Global Information Assurance Certification Paper

Security on Internet Satellite - any different than Wired or Wireless?

Nancy Voorhis
SANS Security Essentials
GSEC Practical Assignment - Part 1 (paper)
Version 1.2c
May 28, 2001

Introduction

On May 24, 2001, Michael L. Cook, Vice President and General Manager of Hughes Network System's Spaceway™ global broadband satellite network system testified before the U.S House of Representatives Small Business Committee with the following statement "Our message to you today is simple. The only technology that will ubiquitously provide cost-effective broadband access across the entire United States is satellite technology." Cook was testifying before the committee to advocate further opening of bandwidth licensing to allow their DirectPC product, a satellite Internet service, to reach further into the consumer market place.

There has been increasing discussion and awareness about wireless security. Any number of references point out that the demand to be free of the wire is on the increase. Most information systems professionals would probably agree with Sean P. McAleer that "These [wireless] devices are here to stay" [PCM] and have increasing awareness that wireless systems have vulnerabilities not present in wired systems. These vulnerabilities need to be addressed if the same level of security is to be present on connections regardless of whether they are made across a wired or wireless medium [MCM][CH].

The recent discussion of wireless security has tended to focus on the threats to wireless LAN's, PDA's and other mobile technologies and the new protocols, such as Bluetooth, being developed for wireless. One type of wireless that has not yet received much attention is that of satellite Internet communications. Satellite links have been providing data services for some time now, providing global links for Internet Service Providers and multicast links for video conferencing, distance learning and other IP multicast applications. Development of satellite technology, investment in infrastructure, lowering prices and consumer demand for more bandwidth are bringing satellite technology to the consumer market place, and making it competitive with terrestrial technologies such as DSL and cable services. Announcements such as the one made on May 14, 2001 by Gilat Satellite Networks Ltd. and partners "Star One, UOL and Gilat Satellite Networks' StarBand Latin America business introduce Brazil's first consumer two-way satellite, broadband Internet service" [GIL] are being made almost weekly and are likely to continue. The Gartner Group states in their January, 2001 report on the future of small and midsize business networking, "Satellite services make sense where other broadband alternatives are unavailable (e.g. rural areas or in less-developed countries)." [GAR]

There are currently 200 operational satellites, with the total predicted to rise to over 2000 by 2008 [TIA].

It seems clear that the use of satellites for providing broadband Internet access to the consumer market has only just begun. So what's the deal? Is satellite just another wireless technology with the same threats and risks as any other wireless technology?

Characteristics of Internet Satellite Technology

Broadband Internet Satellite consumer services are currently being deployed using 2 main types of technology. The 2 types of systems are commonly referred to as "one-way" and "two-way" systems. The one-way systems are also referred to as hybrid satellite-terrestrial systems. They require a standard terrestrial link (dial-up or otherwise) and work by sending outgoing requests on the terrestrial link, with inbound traffic returning on the satellite link. Systems typically use a satellite card and a satellite dish installed at the end user site and work in conjunction with a proxy server/gateway which makes the actual request to the destination host and communicates the response back via the satellite. Further explanation of the topology of these systems can be found in the research paper "Asymmetric Internet Access over Satellite-Terristrial Networks" [ASBD].

More recently being deployed are "two-way systems" which provide a data path for both upstream and downstream data. These systems also use a satellite card and a satellite dish installed at the end user site and bi-directional communication occurs directly between the end user node and the satellite.

Both technologies have asymmetric speeds, providing faster download speeds than upload speeds. Maximum download speeds on systems currently deployed range from 400Kbps - 2200 Kbps and are higher for future planned systems (see Table). Upload speeds for one-way systems are based on the speed of the terrestrial link, while upload speeds for two-way systems range from 20 Kbps - 20 Mps. The speeds experienced by users can be affected by atmospheric conditions, and actual speeds reported by users vary considerably.

More technically, communication satellites being used to provide broadband Internet access are commonly Geostationary Orbit (GSO) or Low Earth Orbit (LEO) orbiting at 22,300 m and less than 1000 miles respectively, as well as Middle Earth Orbit (MEO) satellites . Satellite signals are currently limited to the operating in the C band (6GHz (uplink) and 4GHz (downlink), in the Ku band (14/12 GHz) and the Ka band (30/20 GHz).

Several key differences exist between satellite and other wireless technologies. One of the major differences is the long distance the signal must travel between earth and the satellite. The longer the distance, the longer the propagation time for the signal, creating

latency (delayed response time) at the end user node. Using satellites that are closer to the earth (LEO) to reduce propogation times requires using additional techniques to address the use of multiple satellites to provide continuous cover at the user (terrestrial) node. Another difference in the technology, also due to the distance the signal must travel, is that the link has a decreasing signal-to-noise ratio with increasing distance. This results in susceptibility of the link to atmospheric effects such as rain, distortion created by large objects such as buildings being in the path and higher error rates. A further difference is that satellite links have considerably higher bandwidth potential available. The theoretical throughput for VSAT systems is 40 Mbps downstream and 76.8 Kbps upstream and satellites planning to be deployed have even higher rates.

Security Threats

What do these differences imply in terms of security? Do the risks differ than those for wired or wireless? Is it not possible to use the techniques that are available for assuring the integrity, confidentiality and authenticity of data travelling a wired and wireless medium on satellite links? While some of the threats on a satellite link include those for wireless LAN's [MCM], satellite transmission has unique characteristics that demand security be approached and solutions found which are specifically for satellite transmissions.

Similar to wireless communications, one of the threats to the confidentiality of the data is the potential for eavesdropping on the satellite link. The threat of eavesdropping is far greater than on a land link, given that eavesdropping can occur without detection anywhere within the location within the range of reception. For satellite links, this range is large, very large. Eavesdropping could also be used to launch an availability attack [NASA1].

In general, the systems all use some combination of access technologies, which are required to share the satellite channel amongst many ground receivers. These are code division multiple access (CDMA), time division multiple access (TDMA) and frequency division multiple access (FDMA) and their variations, and make it "at least as difficult as it will be to intercept a digital cellular signal" [BYTE] . Additional deterrents are "that the resources needed to monitor a satellite link are not trivial" [NASA1]. Also in use is the technique of frequency hopping such as that used in the "Bluetooth" wireless standard, which is a deterrent, but is more effective when used in conjunction with an encryption scheme [CH].

All of the satellite systems being deployed and planned for include a terrestrial component: a proxy gateway in the one-way systems or a satellite hub as in the StarBand two-way system. This introduces the same threats that exist for wired communications as the data also will travel across standard terrestrial links and requires that end-to-end security mechanisms should be considered [NASA1].

Issues arise when considering end-to-end security mechanisms for satellite links. Just use a Virtual Private Network (VPN), right? Well, not exactly. The latency in the satellite signal has caused considerable research to be done into enhancing the parameters used for TCP packets in order to boost the performance. Some of the techniques being used impact the ability to apply end-to-end security to the link. TCP Spoofing is a technique that allows splitting of the TCP control link, isolating the satellite portion of the TCP/IP link from the terrestrial portion and allows modifications to the TCP parameters used for the satellite portion of the link, such as window size, that are optimized for the characteristics of the satellite link [ASBD]. According to research done by Byte Magazine's John Montgomery in 1997 and Hughes Network Systems's (HNS) Dennis Conti, " HNS has been using this technique for over three years to deliver Internet/intranet content at high speed to both consumers and enterprises" yet there exists research which indicates that "this [TCP spoofing] protocol is currently incompatible with end-to-end IP security protocols." [ATM]. In some cases, such as the DirecPC system, a VPN is already in use and therefore the customer cannot set up their own VPN (see Table).

Another technique being suggested by research for improving the performance of TCP over the satellite link is the extension for transactions (T/TCP). This technique would allow data to be sent along with the initiating SYN packet of the TCP connection. Along with the recognition of the potential for decreasing the TCP connection setup time is also the recognition of security implications that have already been identified with sending data in the first segment. [NASA2]

Currently Deployed or Planned for Deployment Satellite Systems

The table below lists some of the main characteristics of a sample of Internet Satellite consumer services currently deployed or planned for deployment. Any information regarding the security of a system that was stated at the product web site, press release information or that was determined to be available to an average consumer is listed. The availability of the information regarding the security measures being deployed are given a rating (poor, medium, good), reflecting the ease with which security information is obtainable.

Table. Main Characteristics of a Sampling of Internet Satellite Consumer Services

System Name	DirecPC	DirecPC Satellite Return	Starband	GSI	AstroLink	Internet-In-The-Sky
System Type	one-way	two-way	two-way	one-way	two-way	two-way

Satellite Type	GEO	GEO	GEO (Gilat GE-4 or Telstar 7)	GEO	GEO	LEO
Spectrum	unknown	unknown	Ku-band/ C-band	Ku-2 band (business solution)	Ka-band	Ka-band
Date of Deployment	currently available	currently available	currently available	currently available	2003	2005
Target Market	consumer	consumer	consumer	consumer, business	corporate, government	not specific but includes "e-commerce, telemedicine, sales support"
Download speed (maximum)	400 Kbps	2200 Kpbs	500 Kbps	500 Kbps	155 Mbps	64 Mbps
Upload speed (maximum)	n/a	128 Kpbs	150 Kbps	n/a	800 Kbps, 4 Mbps, 20 Mpbs	2 Mbps
Field tested speeds reported from user base (average)	200 Kbps	2166/19 Kbps (off peak - 5:30AM Sunday)	none	none	n/a	n/a
System security as stated in marketing information or by company contact	"56-bit DES (Digital Encryption Standard) to encrypt information flowing between a modem and gateway to the Internet" "DirecPC also uses CAS (Condition Access System) to provide one more layer."	none	"certain applications do not perform efficiently in a satellite-delivered environment, such as ...VPN services..." " Thanks to the secure firewall and	"Data transmitted through the GSI satellite link uses the most secure encryption method of data transport currently available. GSI provides the functions of a traditional firewall since the only inbound access from the Internet is	"customers will be able to configure virtual private networks (VPN's)"	none

	"Because DIRECPC is already using VPN You can not use VPN on it."		anti-virus protection of WinProxy, StarBand users can be protected against Internet intruders and Web-borne viruses." "prefer not to discuss our security measures" [SDC]	downloaded information through the satellite connection." Gateway login client provided employing128-bit encryption and Mac HW address authentication.		
Availability of security information	medium	poor	poor	good	good	poor
Web site	direcpc.com directpc.com	direcpc.com	starband.com gilat.com	rapidwireless.com networkalpha.com	astrolink.com	teledisc.com

The table indicates that there is limited information available regarding the security measures being deployed. In some cases, the information is somewhat misleading. For example, the StarBand information implies that a firewall at the end user node provides security. While a firewall is a recommended security measure for a satellite link which is an 'always on' connection, it functions only to prevent inbound attacks, and does not address link transmission security. The development and deployment of security measures seems much the same as in 1997 when Byte magazine's John Montgomery reported "All the vendors I spoke with told me that they were aware of the potential security concerns that customers would have. Few, however, had concrete solutions".

Conclusion

On the horizon, is the potential for large number of consumers to be using satellite links to do everything they currently do "on the Internet", including financial transactions and e-commerce. The need to ensure the security of their data is critical. A glance at the technology indicates there is a need for increased awareness both by companies

deploying the technology and consumers using the technology of the need for the deployment of end-to-end security.

While larger organizations are quickly becoming familiar with the unique aspects of security risks posed by wireless connections and are integrating security for wireless connections into their security policies, other consumers targeted by this new market need more information from the companies deploying the technology about the security measures being used on the system. There is also a need for increasing consumer's awareness of the security threats posed by an Internet satellite service.

The large bandwidth available in a satellite link allows the possibility of applying techniques of strong encrpytion and authentication that use processing and bandwidth which may not be feasible for typical wireless LAN or PDA like devices. Techniques being proposed for wireless links are frequently based on the premise that there are "limitations in bandwith, CPU and memory resources, battery life and user interface" [VERI]. There is a need for development of security services that are unique to satellite systems, that can take advantage of the characteristics of satellite links, and can specifically address the modifications being made in the TCP/IP protocol to enhance the performance over satellite links. It's not just another wireless technology.

References

[MLC] Cook, Michael L. "Eliminating the Digital Divide… Who Will Wire Rural America?" http://www.hns.com/news/pressrel/cook_testm_5-24-01.htm Hearing before the U.S. House of Representatives Committee on Small Business Subcommittees on Regulatory Reform and Oversight and on Rural Enterprises, Agriculture and Technology, Hughes Network Systems, May 24, 2001.

[GRT] Pultz, Jay. It's No Pipe Dream: The Future SMB Network Is Broadband. Gartner Group Report. http://www.gartner.com. COM-12-7786. 10 January 2001

[GIL] "Star One, UOL and Gilat Satellite Networks' StarBand Latin America business introduce Brazil's first consumer, two-way satellite, broadband Internet service". http://www.gilat.com/gilat/, Gilat Press Release, May 14, 2001.

[TIA] Highlights of the Workshop on Global Assessment of Satellite Communications Technology and Systems. http://www.tiaonline.org/about/satellite_workshop.cfm, Telecommunications Industry Assocation White Paper, December, 3, 1997.

[MCM] McMurry, Mike. Wireless Security. http://www.sans.org/infosecFAQ/wireless/wireless_sec.htm, SANS Information Security Reading Room, January 22, 2001.

[SPM] McAleer, Sean P. Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs. http://www.sans.org/infosecFAQ/wireless/defense.htm, SANS Information Security Reading Room. January 24, 2001.

[CH] Harrison, Craig. The Wireless Confusion. http://www.sans.org/infosecFAQ/wireless/wireless_confusion.htm, SANS Information Security Reading Room. November 13, 2000.

[BYTE] Montgomery, John. The Orbiting Internet: Fiber in the Sky. http://www.byte.com/art/9711/sec5/art1.htm Byte Magazine, November, 1997.

[ASBD] Arora, V., Suphasindhu, N. , Baras, J.S., Dillon, D. Asymmetric Internet Access over Satellite-Terrestrial Networks. http://www.ccsds.org/documents/pdf/CCSDS-713.5-B-1.pdf, CSHCN T.R. 96-10 (ISR T.R. 96-28).

[NASA1] Allman, M., Glover, D., Sanchez, L. Enhancing TCP Over Satellite Channels using Standard Mechanisms. http://roland.grc.nasa.gov/~mallman/papers/rfc2488.txt, RFC 2488, January, 1999.

[NASA2] Edited by M. Allman.Ongoing TCP Research Related to Satellites. http://roland.grc.nasa.gov/~mallman/papers/rfc2760.txt, RFC 2760, February, 2000.

[SDC] Phone and email communication with Sandy Colony, Starband Communications, May 21, 2001.

[ATM] Rohit Goyal, Raj Jain, Mukul Goyal, Sonia Fahmy, Bobby Vandalore (Ohion State University) and Tom vonDeak (NASA Lewis Research Center). Traffic Management in ATM Networks Over Satellite Links. http://tcpsat.grc.nasa.gov/tcpsat/other-docs/atm-tm.pdf, DRAFT TIA bulletin.

[VERI] Wireless Trust Services from Verisign. http://www.verisign.com, Verisign White Paper.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor