WHITE PAPER

End-to-End Security for Space Assets & Data

CYSEC

CYSEC

WHITE PAPER

About CYSEC

CYSEC SA is a Swiss cybersecurity company founded in May 2018 by Patrick Trinkler (CEO), Yacine Felk (COO) and Alexandre Karlov (CTO)

In November 2020, CYSEC counted 25 employees, mostly located in the EPFL Innovation Park in Lausanne, Switzerland. EPFL is the Swiss Federal Institute of Technology, one of the leading engineering schools in Europe.

CYSEC's vision is to become the European leader in **confidential computing** and a key contributor to the Confidential Computing Consortium[1] alongside leading IT companies, embracing the vision of enabling the protection of data in use.

While confidential computing is now being implemented in the backend of IT infrastructures, CYSEC believes that the overarching principles of protecting data in use will soon also be a necessity in edge computing.

In July 2020, CYSEC published an online article entitled "An introduction to confidential edge computing for IoT security" that promoted the application of confidential computing for the edge, i.e., connected devices that are part of the Internet of Things (IoT).

[1] https://confidentialcomputing.io/

Space assets, in particular satellites, can be considered as “connected objects”. Because of their growing capabilities of not only collecting and transmitting valuable data but also integrating intelligent processing on-board, they are subject to the same trends and challenges as terrestrial edge computing.

CYSEC’s mission is to provide the toolbox that will protect space assets and data in its three states—at rest, in transit and in use—on ground and in space.

What is confidential computing?

*Tom Merrits explains the concept of confidential computing:**

“You can protect data at rest—you encrypt it. You can protect data in transit—it's a little trickier, but you can encrypt that, too. What about while you're using it? You need to unencrypt the data to use it, right?

It would be hard to read your email if it's encrypted while you're trying to look at it. That's a problem because data you're using is in memory, which can be dumped, and then malicious folks have your unencrypted data.

There are some folks who believe you can protect data in use, it’s called confidential computing.”

**https://www.techrepublic.com/article/top-5-things-to-know-about-confidential-computing/*

TABLE OF CONTENTS

INTRODUCTION TO CYBERSECURITY IN SPACE

According to a 2019 European study, the global space economy grew an average of 6.7 percent per year between 2005 and 2017, almost twice the average yearly growth of the global economy.

> Cybersecurity is the only thing that keeps me awake at night.
>
> **- Jean-Marc Nasr,** Head of Systems Airbus Defense and Space

One contribution to this growth has been the "NewSpace" phenomenon, a trend also described as the Space 4.0 evolution. This (r)evolution encompasses a wide range of innovations, including:

- Reusable launchers that make space more affordable and accessible
- The advent of smallsat constellations
- In-orbit re-programmability
- Software-defined satellites
- Inter-satellite communications

Such innovations make new services that are based on the collection and/or transmission of data in space significantly more valuable than before.

This valuable data naturally attracts cyber criminals. Space engineers have been trained to design satellites as durable and as reliable as possible, with little concern for security. Today, the poor security level of some platforms has started to become detrimental to the industry.

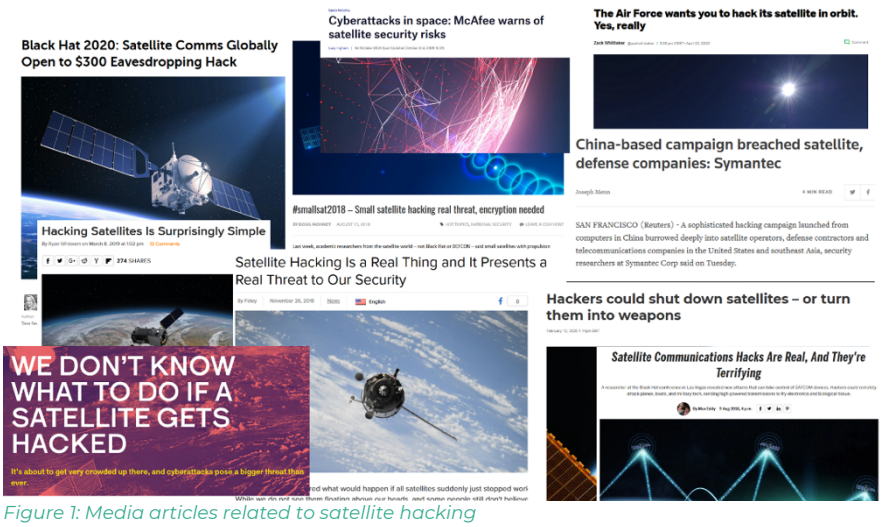

Figure 1: Media articles related to satellite hacking

This paper aims to provide an overview of the cyber risks in a typical satcom architecture, the key concepts of "security by design" and the solutions offered by CYSEC to establish end-to-end security between the space assets and the end-users.

1 CYBER RISKS IN SATALLITE COMMUNICATIONS

1.1 OVERVIEW

Satcom architectures are complex because they rely on multiple interconnected ground and space assets, and each individual node represents a potential entry point into the system. As a result, the satcom attack surface is very large.

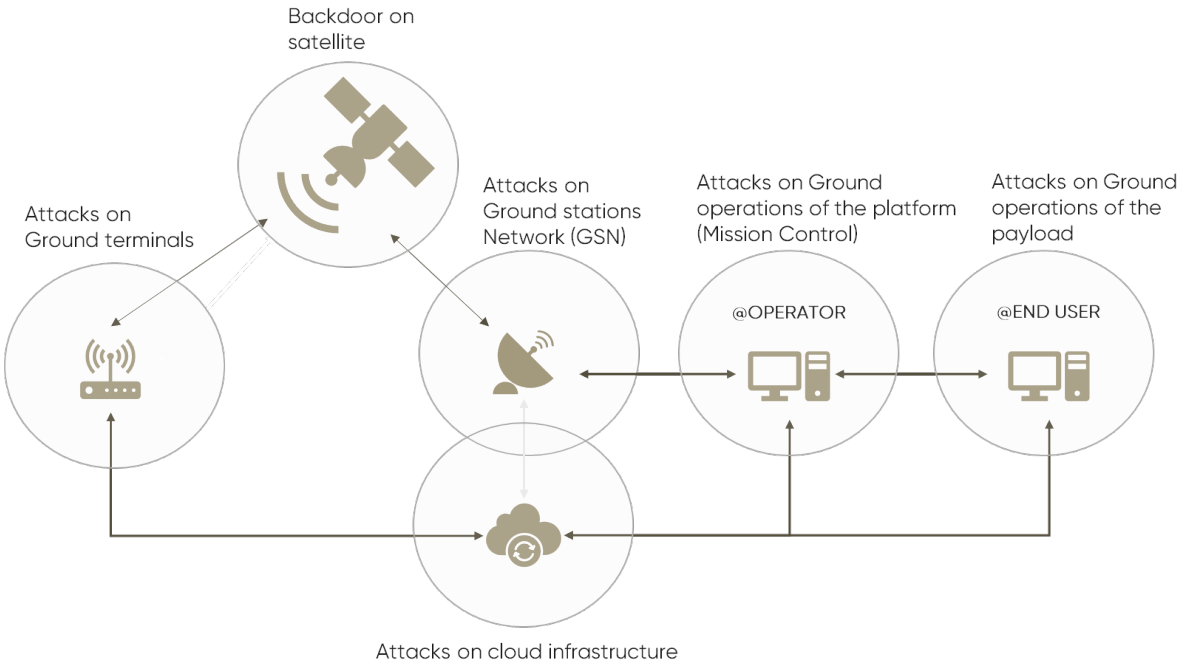

Figure 2: Illustration of the main points of entry for hackers in a typical satellite architecture

Although satellites may be the most "visible" part of the iceberg, they are not actually subject to the most immediate physical threats, at least when they are flying (ruling out the unfriendly alien scenario). The emergence of active debris removal and in-orbit servicing would make physical attacks possible, but it is unlikely that these will be performed on satellites anytime soon.

Therefore, one must consider attacks that could happen when the satellite is still on ground (e.g., during design, development, manufacturing, testing, launch) or attacks that can reach the satellite via the ground infrastructures.

On ground, the primary entry point is the Mission Control Center (MCC), which serves as the core infrastructure for communicating with the satellite. Within the MCC, the Mission Control Software (MCS) is responsible for executing all commands for sending and receiving telemetry and telecommands (TMTC) to and from the satellite. Most of the security mechanisms implemented to protect TMTC are at MCC and MCS levels. As a result, both the MCC and MCS are natural targets for attackers.

The network of ground stations that connect the MCC to the satellite is also considered critical infrastructure. For example, a

simple denial of service (DoS) attack could interrupt the stations' ability to communicate with the satellite and ultimately stop, interrupt or disturb the service.

Still on ground, data coming down from the satellite is likely to be made available to the end user in the cloud, which is a modern and convenient way to store and process data. However, cloud computing has some weaknesses in terms of security that must be addressed. We go into further detail about this in Section 1.2.

Lastly, in some cases (e.g., VSAT terminals for broadband satcom, smaller IoT devices), there are terminals on ground that are able to receive and/or transmit signals. These terminals may also be an entry point into the system, though this has a lower probability to seriously affect the entire service. To date, only eavesdropping attacks have been recorded on Ground terminals.

Ground operations for the satellite itself—from its design until it is standing on the launchpad—are full of opportunities for a hacker. These risks are all related to the sensitive data and software that the satellite will bring into orbit. If the data and software cannot be trusted on the ground, then the data coming down from the satellite in orbit cannot be trusted either.

For example, the cryptographic secrets (keys) that will encrypt the downlink on board the satellite during the mission are vulnerable to attack. They may have been poorly generated, handled or managed on ground, or an unsecure technique may have been used to inject the keys into the satellite. All these uncertainties lead to a decreased level of trust in the secrets on board the satellite, making the mission and the data potentially less valuable.

- The main threats a satcom architecture may be subject to include:
- Unauthorized access to satellite functions (e.g., commands)
- Unauthorized transmission or reception of data (e.g., tracking, telemetry, payload data/user traffic)
- Impersonation, corruption or replay of transmitted/received data
- Corruption of the correct execution of functions within satellites
- Impersonation of a genuine satellite
- Integration/injection of malicious software or hardware components before deployment
- Denial of service of cloud infrastructure, MCC, ground station network or the satellite
- Malicious software update in the on-board computer (e.g., during in-orbit reconfiguration)

- Leakage/theft/loss of sensitive assets of ground or space infrastructure (e.g., credentials, keys, passwords, etc.) before deployment or while in operation

The main scenarios are illustrated on Figure 3.

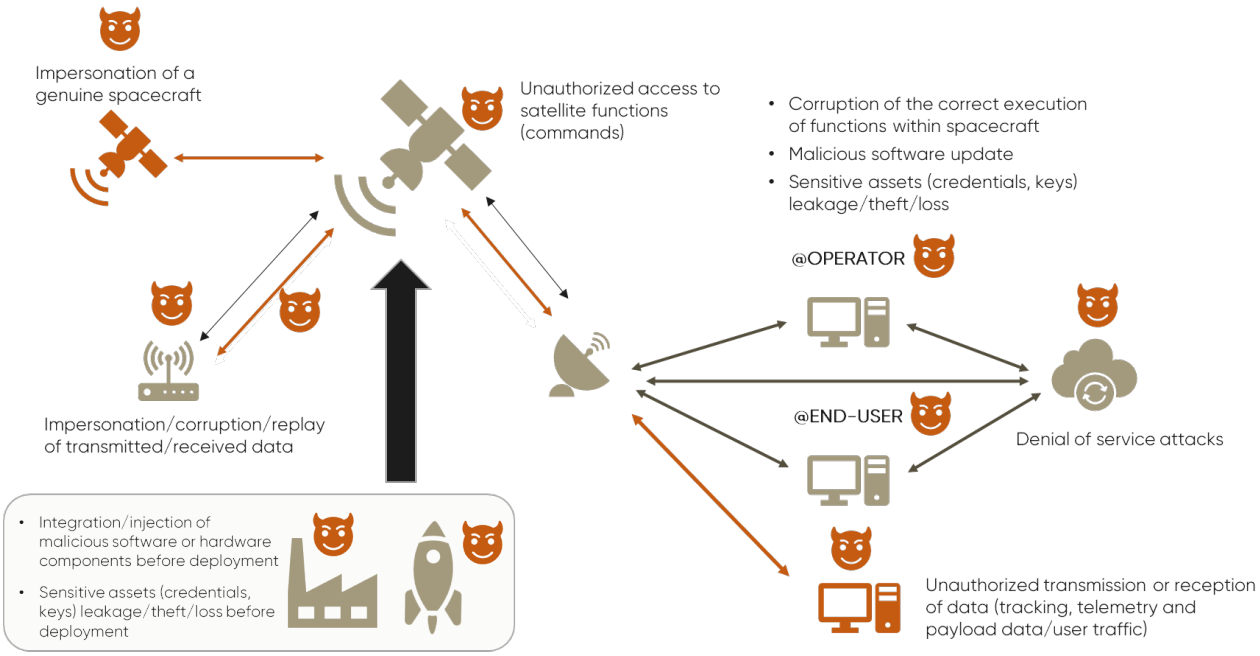

Figure 3: Typical threats in a satcom architecture

The consequences of cyber attacks on satellites include:

- Destruction, theft or loss of resources and services (part or all of a satellite)
- Unavailability of resources and services (part or all of a satellite)
- Communication jamming (from or to a satellite)
- Modification of information (from or to a satellite)
- Eavesdropping of information (from or to a satellite)

These attacks can have a dramatic impact on the business and jeopardize customers' trust in the space industry's ability to protect their assets and data against cyber threats. It could also have disastrous consequences on our ability to use the low earth orbit (LEO) itself. Satellites, which have propulsion capabilities, can be hacked to intentionally generate collisions in space, destroying the satellite and creating a significant amount of debris.

There are already various examples of satellite communication tampering, satellite hacking (e.g., control taken over by hackers, large-scale attacks on satellite operators) and even permanent denial of service (e.g., the case of the ROSAT x-ray satellite in 1998, leading to its later destruction). More references are provided at the end of the document.

The recent Space 4.0 trend increases the attack surface of space systems, making cybersecurity one of the biggest challenges for the space industry in the near future.

1.2 SECURITY CONSIDERATIONS FOR THE MISSION CONTROL CENTER

Mission Control Software (MCS) is a critical part of the ground infrastructure and executes sensitive operations, including:

- Preparing and sending telemetry and telecommand (TMTC) data
- Managing all communications with the satellite/payload
- Performing all security-related operations (e.g. encryption of TMTC data, signature of software updates for reconfiguration, authentication of satellites, etc.)

This crucial role results in the MCS being a prime target for the aforementioned cyber attacks. According to a survey conducted by CYSEC, the most common setups operators use to run their MCS today are air-gapped/offline servers, online servers and cloud hosting solutions. Each of these setups comes with its own risks, which are detailed below.

Air-gapped servers

Using air-gapped or offline servers is a good approach for avoiding remote threats resulting from an internet connection. However, it raises a range of additional concerns related to physical access to the server. Through poor identity and access management (IAM) or employee management, a malicious insider could gain entry to the server. A classic example is embedding a trojan via an infected USB flash drive like the Stuxnet[2] malware that made headlines in the 2010s. A physical attack can also be used to shut down a server.

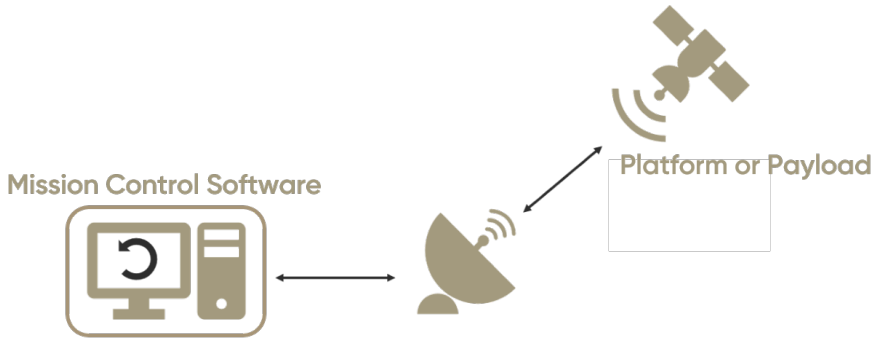

Figure 4: Illustration of MCS hosted on an air-gapped or offline server

[2] https://en.wikipedia.org/wiki/Stuxnet

Risks related to hosting the MCS on an air-gapped server:

- Constraints related to securing physical access to the server
- Software and keys are not protected in case of malicious access to the facilities and the server, leading to the risk of being stolen/leaked
- Software could be altered by a malicious insider (e.g., embedding a trojan or threatening the reliability of mission control)
- Honest employee management requires renewing all the keys as soon as an employee who had access to the server leaves the company
- Keys which are not generated by a secure key generation process could lead to weak keys and easier ways to break the security of the encrypted/authenticated messages from the outside (external threat)
- Denial of service (DoS) attacks breaking/shutting down the server

Online servers

Online servers benefit from all resources being available on the internet but also create opportunities for a hacker to infiltrate the server and eventually the MCS. Properly securing an online server on premises takes a fully skilled IT team.

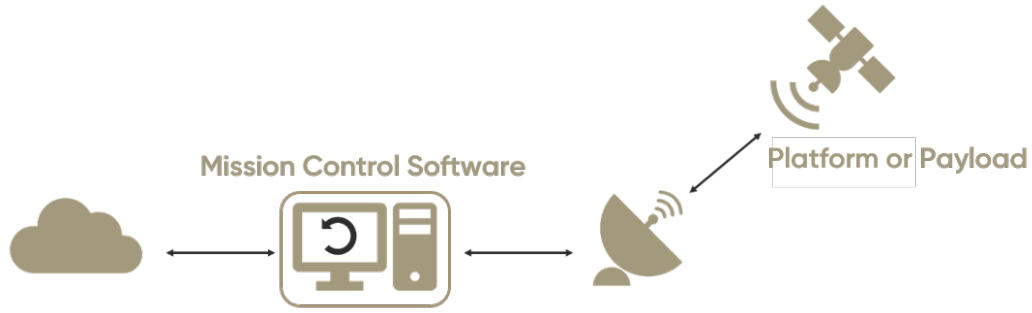

Figure 5: Illustration of MCS hosted on an online server

Risks related to hosting the MCS on an online server:

- Similar risks as offline servers listed above
- All the risks related to a remote hacker taking control of part or all of the server (e.g., key leakage, software leakage, software alteration, DoS attacks)
- Securing an online server requires a skilled IT team (CapEx, OpEx)

Cloud hosting

Cloud services have become popular due to the easy setup of scalable, efficient, cost-effective services as well as a reduction in

CapEx and OpEx related to owning and operating an on-premises IT infrastructure.

However, as large breaches disclosed in public media have shown, these advantages may come at the expense of security. These attacks were mostly due to improper configuration of the cloud services and difficulty safeguarding administrator credentials.

In addition, some companies may not be comfortable storing sensitive data with US-based cloud providers. Indeed, the Cloud Act on data privacy states that the US government may request access to any data in the hands of US companies when necessary. This could be an issue for European companies that have customers worldwide or that are not willing to have their own data shared with or disclosed by the US government.

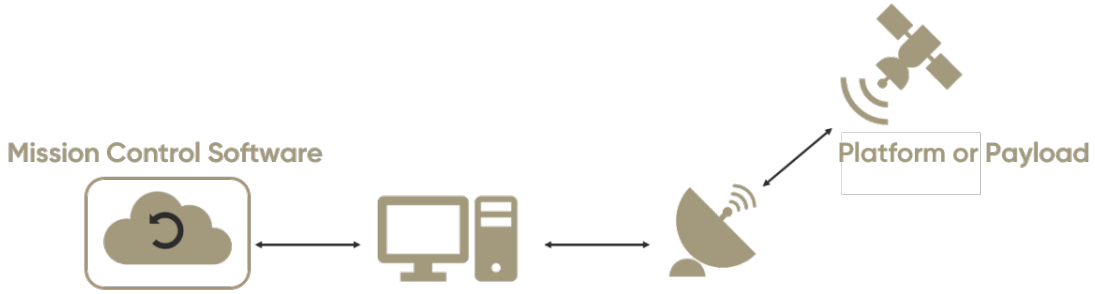

Figure 6: Illustration of cloud-hosted MCS

1.3 SECURITY CONSIDERATIONS SPECIFIC TO THE SPACE SEGMENT

The space segment today is mostly vulnerable to ground attacks, either by accessing the satellite through other ground infrastructures or by attacking the satellite itself during ground operations before launch.

The main risks related to the satellite itself are twofold:

- Compromise of secrets (private keys) used on board for cryptographic operations
- Compromise of software executed on board

In both of these cases, “compromised” means that neither of these elements—private keys and software—can be trusted. The lack of trust in cryptographic secrets has been a prime challenge ever since cryptography has been used to protect data at rest and in transit. This topic has been explored by researchers and security professionals for decades in markets with mature cybersecurity, commercial space not being one of them yet.

Leakage, theft or loss of data due to compromise of cryptographic secrets or software may originate from:

Weak security architecture

One may have the most secure procedures and the best security engineers, but if the architecture is poorly designed, an attacker will be able to find and exploit a vulnerability. Designing the security architecture actually comes only after a number of steps have been completed as it is described in detail in Section 2.

Examples of pitfalls in security architecture design:

- choosing non-adapted or weak cryptographic functions like favoring authentication without encrypting data
- picking a weak algorithm which has been already broken
- misconceiving the key lifecycle management
- misjudging the match between security requirements and the hardware implementation

Lack of procedures

This category is more specific to the space industry. It is paramount to understand that the entire lifecycle of a cryptographic secret must be considered in order to assess its level of trust. This is only possible via specific procedures for generating, exchanging and managing the secrets before their injection onto the satellite. For example, many satellites are shipped months, or sometimes years, ahead of their launch date in parts of the world where it is sometimes difficult to assess the level of risk during transportation or at the launch site. Having a well-defined procedure for the injection of the secrets is therefore crucial.

Poor on-board implementation

Independent of the architecture and the procedures, the hardware and software used on ground and on board are of prime importance. For example, choosing the on-board computer (OBC) or the Microcontroller Unit (MCU) in function of the root of trust (RoT) and cryptographic capabilities available is absolutely critical. On ground, the choice of environment to deploy the MCS in is also of prime importance.

Vulnerable third-party infrastructures

Relying on external sources for critical activities is always a risk. Typically, Ground Segment as a Service (GSaaS), Satellite as a Service (SaaS) or cloud hosting are very convenient, but they require a well-defined security approach.

Lack of education or personnel

This category is a general risk and not specific to the space segment. Today, many of the largest breaches reported are the result of simple but efficient phishing attacks. As in any other industry, security education for company personnel is key.

Lastly, once the satellite is flying, there is still only one risk of physical attack (again without counting the unfriendly alien scenario)—Mother Nature.

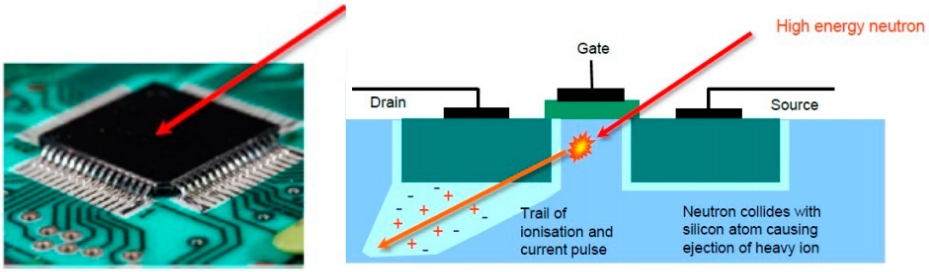

Figure 7: Illustration of Single Event Effects on space electronics, from Guerini et al., 2012

These physical "attacks" on the on-board electronics are due to Single Event Effects (SEEs). In space, electronics, and in particular field-programmable gate arrays (FPGA), can be impacted by solar radiations and, more precisely, ionizing radiation that can generate faults on the underlying FPGA architecture of the OBC as well as on the data being processed by the computations implemented on the FPGA cards themselves (e.g., bit status swap, wrong computation or communication errors). These SEEs can be mitigated with a variety of precautions in software and hardware.

2 DESIGNING AN END-TO-END SECURITY ARCHITECTURE

2.1 OVERVIEW OF SECURITY BY DESIGN

It is a classic pitfall to begin implementing protection mechanisms without having the big picture in mind. The concept of "security by design", however, encompasses an end-to-end process that starts well before the security architecture design phase.

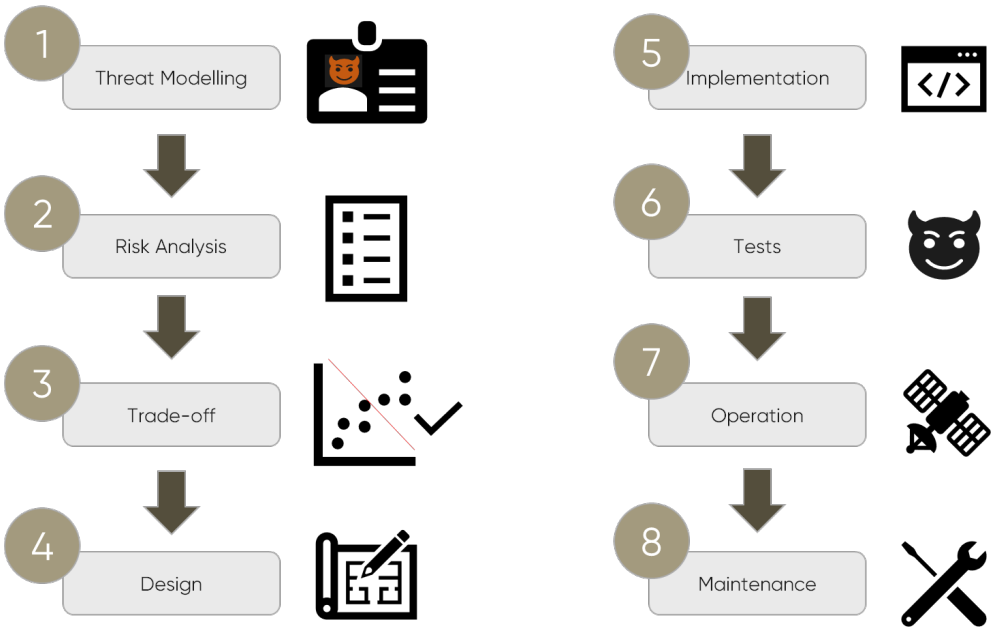

Figure 8: Overall security by design process

Threat modelling

The threat modelling phase aims to define the profile of potential attackers, their level of knowledge, their resources and their motivations as well as the impacts to the system should an attack occur. This phase is essential as it sets the foundation for the rest of the process and drives the ultimate outcome.

For example, a nanosat operator is likely to define potential attackers as "bored students playing around during the weekend trying to hack the university's nanosat just for fun"; whereas a commercial operator contracting its platform to B2G customers is more likely to define its profile of attackers as national agencies with significant resources and experienced hackers.

Risk analysis

Once the attacker profiles have been defined, a list of the potential risk scenarios can be established. This phase usually looks like a brainstorming session with inputs from both the operator's technical team and an external offensive team with qualified ethical hackers.

The scenarios are usually numerous, typically 100+ for a simple smallsat mission. In order to prepare for the risk trade-off phase, the scenarios are plotted on a graph based on their likelihood and their severity.

Figure 9: Illustration of risk trade-off for identified risk scenarios

It's also important for the operator to make a qualitative estimation of efforts required to mitigate each scenario in preparation for the next phase.

Risk trade-off

Once the list of scenarios has been created, the operator decides which risks can be considered acceptable and which ones must be mitigated.

For example, an operator of a CubeSat mission lasting only two years would likely accept the risk associated with not being able to upgrade its cryptographic algorithms in orbit to prevent post-quantum attacks. However, the operator of a sensitive GEO satcom mission lasting 15 years may find this risk unacceptable.

On the scenario plot, these risk trade-offs can be represented visually by a diagonal line that separates the risks to be mitigated (high severity, high likelihood) from the risk identified as acceptable (low severity, low likelihood).

2.2 DESIGNING THE SECURITY ARCHITECTURE

With the first three phases of the security by design approach complete, it is customary to begin designing the architecture. There is no one-size-fits-all architecture.

Each use case or mission scenario is unique, and each operator or client will have its own definition of what is the level of risk to be considered acceptable. However, some central concepts are important to comprehend before diving into the design phase.

Selecting the right cryptographic tools

First, there are many cryptographic tools available to secure data at rest and in transit. Encryption is the most popular and widely used, but it has its limitations and pitfalls. We detail these limitations further in Section 3.

Typically, aerospace engineers are not very familiar with cryptography, and many of these tools remain untouched in the toolbox. There are several types of cryptography (symmetric, asymmetric), techniques based on the concept of public key and other operations like authentication, attestation or signature that are all very powerful tools when the mission scenario requires them.

The main differences between encryption, authentication and signature are provided below:

Figure 10: Definitions for three types of cryptographic tools

To illustrate, the goal of encryption is to ensure the confidentiality of the message, i.e. to prevent the risk of an attacker who intercepts the message being able to read it. But without authentication, an attacker could still impersonate a ground station or the MCC and send malicious commands to the satellite.

Signature is useful for the downlink of payload data that requires proof of authenticity and integrity—e.g., sensitive earth observation images captured by a camera on board.

End-to-end means on ground AND on board

An end-to-end architecture will involve security mechanisms for both ground and space segments. The main operations that can be performed on ground and on board are listed in the figure below:

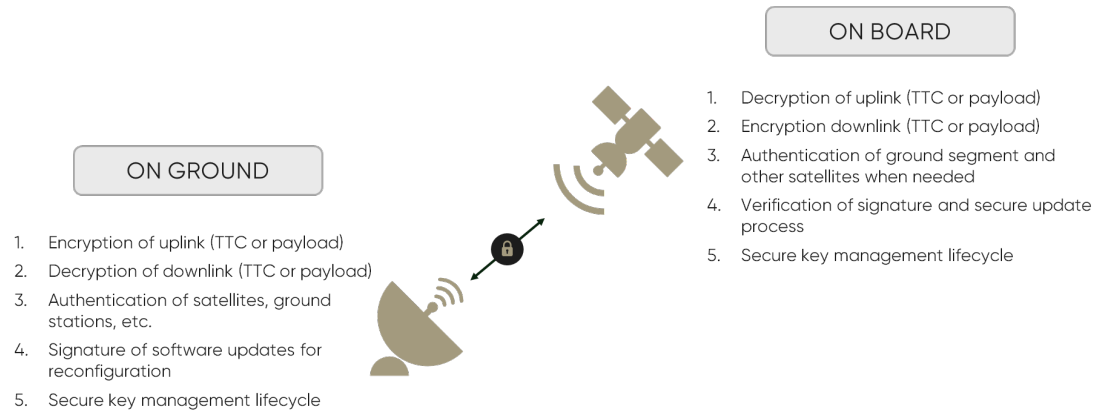

Figure 11: Examples of cryptographic operations on ground and on board

Why a root of trust on ground and on board is non-negotiable

As explained above, it is essential to be able to trust both the cryptographic secrets and the software that is executed on ground and on board. The basis of this trust comes in the concept of **root of trust (RoT)**.

RoT refers to the environment where secrets are generated and stored, typically in the ground servers or cloud infrastructure of the MCC or the OBC.

The existence of RoT is not in and of itself sufficient as it needs to be completed through a set of procedures across all operations.

Towards confidential computing on ground and on board

While the concept of RoT relates to the protection of secrets, an additional layer of security is needed to protect the logic (software) that relies on the secrets.

Protecting data "in use" is the next frontier of cybersecurity. Many recent attacks have shown how hackers were able to exploit vulnerabilities in the hardware and software executing the logic. This typically happens when a hacker takes advantage of data that has to be in memory at some point in order to be processed, and this memory can be attacked in order to retrieve information.

Several approaches are being developed in order to prevent these vulnerabilities. One of them is the trusted execution environment (TEE).

According to the Confidential Computing Consortium (CCC), a TEE is an environment that provides a level of assurance of data integrity, data confidentiality and code integrity[3].

What is a root of trust?

According to NIST, roots of trust (RoT) are highly reliable hardware, firmware and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design.

As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

[3] https://confidentialcomputing.io/

A TEE prevents unauthorized entities from having access to the data and the logic. These entities include other applications on the host, the host operating system and hypervisor, system administrators, service providers and the infrastructure owner or anyone else with physical access to the hardware.

TEEs are gaining adoption in terrestrial markets and represent a way forward for protecting space infrastructures—both on ground to protect the software (MCS) and secrets used to communicate with the satellite at the MCC as well as on board to provide a secure environment for the software executed in the OBC.

3 CHOOSING THE RIGHT CRYPTOGRAPHIC TOOLS

3.1 WHY ENCRYPTING WITH AES IS NOT ENOUGH?

When operators are asked by clients "What security measures are in place to secure satcom links?" it is common to mention encryption of the downlink and uplink using the Advanced Encryption Standard (AES).

AES is a mathematical function called a symmetric block cipher that is used to encrypt electronic data. NIST imposed AES as a standard in 2002, and it has since proved to be resilient to brute force attacks. Only side-channel attacks have broken AES-128, so it is considered an extremely secure way to encrypt data.

Limitations of AES encryption

The AES family of ciphers is recognized by the industry to be secure, however AES is always implemented in a *specific* hardware/software context. This context makes all the difference from a security point of view. Let's review.

First, AES is a symmetric algorithm and requires an algorithm *and* a key to transform plain text into a cipher. For example, the same key used on ground to encrypt a telecommand would be used on board to decrypt it. If this key is compromised (e.g., by leveraging a software or hardware bug or using side-channel attacks), then the confidentiality of the information is compromised. So, we come back to the concept of securing the cryptographic secrets used for all security-related operations based on a RoT on ground and on board.

The figure below provides an illustration of the limitations of AES if the keys used cannot be trusted.

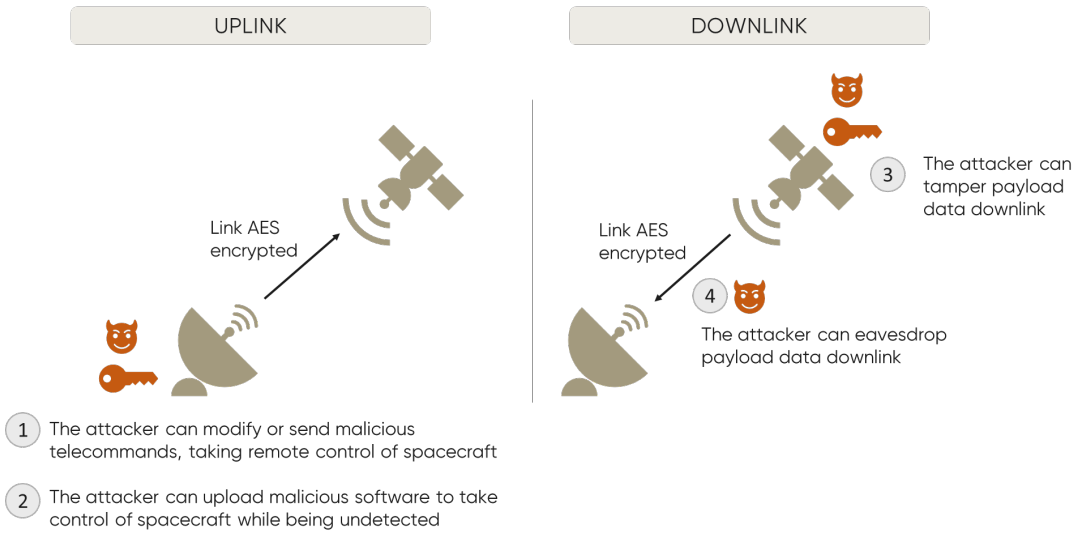

Figure 12: Typical risks if AES key on ground and on board has been compromised

After choosing the right cryptographic tools for the mission scenario and threat model and after having defined a RoT for the cryptographic secrets, there remains the question of protecting the environment executing the software. This is the goal of confidential computing exemplified by the TEE described in Section 2.2.

Last but not least, symmetric encryption shows even greater limitations when many satellites are part of a single constellation. One cannot imagine using the same secret for all of them. This challenge of scalability has been faced by many terrestrial applications and was solved by using a different type of cryptography, asymmetric encryption, which we will cover in the next section.

3.2 SYMMETRIC VS. ASYMMETRIC ENCRYPTION

Symmetric encryption is the simplest kind of encryption, because it uses only one secret key to encrypt and decrypt information.

There are, however, two main drawbacks to the use of symmetric cryptography:

1. For a secret key to be shared, a secure communication channel is required
2. A new key is required for each ground-satellite pair resulting in a high number of keys to manage. Otherwise, compromising one satellite would result in breaking the whole fleet

Asymmetric encryption was introduced to address the inherent problems described above by using a pair of public-private keys consisting of a public key, which is freely available to anyone, and a private key, which is kept secret to ensure that only the recipient can use it.

This concept allows for the exchange of information with a large number of recipients without having to share the same secret with each one of them, assuming the public key is trusted.

A more detailed example of public key infrastructure to secure in-orbit reconfiguration is provided in Section 5.3, and the basics are illustrated below:

What is a Hardware Security Module (HSM)?

An HSM is a piece of equipment that stores cryptographic secrets without the possibility of extracting them. HSMs were developed decades ago and are still perceived today as state-of-the-art in terms of level of protection.

Various international standards and certifications can be found on the market (FIPS, Common Criteria, NATO, etc.).

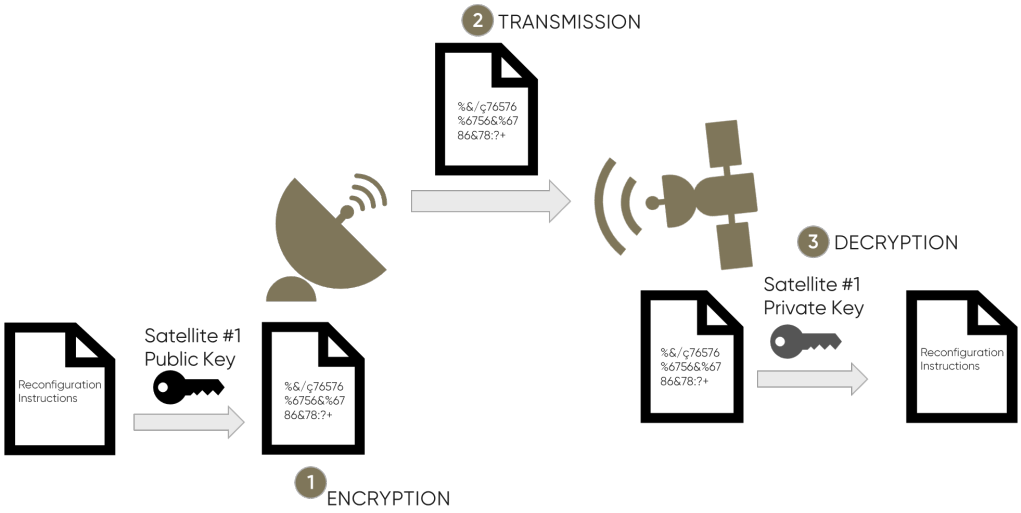

Figure 13: Illustration of asymmetric encryption for satcom

3.3 SECURING SATELLITE COMMUNICATIONS WITH A PUBLIC KEY INFRASTRUCTURE

A popular way to implement asymmetric cryptography and the trust among entities relying on it is through a public key infrastructure (PKI).

Since there is no need for the nodes in a network to store all the public keys for all the other nodes and their link to the corresponding owner, this results in a more efficient and less storage-consuming key management system.

Because only one certificate needs to be issued for each new node, PKI allows networks to scale more easily. However, the central piece of the PKI resides in the CA which holds the private key to sign all certificates.

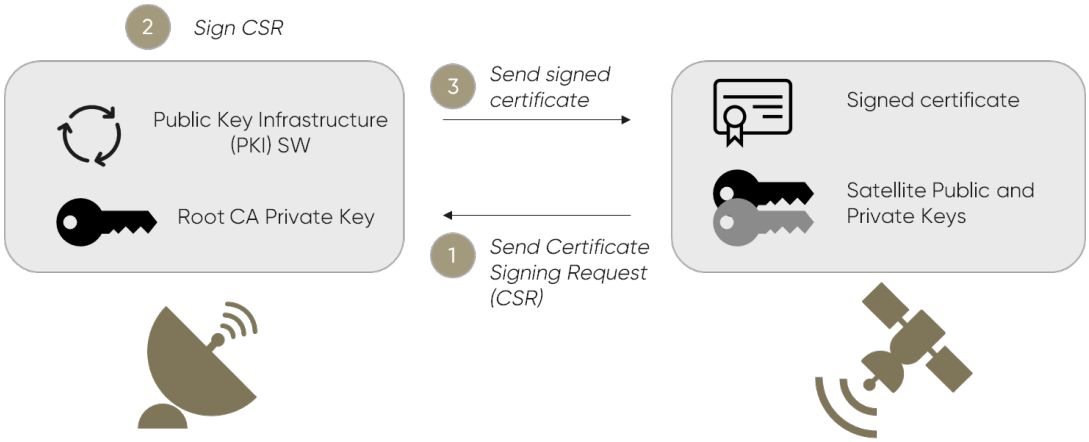

Figure 14: Illustration of the three steps to register a satellite in a Public Key Infrastructure

There are already several research papers and recommendations on PKI deployment for satellites (e.g., from the CCSDS[4]), and even a vision of deploying a CA in space[5], but none discusses the issue of reconfiguration and long-term security.

[4] https://public.ccsds.org/Pubs/350x6g1.pdf

[5] https://arxiv.org/pdf/1710.01430.pdf

4 A PRAGMATIC APPROACH TO IMPLEMENTING END-TO-END SECURITY

4.1 OVERVIEW OF THE ARCA FAMILY

At this point in the security by design process, it is time to implement the security technologies as dictated by the security architecture design.

CYSEC, a Swiss cybersecurity company, provides off-the-shelf products that enable end-to-end security for satellite communications.

Our product portfolio was influenced by the needs and current practices of players in the space industry as well as the best practices of terrestrial markets that are more mature in terms of cybersecurity.

Our goal was to facilitate the use of existing tools through a plug-and-play approach for satellite operators, manufacturers and ground segment providers that does not require any specific security or cryptographic expertise.

The solution offered by CYSEC takes the form of a hardware-based TEE on ground called ARCA that secures the MCS and its associated secrets and ARCA^{SPACE}, its on-board equivalent that provides a RoT on the spacecraft to execute all security-sensitive operations.

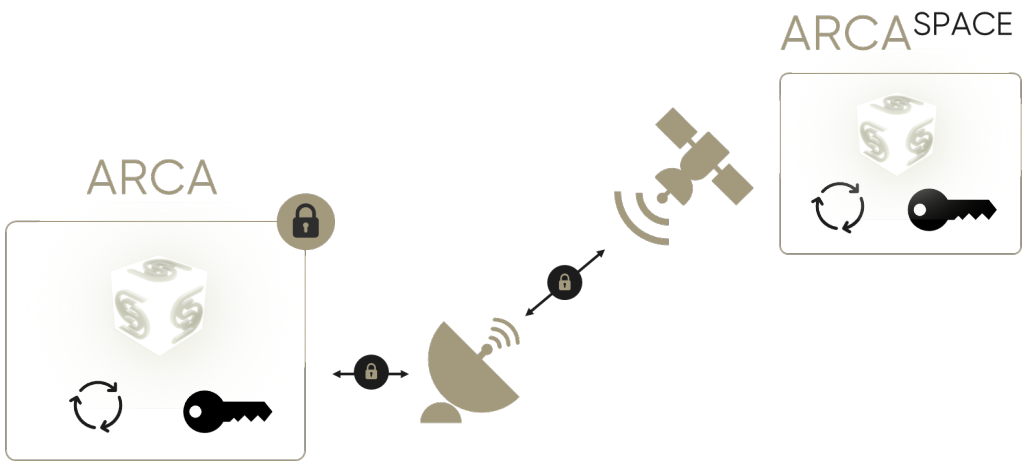

Figure 15: Overview of CYSEC products for end-to-end protection: ARCA on ground and ARCA^{SPACE} on board

4.2 SECURING THE GROUND SEGMENT

CYSEC identified the MCS as one of the critical entry points into a space infrastructure. In order to protect the MCC, CYSEC designed a TEE called ARCA. ARCA enables secure execution of the MCS thanks to its three-layer architecture and its confidential computing approach.

ARCA is available either on premises in the form of a physical appliance with a 1U form factor or as a service for a cloud deployment.

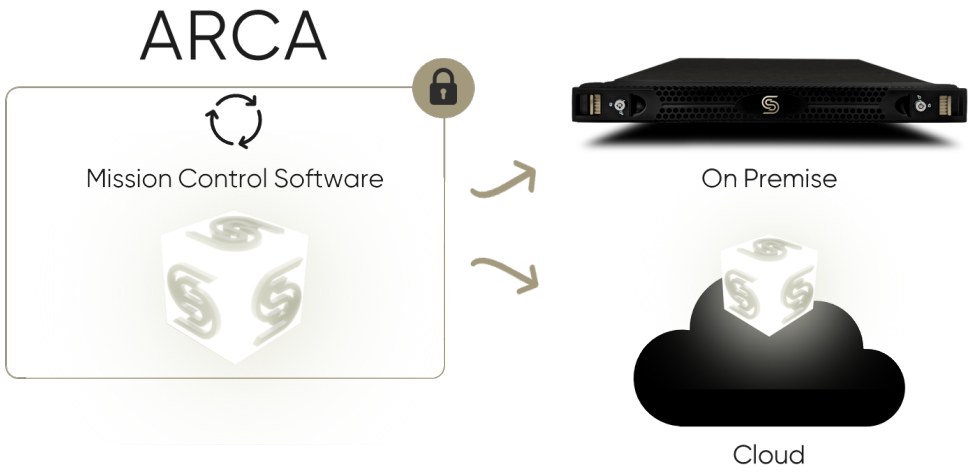

Figure 16: CYSEC's trusted execution environment ARCA to secure the MCS

In order to make TEEs more accessible and easier to use, CYSEC built a custom hardened operating system based on Linux, which is able to connect the application layer (MCS) and the security hardware.

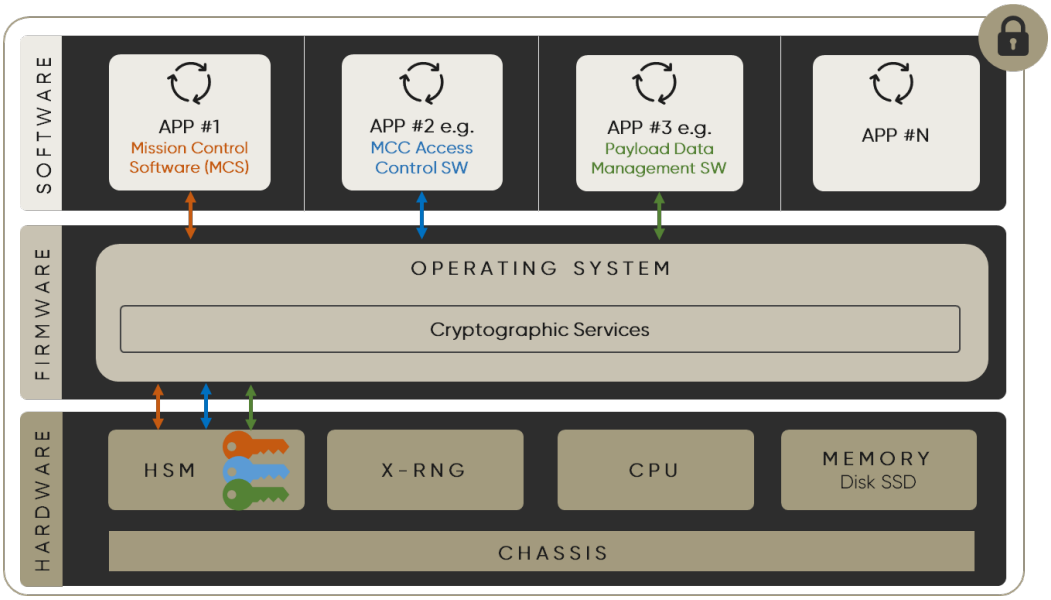

Figure 17: The three-layer architecture of ARCA

The main advantages of the hardened operating system developed by CYSEC are summarized below:

- The architecture of the TEE is designed to protect data at rest, in transit and in use.
- ARCA is capable of deploying software based on modern DevOps practices and using the most popular containerization tools like Docker or Kubernetes for deployment in cloud environments. As a result, deploying the MCS in ARCA takes no extra efforts versus deploying on a traditional server or in a public cloud environment.
- ARCA provides access to all standard cryptographic functionalities and primitives that are pre-integrated in the hardware, typically in a hardware security module (HSM), such as hashing, encryption, decryption, signature, etc.
- An integrated key management system in the hardened OS allows the application layer to natively benefit from all functionalities related to the management of secrets, like key lifecycle management, etc.

4.3 SECURING THE SPACE SEGMENT

ARCA^{SPACE} completes ARCA on ground by providing a RoT on board the satellite to store cryptographic secrets and execute all security-sensitive operations.

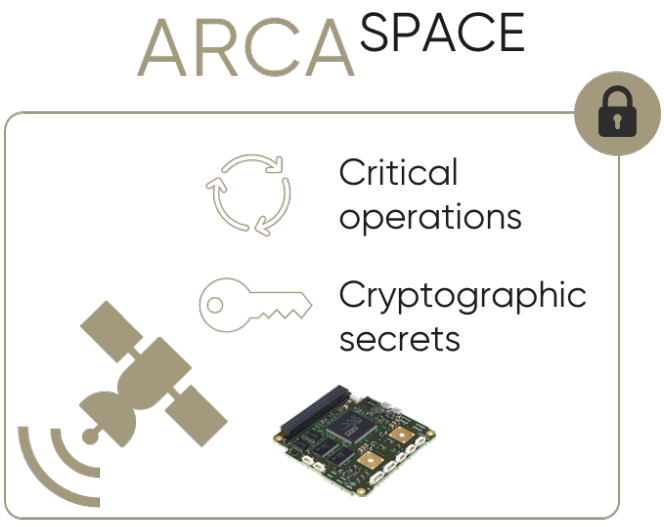

Figure 18: Illustration of ARCA^{SPACE}

The main functionalities of ARCA^{SPACE} include:

Features	***ARCA^{SPACE}***
Complements ARCA on ground by providing a RoT on board	✓
Software or hardware-based storage of secrets and provisioning of certificates	✓
Secure access control and key injection before launch	✓
Secure attestation of ARCASPACE and trusted identity	✓
Extensive library featuring standard cryptographic operations	✓
Trusted key lifecycle management via in-orbit reconfiguration	✓
Software executed in a trusted environment	✓
Support for multiple applications running in fully isolated containerized environment	✓
Post-quantum resilient cryptographic services	✓
Space-qualified software and hardware components	✓

By storing sensitive data and executing critical applications in a TEE on board the satellite, ARCA^{SPACE} will create a secure end-to-end communication channel between the ground and the satellite, guaranteeing the confidentiality, integrity and availability of the transmitted data.

5 USE CASES

5.1 SECURE TELEMETRY AND TELECOMMAND

When discussing cybersecurity for space operations, the primary risk is a satellite being hacked. Hacking a satellite may not be as difficult as expected.

There are many research papers and conferences that have documented such attacks noted in Section 6 of this paper.

In this document, we have described several ways in which an operator could lose control of a satellite, for example by sending malicious telecommands (TC). In order to prevent these scenarios, we have outlined the process and key concepts for establishing a secure-by-design communication link.

Although each mission has its own threat model and constraints, CYSEC's goal in developing ARCA and ARCA^{SPACE} was to provide a highly compatible and pragmatic way to protect the communication channel between the MCC and the satellite.

This is done by running the MCS inside the ARCA enclave where all cryptographic operations—such as encryption of the TMTC data and authentication of the MCC and satellite—are performed with their associated secrets generated and stored in a hardware RoT. Figure 19 illustrates the end-to-end secure satcom link created by ARCA and ARCA^{SPACE}.

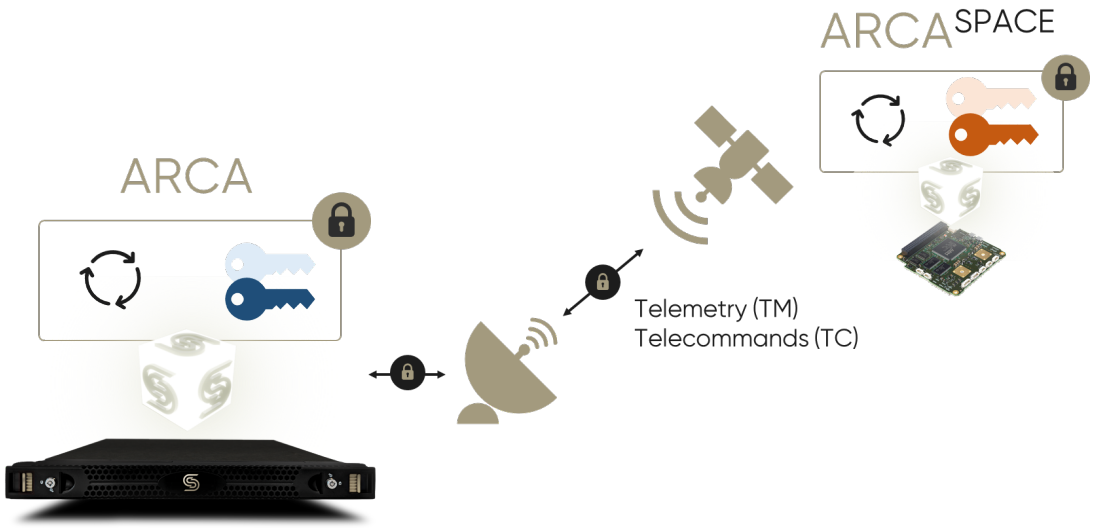

Figure 19: Illustration of end-to-end secure satellite communication link

The equivalent operations (decryption, encryption, authentication, etc.) are performed on board with ARCA^{SPACE}, which also integrates a hardware RoT with secrets that have been securely injected on board before launch.

This general concept can be applied to all exchanges of data between the ground and the satellite as described in the next sections for different use cases.

5.2 PAYLOAD DATA DOWNLINK

Besides securing TMTC data, the second most popular request from operators, (which comes from their own customers) is to secure the downlink of the payload data.

Payload data often comes down on a separate channel than TMTC data for bandwidth reasons. Think of a high-definition camera which requires downloading its images as frequently as possible. The requirements for the link are very different from the lightweight TMTC data.

However, the same basic principles apply in terms of security. Ideally, all cryptographic operations are performed on the payload itself, independent of the main OBC with secrets that have been injected on ground and that are known and managed exclusively by the end user.

This approach is called zero trust and is gaining popularity, especially in cases where the platform is shared with payloads owned by different organizations.

Encrypted data is then sent down through the communication channel all the way to the payload control center, which uses ARCA to perform any security operations—such as secure storage—or to package them in order to benefit from public cloud services (e.g. data analytics).

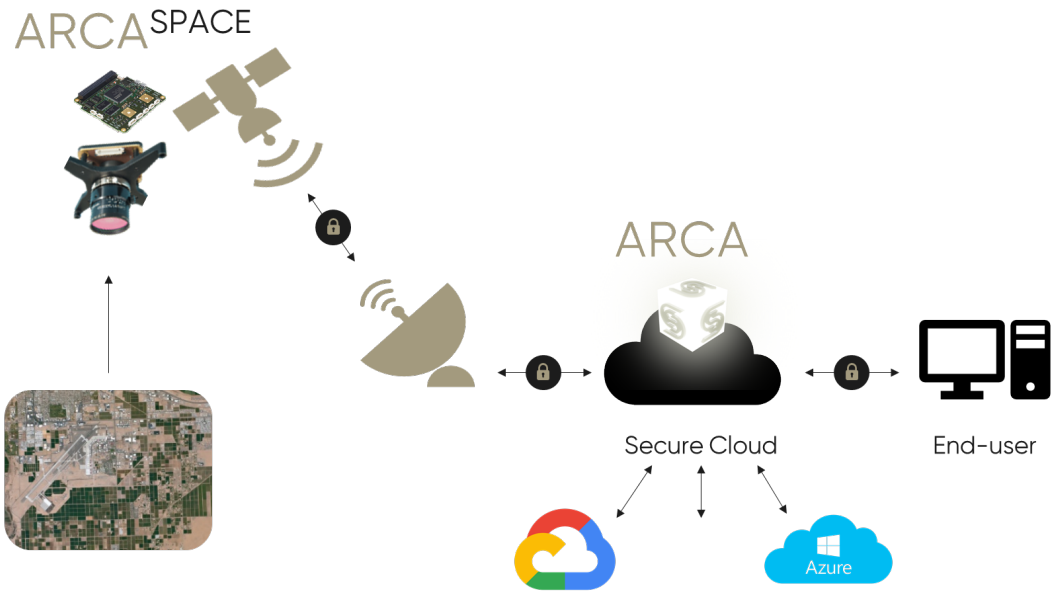

Figure 20: Illustration of end-to-end security for payload data downlink

This approach allows the end user to have full control over its data while being able to securely leverage the services offered by public cloud providers.

5.3 IN-ORBIT RECONFIGURATION

Following the natural evolution of edge devices, satellites are becoming smarter and more connected.

They are now capable of quickly changing their configuration in orbit to better accommodate market changes or customer requests, thus shortening and maximizing the return on investment for the operator.

One way to achieve that goal is by being able to reconfigure the software executed on board while in orbit. As one can imagine, this is a very attractive functionality, but it comes at the expense of greater cyber risks related to the integrity, confidentiality and availability of the transmitted data.

Using asymmetric cryptography in a PKI can provide a secure and reliable reconfiguration solution, in particular for satellite constellations. One approach to implementing a PKI is using ARCA to host the CA and ARCA^{SPACE} to securely store the satellite's public and private keys.

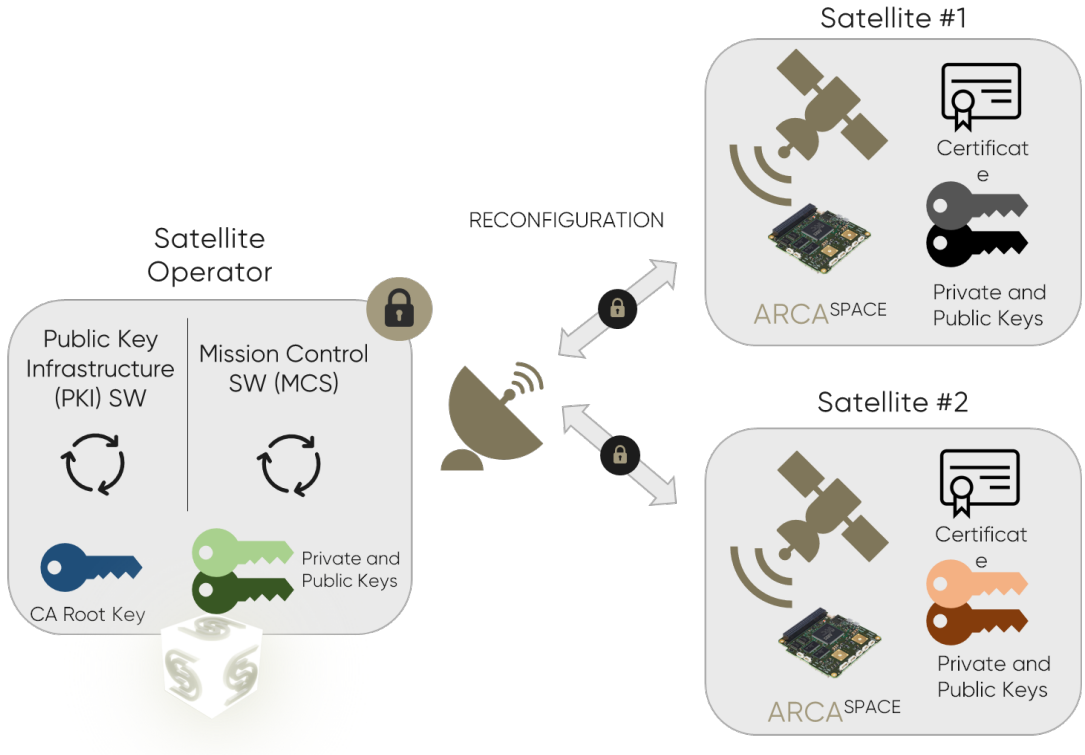

Figure 21: Illustration of a public key infrastructure for in-orbit reconfiguration

The reconfiguration process follows these steps:

1 First, the satellite generates a certificate signing request (CSR) and sends it to the CA. The CSR is a lightweight, non-signed certificate containing the requester's public key and identity information.

2 The CA checks and authenticates the request and signs the CSR, issuing the satellite's certificate that is sent as a reply to the request. The certificate is then stored on board the satellite. This certificate will authenticate the satellite for mission control.

3 Now that the satellite has been authenticated, preventing man-in-the-middle attacks (MITM), the MCC can use the satellite's public key to encrypt the data—e.g., a new version of the OBC software for in-orbit reconfiguration.

4 Once the satellite receives the encrypted packet, it is decrypted using the satellite's private key. The satellite's private key was injected securely on ground before launch following a strict key generation and management process.

The satellite can then decrypt the message and execute the command.

The main advantage of having a CA managing the PKI of a network is that any already existing node (i.e. any previously manufactured small satellite already sent to space) does not need to know the newcomer's public key to authenticate the communication. Instead, only the digital certificate is needed, which can be requested directly from the CA through a secure channel and does not depend on the specific node.

Furthermore, the fact that the digital certificate contains information about the new small satellite removes the burden of needing to remember the link between the new satellite's public key and its identity. The CA is also often in charge of providing a certificate revocation list (CRL). A CRL is a list of revoked certificates that should no longer be trusted by the nodes, allowing for more dynamic trust in the network. Among the most commonly used certificates is X.509, which is a standard in internet communications.

5.4 SATELLITE AS A SERVICE

New and innovative players in the space industry have started offering the ability for clients to share a platform by bringing their own payload and saving them the time and expense of developing, launching and operating their own satellite.

This trend is known as "Satellite as a Service".

Similar to in-orbit reconfiguration, Satellite as a Service has an attractive value proposition that comes at the expense of greater cyber risks. Not only does it carry all the risks associated with standard satellite operations but also the risks associated with payload data downlink and in-orbit reconfiguration.

In addition, platform sharing requires the on-board ability to isolate the secrets and the software used by each specific payload and customer.

Both ARCA and ARCA^{SPACE} have the ability to run fully isolated software with secrets in a dedicated hardware RoT, thus mitigating the risks related to platform sharing and offering the possibility for the operator to provide a zero trust approach to its customers.

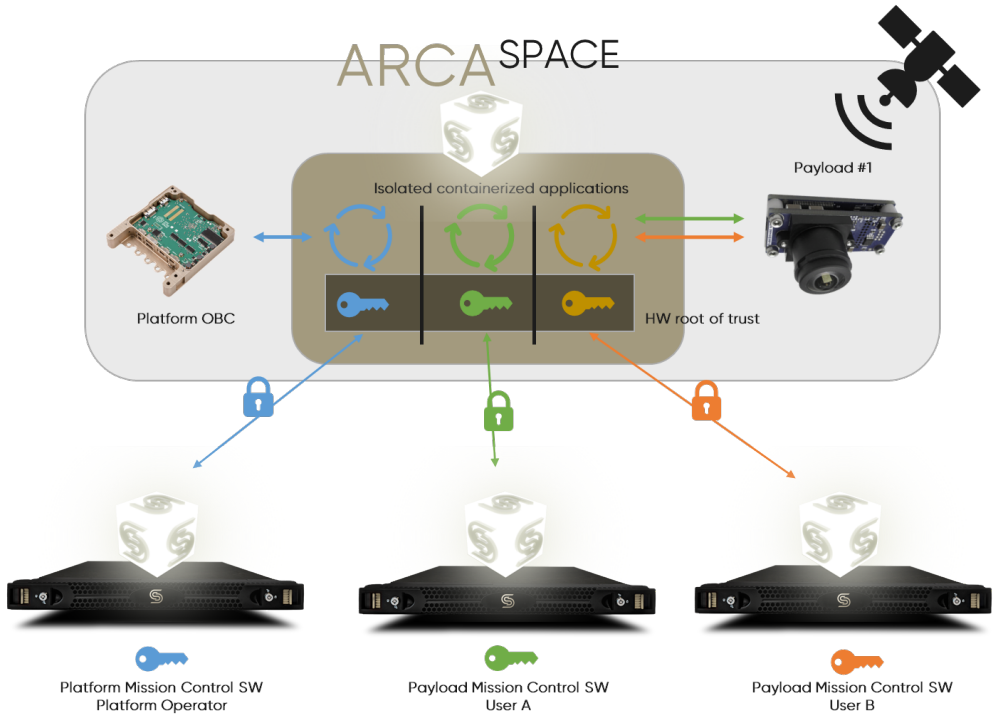

Figure 22: Illustration of secure platform sharing

5.5 GROUND SEGMENT AS A SERVICE

Operating space assets requires a complex architecture with a large attack surface as illustrated in Figure 2.

Although the MCC and MCS constitute prime targets on ground, the network of ground stations responsible for sending and receiving radio signals to the satellite and the interfaces between the MCS and the GSN (Ground Station Network) can also be considered a critical piece of the puzzle.

Indeed, various types of attacks can be conducted at the ground station level to eavesdrop information and disturb or interrupt communications.

Coincidently with the NewSpace (r)evolution, a new model of Ground Segment as a Service (GSaaS) has emerged, avoiding the

hassle and cost of operators building their own antennas[6]. However, the benefits of the "as a service" model come at the expense of delegating the trust to a third party, which can be problematic depending on the threat model of the mission, the actual architecture of the GSaaS and the interaction level between MCS and GSaaS.

As a pragmatic solution to this issue, CYSEC partnered with LEAF Space[7], an Italian GSaaS company, to allow satellite operators to have end-to-end control over the cloud engine behind the ground station network infrastructure.

The proposed concept takes advantage of ARCA's ability to run several applications in parallel in a private cloud, thus ensuring the control and security of the software as well as the secrets.

Figure 23 below illustrates both the MCS and the GSaaS cloud engine running in ARCA.

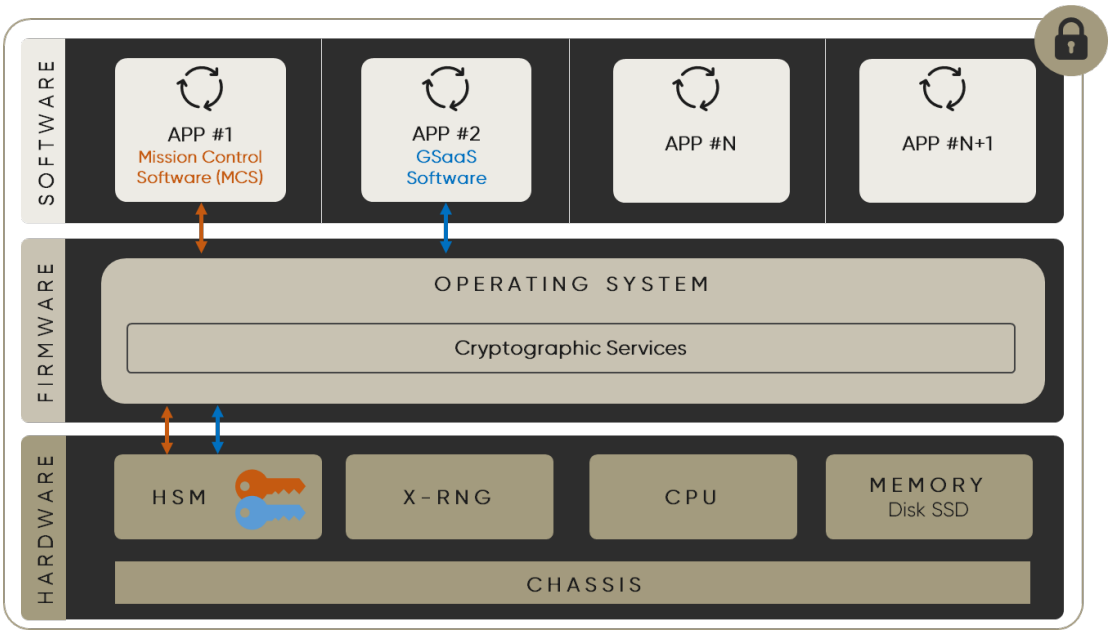

Figure 23: Combining the MCS with the ground station cloud engine in ARCA

[6] https://p.iafastro.directory/download/congress/IAC-20/files/IAC-20/B6/1/IAC-20,B6,1,5,x60462.pdf

[7] https://cysec.com/2020/08/03/cysec-and-leaf-space-partner-to-offer-end-to-end-cyber-security-protection-for-satellite-communications/

6 REFERENCES AND USEFUL LINKS

Standards

Year	Title	Link
2015	Space Data Link Security Protocol	https://public.ccsds.org/Pubs/355x0b1.pdf
2018	Space Data Link Security Protocol – Summary of Concept and Rationale	https://public.ccsds.org/Pubs/350x5g1.pdf
2019	CCSDS Standards	https://public.ccsds.org/Pubs/352x0b2.pdf
2020	Space Data Link Security Protocol – Extended Procedures	https://public.ccsds.org/Pubs/355x1b1.pdf
2016	IMA Separation Kernel Qualification - preparation	http://www.esa.int/Enabling_Support/Space_Engineering_Technology/Shaping_the_Future/IMA_Separation_Kernel_Qualification_-_preparation

Industry reports

Year	Title	Link
2019	The future of the European space sector	https://www.eib.org/attachments/thematic/future_of_european_space_sector_en.pdf
2019	Main trends and challenges in the space sector	https://www.pwc.fr/fr/assets/files/pdf/2019/06/fr-pwc-main-trends-and-challenges-in-the-space-sector.pdf
2016	Space security for Europe	https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/Report_29_Space_and_Security_online.pdf
2015	Handbook of Space Security	https://www.springer.com/la/book/9781461420286
2018	Cyber Security - High Stakes for the Space Sector	https://espi.or.at/news/espi-brief-26-cyber-security-high-stakes-for-the-space-sector
2018	Cybersecurity of Space Missions	https://eisc-europa.eu/images/stories/2018/Workshop/Final_upload/EISC_Presentations/Cybersecurity_-_Jean_Muylaert_and_Luca_del_Monte.pdf
2018	Security in Outer Space: Rising Stakes for Civilian Space Programs	https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwik2emcwcXhAhUPyYUKHdNWDigQFjAAegQIBRAC&url=https%3A%2F%2Fespi.or.at%2Fcomponent%2Fjdownloads%2Fsend%2F58-presentations%2F389-14-rob-heron-security-in-outer-space-rising-stakes-for-civilian-space-programs&usg=AOvVaw1wgGdONE7H0kcylfn9YyzY
2016	ESA Space Capabilities for Space Security	https://eisc-europa.eu/images/stories/2016q1/2016EISC_Workshop_Presentations/04_Giannopapa.pdf
2018	Job One for Space Force: Space Asset Cybersecurity	https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf
2018	ESA facing Cyber security issues	http://www.eu-space.eu/images/2018/document/Slides/Slides-Ferrazzani-Zilioli.pdf

2018	Cloud Computing via Satellite	https://www.nsr.com/wp-content/uploads/2018/11/NSR-White-Paper-Cloud-Computing-via-Satellite-November-2018-1.pdf?utm_source=Satellite%20and%20all%20NSR%20News&utm_campaign=202b3868f4-EMAIL_CAMPAIGN_2018_07_23_09_12_COPY_01&utm_medium=email&utm_term=0_ff2c5c9f7f-202b3868f4-

Research papers

Year	Title	Link
2015	Satellite Hacking, a guide for the perplexed	https://www.slideshare.net/chlick420/satellite-hacking
2017	Exploring a Novel Cryptographic Solution for Securing Small Satellite Communications	http://ijns.femto.com.tw/contents/ijns-v20-n5/ijns-2018-v20-n5-p988-997.pdf
2018	A secure authentication with key agreement scheme using ECC for satellite communication systems	https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.1279
2014	Trust Management Approach to Satellite System Telecommanding Security	https://arc.aiaa.org/doi/10.2514/1.I010025
2017	Modeling and Practice of Satellite Communication Systems Using Physical Layer Security: A Survey	https://ieeexplore.ieee.org/document/8005916
2016	Architecting Information Security Services for Federated Satellite Systems	https://arc.aiaa.org/doi/10.2514/1.I010425
2017	SpaceTEE: Secure and Tamper-Proof Computing in Space using CubeSats	https://arxiv.org/pdf/1710.01430.pdf
2019	Developing and Securing Software for Small Space Systems - PhD	https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=8675&context=etd
2017	Design for security: Guidelines for efficient, secure small satellite computation	https://ieeexplore.ieee.org/document/8059081
2016	Space, the Final Frontier for Cybersecurity?	https://www.semanticscholar.org/paper/Space%2C-the-Final-Frontier-for-Cybersecurity-Dsc-Lewis/086b9d0d86b85d1dcd564390c6d49c06d17c7239
2019	Ensuring Cybersecure Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions	https://www.semanticscholar.org/paper/Ensuring-Cybersecure-Telemetry-and-Telecommand-in-Saha-Rahman/352e8f6cbee9d00fe0748257e516aa90e4da2dd3
2013	Research of centralized multicast key management for LEO satellite networks	https://www.researchgate.net/publication/271483552_Research_of_centralized_multicast_key_management_for_LEO_satellite_networks
2014	Integration and verification of a keyed-hash message authentication scheme based on broadcast timestamps for NUTS	https://core.ac.uk/download/pdf/52107488.pdf
2018	Design of Small Trusted Hardware for Space Applications	https://arc.aiaa.org/doi/abs/10.2514/6.2018-5335

Year	Title	Link
2020	Insecure satellite Internet is threatening ship and plane safety	https://arstechnica.com/information-technology/2020/08/insecure-satellite-internet-is-threatening-ship-and-plane-safety/
2020	CubeSat Communications: Recent Advances and Future Challenges	https://arxiv.org/pdf/1908.09501.pdf
2018	Design and Implementation of a Security Processor for Satellite Communication Systems	https://www.researchgate.net/publication/323870851_Design_and_Implementation_of_a_Security_Processor_for_Satellite_Communication_Systems
2017	Exploring a Novel Cryptographic Solution for Securing Small Satellite Communications	http://ijns.jalaxy.com.tw/contents/ijns-v20-n5/ijns-2018-v20-n5-p988-997.pdf

Research groups

Year	Title	Link
-	Secure Small Satellite Processing Platform	https://www.ll.mit.edu/r-d/projects/secure-small-satellite-processing-platform
-	Communicative Systems Laboratory	https://wwwfr.uni.lu/recherche/fstm/communicative_systems_laboratory_com_sys/research
-	Orbital Security Alliance	https://www.orbitalsecurity.space/about
-	IQM Research Institute	http://www.michman.org/resources/Documents/3%20Dudzik%20-%20Smallsat%20Cyber%20Security%20Presentation.pdf

Conferences

Year	Title	Link
2020	CyberSat Summit	https://www.cybersatsummit.com/
2020	Hack-A-Sat	https://www.hackasat.com/ https://github.com/deptofdefense/hack-a-sat-library
2021	CYSAT	https://cysat.ch/

Online articles & blogs

Year	Title	Link
2020	Let's not make Newspace a paradise for hackers	https://spacewatch.global/2020/10/spacewatchgl-opinion-lets-not-make-newspace-a-paradise-for-hackers/
2020	Securing Space 4.0 – One Small Step or a Giant Leap? Part 1	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/securing-space-4-0-one-small-step-or-a-giant-leap-part-1/
2020	Securing Space 4.0 – One Small Step or a Giant Leap? Part 2	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/securing-space-4-0-one-small-step-or-a-giant-leap-part-2/
2019	Op-ed | Protecting low Earth orbit from becoming the new Wild West	https://spacenews.com/op-ed-protecting-low-earth-orbit-from-becoming-the-new-wild-west/

2020	Why Satellite Cybersecurity Must Be Prioritized in the New Frontier	https://www.nextgov.com/ideas/2020/05/why-satellite-cybersecurity-must-be-prioritized-new-frontier/164977/
2020	Securing the final frontier: Why space systems need cybersecurity too	https://www.kaspersky.com/blog/secure-futures-magazine/cybersecurity-space-exploration/31581/
2020	A Space Cybersecurity Approach	https://www.globalsecuritymag.com/A-Space-Cybersecurity-Approach,20200924,103102.html
2020	How the International Space Station Enables Cybersecurity	https://www.infosecurity-magazine.com/news/international-space-station/
2020	Cybersecurity Threats in Space: A Roadmap for Future Policy	https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy
2020	US issues fifth Space Policy Directive on space cybersecurity	https://spacewatch.global/2020/09/us-issues-fifth-space-policy-directive-on-space-cybersecurity/
2020	Dedicated website with all news regarding cybersecurity and space	https://www.spacesecurity.info/

Online articles on satellite hacking

Year	Title	Link
2019	RSA Conference 2019: The Sky's the Limit for Satellite Hacks	https://threatpost.com/rsa-conference-2019-the-skys-the-limit-for-satellite-hacks/142541/
2019	Hacking Satellites Is Surprisingly Simple	https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think
2014	Chinese hack U.S. weather systems, satellite network	https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?noredirect=on&utm_term=.40fc67829127
2020	Why Satellite Hacking Has Become The 'Biggest Global Threat'	https://eurasiantimes.com/why-satellite-hacking-has-become-the-biggest-global-threat-for-countries-like-us-china-russia-india/
2020	Hackers could shut down satellites – or turn them into weapons	https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932
2020	Hacking satellite internet connections is a lot easier than you'd think	https://www.techradar.com/news/hacking-satellite-internet-connections-is-a-lot-easier-than-youd-think
2020	Hacker Used £270 of TV Equipment to Eavesdrop on Sensitive Satellite Communications	https://www.cbronline.com/news/satellite-hacking

7 ACRONYMS

8 Tag	Description
AES	Advanced Encryption Standard
B2G	Business to Government
CA	Certificate Authority
CapEx	Capital Expenditure
CCC	Confidential Computing Consortium
CCSDS	Consultative Committee for Space Data Systems
CPU	Central processing Unit
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DoS	Denial of Service
FPGA	Field-Programmable Gate Array
GEO	Geostationary
GSaaS	Ground Station as a Service
GVM	Guest Virtual Machine
HSM	Hardware Security Module
HW	Hardware
IAM	Identity and Access Management
IoT	Internet of Things
ISS	International Space Station
IT	Information Technology
MCC	Mission Control Center
MCS	Mission Control Software
MCU	Microcontroller Unit
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OBC	On-Board Computer
OpEx	Operational Expenditure
OS	Operating System

8 Tag	Description
PKI	Public Key Infrastructure
RNG	Random Number Generator
RoT	Root of Trust
Satcom	Satellite Communications
SEE	Single Event Effect
SSD	Solid-State Drive
SW	Software
TEE	Trusted Execution Environment
TMTC	Telemetry and Telecommand
TTC	Tracking, Telemetry and Command
U	Rack unit
VSAT	Very Small Aperture Terminal

8 CREDITS

Dr. Mathieu Bailly
VP Confidential Edge Computing

About the Author

Dr. Mathieu Bailly is heading the Space Business Unit at CYSEC SA, a Swiss cybersecurity company based at the EPFL Innovation park in Lausanne Switzerland. At CYSEC, Mathieu oversees product and business development activities related to the “Edge”, on Earth or in space. Edge computing encompasses a wide range of fast-growing markets where cybersecurity is becoming a critical challenge.

Mathieu has spent his career in innovation management, business development and sales in high-tech industries. He holds an MSc in Materials Science from the Grenoble Institute of Technology in France and a PhD in Chemical Engineering from Queen’s University, ON, Canada.

About CYSEC

CYSEC SA is a data security company based at the EPFL Innovation Park in Lausanne, Switzerland. CYSEC brings 360° security in one click for container-based workloads and platforms through its ARCA trusted OS software. CYSEC partners with leading cybersecurity research centers to develop technological innovations in the area of Confidential Computing and delivers its cybersecurity solutions for any vertical sector. For more information, please visit www.cysec.com.

THANK YOU

CYSEC