NEWSPACE: LES ENJEUX LIES A LA SECURITE DES DONNEES

Mathieu Bailly

COMET Cyber, Toulouse, 7.11.21

D’après le Petit Robert (ou presque)

Newspace?

Ma définition:

Des services visant le profit rendus possibles grâce à l’innovation (pas QUE technologique) et des capitaux privés

Grâce à:anceurs micro, réutilisables

- Smallsats (<500kgs)
- Pas de standards
- COTS
- Constellation
- LEO
- « As a service »
- Edge + Cloud

Données?

- Payload (=client)
- TMTC
- 3 états: At rest, in transit, in use

Sécurité?

Des données:

1. Intégrité
2. Confidentialité
3. Authenticité
4. Disponibilité

- END-TO-END!!
- Aussi du code!!

Enjeux?

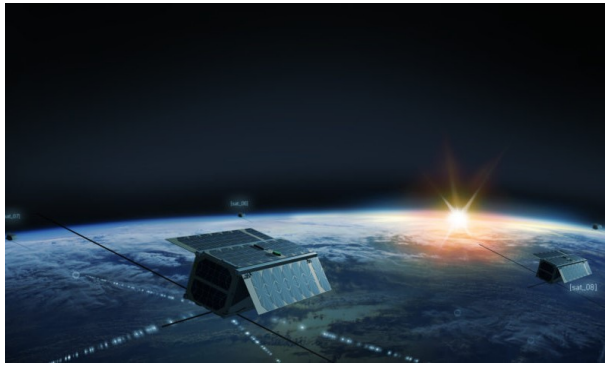
- Newspace > Oldspace!!
- Business
- Géo-politiques
- « Environnementaux »

Exemples de missions « newspace »

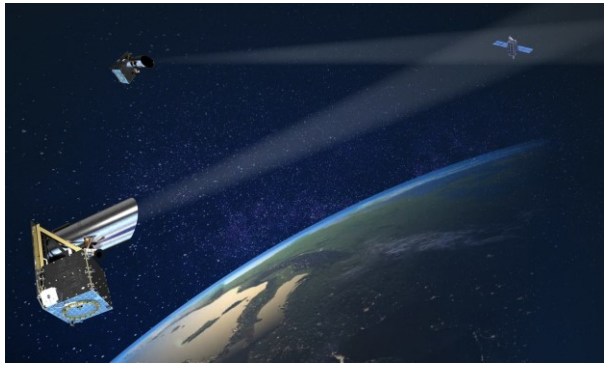
Quelles données ?

Quelle sécurité ?

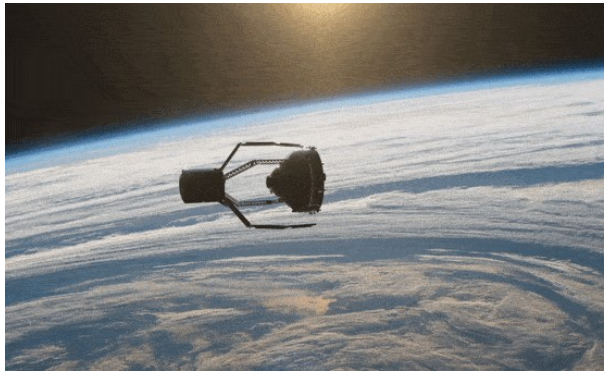
Earth Observation



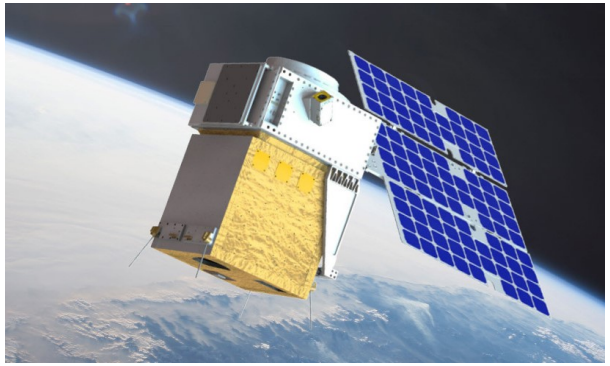
Internet of Things (IoT)



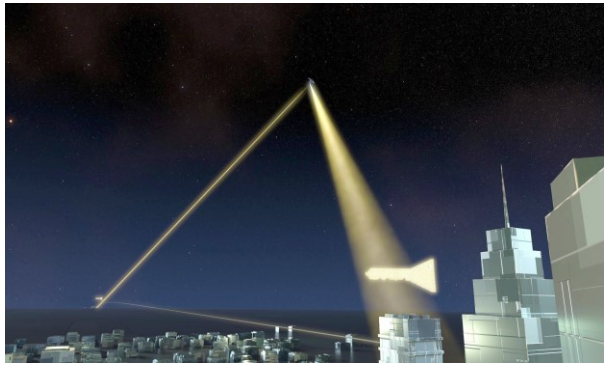
Space Situational Awareness (SSA)



De-orbiting / In-orbit servicing



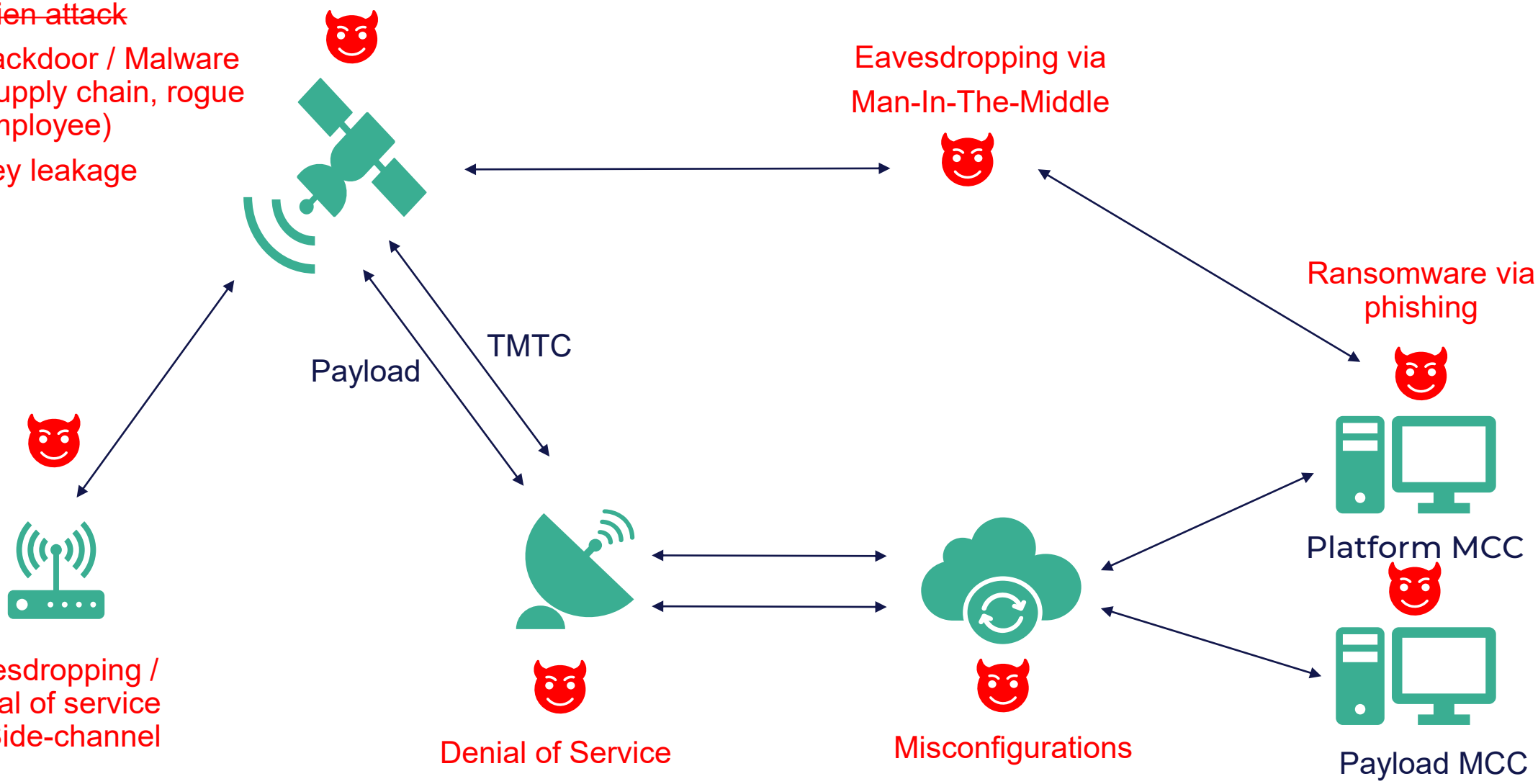
Satellite as a service



Quantum Key Distribution (QKD)

Exemples de menaces

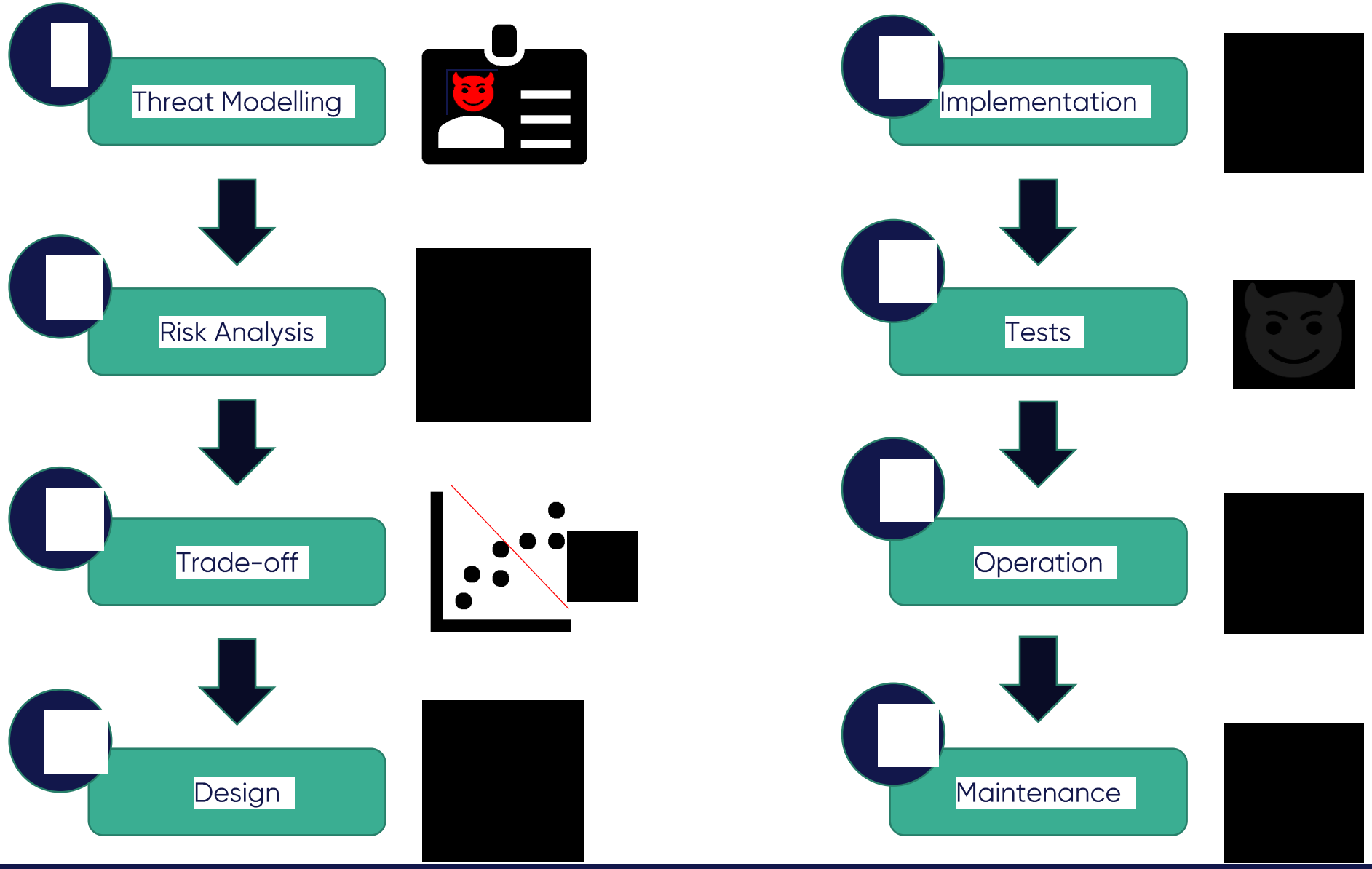
- ~~Alien attack~~
- Backdoor / Malware (supply chain, rogue employee)
- Key leakage



L’impact de l’approche newspace sur la cyber

	Positif	Negatif
Utilisation de COTS / Outils Open Source	• Effet de communauté • Security by transparency	Reverse Engineering
Smallsats = systèmes très contraints	• Connectivité limitée: plus difficile à attaquer (mois d’opportunités, plus visible) • Moins de lignes de code!	Limitations taille des clés, algos de crypto, sécurité OS, risques de fiabilité (redondance)
As a service	Plus de chances d’avoir un client concerné!	Délégation de la confiance: audits et/ou revue architecture, redondance (GSaaS)
Cloud	Nombreux outils à dispo	Expertise spécifique!
Constellation	?	• Take one take all • Automatisation
Courtes missions	• COTS plus modernes (e.g. CPU Arm TrustZone) • Agilité: Upgrades sur la generation suivante	
Software-defined	In-Orbit reconfigurations, security patches	Sécurité du code..

Approche « security by design »



Exemple d’analyse de risques

	Syste	Numb	Risk	Result	Probabil	Impac	Ta	Priorit	Mitigation Plan	Planned Result after mitigation	Due da	To be ca	robabi	Impa	Tal	Priori	Mitigation implemented and verif	Result after mitigation	Verified	robabi	Impa	Prior
2	AS	0011	Physical access to Artracart head quarter to steal data, stop the service	Spy to design data to use it to hack in the system, steal commercial secrets, stop the service	3	5	8	High	Define access control strategy, critical document storage and destruction	Only allow people can access Artracart facilities,		Maybe	2	3	5	Low						High
3	AS	0012	Remote access to Artracart IT infrastructure to steal data	Spy to design data to use it to hack in the system, steal commercial secrets	5	4	9	High	IT infrastructure security plan - Limit external access - separate networks - secure PC - educate employees -	Limited possibility to hack of Artracart IT infrastructure, and quickly identify any possible breach to avoid access to critical data		Yes	2	3	5	Low						High
4	AS	0031	Phishing / Malware attack to Artracart team to steal data	Use information to hack in the system, sell commercial secrets, stop the service	5	5	10	High	Define data security plan - data backup				2	3	5	Low						High
5	AS	0028	Site web hacked	Can learn central and what published online on Artracart	5	2	7	Medium					5	1	6	Medium						Medium
6	AS	0029	Social media accounts hack	Can learn central and what published online on Artracart	5	2	7	Medium							7	Medium						Medium
7	AS	0041	Physical loss or unwanted share of Admin data		4	3	7	Medium					2	3	5	Low						Medium
8	AS	0042	Digital loss or unwanted share of Admin data		4	3	7	Medium					3	3	6	Medium						Medium
9	AS	0050	IT infrastructure suppliers security breach	Can steal access data to Artracart system	5	5	10	High					4	2	6	Medium						High
10	AS	0054	Remote access to mail chimp and others clients data (e.g. pipe	Have access to customers/users private date	5	4	9	High							9	High						High
11	AS	0055	Hacking, steal of Credit card data	Loss of money, stop payments related to infrastructure	4	3	7	Medium					3	2	5	Low						Medium
12	AS	0056	Natural disasters (Fire flooding,...)	Loss of head quarter	1	5	6	Medium					1	5	6	Medium						Medium
13	AU	0013	Physical access to Artracart computers not in the head quarters to steal data	Spy to design data to use it to hack in the system, steal commercial secrets	3	5	8	High					3	2	5	Low						High
14	AU	0026	Remote access to Artracart remote IT infrastructure to steal data	Spy to design data to use it to hack in the system, steal commercial secrets	5	4	9	High					3	2	5	Low						High
15	AU	0052	Kidnapping or physical aggression to access Artracart data	Can have gain access to critical data, can stop the service	1	5	6	Medium							6	Medium						Medium
16	DM	0009	Physical access to the DM	Spy user data, inject fake data, stop Artracart service, steal user data, destroy SM	1	5	6	Medium					1	4	5	Low						Medium
17	DM	0010	Remote access to the DM (not via user interface)	Spy user data, inject fake data, stop Artracart service, steal user dat	5	5	10	High					2	3	5	Low						High
18	DU	0027	Hack into user account to steal data via user interface	Can steal user data or inject fake data to terminals	5	4	9	High					3	2	5	Low						High
19	DU	0028	Hack into DM to steal data or keys via user interface or stop service	Can steal all user data and keys and block service	5	5	10	High					2	2	4	Low						High
20	GD	0029	Spying on GD link	Get user data, get terminal central data, get keys	2	3	5	Low					2	3	5	Low						Low
21	GD	0030	Physical access to GS - GD link	Perturbate the system, steal data, stop data flux	1	5	6	Medium					1	3	4	Low						Medium
22	GD	0040	Hack in the DM or MOC via GD link to copy data, or take control	Can steal data, keys and control the system	3	5	8	High					2	3	5	Low						High
23	GS	0043	Ground Segment external suppliers security breach	Can steal knowledge on Artracart system	5	3	8	High					3	3	6	Medium						High
24	GS	0005	Physical access to the ground segment (mission central room)	Loss of the Artracart system	2	5	7	Medium					2	2	4	Low						Medium
25	GS	0006	Remote access to the ground segment (mission central room)	Loss of the Artracart system control	5	5	10	High					3	2	5	Low						High
26	GS	0007	Physical access to the ground segment (ground stations)	Can take control over a satellite, spy on the data, reduce satellite/GS contacts, inject fake data on Artracart system, destroy	2	5	7	Medium					2	2	4	Low						Medium
27	GS	0008	Remote access to the ground segment (One ground station)	Can spy on the data, reduce satellite/GS contacts, inject fake data on Artracart system, destroy	5	3	8	High	Ensure that the GS has limited remote access and data are encrypted				3	2	5	Low						High
28	MA	0045	Key theft during manufacturing/theft of products		3	4	7	Medium							7	Medium						Medium
29	MA	0046	Terminal theft during manufacturing/testing		2	3	5	Low							5	Low						Low
30	MA	0047	Terminal hacking during manufacturing/testing		3	4	7	Medium							7	Medium						Medium
31	MA	0051	Terminal suppliers security breach	Can add backdoor to user data	5	4	9	High							9	High						High
32	RD	0048	Key theft during R&D phase		5	4	9	High							9	High						High
33	SG	0024	Spy on the UL data to steal user data or satellite commands	Get user data, get keys, get satellite central data	2	4	6	Medium	UL is encrypted, GS has narrow pointing and nea	Very hard to get the data, that would be unusable		Yes	1	2	3	Low						Medium
34	SG	0025	Spy on the DL data to steal the user data or satellite telemetry	Get user data, get satellite data	3	4	7	Medium	DL is encrypted, user data fragmented	Very hard to get the data, that would be unusable		Yes	2	2	4	Low						Medium
35	SG	0034	Try to inject real fake data on the UL data	Disturb operations, get in central of the satellite, send fake message to terminals	2	5	7	Medium	Secure link			Yes	2	2	4	Low						Medium
36	SG	0035	Try to inject real fake data on the DL data	Disturb operations, inject fake user data	2	4	6	Medium	Secure link			Yes	2	2	4	Low						Medium
37	SG	0026	Remote access to take control the satellite once launched	Loss of satellite or malicious software injected that can infect the rest of the system	2	5	7	Medium	Secure link, contingency plan			Yes	1	3	4	Low						Medium
38	SG	0032	Inject random data on the UL channel	Can saturate satellite receiver disturbing operations	2	3	5	Low	Coordination with local OFCOM to quickly react in case of interference	reduce interference time			2	3	5	Low						Low
39	SG	0033	Inject random data on the DL channel	Can saturate ground receiver disturbing operations	2	3	5	Low	Coordination with local OFCOM to quickly react in case of interference	reduce interference time			2	3	5	Low						Low
40	SS	0049	Space Segment external suppliers security breach	Can steal knowledge on Artracart system	5	5	10	High							10	High						High
									Secure all the communication links													

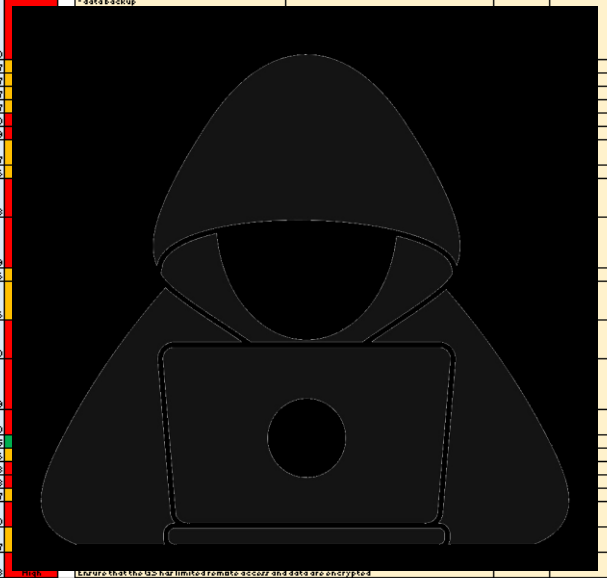
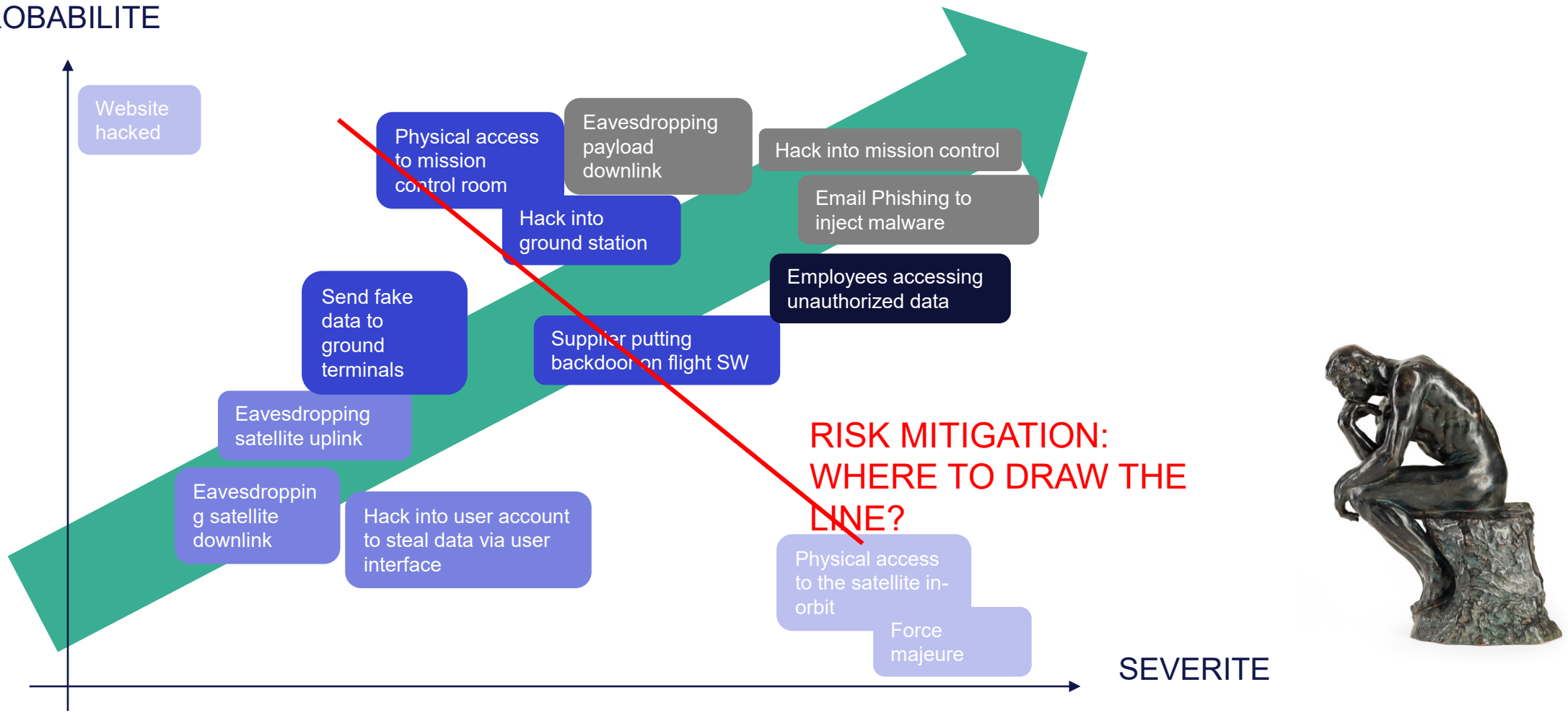


Illustration de trade-off



Quelques recommendations

Approche “Security by design”

- Algorithmes crypto selon le besoin
- Que du standard!

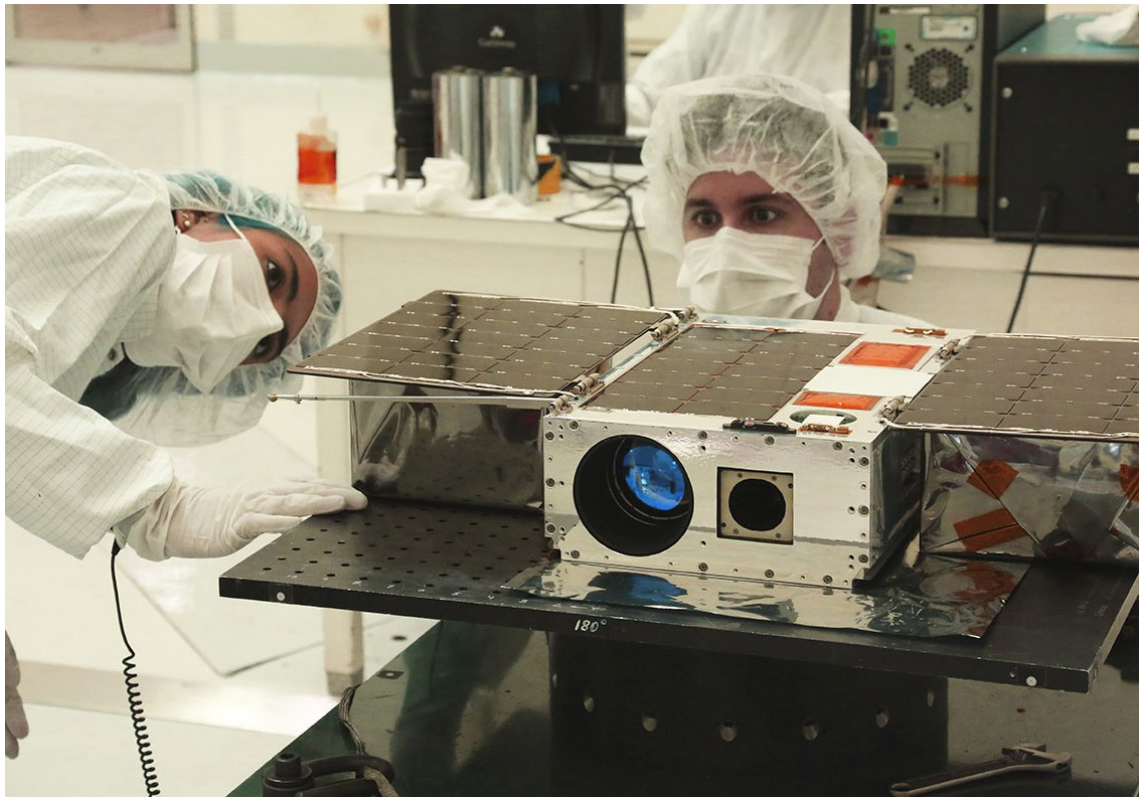
Secrets: HW / SW implementation est critique pour tout le lifecycle (generation, stockage, injection, revocation, mise à jour, etc)

Root of trust: HW est idéal

Equilibration sol - bord

Notre retour d’expérience depuis 2019

- **Sous estimation** globale du risque cyber
- Absence de **démarche sécurité** : saute direct à l’implémentation
- **Obsession pour le chiffrement** au détriment de l’authentification
- **Dilemme du « Develop vs buy »** : Exemple typique d’un KMS
- **Dilemme fiabilité vs sécurité**: ex option de désactiver le chiffrement / authentification, canal de secours ouvert et non protégé, etc
- Méconnaissance des bonnes pratiques de **gestion de clés**



ARCA Space: protéger les données de bout-en-bout

ARCA EMBEDDED

Flight Software

ARCA

Mission Control Software

TMTC & Payload data

ARCA Embedded intégré dans ION

SECOND EDITION

CYSAT

PARIS 2022

www.cysat.eu

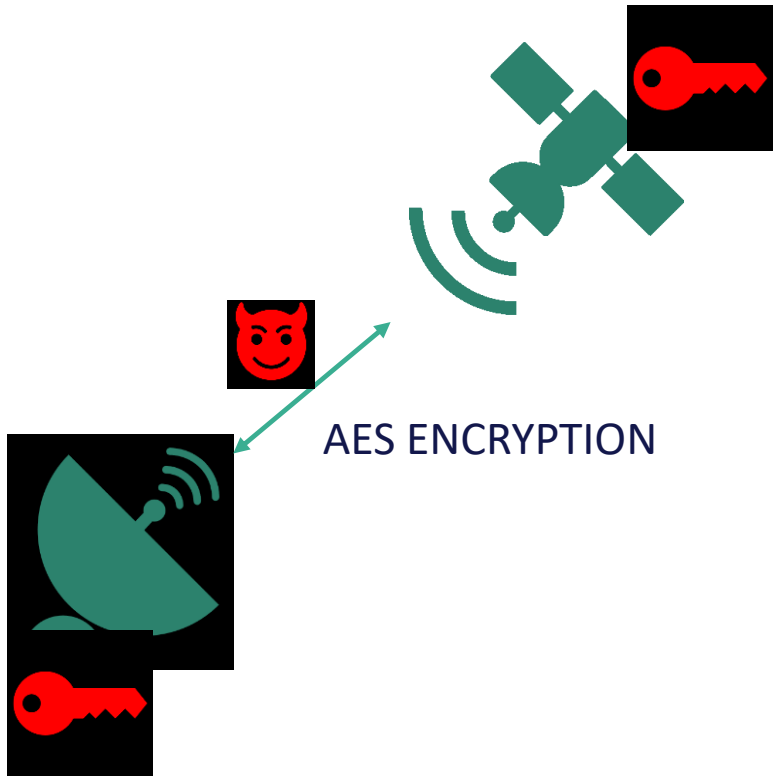
MERCI

CYSEC SA
Lausanne, Toulouse, Paris

Mathieu Bailly
Mathieu.bailly@cysec.com

Although widely used today by operators, AES encryption is insufficient for security-critical operations

Operation	Main risks	Root Causes
Sending uplink commands	Commands can be altered / modified by an attacker then taking remote control of spacecraft	• AES is a symmetric encryption algorithm which means **the same keys are used on ground and on board** →All risks originate from the leakage of AES keys → In case of breach, there is no way to notice it and no way to go back to nominal trust level • Keys used for the MCS can get compromised on ground e.g. due to poor MCC protection • Keys used on board can get comprised on the ground during all steps before launch e.g due to unsecure practices for key exchange, key handling, key injection, etc
Sending payload downlink data	Eavesdropping AND tampering of payload data downlink	
In-orbit software reconfiguration	Upload of faulty / malicious software to take control of satellite	



Hacking a satellite may NOT be that hard

For hackers, space is the final frontier

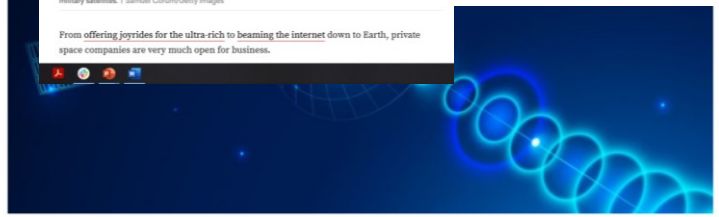
As the commercial space industry heats up, security experts worr cyberattacks.

By Rebecca Heilweil | Jul 29, 2021, 7:00am EDT

SHARE

The Space Force, a military branch created during the Trump administration, is in charge of running military satellites. | Samuel Corum/Getty Images

From offering joyrides for the ultra-rich to beaming the internet down to Earth, private space companies are very much open for business.



The EurAsian Times

Tuesday, May 18, 2021

WORLD AMERICAS ASIA PACIFIC EURASIAN REGION EUROPE MIDDLE EAST SOUTH ASIA

Home

Why Satellite Hacking Has Become The 'Biggest Global Threat' For Countries Like US, China, Russia & India?

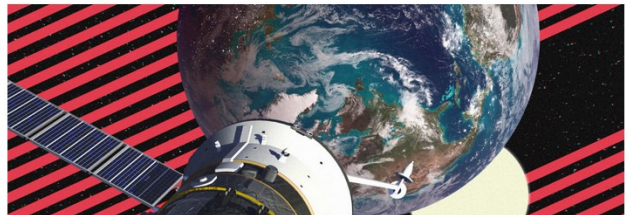
By Younis Dar | October 24, 2020

The US Air Force in April this year organised a hackathon to test the vulnerabilities of its military satellites in orbit. The competitors were asked to hack into an actual US satellite orbiting the earth, during Defcon, one of the world's largest hacker conferences.

02-15-20

What happens when all the tiny satellites we're shooting into space get hacked?

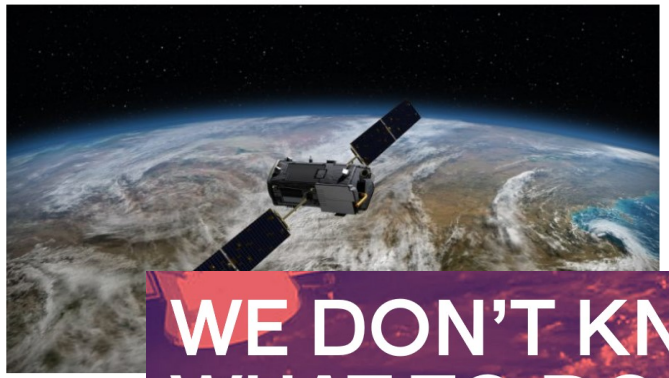
Hackers could shut them down—or turn them into weapons.



Hacking Satellites Is Surprisingly Simple

By Ryan Whitwam on March 8, 2019 at 1:02 pm | 13 Comments

274 SHARES



Satellites are physic
power antennas ma
started taking cybe

#smallsat2018 – Small satellite hacking real threat, encryption needed

BY DOUG MOHNEY AUGUST 13, 2018

HOT TOPICS, NATIONAL SECURITY LEAVE A COMMENT

Last week, academic researchers from the satellite world – not Black Hat or DEFCON – said small satellites with propulsion

Satellite Hacking Is a Real Thing and It Presents a Real Threat to Our Security

By Foley November 26, 2018 News English 0

uld happen if all satellites suddenly just stopped working?
above our heads, and some people still don't believe they

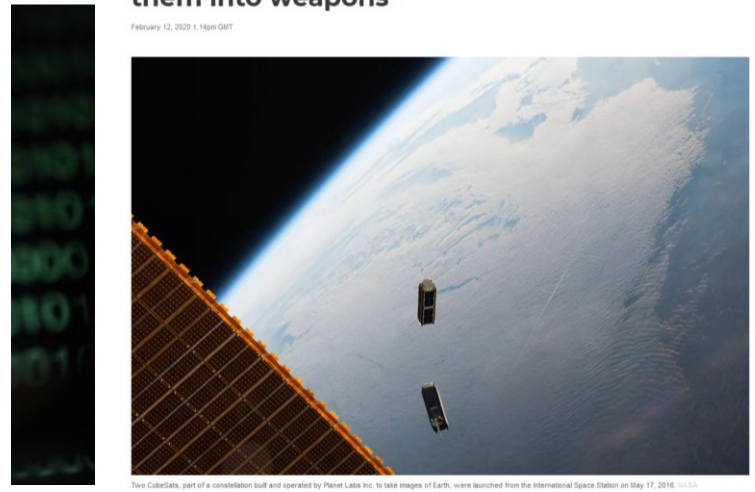
China-based campaign breached satellite, defense companies: Symantec

Joseph Menn 4 MIN READ

SAN FRANCISCO (Reuters) - A sophisticated hacking campaign launched from computers in China burrowed deeply into satellite operators, defense contractors and telecommunications companies in the United States and southeast Asia, security resea

Hackers could shut down satellites – or turn them into weapons

February 12, 2020 1.14pm GMT



Two CubeSats, part of a constellation built and operated by Planet Labs Inc. to take images of Earth, were launched from the International Space Station on May 17, 2016. NASA

Email

Last month, SpaceX became the operator of the world's largest active satellite

WE DON'T KNOW WHAT TO DO IF A SATELLITE GETS HACKED

It's about to get very crowded up there, and cyberattacks pose a bigger threat than ever.

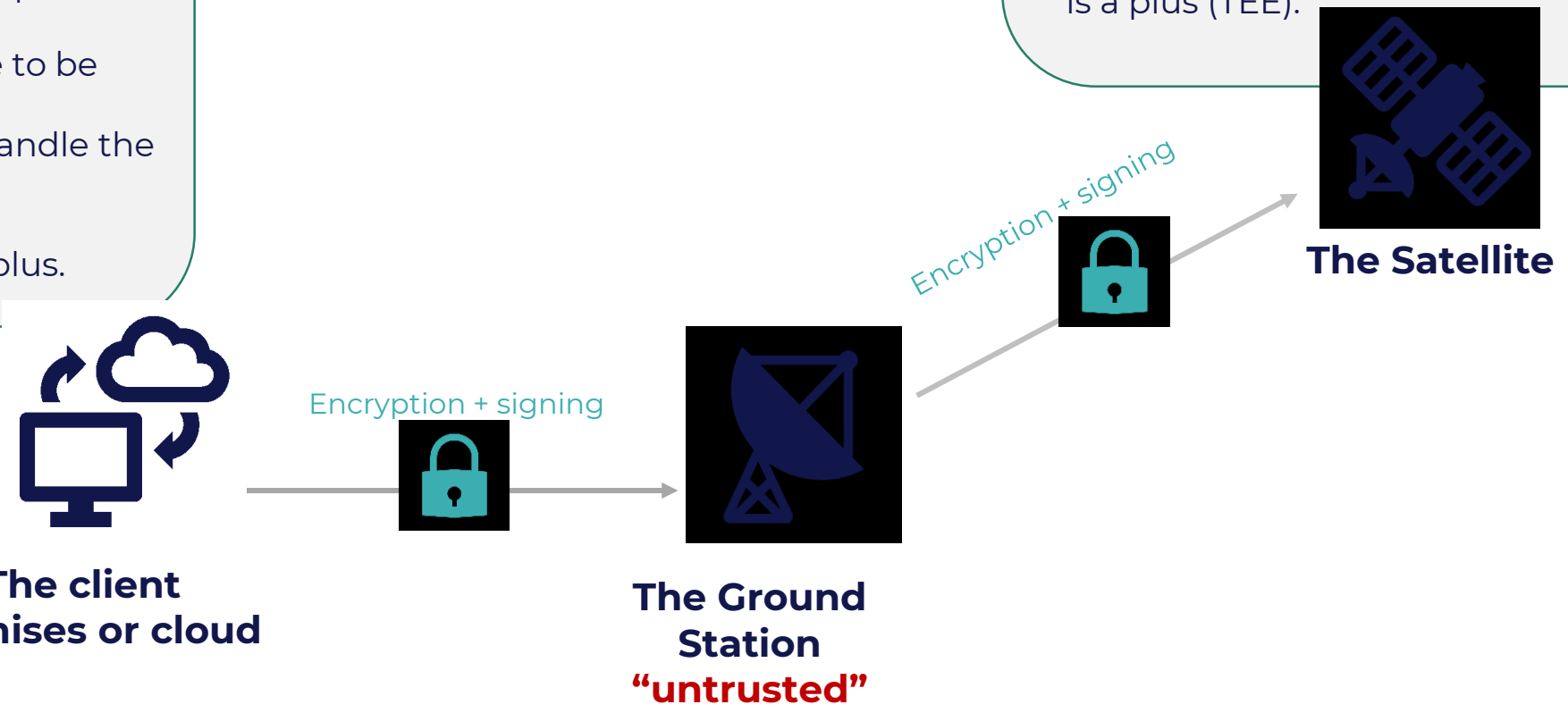
End-to-end security with Trusted Execution Environments (TEEs)

CYSEC ARCA

- The mission control software should run on a TEE / secure enclave to protect it from all the entry points.
- Enforce MFA.
- Authentication of the code to be executed.
- Cryptographic service to handle the cryptographic operations.
- Hardware root of trust.
- DevOps compatibility is a plus.

CYSEC ARCA *Embedded*

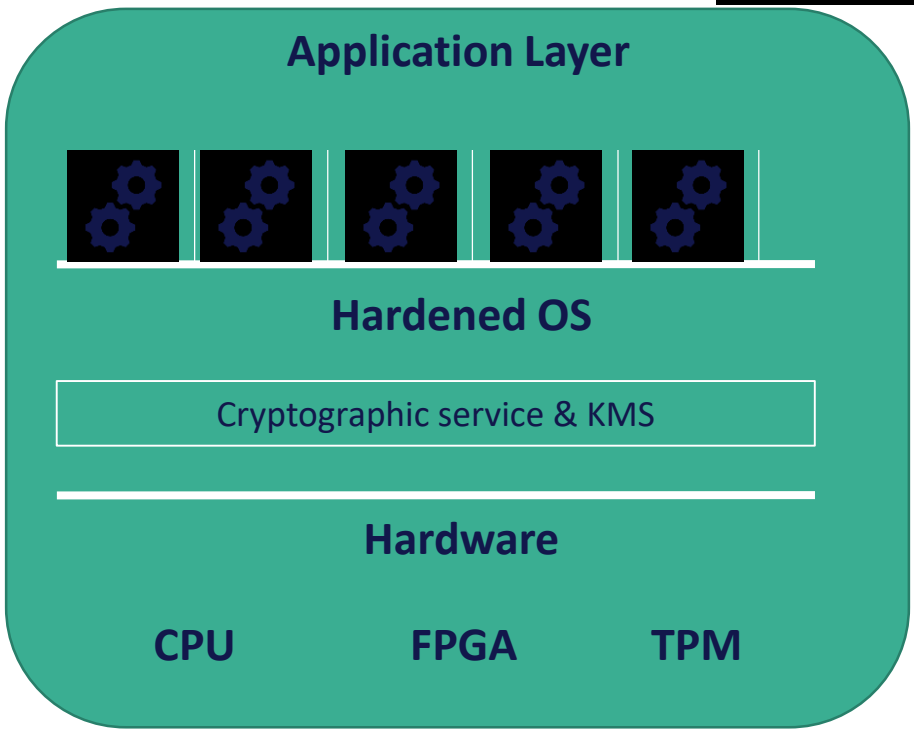
- Authentication and decryption of uplink data.
- Signing and encryption of downlink data.
- Authentication of the code to be executed.
- Hardware root of trust.
- Secure data processing on-board is a plus (TEE).



ARCA Embedded:
Towards confidential computing on board

ARCA Embedded combines:

- The security of a **hardened OS** with full memory encryption , read-only system images and a secure boot
- The ability to run **containerized applications** providing full isolation on board
- The convenience of a built-in **cryptographic service** and **Key Management System** accessible via a simple API
- The possibility to implement a **hardware cryptographic backend** with certified TPMs



ARCA Embedded implementation:
Option 1: on CYSEC secure OBC

- **Xilinx Zynq UltraScale+ MPSoCs** with 64-bit ARM Cortex-A53 and R5 processing cores, combined with LPDDR4 memory.
- Trusted platform module (**TPM**) certified **CC EAL 4+ and and FIPS 104-2 Level 2**
- Reliability, fault tolerance and Single Event Upset (SEU) protection are enhanced though Triple Modular Redundancy **(TMR)** and Error Detection And Correction **(EDAC)** on data and logic.
- Standard mechanical and electrical interfaces are available and offer **compatibility with PC-104 CubeSat standard.**

- **Can be used either as the main OBC / PDHU or as an additional “crypto unit”**
- **IOV/IOD in Q2 2022**

ARCA Embedded implementation:
Option 2: on almost any OBC or PDHU

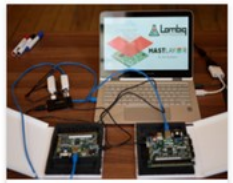
Berlin Space Technologies GmbH
Command and Data Handling System (CDH)
DATASHEET

NanoAvionics
SatBus 3C2
DATASHEET

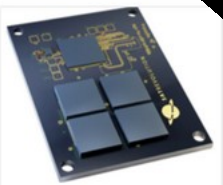
STM
MICROSATPRO Space Qualified Processor Unit
DATASHEET

STM
NANOSATPRO Space Qualified Processor Unit
DATASHEET

EnduroSat
Onboard Computer

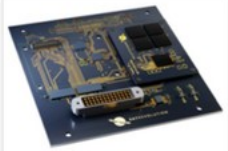


Lombiq Technologies Ltd.
Hastlayer
DATASHEET

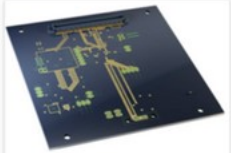


SatRevolution S.A.
Computing Unit

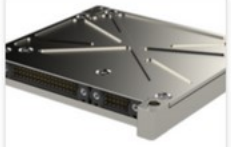
Space Inventor ApS
OBC-P3 Versatile Onboard Computing Platform
DATASHEET



SatRevolution S.A.
Advanced OBC
DATASHEET



SatRevolution S.A.
Basic OBC + IMU
DATASHEET



Space Inventor ApS
Z7000-P3 Versatile Payload and Onboard Computing Platform
DATASHEET

Xiphos Systems Corporation
Q8JS Processor
DATASHEET

Xiphos Systems Corporation
Q8S Processor
DATASHEET

Xiphos Systems Corporation
Q7 Processor
DATASHEET