, and VoIP [90].

2.4 Multiple Access Methods

In a network where many Earth stations want to access the bandwidth of a single transponder, there are several possible methods available for gaining such access. As mentioned previously, the INTELSAT Earth station standards and VSAT networks support a number of multiple access schemes. These schemes are as follows: FDMA, SCPC, multiple channels per carrier (MCPC), DAMA, TDMA, SS/TDMA, and CDMA.

2.4.1 FDMA

FDMA was first used on INTELSAT I. FDMA is an access method in which a portion of available radio frequency (RF) spectrum is divided into channels. Each channel, operating at a different frequency, is assigned to a user to enable multiple users the ability to use this same portion of spectrum. However, since users are assigned fixed amounts of bandwidth, it is difficult for bandwidth to be assigned to another user. One of the disadvantages of using FDMA is that it can create intermodulation (IM) products. However, IM products can be avoided by operating the satellite's traveling wave tube amplifiers (TWTAs) in their linear region, but this decreases the available output power. FDMA is less complex in terms of networking in comparison to TDMA. The amount of Earth station equipment required when using FDMA increases as the amount of simultaneous connectivity increases [143]. See Figure 4 for an illustration of FDM.

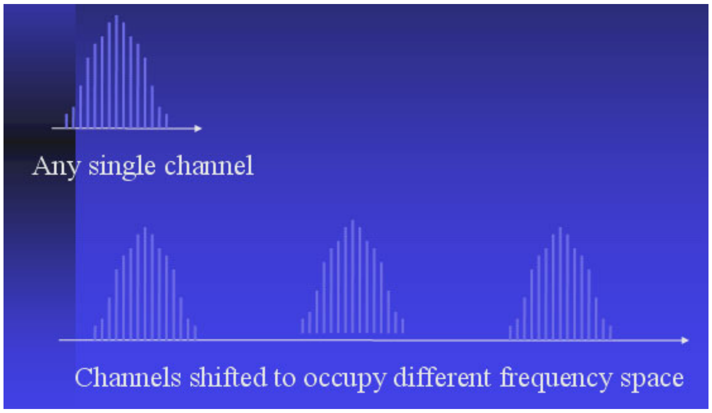


Figure 4. Frequency Division Multiplexing (FDM) Illustration [101]

2.4.2 SCPC

SCPC FDM/FM was first used on the INTELSAT II satellites [143]. In SCPC, one signal operates at a given frequency and bandwidth. SCPC systems are typically used for voice applications. SCPC carriers are pre-assigned and they share transponder power and bandwidth through FDMA. SCPC is typically used for thin route communications traffic, and is as efficient as TDMA when employed with standard Earth stations [2, 143].

2.4.3 MCPC

Like SCPC, multi-carrier FDM/FM (or MCPC) was first used on INTELSAT II series satellites and MCPC carriers are also pre-assigned. For an MCPC system, multiple signals are combined into one bit stream before being modulated onto a carrier. This carrier can then be transmitted to multiple remote sites. Because all signals have to be sent to a single location before being combined for transmission, MCPC is at a major disadvantage compared to SCPC in terms of transmission time. MCPC is very efficient with heavy traffic. In the case of light traffic, the pre-assigned channels go unused and cannot be reallocated [143].

2.4.4 DAMA

Demand assignment is used when communications traffic peaks above pre-assigned channel capacity or in the case of terminals with no pre-assigned channels [108]. A DAMA system can be employed to offer thin routes between PSTN international gateways (for example, Standard A terminals) to support telephony, fax, and data services. A DAMA system can function with Earth stations as small as 1.8 m (i.e. VSATs, in this case used in a star network configuration). DAMA systems increase usage efficiency, thereby releasing transponder capacity to be used for other services. Modulation for DAMA systems is typically chosen to be either QPSK or BPSK [9].

2.4.5 SCPC Pulse Code Modulation (PCM) Multiple Access Demand Assignment Equipment (SPADE)

INTELSAT's use of demand assignment systems, its first digital communications system, began in the early 1970s with SPADE, the use of which ended in 1993 [2, 108]. SPADE is a system in which every channel is shared and assigned according to demand [143]. SPADE is typically employed by Standard B terminals [108].

In SPADE systems, a signal is modulated onto a carrier using QPSK. The carrier is then dynamically assigned according to demand. If there is no speech detected, the carrier will be turned off. SPADE carriers are dynamically assigned over a common signaling channel (CSC). Each Earth station monitors the CSC and is aware of the present state of channel allotments. The CSC is divided up into time slots for Earth stations to request and release channels. SPADE's utilization of bandwidth is more efficient than MCPC and is proportionate to that of SCPC. A SPADE transponder having 800 channels is approximately equal to an MCPC transponder with 3200 channels [143].

2.4.6 TDMA

TDMA has been employed by the INTELSAT system since 1985, specifically in conjunction with INTELSAT Standard A terminals. Application of TDMA to

INTELSAT Standard B terminals was also made possible by the use of improved forward error correction (FEC) decoding schemes [9]. Earth stations can typically not see their own transmissions with INTELSAT's TDMA systems [2].

TDMA is a multiple access scheme which shares a channel by dividing it into different timeslots. Signals are transmitted one after another in rapid succession in their specific timeslot (See Figure 5) [101, 143]. TDMA allows for variation in the allocation of these timeslots based on current user needs [62].

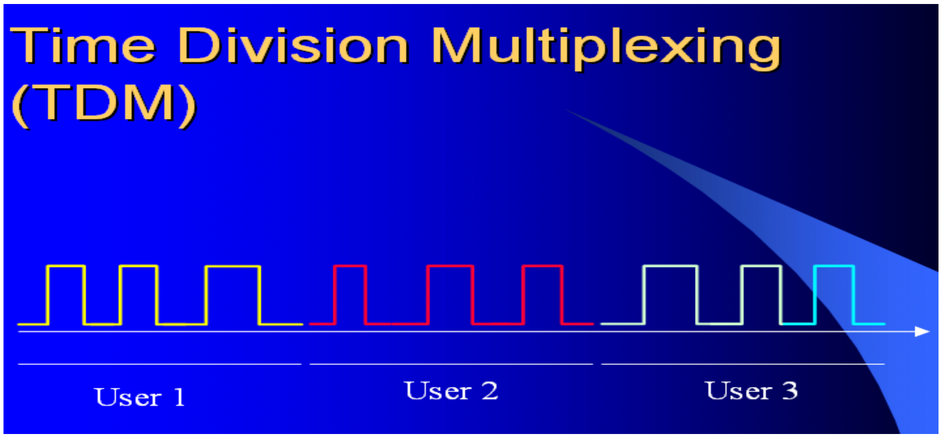

Time Division Multiplexing (TDM)

Figure 5. Time Division Multiplexing Illustration

Precise synchronization between Earth stations and satellites, made possible by precise clocks and high speed switching elements, is essential to TDMA so the signals arrive at the satellite in the correct position in the TDMA frame [143]. Since TDMA uses only one carrier at a time, IM products cannot occur as they can in FDMA [101]. Also, TDMA provides greater capacity than FDMA systems [108]. One disadvantage of using a TDMA scheme is that they cause transmission delays for other Earth stations that may be waiting to utilize the same transponder bandwidth [62].

2.4.7 SS/TDMA

TDMA is well-suited to connecting beams sequentially, which is part of the reason for INTELSAT's switch to SS/TDMA in 1990 [9, 143]. SS/TDMA was first used on the INTELSAT VI series satellites. The fast switch matrices of INTELSAT VI's communications subsystem allowed its repeaters to independently connect to any of six beams for reception and for transmission. This allows Earth stations in different regions to communicate with one another [108]. Complete interconnectivity of a total of N beams can be achieved with $N!$ different satellite switch modes. SS/TDMA was not reused on an INTELSAT system until the INTELSAT IX series satellites, likely due to switch matrix complexity. SS/TDMA systems significantly boost the satellite's capacity in comparison to FDMA systems [108, 143].

2.4.8 CDMA

As mentioned previously, CDMA systems can be used with the INTELSAT VSAT networks, particularly in conjunction with INTELSAT's Intelnet services. CDMA uses spread spectrum technology and a coding scheme in which each transmitter is assigned a particular code. CDMA divides the signal space, as opposed to TDMA's division of time and FDMA's division of frequency. More efficient use of bandwidth is an effect of partitioning the signal space. In addition, the assigned codes offer a level of security in that they can only be decoded by their intended receiver. CDMA is not very susceptible to frequency jamming due in part to its design allowing for flexibility in center frequency, spread rate, and power level. Also, frequency reuse can be accomplished with CDMA without causing unwanted co-channel interference. One disadvantage of CDMA is that it is vulnerable to strong, undesired signals at the receiver blocking weaker, desired user signals from gaining access to the bandwidth [62].

2.5 Emerging and Proposed Systems

Over the past forty years in satellite development, the typical approach has been to keep the satellites as simple as possible, keeping the complexity on the ground. This was done to minimize the damages caused by catastrophic satellite failures. In recent years, the on-board complexity of satellites has been increasing with the incorporation of on-board processing into satellite communications payloads. On-board processing involves frequency translating and re-amplifying the received signal, as well as processing it down to the bit level by decoding, de-interleaving, and demodulating it on-board [45].

At present, in addition to on-board processing, the U.S. and several other countries are in the process of developing satellite laser communications systems. Laser-based communications systems, in addition to providing faster communication, could help to protect communications links against traditional jamming techniques [146].

2.5.1 Internet Routing in Space (IRIS)

One current U.S. military project could potentially benefit commercial satellite communications. The project is called IRIS or Internet Routing in Space. In fact, the U.S. Department of Defense has chosen the INTELSAT General Corporation, a subsidiary of INTELSAT Ltd to manage the IRIS project [25]. The IRIS payload is intended to be carried on-board the INTELSAT 14 satellite, which is planned to be launched during the second quarter of 2009 [25, 147].

INTELSAT has a contract with Space Systems/Loral (SS/L) for the manufacturing of INTELSAT 14. The satellite is based on SS/L's 1300 series satellite platform, and has a design lifetime of 15 years. The satellite carries 40 C-band and 22 Ku-band transponders. It is intended to be located at 45 degrees West longitude where it will be capable of providing coverage of the Americas, Europe, and Africa via its four coverage beams [147].

The IRIS project will come to fruition with the help of commercial industry participants, such as SEAKR Engineering, Inc. SEAKR Engineering, Inc. manufactures the IP router for the IRIS payload. According to the *Management Plan for the Internet Protocol Routing In Space (IRIS) Joint Capability Technology Demonstration (JCTD)*, "the commercially-owned/operated IRIS payload aboard IS 14 (INTELSAT 14) may connect to the Department of Defense (DoD)-controlled global information grid (GIG) and promote developing policy-based network management for satellite communications" [106].

The IRIS program benefits the commercial satellite communications community in the following ways: providing IP routing capability between satellites, reducing transmission times, providing satellite capacity savings, and increasing networking flexibility. The on-board router would eliminate the need for a signal's round trip to an Earth station, thereby decreasing the number of needed Earth stations. IRIS' IP routing technology will allow transponders to communicate with one another by "decoding what comes up in the C-band or Ku-band and interconnecting the two" [25].

2.6 Hacking Satellite Communications Links

2.6.1 Tamil Tigers Liberation Front

The Tamil Tigers Liberation Front (or Liberation Tigers of Tamil Eelam - LTTE), a Sri Lankan separatist group known as terrorist in at least 32 countries, have recently been blamed for illegally using INTELSAT satellites to broadcast radio and TV transmissions via the use of an empty transponder on-board INTELSAT 12 [51, 144]. INTELSAT 12 was formerly known as Europe Star 1, a PanAmSat satellite, until PanAmSat was acquired by INTELSAT Ltd in July 2006 [51]. LTTE was broadcasting their "National Television of Tamil Eelam and Pulikalin Kural ('Voice of Tigers') radio transmissions" for four hours each day across INTELSAT 12's transponder 2. The uplink transmissions are believed to have come from within Vavuniya, northern Sri Lanka, according to Sri Lankan intelligence officials [51].

INTELSAT 12 is a bent-pipe satellite, which is the most common type of communications satellite on orbit, mainly due to the fact that this type of satellite is much less expensive than those with on-board processing. When bent-pipe transponders are not being fully-used, the empty transponders can be identified by a spectrum analyzer in combination with a satellite receive antenna. These empty transponders are configured to retransmit any signal being sent to them. The uplink signal from the hijacker is transmitted to the satellite in a highly-directed beam which makes finding the hijacker extremely difficult [51, 144]. There are systems available for locating interferences, but these systems only can find the general area where the interference came from [144].

2.6.2 TLS NexGen Interference Locating System

The TLS NexGen system by Transmitter Location Systems, LLC is one system used to locate interferences. Optional software is available that can be added to TLS NexGen making it able to geolocate interferences with only one satellite's orbital elements (usually an adjacent satellite). This software is called Single Satellite Ephemeris Solution (SSES). Orbital elements from an adjacent satellite that is receiving sidelobe energy from the interfering signal in addition to orbital elements of the satellite receiving the interference are necessary for TLS NexGen without SSES. TLS NexGen finds the transmitter's location by calculating the difference in arrival times and frequencies caused by transmitting the interfering signal through two satellites [151]. In the time difference of arrival (TDOA) technique, the difference in the arrival time of the interfering signal from the two satellites is used to determine a longitudinal line of position (LOP). In the frequency difference of arrival (FDOA) technique, frequency difference of the interfering signals from the two satellites due to the motion of the satellites is used to determine a latitudinal LOP. Where the TDOA and FDOA LOPs intersect is a probability ellipse that contains the interference location [13]. Position accuracy of the transmitter's location is typically within a few kilometers. TLS also has a global network of processing stations, with stations located in Bosque Alegre, Argentina; Perth, Australia; Ontario, Canada; Beijing, China; Hong Kong, China; Paris, France; Fucino, Italy; Mexico City, Mexico; Pretoria, South Africa; and Dubai, United Arab Emirates. Data from these stations on interference incidents is sent to the Global Operations Center in Chantilly, Virginia for processing [151].

2.6.3 Falun Gong

Another satellite interference event occurred in 2002 when the Falun Gong hacked the SinoSat satellite. The interferences on SinoSat were traced back to a “pirate broadcast operation in Taipei, Taiwan.” This interference event disrupted broadcasts of China Central TV (CCTV) to remote regions of China and transmission of China Education TV and in some cases cut off TV entirely in the rural and mountainous regions. CCTV is a Chinese government-run network. The Falun Gong continually attempts to broadcasts its transmissions proclaiming the benefits of being a member of the group and attempting to convince the rest of the Chinese citizens that they have been unfairly treated by Chinese authorities [17, 51, 144]. In fact, in November 2004 the Falun Gong hacked into AsiaSat and disrupted signals for approximately four hours [51].

2.6.4 Other Jamming Events

In 2006, Thuraya mobile satellite communications were jammed by Libyan nationals for nearly six months. In this case, the jamming was aimed at Thuraya satellite phone-using smugglers of contraband into Libya. During the 2006 Israel-Lebanon war, Israel attempted to jam the Al-Manar satellite channel which is transmitted by the Arab Satellite Communications Organization (ARABSAT), illustrating the potential for commercial satellites to become targets during conflict [146].

2.6.5 Conclusions

This ability to hack into commercial COMSATs could lead to a disastrous situation in regards to worldwide communications. Potentially, a hijacked satellite in geostationary Earth orbit (GEO) could be directed to crash into another nearby satellite causing a lot of damage not just to the other satellite but to many satellites in GEO due to the debris this crash would create. Al-Qaeda being able to use COMSATs in order to launch an attack against the U.S. may even be possible [144]. It appears that nearly everyone could pirate satellite capacity if they wanted. In fact, Extreme Media of Garden City, Michigan reportedly is selling the following videos from its website: "Satellite Piracy" and "Hacking Digital Satellite Systems" [51].

There are several ways that COMSATs can be protected from potential interferences, including: data encryption, the use of error protection coding which makes greater the amount of interference that is acceptable before communications are disrupted, the employment of directional antennas which reduce vulnerability to jamming, and shielding which decreases the amount of energy that can be intercepted for the purpose of jamming. Further protection capabilities are available, but are currently primarily used for military COMSATs. These protection capabilities are as follows: narrowband excision schemes that use less bandwidth, burst transmissions and frequency hopping techniques that prevent potential jammers from "locking-on" to signals, antenna side lobe reduction increase the focus of the main communications beam and reduce jamming incidents in the beam side lobes, and nulling antenna systems which observe interference and combine antenna elements developed to cancel interference [146].

2.7 Summary

The U.S.'s heavy reliance on and need to protect its space assets is apparent. In fact during the Gulf War, the U.S. relied heavily on the INTELSAT fleet of commercial COMSATs. Therefore, a brief history of INTELSAT and the evolution of INTELSAT's satellite capacity were discussed in this chapter. A brief discussion of the INTELSAT satellite access points identified a few of the possible areas where space systems may be vulnerable to attack, to include the Earth stations, VSAT networks, and multiple access methods. A more in-depth analysis of a typical space system's access points will be provided in Chapter 3 as the next step to achieving the end-goal of providing a vulnerabilities assessment of a space system.

This chapter highlighted several emerging (or proposed) satellite system technologies, including on-board processing, satellite laser communications, and Internet routing in space (IRIS). This information will allow an assessment of future vulnerabilities of space systems and possible ways to protect these emerging systems from attack.

Finally, to illustrate the susceptibility of U.S. space systems to attack, several examples were provided of hacking events involving satellite communications links that have occurred in the recent past. These include the hacking of INTELSAT 12 by the Tamil Tigers Liberation Front and the hacking of SinoSat by the Chinese Falun Gong. Several ways to stop these RF interference events from taking place were discussed, such as: using an interference locating system, data encryption, error protection coding, frequency hopping, and antenna sidelobe reduction.

III: Methodology

3.1 Introduction

In order for the U.S. to develop ways to protect its space assets, it is necessary first to understand the vulnerabilities of the U.S.'s space assets. To accomplish this vulnerabilities assessment, the space systems need to be analyzed at the component-level in order to determine possible access points for attackers. As stated in Chapter 2, the Earth stations and the communications links (between user terminals, Earth stations, NOCs, and satellites) are the most vulnerable components of U.S. satellite systems to attack. Therefore, it is necessary to take a closer look at these components to determine possible access points in each.

3.2 Satellite

A typical satellite communications link involves a satellite and two or more Earth terminals. Information is exchanged between the satellite and these terminals via RF antennas located on-board the satellite and at the Earth station facilities (or user locations). The antennas are the main access points to the satellite. Access to information being passed across the satellite goes even further than just the antennas. It passes from the antennas to one of the many on-board transponders. In a typical bent-pipe satellite, the transponders amplify the information signal and frequency-translate it before transmitting it back down to the ground. Transponder amplifiers are usually either traveling-wave tube amplifier (TWTA)-type or solid state power amplifier (SSPA)-type.

In the case of INTELSAT 14, which is the satellite intended to carry the IRIS payload, there will be an access router on-board the satellite. The access router will not only be able to route incoming information to the proper destination, but it will also enable all elements of the satellite to be addressed individually via IP and be interconnected via on-board routing [145]. See Figure 6 for an illustration of the breakdown of the satellite access points.

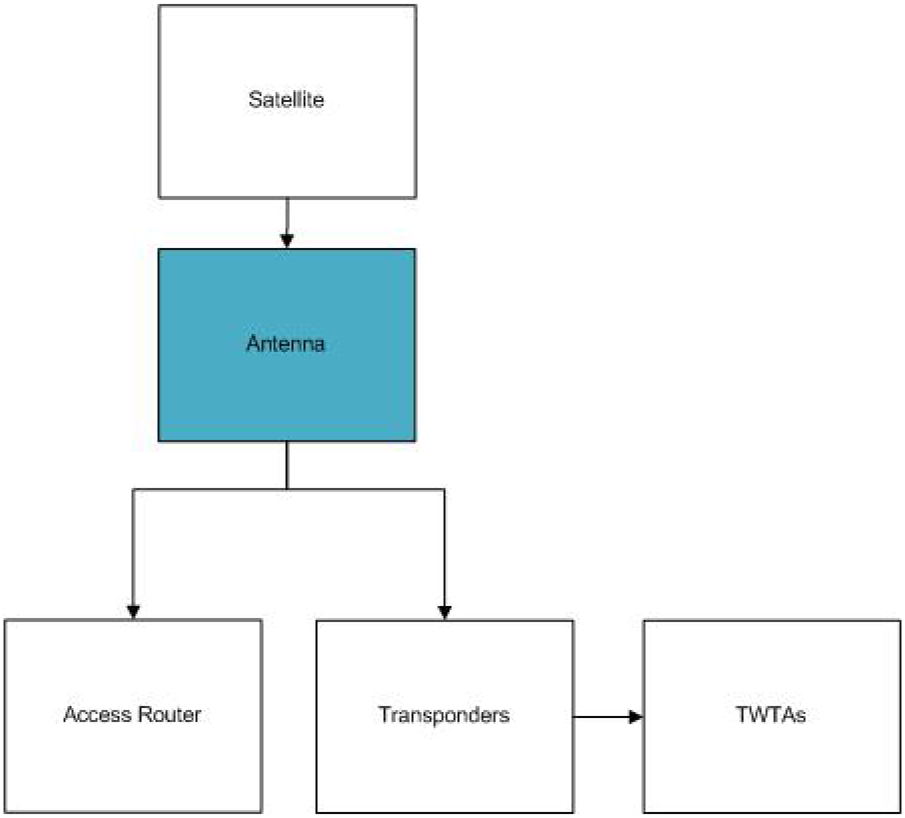


Figure 6. Satellite Breakdown Showing Access Point Components

Notice that only the TWTA-type power amplifiers are shown in Figure 6. This is due to the fact that this type of power amplifier is susceptible to high-voltage breakdown. SSPAs do not have these types of failure modes [158].

3.2.1 Satellite Access Router

Since Internet routing in space is an emerging advancement in satellite communications technology, there is no current standard for the on-board access router's implementation and usage. Therefore, examining a specific example where Internet routing in space will be implemented is necessary. This discussion will focus on the IRIS payload to be carried on the INTELSAT 14 satellite.

The IRIS payload will be capable of interconnecting between the C-band and Ku-band communications payloads on INTELSAT-14. This interconnectivity will allow "flexible reconfigurable IP packet routing," enabling a C-band user to directly communicate with a Ku-band user and vice versa. All of this is to be accomplished without the use of an Earth station relay [106].

In the case of the IRIS payload, the uplink signal received by the satellite will first be demodulated and decoded before being routed by the on-board access router on a packet-by-packet basis (See Figure 7.). The router allows for voice, video, and data packets all to be transmitted simultaneously, thereby more efficiently utilizing each transponder than in the case of a bent-pipe COMSAT [106].

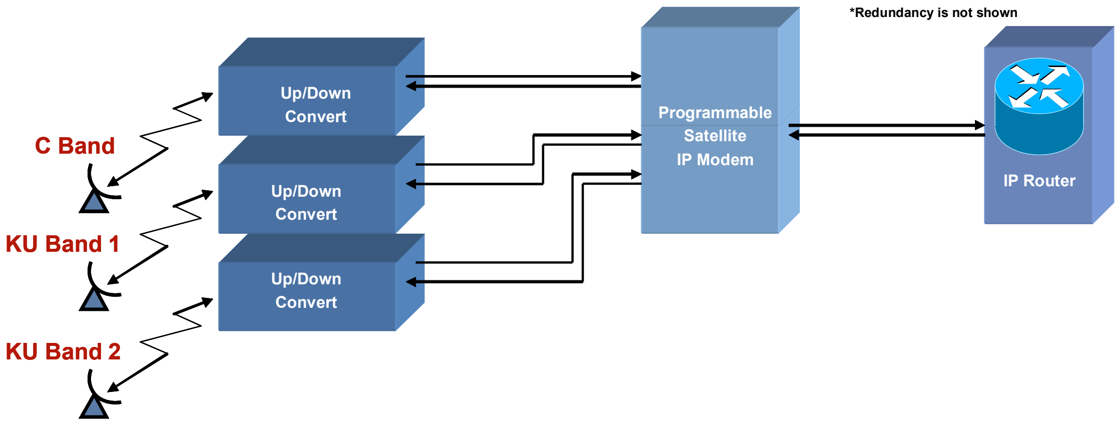


Figure 7. IRIS Payload Diagram

An illustration of the IRIS access router from SEAKR Engineering, Inc. is shown in Figure 8 below [138].

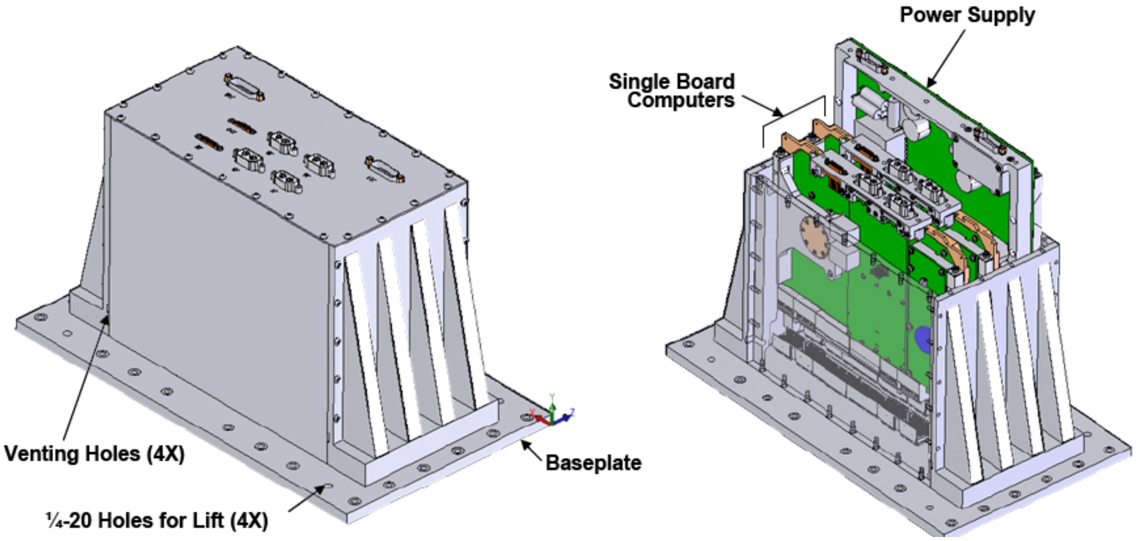


Figure 8. IRIS Access Router Configuration

3.2.2 Transponders

In general, COMSATs carry multiple transponders which are separated in frequency to avoid interference. Bent-pipe transponders receive the incoming information signals, amplify them, frequency-translate them, and separate them into individual transponder channels before re-transmitting them to the required destination. Figure 9 shows the basic structure of a bent-pipe transponder [57]. In order to get the most out of any transponder, multiple signals are usually passed through each transponder using a multiple access scheme. As discussed in Chapter 2, there are several multiple access schemes that can be utilized, such as: CDMA, TDMA, and FDMA, as well as variations of each of these [54, 58].

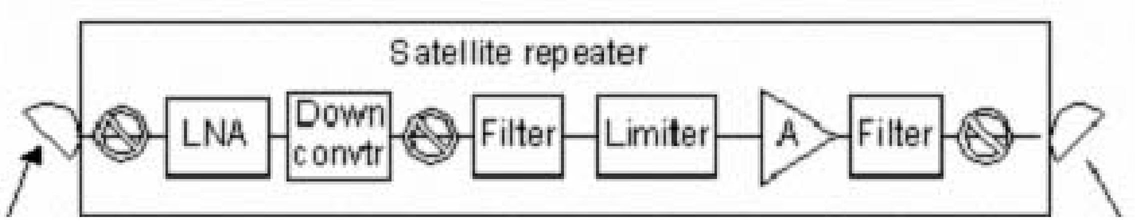


Figure 9. Basic Structure of a Bent-Pipe Satellite Transponder

CDMA allows multiple signals to be sent across each transponder by assigning a unique code sequence for each signal. This type of multiple access scheme is used for secure communications. TDMA allows the entire transponder bandwidth to be used by one user for a limited period of time and once that time is up another user gets their turn. Multi-frequency (MF)-TDMA is popular for use with VSATs. MF-TDMA employs frequency hopping to time and bandwidth utilization. With FDMA, each user is assigned a frequency band. FDMA is used, for example, for point-to-point connectivity [54, 58].

The aforementioned types of multiple accesses are considered fixed assignment multiple access schemes. DAMA may also be used in which bandwidth is allocated based on user demand. Bandwidth allocation is controlled at the Network Operations

Center (NOC) (or on-board the satellite in the case of a satellite with on-board processing capabilities).Combined Free DAMA (CFDAMA) allows unused channels to be accessed in a round-robin manner [84].

3.2.3 TWTAs

As mentioned previously there are generally two types of high power amplifiers (HPAs) that are used on COMSATs, either the TWTA or the SSPA. TWTAs are more efficient than SSPAs; however TWTAs require relatively high voltages whereas SSPAs operate at low DC voltages. Therefore, TWTAs can be exposed to a number of possible failure modes, such as high voltage breakdown [110, 154]. High voltage breakdown failures can cause spurious discharges and even TWT failure [158].

3.3 Earth Station

As stated in the previous section, the satellite's on-board antennas are the main access points to the satellite. The satellite's antennas are used to pass messages between Earth stations, NOCs, and user terminals. Earth stations act as interfaces between the space segments (the satellites) and the terrestrial networks, accessing the satellites' antennas by way of their own antennas on the ground. The Earth stations also act as central hubs for VSAT networks, receiving data from the surrounding VSATs and routing it accordingly. Each Earth station is connected to a network of other Earth stations and the NOC via the satellite. The Earth station network interconnects each Earth station and the users in the terrestrial fixed networks in the region which the Earth station covers. User terminals can access this Earth station network via network access points (NAPs).   Each Earth station is also connected to the satellite's entire network of Earth stations across the globe, allowing interconnections to other Earth stations in regions outside of the coverage area of the local Earth station [81]. See Figure 10 for a breakdown of Earth station access points.

In the case of on-board processing satellites, NAPs can be located directly at the user's location, providing direct access to the NOC. The on-board processor of the satellite is capable of routing user information without the need for sending it first through an Earth station [102].

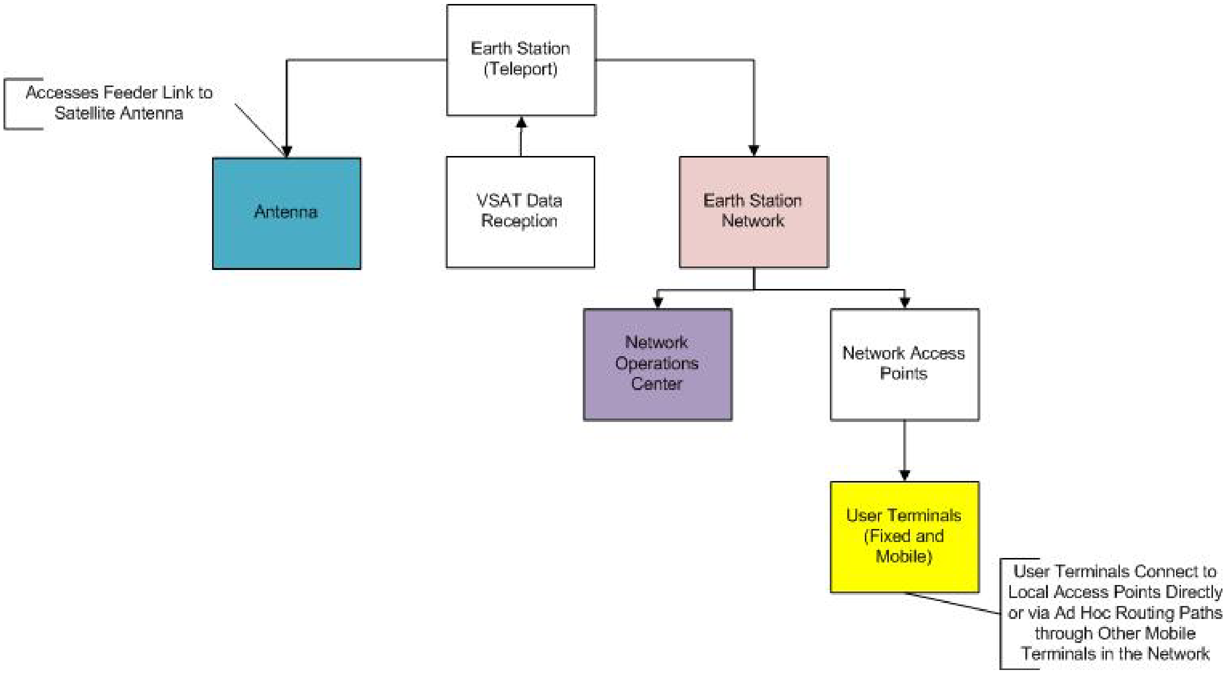

Earth Station (Teleport)
Accesses Feeder Link to Satellite Antenna
Antenna
VSAT Data Reception
Earth Station Network
Network Operations Center
Network Access Points
User Terminals (Fixed and Mobile)
User Terminals Connect to Local Access Points Directly or via Ad Hoc Routing Paths through Other Mobile Terminals in the Network

Figure 10. Earth Station Breakdown Showing Access Point Components

The access point components linked to the antenna were analyzed in the previous section and will not be analyzed here. The Earth station's VSAT data reception capability will be discussed first.

3.3.1 VSAT Data Reception

VSATs access satellites to relay data from user terminals to Earth stations if operating in a star configuration. If operating in a mesh configuration, the data can be relayed from one user terminal to another user terminal via satellite without the need for a centralized Earth station hub. In some cases a combination of these topologies is used. For example, several Earth stations (with VSATs connecting to them in star configurations) can be connected in a multi-star topology. Each star (Earth station and connecting VSATs) is then connected to every other star in a mesh configuration [156]. Refer to Chapter 2 for more details on VSAT network topologies.

3.3.2 Earth Station Network

Each Earth station that is in the coverage area of the satellite is connected to every other Earth station in the coverage area via the satellite, thus creating an Earth station network. This Earth station network is interconnected with the NOC. User terminals access the Earth station network via NAPs. User terminals can access the NAPs directly or by using ad hoc routing paths through other mobile terminals in the network [21].

3.4 Network Operations Center (NOC)

The NOC is connected to each Earth station via the Earth station network, and it controls the network of user terminals. The NOC provides a web-based interface for users which is used in disseminating data, a connection to a terrestrial fiber network through fiber access points for public and private networks, and controls access to services [122]. In addition, the NOC can be utilized to connect user terminals in one beam to user terminals in other beams [24].

Whereas in the case of the IRIS payload, the access router is carried on-board the satellite, in general access routers are located at the NOC. As mentioned previously, access routers route information packets on a packet-by-packet basis to and from user terminals and Earth stations. See Figure 11 for a breakdown of NOC access points.

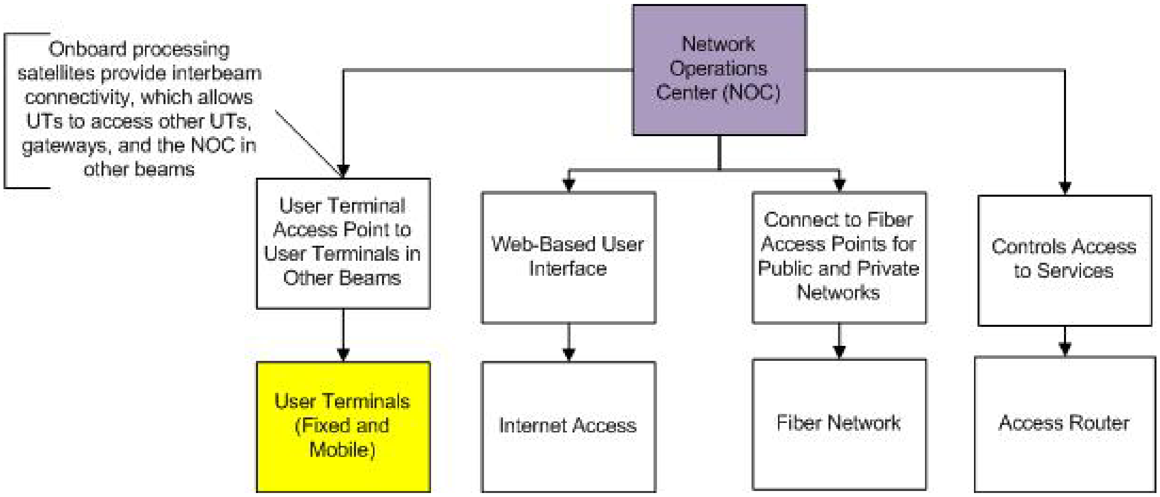

Onboard processing satellites provide interbeam connectivity, which allows UTs to access other UTs, gateways, and the NOC in other beams
Network Operations Center (NOC)
User Terminal Access Point to User Terminals in Other Beams
Web-Based User Interface
Connect to Fiber Access Points for Public and Private Networks
Controls Access to Services
User Terminals (Fixed and Mobile)
Internet Access
Fiber Network
Access Router

Figure 11. Network Operations Center Breakdown Showing Access Point Components

Note that in the case of an on-board processing satellite, the on-board processing payload allows inter-beam connectivity, enabling user terminals in one beam to access user terminals, Earth stations, and NOCs in other beams. These types of satellites do not require the NOC in order to connect to other beams [24].

3.4.1 NOC Access Router

As seen in Figure 11, access routers allow (or deny) access to services. These services can range from dial-up connections to on-demand cable services to wireless Internet access. The NOC access router can also provide access to Internet service provider (ISP) critical services. "Critical services" usually refers to situations in which a "priority dial tone" is provided. These situations typically involve national security and/or emergency preparedness [14, 60]. In addition, the NOC access router helps provide Earth station network security by allowing the NOC manager to control access to services [37].

3.4.2 Fiber Network

The NOC is connected to a private, terrestrial fiber network which provides users and Earth stations access to the Internet or to a private Intranet. The links between the NOC and the terrestrial fiber network are usually protected with network firewalls [21]. Internet (and Intranet) access services, such as web browsing, file transfer protocol (FTP), email, and peer-to-peer, provide user terminals and Earth stations access to public (or private) Internet protocol (IP) networks. In order to provide email services through private IP networks, access to external networks (such as the Internet) is necessary [16]. See Figure 12 for a breakdown of the access points of the terrestrial fiber network.

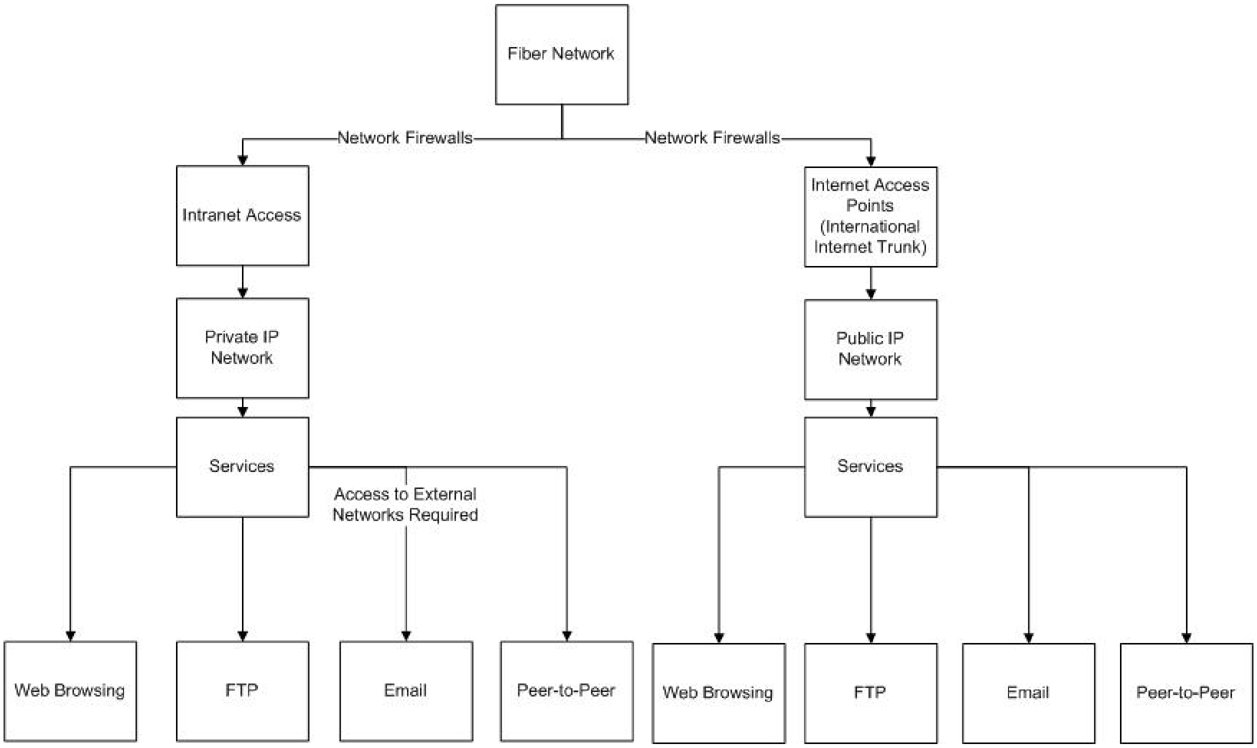


Figure 12. Fiber Network Breakdown of Access Points

FTP is a network protocol for sending data between computers through a network, such as the Internet [64]. Peer-to-peer refers to a network that connects computers via mostly ad hoc connections. This type of network can be used to offer a variety of services, including: audio, video, and data file sharing or sending telephony traffic [123].

3.5 User Terminals

User terminals make it possible to access corporate Intranets, the Internet, and cellular networks from anywhere worldwide by way of satellite connectivity. If a user is not in a satellite coverage region but wants to access a service offered by this satellite, the user can access it through a satellite service provider (SSP). The user will connect to the SSP via a terrestrial IP network, such as the Internet [16]. ISPs, for example, provide Internet access to their customers in remote locations directly or via points-of-presence (PoPs) using wireless links [6]. In these remote locations where there is no access to landlines, user terminals can be connected to standard PC devices to allow access to the desired multimedia services [77].

Mobile user terminals can be used for both cellular network and satellite access. When the terminal is within range of the terrestrial cellular network, the user can connect through the terrestrial network. When the user is outside of the terrestrial network's range, the terminal provides cellular access via satellite connectivity [77]. See Figure 13 for a breakdown of user terminal access points.

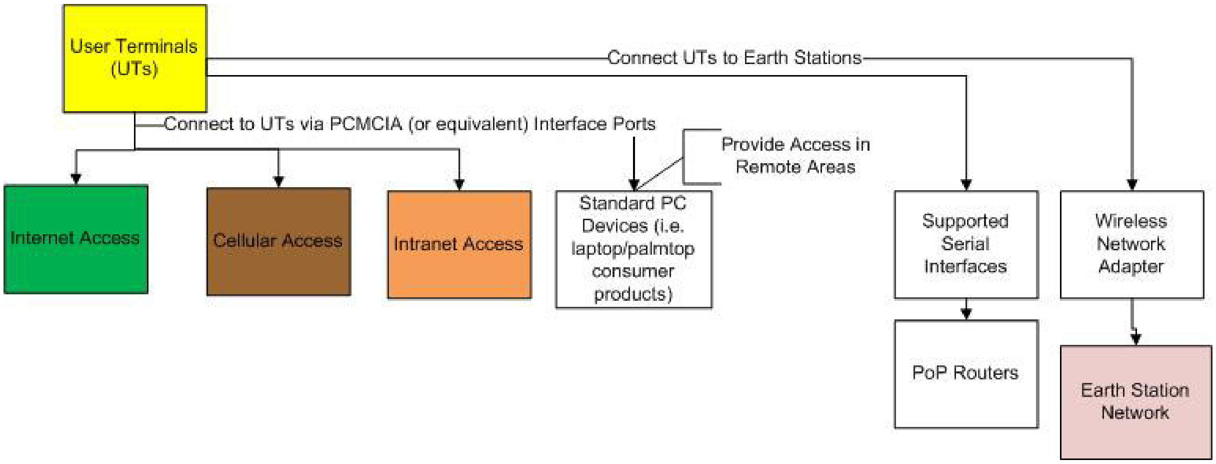

User Terminals (UTs)
Connect UTs to Earth Stations
Connect to UTs via PCMCIA (or equivalent) Interface Ports
Provide Access in Remote Areas
Internet Access
Cellular Access
Intranet Access
Standard PC Devices (i.e. laptop/palmtop consumer products)
Supported Serial Interfaces
Wireless Network Adapter
PoP Routers
Earth Station Network

Figure 13. User Terminals Breakdown Showing Access Point Components

3.5.1 Wireless Network Adapter

As mentioned previously, user terminals can connect to local Earth station NAPs directly. These connections may be made through a wireless network adapter at the user location. The network adapter controls access rights and provides network services [44].

3.5.2 Points-of-Presence (PoPs)

A PoP enables users to access company Intranets, the Internet, and cellular networks through a local phone number or a dedicated landline [107]. PoP routers provide access points for user connections. Users can connect to the PoP routers with a supported serial interface. Access to the router can be provided by one of many protocols, such as: high-level data link control (HDLC), link access procedure balanced (LAPB), or point-to-point protocol (PPP) [77]. See Figure 14 for a breakdown of the PoP access points.

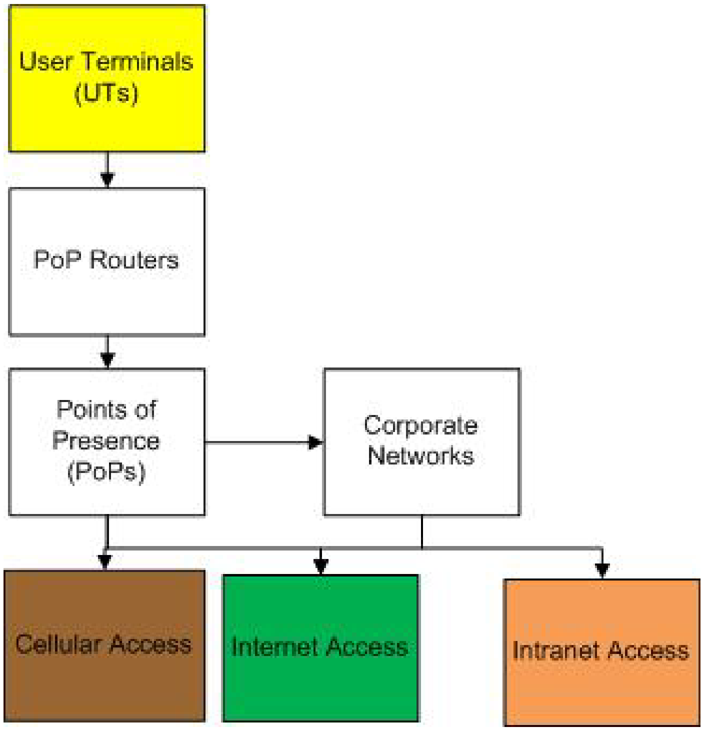


Figure 14. Points-of-Presence Access Points Breakdown

HDLC is a “bit-oriented synchronous data link layer protocol”. It is used to transfer data packets between nodes in a network regardless of packet contents. HDLC provides connection-oriented and connectionless protocol services. Connection-oriented protocols associate traffic flows with an integer connection identifier which makes network switches faster. An example of a connection-oriented protocol is transmission control protocol (TCP)/IP. Connectionless protocols allow messages to be sent between two network nodes without prior arrangement of the transmission. An example of a connectionless protocol is IP. HDLC is typically used for point-to-point communications using asynchronous balanced mode (ABM). ABM supports peer-to-peer communications [79].

LAPB is a bit-oriented data link layer protocol derived from HDLC. It is in the X.25 protocol stack. X.25 is a network layer protocol for packet-switched wide area network (WAN) communications. X.25's major use is in processing credit card transactions and for automatic teller machines (ATMs). LAPB ensures that packets are free of errors and in the right order sequentially [103].

PPP is a data link layer protocol that is typically used to make direct connections between two network nodes via a land line or cellular telephone. Most ISPs use PPP for dial-up Internet access. PPP works with a variety of network layer protocols, such as IP [127].

3.5.3 Standard PC Devices

Portable user terminals make multimedia services accessible anywhere in the world. User terminals can be connected to standard PC devices to allow users in remote locations access to these services. The user terminal to PC device connection is made via personal computer memory card international association ((PCMCIA) or equivalent) interface ports [81]. The PCMCIA interface is designed for laptop computers. All PCMCIA (or simply PC) cards use a 68 pin dual-row connecting interface. They can have either a 16- or a 32- bit interface [121].

3.6 Summary

Each piece of a typical space system, to include the satellite, the Earth stations, the NOC, and the user terminals, has been broken down to the component-level. Possible access points for attackers were determined in each. Now an assessment of the vulnerabilities associated with these access points can be made.

IV: Results

4.1 Introduction

The multitude of vulnerabilities associated with a space system's access points will be presented and analyzed, beginning with those of the space segment (or satellite). From this analysis, the most vulnerable component of each segment (space, Earth, and user) of the space system will be determined. A specific example relating to an emerging space system, IRIS, will present a possible attack methodology for this system as well as other similar systems. The information provided in this chapter serves to warn developers of future space systems of the susceptibility of their systems to the types of attacks mentioned and the need to take steps to prevent these attacks from occurring.

4.2 Space Segment Vulnerabilities

As mentioned in the previous chapter, in regards to a typical Earth-orbiting satellite, there are three access points which may be susceptible to vulnerabilities. These are the antennas, the transponders, and the TWTAs. In addition, in relation to the emerging IRIS payload to be carried on INTELSAT 14, the on-board access router may also be considered a vulnerable access point.

4.2.1 Satellite Antenna Vulnerabilities

The satellite's on-board antennas and the RF links being sent to and from them may be susceptible to both environmental and human factors. These factors can degrade antenna operations intentionally or unintentionally. The causes of unintentional antenna performance degradation can include: unintentional RF interference from the side lobes of an adjacent satellite, due to equipment error, due to human (operator) error, from the satellite's own or another nearby Earth station, and ionospheric interference during solar max; frequency spectrum congestion; multipath; and physical damage caused by the surrounding environment. The causes of intentional satellite antenna performance degradation include: intentional RF interference (i.e. RF jamming), spoofing (or intrusion), meaconing (described below), and deliberate physical attack.

When a signal is masked by another RF signal or by natural RF emissions, such as during solar max or emissions from other on-board equipment, this is deemed unintentional interference [27]. An illustration of antenna side lobe interference is shown in Figure 15.

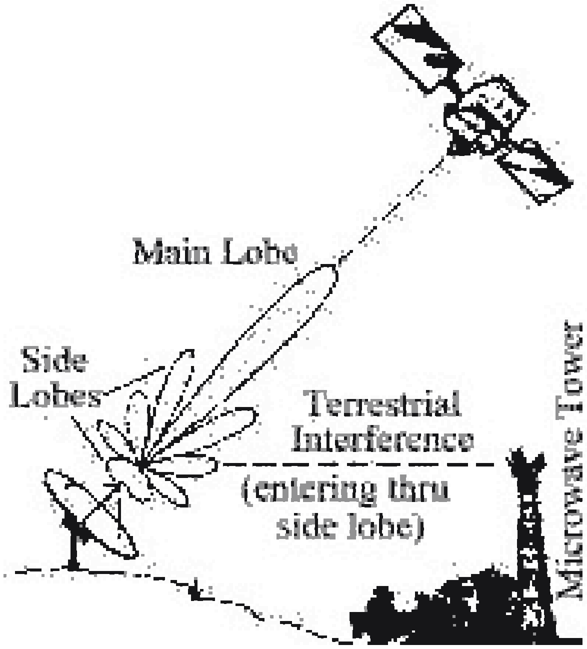


Figure 15. Antenna Side Lobe Interference Illustration [118]

An Earth station that is located nearby the satellite's Earth station could be transmitting at the same time as the satellite's Earth station. RF interference from the nearby Earth station's antenna's side lobes could reach the satellite antenna at the same time as the intended signal, thereby causing interference with the intended signal if the two signals are of the same frequency. This side lobe interference can also be caused by an adjacent satellite's antennas [118]. Antenna pointing errors are a main contributor to side lobe interference. These pointing errors can come from misalignment, foundation settling, spacecraft station-keeping or wind deflection among other factors. An error in antenna pointing results in an increase in antenna gain in the direction of an adjacent satellite. Signals from the adjacent satellites can then interfere with the intended signal [28]. Also, notice from Figure 15 that RF interference from terrestrial sources, such as microwave towers, can cause interference in the signal being transmitted to the satellite by entering through the signal's side lobes.

As can be seen in Figure 16, an antenna's main lobe contains the majority of the beam power. Typically, the side lobes have at most 18 decibels less power than the main lobe. However, the side lobes still radiate strong enough to cause signal interference.

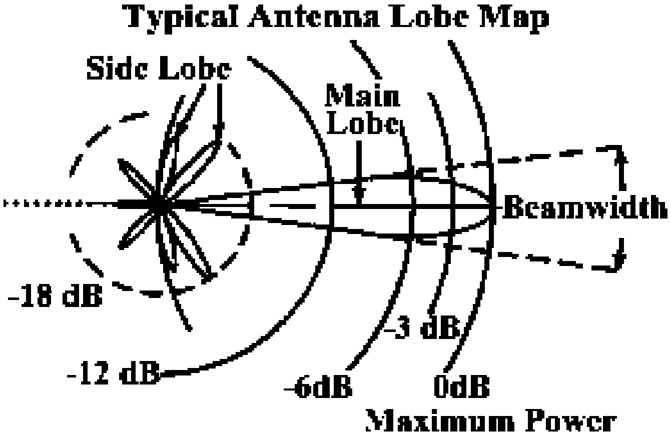


Figure 16. Typical Antenna Beam Pattern [118]

Decibels represent a power ratio. They express how many times more or less power is contained in a signal (in this case, the side lobes), compared to a certain reference signal (in this case, the main lobe). Decibels are defined by the following equation:

dB = 10 * log10(P2/P1) [Equation 1]

log10 = logarithm, base 10

P1 = the power of the signal we are interested in (from the side lobes)

P2 = the power of the reference signal (from the main lobe)

When the spring and fall equinoxes occur each year, the Sun crosses the equator and passes directly behind each satellite in the GEO belt (See Figure 17.). This causes the main beam of the Earth station receive antenna to be in direct line-of-sight with the Sun, causing Sun outage. The Earth station receive antenna picks up the Sun's interference, which overwhelms the satellite signal resulting in the Sun's noise being the only thing heard at the receive end. Sun outage lasts for approximately ten minutes [118].

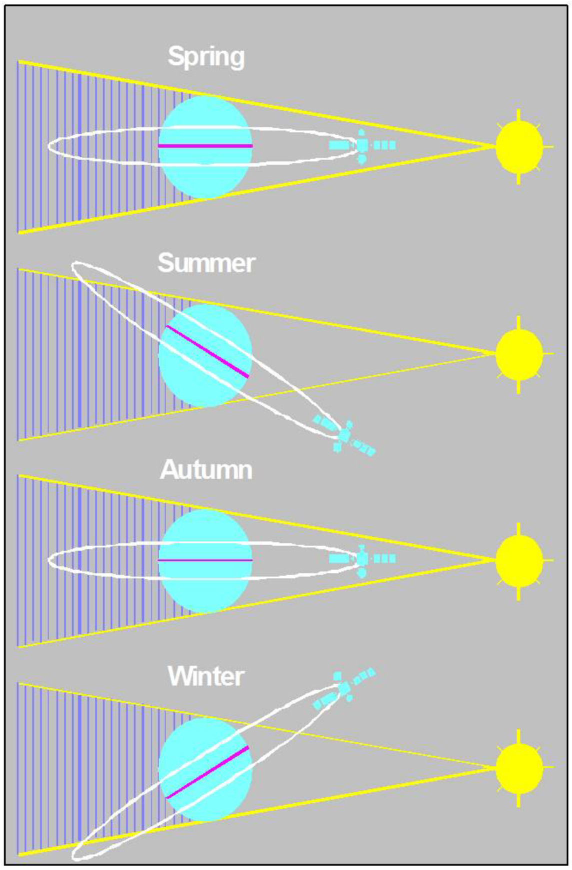


Figure 17. Sun Outage Illustration [104]

Since bandwidth is in high demand and the frequency spectrum is limited, the spectrum is congested with users. Previously unused portions of the frequency spectrum, such as the Ka-band, are beginning to be used in emerging systems in order to meet demand. Also, satellites are employing frequency reuse techniques, such as dual-polarization and spot beams. The International Frequency Registration Board (IFRB) (formerly International Telecommunication Union (ITU)) is in charge of allocating this frequency spectrum to different users. Interference can occur when simultaneously transmitting satellites (or Earth stations) are using frequencies that are too close together, implying that the channel spacing (or frequency guard bands) is not wide enough. Insufficient channel spacing can cause overlapping of frequency sidebands and carrier frequencies of adjacent satellites (or sidebands of adjacent satellites can cause interference with the carrier frequency of the satellite in question). The sidebands are bands of frequencies that are higher or lower than the carrier frequency that contain energy. These sidebands result from the signal modulation process. Congestion of the frequency spectrum causes difficulty in discriminating the intended signal from the adjacent satellite (or Earth station) signal and can result in interference due to slight frequency shifts or phase shifts due to ionospheric reflection. Ionospheric reflection is a bending of the signal back toward the Earth, which depends on the signal's frequency, angle at which the signal is sent traveling through the ionosphere (i.e. angle of incidence), signal polarization, and ionospheric conditions. These ionospheric conditions include electron density, which indicates the amount of ionization in the atmosphere. Atmospheric ionization increases with increases in solar activity [66].

Multipath occurs when RF signals reflect or refract off of objects as they travel from the satellite to the Earth station and vice versa. These objects can include structures surrounding the receive antenna such as buildings, as well as objects in the atmosphere such as ions (as described in relation to ionospheric reflection above). The transmitted signal can also bend due to changes in refractive index as it travels through the atmosphere. Passing through various mediums also causes a change in signal velocity. Refractive index is a measure of how much the speed of light decreases when traveling through a particular medium, such as the atmosphere. Multipath can cause signal fading due to the reflected signal, which will reach the antenna after the intended signal, interfering with the intended signal. The combined received signal (intended plus reflected) suffers from time-varying fading [57]. See Figure 18 for an example of multipath fading.

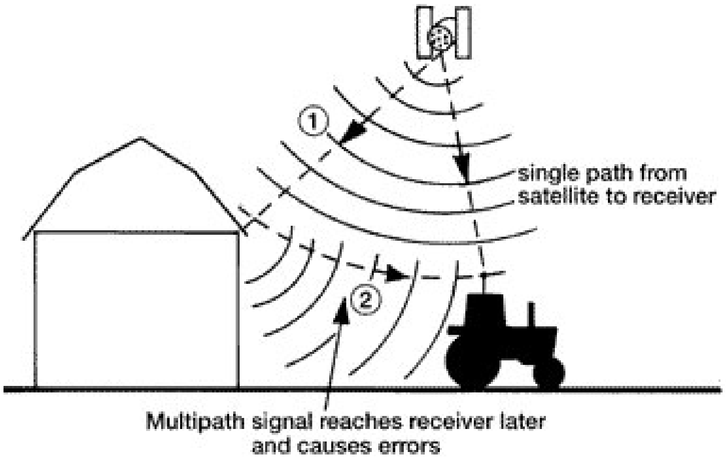


Figure 18. Multipath Signal Fading Illustration [31]

When a signal is refracted, there is a change in signal polarization. When the signal is reflected, the polarization is reversed (for example from right-handed circular to left-handed circular polarization). In this case, when the reflected and intended signals meet at the antenna, they will cancel each other. The two signals will only cancel each other completely if the polarization was fully-reversed in the reflected signal and if the amplitudes of both of the signals are equal. Otherwise, the multipath signal will only partially cancel the intended signal. If the multipath signal goes through two reflections before arriving at the antenna, it will have reversed its polarization twice resulting in the multipath signal ending up with the same polarization as the intended signal. If these two signals converge at the antenna, the two signals will add causing the amplitude of the total received signal to be increased. These variations in signal amplitude can cause problems for the automatic gain controller (AGC) which is supposed to keep the signal levels constant [119].

With the antennas being one of the major objects protruding from the satellite's surface, they are obviously one of the most vulnerable of the satellite's components to physical damage. This damage could come from any number of objects in the space environment, to include space debris and possibly even meteoroids. Also, the space environment itself may cause damage to the antenna. Outgassing of materials may occur, as well as damage caused by the extreme temperatures. Outgassing is the slow release of a gas that was trapped in a material. The gas can be released from cracks or impurities in a metal, as well as from sealants, lubricants, and adhesives. Outgassing increases with increases in temperature. In addition, the sun releases highly-energetic particles into the space environment during solar flares and coronal mass ejections (CMEs) which can result in surface charging. Solar flares are violent explosions in the Sun's atmosphere which causes a surge of high-energy particles to be released resulting in a proton storm. A CME involves the Sun ejecting a plasma from the solar corona. The plasma consists of mainly electrons and protons.

The low-power signals coming from satellite antennas, like any RF transmission (including those being sent to the satellite), can be jammed. Jamming involves intentionally masking a target signal with another RF signal. The signals coming from the satellite can be jammed using very little jamming power. Jamming can result in signal degradation or total signal loss [23, 27]. Please refer to Section 2.6 for several examples of satellite jamming events that have occurred in the past.

Spoofing involves intentionally transmitting false information to the COMSAT in order to "deceive or computationally overwhelm" the satellite, thereby overriding the intended signal [27]. The objective of spoofing is to send the receiver a malicious signal that overpowers the intended signal, fooling the receiver into using a false signal for further processing. The composite signal received at the antenna is that of the intended signal plus the spoofed signal plus the signal noise. Spoofing is only possible on satellites with on-board processing capabilities, because it is at the analog-to-digital (A/D) conversion stage that the spoofed signal overrides the intended signal. Most on-board processing satellite receivers have automatic gain control which is important for a spoofing attack to be successful (See Figure 19.). Spoofing is more serious than jamming, because the attacker can take control of the receiver with spoofing, while in the case of jamming the attacker only causes signal degradation [15].

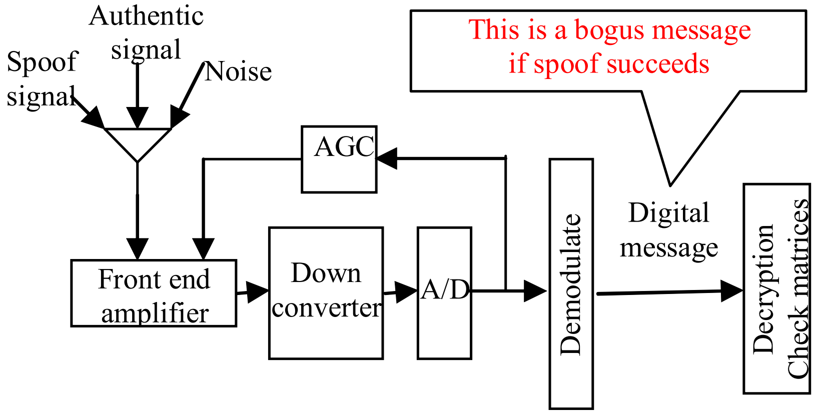


Figure 19. Spoofing Vulnerability Illustration [15]

Satellite side lobe energy can be received (via a high gain antenna) by an unintended target and retransmitted. This is termed meaconing. Meaconing causes the signal to be delayed in reaching its target. Should a disgruntled employee obtain access to the satellite and its antennas before launch, the employee could connect a delay device (such as a wideband analog-to-digital or digital-to-analog converter or a digital delay line) to the antenna. This would be somewhat easier than trying to capture the satellite signal, however the likelihood of no one noticing the delay device prior to launch is very low. The delay device attack is more likely to take place at an Earth station [27].

Intentional physical attack of a satellite became a very real possibility as the U.S. watched China's first successful anti-satellite missile test take place in January 2007. On 11 January 2007, a ground-based missile destroyed an obsolete Chinese weather satellite. According to senior U.S. officials, in 2006 China tried to "blind American satellites" with lasers. These types of attacks are feasible for low Earth orbit (LEO) satellites, but medium Earth orbits (MEO) and GEO orbits are likely out of range. As these attack technologies advance in the years to come, the capability to physically damage an in-orbit COMSAT and knock out critical communications components becomes closer to reality [114].

4.2.2 Transponder Vulnerabilities

If an attacker's signal is sent to a bent-pipe transponder from the satellite's antenna and the signal is at the correct carrier frequency, it will be processed along with the intended signals and re-transmitted along with them down to the receiver. The attacker's signal may obscure the intended signal at the receiver if it has a great enough signal-to-noise ratio (SNR) making the receiver unable to discern the intended signal from the attacker's signal. In addition, the attacker's signal raises the noise floor (i.e. the background noise) of the transponder and causes a reduction in the SNR of all of the intended signals. If an intended signal gets lost in the background noise, it cannot be recovered [118, 130].

Typically attackers will utilize a narrowband, high SNR, un-modulated carrier because these types of carriers can have a greater SNR than modulated carriers. By using an un-modulated carrier, the attacker achieves the raised noise floor of the intended signal. Therefore, the attacker's signal will degrade or completely cut-off communications across the transponder [130].

In order to carry multiple signals on a single carrier frequency (i.e. a single transponder) and more efficiently utilize the limited bandwidth available, differing polarizations are used. Polarization is a property of electromagnetic (EM) waves which describes the orientation of the oscillations in the plane perpendicular to the direction in which the EM wave is travelling. Linear polarization consists of either vertical or horizontal polarizations which are used in conjunction with each other on a single carrier frequency to differentiate between signals. Circular polarization consists of either right-handed circular or left-handed circular polarizations depending on which way the EM wave oscillates about the perpendicular plane. Right-handed and left-handed circular polarizations can also be used to differentiate between signals on the same carrier frequency. If an attacker transmits to the satellite with an improper polarization setting (i.e. when the attacker's polarization does not exactly match the polarization being accepted by the satellite antenna feed horn, the result is excess power creeping onto the other polarization which is likely being used by a legitimate customer. This effect is called cross-polarization, and it can result in interference with the legitimate customer's signal (which is using the opposite polarization on the same transponder) [130].

As mentioned in Section 3.2.2, multiple access schemes are also utilized to enable each transponder to carry multiple signals. CDMA is used for secure communications because it offers protection against frequency jamming and co-channel interference. Co-channel interference is interference from other signals using the same frequency channel. However, if the intended signal's modulation, frequency, and code are known, jammers can concentrate all their power at that particular frequency to corrupt the intended signal. If the jammer transmits at a power high enough to compensate for the CDMA jamming resistance advantage, the jammer could interfere with the intended signal [62, 124]. TDMA avoids interference between user signals by strictly following timeslot schedules. As discussed in Section 2.4.1, FDMA is susceptible to intermodulation (IM) products. IM products can cause interference and noise, as well as reduce the power output of the satellite that is available for communications. Also, FDMA is vulnerable to co-channel interference if the channel spacing is not sufficient [62].

Satellites may use spread spectrum which is intended to increase resistance to jamming by spreading the signal out by way of a spreading code (for example, a unique pseudorandom number sequence). Because the signal is spread across a wide bandwidth, spread spectrum is able to lessen multipath signal fading and interference. The spreading code is typically protected via encryption. Only users with the encryption key can obtain the spreading code which enables them to de-spread the signal. If an attacker gains access to the signal's spreading code, the attacker could spoof other users of the signal [62, 128].

If linear feedback shift registers (LFSR) are used to create the spreading sequences for spread spectrum (codes for CDMA) and the pseudorandom number generator (PRNG) seed (or start) values are known, jamming of a spread spectrum or CDMA signal becomes relatively easy. The PRNG seed values are the key to the PRNGs and can be obtained through cryptanalysis or theft [49].

4.2.3 TWTA Vulnerabilities

As was mentioned previously in Section 3.2.3, TWTAs are susceptible to high voltage breakdown failures that can result in spurious emissions and TWT failure. Spurious emissions are unintentionally created RF signals which could interfere with the intended signal. This high voltage breakdown in the TWTA is referred to as multipaction, or high voltage breakdown in a vacuum. Multipaction is generally a product of the transmitted frequency and electrode separation [41]. Multipaction occurs typically in vacuum environments, such as that inside a TWTA. Charged particles inside the gap between the TWT electrodes oscillate due to a strong, external electric field. RF energy, such as that of the signal being passed through the TWTA, puts stress on these charged particles. Every time the particles hit the walls of the gap other charged particles are released. More and more charged particles are released as more and more of them hit the walls of the gap eventually creating enough charged particles to cause a spark which can cause hardware damage [76, 113].

4.2.4 Satellite Access Router Vulnerabilities

The on-board access router communicates with and is commanded by the satellite's on-board computer. The two devices are connected via the router's console interface. The satellite's on-board computer operates all the other spacecraft mechanisms as well. Almost all current computing systems utilize digital technology which is vulnerable to interference from ionic disturbances and radiation, for example. Exposure to these elements of the space environment could result in malfunctions of the on-board computer and thus the satellite systems that it commands [20]. In fact, many times space system on-board computers use older technology and older software. These systems are operating in orbit for ten to fifteen years. By the time they are mission-ended, the on-board computing capabilities are out-dated. In April 2008, hackers are thought to have loaded a Trojan horse in the computers at Johnson Space Center in Houston, Texas. These hackers then used the Trojan horse to access the uplink to the International Space Station (ISS) and disrupt certain operations on-board, such as email. The attack was helped by the fact that ISS on-board computers are running older software for which security fixes are no longer available. If this is true, and such an attack can be executed against the ISS, all earth-orbiting satellites may be at risk. If a hacker could gain access to the satellite Earth station to plant a virus on the Earth station's computers, then the hackers could access the satellite and impede or disrupt communications across the satellite [75]. In addition, bugs in on-board software in both the on-board computer and on-board access router could render one or both of these components unable to complete their respective missions.

In reference to the IRIS payload that is planned to be carried on-board INTELSAT 14 that has been discussed in previous examples, its use of Internet protocol (IP) packet routing may cause the satellite to be susceptible to all of the vulnerabilities of IP packet routing [106]. IP packet routing was intended to make routing as easy as possible. A packet routed with IP could be accessed, re-routed, or copied by anyone connected to the network [112]. IP networks are susceptible to spoofing, sniffing, and session hijacking. Spoofing indicates that an attacker's machine on the network can impersonate as another legitimate user's machine. Sniffing involves an attacker listening in on communications between other legitimate users. An attack in which the attacker uses spoofing to take over an existing communications session and acts as one of the former communicating parties is termed session hijacking [11].

4.2.5 Space Segment Vulnerabilities Summary

Of the satellite access points, the antennas are the outermost, and thus are the most vulnerable to attack. All signals must pass through the antennas first before being passed to the other satellite access point components. Therefore, the satellite antenna will be the first component compromised before attacks can be placed against any of the other components such as the transponders, TWTAs, or on-board access router.

4.3 Earth Segment Vulnerabilities

As mentioned in Section 3.3, the Earth stations interface between the satellites and the terrestrial networks via their own antennas on the ground. The Earth stations serve as central hubs for VSAT networks, and they are connected to a network of other Earth stations and the Network Operations Center (NOC) via the satellite. User terminals access the Earth station network via network access points (NAPs). These access points and connections not only serve to provide satellite communications services across the globe, but they also make the Earth station network vulnerable to attack.

The NOC controls the network of user terminals. It provides a web-based interface for users, a connection to the terrestrial fiber network, and controls access to services with the help of the NOC access router. In the case of the IRIS payload, the satellite on-board access router carries the responsibility for controlling access to services. Since the NOC has additional functions on top of those of a typical Earth station, there are other supplementary vulnerabilities that could make the NOC susceptible to attack.

4.3.1 Earth Station Antenna Vulnerabilities

Earth station antennas are susceptible to some of the same vulnerabilities as the satellite antennas, such as RF jamming, interference (co-channel, IM product, and antenna side lobe), multipath, environmental conditions, and deliberate attack. However, since these antennas are located on the ground, there are also different vulnerabilities associated with these systems.

Like satellite antennas, Earth station antennas are susceptible to damage due to environmental conditions. However, the differences in the Earth and space environments bring about different types of vulnerabilities in Earth station antennas. Since Earth station antennas need to have a clear view of the on-orbit satellites, many times they are located on rooftops. This particular location makes these antennas susceptible to damage or destruction by extremely strong winds. If antennas are located in regions that are prone to storms involving high winds, such as hurricanes or tornadoes, placing them on building rooftops might not be ideal.

Since Earth station antennas protrude from buildings in order that they can be keep the satellites in view, they are also the most visible and thus the most vulnerable components of Earth stations to physical attack. The only weapon an attacker would need to damage or destroy an Earth station antenna would be a high-powered rifle. Most metal parabolic dish antennas can withstand a number of bullet impacts before any degradation in performance occurs. However, fiberglass antennas are more vulnerable to bullets. They will begin to break with the first bullet impact, causing degradation in performance right away. If the attackers knows to instead attack the antenna's feed horn, just a few rounds of bullets could knock out communications across any antenna. Located at the focal point of the antenna dish (reflector), the feed horn transmits RF signals between the transmitter/receiver and the reflector. The feed horn selects the polarization of the received signal and helps to attenuate co-channel interference. In addition, Earth station antennas could also be vulnerable to vehicle collisions. If an attacker can gain access to the Earth station facility, they could easily just run their vehicle into a ground-mounted Earth station antenna, causing damage and possibly knocking out communications [32].

If an attacker is able to gain control of the telemetry, tracking, and control (TT&C) link from the operator on the ground to the satellite, there are several possible attacks that could take place and may result in loss of control of the satellite. For example, if multiple Earth stations were used to send a series of tones to a satellite transponder and then observe the differences in phase of the signals returning from the satellite, the spoofer could transmit false responses to the satellite to cause incorrect orbit determination. Also, the attacker could send commands to the satellite via this link or record commands from the TT&C station to be replayed later and cause duplicate actions to take place on-board the satellite. Since spare satellites are not always tracked by TT&C, these satellites are vulnerable to takeover. Then the attacker could move or use them as they like [155].

In addition to antenna side lobe interference from nearby Earth stations, as discussed previously in relation to satellite antennas, other forms of terrestrial interference can cause degradation in the Earth station communications signal. This interference can come from such devices as radars or radar altimeters which emit pulsed signals. This type of interference can cause symbol errors in the intended signal. When there exists a long series of consecutive symbol errors, the result may be receiver failure. Long-pulse-width interference causes many consecutive symbol errors. As the number of consecutive errors increases, the sensitivity of the antenna system to interference increases [133]. Electromagnetic pulse (EMP) energy, such as that emitted during a nuclear detonation, is also an interference concern. EMP has far-reaching effects. It can cause performance degradation up to 6,000 kilometers from the detonation site. EMPs are roughly 1,000 times more intense than radar pulses and are capable of temporarily halting communications [65]. EMP could even cause interference to a satellite antenna should a nuclear weapon be launched and detonated in space. The weapon does not necessarily have to impact the satellite to cause damage to communications. The EMP energy could degrade performance on any nearby satellites.

Earth station antenna interference can also come from terrestrial sources such as radio towers, as illustrated in Figure 15. A radio broadcast can enter the Earth station antenna system at the intermediate frequency (IF) level of the Earth station due to a bad connection between the Earth station baseband equipment (such as modems and multiplexers) and the Earth station RF equipment (such as low noise amplifiers (LNAs) and TWTAs) (See Figure 20.). The radio broadcast would then be transmitted to the satellite, causing interference with the intended signal.

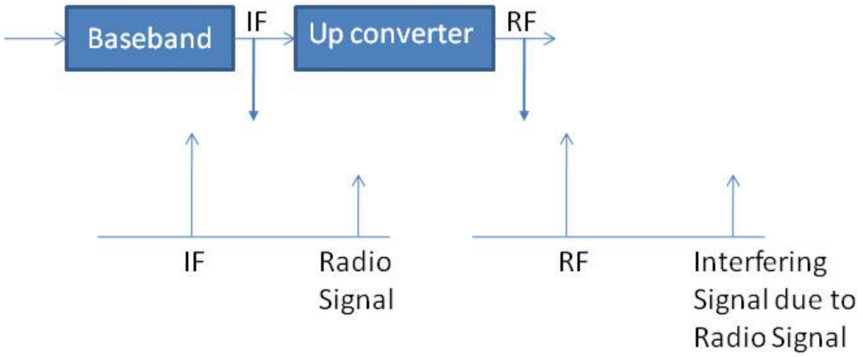


Figure 20. Radio Frequency Interference Illustration [135]

4.3.2 VSAT Central Hub Vulnerabilities

An important part of an Earth station's mission as a VSAT central hub is ensuring that user terminals connecting to the Earth station network are authorized users. Bandwidth is typically dynamically allocated to user terminals in TDMA VSAT networks (for example, mesh networks). As a result of this dynamic allocation, control data must be sent to each of the user terminals requesting bandwidth. This control information can be exploited by attackers. If the attacker can obtain a VSAT terminal and spoof the device ID, the attacker can then insert the rogue device into the network [86].

In the case of a star topology VSAT network (refer to Section 2.3.9 for details), the VSAT central hub is a single point of failure. The central hub acts as a control center and traffic gateway for all of the VSATs that are connected to it. Since the central hub is the only connection these VSATs have to the rest of the Earth station network, if the central hub is somehow compromised, then the network of VSATs connected to it will lose communications. On the other hand, mesh topology VSAT networks do not have this single point of failure vulnerability because mesh networks have a way of ensuring messages reach their destination despite any node failures. If an intermediate node along the route to the message's final destination node has failed, the mesh VSAT network is capable of re-routing the message along an alternative route to ensure message delivery [159].

VSAT networks are also vulnerable to eavesdropping. If an attacker with an understanding of data link layer protocols purchases a VSAT user terminal, the attacker can eavesdrop data intended for other legitimate users. In order to listen in on data intended for others, the attacker must tune the terminal to the correct frequency (and timeslot in the case of TDMA networks) and "reverse engineer the VSAT's embedded code" [152]. Eavesdropping can result in the compromise of passwords and other secret information.

Due to the burst-like nature of VSAT data, fixed-assignment multiple access schemes such as FDMA and TDMA are not typically utilized because they do not provide efficient bandwidth utilization in this situation. Therefore, some VSAT terminals employ random access protocols, such as Aloha and its variations (Refer to Section 2.3.9 for more details on the Aloha random access protocols). The Aloha protocols rely on each VSAT terminal being able to "hear" its own transmissions, and therefore these protocols are not used in VSAT star topology networks. VSATs in star networks cannot hear their own transmissions due to the differing bit rates used to transfer data on the inbound versus the outbound carriers [74]. Since the Aloha protocol allows any user to transmit at any time, there is a vulnerability to loss of packets due to collisions with other users' packets. The probability of packet collision is proportional to the traffic (or the duty cycle which is the fraction of time that the channel is active) [3]. Due to the fact that the Aloha protocols are contention-based, they may be unstable during periods of high-traffic loads. When a channel becomes unstable, an increased number of packets are sent due to retransmissions and the number of successfully delivered messages diminishes [74].

4.3.3 Earth Station Network Vulnerabilities

The Earth station network is vulnerable to the same vulnerabilities as each individual Earth station, including all of the Earth station antenna vulnerabilities. The Earth station network is susceptible to natural disasters, as well as intentional attacks, like each Earth station. Continuing with the example of the INTELSAT 14 satellite (which is planned to carry the IRIS payload), the details of the INTELSAT Earth station network and network vulnerabilities will be presented.

INTELSAT owns and leases thirteen Earth stations across the globe in the following locations: Ellenwood, GA; Napa, CA; Fillmore, CA; Hagerstown, MD; Castle Rock, CO; Paumalu, HI; Riverside,CA; Fuchsstadt, Germany; Clarksburg, MD; Kumsan, South Korea; Fucino, Italy; Perth, Australia; and Pretoria, South Africa. The Ellenwood, GA (i.e. the Atlanta Teleport) Earth station is the primary Atlantic Ocean Region (AOR) gateway for INTELSAT. This will likely be the Earth station used by INTELSAT 14, as it will be located in the AOR and this is the same Earth station used by IS-1R. INTELSAT 14 will be replacing IS-1R in its same orbital location. Figure 21 is a general overview of an INTELSAT Earth station configuration.

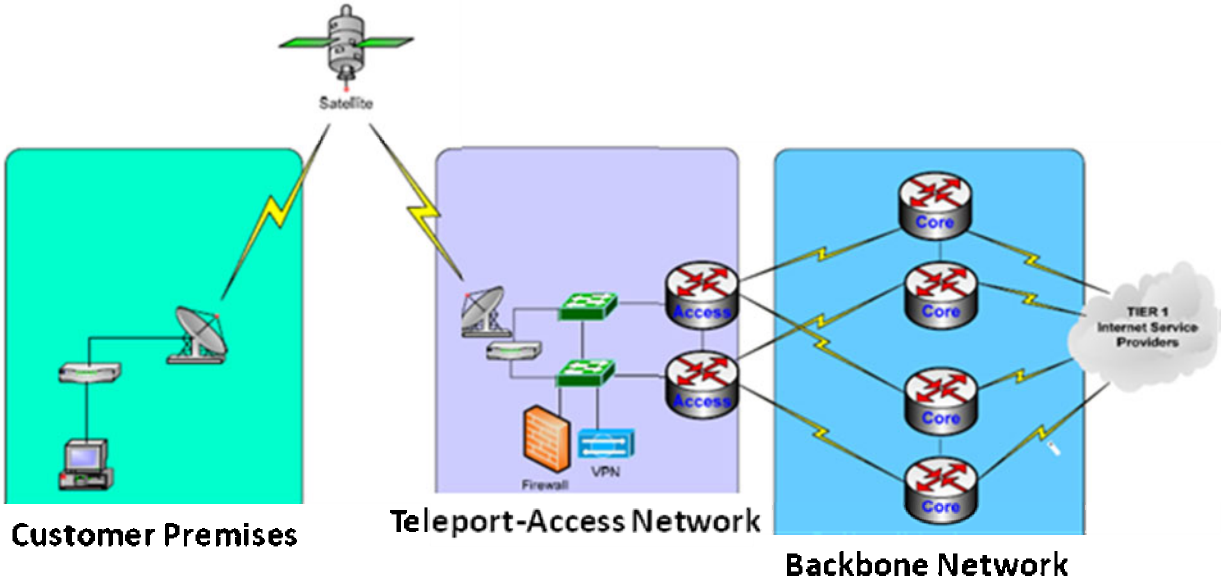


Figure 21. INTELSAT Earth Station Configuration Overview [87]

From Figure 21, it is important to focus on the main components, such as the access routers and the connection to the Internet backbone. These components will be discussed in a later section on the NOC. However, they are important components to consider in this vulnerability analysis.

INTELSAT's Earth station network utilizes secure shell (SSH) and IP security (IPsec) for securing communications [87]. However, SSH has several vulnerabilities associated with it that could allow an attack on the network. A malformed protocol message can cause buffer overflows or denial of service (DoS) in the firewalls and virtual private networks (VPNs) that are shown in Figure 21. If a VPN is compromised, the attacker could then gain access to the protected Earth station network [40]. Buffer overflows involve "data fields overflowing and overwriting memory segments for executable code," resulting in an attacker being able to remotely control the VPNs. Denial of service attacks prevent systems from performing routine operations by flooding the systems (VPNs or firewalls) with control messages that can cause them to become overloaded [49].

4.3.4 Network Access Point Vulnerabilities

As mentioned in the previous chapter, network access points connect SSPs and user terminals to the Earth station network via wireless network adapters or fiber connections. A NAP must determine its location and send that information (i.e. its IP address) to a connecting user terminal. In doing so, the NAP along with the rest of the network becomes vulnerable to attack. The NAP location information sent to the connecting user may be intercepted by an attacker who could then use this information to set up a rogue access point. If an attacker is able to intercept the IP address of the NAP, then the attacker can send false address resolution protocol (ARP) responses that include the IP address of the (legitimate) NAP and the media access control (MAC) address of the attacker's rogue device to other legitimate user terminals connected to the network. This will result in the legitimate users updating their ARP tables with the mapping to the rogue access point (in place of the mapping to the legitimate NAP). All future data packets sent from these legitimate users will now go to the attacker's rogue access point and allow the attacker access to sensitive data and an possibly even an access to corporate networks from outside the facilities [67]. This access to corporate networks would require the attacker to install the rogue access point (AP) directly at an active network port inside the company facility; however passing through physical security at most companies is not very difficult [69].

4.3.5 Wireless Network Adapter Vulnerabilities

During normal operations, wireless network adapters (WNAs) receive data packets indicating new networks are present. If an attacker can gain access to these data packets and manipulate them, the attacker can trigger an error condition which could allow the attacker to run programs and access files on the targeted user terminal [53]. Whenever a WNA is active, the user terminal's operating system automatically will look for networks the user has connected to in the past. A user terminal could end up connecting to an attacker's network without even knowing it. "Suppose the attacker provides a rogue AP with a common name (such as a default service set identifier (SSID) of a popular home-office AP, like Linksys)" [139]. Then, a nearby user, who has connected to a similarly-named AP in the past, may mistake the rogue AP for the legitimate, similarly-named AP. This could allow an attacker access to sensitive user data [139]. In the case that a user terminal is already connected to a network, an attacker can force the user to start searching again for available networks by spoofing IEEE 802.11 disassociation frames from the NAP to which the user is already connected. IEEE 802.11 is a set of standards for wireless local area network computer communication. A disassociation frame is sent to a user if the AP wishes to terminate the user's connection. Upon receiving these disassociation frames, the user terminal would disconnect from the NAP and start searching for other available nearby networks. The only piece of information the attacker would need to spoof the 802.11 disassociation frames from the NAP is the IP address of the NAP. The NAP's IP address can easily be obtained from the beacon frames the NAP is required to transmit continuously. The 802.11 beacon frames are management frames that allow user terminals to establish and maintain communications by identifying the presence of APs. The user's search for other available nearby (unencrypted) networks will likely resulting in the user joining the attacker's AP [50].

4.3.6 NOC Internet Connection Vulnerabilities

The NOC web-based user interface implies a connection to the Internet backbone. The NOC can be connected to an Internet backbone provider via a fiber connection. There are several vulnerabilities associated with fiber connections, such as physical vulnerabilities to breakage and vulnerability to the fibers being cut by attackers.

The NOC's Internet connection allows user terminals to access network services remotely. Unfortunately, Internet connections are susceptible to a variety of attacks, such as: spyware, phishing attempts, viruses, backdoors, Trojan horses, and worms, all of which could try to slip into the Earth station network through the NOC Internet connection [109]. Spyware is computer software that is installed on a user's terminal (or the network) without the user's (or network's) knowledge. Spyware can collect user information, install unwanted software, change computer settings, and cause Internet connection problems among other things [148]. Phishing attempts are made to obtain sensitive information. This information is acquired by the attacker pretending to be a known or trusted source in order to fool the user (or the network) into sending sensitive information. A computer virus, like spyware, infects a user terminal (or network) without the user's (or network's) knowledge. A computer virus is capable of copying itself and spreading from one terminal to another. Computer viruses can delete files, damage programs, take up computer memory, cause erratic behavior, and even cause the system to crash [46]. Backdoors can be put in software either during design or via a virus and allow the attacker to gain access or even take control over systems. A Trojan horse can cause just as much damage as viruses, but they do not copy themselves. A Trojan horse acts as if it is a legitimate program when really it is a destructive one. For instance, a Trojan horse can fool users into believing that it is anti-virus software when in fact it actually installs viruses onto the user's terminal. Worms, like viruses, are able to copy themselves and spread the copies to other user terminals without the user's knowledge. Viruses and worms differ in that worms do not attach themselves to existing programs. Also, worms generally harm the network by using up bandwidth, while viruses typically corrupt or modify files on user terminals [46, 47].

4.3.7 NOC Connection to Terrestrial Fiber Network Vulnerabilities

The NOC connection to the terrestrial fiber network has all of the vulnerabilities associated with the fiber connection that were discussed in the previous section. In addition, since the NOC connection to the terrestrial fiber network provides user terminals and Earth stations access to the Internet or to private Intranets, this connection is susceptible to all of the vulnerabilities associated with Intranet and Internet access.

There are over 5,000 known vulnerabilities to Internet connections and more are added every day [129]. Some of these vulnerabilities were discussed in the previous section. In addition, there are variations on the vulnerabilities mentioned in the previous section, as well as operating system specific vulnerabilities. The important thing to remember is that Internet connections present a multitude of vulnerabilities, because the

Internet interconnects people from all across the world, giving access to those that might be trying to attack U.S. satellite systems.

Since Intranets are private corporate networks and not open to everyone, connections to Intranets are subject to a different set of vulnerabilities than Internet connections. For instance, Intranets could be subject to cross-site request forgery (CSRF) attacks and cross-site scripting (XSS) attacks. During a CSRF attack, "the attacker fools the user into loading a web page that contains a malicious request. The attacker then tries to steal victims' identities and privileges to carry out activities such as changing their passwords to gain entrance to Intranets. Attackers can essentially access prior web browser sessions and remain logged into any sites that have been accessed by the user to carry out illicit activities" [80]. On the other hand, during XSS attacks, attackers set up a malicious webpage to masquerade as a trustworthy website, one that likely will not be blocked from the company network. This type of attack can lead to session hijacking and user impersonation, worms, viruses, phishing attacks, and Trojan horses, just to name a few [73, 80]. If VPNs are offered to allow employees in remote locations to connect to the company Intranet, the vulnerabilities associated with VPNs may offer another entry point for attackers to gain access to the private Intranet [80]. These VPN vulnerabilities will be discussed in the following section. Also, there is a susceptibility to domain name system (DNS) rebinding attacks in Java which can allow an attacker to bypass the perimeter firewall and gain access to a corporate Internet. DNS rebinding involves an attack on code embedded in web pages, such as Java or JavaScript. DNS rebinding improves the ability of Java (or JavaScript) to infiltrate private Intranets. First, the attacker must register a domain, which is then added to the DNS server controlled by the attacker. The DNS server responds with time to live (TTL) parameter sets. The first server response has the IP address of the server with the malicious code. The next set of responses will contain IP addresses from targeted private Intranets. By iterating, the attacker is able to scan the Intranet or perform other malicious acts [56, 93]. This is just one example of the vulnerabilities associated with different coding languages being embedded inside one another. This occurs frequently with web pages, hypertext markup language (HTML) typically used for web pages is often times embedded with Java, JavaScript, or Adobe Flash. Flash is used to create animations and incorporate video in web pages. Java is a programming language used to include the capability of running secure Java applets in web pages. JavaScript is a scripting language used in web pages [94].

4.3.8 NOC Access Router Vulnerabilities

As mentioned in Section 3.4.1, the NOC access router enables the NOC manager to allow or deny users access to satellite services. Flaws in this router could allow an attacker to prevent traffic from entering or leaving the NOC and to interrupt services. Within routers there are several buffers, including the output buffer which is important for packet switching. Due to the fact that buffer size is finite, routers are susceptible to buffer overflow attacks. Since the output buffer can cause queuing delays and packet loss when it is completely filled, if an attacker continually sends many packets to the router, they are capable of causing a buffer overflow resulting loss of data packets [22]. The NOC access router may also be susceptible to the same IP packet routing vulnerabilities as discussed in relation to the IRIS satellite access router in Section 4.2.4.

In terms of routing protocols, there are several options that can be used for packet routing. The Border Gateway Protocol (BGP) is the main routing protocol used for the Internet. It works by keeping up-to-date a routing table of the autonomous systems that are crossed in reaching the destination. An autonomous system is a collection of IP networks and routers that are controlled by one entity and use a common routing protocol. BGP is a path vector protocol, which means that the path that routing table updates take as they are sent across the network are maintained in order that the current network topology is known to each router and is updated in all routing tables across the network. BGP Version 4 has been in use since 1994 [26]. Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP) are both examples of distance vector routing protocols which use the Bellman-Ford algorithm for determining routing paths by calculating the direction and distance to any node in the network. Routers using these protocols must inform neighboring routers of network topology changes periodically, so that routing tables can be updated. EIGRP is a Cisco proprietary routing protocol. It minimizes routing instabilities after network topology changes [59]. RIP enables routers to adapt to a continually changing network topology by sending information about which networks are reachable by each router and about the distance to each of those networks from the routers. Open Shortest Path First (OSPF) and Intermediate system to intermediate system (IS-IS) link state routing protocols are now preferred over RIP [132]. Link state routing protocols also send network topology information across the network, upon which each routing updates its routing tables to maintain clear picture of the current network state. Packets are sent via the best path through the network to the destination which is determined by Dijkstra's Shortest Path algorithm. OSPF does error detection and correction on its own, avoiding the use of either transmission control protocol (TCP) or user datagram protocol (UDP). OSPF is generally used in large corporate networks [120]. IS-IS, on the other hand, is typically used in large service provider networks because it can support more routers than OSPF. IS-IS does not use IP for transporting routing information [92].

The BGP routing protocol has several vulnerabilities associated with it, to include: de-aggregation attacks, unauthorized route injection, bogon (or Martian) routes, and Distributed DoS (DDoS) attacks [134]. A de-aggregation attack consists of a mis-configured router flooding the network with BGP routes which caused routing to be disrupted globally and many routers to crash. The whole network could experience connectivity issues. Bogon routes are unused or not-widely-publicized routes, typically for private use. These routes can be hijacked and actively advertised making it possible for an attacker to redirect traffic to their router instead of the intended destination. In order to intercept the traffic, the attacker can use a de-aggregation type attack and try to manipulate the path to their router so that it appears shorter than the path to the legitimate router. This form of attack can allow traffic eavesdropping or cause DoS [18]. DDoS attacks involve infecting a multitude of user terminals with viruses that all attack at the same time [49].

Cisco's EIGRP is susceptible to ARP DoS attacks as well as Directed DoS attacks. The ARP DoS attack is accomplished by sending spoofed EIGRP announcements. The announcements will result in an ARP storm which will take up network capacity while routers try to contact the announcing router. The Directed DoS attack is possible by sending forged packets into the network which could cause routers to change their routing neighbor relationships. Iterating this attack could cause sustained DoS. Also, if the attacker is inside the network, the attacker may be able to divert and modify messages before returning them to the traffic flow [38].

The RIP protocols can enable an attacker to inject routes into the network and allows the disclosure of routing information [70]. Since RIP has no built-in authentication, an attacker can masquerade as a legitimate user by causing traffic intended for the legitimate user to be sent to the attacker instead. As is in the case with BGP bogon route attacks, an attacker can send false RIP packets announcing the attacker's route is the shortest causing subsequent data packets sent out in the network to be routed through the attacker's router. The data packets could then be viewed and modified [115].

OSPF is also susceptible to DoS attacks. These DoS vulnerabilities can stop traffic from entering a victim's router [153]. If an attacker is able to change the value of the "age field" in a legitimate router's link state advertisement (LSA) to "MaxAge", then the attacker could interrupt routing through that legitimate user's router. The LSA contains the routing information for the particular router disseminating it. MaxAge is used to eliminate old LSA's from the distributed database. By changing the age field to almost the MaxAge, the LSA would age prematurely causing it to be deleted from the database prematurely. If two LSA ages are within a "MaxAgeDiff" window, OSPF will call them equal. The false LSA could replace the legitimate LSA and cause it to be eliminated prematurely from the database. This would only happen if the legitimate LSA was also in the MaxAgeDiff window. MaxAgeDiff is defined as one quarter of MaxAge and one half of the normal refresh interval. There is no way to protect against routers in the network announcing false information about their own links, such as announcing a connection that does not exist. These false announcements could result in this internal router receiving data packets that are bound for the network to which it announces the false connection. The packets would not reach their destination, unless the router passed on the data packets to their correct destination network [19].

IS-IS is widely used by network operators due to the fact that it runs over open systems interconnection (OSI) Layer 2 (Data Link layer) protocols and disturbances on the IP Layer (Network layer, Layer 3). Attacks like DDoS attacks do not have an effect on IS-IS [7]. Data link layer protocols include PPP and LAPB.

In summary, routing protocols were not designed to protect against insertion and propagation of false routing information. The capability exists for attackers to modify, delete, replay, or generate false routing information and send it propagating through the network. If an attacker announces that their route is the shortest route to many networks, they can cause congestion and increase the load on the network. Also, by injecting incorrect routing information into the network, an attacker can make areas of the network seem unreachable, when in fact they are actually reachable. Also, a router internal to the network could send incorrect routing information about its own links to the rest of the network [19]. The least vulnerable of the routing protocols mentioned in this section seems to be IS-IS.

Since the NOC access router allows (or denies) access to satellite services, the vulnerabilities associated with those particular services also need to be taken into consideration. These service vulnerabilities will be discussed in a later section on the SSP. Since there are a multitude of services that are currently available via satellite, the example of INTELSAT 14 will be continued in the discussion of service vulnerabilities, and only the vulnerabilities associated with the services to be offered by INTELSAT 14 and the IRIS payload will be discussed.

4.3.9 Earth Segment Vulnerabilities Summary

The Earth station network is the most vulnerable component of the satellite system's Earth segment. It incorporates all of the vulnerabilities of each Earth station that is part of the network. In addition, since the NOC is also a part of the Earth station network, the Earth station network is subject to all NOC vulnerabilities, as well.

4.4 User Segment Vulnerabilities

As mentioned in Section 3.5, the user segment consists of user stations that enable access to corporate Intranets, the Internet, and cellular networks. Remote users can connect via the Internet to an SSP to access services. Points of Presence (PoPs) may act as the "middle man" in providing remote users Internet access via ISPs. Standard PC devices are also an option for remote users in the case where access to the terrestrial fiber network is impossible. All of these accesses to various satellite services make the user segment susceptible to a variety of attacks. Also, connections via SSPs, PoPs, and standard PC devices may have additional vulnerabilities associated with them. The vulnerabilities associated with Internet and Intranet access were discussed previously in Section 4.3.7 and will not be repeated here.

4.4.1 Cellular Network Access Vulnerabilities

Many of the vulnerabilities associated with cellular network access are due to the interaction between these cellular networks and the Internet. If these attacks target user terminals, as opposed to the cellular network, they are usually harder for the network operators to defend against. An example of one particular attack involves attackers exploiting multimedia messaging service (MMS) vulnerabilities in order to drain user terminal batteries. The attack was executed by first creating a list of target user terminals with active Internet connections. This list was compiled by exploiting the insecurities of the MMS protocol. Once the target list was created, the attackers could drain the terminals' batteries faster than normal by exploiting the packet data protocol (PDP) context retention. Before a user terminal can use any general packet radio services (GPRSs), the terminal must be registered with a Serving GPRS Support Node (SGSN). A PDP context is created during this registration procedure. Upon ending a communication session, the terminal would go into standby mode; however the PDP context is still allocated to the terminal. This is done to keep from having to deactivate and reactivate a new PDP context after ending every communication. Deactivating and reactivating a new PDP context could cause applications to restart and require the user to re-enter all passwords. Since user cellular terminals will accept any MMS message it receives as long as the message format is correct, an attacker can send as many MMS messages to the terminal as they want without alarming the cellular services provider. Phones reveal information such as: hardware description, display capabilities, and the current and compatible software whenever they communication over HTTP. An attacker could easily obtain the terminal model number from this information. In order to build the target list, the attacker sends an MMS message with their web server location to the target terminals, and then waits for HTTP request messages from the terminals to come to their web server. Since most cellular terminals download MMS messages automatically upon receipt, the terminals will automatically make HTTP requests, which usually contain the profiles and IP addresses of the terminals, to the attacker's web server. Also, the terminal's reply to the attacker's MMS message activates a PDP context, making the battery draining attack easy to execute. The active PDP enables the attacker to send extraneous IP packets to the target user terminals to drain their batteries. Since cellular terminals are usually in standby mode, when a message is received a page on the paging channel will bring the terminal to the ready state and cause it to perform a location update. This process causes the terminal to use up battery power [35].

Cellular networks themselves are susceptible to various attacks, including: worms, eavesdropping, spamming, masquerade attacks (impersonating users and networks), DoS, man-in-the-middle attacks, and hijacking of services. An attacker could sending a multitude of messages to many target user terminals in one area and cause DoS in that area of the network by saturating network control channels which are used for both voice and short message service (SMS) services. Since cellular network providers allow email and web-based interfaces to message user terminals directly, a spam attack combined with a phishing attack could allow an attacker to gain access to users' sensitive data. Worms can also be used to attack a cellular network. They can be spread via email attachments or Bluetooth. Worms can cause DoS attacks or change user terminal operating systems and then search for other terminals to infect, for example. By changing the terminal's operating system, the attacker could drain the terminal's battery by setting the terminal's transceiver to run continuously at maximum strength [35]. An attacker can gain entry into the cellular network by exploiting a buffer overflow vulnerability in dual-mode cellular terminals which enable users to access both cellular and Wi-Fi services. By exploiting the buffer overflow vulnerability in these dual-mode terminals, an attacker can execute arbitrary code which will enable them to use the terminals as gateways into the cellular network. Also, these dual-mode phones open the cellular network up to the vulnerabilities associated with using Wi-Fi services [96].

Since wireless communications are passed through the air, anyone within range is capable of eavesdropping on or intercepting these communications. All an attacker needs to eavesdrop wireless communications is a "packet sniffing" program, many of which are available for free. "Packet sniffing" programs display all data they find being transmitted in the public WiFi local area network (LAN) [126]. In addition, Wi-Fi networks and users continue to use the highly vulnerable wireless encryption protocol (WEP) to protect these communications. WEP headers are not encrypted, so source and destinations addresses of every packet sent are easily identifiable. Also, since the WEP encryption key never changes unless manually changed by the network administrator, an eavesdropping attacker could monitor communications over a period of time and gather information to enable them to determine the encryption key via statistical analysis and decrypt the data [111]. Wi-Fi Protected Access (WPA) replaced WEP and provides better protection for wireless communications. However, WPA is still not completely secure. WPA uses mathematical algorithms in order to provide authentication of users to the network. The use of these mathematical algorithms makes WPA vulnerable to attack. If a legitimate user (or an attacker) sends two unauthorized data packets within one second, WPA thinks it is being attacked and shuts down. An attacker can take advantage of this aspect of WPA by sending unauthorized data packets periodically. This would cause periodic shutdowns of WPA [68].

Wi-Fi networks are also vulnerable to man-in-the-middle attacks. If an attacker can masquerade as a legitimate Wi-Fi network, once legitimate users are connected to the attacker's network, the attacker can view, modify, and replay data, inject data, and impersonate legitimate users all without the users' knowledge. If the attacker sends the users' data on to the legitimate wireless network after it passes through the attacker's network, the legitimate user will not notice any change in services [52]. Wi-Fi networks are susceptible to malicious software, such as viruses, worms, and Trojan horses, as are all networks connecting to the Internet. They are also subject to DoS attacks which can be implemented on Wi-Fi networks to overwhelm legitimate network signals by introducing a strong interfering signal or by flooding a NAP by exploiting the IEEE 802.11 medium arbitration algorithm which is supposed to prevent users from trying to send signals at the same time [125]. The attacker would need a powerful transmitter and would need to be located somewhere nearby to introduce a sufficiently strong interfering signal into the network to cause DoS. This would make locating the attacker relatively easy. In the case of the network flooding attack, the attacker will use up available bandwidth and cause DoS to legitimate users. In addition, Wi-Fi networks are susceptible to ARP spoofing as discussed previously in Section 4.3.4 as well as hijacking, phishing, and man-in-the-middle attacks as discussed in Section 4.2.4, Section 4.3.6, and Section 4.4.1, respectively.

4.4.2 Satellite Service Provider (SSP) Connection Vulnerabilities

SSPs offer satellite services to remote users via the network of ground- and space-based infrastructure. Users connect to SSPs via the Internet. Therefore, SSPs are susceptible to the vulnerabilities of Internet connections as discussed in Section 4.3.6. Also, SSPs operate the hub Earth stations for VSAT networks. Therefore, SSPs are subject to the vulnerabilities discussed in Section 4.3.2 relating to VSAT central hubs. Since SSPs provide satellite services to users, SSPs are susceptible to all the vulnerabilities associated with these services, as well. The services offered are specific to the satellite under consideration. In this case, the example of INTELSAT 14 and the IRIS payload will be continued and the vulnerabilities of the services to be offered by this satellite's payloads will be analyzed.

The IRIS payload is intended to be capable of providing ad hoc networking; voice over IP (VoIP) services; virtual private network (VPN) services; video teleconferencing services; bandwidth on demand; voice, video, and data transmission services; and cross-beam, cross-band, and multicast information services without the use of an Earth station relay. Therefore, the IRIS payload (and INTELSAT 14 satellite) may be susceptible to the vulnerabilities associated with each of these services.

Ad hoc networking is vulnerable to a multitude of routing attacks, such as spoofing routing information, altering routing information, replaying routing information, selective forwarding, and sinkhole attacks. These attacks can be performed by dropping, changing, or injecting packets into the network. Spoofed, altered, and replayed routing information can cause such effects as generating false error messages, dividing the network, and increasing end-to-end transmission time. Selective forwarding indicates that some messages are always dropped, degrading network services. Sinkhole attacks force traffic to go through the attacker, enabling the occurrence of other types of attacks [63].

VoIP phone default settings generally do not include traffic encryption. If VoIP data is not encrypted, it is relatively easy for an attacker to intercept data, eavesdrop VoIP calls, and record VoIP calls [12]. VoIP phones are vulnerable to buffer overflow attacks that would cause the phone to crash. An attacker can use the Session Initiation Protocol (SIP) to take advantage of the buffer overflow attack enabling the attacker to connect to the victim's terminal and view, copy, delete, modify, or steal user files. SIP is a signaling protocol used to set up and terminate multimedia communications, such as VoIP calls [78]. Many VoIP phones are susceptible to DoS and DDoS attacks, spam, viruses, ARP spoofing attacks, packet injection, and VoIP data interception [12, 91, 142]. In addition, VoIP is vulnerable to call hijacking, malicious call termination, and information spoofing [142]. Also, since VoIP phones have web-based user interfaces, they are susceptible to man-in-the-middle attacks. These man-in-the-middle attacks require knowing the victim terminal's IP address. In order to obtain this information, the attacker can try guessing, using an XSS Intranet scanning attack (as discussed in Section 4.3.7), or by doing an Nmap scan. An Nmap scan is used to make a map of the network by scanning for terminals and services on the network. Once the IP address is discovered, the attacker can steal data, gain control over the victim's VoIP phone, disable the victim's VoIP phone, monitor the victim's use of the VoIP phone, or even eavesdrop the conversations going on in the victim's surroundings [72].

The applications of these VoIP services over INTELSAT satellites include: interoffice trunking over the Internet or corporate Intranets, business continuity and disaster recovery, pre-paid calling card services, VoIP peering, Internet cafés, and IP Central Office Exchange (Centrex) [88]. Some of these applications have additional vulnerabilities associated with them on top of the VoIP vulnerabilities discussed above. VoIP peering, or call forwarding between Internet telephony service providers (ITSPs), decentralizes the call routing which normally involves the use of a central hub. This decentralization of the routing makes it easier for an attacker to take over a legitimate user's number [137]. This application typically uses the session initiation protocol (SIP) signaling protocol. This protocol has several vulnerabilities associated with it that may affect the VoIP peering application [99]. For instance, SIP vulnerabilities could allow an attacker to access a user terminal and cause it to become unstable, cause a DoS attack, or cause VoIP services to be interrupted [34]. There is a particular vulnerability in SIP forking proxies that can enable an "exponentially-growing message exchange attack" which would result in the network being flooded with traffic. SIP forking proxies are servers that are used to search for correspondents [30]. SIP is also subject to spoofing attacks. An attacker could send INITIATE requests (to begin a communication session) with false IP addresses to spoof a legitimate user or send spoofed BYE requests to cause call termination [140]. In addition, SIP may be vulnerable to eavesdropping, man-in-the-middle attacks, attacks forcing a VoIP phone to reboot, call redirection, and registration manipulation (erasure or hijacking of a legitimate user's registration attempt, or addition of false registrations). In the case of man-in-the-middle attacks, an attacker would inject their rogue terminals into the network between proxies [42]. IP Centrex is a business-grade phone service. It is also susceptible to the aforementioned SIP vulnerabilities [43].

VPN's are subject to the SSH vulnerabilities previously discussed in Section 4.3.3. In addition, VPN's are vulnerable to viruses, man-in-the-middle attacks, hijacking, and VPN spoofing. Viruses may be passed onto the VPN via a user Internet connection if the user is connected to both simultaneously. VPN man-in-the-middle attacks can allow an attacker to intercept, replay, redirect, delete, modify, or insert data as well as reflecting data back to the sender. VPN hijacking involves an attacker taking over a legitimate user's already-initiated VPN connection and masquerading as the legitimate user to the network [82]. VPN spoofing, if successful, can allow an attacker unauthorized access to a VPN. The attack is implemented by first creating packets with false IP addresses. These packets are sent to legitimate users and to make the user think the attacker's device is legitimate. The attacker then may be able to alter routing information and obtain access to authentication sequences. This information may yield unauthorized access to the VPN for the attacker [36]. IP VPNs are intended to enable a company's customers and partners to securely connect to the company's Intranet and connect the company with an IP wide area network that can carry voice, video, and data over a single connection [71]. IP VPNs run over TCP/IP (See Figure 22.).

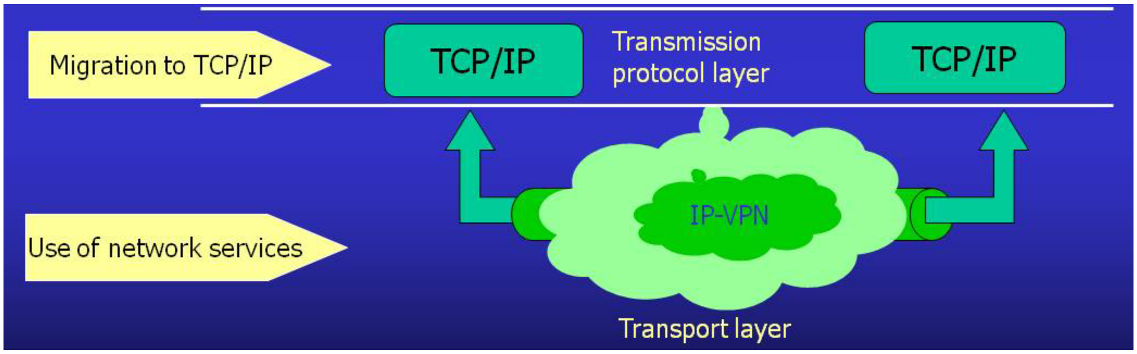


Figure 22. IP-VPN over TCP/IP Illustration [85]

TCP/IP is vulnerable to packet sniffing, IP spoofing, and TCP session hijacking, to name a few. IP spoofing refers to a process in which an attacker creates false packets with a legitimate user's IP address, impersonating packets sent by the legitimate user. IP spoofing can be used cause DoS or to gain unauthorized access to a network [55]. If an attacker sends a SYN packet with a spoofed IP address to a host in order to request a connection with the host, then the host will reply to the attacker's spoofed IP address with a SYN/ACK packet. The SYN packet is the first packet in a connection indicating that the attacker wants to create a connection with the host server. The SYN/ACK packet acknowledges the hosts receipt of the attacker's SYN packet and sends the host's SYN information in return. The attacker then never sends an ACK packet to the host to acknowledge receipt of the SYN/ACK packet, so the connection request remains on the stack. The attacker then continues to send SYN packets with the spoofed IP address, thereby leaving many unanswered connection requests on the stack, using up system resources and causing DoS. This type of attack is called SYN flooding. Also, TCP/IP is subject to packet spoofing. An attacker could inject a packet into the network and then give it a false source IP address. By specifying the route the packet takes through the network instead of letting it go through the network routers, the attacker's packet can be sent with a spoofed IP address. TCP session hijacking involves the attacker taking over an already-initiated connection and masquerading as a legitimate user. This can be done via a man-in-the-middle attack, for example [141]. The Internet Control Message Protocol (ICMP) is used in the TCP/IP IP layer to send one-way messages to a host. ICMP can be used in DoS attacks or allow attackers to intercept packets. An attacker can send a false "time exceeded" or "destination unreachable" message to a victim causing the victim to end their connection. The ICMP "redirect" message can be used to intercept packets. If an attacker sends a false ICMP "redirect" message to a victim, the victim will then end up sending certain connection packets through the attacker's device [95].

One of the applications of INTELSAT's bandwidth on demand services is maritime communications [89]. Maritime communications depend on the Global Positioning System (GPS) for timing synchronization. GPS timing is vulnerable to bad weather and may be lost during severe storms [97]. Also, GPS timing, since it is provided by the GPS satellites, is susceptible to all of the vulnerabilities associated with satellites discussed previously in Section 4.2, such as jamming or intentional physical attack.

The implications of the IRIS payload multicasting information to users are that user terminals will be subject to the vulnerabilities associated with multicasting. The nature of multicasting is that anyone can join a multicast group, and when packets are sent to the multicast group address, all members receive those packets. The vulnerabilities of multicasting include: DoS attacks, flooding attacks, forged data attacks, sending of false acknowledgements (ACKs), Scalable Reliable Multicast Protocol

(SRMP) vulnerabilities, buffer overflows, rushing attacks, neighbor attacks, black hole attacks, and jellyfish attacks [100, 105, 117]. Flooding attacks involve the attacker sending many data packets to the multicast group, using up network resources and degrading services. Since the Reliable Multicast Protocol (RMP) does not verify that a packet's network address matches the multicast group identifier, the attacker can send forged data to the multicast group. An attacker can modify the order of data packets by sending false ACKs to the multicast group. The SRMP can be manipulated by an attacker to generate negative ACKs (NAKs). These NAKs can be created by changing the TTL in the packet header. These NAKs are only received by some of the multicast group members. If the group members receiving the attacker's NAKs try to send their own NAKs, the group members' NAKs will be blocked, and therefore a retransmission of the data packets that were not received will not be initiated. In addition, an attacker can cancel any retransmissions from legitimate multicast group members by creating their own retransmissions with a shortened TTL [100]. Rushing attacks involve an attacker entering routing paths between legitimate users. As an intermediate node, the attacker's device only processes the first non-duplicated data packet and avoids processing any duplicate packets sent later. When a legitimate user sends route discovery packets into the network in order to determine the best route to the desired destination for their packets, the attacker's device can quickly forward these route discovery packets. The attacker's device then gains priority when routing paths are being selected by legitimate users, increasing the chances of a user's packets passing through the attacker's device on their way to their final destination. If instead of forwarding the route discovery packets, the attacker replays them without updating their routing information, this is termed a neighbor attack. When the attacker replays the route discovery packets, it can cause two users that are not within range of each other to think that they are neighbors. These two users then will try to directly send packets to each other, resulting in the packets being lost. If instead of forwarding the route discovery packets as in the rushing attack case the attacker drops some (or all) of the data packets, this is termed a black hole attack. This type of attack degrades network performance by reducing packet delivery. A jellyfish attack involves the attacker beginning with a rushing attack, but instead of forwarding the route discovery packets the attacker delays them and then forwards them. Jellyfish attacks diminish the ability to provide real-time communications by increasing the end-to-end communications delay [117].

4.4.3 Point-of-Presence (PoP) Connection Vulnerabilities

Since PoPs enable remote users to access the Internet, Intranets, and cellular networks, PoPs subject users to the vulnerabilities associated with Internet, Intranet, and cellular network access. All of these vulnerabilities were discussed in previous sections and will not be repeated in this section. PoPs use routers to provide access points through which user terminals can connect, and these PoP routers can support any of the data link layer protocols mentioned in Section 3.5.2 in order to provide this access to users. These PoP routers and the data link layer protocols they support increase the number of vulnerabilities that a user terminal becomes susceptible to when connecting to satellite services via a PoP.

HDLC and LAPB are both based on the American National Standards Institute (ANSI) standard Advanced Data Communication Control Procedures (ADCCP) data link layer protocol. HDLC, ADCCP, and PPP can all be used to make point-to-point connections, while the Ethernet data link layer protocol is generally used for local area networks [5]. HDLC and ADCCP were both precursors to the Ethernet protocol. PPP, or point-to-point tunneling protocol (PPTP) as it is also known, relies on a single user name and password for authentication. This user name and password can be easily obtained by an attacker by monitoring user data packets. The PPP encryption key can also be broken relatively easily. It is only a 128-bit key and the same key is used at each end of the transmission [29]. Once the attacker has obtained the user name, password, and encryption key, they have access to sensitive user data and can even launch a DoS attack against the PPP server. The vulnerabilities associated with PPP are not due to flaws in the protocol itself, but are due to flaws in Microsoft's implementation of the protocol [136]. The Ethernet protocol utilizes a carrier-sense-multiple access/collision detection (CSMA/CD) scheme. The CSMA/CD scheme works by instructing users that want to transmit data that they must wait until other users have finished transmitting. The data that is transmitted can be seen by all other users on the network, creating a vulnerability to packet sniffing. The Ethernet protocol is also subject to data collisions. If two users decide to transmit data at the exact same time, the data will collide. The users then must wait and retransmit their data at a later time, increasing the end-to-end transmission delay [61]. If instead an attacker continues to send packets and does not wait until the line is clear to retransmit, the attacker can cause DoS. Since the Ethernet protocol does not have built-in authentication, it is also vulnerable to packet spoofing and ARP spoofing (as discussed in Section 4.3.4) [116].

PoP routers may be susceptible to such attacks as: IP address spoofing, unauthorized access, DoS attacks, and buffer overflow attacks. PoP routers may use the simple network management protocol (SNMP) to support router access control [131]. SNMP is an application layer protocol that is used in the exchanging of management information between network devices. Cisco Systems, one of the companies collaborating on the IRIS project, supports SNMP in its router software [39]. SNMP vulnerabilities may allow unauthorized access to the PoP router, DoS attacks, buffer overflow attacks, may cause service interruptions, or may cause the router to become unstable. SNMP trap messages are sent from user terminals to the network management system (NMS) and are meant to update the NMS on the state of the user terminal. SNMP trap messages may notify the NMS of warnings or errors on the user terminal. The NMS must decode and process the SNMP trap messages from the user terminals. It is this decoding and processing of SNMP trap messages that makes the SNMP vulnerable to DoS and buffer overflows. The NMS also sends requests for information to the user terminals or sends messages to user terminals indicating they need to change their configuration settings. These messages must be decoded and processed by the user terminals. The decoding and processing of these SNMP request messages again makes SNMP vulnerable to DoS and buffer overflows [33]. SNMP uses community strings (i.e. the community names) to provide some level of authentication for NMS requests. However, these community strings are in clear text in SNMP messages making them easily accessible to attackers. If an attacker can access an SNMP community string, the attacker can gain access to the SNMP Management Information Base (MIB). This SNMP community string vulnerability may result in DoS or the information gained by the attacker through accessing the MIB may allow them to launch further attacks against the network [149]. In terms of routing protocols, the PoP router may use the BGP or any of the other routing protocols discussed in Section 4.3.8.

4.4.4 Standard PC Device Connection Vulnerabilities

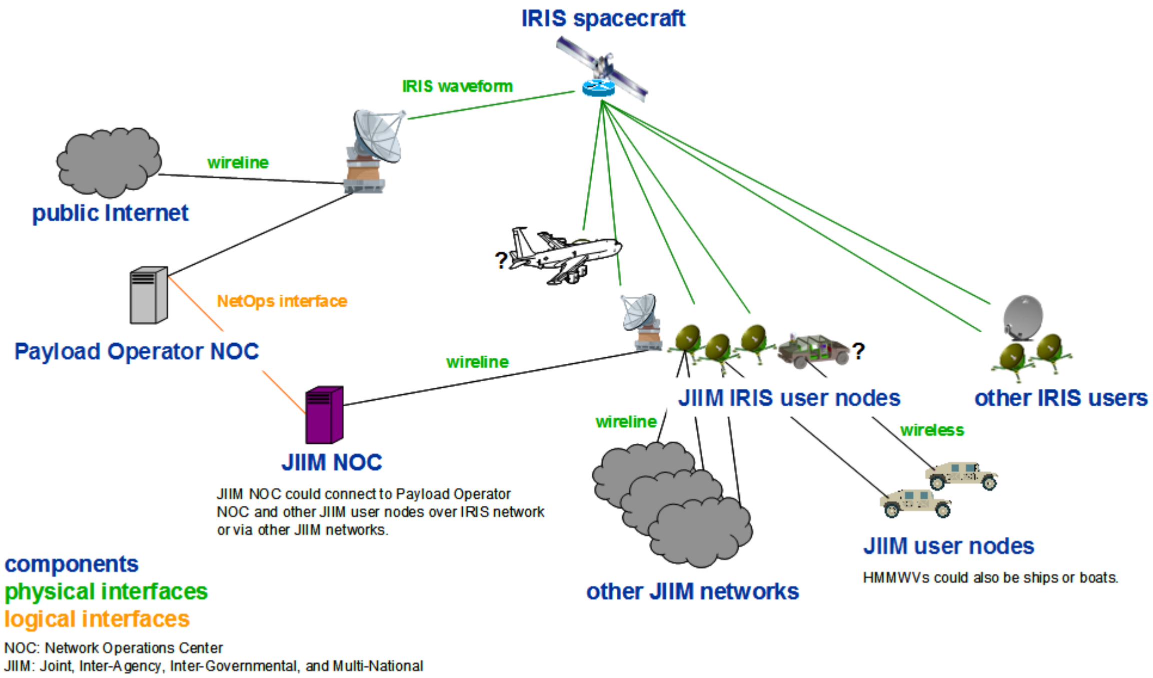
Remote users can also access satellite services via standard PC devices, as discussed in Section 3.5.3. The PCMCIA interface ports used to connect the user terminals to standard PC devices may be susceptible to attack, as well as the PC devices themselves. Wireless local area network (WLAN) Cardbus devices can be installed in the PCMCIA ports, enabling a wireless connection from user terminal to PC device. These WLAN Cardbus adapters use either WEP or WPA encryption [1]. The vulnerabilities associated with WEP and WPA were discussed in Section 4.4.1. Also, since PC devices are generally also connected to the Internet, the vulnerabilities associated with Internet connectivity discussed in Section 4.3.6 apply to these standard PC device-to-user terminal connections.

4.4.5 User Segment Vulnerabilities Summary

SSPs and PoPs are the most vulnerable components of the user segment. SSPs not only incorporate all of the vulnerabilities of the satellite services offered by the particular satellite in question, but they also suffer the vulnerabilities of Internet connectivity. In addition, since SSPs operate the VSAT central hub, the vulnerabilities associated with the hubs are included in the SSP vulnerabilities. PoPs, on the other hand, are susceptible to the vulnerabilities of the PoP routers, the PoP router protocols, Internet access, Intranet access, and cellular network access. The offerings provided by each of these components of the user segment make them vulnerable to a multitude of different attacks.

4.5 Attacking INTELSAT 14 and the IRIS Payload

The IRIS space system, which is intended to offer IP routing via satellite, will consist of the IRIS satellite (i.e. INTELSAT 14), IRIS payload operator facilities, and the IRIS users. The IRIS satellite and payload operator facilities will manage the services being offered by the IRIS payload and will provide Internet connectivity. Figure 23 illustrates the planned configuration for the IRIS space system.



JIIM NOC could connect to Payload Operator NOC and other JIIM user nodes over IRIS network or via other JIIM networks.

HMMWVs could also be ships or boats.

NOC: Network Operations Center
JIIM: Joint, Inter-Agency, Inter-Governmental, and Multi-National

Figure 23. Illustration of Planned IRIS Space System Configuration [106]

Note that the Joint, Inter-Agency, Inter-Governmental, and Multi-National (JIIM) NOC shown in Figure 23, which will manage IRIS services for JIIM missions, may only be present in a “virtual sense”. The JIIM users include U.S. Department of Defense air, maritime, and land forces [106].

The design aspects of the IRIS satellite that make it different from a traditional, bent-pipe COMSAT are its on-board processing capabilities and the IP router that it will carry. The IP router will enable the satellite to receive packets directly from user terminals without the use of an Earth station. Since the IRIS IP router is the new technology being tested on-board this satellite, it is necessary to examine the possibilities for attacking this new technology in order that it can be protected. Therefore, the remainder of this document will focus on attacking the IRIS IP router. In order to accomplish this feat, an attacker would need to attack the satellite uplink (the communications link from the Earth to the satellite). If the case of an attack on the satellite downlink were examined, the signal would have already gone through the routing process on-board the satellite, and therefore that case will not be discussed here.

According to Figure 23, an attacker would have a few possible options for gaining access to the satellite uplink. Suppose that the JIIM user is in the midst of a conflict and is under attack. If the JIIM user is overtaken or captured, then the attackers will likely be able to gain access to the JIIM user terminal. With access to the JIIM user terminal, the attackers can pose as a legitimate JIIM user and send signals to the IRIS satellite. Accessing the JIIM user terminal may require a user name and password. Since the JIIM users are connected to the Internet via the IRIS spacecraft, packet sniffers may have revealed the JIIM user’s user name and password prior to the attack making takeover of the JIIM user terminal relatively easy. Suppose instead, that the attackers are able to gain access to the payload operator NOC. Since INTELSAT 14 is a commercial satellite, the payload operator NOC will likely be a commercial facility, and therefore will not secured with strong physical security measures. It would likely be relatively easy for an attacker to gain access to the commercial payload operator NOC. If hackers can gain access to Johnson Space Center (JSC) as they allegedly did in April 2008 and cause disruptions on-board the ISS (see Section 4.2.4 for a discussion of this event), then the IRIS payload operator NOC could be at risk. The JSC hackers used a Trojan horse to gain access to the satellite uplink after they had gained entry to the facility. Attackers of the IRIS payload operator NOC could take a similar approach to gain access to the uplink to the IRIS satellite. An attacker may be able to gain access to the satellite uplink remotely via the Internet connection provided by the IRIS satellite and the payload operator NOC. An attacker may be able to install a backdoor onto the JIIM user terminal by using a virus that is passed to the terminal via the Internet, as discussed previously in Section 4.3.6. Once the backdoor is in place, the attacker may then be able to take control over the user terminal, thereby gaining access to the satellite uplink. Again in this case, a packet sniffer (or phishing attack) used previous to the backdoor attack may be necessary to gain knowledge of the JIIM user's user name and password.

Once the attacker has gained access to the satellite uplink, they can send malicious signals to the satellite that will be passed to the IRIS IP router by way of the satellite antenna. In the cases where the attackers actually took over the JIIM user terminal, a session hijacking attack (discussed in Section 4.2.4) may be possible. The attackers can masquerade as the legitimate JIIM user and possibly intercept sensitive communications from other JIIM users. If the attackers instead just send a multitude of packets to the IRIS IP router, they may cause a buffer overflow. As discussed in Section 4.3.8, this type of attack could cause the router's output buffer to become full, resulting in queuing delays, packet loss, and interruption of services. If other JIIM users' packets are lost, they may try to retransmit their data, which would only result in further queuing delays and packet loss. In addition, the routing protocol to be used on the IRIS IP router will likely be vulnerable to insertion of false routing information. Routing protocols are not generally designed to protect against the insertion and propagation of false routing information. The injection and propagation of false routing information in the JIIM user network could be disastrous especially where real-time communications are needed. However, the IRIS IP router routing protocol is unknown at this time, and so further analysis of its exploitation is not possible. In terms of protocols that support router access control, the IRIS IP router may use SNMP. As discussed in Section 4.4.3, Cisco Systems uses SNMP in its router software, and Cisco happens to be the company providing the IP networking software for the IRIS IP router. An attacker with access to the satellite uplink could send SNMP trap messages to the IRIS IP router, which would likely result in DoS and buffer overflows.

A knowledgeable attacker, upon gaining access to the satellite uplink, could wreak havoc on the IRIS satellite network, causing anywhere from denial of services to interception of sensitive data. Therefore, it is necessary to protect the IRIS space system components that could allow the attacker to access the satellite uplink. Strong physical security at the payload operator NOC will be required, as well as protection for user terminals. User terminal protection needs to include strong anti-virus software that can eliminate the possibility of an attacker installing a backdoor onto a user terminal via a virus.

V: Conclusions and Suggestions for Future Work

The purpose of this research was to provide an understanding of potential vulnerabilities in satellite communications systems by first identifying various attacker entry points into a typical system and then determining the specific vulnerabilities at each identified access point. An attack scenario on the IRIS payload was presented as an example in order to provide an understanding of the possible impact of attacks on U.S. satellite communications systems. This thesis attempts to provide a basis for finding ways to avoid future attacks on U.S. space assets by supplying information on the ways satellite communications systems can be attacked.

Since satellite communications have become increasingly important in both the U.S. and in countries across the globe, the protection of space assets will become vital in order to keep these communications from being disrupted. Satellite communications have become an important component of the U.S.'s net-centric warfare doctrine. Therefore, an attack on U.S. space systems could have serious impacts on U.S. war fighting capabilities. Given that the U.S. relies on commercial COMSAT capacity to help meet military bandwidth needs, commercial space systems, as well as military-dedicated space systems, are vulnerable to attacks from U.S. adversaries. While military satellites employ some protection techniques, commercial COMSATs are predominantly unprotected against attacks such as RF jamming. An understanding of the vulnerabilities of these systems is required in order to know how to protect these space systems from future attacks.

This research determined that the most vulnerable component of the satellite communications system's space segment is the satellite antenna. The satellite antenna is vulnerable to intentional attacks including: RF jamming, spoofing, meaconing, and deliberate physical attack. RF jamming can cause signal degradation or even total signal loss. Spoofing is generally only a problem for COMSATs with on-board processing capabilities. This type of attack can allow the attacker to take control of the satellite receiver. Meaconing can result in transmission delays. Deliberate physical attack of the satellite can, of course, result in total loss of communications and likely total loss of the satellite.

The most vulnerable Earth segment component was found to be the Earth station network. It is vulnerable to both Earth station and NOC vulnerabilities, to include: RF jamming, deliberate physical attack, and Internet connection vulnerabilities. Internet connectivity is susceptible to spyware, phishing attacks, viruses, backdoors, Trojan horses, worms, session hijacking, and user impersonation, to name a few. In addition, if an attacker can gain control of the TT&C link, the result may be loss of satellite control. Also, access router flaws and router protocol vulnerabilities could enable an attacker to stop traffic from entering or leaving the NOC or enable an attacker to gain access to the Earth station network, both of which could cause service interruptions to occur.

This research found that the most vulnerable user segment components are the SSPs and PoPs. SSPs are subject to the vulnerabilities of the services offered, the vulnerabilities of Internet connectivity (as mentioned in the previous paragraph), and the vulnerabilities associated with operating the VSAT central hub. VSAT networks vulnerable to attackers inserting rogue devices into the network which could allow the attackers to eavesdrop data being sent to legitimate users. In a star topology VSAT network, if the central hub is compromised, the entire network is likely at risk, because all neighboring VSATs are connected to one hub. The vulnerabilities of services were discussed in terms of the IRIS payload, which is intended to offer such services as: ad hoc networking, VoIP, VPN, and multicasting. Ad hoc networking is susceptible to routing attacks which could divide the network and increase end-to-end transmission times. VoIP is vulnerable to data interception, eavesdropping, call recording, phones being caused to crash, and all of the vulnerabilities associated with Internet connectivity. VPNs are subject to SSH protocol vulnerabilities, as well as viruses, hijacking, spoofing, and man-in-the-middle attacks. VPN vulnerabilities could allow an attacker to gain access to the VPN, cause DoS, and intercept data. Multicasting is vulnerable to several attacks, including: flooding, black hole, and jellyfish. Flooding attacks and black hole attacks both can cause degradations of network services. Jellyfish attacks increase end-to-end transmission times.

PoPs are subject to Internet (and Intranet) access vulnerabilities, as discussed previously. Also, PoPs are open to additional vulnerabilities from providing cellular network access, such as eavesdropping and DoS. PoP routers are vulnerable to attackers gaining unauthorized access, service interruptions, and router instabilities caused by SNMP exploitation. In regards to routing protocols, PPP and the Ethernet protocol, for example, are subject to attackers gaining access to sensitive user data and DoS attacks.

The example presented of the attack on the IRIS payload, showed that the IRIS spacecraft may be susceptible to session hijacking, buffer overflow attacks, and exploitation of SNMP vulnerabilities all due to the IP router on-board. Session hijacking could allow interception of sensitive communications, while buffer overflow attacks and exploitation of SNMP vulnerabilities could result in service interruption or complete denial of services. All of these attacks can occur only after the attackers gain access to the satellite uplink.

There remain many possibilities for future work on the topic of satellite communications system vulnerabilities, and in particular the IRIS system. For example, once the IRIS IP routing protocol becomes known, further vulnerability analysis may reveal additional vulnerabilities that an attacker could exploit. Also, it would be beneficial to model and simulate the results for one of the possible IRIS system attacks in order to verify that it is indeed possible and provide some insight on ways to protect against this type of attack.

Bibliography

1. "802.11g Wireless LAN CardBus Adapter User's Manual," http://www.tellus.com.tw/supporting/M200.pdf, Version 1.0, pages 1-24.

2. Abdel-Nabi, T., M.P. Brown, Jr., and J.F. Phiel, Jr., "The Evolution of Digital Modulation and Access Techniques in the Intelsat System," INTELSAT, published by American Institute of Aeronautics and Astronautics, Inc., 1993.

3. Abramson, Norman, "Fundamentals of Packet Multiple Access for Satellite Networks," IEEE Journal on Selected Areas in Communications, Volume 10, Number 2, pages 1-8, February 1992.

4. Ackerman, Robert K., "Space Vulnerabilities Threaten U.S. Edge in Battle," http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=973&zoneid=158, June 2005, accessed 7 May 2008.

5. "Advanced Data Communication Control Procedures," http://en.wikipedia.org/wiki/ADCCP, 8 April 2008, accessed 5 May 2008.

6. "Advanced in Mobile Communications Technologies," http://www.msndiyari.com/yabanci-dil/31416-4/, 14 December 2007.

7. Ahola, Kimmo, Eija Myotyri, Ilkka Norros, Leena Norros, Urho Pulkkinen, Pertti Raatikainen, and Taipo Suihko, "The dependability of an IP network – what is it?," http://iplu.vtt.fi/iplu_baseline_2006.pdf, pages 1-27, 16 May 2006, accessed 2 May 2008.

8. AIAA-1994-4606-501, "The INTELSAT System: An Overview," Wernek, S.B., 27-29 September 1994.

9. AIAA-1996-1016-708, "Intelsat TDMA and DAMA," Forcina, G, S. Oei, and R. Bedford, 25-29 February 1996.

10. Albuquerque, J., L. Buchsbaum, C. Meulman, F. Rieger, and X. Zhu, "VSAT Networks in the Intelsat System," pp. 229-239, International Journal of Satellite Communications, Volume 11, 1993.

11. Alcatel, "Understanding the IPSec Protocol Suite," http://faculty.capitol-college.edu/~dward/MSIA%20711%20upload/suppl_readings1/alcatelwhitepaperipsecprotocolsuite.pdf, October 2000.

12. Allsopp, Wil, "VoIP – Vulnerability over Internet Protocol?," http://www.continuitycentral.com/feature074.htm, 19 March 2004, accessed 9 April 2008.

13. Amruther, Chandi and Robert W. Ames Jr., "Mitigating Interference into Communication Satellites," IEEE, 2001.

14. APNIC, "Network planning essentials," http://www.apnic.net/training/download/routing/apnic-REW-Network_Planning_Essentials.pdf, pgs. 1-5, accessed 4 April 2008.

15. Archinal, Andy, John Dyer, John Fagan, Peter Yih-Ru Huang, and Hengqing Wen, "Countermeasures for GPS Signal Spoofing," http://129.15.114.75/download/ION/Wen_Spoof.doc, pages 1-6, accessed 25 April 2008.

16. Arnal, Fabrice, Cedric Baudon, Elisa Callejo, Miriam Catalan, Laurence Duquerroy, Thierry Gayraud, Jose A. Guerra, Ignacio Jimenez, Pierre Loyer, Raul Munoz, Josep Prat, Filippo Rodriguez, Ana Yun, and Peter Zautasvili, "Integrated Project 026950: SATSIX: 01000_4: Satellite Network Requirements," www.ist-satsix.org/DOC/SATSIX_D1000-4_final_v1-1.pdf, pgs. 1-111, January 2007.

17. Associated Press, "Falun Gong Hijacks Chinese TV", http://www.wired.com/politics/law/news/2002/09/55350?currentPage=all, 24 September 2002, accessed 27 December 2007.

18. "Attacking BGPV4," http://iphelp.ru/faq/35/0086.html, accessed 30 April 2008.

19. Badger, M. R. and S. L. Murphy, "Digital Signature Protection of the OSPF Routing Protocol," IEEE, pages 1-10, 1996.

20. Bain, Sean Patrick, “The Increasing Threat to Satellite Communications,” http://satjournal.tcom.ohiou.edu/pdf/issue6/bain.pdf, 20 November 2003.

21. Baras, John S., Michael Hadjitheodosiou, Nicolas Rentz, and Ayan Roy-Chowdhury, “Hybrid Networks with a Space Segment – Topology Design and Security Issues.”

22. Bennour, Imed E., Salaheddine Hamza Sfar, and Rached Tourki, “Transaction Level Modeling of an OSI-Like Layered NOC,” http://ieeexplore.ieee.org/iel5/11202/36064/01708669.pdf?isnumber=36064&prod=CNF&arnumber=1708669&arst=+404&ared=+408&arAuthor=+Sfar%2C+S.H.%3B++Bennour%2C+I.E.%3B++Tourki%2C+R., 2006.

23. Benshoof, Paul, “Civilian GPS Systems and Potential Vulnerabilities,” http://radio.feld.cvut.cz/satnav/CGSIC/presentations/DAY_1_am/Benshoof_CGSIC_050314.ppt, slides 1-23.

24. Bever, Mark, Joseph Freitag, Stuart Linsky, James M. Myers, Raymond M. Nuber, Jaime L. Prieto, Jr., and Eric R. Wiswell, “Fast Packet Vs. Circuit Switch and Bent Pipe Satellite Network Architectures,” www.st.northropgrumman.com/capabilities/SiteFiles/technicallibrary/SatNetArch.pdf, pgs. 1-17, presented at the 4th Ka-Band Utilization Conference, 2-4 November 1998.

25. Blau, John, “U.S. military plans to put Internet router in space,” http://www.itworld.com/Net/3069/070412spacerouter/index.html, 12 April 2007, accessed 3 January 2008.

26. “Border Gateway Protocol,” http://en.wikipedia.org/wiki/Border_Gateway_Protocol, 30 April 2008, accessed 30 April 2008.

27. Bretheim, Sam, “Cryptographic Authentication of Navigation Protocols,” http://arxiv.org/PS_cache/cs/pdf/0510/0510022v1.pdf, pages 1-12, 9 October 2005, accessed 24 April 2008.

28. Brooker, Ralph and Dan Vorderbrueggen, “Antenna Pointing Accuracy Impact on Geostationary Satellite Link Quality and Interference,” Andrew Corporation White Paper, pages 1-13, February 2006.

29. Cameron, James, “Why not use PPTP?” http://poptop.sourceforge.net/dox/protocol-security.phtml, 10 August 2005, accessed 23 April 2008.

30. Campen, B., A. Hawrylyshen, S. Lawrence, and R. Sparks, “Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies,” http://www.ietf.org/internet-drafts/draft-ietf-sip-fork-loop-fix-06.txt, 3 November 2007, expires 6 May 2008, accessed 5 May 2008.

31. Casady, William, Donald Pfost, and Kent Shannon, “Precision Agriculture: Global Positioning System (GPS),” http://extension.missouri.edu/explore/envqual/wq0452.htm, November 1998, accessed 24 April 2008.

32. Castronova, Tony, “Earth Station Antenna Security and Survivability,” http://www.milsatmagazine.com/cgi-bin/display_article.cgi?number=589764666, MilsatMagazine.com, October 2007, accessed 18 April 2008.

33. CERT, “CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP),” http://www.cert.org/advisories/CA-2002-03.html, 13 February 2008, accessed 5 May 2008.

34. CERT, “CERT Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP),” http://www.cert.org/advisories/CA-2003-06.html, 21 May 2003, accessed 5 May 2008.

35. Chen, Hao, Denys Ma, and Radmilo Racic, “Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone’s Battery,” http://www.cs.ucdavis.edu/~hchen/paper/securecomm06.pdf, pages 1-10.

36. Cisco, “Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNS Such as ATM and Frame Relay, and Deployment Guidelines,” http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/mpvpn_wp.pdf, pages 1-13, accessed 5 May 2008.

37. CISCO, “Cisco Access Router Manager 1.1 Data Sheet,” http://www.cisco.com/en/US/products/sw/netmgtsw/ps260/products_data_sheet09186a0080141822.html, accessed 4 April 2008.

38. Cisco, “Cisco Security Response: Full-Disclosure: Multiple Vulnerabilities within Cisco EIGRP,” http://www.cisco.com/warp/public/707/cisco-sr-20051220-eigrp.shtml, 20 December 2005, accessed 30 April 2008.

39. Cisco, “Simple Network Management Protocol (SNMP),” http://www.cisco.com/warp/public/535/3.html, accessed 24 April 2008.

40. Codenomicon, “Is your Virtual Private Network really private?,” http://www.codenomicon.com/resources/whitepapers/solutions%20brief_vpn_01.07.pdf, solutions brief n.01.07, accessed 10 April 2008.

41. Cohen, Herbert D., “Spacecraft Technology for Broadcasting Satellites – An Update,” IEEE Journal on Selected Areas in Communications, Volume SAC-3, Number 1, January 1985, Manuscript received 1 August 1984 and revised 1 October 1984.

42. Collier, Mark D., “Session Initiation Protocol (SIP) Vulnerabilities,” http://www.hackingvoip.com/presentations/IPCOMM_SIP.pdf, IPCOMM 2006, slides 1-46, 25-27 September 2006, accessed 5 May 2008.

43. Collier, Mark, “The Value of VoIP Security,” http://www.callcentermagazine.com/shared/printableArticle.jhtml?articleID=22103933, 6 July 2004, accessed 14 April 2008.

44. “Community Wireless LANs: Broadband Internet by Satellite,” http://www.azurebroadband.com/services/com.htm, 9 February 2005, accessed 9 March 2008.

45. Comparetto, Gary, “Satellite Communications – Current Features and Future Trends,” originally presented at WESCON ’96, 22-24 November 1996.

46. “Computer virus,” http://en.wikipedia.org/wiki/Computer_virus, 29 April 2008, accessed 29 April 2008.

47. “Computer worm,” http://en.wikipedia.org/wiki/Computer_worm, 15 April 2008, accessed 29 April 2008.

48. COMSYS, "VSAT Network Types," http://www.comsys.co.uk/vsatnets.htm, accessed 4 April 2008.

49. Cruickshank, Dr. Haitham S., Frank Hermanns, and Sunil Iyengar, "Protection of the European Space Infrastructure," pages 1-5.

50. Dai Zovi, Dino A. and Shane A. Macaulay, "Attacking Automatic Wireless Network Selection," Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, pages 365-372, 2005.

51. Daly, John C. K., "LTTE: Technologically innovative rebels," http://www.energypublisher.com/article.asp?id=9803, 5 June 2007, accessed 21 December 2007.

52. De Avila, Joseph, "Wi-Fi Users, Beware: Hot Spots Are Weak Spots," http://online.wsj.com/article/SB120043982997492645.html?mod=rss_most_emailed_week, *The Wall Street Journal*, page D1, 16 January 2008, accessed 11 April 2008.

53. Dell Technical Support, "Urgent Driver Update to Address Security Vulnerability on Dell Wireless Network Cards," http://support.dell.com/support/topics/global.aspx/support/dsn/en/dcoument?docid=314102, 17 April 2008, accessed 21 April 2008.

54. DeVilbiss, Lt Col Stew and Dr. Richard Raines, EENG 571 Satellite Communications course notes, Winter Quarter 2006, Air Force Institute of Technology (AFIT).

55. Dittrich, Dave, "Some TCP/IP Vulnerabilities," http://staff.washington.edu/dittrich/talks/agora/, 9 December 1999, accessed 5 May 2008.

56. "DNS rebinding," http://en.wikipedia.org/wiki/DNS_rebinding, 9 April 2008, accessed 30 April 2008.

57. Elbert, Bruce and Maurice Schiff, "Simulating the Performance of Communication Links with Satellite Transponders," http://www.applicationstrategy.com/Communications_simulation.htm, 2002, accessed 3 April 2008.

58. Elbert, Bruce, "Ground Segment Engineering for Satellite Communications" training course slides, Wright-Patterson AFB, OH, August 2007.

59. "Enhanced Interior Gateway Routing Protocol," http://en.wikipedia.org/wiki/EIGRP, 30 April 2008, accessed 30 April 2008.

60. "Essential service," http://en.wikidpedia.org/wiki/Essential_service, 27 November 2007, accessed 4 April 2008.

61. "Ethernet's History and a bit of Security," http://neworder.box.sk/newsread.php?newsid=1010, 22 November 2001, accessed 23 April 2008.

62. "Executive Summary of the Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html, pp. 1-19, accessed 2 April 2008.

63. Festag, Andreas and Emanuel Fonseca, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS," http://www.network-on-wheels.de/downloads/survey_sec_routing_v1-1_cite.pdf, Version 1.1, 2 June 2006.

64. "File Transfer Protocol," http://en.wikipedia.org/File_Transfer_Protocol, 3 April 2008, accessed 7 April 2008.

65. "FM 24-11 Chapter 1 Introduction," http://www.fas.org/spp/military/docops/army/fm24-11/Ch1.htm, accessed 18 April 2008.

66. "Frequency Spectrum Congestion," http://www.its.bldrdoc.gov/fs-1037/dir-016/_2390.htm, 23 August 1996, accessed 24 April 2008.

67. Geier, Jim, "Beware of ARP Attacks," http://www.wi-fiplanet.com/tutorials/article.php/3112991, 24 November 2003, accessed 9 April 2008.

68. Geier, Jim, "Denial of Service a Big WLAN Issue," http://www.wi-fiplanet.com/tutorials/article.php/2200071, 1 May 2003, accessed 9 April 2008.

69. Geier, Jim, "Identifying Rogue Access Points," http://www.wi-fiplanet.com/tutorials/article.php/1564431, 6 January 2003, accessed 9 April 2008.

70. Gentoo Linux, "Quagga Routing Suite: Multiple vulnerabilities," http://www.gentoo.org/security/en/glsa/glsa-200605-15.xml, 21 May 2006, accessed 30 April 2008.

71. Global Crossing, "IP VPN Deep Dive," http://www.globalcrossing.com/ipkc/ipkc_ipvpn_deep_dive.aspx, accessed 5 May 2008.

72. Gnucitizen, "Total Surveillance Made Easy with VoIP Phones," http://www.gnucitizen.org/projects/total-surveillance-made-easy-with-voip-phones/, 11 February 2008, accessed 9 April 2008.

73. Grossman, Jeremiah and T.C. Niedzialkowski, "Hacking Intranet Websites from the Outside: JavaScript Malware Just Got A Lot More Dangerous," http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grossman.pdf, slides 1-36, 3 August 2006, accessed 14 April 2008.

74. Grossman, M., W.P. Osborne, D. Taylor, and C. J. Wolejsza, "Multiple Access Protocols for Data Communications via VSAT Networks," IEEE Communications Magazine, Volume 25, Number 7, pages 30-39, July 1987.

75. "Hackers attack International Space Station," http://www.securecomputing.net.au/print.aspx?CIID=107187, 2 April 2008, accessed 17 April 2008.

76. Harkins, Wilson, "Public Lessons Learned Entry: 0770, Subject: RF Breakdown Characteristics," http://www.nasa.gov/offices/oce/llis/0770.html, 1 February 1999, accessed 17 April 2008.

77. Headquarters US Army Information Systems Engineering Command, "Automated Information System (AIS) Design Guidance Long Haul Transmission Systems," http://www.fas.org/spp/military/docops/army/tmpl/longhau2.htm, 15 April 1997, accessed 9 March 2008.

78. Hickey, Andrew R., "Unified Communications News: VoIP vulnerability threatens data," http://searchunifiedcommunications.techtarget.com/news/article/0,289142,sid186_gci1267128,00.html#, 7 August 2007, accessed 9 April 2008.

79. "High-Level Data Link Control," http://en.wikipedia.org/wiki/HDLC, 29 March 2008, accessed 7 April 2008.

80. Hines, Matt, "Black Hat: Security researchers show how corporate intranets are ripe for emerging attacks," http://www.infoworld.com/article/07/08/01/black-hat-intranet-security_1.html?source=rss&url=http://www.infoworld.com/article/07/08/01/black-hat-intranet-security_1.html, 1 August 2007, accessed 14 April 2008.

81. Howell, Alan, "INMARSAT HORIZONS PROGRAM," Institution of Electrical Engineers, Savoy Place, London, 1998.

82. http://www.infosec.gov.hk/english/itpro/sectips/VPN_eng.pdf

83. https://edit.britannica.com/getEditableToc?tocId=224536

84. Hu, Yurong and Victor O. K. Li, "Satellite-Based Internet: A Tutorial," http://www.comsoc.org/ci/private/2001/mar/li.html, published in March 2001 issue of IEEE Communications.

85. Ichijo, Hiroyuki, "IMTN and managed data network services," http://www.wmo.ch/pages/prog/www/TECO-WIS/2-1-2_Japan-Ichijo_Improved-MTN.pps, Technical Conference on the WIS, slides 1-16, 6-8 November 2006, accessed 5 May 2008.

86. iDirect Technologies, "Transmission Security (TRANSEC) in an IP based VSAT Architecture," http://www.idirect-tech.com/galleries/default-file/TRANSEC%20in%20an%20IP%20based%20VSAT%20Architecturev2.pdf, pages 1-5, April 2007.

87. INTELSAT, "Intelsat Network Overview" briefing, Network Management.pdf, slides 1-38, provided by Major Paul K Harmer, USSTRATCOM/JIOWC on 18 January 2008.

88. INTELSAT, "Intelsat Technical Paper: VoIP over Satellite 2006," 5136-VoIP.pdf, pgs. 1-36, provided by Major Paul K Harmer, USSTRATCOM/JIOWC on 14 January 2008.

89. INTELSAT, "OnDemand – bandwidth on your terms," 5221-OnDemand.pdf, pgs. 1-2, August 2006, provided by Major Paul K Harmer, USSTRATCOM/JIOWC on 14 January 2008.

90. Intelsat, "Services: Telecom: VSAT: Global VSAT Services," http://www.intelsat.com, accessed 3 January 2008.

91. Irland, Kevin W., "Verizon Business Enhances Service to Help Secure Customers' IP Telephony Systems," http://newscenter.verizon.com/press-releases/verizon/2006/page.jsp?itemID=29670068, 20 June 2006, accessed 10 April 2008.

92. "IS-IS," http://en.wikipedia.org/wiki/IS-IS, 5 April 2008, accessed 30 April 2008.

93. Jackson Higgins, Kelly, "Hack Sneaks Past Firewall to Intranet," http://www.darkreading.com/document.asp?doc_id=129431, 18 July 2007, accessed 14 April 2008.

94. "Java (programming language)," http://en.wikipedia.org/wiki/Java_%28programming_language%29, 30 April 2008, accessed 30 April 2008.

95. Javvin, "TCP/IP Network Vulnerability and Security," http://www.javvin.com/networksecurity/tcpipnetwork.html, accessed 5 May 2008.

96. Joglekar, Sachin, "White Paper on Vulnerabilities in Dual-mode/Wi-Fi Phones," http://www.blackhat.com/presentations/bh-usa-07/Joglekar/whitepaper/bh-usa-07-joglekar-WP.pdf, Black Hat Briefings 2007.

97. John A. Volpe National Transportation Systems Center, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System: Final Report," http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-V4.6.pdf, prepared for the Office of the Assistant Secretary for Transportation Policy U.S. Department of Transportation, 29 August 2001, accessed 10 April 2008.

98. JPL's Wireless Communication Reference Website, "The ALOHA Protocol," http://www.wirelesscommunication.nl/reference/chaptr06/aloha.aloha.htm, accessed 3 April 2008.

99. Kaplan, Hadriel, "Securing Carrier VoIP: Session Border Control," http://www.nanog.org/mtg-0505/pdf/kaplan.pdf, slides 1-27, 15-17 May 2005, accessed 14 April 2008.

100. Kassay, David A., Thomas M. Parks, and Clifford J. Weinstein, "Vulnerabilities of Reliable Multicast Protocols," http://citeseer.ist.psu.edu/cache/papers/cs/30979/http:zSzzSzwww.ll.mit.eduzSzISTzSzpubszSzmilcom98-parkszSzmilcom98.pdf/parks98vulnerabilities.pdf, pgs. 1-5, October 1998, accessed 11 April 2008.

101. Kesden, Gregory, "Communications and Networking," http://courseweb.sp.cs.cmu.edu/~netcomm/applications/lectures/, accessed 2 January 2008.

102. Kuhlen, H.P., "An Example of On-board Processing in a Satellite Integrated Communications Network," MBB Space Systems Group, 1988.

103. "LAPB," http://en.wikipedia.org/wiki/LAPB, 3 February 2008, accessed 7 April 2008.

104. "Link Budget," http://electronica.udea.edu.co/cursos/sistemasc/LINK%20BUDGET.ppt, accessed 28 April 2008.

105. Long, Fred, Dave Price, Edel Sherratt, and Sandy Spence, "IPv4 Multicast on JANET," http://www.ja.net/documents/publications/technical-guides/ipv4-multicast-web.pdf, pgs. 1-88, April 2006, accessed 11 April 2008.

106. "Management Plan for the Internet Protocol Routing in Space (IRIS) Joint Capability Technology Demonstration (JCTD)," pgs. 1-22, 21 May 2007, received via email from Mr. Scott Anderson of SEAKR Engineering, Inc. on 30 January 2008.

107. "Market Survey of the Potential for Satellite Services in Central and Eastern Europe – Executive Summary," www.cto.cz/ukazky/master-esa.pdf, pgs. 1-22, submitted to Nathalie Ricard, European Space Research and Technology Centre, July 2004, accessed 9 March 2008.

108. Martin, Donald H., Communication Satellites, fourth edition, pp. 53-96, the Aerospace Corporation, 2000.

109. Millard, Elizabeth, "Internet Security Vulnerabilities: Tools Have Become Stronger, But So Have Digital Miscreants," http://www.processor.com/editorial/PrntArticle.asp?prnt=1&article=articles%2Fp3010%2..., Processor, Volume 30, Issue 10, 7 March 2008, accessed 21 April 2008.

110. Mimix Broadband, "Terrestrial Radio Link Solid-State TWT Replacements," http://www.mimixbroadband.com/PDFfiles/Why%20Not%20Solid-State%20-%20Mimix.pdf, 2 May 2002, accessed 3 April 2008.

111. Moran, Joseph, "Wireless Home Networking, Part III – Wi-Fi Security," http://www.wi-fiplanet.com/tutorials/article.php/1495811, 6 November 2002, accessed 9 April 2008.

112. Morphew, Graham, "IP networks get security at the edge," http://www.eetimes.com/showArticle.jhtml?articleID=16502518, 25 November 2003, accessed 17 April 2008.

113. "Multipaction," http://en.wikipedia.org/wiki/Multipaction, 27 December 2007, accessed 17 April 2008.

114. Muradian, Vago, "U.S. gauges China's anti-satellite strategy," http://www.airforcetimes.com/news/2007/02/afDFNSpace070202/, 2 February 2007, accessed 25 April 2008.

115. Network dictionary, "TCP/IP Network Vulnerability and Security," http://www.networkdictionary.com/security/tcpipnetwork.php, accessed 30 April 2008.

116. "Network Security," http://www.cs.berkeley.edu/~daw/teaching/cs261-f07/scribenotes/1009-yanpei.pdf, 9 October 2007, accessed 5 May 2008.

117. Nguyen, Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," http://www.cse.yorku.ca/~lan/seminars/icn06.ppt, slides 1-35, accessed 11 April 2008.

118. "Noise, Signal Loss and TI," http://www.geo-orbit.org/sizepgs/Noise.html, accessed 24 April 2008.

119. Novatel, "Discussions on RF Signal Propagation and Multipath," http://www.novatel.com/Documents/Bulletins/apn008.pdf, pages 1-15, 3 February 2000.

120. "Open Shortest Path First," http://en.wikipedia.org/wiki/Open_Shortest_Path_First, 17 April 2008, accessed 30 April 2008.

121. "PC Card," http://en.wikipedia.org/wiki/PC_card, 28 March 2008, accessed 7 April 2008.

122. Pedersen, Jan Petter, "Kongsberg: Satellite Services Ground Segment and Licensed Mission Operations," http://earth.esa.int/gscb/papers/13_Pedersen.pdf, pgs. 1-19, presented at GSCB Workshop, 19-20 June 2007.

123. "Peer-to-peer," http://en.wikipedia.org/wiki/Peer-to-peer, 2 April 2008, accessed 7 April 2008.

124. Pinker, Aron and Charles Smith, "Vulnerability of the GPS Signal to Jamming," http://www.springerlink.com/content/kcwbfhg5k1y7x8du/fulltext.pdf, *GPS Solutions*, Volume 3, Number 2, pages 19-27, 1999.

125. Piscitello, David, "Hot Spot or Hot Zone? Understanding the Hazards of Public WiFi LANs," http://www.corecom.com/external/livesecurity/hotspot.htm, accessed 11 April 2008.

126. Pogue, David, "How Secure Is Your Wi-Fi Connection?," http://pogue.blogs.nytimes.com/2007/01/04/04pogue-email/, 4 January 2007, accessed 11 April 2008.

127. "Point-to-Point Protocol," http://en.wikipedia.org/wiki/Point-to-Point_Protocol, 1 April 2008, accessed 7 April 2008.

128. Pozzobon, Alessandro, Oscar Pozzobon, and Chris Wullems, "Secure Tracking for Critical Applications," http://www.geospatial-solutions.com/geospatialsolutions/content/printContentPopup.jsp?id=366117, pages 1-8, 1 August 2006, accessed 16 April 2008.

129. Qualys, Inc., "Vulnerability list," http://www.internetbankingaudits.com/list_of_vulnerabilities.htm#WINDOWS, accessed 10 April 2008.

130. Rausch, Hank, "Jamming Commercial Satellite Communications During Wartime: An Empirical Study," pages 1-8, 2006.

131. Rexford, Jennifer, "Internet Routing (COS 598A): Today: Router Configuration," http://www.cs.princeton.edu/~jrex/teaching/spring2005/lectures/spring05-apr05.ppt, April 2005.

132. "Routing Information Protocol," http://en.wikipedia.org/wiki/Routing_Information_Protocol, 26 April 2008, accessed 30 April 2008.

133. Sanders, Frank H., "Measurements of Pulsed Co-Channel Interference in a 4-GHz Digital Earth Station Receiver," http://www.its.bldrdoc.gov/pub/ntia-rpt/02-393/02-393.pdf, NTIA Report 02-393, pages 1-20, May 2002.

134. Sardella, Alan, "Securing Provider Backbone Networks: Packet Filters, Traffic Shaping, and Related Best Practices," http://cn.juniper.net/solutions/literature/white_papers/200180.pdf, April 2006.

135. "Satellite Communication (TC-612)," http://radarcafe.com/documents/Satellite_Comms_Interference.pdf, accessed 21 April 2008.

136. Schneier, Bruce, "Frequently Asked Questions – Microsoft's PPTP Implementation," http://www.schneier.com/pptp-faq.html, accessed 23 April 2008.

137. Schneier, Bruce, "Schneier on Security," http://www.schneier.com/blog/archives/2008/02/voip_threats.html, Posting by Michael, 6 February 2008, accessed 14 April 2008.

138. SEAKR Engineering, Inc., "IRIS Program," slides 1-4, August 2007, received via email from Mr. Scott Anderson of SEAKR Engineering, Inc. on 30 January 2008.

139. SecuriTeam, "Attacking Automatic Wireless Network Selection," http://www.securiteam.com/securityreviews/5ZP0L1FHGY.html, 23 January 2006, accessed 21 April 2008.

140. "Session initiation protocol (SIP) essentials," http://searchtelecom.com/generic/0,295582,sid103_gci1263339,00.html, 5 July 2007, accessed 5 May 2008.

141. Shaun2k2, "TCP/IP Vulnerabilities and Weaknesses," http://www.governmentsecurity.org/archive/t1753.html, 23 August 2003, accessed 5 May 2008.

142. "Sipera LAVA Tool: VoIP Vulnerability Analysis," http://www.sipera.com/index.php?action=products,lava, accessed 9 April 2008.

143. Sklar, Bernard, Digital Communications – Fundamentals and Applications, 2nd Edition, pp. 689-707, Prentice Hall PTR, 2001.

144. "Slashdot|Sri Lankan Terrorists Hack Satellite", http://it.slashdot.org/article.pl?sid=07/04/13/068222, posted by CowboyNeal, 13 April 2007, accessed 21 December 2007.

145. "Space-Based Internet," http://www.cisco.com/web/strategy/docs/gov/GroundSpace_Words_300.pdf, accessed 2 April 2008.

146. Space Security Index 2007, http://www.spacesecurity.org/SSI2007.pdf, pp. 14-132, August 2007.

147. Space Systems/Loral, "Space Systems/Loral Wins Contract to Build New Satellite for INTELSAT Corporation," http://ssloral.com/html/pressreleases/pr20070119.html, 19 January 2007, accessed 2 April 2008.

148. "Spyware," http://en.wikipedia.org/wiki/Spyware, 28 April 2008, accessed 29 April 2008.

149. "Surecom Router SNMP Default Community Strings Vulnerability," http://www.securityfocus.com/bid/6176/info, discovery of vulnerability credited to Andrei Mikhailovsky, 13 November 2002.

150. The Internet Encyclopedia of Science, Satellites & Space Probes, Intelsat, http://www.daviddarling.info/encyclopedia/I/Intelsat.html, accessed 2 January 2008.

151. TLS, LLC Geolocation Products, http://www.tls2000.com/Products.html, accessed 27 December 2007.

152. Totsline, Gregory, "Issues When Using IPsec Over Geosynchronous Satellite Links," www2.sans.org/reading_room/whitepapers/vpns/770.php?portal=b0d02654be90d30da02b794c74805823, pages 1-11, 12 August 2002.

153. U.S. Department of Energy Computer Incident Advisory Capability, "S-242: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720," http://www.ciac.org/ciac/bulletins/s-242.shtml, 27 March 2008, accessed 30 March 2008.

154. Van Fleteren, Stephan, "Traveling Wave Tube vs. Solid State Amplifiers," http://www.djmelectronics.com/articles/twt-vs-solid-state.html, 2000, accessed 3 April 2008.

155. Veeneman, Dan, "Hypothetical Attacks," http://www.decodesystems.com/attacks.html, 2 November 2002, accessed 16 April 2008.

156. “Very small aperture terminal,” http://en.wikipedia.org/wiki/VSAT, 30 March 2008, accessed 4 April 2008.

157. ViaSat, Inc., “VSAT: Case Studies: Intelsat: Intelsat Broadband VSAT Network,” http://www.viasat.com, accessed 3 January 2008.

158. Wetzer, J.M. and P.A.A.F. Wouters, “The Design of High-Voltage Insulators for Spacecraft Traveling Wave Tubes,” http://ieeexplore.ieee.org/iel2/654/6327/00247058.pdf, pgs. 1-5, presented at 1992 IEEE International Symposium on Electrical Insulation, 7-10 June 1992.

159. Wotton, Peter, “Providing reliable sensing and control using ZigBee wireless networks,” http://rfdesign.com/next_generation_wireless/short_range_wireless/radio_providing_reliable_sensing/, 1 July 2006, accessed 21 April 2008.

Vita

Jessica A. Steinberger was born at Fremont Memorial Hospital in Fremont, OH in 1982. She graduated from Fremont Ross High School in 2000. She chose to attend the University of Cincinnati in Cincinnati, OH, and graduated from that institution in June 2005. While a student at the University of Cincinnati, she participated in the cooperative education program through the College of Engineering through which she co-oped at General Electric Aircraft Engines in Evendale, OH and National Aeronautics and Space Administration (NASA) Kennedy Space Center in Cape Canaveral, FL. She received her Bachelor's of Science Degree in Aerospace Engineering, with a business certificate in French.

Upon graduation from the University of Cincinnati, Ms. Steinberger began working at the National Air and Space Intelligence Center (NASIC) at Wright-Patterson Air Force Base, OH. Through the Long-Term, Full-Time (LTFT) training program offered at NASIC, she was able to take courses at the Air Force Institute of Technology (AFIT). She will graduate from AFIT in June 2008, with a Master's Degree in Astronautical Engineering. After graduation she will return to NASIC and resume her position as a communications satellite systems analyst.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)* 19-06-2008	**2. REPORT TYPE** **Master's Thesis**	**3. DATES COVERED** *(From – To)* Jan 2006 – Jun 2008

4. TITLE AND SUBTITLE

A SURVEY OF SATELLITE COMMUNICATIONS SYSTEM VULNERABILITIES

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Steinberger, Jessica A.

5d. PROJECT NUMBER
08-269

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GA/ENG/08-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Maj. Paul Harmer
USSTRATCOM JIOWC/JEWC/EW2
2 Hall Blvd; Suite 217
San Antonio, TX 78243-7074
Paul.Harmer@jiowc.osis.gov DSN: 945-4752

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The U.S. military's increasing reliance on commercial and military communications satellites to enable widely-dispersed, mobile forces to communicate makes these space assets increasingly vulnerable to attack by adversaries. Attacks on these satellites could cause military communications to become unavailable at critical moments during a conflict. This research dissected a typical satellite communications system in order to provide an understanding of the possible attacker entry points into the system, to determine the vulnerabilities associated with each of these access points, and to analyze the possible impacts of these vulnerabilities to U.S. military operations. By understanding these vulnerabilities of U.S. communications satellite systems, methods can be developed to mitigate these threats and protect future systems.

This research concluded that the satellite antenna is the most vulnerable component of the satellite communications system's space segment. The antenna makes the satellite vulnerable to intentional attacks such as: RF jamming, spoofing, meaconing, and deliberate physical attack. The most vulnerable Earth segment component was found to be the Earth station network, which incorporates both Earth station and NOC vulnerabilities. Earth segment vulnerabilities include RF jamming, deliberate physical attack, and Internet connection vulnerabilities. The most vulnerable user segment components were found to be the SSPs and PoPs. SSPs are subject to the vulnerabilities of the services offered, the vulnerabilities of Internet connectivity, and the vulnerabilities associated with operating the VSAT central hub. PoPs are susceptible to the vulnerabilities of the PoP routers, the vulnerabilities of Internet and Intranet connectivity, and the vulnerabilities associated with cellular network access.

15. SUBJECT TERMS

Communications satellite, vulnerabilities, attack, IRIS, Internet Routing in Space, INTELSAT

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. R. A. Raines (ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, e-mail: Richard.Raines@afit.edu
U	U	U	UU	139	