UK web site at www.g6lvb.com/Articles/operatingSO50.htm.

Satellite Data Resources

With the advent of the internet, obtaining amateur radio satellite operating mode and status information is now easier than ever. Unfortunately, because it has become so easy, obtaining the most current information from a reliable source is NOT an easy task because of what I have come to call "information overload."

So, that said, what follows are several of my recommendations on where to look that will (hopefully) make your search for the most current satellite information just a bit easier.

The AMSAT Web Site

My go-to source for the most current satellite information continues to be our own AMSAT web page at www.amsat.org. A quick scroll down from the main page header will bring you to our "Apogee View" column where our current AMSAT president shares his views on the very latest doings of the organization. A further scroll down on that same page will bring you to the "Updates" area that contains current items of satellite status and information. Many of these items are re-posts from AMSAT News Service (ANS) bulletins.

Speaking of the AMSAT News Service, this bulletin service dates from the very earliest days of Packet Radio (that is, WELL before the rise in popularity of the Internet!) when AMSAT began to send out a weekly bulletin of satellite news and information via the (then) worldwide Packet Radio network. Those bulletins are still being sent worldwide via Internet subscription and, as the headers of the bulletins still contain Packet Radio routing information, some are actually still finding their way into what remains of the Packet Radio network!

However, you, too, can now sign up to receive these bulletins in your e-mail directly from AMSAT by clicking on "Services" and then "Mailing List Services." Scroll down to the "ANS" link and follow the directions about how to subscribe. However, if you don't want yet more e-mail filling up your (most likely) overloaded e-mail inbox, you can also browse through the ANS Archive by clicking on the "AMSAT News Service" link under the "Services" tab off the main AMSAT web page and then selecting the timing and/or threads you'd like to read.

AMSAT also offers some other mailing lists that you can subscribe to. And, what's nice is that subscribing to one or more of them is still very much free to members and non-members alike. These lists include, among others, the AMSAT-BB, an online forum for satellite discursions, as well as our weekly Keplerian Element Bulletin.

AMSAT UK

Another excellent source of amateur satellite information from "across the pond" is contained on the AMSAT United Kingdom (AMSAT UK) web site at amsat-uk.org. Of particular note is their very extensive list of resources under the "BEGINNER" tab off the main page. Also, the AMSAT-UK folks routinely post full-motion videos of their various meetings (such as their annual colloquium) and other such gatherings.

Gunter's Space Page

I don't know how he does it, but Gunter Krebs, via his "Gunter's Space Page" (space.skyrocket.de), has his finger on the pulse of the entire worldwide "space biz," including a wealth of amateur radio satellite information. He routinely gathers, correlates and catalogs a whole host of rocket launch and satellite information from various sources and puts it all in one place on his page. Indeed, if I'm looking for more background, construction and/or historical information regarding a particular satellite, Gunter's page is my first stop.

The N2YO Page

Another very useful web page is Ciprian Sufitchi's N2YO Web Page (**n2yo.com**). Ciprian's site focuses mainly on satellite tracking and offers real-time pass predictions for various popular satellites by using your internet IP address to set your location. The main thrust of his page is tracking the International Space Station (ISS) showing via a map on his home page where the Station is at the moment, and when it might be visible from your location.

Wrap Up

These are but a few of the many satellite information pages that I have found most useful out of the tens (if not hundreds) of similar pages now springing up on the web. Usually, searching for "amateur radio satellite information" will bring up related links.

In future columns, I'll again be shining the spotlight on other interesting amateur radio satellite launches of late as well as keeping you apprised of what AMSAT (and its worldwide sister organizations) are up to in space. See you then!

Satellite Cyber Threats: Important Issues to be Considered

Omar Álvarez-Cárdenas, XE1AO;
Miguel A. García-Ruiz, VE3BKM;
Margarita G. Mayoral-Baldivia, XE1BMG;
Raúl T. Aquino-Santos (SWL)

ABSTRACT

Satellites are important for maintaining the actual balance of the economy, society, and military activities. That is why many nations are increasingly recognizing satellites as critical infrastructure. Satellites provide a significant function in meteorology, natural disaster monitoring, communication, navigation, remote sensing, security, solar activity, among other applications, and a strong contribution to the improvement of science. Satellites use electromagnetic signals to transport information across different frequencies and modulation schemes. However, all their transmissions are susceptible to be intercepted. This increases the risk of cyber-attacks to compromise critical infrastructure functions dependent on satellite networks in sectors that include Information Technology (IT) and telecommunications (DHS, 2003). However, satellite networks employ a set of security tools and mechanisms for detecting and containing cyber incursions and, in consequence, ensuring the continuity of critical infrastructure operations. Some cyber-attacks have a political background and their aim is to affect essential services in some nations to cause damage, malfunction, or resulting in chaos in their population, which is considered as cyber terrorism. This paper presents an overview of satellite hacking, common types of attacks that can occur and some recommendations to consider for those involved in critical satellite communications systems, as well as those used for amateur radio services.

INTRODUCTION

As Fritz (2013) indicates, a satellite system includes interrelated and interconnected parts that perform a specific task. There are three common types of satellite systems: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and High Earth Orbit (HEO). In general, a satellite system consists of the satellite itself, communications ground stations in which data is processed, such as voice and images, TT&C (Tracking, Telemetry and Control) ground station that

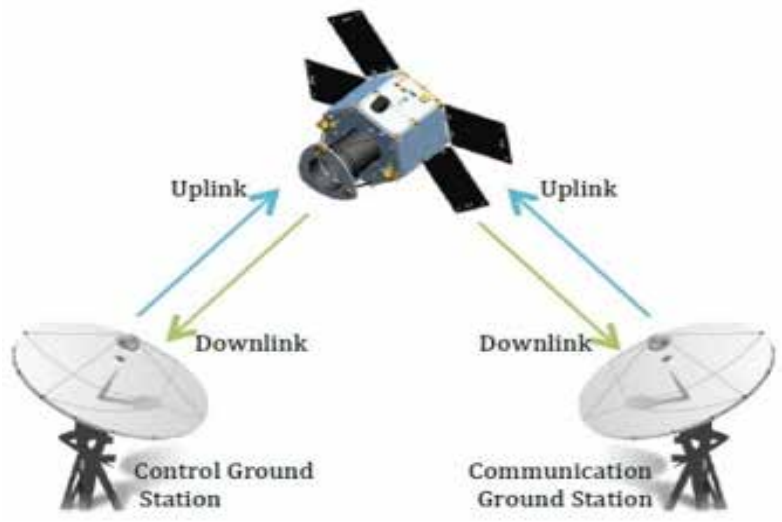

Figure 1 — Space and Ground Satellite systems (Alshaer, 2013).

guarantees the functionality of the satellite in the orbit by tracking it, and communicating to the satellites using the downlink and uplink frequencies that connect the satellite with these ground stations (Figure 1).

Satellite exploits differ from system to system. Some researchers have found weaknesses that allow easy hacking like the execution of malware code. These vulnerabilities may include insecure protocols, several backdoors, weak-encryption algorithms, and encrypted credentials which are the password used to login with administrative privileges. (Constantin, 2014). If we analyze it from a hacker's perspective, it is not a concern for them if they do not master all the technical details of a satellite communications system (there are satellite scripting codes for non-technical people), it is much easier to damage or disrupt hardware to affect its proper function. For example, hackers can simply purchase ready-made equipment available instead of knowing how to find an open satellite frequency, or how to build an extra-gain satellite antenna (Laurie, 2009).

In the context of this entire scenario, an important issue may have been overseen: there is an urgency to develop cybersecurity standards and regulations for commercial and amateur satellites internationally. If hackers take control of them, the consequences would be very serious. First, hackers could simply shut satellites down, denying access to their services and affecting the main infrastructure. Some of these new satellites have thrusters that allow them to speed up, slow down and change direction in space. As Akata (2020) pointed out, "if hackers took control of these steerable satellites, they could alter the satellites' orbits and crash them into other satellites or even the International Space Station".

THREATS TO SATELLITES

In a satellite communications system, threats can be unintentional or intentional but regardless of the nature of the threat, its effects can range from loss of information, infrastructure, or significant economic damage. To simplify these two types of threats, we will try to summarize them in the following two figures: Figure 2 resumes the unintentional threats and Figure 3 specifies the intentional ones. When you have a satellite communications system, you must start by identifying the possible threats to develop a proper contingency strategy to deal with them.

Unintentional threats affect the ground system, the space segment, and its radio communication link. However, their origins are related to natural events, environmental effects inside and outside Earth and in some cases by human installations or services. This type of threat, despite having an unpredictable origin in advance, must be included in the contingency action plan for the satellite communication network.

Intentional threats have a different origin with respect to the scope and damage they intend to achieve in any element of the satellite communication system. From Figure no. 3 we are more interested in aspects related to cyber-attacks focused on causing interference and content-oriented damage. As ham radio operators, we are focused on the CubeSat LEO satellites that use off-the-self-technology to keep their development costs low. However, this represents a great advantage for hackers because their wide availability makes it easier for them to analyze their vulnerabilities. In addition, the components used for making CubeSats are open source technology which allows a hacker to implement malware and other vulnerabilities in the software or hardware of the satellite. When the satellite is in orbit, the owners of the satellites subcontract their daily management to other companies, increasing the opportunity to hack the space or ground system as simply as waiting to a specific satellite orbit to send malicious commands. Remember that satellites are controlled from ground stations and use computers. Even if those computers are not directly connected to the Internet, they can still have software vulnerabilities that can be exploited by hackers. If they infiltrate these computers, it is possible to send malicious commands to the satellites without the need for a specially manufactured satellite ground station. (Akoto, 2020).

Regardless of the type or orbit of a satellite, they will all be targets of a possible attack at any time during their life operation. For example, the following is a select timeline of intrusions into NASA's computer systems, many of which are alleged to be Chinese or Russian-state sponsored. Many of these incidents are cases of computer hacking, rather than satellite hacking, yet they can be used as a stairway to attack satellites from part of the ground-based terrestrial network. The following is a summary of NASA´s incidents related to satellite control:

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 onboard computers are running older software for which security fixes are no longer available.…" (Steinberger, 2008).

2008.- "On June 20, 2008, Terra EOS [earth observation system] AM–1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands" (USCC, 2011).
2008.- "On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands" (USCC, 2011).

Type of threat	Vulnerable satellite system components
Ground-based:	
Natural occurrences (including earthquakes and floods; adverse temperature environments)	Ground stations; TT&C and data links
Power outages	
Space-based:	
Space environment (solar, cosmic radiation; temperature variations)	Satellites; TT&C and data links
Space objects (including debris)	
Interference-oriented:	
Solar activity; atmospheric and solar disturbances	Satellites; TT&C and data links
Unintentional human interference (caused by terrestrial and space-based wireless systems)	

Figure 2 — Unintentional Threats to Satellite (Malik, 2019).

2008.- 'Landsat-7, a U.S. earth observation satellite jointly managed by NASA and the U.S. Geological Survey experienced 12 or more minutes of interference" (USCC, 2011).
2010.- "A Chinese national was detained for hacking activity targeting US government agencies. Seven NASA systems, many containing export-restricted technical data, were compromised" (Martin, 2012).

2010.- "For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from U.S. government (".gov") and military (".mil") sites, including those for NASA" (USCC, 2010).

2011.- "Romanian hacker TinKode allegedly obtained sensitive information from NASA's Goddard Space Flight Center and the European Space Agency which he then made publicly available online. The information included Login credentials for admin, content management, databases, email accounts, file upload, and other key systems" (Leyden, 2011; Prime, 2012).

2011.- "NASA's Jet Propulsion Laboratory (JPL) "reported suspicious network activity involving Chinese-based IP addresses... giving the intruders access to most of JPL's networks" (Martin, 2012).

2013.- "Chinese national Bo Jiang, a former NASA contractor, was arrested as he was

Type of threat	Vulnerable satellite system components
Ground-based:	
Physical destruction	Ground stations; communications networks
Sabotage	All systems
Space-based (anti-satellite):	
Interceptors (space mines and space-to-space missiles)	Satellites
Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites; TT&C and data links
Interference and content-oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth)	All systems and communications networks
Jamming	All systems

Figure 3 — Intentional Threats to Satellite (Malik, 2019).

attempting to return to China with "a large amount of information technology that he may not have been entitled to possess,"… NASA shut down access to an online database and banned new requests from Chinese nationals seeking access to its facilities amid mounting concerns about espionage and export control violations…. The security measures include a complete ban on remote computer access by Chinese contractors already working at NASA centers (Klotz, 2013). NASA employs 118 Chinese nationals in "remotely-based" information technology jobs that may enable them to penetrate the space agency's national security database servers, and 192 Chinese nationals in positions with "physical access" to NASA facilities" (Pollock, 2013).

2013.- "The US Congress passed a provision which prohibits the Commerce and Justice departments, NASA and the National Science Foundation from buying any information technology system that is "produced, manufactured or assembled" by any entity that is "owned, operated or subsidized" by the People's Republic of China. The agencies can only acquire the technology if, in consulting with the FBI, they determine that there is no risk of "cyberespionage or sabotage associated with the acquisition of the system," according to the legislation. In addition to condemnation from China, this rule could upset US allies whose businesses rely on Chinese components in some of the equipment they sell to the US" (Fritz, 2013).

TYPES OF SATELLITE HACKING

Nowadays, getting a satellite into orbit and stating its initial basic functions is no longer a major concern. The space segment and the ground segment are vulnerable to the same types of attacks as any other computer system on the network. The perpetrator can trick the satellite into confusing it with the ground station and then start the hacking through a physical connection, or through the radio communications system. Under these conditions, satellite hacking can be analyzed into four different categories: Jamming, Spoofing, Hijacking and Controlling.

Jamming

Jamming is a technique used to interrupt radio frequency transmissions by replacing them with different ones to avoid the receivers being able to acquire the data they were expecting and is considered as the easiest way of hacking. Jamming the uplink frequency has less impact but on the other hand, jamming radio frequency uplink control prevents the satellite from receiving control commands from earth stations with no possibility of tracking their main functionalities. Furthermore, any single cyber-attack on ground operation station equipment can produce a satellite jamming, with the consequent impact on financial transactions or data services. A DDoS attack against the computer network used by the ground station could also effectively jam a satellite without having to get involved with radio frequency issues. Even if the uplink signal is not targeted, an essential component of the satellite system would be, causing the systematic failure of the satellite communications network (Fritz, 2013).

Spoofing

When a satellite communications system is under spoofing attack, the receiver in the space segment or ground segment accepts some type of validation or altered control information, causing false signals in the whole system This type of threat is common for several satellite systems because its developers fail to encrypt the monitoring and control of the uplink/downlink for radio communications, resulting in a high vulnerability to spoofing threats (Alshaer, 2013).

Hijacking and Controlling

The term hijacking refers to an unauthorized, usually illegal, transmission that is generated with the purpose of being switched to a different one to be received by as many systems as possible. When this is combined with control of the system, hijacking is an illegal transmission that uses a satellite to exchange its transmission for another. In this category, Control is the most difficult part to be achieved by a hacker, but when it is done, it is possible to get complete control of the satellite, its payload and therefore the overall ground segment. By taking control of ground station links, hackers can issue commands for a satellite to misdirect it, burn it up on re-entry to the earth's atmosphere. The high security of the satellite parts at this level makes the control of a satellite significantly difficult, but hackers only need just one weakness to control and hijack all the satellite networks (Fritz, 2013).

ACTIONS TO BE TAKEN

Hacking a satellite system is an undesired possibility that will always be present. However, it is possible to mitigate or avoid this kind of action if we start to develop regulations and cybersecurity standards in the design and construction of satellites to achieve a standardization about this security problem. The legal framework for defining who can be considered guilty of hacking and what criminal charges will be incurred for the actions taken, ensuring that the parties involved take the necessary steps to secure those systems. To minimize the damage caused by hacking a satellite system, it is necessary to make great efforts in a systemic detection of specific threats, documentation of the weaknesses encountered and having an immediate response team against cyber-attacks. (Fritz, 2013).

Threat modeling is a technique for better understanding and prioritizing the threat and risk faced by the network itself. Once the security threat or risk is detected, actions can be taken to prevent or recover from the attack as quickly as possible (Alshaer, 2013). Anti-jamming prevention includes the use of spread spectrum, empowering the signal power so it exceeds the interfering signal (jamming). Most of the information can be received with a low error rate. In a low-cost satellite infrastructure such as CubeSats, increase the embedded security processor with encryption, digital signing and identity management at their authentication and authorization access. The use of standards to improve security is important, for example, the ISO 7498-2 related to authentication, authorization, encryption, data integrity and non-repudiation. It will be important to have a response threats team to prevent, monitoring, logging and react as a part of the satellite systemic detection group (Malik, 2019).

CONCLUSION

The security of satellite systems will be efficient when instruments, mechanisms, standards, protocols, laws, and procedures are designed and applied to prevent unauthorized persons or groups from accessing ground stations to spy confidential satellite transmissions, alter information from orbiting satellite, falsifying commands and control data. This will generally affect the infrastructure of the space and ground segment of satellite systems. These systems can be attacked through computer networks connected to the Internet, which is the most common form of hacking at present, but it is also possible to do it using radiofrequency stations that simulate the uplink and downlink of the satellite communications system. The main constraints to understanding the complexity of satellite threats are the variety of systems and the lack of standards in their development. Most satellite manufacturers keep their design information secret as a security action but restrict the development of industry standards related to construction, interoperability, and security. Despite the cost and technological difficulty of reaching space, it is relatively easy to carry out cyber-

attacks to satellites. It is very important to secure ground stations that have Internet connectivity because it would be one of the primary targets for a cyber-attack, but as revealed in the NASA case study, there is still much to be done on security issues in IP networks.

SpaceX is currently the world's largest low-orbit satellite operator, with plans to have 42,000 satellites in space over the next 10 years. This number of satellites is intended to provide satellite Internet services around the world. However, SpaceX and other rival companies are under pressure to achieve this goal by accelerating the production of their satellites at low cost, which could result in a lack of security in their construction and operation. These types of actions are the ones hackers are currently looking for to infiltrate while the satellite service companies are worried to be first in space by sacrificing costs and security in their systems.

Finally, no matter what actions the satellite industry and governments take on cybersecurity in satellite systems, only one thing is sure: something must be done about it, and soon. It will be a serious mistake to continue developing satellites that do not satisfy minimum security standards, making it easy for hackers to gain control of commercial or amateur satellites to put human lives in danger or to damage space and ground segment services or infrastructure.

REFERENCES

• Akata, W. (2020). Hackers could shut down satellites — or turn them into weapons. Astronomy Magazine. Available at astronomy.com/news/2020/02/hackers-could-shut-down-satellites--or-turn-them-into-weapons.

• Alshaer, M. K. (2013). Cyber Attacks On Satellites Review & Solutions. Available at www.academia.edu/18156391/Cyber_attacks_on_satellites_Review_and_solutions.

• Constantin, L. (2014, April 18). Satellite communication systems are rife with security flaws, vulnerable to hackers. Computer World.

• Fritz, J. (2013). Satellite Hacking: A guide for the perplexed. Culture Mandala: The Bulletin of the Center for East-West Cultural and Economic Studies. Vol 10, No.1.

• Klotz, I. (2013). NASA Steps Up Security After Arrest of Former Contractor. Available from www.reuters.com/article/us-space-espionage-idUSBRE92J1FR20130320.

• Laurie, A. (2009). Satellite Hacking for Fun and Profit. Retrieved from www.securitytube.net/video/263.

• Leyden, J. (2011). Inside the mysterious U.S. satellite hacking case. Available from www.theregister.co.uk/2011/11/21/us_sat_hack_mystery/print.html.

• Malik, W. (2019). Attack Vectors in Orbit: The Need for IoT and Satellite Security. RSA Conference, San Fco. USA.

• Martin, P. (2012). NASA Cybersecurity: An Examination of the Agency's Information Security. Available from oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.

• Pollock, R. (2013). NASA Chief Failed to Tell Congress of 118 Chinese Nationals Working in IT. Available from washingtonexaminer.com/nasa-chief-failed-to-tell-congress-of-118-chinesenationals-working-in-it/article/2525324.

• Prime: Cybersecurity Risk Management Strategies for SATCOM Networks. (2012). Available from www.milsatmagazine.com/cgi-bin/display_article.cgi?number=1142237172.

• Steinberger, J. (2008). A Survey of Satellite Communications System Vulnerabilities. Available from www.dtic.mil/dtic/tr/fulltext/u2/a487592.pdf.

• USCC. (2010). Report to Congress of the US-China Economic and Security Review Commission. Available from www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf.

• USCC. (2011). Report to Congress of the US-China Economic and Security Review Commission. Available from **origin.**www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

• U.S. Department of Homeland Security (DHS). (2003). The national strategy to secure cyberspace. Washington, D.C.

Integration of a Distributed Ground Station Network Based on Amateur Radio Infrastructure for Scientific Space Missions

M.A.Mendoza-Bárcenas (SWL);
Rafael Prieto-Meléndez (SWL);
Alejandro Padrón-Godínez (SWL);
Gerardo Calva-Olmos (SWL),
Omar Álvarez-Cárdenas, XE1AO;
Margarita G. Mayoral-Baldivia XE1BMG;
Alfonso Tamez-Rodríguez, XE2O

1. Abstract

The rapid increase of scientific and low-cost experimental satellite missions has made it necessary to develop new proposals for the integration of space platforms and ground stations for telemetry control and data downloading from sensors onboard. In recent years, the number of radio amateurs around the world with technological capabilities for downloading satellite data has grown significantly, becoming a fundamental part of international communications. In this work, a novel proposal for the integration of a network of ground stations distributed worldwide, based on Amateur Radio Infrastructure for Scientific Space Missions, is shown.

2. Introduction

The relationship between ham radio and space technology dates back from 1961 when the OSCAR-1 satellite (acronym of Orbiting Satellite Carrying Amateur Radio) was launched. Until January 2018, near 92 satellites of all sizes, carrying amateur radio and several related experiments, have been launched and successfully operated by hams in countries around the world according to AMSAT (2018).

In the context of the architecture of a typical space mission, and according to the general scheme shown in SMAD (1999), this is integrated by three main segments: space segment (SS), ground segment (GS) and launch segment (LS). The SS is integrated