iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3443

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Cyber Security- How Vulnerable are Satellites - to Cyberattacks

Dr. Alex Roney Mathew
*Department of Computer Science (**Cyber Security**), Bethany College, West Virginia, USA*

Abstract— Over the years, the number of satellites has increased resulting in an increased and improved communication system which enhances the connection between people. The advancement of technology has also boosted the development of digital gadgets and increased internet access. However, it has been a challenge for cybersecurity to keep up with the tremendous growth, and the cost of in-built security input in satellites is expensive. The cost of cybersecurity has increased, and most people opt to leave it unsecured and hope for the best. In 2016, the Dyn attacked to deny services which were streamed online, taped personal home computers that were poorly secured and to other interconnected computers within and in different states through routers

Keywords— Cyber-attacks, DDos, VSATs

I. INTRODUCTION

Recently, the reliance on satellite technologies has increased over the years due to technological advancement. Satellites are among the most critical assets a nation can own in the world. This is because of the enormous costs associated with making one, the expenses incurred to operate it, the resources needed to make it operational. Lastly the value it offers to the state. Many countries use satellites for navigation, communication, defense system, monitoring, multiple applications, and remote sensing. Despite the huge budget set aside to protect these satellites, advanced technology has made these satellites prone to cyber-attacks making them vulnerable. These increased cyber-attack rates pose threats to satellites rendering them vulnerable. The main attacks on satellites discussed herein include jamming, data theft, hijacking, and spoofing.

II. CYBER SECURITY

This increased cyber-attacks have become a significant concern since it poses considerable threats to regional, national, and international security. Additionally, they can be scandalous for those firms, government institutions, and trade industries that use satellites to operate. Therefore, all these parties should come together and complement each other in enhancing cybersecurity and minimize these attacks. This paper acknowledges that space security to cyber-attacks remains a significant challenge due to the lack of an international body dedicated to offering security services.

Spaced-based satellite faces many threats from jamming to spoofing to hacking communication or navigation controls. Other risks include hijacking the satellites for various missions, shutdowns that cause huge catastrophes, and alteration of the satellite from its orbit or expose it to radiation which causes damage to its solar cell rendering it useless. Ground satellites are prone to strikes that make them defective. These threats may be executed by a group of people who want to prove their skills especially hackers, a terrorist who wants to cause chaos in the country, organizations that want to tap competitive information of other organization with the aim of gaining a market advantage.

Besides, these attacks may be executed by states that are at war with each other and seek to acquire a military advantage. According to research, threats to military technology have received less attention over the years, leaving it vulnerable to attacks. These threats aim at emasculating the integrity of the rival's weapon system a move that discourages international relationship between such countries. Such attacks threaten the military operations conducted through the help of satellites such as missile control systems and communication increases the risks at the ground spaced based satellites stations and other commands, and control stations. During a military crisis, the presence of cyber-attacks increases tension between countries due to the increased risk of misperception.

Generally, the fact that cyber technology is currently in reach for every state or non-state, it creates an opportunity for terrorist and other group or country to initiate attacks that can cause great catastrophes. During such times a lot can be at stake as identified above. Therefore, immediately such security breach alerts are received, necessary measures need to be taken instantly to reduce the impacts of cyber- attack or threats [10].

In 1999, the British Military communication received a security alert after being hacked from a home computer from southern England [2]. For almost a whole month, the group exploited the defense system, hacked and cut off the control of all types of communications. It was later discovered that they used military communication channels, television, and telephone calls to get access to their satellites. Research shows that it is easy for one to convey a satellite and use it for personal reasons. Such attacks do not necessarily have to be from the satellite itself, but also through upward and downward transmission or from its earth

station. Scientists argue that just like it is easy to take feeds from the TV station by using a microwave transmitter when close to the transmitter and use a slightly different frequency to give repeated radio signals, the same concept can be applied to satellites. The use of transmitters, satellite dish, an upconverter, and other few things can it is easy to hack into a satellite and gain control.

A communication satellite is compared to a radio repeater that has about 24 transponders and uses a specific frequency block. The uplink sends signals at the range of 6 GHz, the satellite receives and converts it to 4 GHz and transmits it back to earth. The only form of security is through encryption and encoding the signals which are not efficient to keep the attackers away. It is easy for an attacker to interfere with a satellite's service during a double illumination, where one frequency carries two or more carriers. Although the carriers may be from uplinks of different location, the effects of illumination range from zero audible change to great damage reliant on the power of the carrier among other factors. For example, a person may wipe through other services by moving his/her uplink dish towards the wrong space satellite accidentally or purposefully [6]

Incomprehensible to such satellites cyber-attacks, great focus has been on analytics and information security to mitigate these threats and attacks. Traffic and defense communication, broadcast, and financial information operate through the help of satellites. Most of the data centers run the risk of countless cyber-threats [3]. In this area, attackers use the DDoS technique where they implant foreign devices on ground satellites and exploit it later after gaining access. This device decrypts and decodes the system granting access to the attackers. With this access, they can alter the traffic system and cause significant damages in the country, gain access to financial information, and even alter television broadcast to their preference. Additionally, hackers have become more skilled, and they use Very Small Aperture Terminals (VSATs) to penetrate passwords of factories and industries they were never changed. They jam, hack and exploit the signals gaining access to the satellite's system.

The commonly known satellite is a communication satellite system that is used in boosting communication signals from earth to space and back to land directly to the recipient. For example, marine vessel, planes, and the navy use this satellite for secure and easier communication and navigation. The distance from the shore and its isolation render it vulnerable to ground cyber-attacks by companies, states or even individuals. This satellite allows access to offshore vessels internal systems posing more significant risks of the vessels to be hacked. The data of this system is saved on the SQLite database since it uses logins; it is easy for attackers to jam the signals or spoof it to their advantage. The signals transferred from one location to another can be another form of gateway for these attackers to obtain the logins which give them access to the internal vessel network. In this case, once the system is hacked, the attackers have full access of the navigation system, and it makes it very easy for them to make the vessels collide with other ships or running through the ground [9]. These pose a risk on the global economy since most the trade has to be transported by ships.

Recent research has shown that commercial and government satellites are the new targets for cyber-attacks [4]. Most attacks are in search of effective and inexpensive ways to limit the capabilities of the space-based satellites. As much as developers and manufacturers are trying to correct the efficiency and security of the ground satellite they have been unable to modify those that are space-based. The attackers have realized that they can still apply the same technique used for the ground satellite to attack the space-based satellite rendering it vulnerable. The government, economies and other critical infrastructure are dependent on satellites for services such as Global Positioning System which is vulnerable to the cyber-attacks. Reports have shown that electronics from Chinese and software from Russia that are used in the supply chain of the aerospace structure are more susceptible to backdoors threat. It was noted that Chines have been targeting U.S cyber espionage operations while others have beleaguered the control and command system and its data station. Most of these attacks use unmanned aerial systems, weather balloons or flyover with manned aircraft technique to disrupt the signals or hijack by use of broadcasting equipment of high power signals. Moreover, they have also tried to tap through the Ethernet cables or internet structure and even tried to attack and exploit network by converting filtration or through social engineering to gain physical access. With advanced technology, satellites facilities can withstand against such attackers. However, other professional attackers manage to infiltrate the system.

[1]Over the years the military is immensely increasing its dependence on satellites for its mission; therefore, they have tried to improve the cybersecurity to protect their system against attackers. Consequently, they have been able to prevent attacks by using strong encryption; however, the susceptibility of commercial satellite remains a challenge since it holds their payloads. The air force is willing to add encryption to the payloads even though the attackers can come and attack their host satellites hence help improve the security of commercial satellites. It is noted that military satellite has an added advantage due to its orbit positioning, its age, and access as compared to commercial satellites. The new technological trends have led to the innovation and growth of small satellites which has increased satellites vulnerability to cyber-attacks and threats. There have been increased cases of signal disruption due to direct mapping to deny services and malicious misdirection. In other cases, we have attackers who use electromagnetic spyware attacking the ground satellites. These attackers lay low for a while and activate their devices when its least expected and when they can cause significant damages. Moreover, there are cases where cyber-attacks

begin their malicious operations as early as during manufacturing, or distribution or even during installation of the satellites. The equipment comes with malware and spyware already installed in them, or they get attached during installation increasing the vulnerability of the satellite before beginning its operation.

The commercialization of space equipment has also increased cybersecurity due to incentives of the market to reduce cost and enhance innovation. There has been an emergence of more space tourism, asteroids mining, lunar operations, space transport and other missions to missions. These kinds of exposure to space increase the risks to satellite security through spying. These changes in space technology have created unregulated demand for space equipment forcing manufacturers and developers to increase the supply of the equipment. Consequently, this kind of pressure due to market demand forces the developers and manufacturers to give less attention to the security control system. The satellites have also evolved due to technology and have significantly improved its functionality and capabilities. Satellites in this era make use of artificial intelligence, electronics, sensor, miniaturization, and computing innovations. Its ability to support many policies and other functional operations, it dramatically impacts agricultural activity, monitoring of the environment and transportation efficiency. By use of this cutting edge technology, satellites have been able to produce valuable data that renders it vulnerable and targeted for cyber espionage [8].

It is stated that to protect all types of satellites, it required a more in-depth understanding of the vulnerability of each of these satellites and how it arises in various activities. It is noted that to mitigate these attacks; the agencies should reason more like them to have a deeper insight into their tactics and strategies. Moreover, there is a need to come up with infrastructures and procedures that can assess the vulnerability of the system taking into account the inbuilt foreign gadgets and malware. Research has proven that, more trusted personnel or cooperation licensed by the government who should be given the responsibility of distribution and installation to reduces the cases of inbuilt foreign devices and malware. Multinational commercialization of space equipment should be reduced, and allowing a governed international cooperation to be the supreme developers and manufacturers. The governments are also urged to come up with comprehensive space infrastructure regimes and strategies to improve cyber-security [7][2]. All the national cooperation should come together and discuss ways forward on how to mitigate cyber-attacks. NASA is also argued to make cybersecurity a priority since they are one of the leading cooperation in research and development of space activities and operations. Regulation policies should be enacted on commercialization of space gadgets to reduce spyware and destruction of space-based satellites.

III. CONCLUSIONS

It is evident that satellites are very vulnerable to cyber-attacks. It is evident that space-based satellite receives more attacks than ground satellites, despite the distance between them and the ground. Despite the tremendous technological innovation and advancement, cybersecurity remains a significant challenge in the world. Satellites remain the most crucial asset since they control more than 80% of the world operation, procedures, and activity; hence its security should be the world priority. It is evident that the only way they the attacks can come mitigated is by the collaboration of the national associations and cooperation to enhance the security of their systems. Lastly, to prevent these attacks, states need to develop an independent body mandated with roles such as assessing the quality of satellites, maintaining satellites, and establishing laws aimed at discouraging cyber-attacks. This body should monitor all activities of the satellites and look for discrepancies in their operations. They should also train individuals who will be mandated with the role of protecting satellites from cyber-attacks.

REFERENCES

[1] S. Erwin, "Air Force exploring ways to protect satellite networks from cyberattacks - SpaceNews.com", *SpaceNews.com*, 2017. [Online]. Available: https://spacenews.com/air-force-exploring-ways-to-protect-satellite-networks-from-cyberattacks/. [Accessed: 20- Mar- 2019].

[2] S. Northcutt, "Are Satellites Vulnerable to Hackers?", *Sans.edu*, 2007. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/satellite-dos. [Accessed: 20- Mar- 2019].

[3] N. Goud, "Cyber Threat to Satellites is Fathomless! - Cybersecurity Insiders", *Cybersecurity Insiders*, 2019. [Online]. Available: https://www.cybersecurity-insiders.com/cyber-threat-to-satellites-is-fathomless/. [Accessed: 20- Mar- 2019].

[4] M. Gruss, "A new target for hackers? Satellites", *Fifth Domain*, 2018. [Online]. Available: https://www.fifthdomain.com/dod/2018/04/11/a-new-target-for-hackers-satellites/. [Accessed: 20- Mar- 2019].

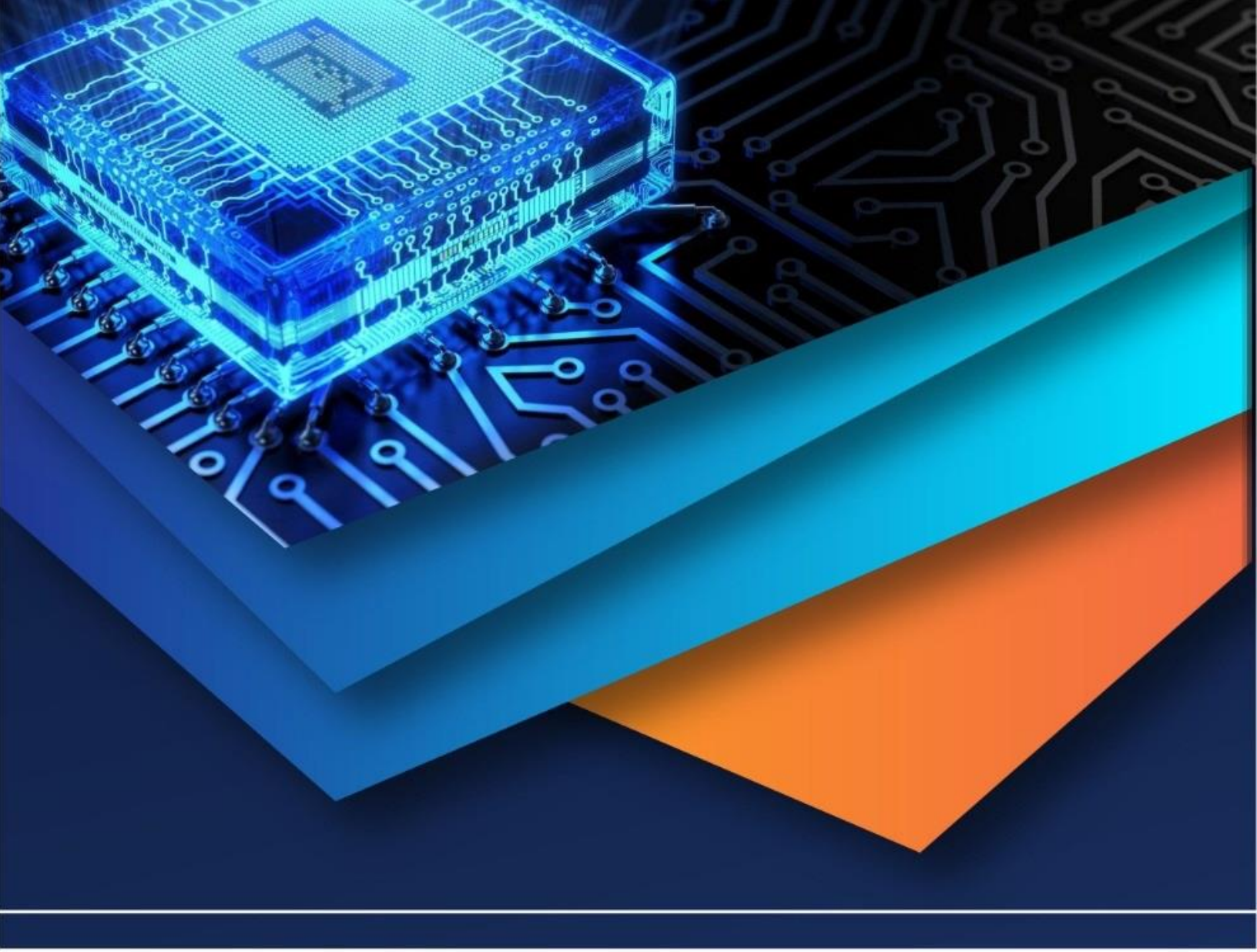
[5] P. Lewis and D. Livingstone, "The cyber threat in outer space - Bulletin of the Atomic Scientists", *Bulletin of the Atomic Scientists*, 2016. [Online]. Available: https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space/. [Accessed: 20- Mar- 2019].

[6] R. Banta, "Cyber Attacks on Satellites Could Lead to Unexpected Catastrophe | Lifeline Data Centers", *Lifeline Data Centers*, 2017. [Online]. Available: https://lifelinedatacenters.com/data-center/cyber-attacks-on-satellites/. [Accessed: 20- Mar- 2019].

[7] D. Livingstone and P. Lewis, "Space, the Final Frontier for Cybersecurity?", *Chathamhouse.org*, 2016. [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf. [Accessed: 20- Mar- 2019].

[8] R. Hutchins, "Cyber Defense of Space Assets", *Cs.tufts.edu*, 2016. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf. [Accessed: 20- Mar- 2019].

[9] B. Weeden, "Electronic Warfare and Satellites Challenges in Assuring Space Capabilities", *Swfound.org*, 2016. [Online]. Available: https://swfound.org/media/205651/bw_ew_satellitesatellites-gcc_oct2016.pdf. [Accessed: 20- Mar- 2019].
[10] M. Alshaer, "Cyber attacks on satellites: Review and solutions", *ACADEMIA*, 2017. [Online]. Available: https://www.academia.edu/18156391/Cyber_attacks_on_satellites_Review_and_solutions. [Accessed: 20- Mar- 2019].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY