October 2020

THIRD WEBINAR REPORT - *Space for the IoT: between the race for connectivity and cybersecurity concerns*

James Pavur
Rémi Ferrier

Acknowledgments

The organisers wish to express their gratitude to Mr. Rémi Ferrier and to Mr. James Pavur for their outstanding presentations on "*Space IoT and Cybersecurity*" and "*Emerging Threats in Emerging Space Technology*".

The Webinar immensely benefited from their valuable insights and expertise on cybersecurity and space issues.
Appreciation is also extended to Clémence Poirier for her support in the organisation of this webinar, for moderating it and for writing this report.

Also, the organisers would like to express their appreciation to the attendees for their participation, time and input. Finally, many thanks are expressed to the members of the Project Group for contributing to the organization of the Webinar.

About the organisers

Project Overview

The Space and Cybersecurity Project Group follows the outcomes of the Space & Cybersecurity working group at the European Space Generation Workshop 2018, hosted in Bucharest, to emphasize the need to reflect on the nature of space and cybersecurity, what the priorities of governments and international institution should be, whether data should remain open source or limited in its availability, possible technical solutions to the challenges posed above, and the shape and origin of threats to cybersecurity in space.

Objectives

The Project Group aims to create an international forum to further the discussions we had in Bucharest, which we aspire to lead to papers being published.

The Group is supporting SGAC's goals to providing a dynamic forum, where members can share their thoughts, views and opinions on international space policy issues, and raise awareness among the next generation of space professionals about the global scale of space activities.

The United Nations has also shown interest in the topic of cybersecurity, through resolutions and reports. We wish to push the cybersecurity agenda at UN Committee on the Peaceful Uses of Outer Space. The Project Group has 9 advisors, which supports SGAC's strategy to strengthen relationships and partnerships with academia and industry.

More information about the Space and Cybersecurity Project Group are available at:

https://spacegeneration.org/projects/space-cybersecurity

Additional note

The report was drawn up by Clémence Poirier with assistance from Thea Flem Dethlefsen. Pictures edited by Laetitia Zarkan.

It summarizes the presentations and exchanges of the 3rd Webinar organized by the Space and Cybersecurity Project Group, held on October 8, 2020.

The views and opinions expressed in this document are the sole responsibility of the Space and Cybersecurity Project Group.

The report aims to reproduce — to the greatest extent practicable and in a comprehensive manner — the content of the

presentations and of the debates that followed the webinar.

Where this document reports or refers to statements made by panellists, every effort has been made to provide a fair representation of their views.

About the speakers

Rémi Ferrier is a Chief Product Officer at Kineis, a French company specialised in satellite constellations for the IoT.
He previously worked as an engineer at CLS Group and as a technical engineer at Thales Alenia Space.
He also worked in the public sector for the Région Midi-Pyrénées (south of France).
Rémi graduated in engineering from Ecole Polytechnique and Institut les Mines-Télécom in France.

James Pavur is a doctoral researcher in cybersecurity at the University of Oxford. He graduated from Georgetown University where he majored in Science, Technology and International Affairs. His research focuses on satellite systems security with a particular interest in satellite broadband communications, space situational awareness data and satellite hardware security. He recently presented his research at the Black Hat conference and at DEFCON where he shared a number of vulnerabilities of satellite communications.

About the webinar

SGAC organizes free webinars open to all and gives the participants the opportunity to engage with experts on space-related topics.

About the moderator

Clémence Poirier is a researcher at the European Space Policy Institute (ESPI) in Vienna, Austria. She holds a Master's degree in International Relations, International Security and Defense from the University Jean Moulin Lyon 3, France**.**

RÉMI FERRIER

Space IoT and Cybersecurity

Mr. Ferrier focused his presentation on satellite connectivity for the Internet of Things, how it works as well as the cyber threats faced by commercial actors providing satellite connectivity for IoT devices.

Today everything is connected and the number of connected devices is increasing as well as the demand for connectivity. The internet mostly relies on submarine cables and other terrestrial infrastructure. However, terrestrial systems are not available everywhere (High Seas, remote areas, etc) which create the need for an alternative: satellite connectivity. This is the solution that Kineis, the company Mr. Ferrier works for, aims to use to provide global coverage for IoT devices.

According to Mr. Ferrier, the advantages of Satellite IoT are the global coverage provided by space systems, the absence of problems related to roaming and frequencies between neighbouring countries as well as the absence of white zones. Terrestrial IoT is more suited for densely populated areas, high volumes of data and indoor applications.

In addition, in the last few years, there has been increasing developments and improvements in satellite connectivity such as smaller devices, new modulations to reduce power costs and better latency.

The actors involved in satellite IoT are established space companies such as Iridium or GlobalStara and Kineis which have been involved in IoT for a long time. They are now diversifying their activities in the IoT sector, targeting different markets (broadband, internet, voice). New Space companies are also involved in the IoT business with the launch of large constellations for the internet (SpaceX, OneWeb). Some startups are also involved in low data rate IoT constellations. In addition, terrestrial IoT players are also trying to include satellite systems in their networks (as part of 5G standards for example).

Mr. Ferrier outlined that New Space has significantly improved the opportunity for satellite IoT as payloads are smaller, access to space is cheaper, large satellite constellations are providing better connectivity and latency that enable global coverage. Improvements in electronics (SDR or microcontrollers) enable new protocols and devices to be installed on board of satellites.

Mr. Ferrier briefly explained how satellite connectivity works. A device on ground generates a modulation that is transmitted to its antenna, reaches the satellite whenever it is in view, then the satellite receives the data and modulates it, puts it on its telemetry and sends it back to the ground station. A network of ground stations is needed, otherwise, the satellite will have to wait a longer time before it can send back the data to the ground station. The data is then sent to a mission center which is then processed and delivered to customers.

Mr. Ferrier explained the Space IoT project conducted by his company. Kineis was created by CLS and CNES in 2018 and raised €100 million in 2020 to launch a constellation dedicated to the IoT and is now operating 8 satellites that currently connect 20,000 devices. Kineis will launch 25 nanosatellites and will establish 20 ground stations with its main partners (CNES, Thales Alenia Space and Hemeria). The constellation will cover all continents with 5 satellites per orbital plan. Each satellite will contain one IoT payload and AIS payload will also be available for ship tracking. IoT for Space can be used for outdoor activities, agriculture, fishing, scientific activities (animal telemetry), logicitics (cargo tracking) and search and rescue systems.

In order to connect IoT devices through space, Kineis is building a small chipset for modulation, transceiver module with integrated network management stack and evaluation boards as well as development kits for testing and prototyping.

Futhermore, Mr. Ferrier mentioned the various cyber threats and some of the actions taken by Kineis to reduce cyber risks. When the data goes from the ground station to the mission center, it goes through the internet. Therefore, standard cybersecurity protocols are applied. Kineis makes sure that every component of the chain is secure and isolated from other networks. The number of people with access to the network is also restrained to the minimum to avoid additional human-related risks. Proprietary data protocols are being used for Kineis data collection and standard protocol are used for AIS. Regarding telecommand and telemetry, encrypted and authenticated communications are in place with proprietary protocols.

The cyber threats identified by Kineis are: interception, spoofing, replay attacks and signal interference (jamming). To reduce the risks, data encryption is the basis as well as authentication and integrity checks of each message that is sent on the network. These are mainly protection against spoofing and replay attacks. Proprietary communication protocols are needed along with device certification processes to have an awareness of all the devices connected to the network. IoT traffic is not very busy, as a device can send one to twenty messages a day. Device certification is used to check all the devices that are allowed to talk on their network. To reduce the jamming threats, doppler localisation can be used through a beacon which creates a doppler effect. Devices can send multiple messages over the same satellite and the satellite receives it from different positions. The messages will have a different speed depending on the position of the beacon. This gives a very precise frequency measurement making it easier to detect the doppler localisation of the device at various times. Using this technique enables jammers localisation and cross validation of GNSS signals, thereby adding one more layer of security.

JAMES PAVUR

Emerging Threats in Emerging Space Technology

Mr. Pavur first mentioned that hacking a satellite has long been a complicated endeavour. First of all it is usually expensive as a hacker would need to buy millions worth of equipment to look for vulnerabilities. In addition, the space sector has long been very secretive due to the nature of many governmental space missions and because the space industry is very insular and does not interact with the cybersecurity or computer science sectors. As a result, the two sectors evolve in silos and applying cybersecurity to space systems is more complicated than it seems. Also, space systems have long been very diverse and custom-made for specific contracts and purposes. In this case, finding a vulnerability in a satellite does not mean it will be present in other systems.

However, Mr. Pavur assessed that the space sector is changing and hacking satellites is becoming easier. As part of his research at Oxford University, he conducted an experiment to find vulnerabilities in satellite communications, more precisely VSAT internet services. Mr Pavur proceeded to explain how the changing landscape in the space sector enabled him to find vulnerabilities:

Firstly, VSAT services cost thousands of dollars (+$50k) but VSAT services also operate on the same spectrum as satellite television. Therefore, he tried to use cheap home TV equipment such as a PCIE Tuner (printed circuit board to watch satellite TV on a computer) and a satellite dish to receive signals from VSAT.

Secondly, Mr. Pavur outlined that he needed to find the right signal. He used free radio-frequency scanning software. He then looked into FCC licence fillings to find information of the spectrum used by these satellites. Mr Pavur declared that the standardisation linked to satellite internet services enabled him to find the protocols used by these systems. As a result, he easily found out that VSAT were using the DVB-S protocol and GSE, which are open source standards. He only had to write an algorithm that would understand these standards.

Thirdly, he built a tool named “GSE-Extract” which is a system that focuses on the easiest IP packets to capture. While this method was not targeted on a precise system or information, he still managed to grasp very interesting and sensitive information, which shows the high vulnerability of VSAT services.

As a result, he managed to find crew passport data and immigration information from cargo vessels, health information, credentials of personal email accounts from yachts which could enable a hacker to conduct phishing operations, and navigational charts in clear text that could be modified by a hacker and cause accidents or operational problems. Finally, he was able to read in-flight messages. As part of the IOT came the emergence of femtocells, which are essentially miniturature cell towers put in airplanes, making it possible for passengers to send or receive text messages while in the air. However, the traffic on the other side of these towers are broadcasted across these satellite feeds. Mr Pavur showed an example of a text informing the passenger of a negative corona test, revealing the potentially sensitive content of such text messages.

Mr. Pavur declared that these systems have never been protected against such attacks because the space industry thought it was impossible to hack them because the barriers used to be high (expensive, secretive, diversity of systems). However, now that the landscape is changing, it is becoming easier for hackers to penetrate a SATCOM network.

Mr. Pavur then proceeded to explain that New Space is making space systems cheaper and enabling hackers to buy cubesats for a very affordable price to search for vulnerabilities. As a result, the assumption that space systems are too expensive to get hacked is fading away. Hackers can now easily buy COTS components that are present in many satellites and look for vulnerabilities. In addition, SATCOM equipment used to be very expensive for an attacker to buy but now that many SATCOM systems are software defined, it is easier to receive and intercept data or enter networks than ever before. Also, Ground Station as a Service (GSaaS) such as AWS Ground Station can provide an attacker with access to the service in order to look for vulnerabilities. These trends lower the barrier of entry for a cyber attack.

However, Mr. Pavur highlighted that an attacker would still need to know and understand the target satellite. This task is getting increasingly easier for attackers with the emergence of Open Source Satellite OS or source code for space companies such as NASA Core Flight System. It gives an attacker many details about the functions of a satellite and enables them to look for vulnerabilities as well. Moreover, open communications standards can provide an attacker with critical information about your communication system. Finally, New Space commercial space companies are more open and communicative than traditional space companies and often publicly announce some of the hardware or the software they use or specific partnerships with other companies that can provide information that would enable an attack. Commercial companies also have to register their frequencies with administrative entities. For example, SpaceX's exact frequencies and antennas for Falcon9 are publicly available on FCC filings. Mr. Pavur reassured that this kind of information is much harder to get for governmental systems and missions.

Mr. Pavur concluded the presentation by addressing the future space system, and whether they will stay unique and diverse. He mentioned Lockheed Martin's SmartSat, a software defined satellite which puts together all the essential parts needed for a satellite to function and let the customer add its mission specific components (camera, sensors, communication antennas). This type of system makes satellites less diverse and less expensive and implies that a vulnerability in one system can be found in many others. Satellites in constellations are also all identical. As a result, an attack on one satellite would enable an attacker to hack the entire constellation.

The space industry has always been able to hide from cyberattacks, due to the barriers to entry for attackers because of the lack of information about how space structures work, how satellites are built and designed. However, going forward the small tech changes creates incidental opportunities for hackers. New Space is a great trend that improves the benefits of space and makes it more affordable but cybersecurity needs to be taken into
account as a conscious choice.

Martinovic, Ivan, Pavur, James (2019) The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space, 11 International Conference on Cyber Conflict, NATO CCDCOE

DEFCON 28 Briefing https://www.youtube.com/watch?v=ku0Q_Wey4K0

QUESTIONS AND ANSWERS

The presentations were followed by discussions.

What role can insurance against cyberattacks play?

James Pavur: One of the appeals would be to hand over the difficult risk calculous of the likelihood of a cyber-threat to someone who has more expertise. This way, it can help determine what level of risk is acceptable and use that to design the mission accordingly. The downside is, that it can be quite expensive, as insurance companies might pass on the inherent unknowability of the risk to the cost of the policy.

Rémi Ferrier agrees and adds the difficulty of how to evaluate the consequence of the attack, as there are many different ways to attack a satellite. For example stealing data, controlling the satellite, uploading something on the satellite can all have different consequences. This makes it difficult to find a business model for an insurance company.

Where does the security requirements for the Kineis constellations come from?

Rémi Ferrier: The French space law is one of the most advanced legislations on space operations regarding the control of the space operation and launch, but he is not sure how far they go in putting security protocols in place. However, Kineis security protocols are based on previous knowledge from CNES and previous missions. For example, Kineis' security protocols benefit from the experience of big space industry players like Thales Alenia Space, who have experience with bigger satellites and secure infrastructures.

James Pavur: His experience in disclosing vulnerability to internet providers showed that they perceived it with a lot of ambiguity in terms of who was responsible for encrypting communications and ensuring they were secure. For example, when disclosing vulnerability to a satellite operator, they would point towards the company they were renting the transponder from as being responsible for encryption. Regulatory clarity would go a long way in ensuring that the person who should take control of the risk is aware of this responsibility.

What is the difference between encrypting in LEO and GEO?

James Pavur: it is easier to encrypt internet traffic from LEO because latency is lower. There are all kinds of specific properties of the TCP protocol that are often used by internet websites that make it really sensitive to high latency systems. When we are beaming something all the way to GEO and back the latency problems means that if you are using a VPN the internet service provider cannot optimize that traffic as well as they could if it was unencrypted. LEO latency is not as good as on the ground, but the effect is much lower, so you can use a VPN and not have the connection become slow in the same way.

Rémi Ferrier: Relating what James said about internet and broadband to space IoT, here real-time does not matter as much. Whether it takes one second more to decode everything will not make that much of a difference, meaning that there will not necessarily be any difference between LEO and GEO for this application.

Is it a good idea to apply cyber situational awareness, meaning awareness of the data in the system, to satellites?

Rémi Ferrier: As long as you control everything on the ground you can go very far in monitoring the traffic and to identify abnormalities in the data. On the satellite itself, there are also already a lot of parameters that are monitoring the data.

James Pavur: A satellite is in theory not different from a computer that you leave on a street corner other than the fact that it is a little bit harder to physically reach. Monitoring a satellite is a tall order because a hacker that successfully gets access to the system could also potentially compromise the monitoring application itself. Therefore, it is important to understand how you can trust your telemetry data and your housekeeping data.

Accountability in IoT systems and in space operations

Rémi Ferrier: Frequency is monitored by the national frequency agency, and how you use this spectrum is regulated, meaning you are accountable for what you do with the frequency. Some countries have started to implement harder laws on space operations, allowing for accountability if you violate the rules. In the future such laws may be more strict regarding cyber security threat management.

James Pavur: accountability in terms of cybersecurity is about consciously deciding who is in charge of different threats and who is in charge of controlling different risks when you deal with a shared system like an IoT network.