

A Brief Overview on **SATELLITE HACKING**

By Anchises Moraes Guimarães de Paula, *iDefense*



As a large portion of worldwide Internet users increasingly rely on satellite communication technologies to connect to the Web, a number of vulnerabilities within these connections actively expose satellites to potential attacks. The implications of such a successful attack are massive, as satellites are the only means of broadcasting communications in many regions around the globe and an attacker could act from everywhere.

Broadband Internet access via satellite is available almost worldwide. Satellite Internet services are the only possible method of connecting remote areas, the sea or countries where traditional Internet cable connections are still not accessible. Satellite communications are also widely adopted as backup connection providers by several organizations and countries for those times when the terrestrial communications infrastructure is not available, damaged or overloaded. By the end of 2008, an estimated 842,000 US consumers relied on satellite broadband Internet access.¹

Communications satellites routinely receive and rebroadcast data, television, image and some telephone transmissions without the proper security measures, leading to frequent fraud and attacks against satellite services. Traditional fraud techniques and attack vectors include satellite TV hacking and the use of illicit decoding technology to hack into television satellite signals. In addition, satellite communications are easily susceptible to eavesdropping if not properly encrypted.

SATELLITE BASICS

Satellites are an essential part of our daily lives. Many global interactions rely on satellite communications or satellite-powered

services, such as Global Positioning Systems (GPSs), weather forecasts, TV transmissions and mapping service applications based on real satellite images (such as Google Maps). "Although anything that is in orbit around Earth is technically a satellite, the term "satellite" typically describes a useful object placed in orbit purposely to perform some specific mission or task."² There are several satellite types, defined by their orbits and functions: scientific, Earth and space observation, reconnaissance satellites (Earth observation or communications satellites deployed for military or intelligence applications) and communications, which include TV, voice and data connections. Most satellites are custom built to perform their intended functions.

Organizations and consumers have used satellite communication technology as a means to connect to the Internet via broadband data connections for a long time. Internet via satellite provides consumers with connection speeds comparable or superior to digital subscriber line (DSL) and cable modems. Data communication uses a similar design and protocol to satellite television, known as Digital Video Broadcasting (DVB), a suite of open standards for digital television. DVB standards are maintained by the DVB Project, an international industry consortium. Services using DVB standards are available on every continent with more than 500 million DVB receivers deployed, including at least 100 million satellite receivers.³ Communications satellites relay data, television, images

and telephone transmissions by using the transponder, a radio that receives a conversation at one frequency and then amplifies it and retransmits the signal back to Earth on another frequency that a ground-based antenna may receive. A satellite normally contains 24 to 32 transponders, which are operating on different frequencies.⁴

Modern communications satellites use a variety of orbits including geostationary orbits,⁵ Molniya orbits,⁶ other elliptical orbits and low Earth orbits (LEO).⁷ Communications satellites are usually geosynchronous because ground-based antennas, which operators must direct toward a satellite, can work effectively without the need to track the satellite's motion. This allows technicians to aim satellite antennas at an orbiting satellite and leave them in a fixed position. Each satellite occupies a particular location in orbit and operates at a particular frequency assigned by the country's regulator as the Federal Communications Commission (FCC) in the U.S. The electromagnetic spectrum usage is regulated in every country, so that each government has its regulatory agency which determines the purpose of each portion of radio frequency, according to international agreements.

The satellite provider supports Internet access and Internet applications through the provider teleport location, which connects to the public switched telephone network (PSTN) and the Internet. There are three types of Internet via satellite access: one-way multicast, unidirectional with terrestrial return and bidirectional access. One-way multicast transmits IP multicast-based data, both audio and video; however, most Internet protocols will not work correctly because they require a return channel. A single channel for data download via a satellite link characterizes unidirectional access with terrestrial return, also known as "satmodem" or a "one-way terrestrial return" satellite Internet system, and this type of satellite access uses a data uplink channel with slower speed connection technologies (see Exhibit 1).

Unidirectional access systems use traditional dial-up or broadband technology to access the

Exhibit 1. Unidirectional Access with Terrestrial Return (also known as Satmodem)⁸



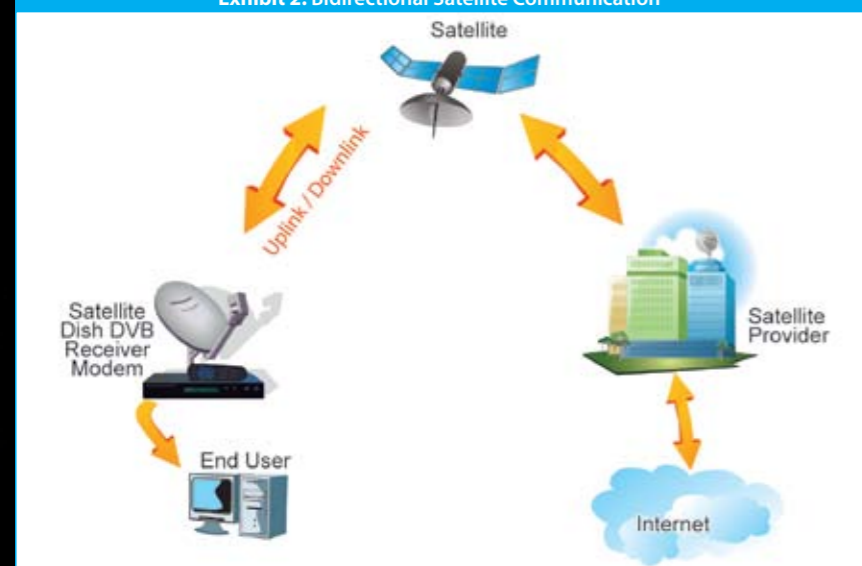
Internet, with outbound data traveling through a telephone modem or a DSL connection, but it sends downloads via a satellite link at a speed near that of broadband Internet access. Two-way satellite Internet service, also known as bidirectional access or "astro-modem," involves both sending and receiving data via satellite to a hub facility, which has a direct connection to the Internet (see Exhibit 2).

The required equipment to access satellite communication includes a satellite dish, a receiver for satellites signals, which is a low-noise block (LNB) converter, a decoder, a satellite modem and special personal-computer software. Usually, a single device or PCI card integrates the decoder and modem. Several software programs and online tools are widely available.

Satellite Internet customers range from individual home users to large business sites with several hundred users. The advantages of this technology include a greater bandwidth than other broadband technologies, nearly worldwide coverage, and additional support to television and radio services. Satellite broadband service is available in areas that terrestrially based wired technologies (e.g., cable and DSL) or wireless technologies cannot operate. The disadvantages, however, are numerous: weather conditions (rain, storms or solar influences) might affect satellite communications, satellites demand expensive hardware and have a complex setup (install-

Satellites are an essential part of our daily lives. Many global interactions rely on satellite communications or satellite-powered services.

Exhibit 2. Bidirectional Satellite Communication⁹



ing a satellite dish takes some knowledge to configure the satellite's polarization and orientation), and the satellite providers charge relatively high monthly fees. Moreover, many types of applications, such as voice-over Internet protocol (VoIP) and videoconferencing, are not suitable for this type of connection due to the high latency. Typical satellite telephone links have 550- 650 milliseconds of round-trip delay up to the satellite and back down to Earth.¹⁰

RESEARCH ON HACKING SATELLITES

Typical attacks against satellite networks include satellite television hacking (the use of illegal reprogrammed descrambler cards from legitimate satellite equipment to allow unlimited TV service without a subscription)¹¹ and hacking into satellite networks to transmit unauthorized material, such as political propaganda.¹² In March 2009, Brazilian Federal Police arrested a local group that was using U.S. Navy satellites for unauthorized communication.¹³ According to WIRED, "to use the satellite, pirates typically take an ordinary ham radio transmitter, which operates in the 144- to 148-MHZ range, and add a frequency doubler cobbled from coils and a varactor diode." Radio enthusiasts can buy all the hardware near any truck stop for less than USD \$500, while ads on specialized websites offer to perform the conversion for less than USD \$100.¹⁴ To help the industry fight such incidents, information security researchers have been investigating the inherent security, de-

Radio enthusiasts can buy all the hardware near any truck stop for less than USD \$500.

sign and configuration flaws in publicly accessible satellite communication networks and protocols, and they are making impressive progress.

In 2004, security researcher Warezman presented early studies on satellite hacking at the Spanish conference UNDERCON 0x08.¹⁵ In July 2006, Dan Veeneman presented additional studies on satellite hacking at Defcon 04.¹⁶ Recently, various security researchers are leading the innovation in this area, notably, Jim Geovedi, Raditya Iryandi and Anthony Zboralski from the consulting company Bellua Asia Pacific; Leonardo Nve Egea from the Spanish information security company S21SEC; and white-hat hacker Adam Laurie, director of security research and consul-

tancy at Aperture Labs Ltd.

In September 2006, Geovedi and Iryandi presented a "Hacking a Bird in the Sky"¹⁷ talk about hijacking very small aperture terminal (VSAT) connections at the 2006 Hack in the Box security conference (HITBSecConf2006) in Malaysia.¹⁸ They listed various hypothetical attacks against satellite communication systems, such as denial of service (DoS) conditions (uplink or downlink jamming, overpower uplink) and orbital positioning attacks (raging transponder spoofing, direct commanding, command replay, insertion after confirmation but prior to execution), and gave a presentation about how to get access to the data link layer. Later, at the 2008 edition of the Hack In The Box Security Conference, Geovedi, Iryandi and Zboralski gave a presentation about how to compromise the satellite communication's network layer and how to run a practical "satellite piggybacking" attack, which exploits the satellite trust relationship on a VSAT network by finding a "free" (unused) frequency range inside a user-allocated frequency to transmit and receive data.

At the February 2009 Black Hat DC conference, Adam Laurie presented how to hack into satellite transmissions using off-the-shelf components that Laurie assembled himself by spending just \$785 US. Laurie claimed that he has been doing satellite feed hunting¹⁹ since the late 1990s. By using a modified Dreambox, a German receiver for digital TV and

radio programs based on a Linux operating system, he was able to monitor Internet satellite transmission and to pipe its feed into his laptop. From there, he could analyze packets using standard programs such as the popular network protocol analyzer Wireshark. According to The Register, "Laurie has also developed software that analyzes hundreds of channels to pinpoint certain types of content, including traffic based on transmission control protocol (TCP), user datagram protocol (UDP), or simple mail transfer protocol (SMTP). The program offers a 3D interface that allows the user to quickly isolate e-mail transmissions, Web surfing sessions or television feeds that have recently been set up."²⁰

In 2009, Leonardo Nve, a Spanish senior security researcher, presented his experiments on satellite communications security at several conferences around the world, including the Argentinean Ekoparty²¹ and the t2'09 Information Security Conference in Finland,²² as well as the 2010 edition of BlackHat DC, among others. His investigation is concentrated on malicious attacks on satmodem communications and how to get an anonymous connection via the satellite provider's broadband network. Previously, satellite studies focused only on feeds interception and data capture, since researchers were focusing on passive vulnerabilities. Nve was able to run active attacks against the satellite clients and providers using easy-to-find tools such as a satellite dish, an LNB, cables, support, a digital video broadcast (DVB) system PCI card, a Satfinder tool and a Linux box with the necessary free software, such as Linuxtv, kernel drivers for DVB PCI cards, Linuxtv application tools and DVBSnoop (a DVB protocol analyzer console available at <http://dvbsnoop.sourceforge.net>), and the Wireshark tool for data capture.²³

Nve based his attack research on finding open Internet satellite connections by running blind scans on available satellite channels and hacking into DVB protocol. During his tests, he was able to capture 7,967 data packets from typical Internet traffic in just 10 seconds. According to his reports, data packets transmitted most of the sensitive communication in plain text with no encryption.²⁴

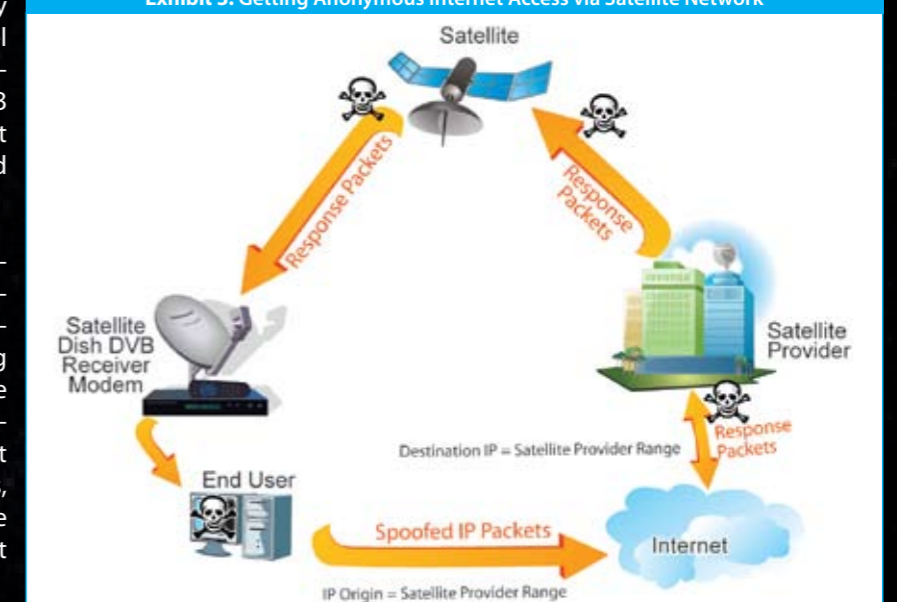
To get an anonymous Internet connection via the satellite broadband network, Nve used this local Internet access connection as an uplink and the hacked satellite connection as a downlink since he had the necessary means to capture all satellite traffic, including the IP response packets. By figuring out the ISP satellite IP address range and using a satellite IP address not in use, Nve established a TCP connection by sending packets with the spoofed satellite network's IP address via his local Internet connection (a dial-up or regular broadband connection) and he received the response by sniffing the packets via the satellite interface (see Exhibit 3).

Such attack is virtually untraceable, once the attacker can establish his or her connection from anywhere in the world, due to the fact that the satellite signal is the same for everyone within the satellite coverage area. That is, if a user based in Berlin uses a satellite company that provides coverage throughout Europe, a malicious user could capture the downstream channel in Sicily or Paris. This technique leads to several new possible attacks, such as domain name system (DNS) spoofing, TCP hijacking and attacking generic routing encapsulation (GRE) protocol.

Proven insecure, satellite communications provide almost no protection against unauthorized eavesdropping since they broadcast all communications to a large area without

... Data packets transmitted most of the sensitive communication in plain text with no encryption.

Exhibit 3. Getting Anonymous Internet Access via Satellite Network



[INFORMATION SECURITY]

proper confidentiality controls. Various passive and active threats against insecure Internet satellite communications include sniffing, DoS attacks and establishing anonymous connections. Hacking into satellite receivers is much easier now than it was in the past, thanks to the widespread availability of Linux tools and several online tutorials.

CONCLUSION

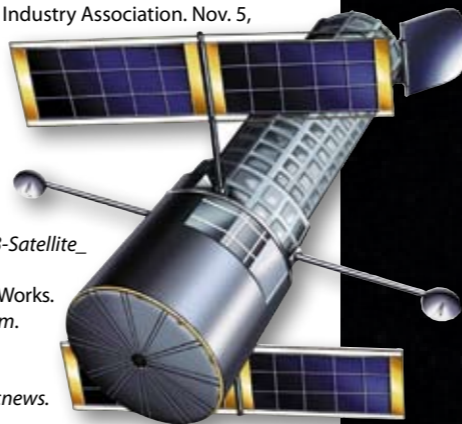
Governmental, Military organizations and most of the companies included within the critical infrastructure sector such as transport, oil and energy, are using satellite communications for transmitting sensitive information across their widespread operations. This includes the use of satellite communication at industrial plants operating supervisory control and data acquisition (SCADA) systems. The relevance of satellite communication protection and the consequences of a security incident should enforce these organizations to deploy additional security measures to their internal communication technologies. Companies and organizations that use or provide satellite data connections must be aware of how insecure satellite connections are and aware of the possible threats in this environment. Companies and users must implement secure protocols to provide data protection, such as virtual private network (VPN) and secure sockets layer (SSL), since most traffic transmits unencrypted and is widely available in a large geographic area under the satellite's coverage.


ABOUT THE AUTHOR

Anchises M. G. de Paula, CISSP, is an International Cyber Intelligence Analyst at iDefense, a VeriSign company. He has more than 15 years of strong experience in Computer Security, and previously worked as Security Officer in Brazilian telecom companies before becoming Security Consultant for local infosec resellers and consulting companies. Anchises holds a Computer Science Bachelor degree from Universidade de Sao Paulo (USP) and a master degree in Marketing from ESPM. He has also obtained various professional certificates including CISSP, GIAC (Cutting Edge Hacking Techniques) and ITIL Foundations. As an active member of Brazilian infosec community, he was the President of ISSA Chapter Brazil in 2009 and one of the founding members of Brazilian Hackerspace and Brazilian Cloud Security Alliance chapter. •

>>REFERENCES

1. "State of the Satellite Industry Report." June 2009. Satellite Industry Association. http://www.sia.org/news_events/2009_State_of_Satellite_Industry_Report.pdf.
2. Brown, Gary. "How Satellites Work." HowStuffWorks. <http://science.howstuffworks.com/satellite1.htm>. Accessed on Nov. 5, 2009.
3. "Introduction to the DVB Project." Mar. 23, 2010. DVB. http://www.dvb.org/technology/fact_sheets/DVB-Project_Factsheet.pdf.
4. "Satellite Technology." Nov. 5, 2009. Satellite Broadcasting & Communications Association (SBCA). <http://www.sbca.com/receiver-network/satellite-receiver.htm>.
5. Geostationary orbits (also called geosynchronous or synchronous orbits) are orbits in which a satellite always positions itself over the same spot on Earth. Many geostationary satellites (also known as Geostationary Earth Orbits, or GEOs) orbit above a band along the equator, with an altitude of about 22,223 miles. (Brown, Gary. "How Satellites Work." HowStuffWorks. <http://science.howstuffworks.com/satellite5.htm>. Accessed on Nov. 5, 2009.)
6. The Molniya orbit is highly eccentric — the satellite moves in an extreme ellipse with the Earth close to one edge. Because the planet's gravity accelerates it, the satellite moves very quickly when it is close to the Earth. As it moves away, its speed slows, so it spends more time at the top of its orbit farthest from the Earth. (Holli Riebeck. "Catalog of Earth Satellite Orbits / Three Classes of Orbit." Nov. 5, 2009. NASA Earth Observatory. <http://earthobservatory.nasa.gov/Features/OrbitsCatalog/page2.php>.)
7. A satellite in low Earth orbit (LEO) circles the earth 100 to 300 miles above the Earth's surface. ("What Is a Satellite?" Satellite Industry Association. Nov. 5, 2009. Boeing. http://www.sia.org/industry_overview/sat101.pdf.)
8. Warezzman. "DVB: Satellite Hacking For Dummies." 2004. Undercon. http://www.undercon.org/archivo/0x08/UC0x08-DVB-Satellite_Hacking.pdf.
9. Based on "DVB: Satellite Hacking for Dummies" by Warezzman source: http://www.undercon.org/archivo/0x08/UC0x08-DVB-Satellite_Hacking.pdf.
10. Brown, Gary. "How Satellites Work." HowStuffWorks. <http://science.howstuffworks.com/satellite7.htm>. Nov. 5, 2009.
11. Berry, Walter. "Arrests Made in TV Satellite Hacking." Jan. 25, 2009. abc News. <http://abcnews.go.com/Technology/story?id=99047>.
12. Morrill, Dan. "Hack a Satellite while it is in orbit." April 13, 2007. Toolbox for IT. <http://it.toolbox.com/blogs/managing-infosec/hack-a-satellite-while-it-is-in-orbit-15690>.
13. "PF descobre equipamento capaz de fazer 'gato' em satélite dos EUA" ("PF discovered equipment to hook into U.S. satellite"). March 19, 2009. Jornal da Globo. (Global Journal). <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1049142-6174,00-PF+DESCO+BRE+EQUIPAMENTO+CAPAZ+DE+FAZER+GATO+EM+SATELITE+DOS+EUA.html>.
14. Soares, Marcelo. "The Great Brazilian Sat-Hack Crackdown." Apr. 20, 2009. WIRED. <http://www.wired.com/politics/security/news/2009/04/fleetcom>.
15. Undercon home page. <http://www.undercon.org/archivo.php?ucon=8>. Accessed on Nov. 5, 2009.
16. DEF CON IV home page. <http://www.defcon.org/html/defcon-4/defcon-4.html>. Accessed on Nov. 5, 2009.
17. Note: "Bird" is a term for satellite.
18. HITBSecConf2006 home page. <http://conference.hitb.org/hitbsecconf2006kl>. Accessed on Nov. 5, 2009.
19. Note: "Feed Hunting" means looking for satellite feeds that no one is supposed to find.
20. Goodin, Dan. "Satellite-hacking boffin sees the unseeable." Feb. 17, 2009. The Register. http://www.theregister.co.uk/2009/02/17/satellite_tv_hacking.
21. Ekoparty Security Conference home page. <http://www.ekoparty.com.ar>. Accessed on Nov. 5, 2009.
22. t2 '09 Information Security Conference home page. <http://www.t2.fi/conference>. Accessed on Nov. 5, 2009.
23. Nve, Leonardo. "Playing in a Satellite environment 1.2.". Black Hat. http://blackhat.com/presentations/bh-dc-10/Nve_Leonardo/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf. Accessed on May 28, 2010.
24. Nve, Leonardo. "Satélite: La señal del cielo que estabas esperando (II)" ("Satellite: The sign from sky that you were waiting for (II)"). Jan. 16, 2009. S21sec. http://blog.s21sec.com/2009/01/satelite-la-seal-del-cielo-que-estabas_16.html.



 High Security Lab: <http://lhs.loria.fr>

Malware 2010



**5th IEEE International Conference
on Malicious and Unwanted Software**

Nancy, France, Oct. 20-21, 2010

<http://malware10.loria.fr>

Important dates

Submission: June 30th, 2010

Notification: August 27th, 2010

Final version: September 10th, 2010

General Program Chair

Fernando C. Colon Osorio, WSSRL and Brandeis University

Chairs of Malware 2010

Jean-Yves Marion, Nancy University

Noam Rathaus, Beyond Security

Cliff Zhou, University Central Florida

Publicity Co-Chairs

Jose Morales, University of Texas

Daniel Reynaud, Nancy-University

Local Chair

Matthieu Kaczmarek, INRIA

Program Committee

Anthony Arrott, Trend Micro

Pierre-Marc Bureau, ESET

Mila Dalla Preda, Verona University

Saumya Debray, Arizona University

Thomas Engel, University of Luxembourg

José M. Fernandez, Ecole Polytechnique de Montréal

Dr. Olivier Festor, INRIA

Prof. Brent Kang, North Carolina University

Prof. Felix Leder, Bonn University

Bo Olsen, Kaspersky

Dr. Jose Nazario, Arbor networks

Dr. Phil Porras, SRI International

Fred Raynal, Sogeti

Andrew Walenstein, Lafayette University

Jeff Williams, Microsoft

Yang Xiang, Deakin University