Satellite Cybersecurity Reconnaissance

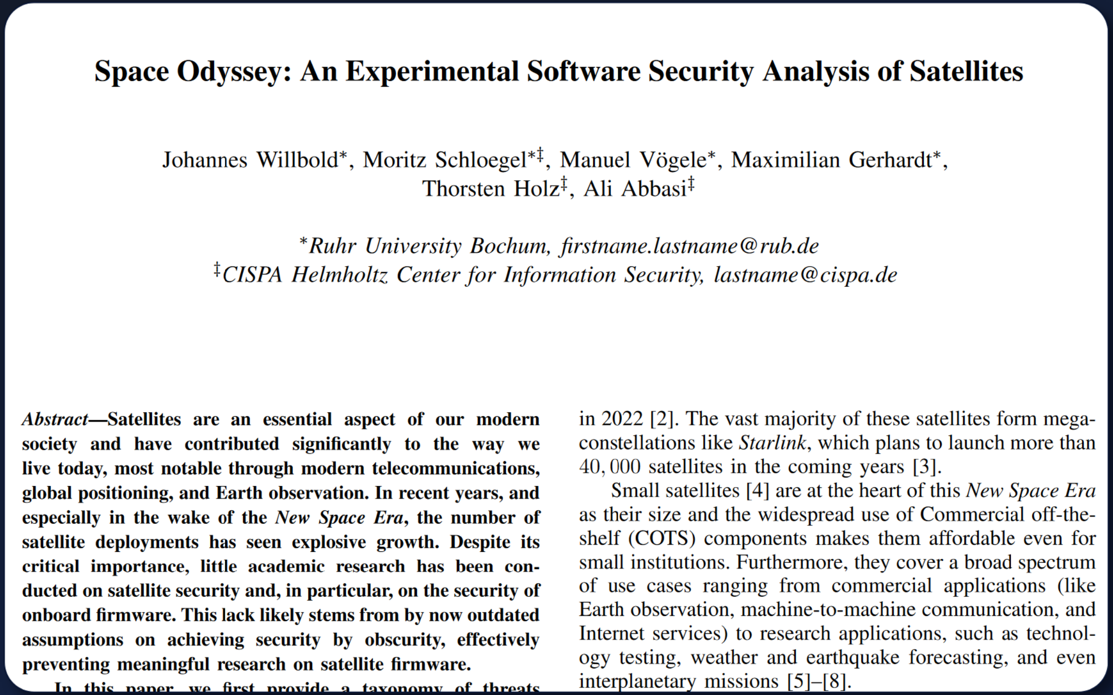
Strategies and their Real-world Evaluation

Johannes Willbold*, Franklyn Sciberras‡,
Martin Strohmeier^, Vincent Lenders^

*Ruhr University Bochum, Chair for Systems Security
‡ETH Zürich, Department of Computer Science,
^armasuisse Science + Technology, Cyber-Defence Campus

v1.0

Security by Obscurity



Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold[*], Moritz Schloegel[*‡], Manuel Vögele[*], Maximilian Gerhardt[*],
Thorsten Holz[‡], Ali Abbasi[‡]

[*]*Ruhr University Bochum, firstname.lastname@rub.de*
[‡]*CISPA Helmholtz Center for Information Security, lastname@cispa.de*

***Abstract*—Satellites are an essential aspect of our modern society and have contributed significantly to the way we live today, most notable through modern telecommunications, global positioning, and Earth observation. In recent years, and especially in the wake of the *New Space Era*, the number of satellite deployments has seen explosive growth. Despite its critical importance, little academic research has been conducted on satellite security and, in particular, on the security of onboard firmware. This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.**

In this paper, we first provide a taxonomy of threats

in 2022 [2]. The vast majority of these satellites form mega-constellations like *Starlink*, which plans to launch more than 40, 000 satellites in the coming years [3].

Small satellites [4] are at the heart of this *New Space Era* as their size and the widespread use of Commercial off-the-shelf (COTS) components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications (like Earth observation, machine-to-machine communication, and Internet services) to research applications, such as technology testing, weather and earthquake forecasting, and even interplanetary missions [5]–[8].

- Unsecured satellites
- Satellites rely on Security-by-Obscurity
- Where is the obscurity-breaking information coming from?

Reconnaissance

- How can attackers break obscurity?
- => How feasible is reconnaissance for satellites?
- What information is public?

Attacker Models

External Attacker

Attacker Models

External Attacker

Privilieged Attacker

Privileged Attacker

Privilieged Attacker

No Technical Insights

Received Access Credentials

→ **On-Board Reconnaissance**

Approach

18 Reconnaissance Goals

12 Reconnaissance Strategies

2 Strategy Evaluations

Reconnaissance Goals

Spacecraft Tracking & Operations

Radio Communication Parameters

Network Protocol Stacks

TMTC Protocols

Reconnaissance Goals

Spacecraft Tracking & Operations

Radio Communication Parameters

Network Protocol Stacks

TMTC Protocols

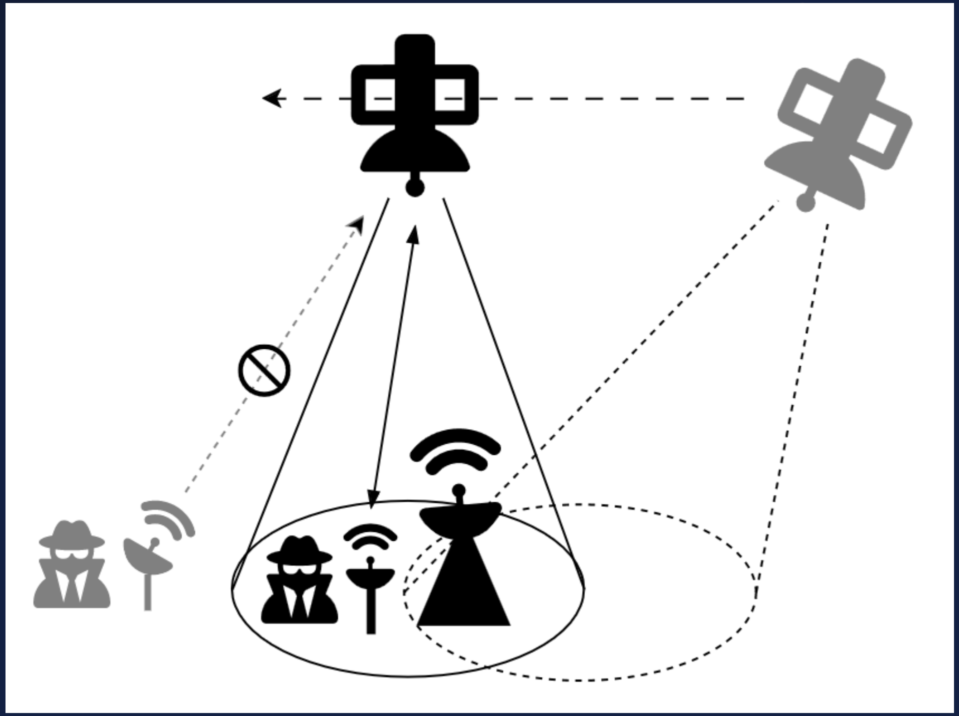
=> **Common** goals not **all**

Spacecraft Tracking & Operations

- **Tracking (TLE)**
- GS Pointing
- Satellite Attitude
- Operational Time Frame

Spacecraft Tracking & Operations

- Tracking (TLE)
- **GS Pointing**
- **Satellite Attitude**
- Operational Time Frame



Spacecraft Tracking & Operations

- Tracking (TLE)
- GS Pointing
- Satellite Attitude
- **Operational Time Frame**

Radio Communication Parameters

- **Signal Strength**
- Frequency
- Error Correction

Radio Communication Parameters

- Signal Strength
- **Frequency**
- Error Correction

Radio Communication Parameters

- Signal Strength
- Frequency
- **Error Correction**

Network Protocol Stacks

- Point-to-Point Protocols
- Vendor-specific Implementation Details
- Cryptographic Communications Protection
- Network Protocols and Routing

TMTC Protocols

- **Telecommand Set**
- **TMTC Formats**

Strategies

Open Databases

Public Regulator Filings

Common Options

COTS Analysis

Passive Traffic Analysis

Active Enumeration

Open Databases

- Launch: YYYY-XXX
- INTELDES/COSPAR ID: YYYY-XXXA/B/…
- JWST: 2021-130A

Open Databases

- Launch: YYYY-XXX
- INTELDES/COSPAR ID: YYYY-XXXA/B/...
- JWST: 2021-130A

- US Space Surveillance Network (SSN)
- Tracked Obj -> SATCAT/NORAD ID
- => TLE

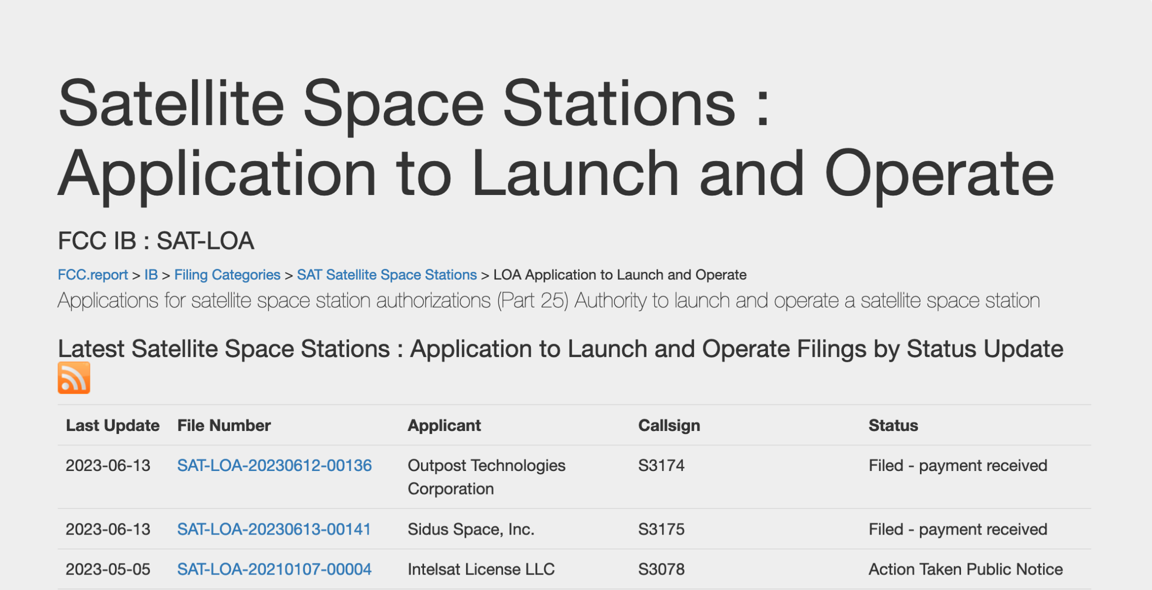
Open Databases

- Launch: YYYY-XXX
- INTELDES/COSPAR ID: YYYY-XXXA/B/...
- JWST: 2021-130A

- US Space Surveillance Network (SSN)
- Tracked Obj -> SATCAT/NORAD ID
- => TLE

- space-track website: COSPAR ID <=> NORAD ID

Public Regulator Filings



Satellite Space Stations : Application to Launch and Operate

FCC IB : SAT-LOA

FCC.report > IB > Filing Categories > SAT Satellite Space Stations > LOA Application to Launch and Operate

Applications for satellite space station authorizations (Part 25) Authority to launch and operate a satellite space station

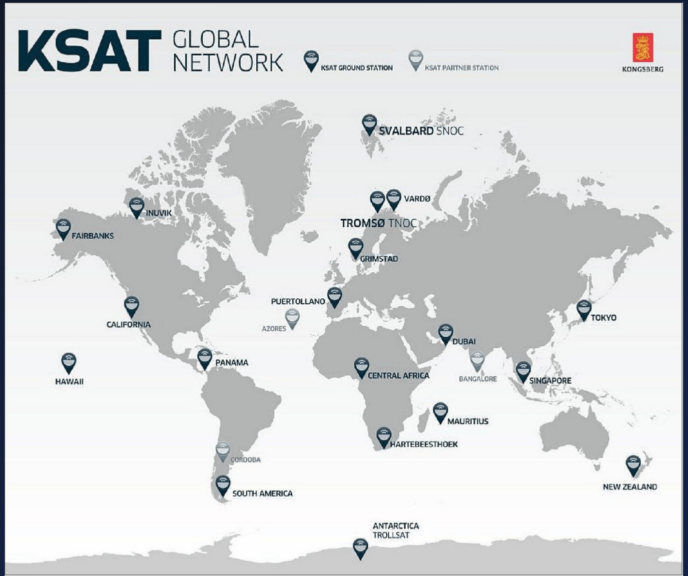
Latest Satellite Space Stations : Application to Launch and Operate Filings by Status Update

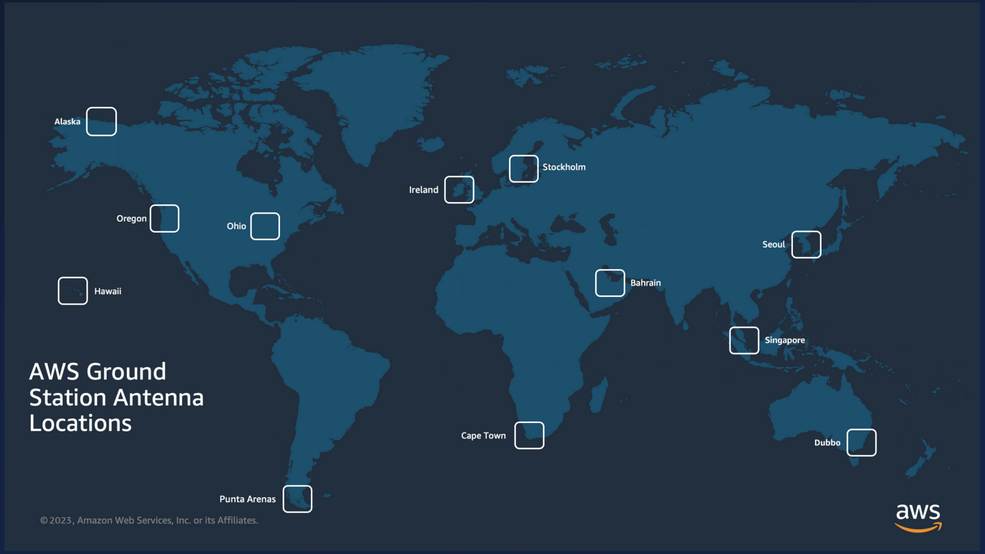
Last Update	File Number	Applicant	Callsign	Status
2023-06-13	SAT-LOA-20230612-00136	Outpost Technologies Corporation	S3174	Filed - payment received
2023-06-13	SAT-LOA-20230613-00141	Sidus Space, Inc.	S3175	Filed - payment received
2023-05-05	SAT-LOA-20210107-00004	Intelsat License LLC	S3078	Action Taken Public Notice

Satellite Space Stations: Application to Launch and Operate

- TT&C Frequency
- Payload Frequency
- GS Location
- Other

Common Options

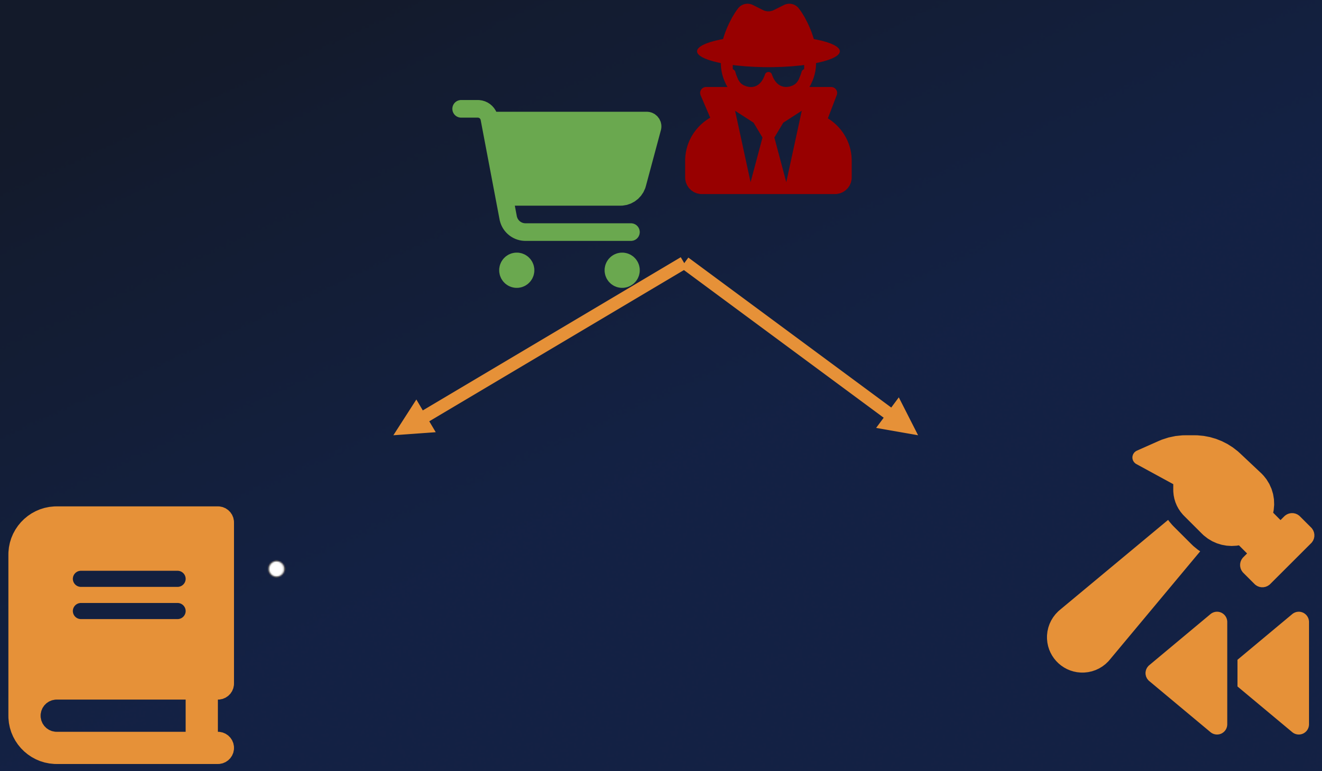




© 2023, Amazon Web Services, Inc. or its Affiliates.

GS Location Inference

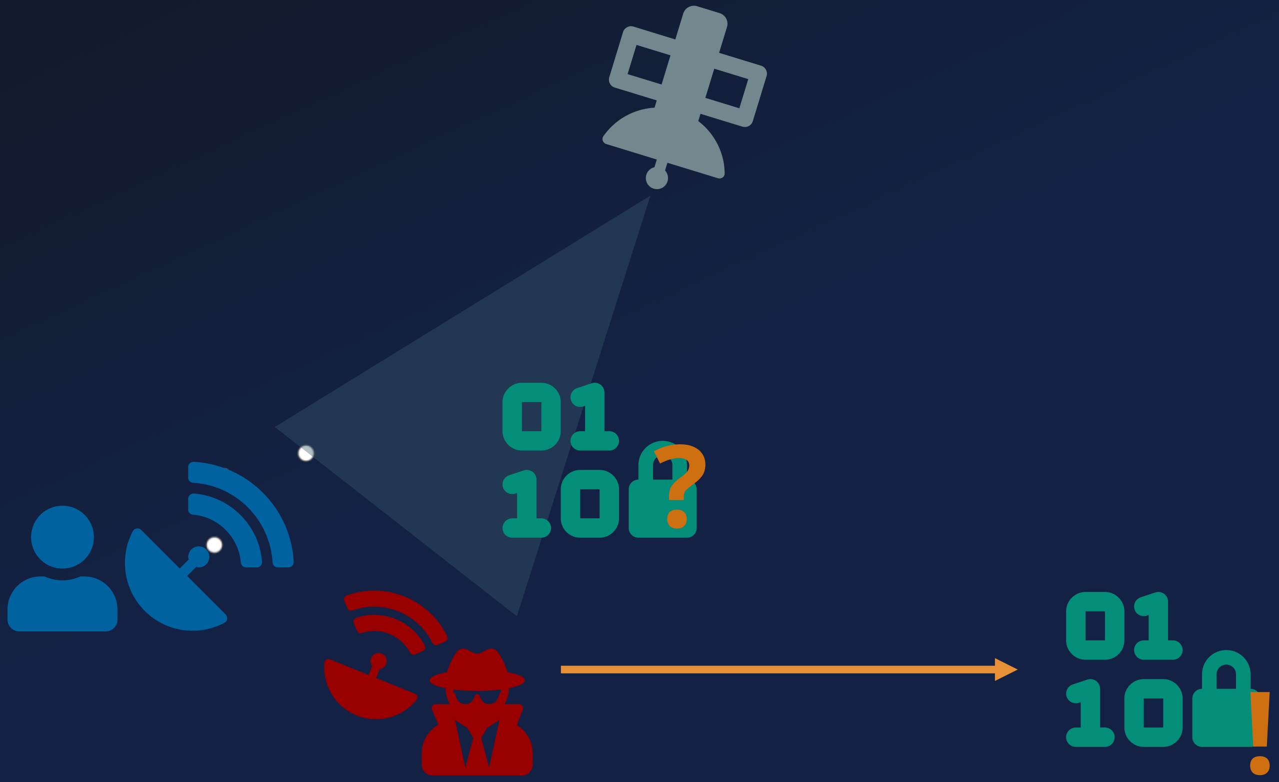
COTS Analysis



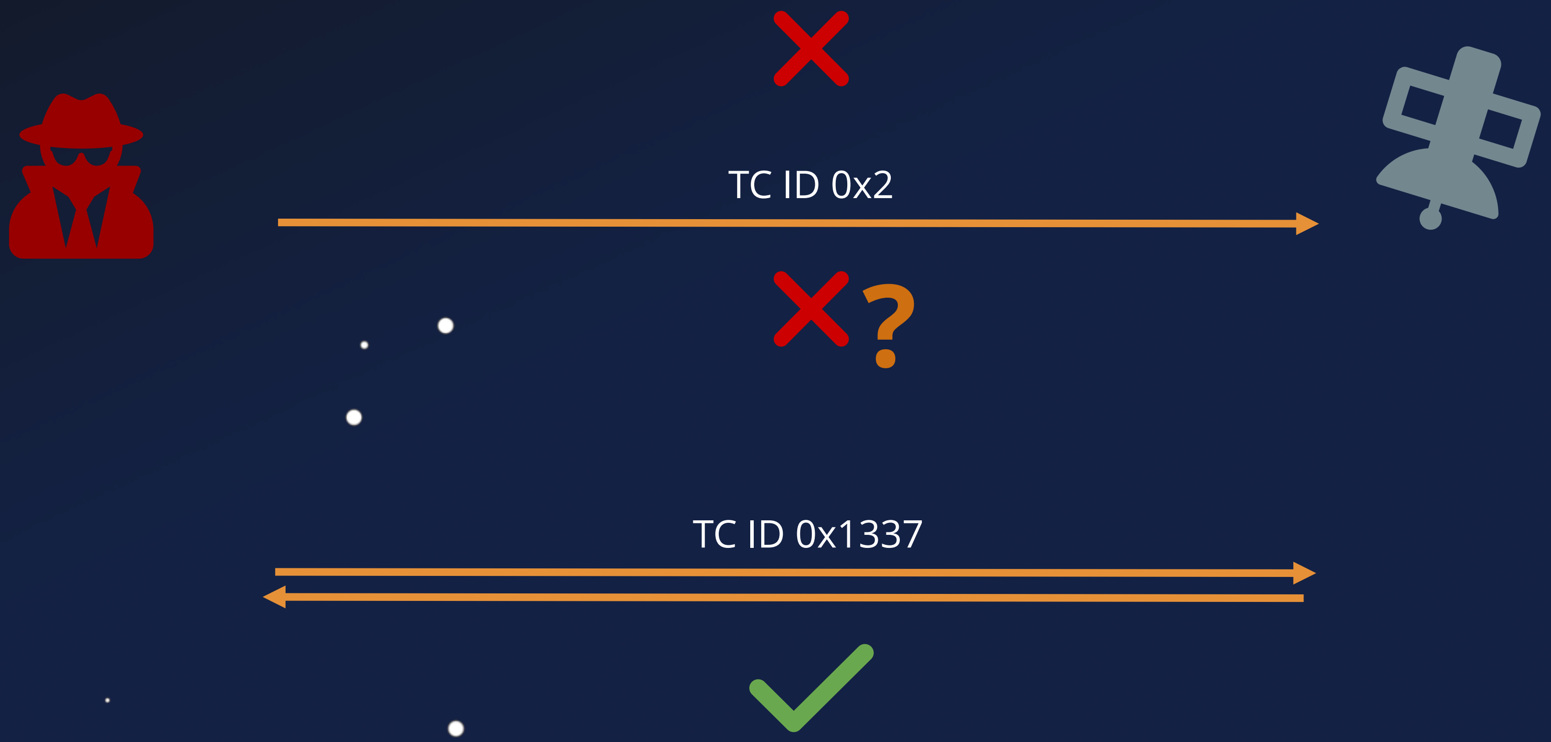
Vendor Documentation

Software Reverse Engineering

Passive Traffic Analysis



Active enumeration



TC ID 0x1

✗

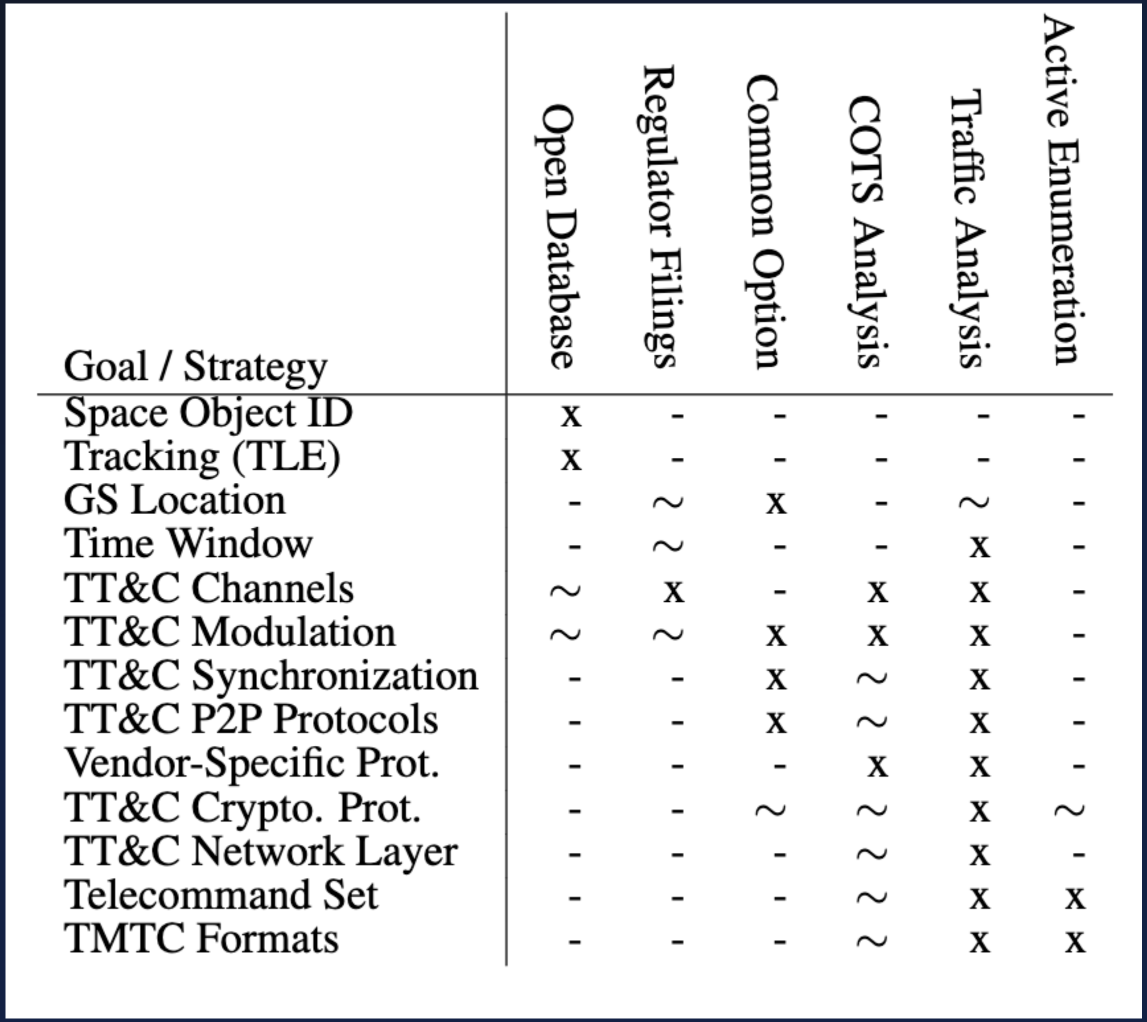
TC ID 0x2

✗?

TC ID 0x1337

✓

Goal-to-Strategy



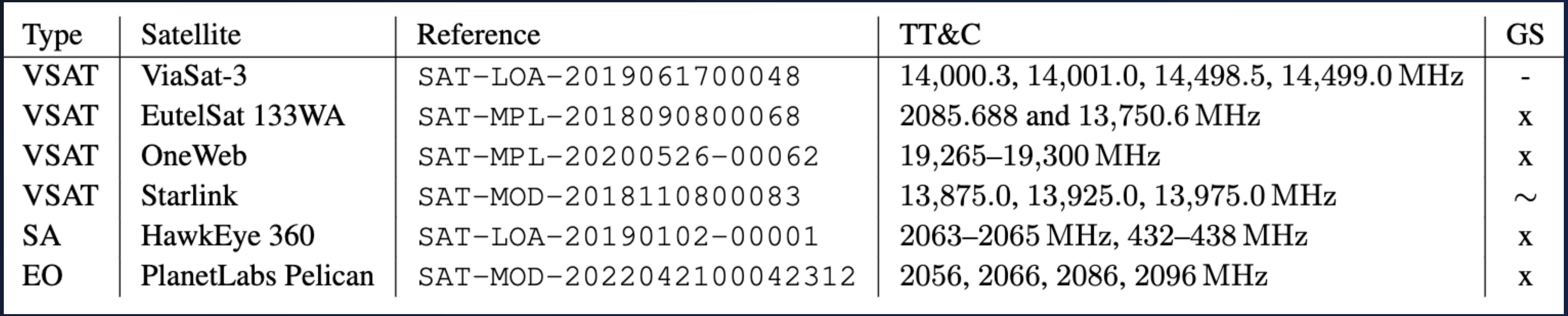
Goal / Strategy	Open Database	Regulator Filings	Common Option	COTS Analysis	Traffic Analysis	Active Enumeration
Space Object ID	x	-	-	-	-	-
Tracking (TLE)	x	-	-	-	-	-
GS Location	-	∼	x	-	∼	-
Time Window	-	∼	-	-	x	-
TT&C Channels	∼	x	-	x	x	-
TT&C Modulation	∼	∼	x	x	x	-
TT&C Synchronization	-	-	x	∼	x	-
TT&C P2P Protocols	-	-	x	∼	x	-
Vendor-Specific Prot.	-	-	-	x	x	-
TT&C Crypto. Prot.	-	-	∼	∼	x	∼
TT&C Network Layer	-	-	-	∼	x	-
Telecommand Set	-	-	-	∼	x	x
TMTC Formats	-	-	-	∼	x	x

Evaluation

Public Regulator Filings -
> FCC Filings

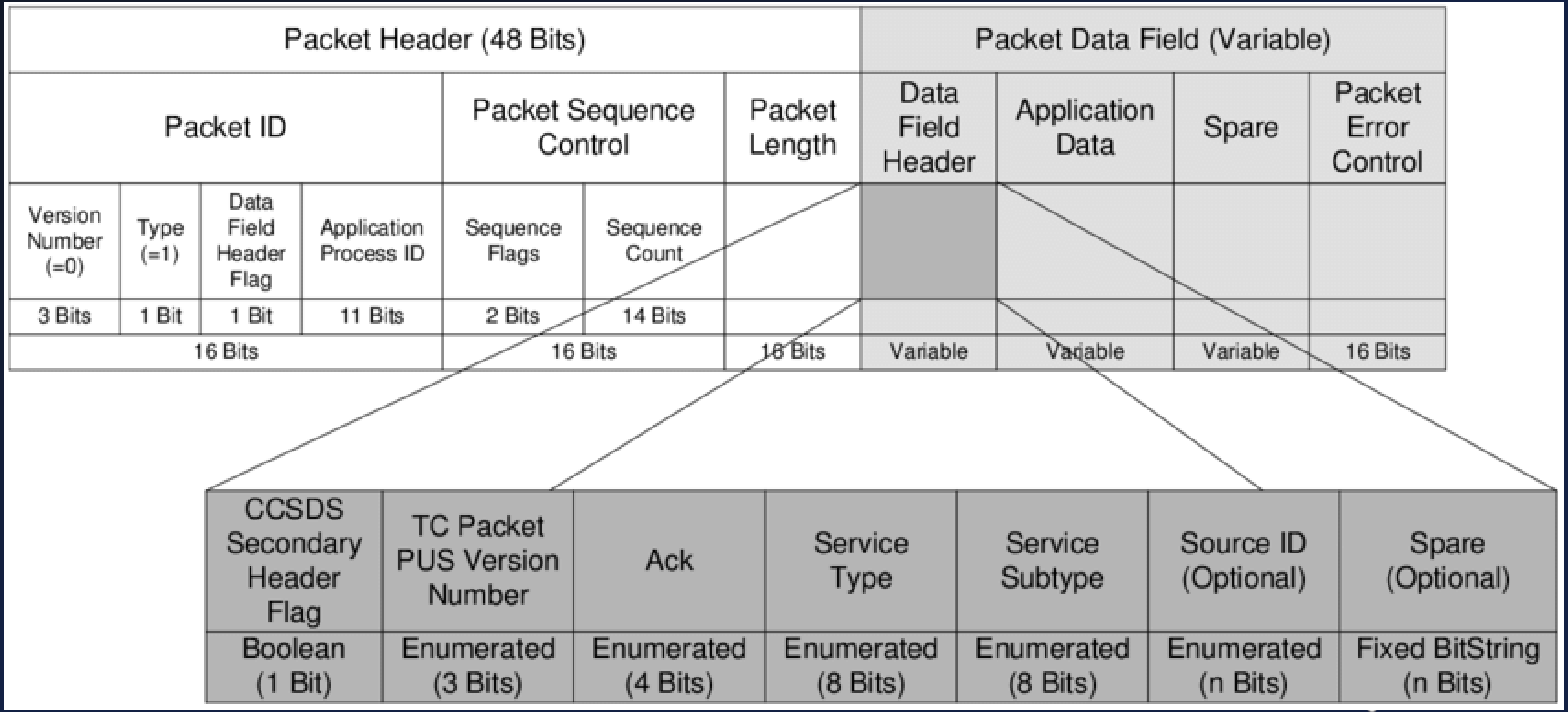
Active Enumeration
-> ECSS PUS Analysis

FCC Filings



Type	Satellite	Reference	TT&C	GS
VSAT	ViaSat-3	`SAT-LOA-2019061700048`	14,000.3, 14,001.0, 14,498.5, 14,499.0 MHz	-
VSAT	EutelSat 133WA	`SAT-MPL-2018090800068`	2085.688 and 13,750.6 MHz	x
VSAT	OneWeb	`SAT-MPL-20200526-00062`	19,265–19,300 MHz	x
VSAT	Starlink	`SAT-MOD-2018110800083`	13,875.0, 13,925.0, 13,975.0 MHz	∼
SA	HawkEye 360	`SAT-LOA-20190102-00001`	2063–2065 MHz, 432–438 MHz	x
EO	PlanetLabs Pelican	`SAT-MOD-2022042100042312`	2056, 2066, 2086, 2096 MHz	x

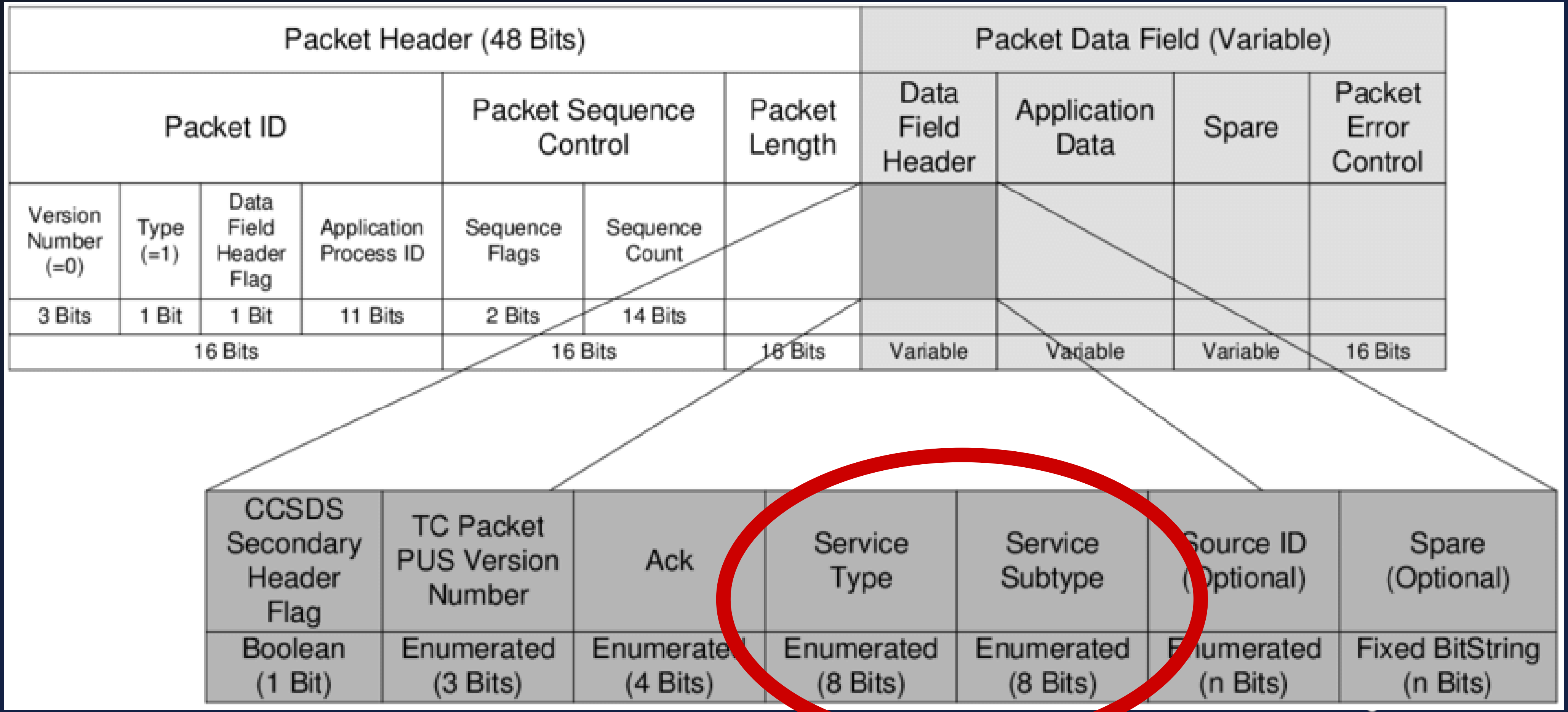
TT&C Analysis



Packet Header (48 Bits)							Packet Data Field (Variable)			
Packet ID				Packet Sequence Control		Packet Length	Data Field Header	Application Data	Spare	Packet Error Control
Version Number (=0)	Type (=1)	Data Field Header Flag	Application Process ID	Sequence Flags	Sequence Count					
3 Bits	1 Bit	1 Bit	11 Bits	2 Bits	14 Bits					
16 Bits				16 Bits		16 Bits	Variable	Variable	Variable	16 Bits

CCSDS Secondary Header Flag	TC Packet PUS Version Number	Ack	Service Type	Service Subtype	Source ID (Optional)	Spare (Optional)
Boolean (1 Bit)	Enumerated (3 Bits)	Enumerated (4 Bits)	Enumerated (8 Bits)	Enumerated (8 Bits)	Enumerated (n Bits)	Fixed BitString (n Bits)

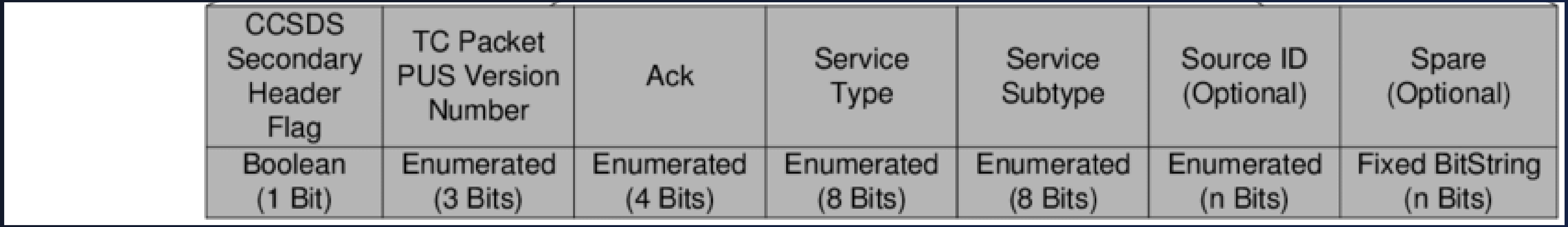
TT&C Analysis



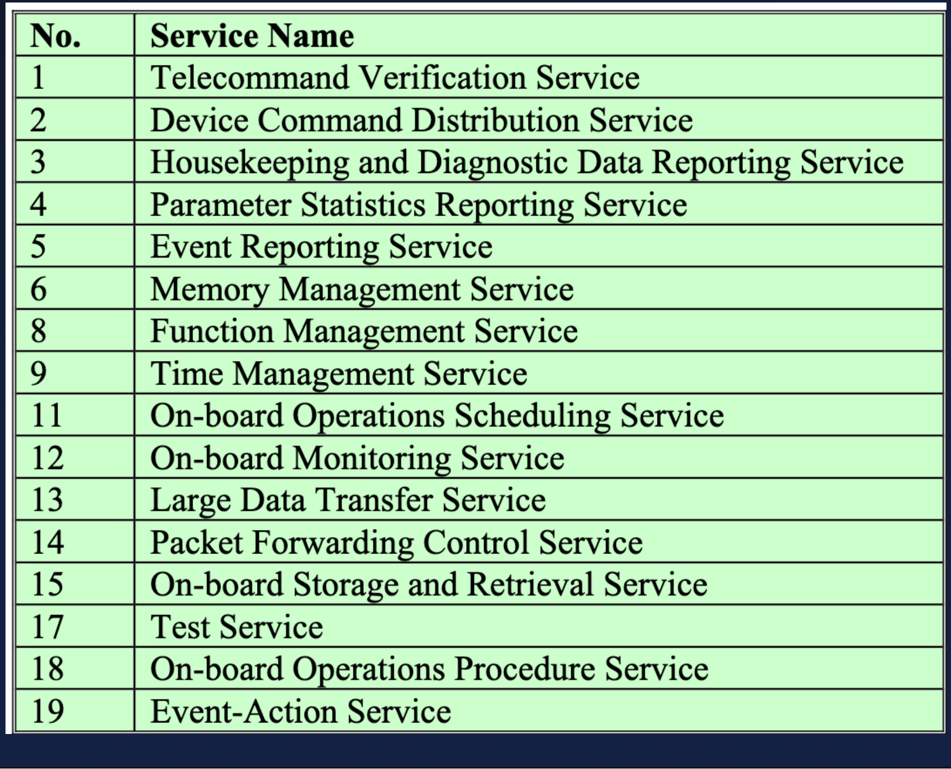
Packet Header (48 Bits)							Packet Data Field (Variable)			
Packet ID				Packet Sequence Control		Packet Length	Data Field Header	Application Data	Spare	Packet Error Control
Version Number (=0)	Type (=1)	Data Field Header Flag	Application Process ID	Sequence Flags	Sequence Count					
3 Bits	1 Bit	1 Bit	11 Bits	2 Bits	14 Bits					
16 Bits				16 Bits		16 Bits	Variable	Variable	Variable	16 Bits

CCSDS Secondary Header Flag	TC Packet PUS Version Number	Ack	Service Type	Service Subtype	Source ID (Optional)	Spare (Optional)
Boolean (1 Bit)	Enumerated (3 Bits)	Enumerated (4 Bits)	Enumerated (8 Bits)	Enumerated (8 Bits)	Enumerated (n Bits)	Fixed BitString (n Bits)

TT&C Analysis



CCSDS Secondary Header Flag	TC Packet PUS Version Number	Ack	Service Type	Service Subtype	Source ID (Optional)	Spare (Optional)
Boolean (1 Bit)	Enumerated (3 Bits)	Enumerated (4 Bits)	Enumerated (8 Bits)	Enumerated (8 Bits)	Enumerated (n Bits)	Fixed BitString (n Bits)

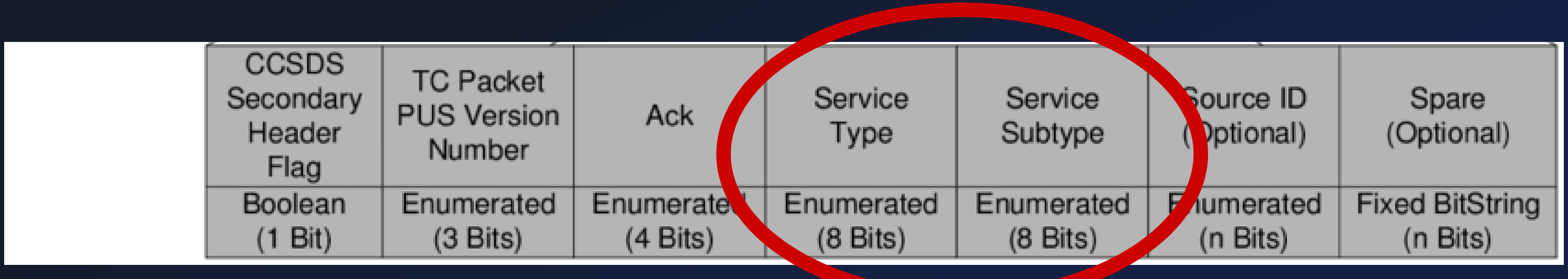


No.	Service Name
1	Telecommand Verification Service
2	Device Command Distribution Service
3	Housekeeping and Diagnostic Data Reporting Service
4	Parameter Statistics Reporting Service
5	Event Reporting Service
6	Memory Management Service
8	Function Management Service
9	Time Management Service
11	On-board Operations Scheduling Service
12	On-board Monitoring Service
13	Large Data Transfer Service
14	Packet Forwarding Control Service
15	On-board Storage and Retrieval Service
17	Test Service
18	On-board Operations Procedure Service
19	Event-Action Service

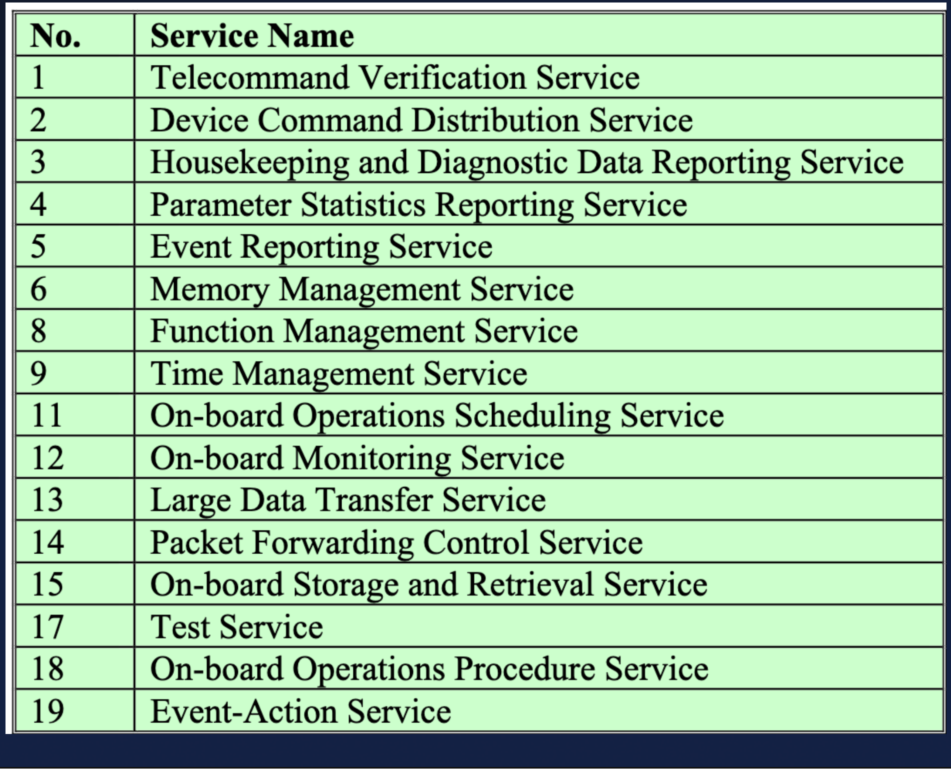
- 255 potential services
- Each Services: 255 potential subservices

=> 65.035 potential Subservices

TT&C Analysis



CCSDS Secondary Header Flag	TC Packet PUS Version Number	Ack	Service Type	Service Subtype	Source ID (Optional)	Spare (Optional)
Boolean (1 Bit)	Enumerated (3 Bits)	Enumerated (4 Bits)	Enumerated (8 Bits)	Enumerated (8 Bits)	Enumerated (n Bits)	Fixed BitString (n Bits)

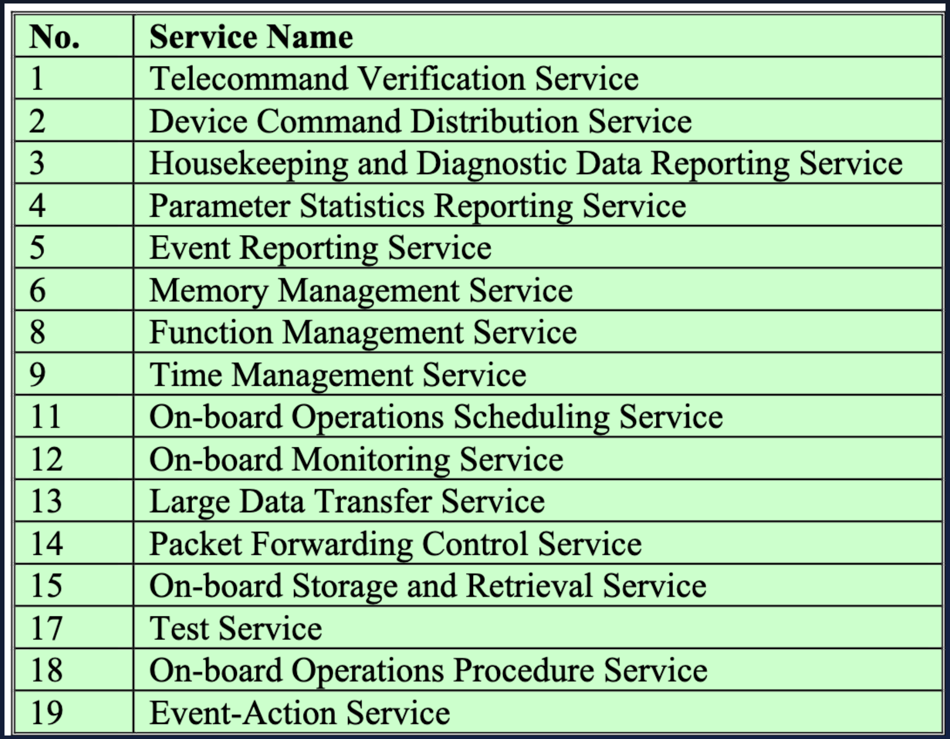


No.	Service Name
1	Telecommand Verification Service
2	Device Command Distribution Service
3	Housekeeping and Diagnostic Data Reporting Service
4	Parameter Statistics Reporting Service
5	Event Reporting Service
6	Memory Management Service
8	Function Management Service
9	Time Management Service
11	On-board Operations Scheduling Service
12	On-board Monitoring Service
13	Large Data Transfer Service
14	Packet Forwarding Control Service
15	On-board Storage and Retrieval Service
17	Test Service
18	On-board Operations Procedure Service
19	Event-Action Service

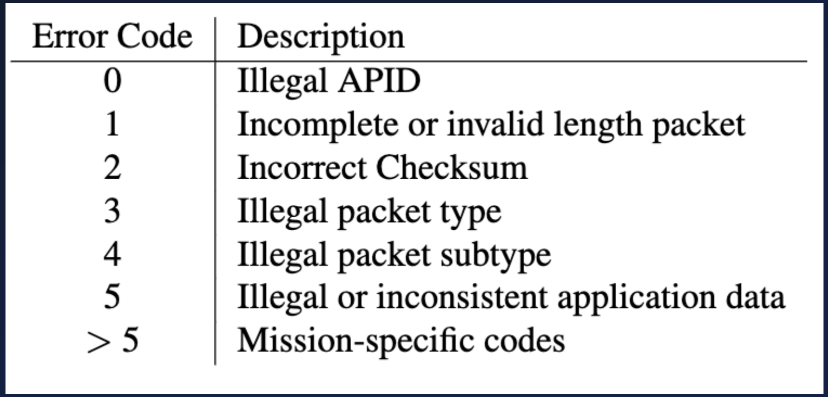
- 255 potential services
- Each Services: 255 potential subservices

=> 65.035 potential Subservices

TT&C Analysis



No.	Service Name
1	Telecommand Verification Service
2	Device Command Distribution Service
3	Housekeeping and Diagnostic Data Reporting Service
4	Parameter Statistics Reporting Service
5	Event Reporting Service
6	Memory Management Service
8	Function Management Service
9	Time Management Service
11	On-board Operations Scheduling Service
12	On-board Monitoring Service
13	Large Data Transfer Service
14	Packet Forwarding Control Service
15	On-board Storage and Retrieval Service
17	Test Service
18	On-board Operations Procedure Service
19	Event-Action Service



Error Code	Description
0	Illegal APID
1	Incomplete or invalid length packet
2	Incorrect Checksum
3	Illegal packet type
4	Illegal packet subtype
5	Illegal or inconsistent application data
> 5	Mission-specific codes

- Service 1, SubService 1 => Error 3
  - Service doesn't exist
- Service 2, SubService 1 -> Error 5
  - Service exists, SubService exists, Wrong data
- Service 2, SubService 2 -> Error 4
  - Service exists SubService does not exist

TT&C Analysis

- Command ID
- Subcommand ID
- Error Message

=> Simple Iteration

Q&A

18 Reconnaissance Goals

12 Reconnaissance Strategies

2 Strategy Evaluations

@jwillbold

/jwillbold

Johannes Willbold - johannes.willbold@rub.de