EPFL

SPACE4IMPACT

EZMC

eSpace
EPFL Space
Center

SPACE
INNOVATION

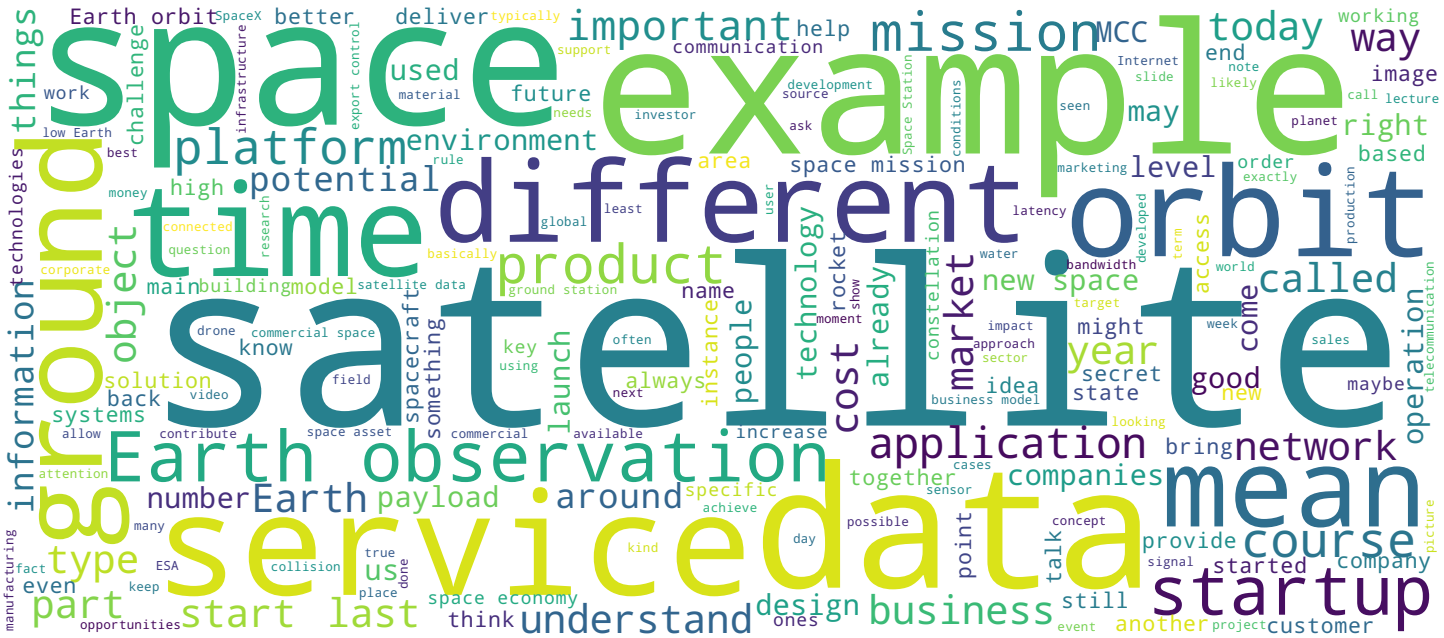
CYSEC

Cybersecurity

New Space Economy

Mathieu Bailly
VP Space
CYSEC SA

École
polytechnique
fédérale
de Lausanne



Search MOOC

Video

EPFL

Cybersecurity for Newspace

Hi. Welcome. My name is Mathieu Bailly, and I have the pleasure to give you an introduction to my favorite topic, Cybersecurity, for Commercial Space Missions. Every day we all read news about cyber attacks. This is the nightmare of any company turning on the laptop in the morning and reading a ransomware message, that's the absolute worst. Can this type of cyberattack happen to a commercial space company? What would be the consequences? What exactly are the cyber risks related to commercial space operations? What can be done to secure space assets and data? This is what I'll be talking about today. So let's get started.

Notes

Summary

0m 05s

Let's consider the idea of hacking a satellite. This should be really hard, right? Satellites are very far away. They are extremely costly to develop and launch, so they must be very well protected. Who would leave an asset worth hundreds of thousands, even millions of dollars unprotected? Well, actually, you would be surprised, hacking a satellite may be much easier than you think. Why? For a mix of reasons/. Historically, space engineers have focused on making satellites reliable and not secure. Security is not part of space engineering programmes today, so there is still very little awareness on the topic. Even worse, there are no space qualified security products that you can buy off the shelf today, and not to mention that commercial operators are under tremendous pressure to launch their service, thinking that security can wait.

Notes

Summary

0m 52s

Is the security issue going to solve itself? Not exactly.

Newspace trends making the case for cybersecurity more and more pressing:

- Software defined satellites
- Connectivity
- On-board intelligence
- Sensors capabilities
- Constellations

And some more bad news. Current trends in space tech show that things will just get worse. Let's review. Software defined satellites. They bring a lot of flexibility to space missions, for example, by enabling full in-orbit reconfigurations very handy. But more lines of code executing on board simply represent more opportunities for an attacker. Increased connectivity, between satellites and also with the ground is making satellites part of the Internet of things. Onboard intelligence, will also bring more opportunities for an attacker to disrupt the business logic of a service. High performance sensors, will make satellites capable of collecting data that are more precise, which means more sensitive and more valuable. So in the end, more attractive for the bad guys. And last but not least, large constellations, represent a greater security risk, considering the potential of an attacker to take control of the entire fleet in one shot.

Notes

Summary

1m 55s

3 consequences of a cyber attack on satellites

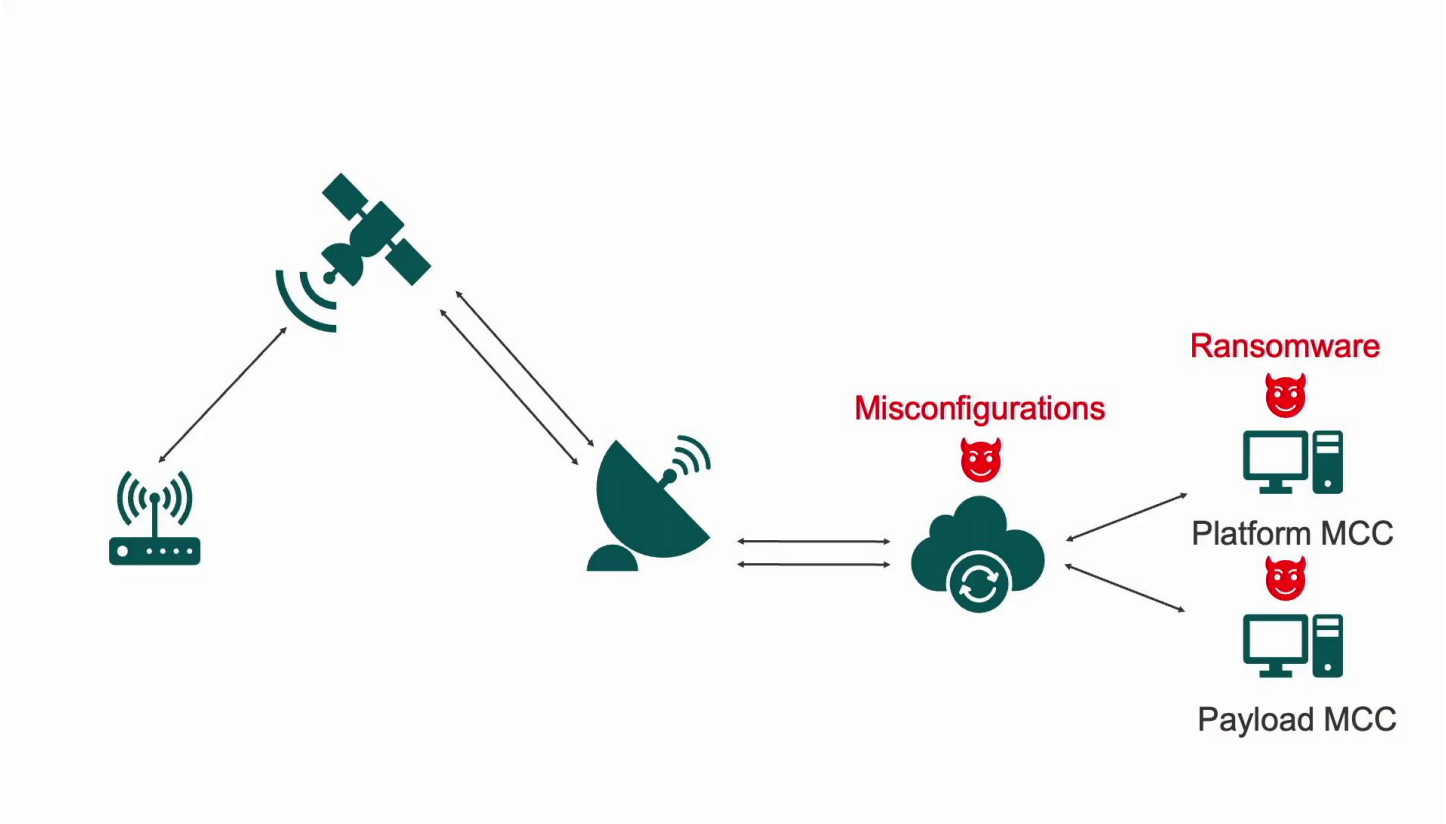
- Eavesdropping data
- Interrupting or shutting down services
- Taking active control of the spacecraft

So what exactly are the different consequences that an operator could suffer after an attack? Well, the first one is when hackers manage to access information they're not supposed to. Operators spend a lot of money to collect valuable data using space assets. So it would be a pity if this data falls into somebody else's hands, for example, end up being disclosed publicly or sold on the dark Web or bought by competitors or even used for political purposes. Even more serious an attack may lead to interruption or complete shutdown of the service. Typical scenario here is a ransomware attack, as we have seen hackers targeting critical infrastructures that were not well protected. And lastly, worst case scenario is when hackers managed to take active control of the spacecraft, potentially using it as a weapon. As even small stats today have propulsion capabilities.

Notes

Summary

3m 06s

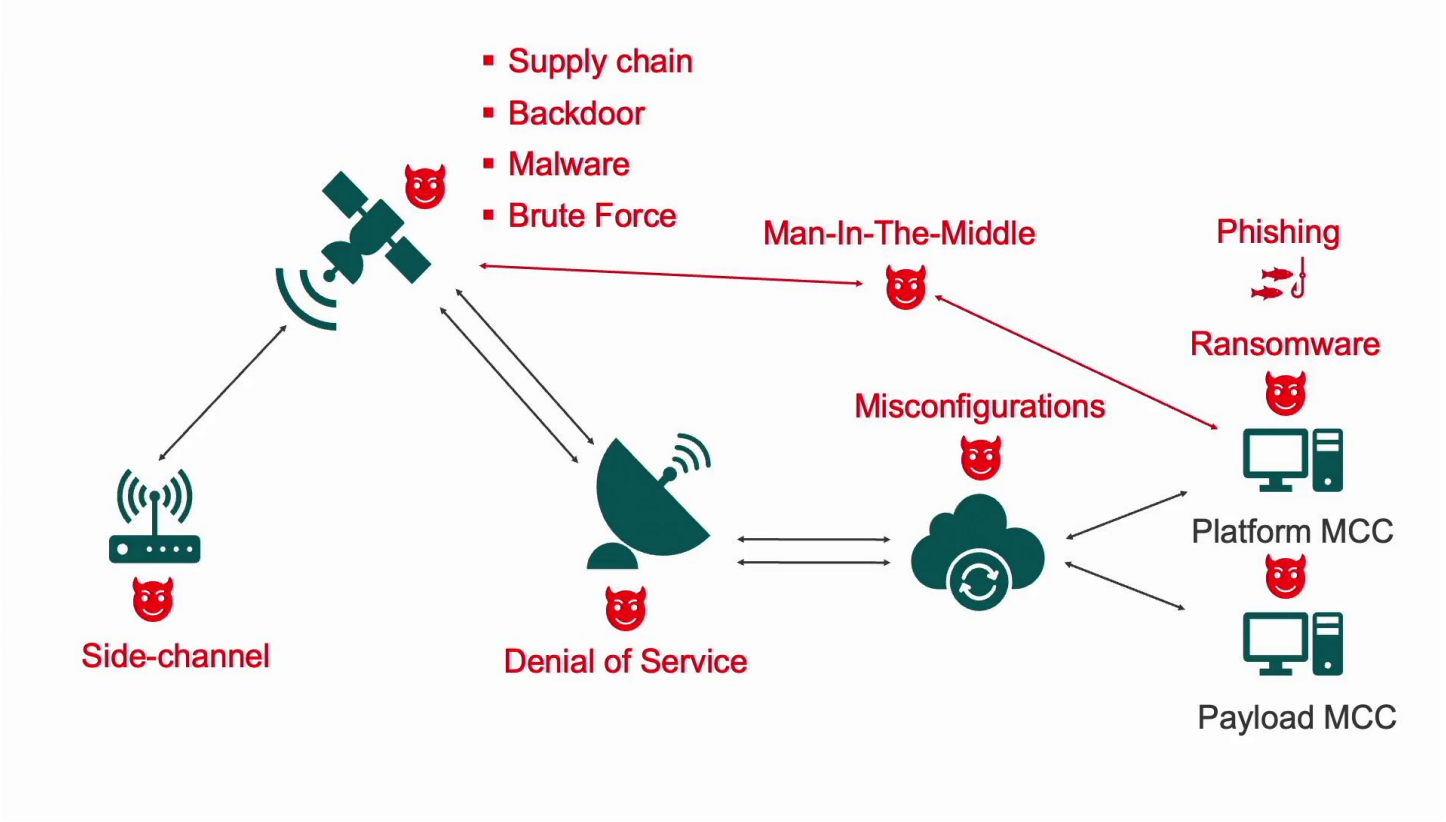


As the lower Earth orbit is getting more and more crowded, nobody wants to increase the risk of collision, so let's take a closer look at the potential entry points, considering both the ground and space segments, as well as the entire life cycle of a space mission. Here is a typical architecture. It features an orbiting satellite, some ground terminals or modems, a network of ground stations, two mission control centers or MCC, one for the platform and one for the payload, both connected to the cloud. Note that the satellite is only the tip of the iceberg and that the ground segment actually represents the largest surface of attack. So let's look at some potential threats. On ground, the most obvious target is the MCC. For the platform, the MCC is where the software sending and receiving the Telekom on and Telemetry is being executed. A hacker breaking into the MCC will literally do anything with the spacecraft. The MCC would typically be a prime target for a ransomware attack, and the same applies for the payload where hacker could access the data collected. Still on ground, many operators are now using cloud services. They are then subjected to the same cyber threats as any other business.

Notes

Summary

4m 12s



Note that most of the cyber incidents in the cloud come from miss configurations like poor access control settings for example. The ground station network is also a potential target, since it is the communication channel between the ground and the satellite. Hackers could, for example use, denial of service attacks to interrupt it or shut it down. The satellite itself can be a target. A backdoor or a malware can be introduced in the software running on board via supply chain attack for example. Cryptographic secrets like private keys can also be cracked by brute force attacks or leaked, for example, via side channel attacks. The same is true for ground terminals. Hackers can also pretend being a satellite or a mission control via Masquerade and Man-In-The-Middle attacks. And last but not least, operators may also suffer from more traditional attacks like Phishing.

Notes

Summary

5m 42s

Cyber Defense for Newspace: key concepts

Cryptography = algorithms + keys

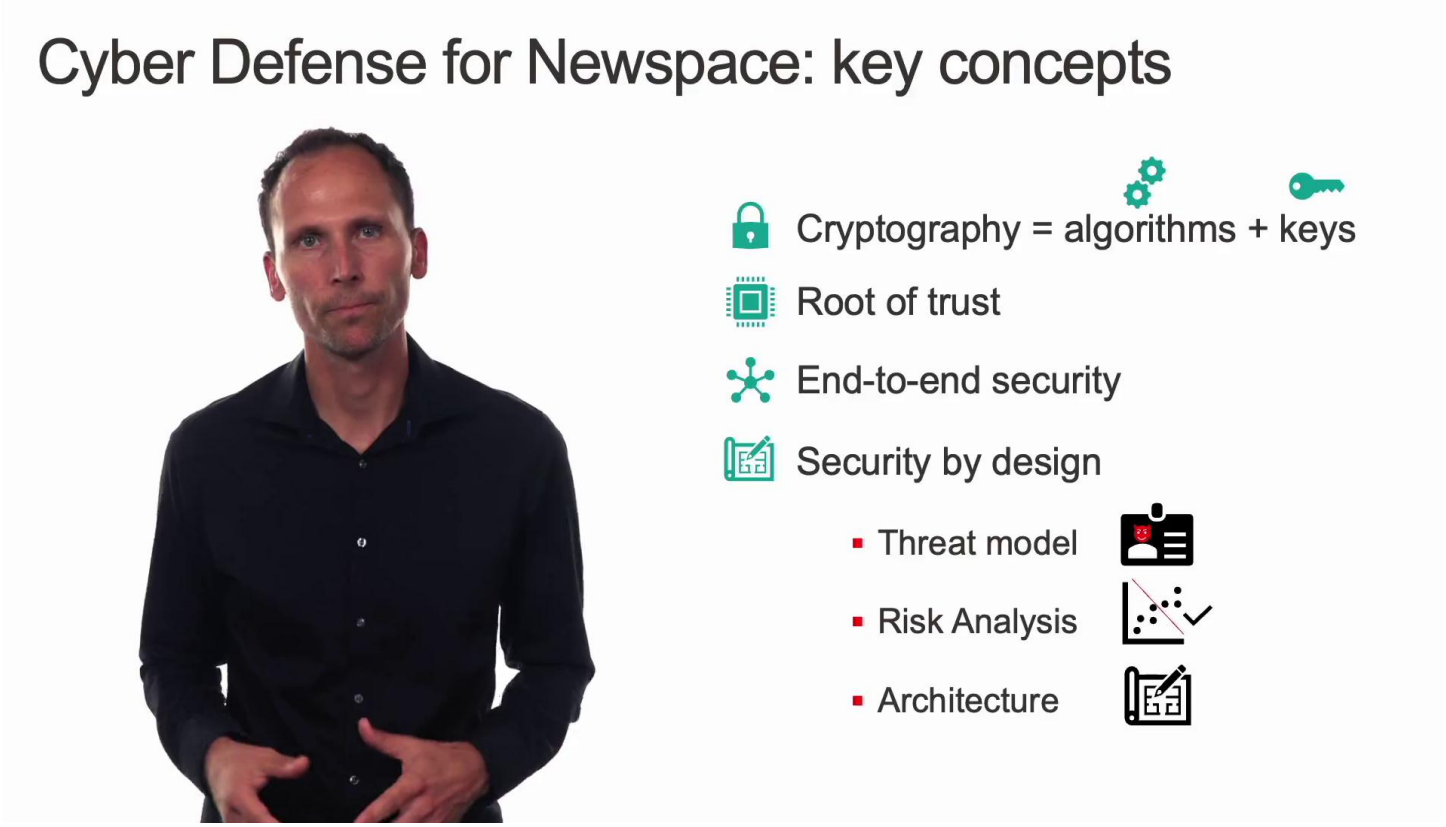
Root of trust

Before we dive into the various protection mechanisms. Let's take a moment to get you familiar with some key concepts. All cryptographic operations like encryption that consist in transforming plain text into a Cypher, requires an algorithm and a cryptographic key, also known as a secret. Cryptographic algorithms, are publicly available. It is recommended to use the versions that are approved by international security standards like Dennis, for example, and not to make up your own, this is a terrible idea. But note that if the key is compromised in any way, then the information transmitted is also compromised. So the level of protection provided by cryptography is directly linked to the level of trust one can have in the secret, so protecting the secret Aka the keys is absolutely critical. To achieve that. The concept of rule of trust comes in. A rule of trust refers to the environment where the secrets are generated and stored. This environment must be trustworthy as it lays out the foundations for all defense mechanisms using cryptography. Being able to encrypt and decrypt a message requires to use secrets on both sides of the communication channel.

Notes

Summary

6m 47s



In our case, it means that both the ground segment and the space segment must be equally protected. This is what we call End-to-end security. And now, to achieve all that, it is best to take it into account right from the beginning. This approach is called security by design. It starts by completing a threat model which describes what are the potential attackers and what are their capabilities. Based on the attacker profile, we can map out the different risks and scenarios with their associated consequences and decide which ones we want to mitigate and which ones we find acceptable and only then start thinking about the defense mechanisms that will need to be implemented.

Notes

Summary

8m 15s

Top recommendations

DESIGN

- Security-by-design

IMPLEMENTATION

- Certified crypto algorithms with high key size
- Trusted Execution Environment: HW + SW
- End-to-end: on ground and.. on board
- Pen tests

OPERATIONS

- Updates, patches, upgrades, etc

New space companies have often this tremendous advantage to start from a blank page, it's a unique chance to apply security by design. It has been proven many, many times that it is always more costly to fix vulnerabilities. Security by design also makes the implementation phase a lot easier. Typical recommendations there include, carefully choosing the cryptographic tools that will be used. Encryption is the most popular, but it only guarantees the confidentiality of the data. Authentication is often forgotten, but it's an absolute must. Signature may be needed depending on mission scenarios. For example, for protecting Earth observation data. Any of these should be based on certified algorithms with significant key size. Protecting the secrets as we explained before, ideally with hardware based generation and storage and with a key management system to handle them more efficiently. Executing all operations in a trusted software and hardware environment and both on ground and on board. And once the system is ready, it is always a good idea to ask a red team to regularly Pen test it. And finally, security never stops, even when the satellite is flying. Regular updates, upgrades, patches, et cetera are needed to keep the system up to date.

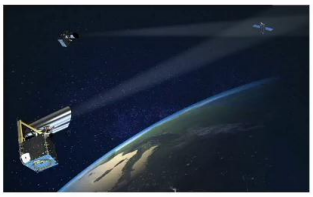
Notes

Summary

9m 04s

Examples of sensitive newspace missions

Earth Observation



Space Situational Awareness (SSA)

In-orbit servicing

What are the missions most likely to be attacked? The answer is every single one will be attacked at some point, it's the attacker profile that will make all the difference. That's why all space missions should implement at least the very basic level of security. But it is true that some missions are more likely to be targeted by serious groups of hackers and for which basic security will not be sufficient. Earth observation missions capable to collect data in the entire spectrum, revealing sensitive and secret activities happening on Earth. Some data, like high definition images of war zones or critical infrastructures, need to remain confidential, while in some other cases, like tracking sources of greenhouse gases, protection of data integrity and authenticity is more important. Missions to track other satellites. For example, to contribute the Space Situational Awareness and in case of SSA, protecting the integrity and availability of the data is paramount. In-orbit services, for example, refueling or deorbiting are absolutely security critical. One wants to make sure that the correct satellite is being serviced, protecting the TMTC link and the flight software is key.

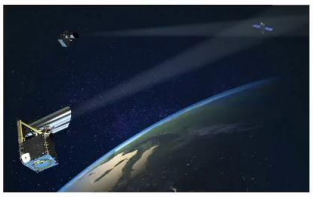
Notes

Summary

10m 45s

Examples of sensitive newspace missions

Earth Observation



Space Situational Awareness (SSA)

In-orbit servicing

Satellite as a service

Quantum Key Distribution (QKD)

Satellite as a service missions, flying multiple users on single platform is making confidentiality a priority. And finally, security can also be a mission by itself. For example, with Quantum key distribution. And Besides, the QKD Channel, protecting the RF channel is also critical. On this note, I thank you for your attention and I hope that you are now convinced that cybersecurity is key for the new space economy. Thank you you.

Notes

Summary

12m 18s