Bellew, Nathan

Dr. Rick White

CS 4950 Homeland and Cyber Security

Satellites in Danger: Cyber Security In Space Still Being Invented

With thousands of satellites in earth's orbit and with the rise of commercial satellites will space be the next battleground in the cyber war? Satellites can be used for day to day needs such as weather, communication, and exploration. Satellites have been primarily used and operated by the military to carry out a variety of missions. In recent years the unfolding of the internet has shown the constant discovery of new vulnerabilities that have caused millions in repairs. Considering the internet was also a military project, this poses the question how secure is space? Space is far and the average person has no reason to worry about what happens in space - the government uses space so the government should handle it. This mindset will soon change with the rise of commercial satellites for internet communication like SpaceX. The question then becomes – how well has the government handled cybersecurity in space and how difficult will it be to move forward? At the current rate of growth in cybersecurity and satellite communication – space is already not secure and will grow to be worse as time passes.

Satellites do not have the same level of security as most computers do, this is reflected in the current policies in place and the ground communication system. The National Institute of Standards and Technology (NIST) is known for handling risk mitigations with regards to most vulnerability problems in software around the US. So in order to understand how secure a system is, most organizations can compare their current security with the NIST security standards. It has now become a common problem among satellite companies in determining how secure a satellite should be,

> "Satellite Companies vying to sell to the government and defense markets know their prospective customers want them to be cyber-secure, but the absence of industry standards and guidance leaves them scratching their heads about exactly how secure they need to be.." (Waterman, Shaun).

So there exists no standards for satellite cyber-protection, this means that any company can sell a satellite and set their own standards for cyber-surety. Satellite companies are still able to rely on NIST with regards to cybersecurity standards so long as they are using a ground communication system. Though satellite's do not have security standards, the computers used to control, monitor, and design satellites do have NIST standards. So is the use of NIST guidelines to secure a ground communication system should be enough to ensure a moderate amount of safety? No, as the article Cyber Security in Space News points out, "Compromising the ground station is ultimately the easiest way to control a satellite as it provides the equipment and software required to legitimately control and track it, and it uses existing and established terrestrial systems and attack vectors." (Manulis) So if a company is doing all it can to provide the highest quality security to a satellite system, this means that the computers that are operating the satellite as well as the computers that designed and built the satellite, are being maintained to general standards. As was mentioned, there are no satellite specific standards for cybersecurity

so there is no guarantee that the current standards mitigate any of the current satellite vulnerabilities. Though this is not an easy task it is still possible as noted in Cyber Security in Space News,

> "Vulnerabilities in the software and hardware in use on the satellite can occur and can impact the satellite's operation and robustness of security controls… Even agencies such as NASA and government organizations are not immune to threats such as these, with several examples of satellites being under the control of attackers." (Manulis)

The solution here is to implement security standards into the design of each satellite built prior to its launch. This means securing the device first instead of attempting to implement security after-the-fact. Though a lack of policies and a poorly run ground communication system could still stand in the way of a perfectly secured satellite.

Satellite attacks are constantly happening, what adverse side effects occur if a satellite is attacked and how would that effect the average citizen? Thousands of satellites have been launched into Earth's orbit since the 1960s, and thousands more will likely be launched over the next several decades. How many satellites have been launched? Nibedita Mohanta from Geospatial World claims,

> "There are 6,542 satellites, out of which 3,372 satellites are active and 3,170 satellites are inactive, as recorded by 1st January, 2021… according to the Index of Objects Launched into Outer Space, maintained by the United Nations Office for Outer Space Affairs, there were 7,389 individual satellites in Space at the end of April, 2021; an increase of 27.97% compared to 2020. The database also shows that since inception 11,139 satellites have been launched, out of which only 7,389 are in the Space, while the rest have either been burnt up in the atmosphere or have returned to Earth in the form of debris, much like the recent Chinese Long March 5C rocket, which dived into the Indian Ocean. " (Mohanta, Nibedita)

Many satellites are launched into a satellite constellation in order to maintain efficient ground communication and most satellite constellations are used for satellite communication. Usually satellite constellations are 10-30 satellites which communicate through wireless network crosslinks. SpaceX's Starlink is a satellite communication company which strives to create a mega-constellation with around 42,000 satellites (Mann, Adam). So considering the 11,139 satellites that were launched and the remaining 7,389, it can be assumed that a third of satellites end up crashing. Of the satellites that do not crash only half have remained active while the rest have become falling trash. Taking this and applying it to SpaceX's desire to add a mega-constellation it can be assumed that around 14,000 will likely stop working. How do satellites stop working? As stated before satellites can be vulnerable to attacks, this is not from a security analysis, instead some satellites have been successfully hacked and brought down,

> "in 1998 when hackers took control of the U.S.-German ROSAT X-Ray satellite. They did it by hacking into computers at the Goddard Space Flight Center in Maryland. The hackers then instructed the satellite to aim its solar panels directly at the sun. This effectively fried its batteries and rendered the satellite useless. The defunct satellite eventually crashed back to Earth in 2011." (Akoto, William)

Attacks such as these are effective and have been launched thousands of time a year. The real danger of an effective attack on a satellite is not bringing it down, it is the loss of communication and the threat of a space botnet. As noted around 14,000 could stop working and as noted a hacked satellite could be the cause of either a fallen satellite or an orbiting dead satellite. What if instead of ransoming satellites or forcing them to fail, an attack used the satellite crosslinks as a way to create a satellite botnet. As noted in the paper When Satellites Attack it is clear that the future could see satellites hack other satellites,

> "As opposed to attacks popularized in the media involving physical altercations between satellites, the satellite-to-satellite attacks described herein are cyber attacks. Such attacks target the sensors and actuators that facilitate satellites mission capabilities and can result in cyber-physical consequences." (Falco, Gregory)

Should something like this happen for SpaceX's Starlink, then it would be the equivalent of a worldwide Verizon blackout. Though with several thousand satellites it could be mitigated, the cost for fixing even a single satellite could be astronomical. With ineffective security standards set to protect thousands of satellites that is aimed to be used by daily consumers, it is easy to see the damage that a few well executed attacks could do.

Innovations in cybersecurity could hold the key to using space safely, but the creation of these tools is so slow that they are becoming vulnerable before they can be used. One of the biggest modifications to satellites is using embedded software to ensure cyber surety. These pieces of embedded software are secured by as many NIST standards as possible but a new way to ensure security is to embed security into the power system itself. The Cyber-Physical Power System (CPPS) as defined by R. V. Yohanandhan:

> "The integration of physical and cyber system evolves into a new digital technology called Cyber-Physical System… The integration of the physical power system with a cyber system, evolves into a strongly coupled cyber-physical power system." (R. V. Yohanandhan)

This is a piece of embedded software that is meant to secure not just satellites but really any piece of tech that is concerned with power in some way. CPPS basically manages the physical and cyber power systems ensuring the power cannot be tampered with and is being correctly managed. The power of CPPS is that it could solve many problems currently plaguing the threats of a cyber attack on the power industry. So integrating it to satellites is a step that many companies such as SpaceX are taking to ensure their satellite systems are secured. This is far from a perfect solution, currently there does exist chances of the CPPS failing, as described by Tong Duan,

> "Fortunately, due to the low orbit (550 km altitude) and fast transmission speed in vacuum, the propagation delay difference between the SpaceX's Phase I Starlink constellation and the terrestrial optical fiber network is small, and the delay of space propagation could be even smaller when the hop distance is longer than 2500 km. Therefore, the Starlink network could be exploited in the CPPS for wide area measurement, protection and control (WAMPAC) applications in the areas with weak network connections." (T. Duan)

It is a good sign of understanding vulnerabilities well before an attack can occur, but these vulnerabilities show the vast chasm that needs to be crossed before satellites can be considered secure. CPPS have a known vulnerability there are ways to mitigate the risk and avoid an

exploitation to occur. It should be noted that CPPS are not he fix-all solution for satellite security they are instead a stepping stone for the future of security of physical power. CPPS are not made for satellites and will most likely be implemented in other more testable systems. Thousands of satellites are going to be launched by SpaceX, each will be made to be secure, but there is no guarantee that security implementations are safe.

Space may be the next frontier but the challenges humans will face will come from not only space itself but also Earth and those looking to improve their own agendas. The Department of Homeland Security may not have jurisdiction in space but a hacked satellite could effect the wider population of the US. It is important to understand the threats of space because the future of the information era may well rest on the resilience of communication satellites. Having worked for the Space Force for three years, I have seen the importance and lack of cyber security in space systems. Commercial systems will soon take up a majority of space vehicles, the effectiveness of their security is all that stands between thousands of satellite crashes and an effective communication system.

National Institute of Standards and Technology (2001) Security Requirements for Cryptographic Modules. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002. https://doi.org/10.6028/nist.fips.140-2

Waterman, Shaun. "Satellite Providers Stymied by Lack of Cyber Standards." Satellite Today, Access Intelligence, 14 Nov. 2019, www.satellitetoday.com/cybersecurity/2019/11/14/satellite-providers-stymied-by-lack-of-cyber-standards/. Accessed 10 Apr. 2022.

Manulis, M., Bridges, C.P., Harrison, R. et al. Cyber security in New Space. Int. J. Inf. Secur. 20, 287–311 (2021). https://doi.org/10.1007/s10207-020-00503-w

Mohanta, Nibedita. "How Many Satellites Are Orbiting the Earth in 2021?" Geospatial World, 28 May 2021, www.geospatialworld.net/blogs/how-many-satellites-are-orbiting-the-earth-in-2021/.

Mann, Adam. "Starlink: SpaceX's Satellite Internet Project." Space.com, Space, 17 Jan. 2020, www.space.com/spacex-starlink-satellites.html. Accessed 7 Feb. 2020.

Akoto, William. "Hackers Could Shut down Satellites -- or Turn Them into Weapons." GCN, The Conversation, 12 Feb. 2020, gcn.com/cybersecurity/2020/02/hackers-could-shut-down-satellites-or-turn-them-into-weapons/291164/. Accessed 10 Apr. 2022.

Falco, Gregory. "When Satellites Attack: Satellite-To-Satellite Cyber Attack, Defense and Resilience." ASCEND 2020, 2 Nov. 2020, 10.2514/6.2020-4014.\

R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," in *IEEE Access*, vol. 8, pp. 151019-151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

T. Duan and V. Dinavahi, "Starlink Space Network-Enhanced Cyber–Physical Power System," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3673-3675, July 2021, doi: 10.1109/TSG.2021.3068046.