CISPA

RUHR
UNIVERSITÄT
BOCHUM
RUB

Space Odyssey

An Experimental 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

Distinguished
Paper

v1.3

Applications

Telecommunications

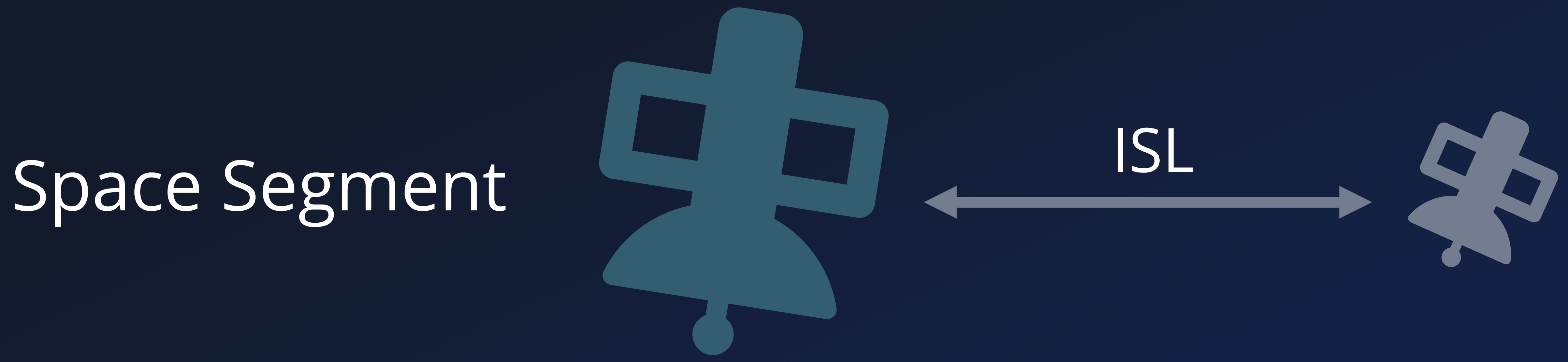
Global Positioning

Earth Obervation

Research

Technology Testing

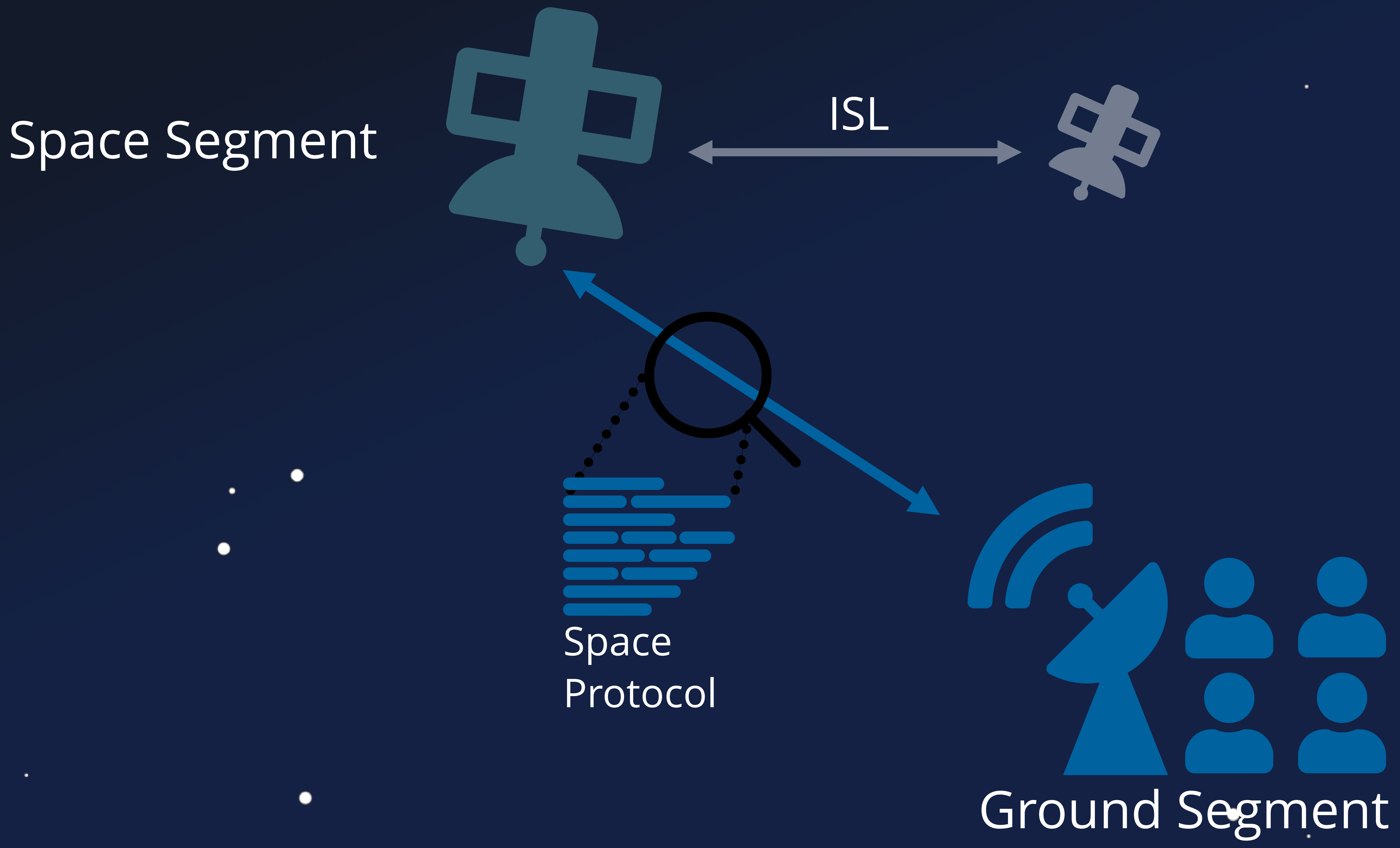
Context



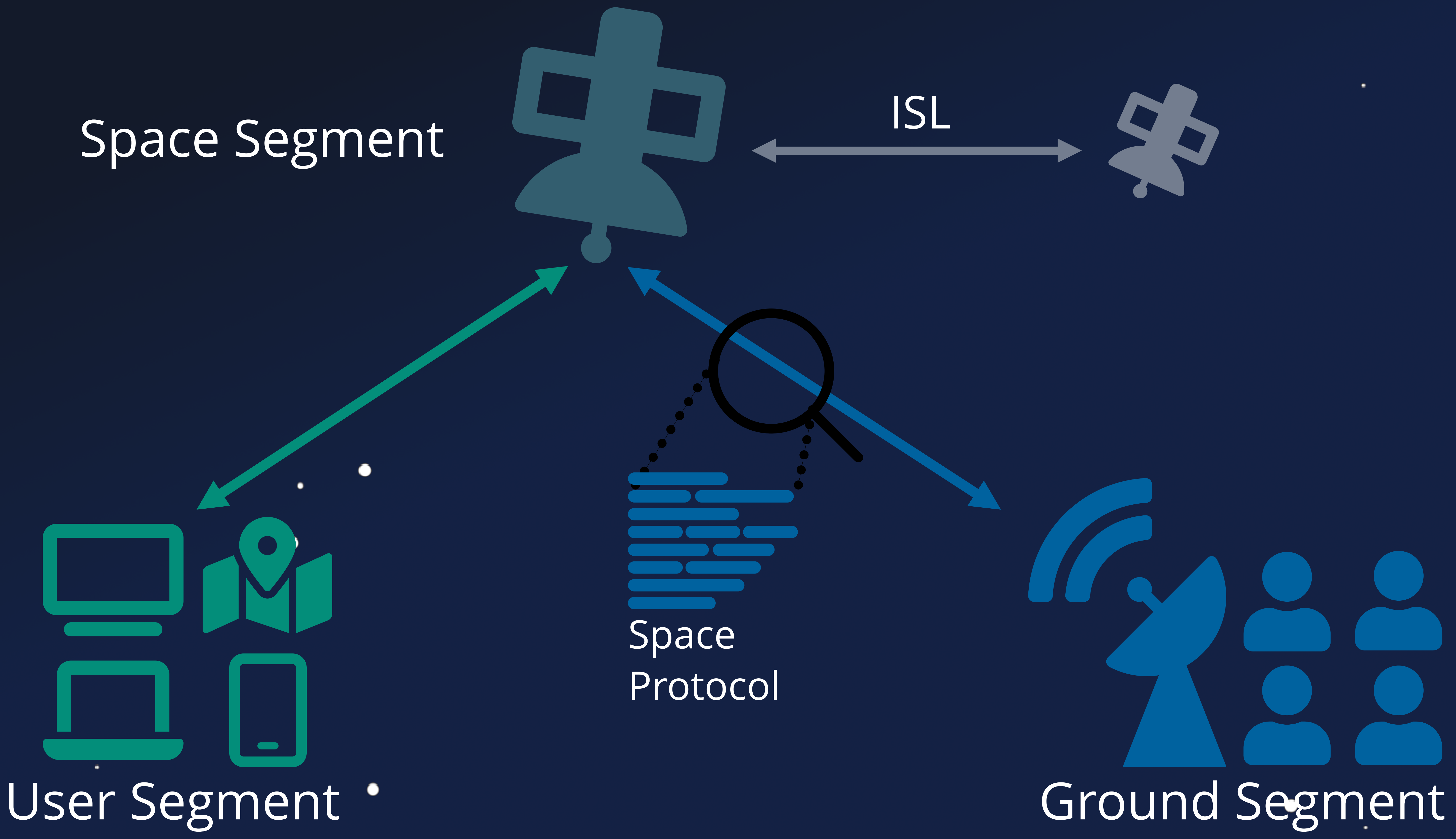
Space Segment

ISL

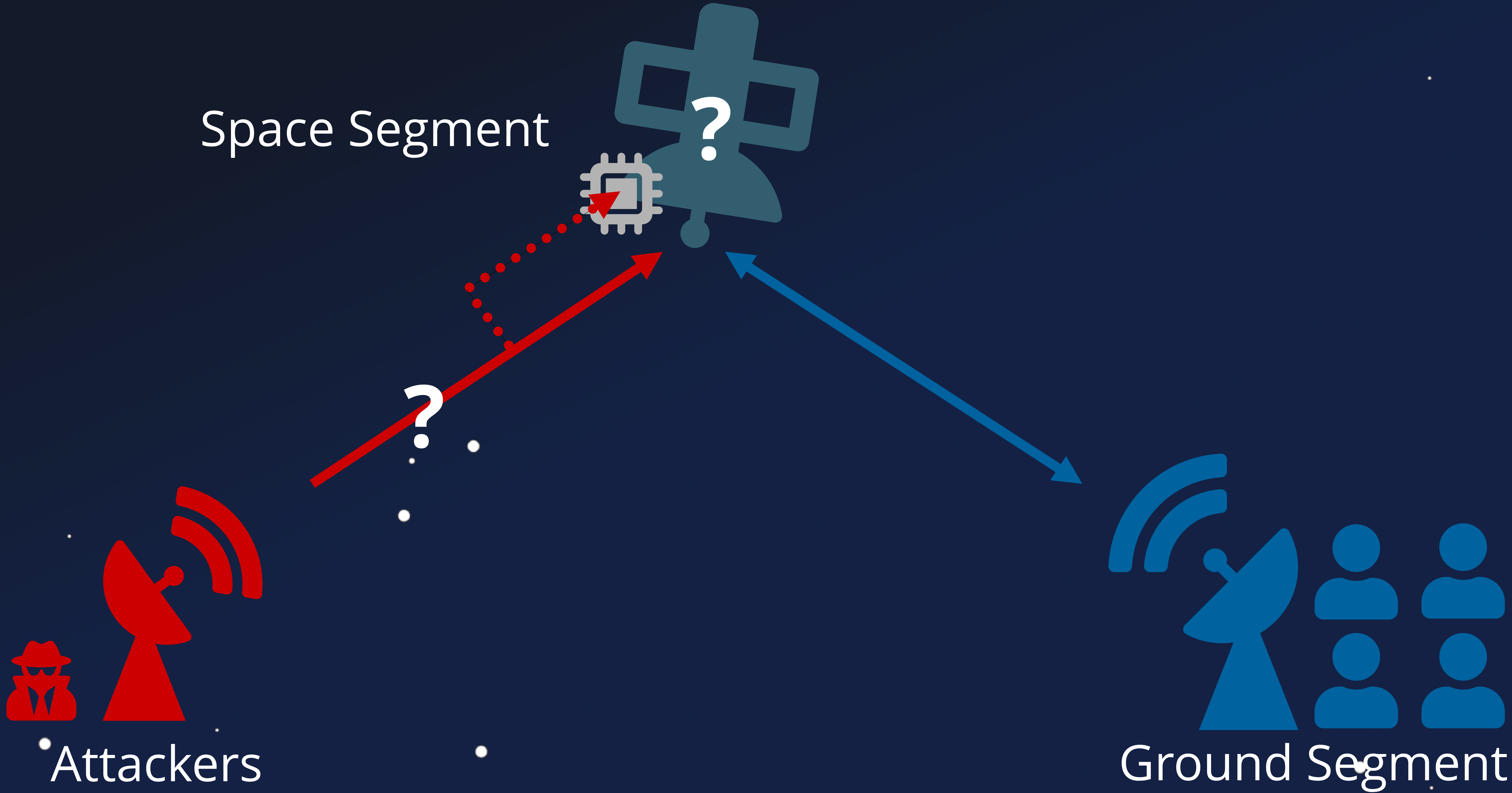
Context



Context


Space Segment
ISL
Space
Protocol
User Segment
Ground Segment

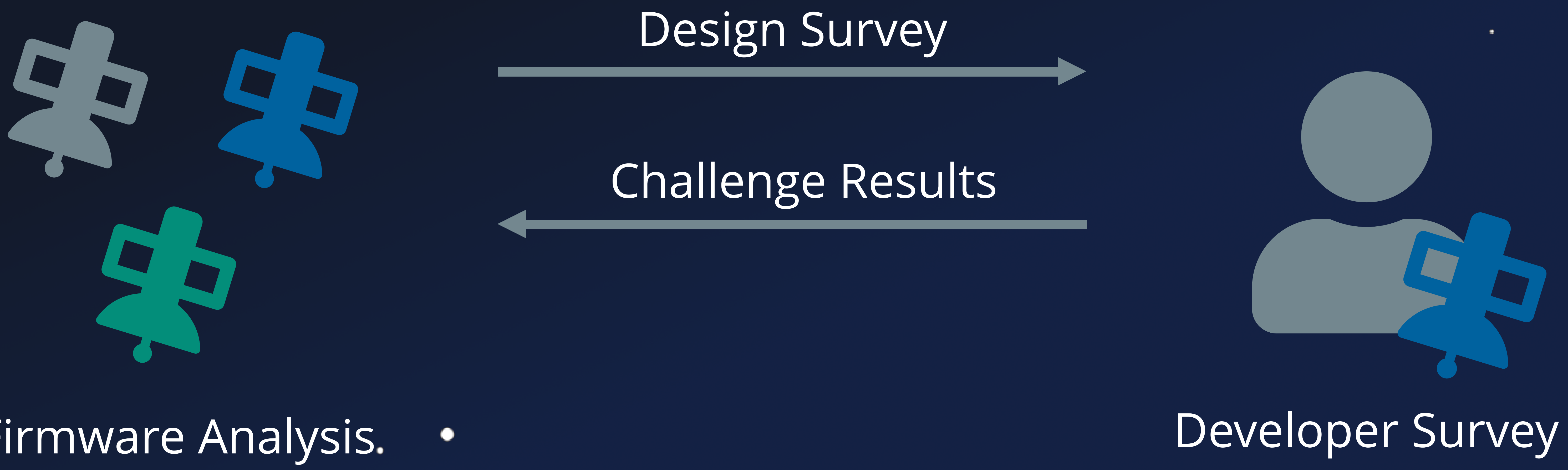
Motivation



Approach

Firmware Analysis.

Approach



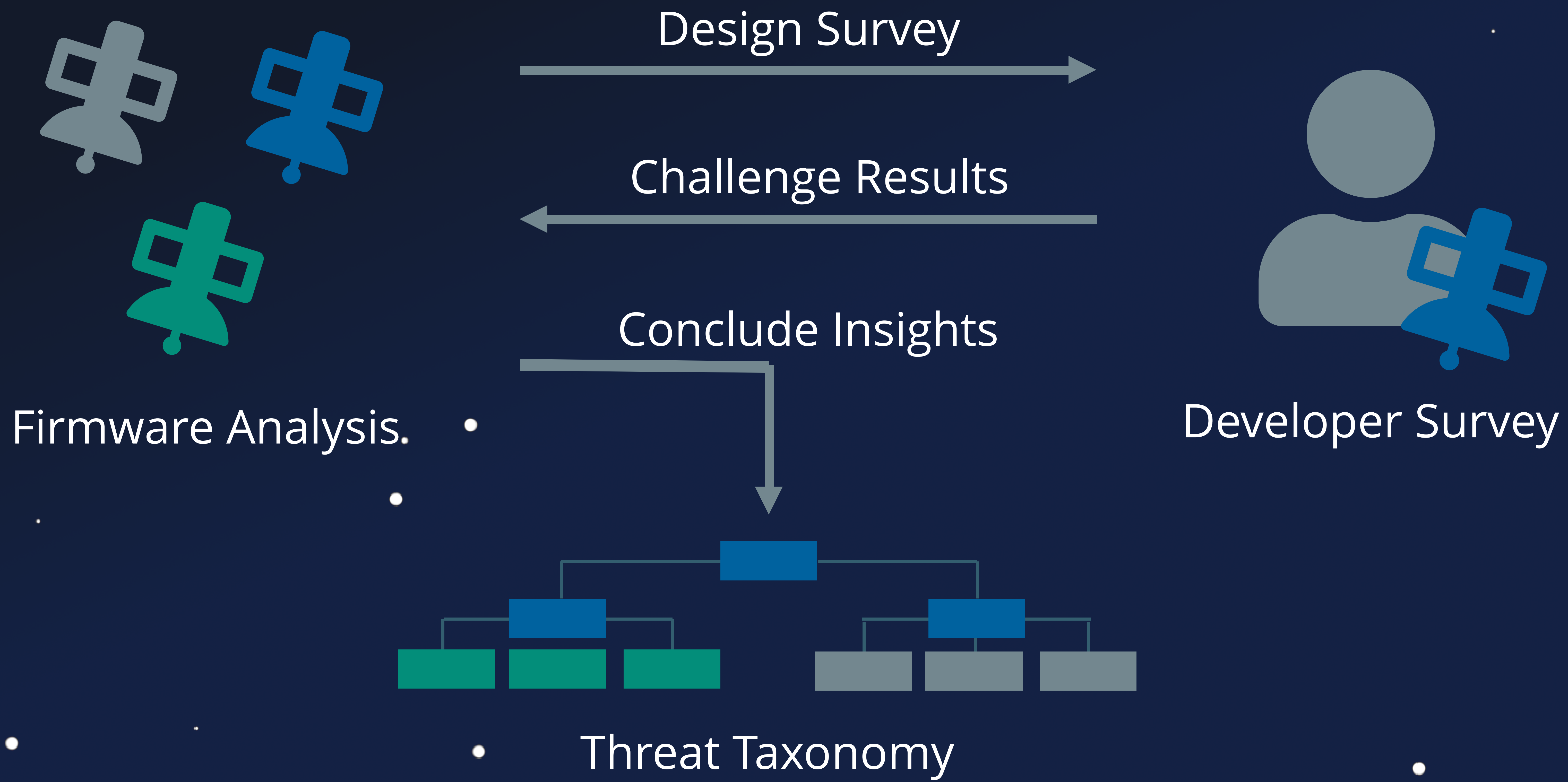
Design Survey

Challenge Results

Firmware Analysis

Developer Survey

Approach



Design Survey

Challenge Results

Conclude Insights

Firmware Analysis.

Developer Survey

Threat Taxonomy

Attack Goals

Attack Goals

Denial of Service

Attack Goals

Denial of Service

Malicious Data Interaction

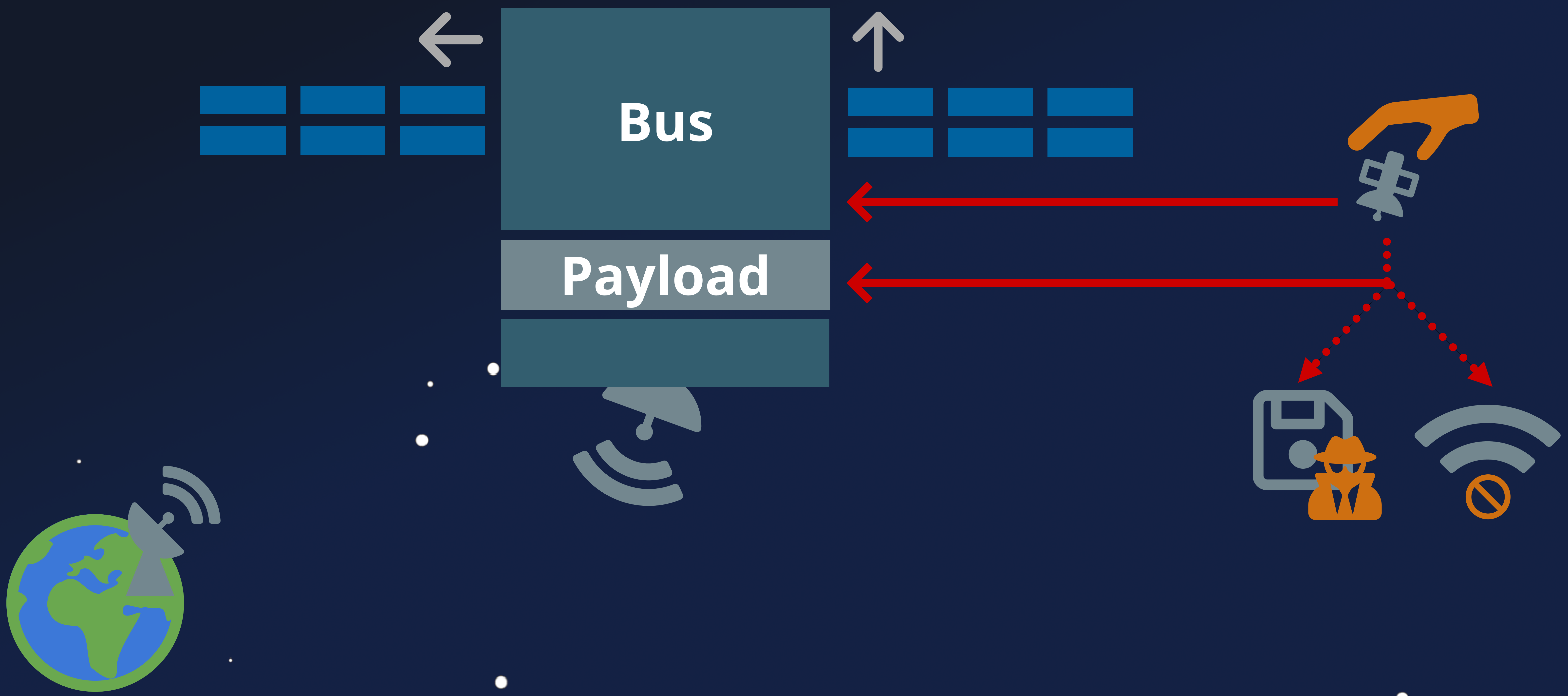
Attack Goals

Denial of Service

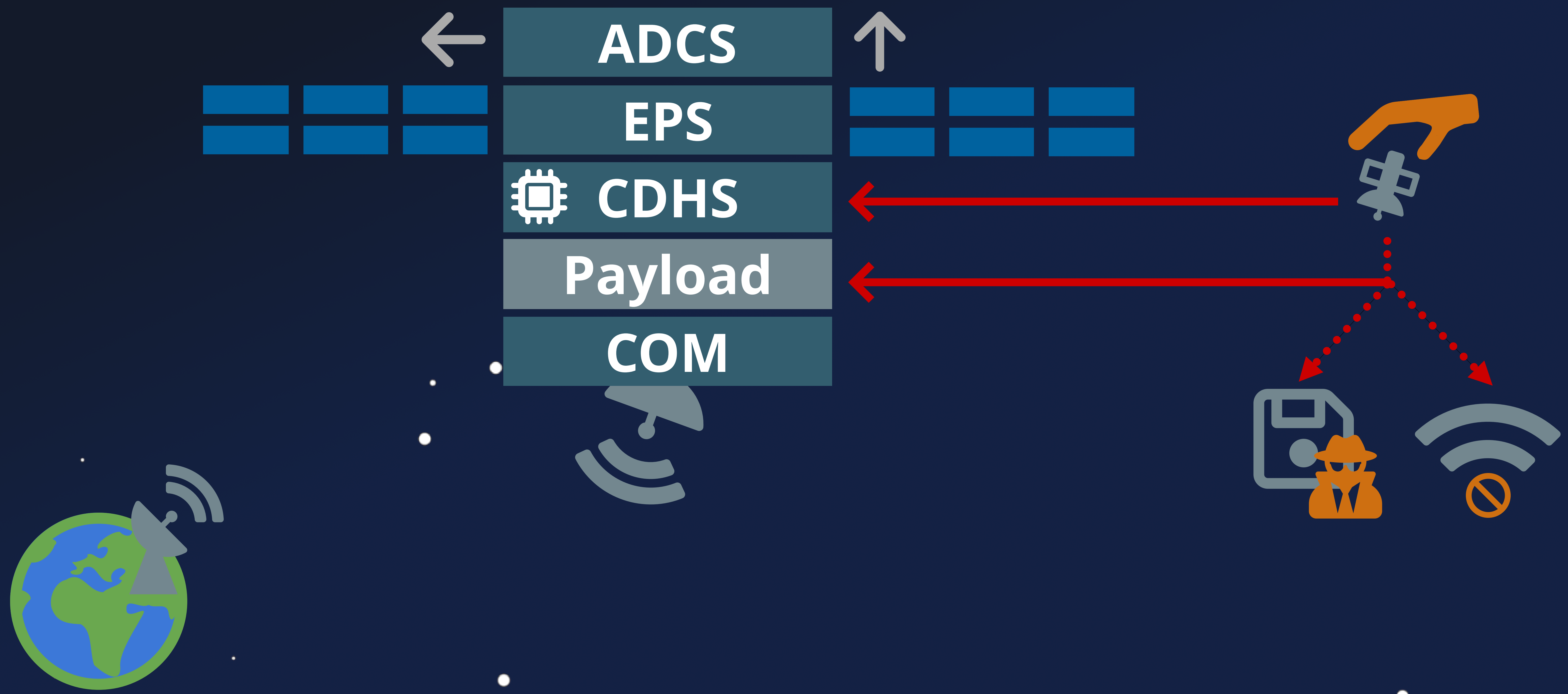
Seizure of Control

Malicious Data Interaction

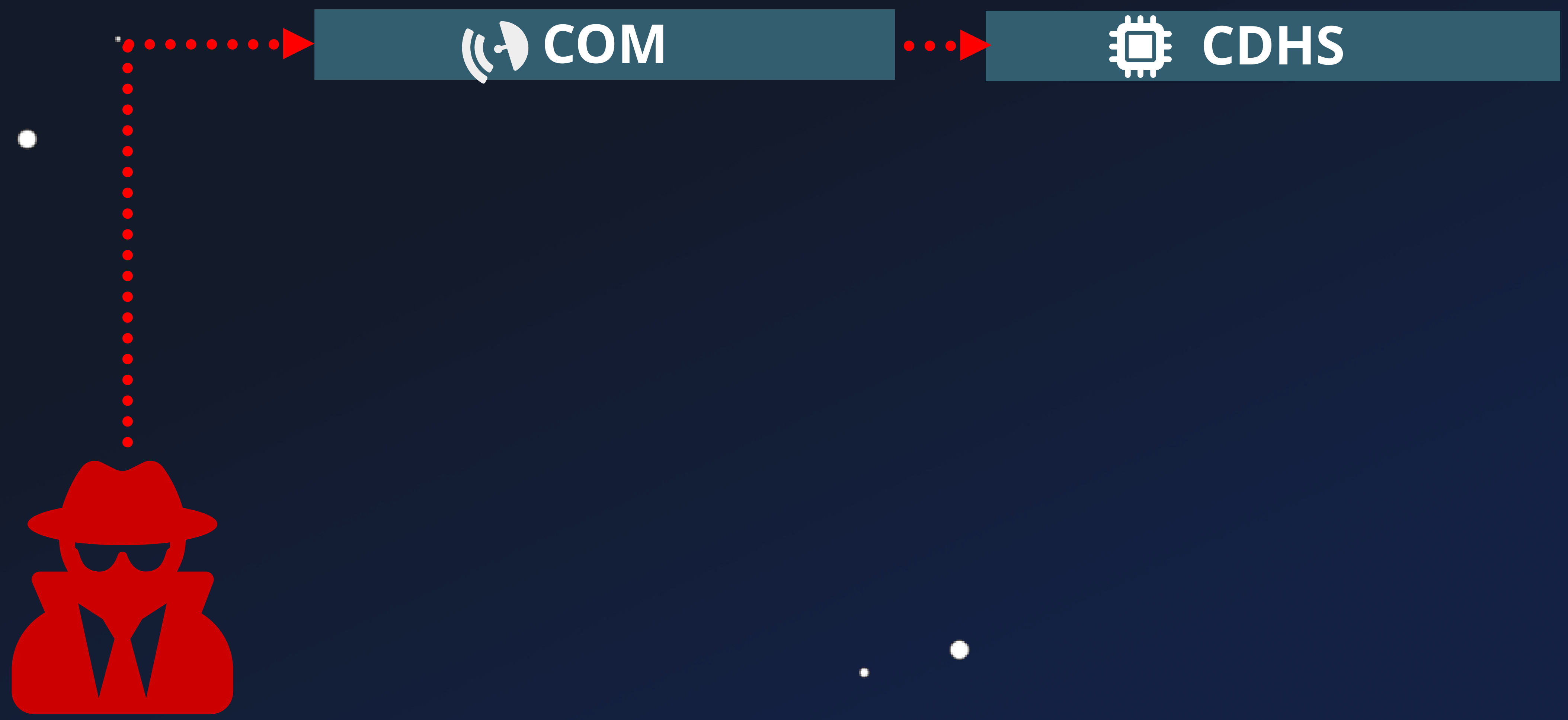
Bus / Payload



Bus / Payload



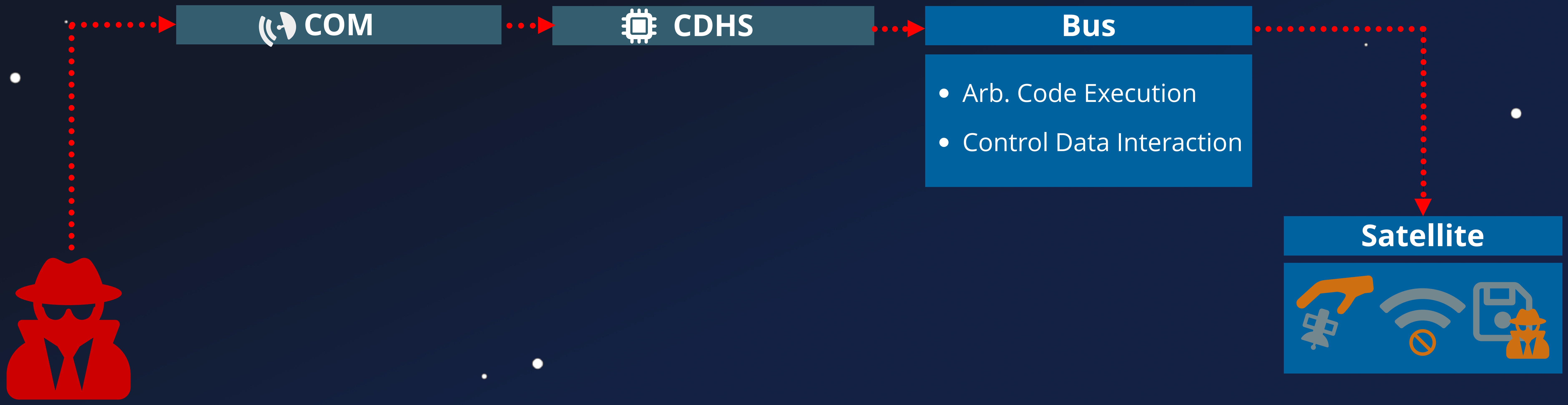
Threats



COM

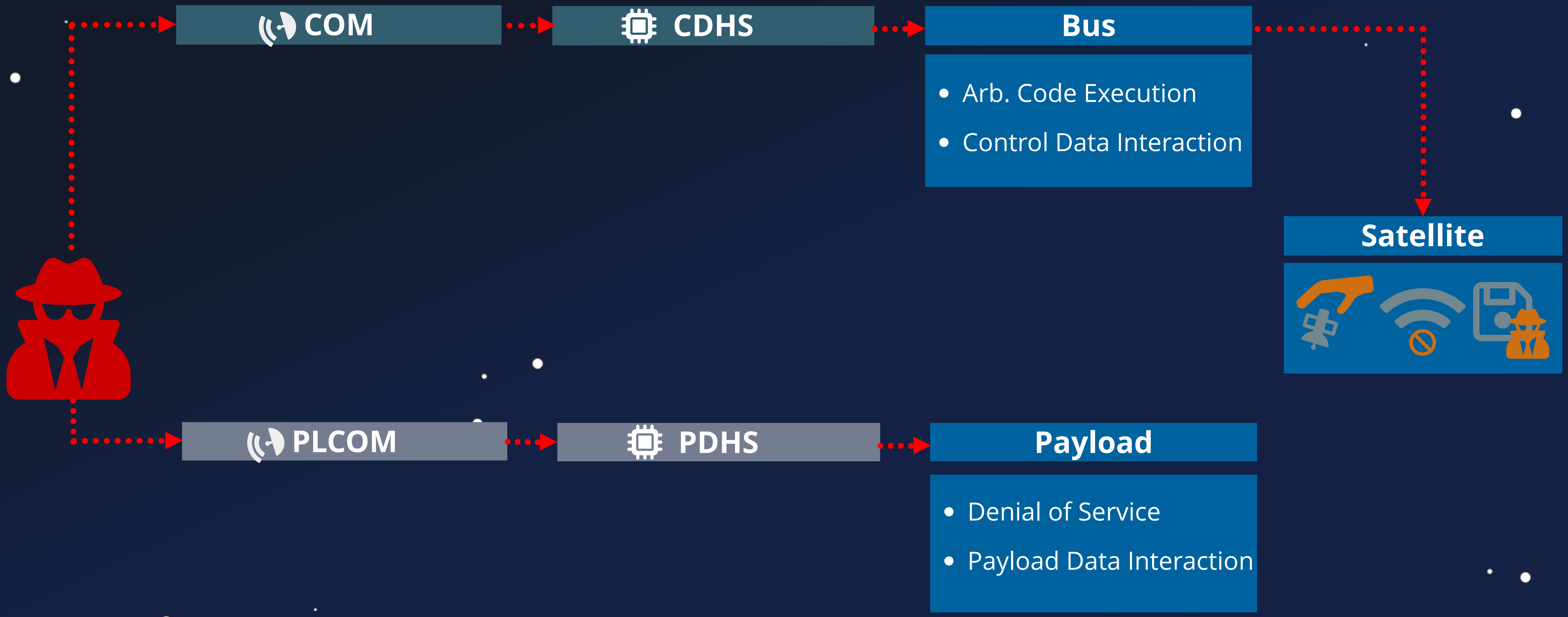
CDHS

Threats



- Arb. Code Execution
- Control Data Interaction

Threats



COM

CDHS

Bus

- Arb. Code Execution
- Control Data Interaction

Satellite

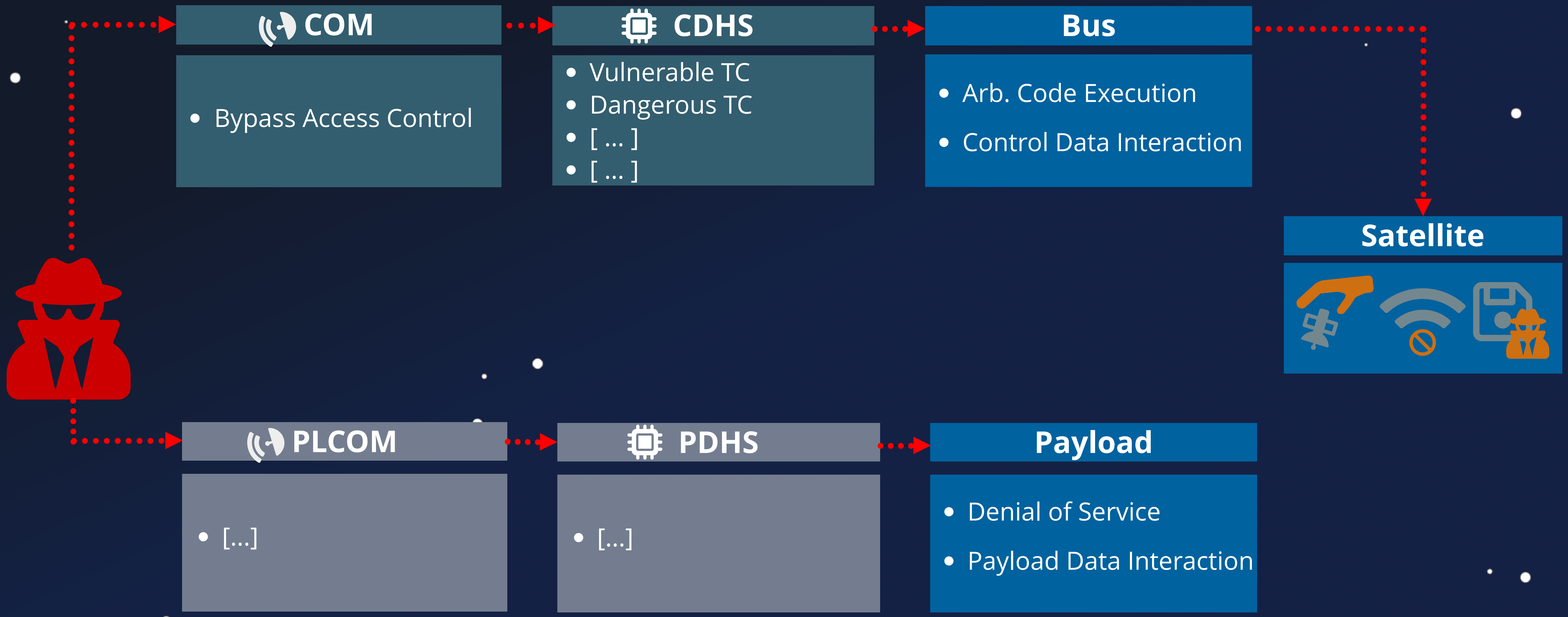
PLCOM

PDHS

Payload

- Denial of Service
- Payload Data Interaction

Threats



COM

- Bypass Access Control

CDHS

- Vulnerable TC
- Dangerous TC
- […]
- […]

Bus

- Arb. Code Execution
- Control Data Interaction

Satellite

PLCOM

- […]

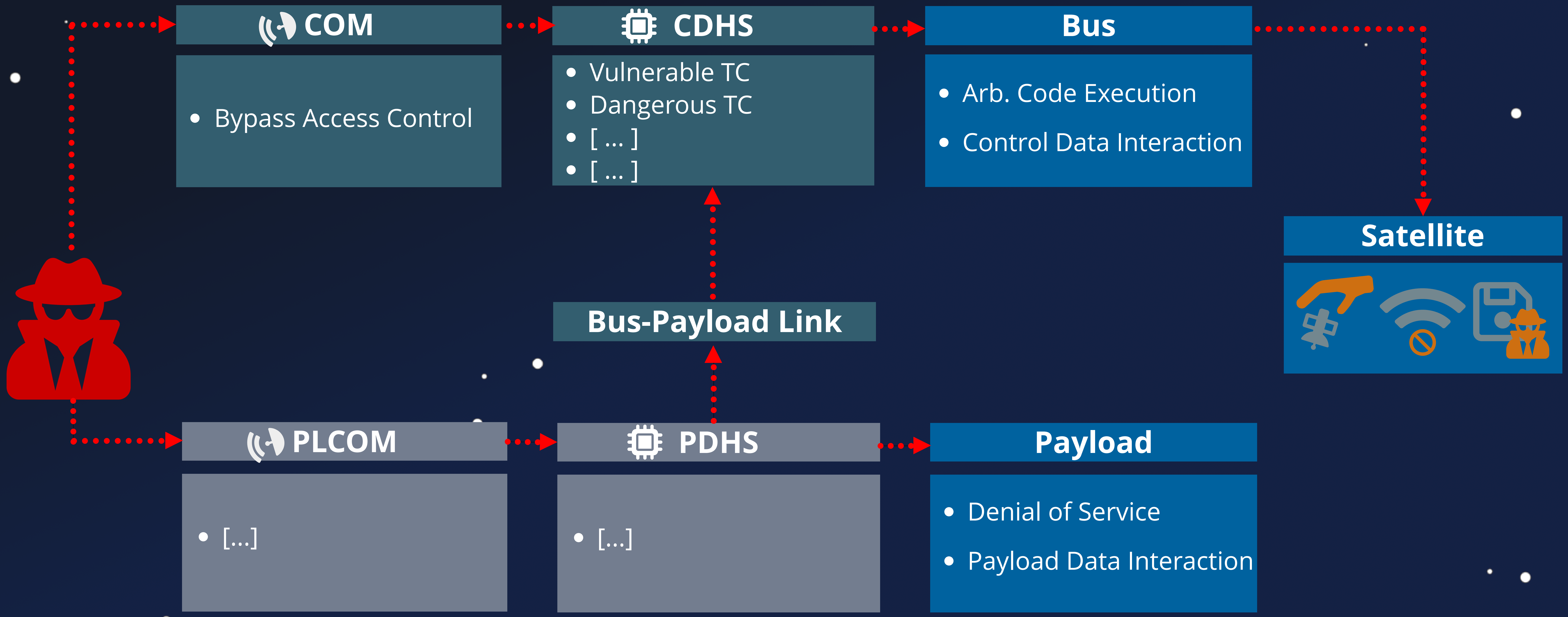
PDHS

- […]

Payload

- Denial of Service
- Payload Data Interaction

Threats



COM

- Bypass Access Control

CDHS

- Vulnerable TC
- Dangerous TC
- […]
- […]

Bus

- Arb. Code Execution
- Control Data Interaction

Satellite

Bus-Payload Link

PLCOM

- […]

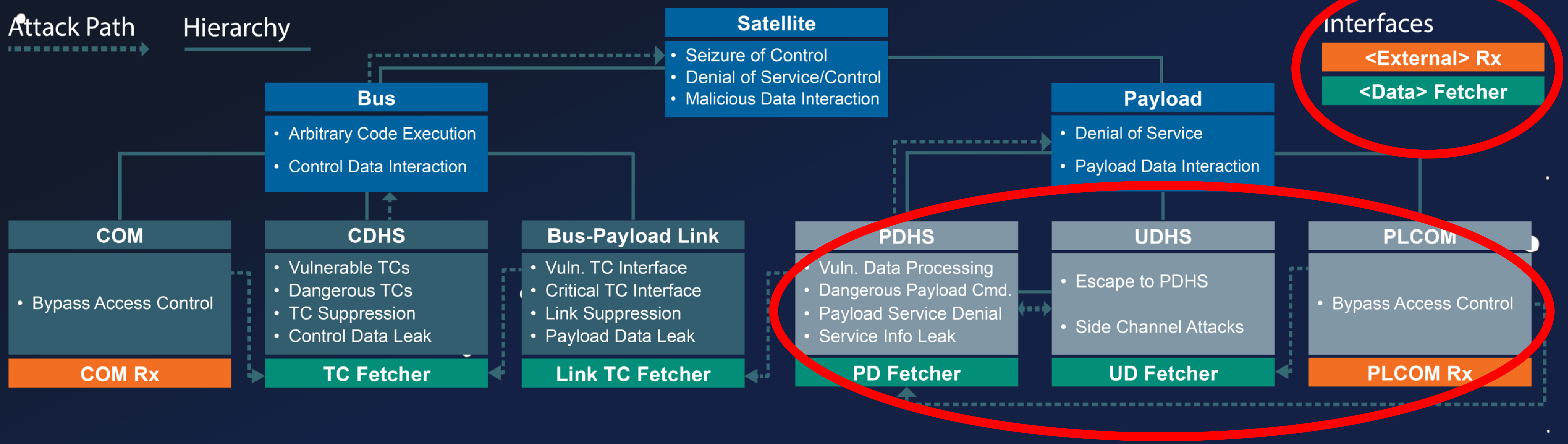
PDHS

- […]

Payload

- Denial of Service
- Payload Data Interaction

More Threats



Attack Path

Hierarchy

Interfaces

<External> Rx

<Data> Fetcher

Satellite
- Seizure of Control
- Denial of Service/Control
- Malicious Data Interaction

Bus
- Arbitrary Code Execution
- Control Data Interaction

Payload
- Denial of Service
- Payload Data Interaction

COM
- Bypass Access Control

COM Rx

CDHS
- Vulnerable TCs
- Dangerous TCs
- TC Suppression
- Control Data Leak

TC Fetcher

Bus-Payload Link
- Vuln. TC Interface
- Critical TC Interface
- Link Suppression
- Payload Data Leak

Link TC Fetcher

PDHS
- Vuln. Data Processing
- Dangerous Payload Cmd.
- Payload Service Denial
- Service Info Leak

PD Fetcher

UDHS
- Escape to PDHS
- Side Channel Attacks

UD Fetcher

PLCOM
- Bypass Access Control

PLCOM Rx

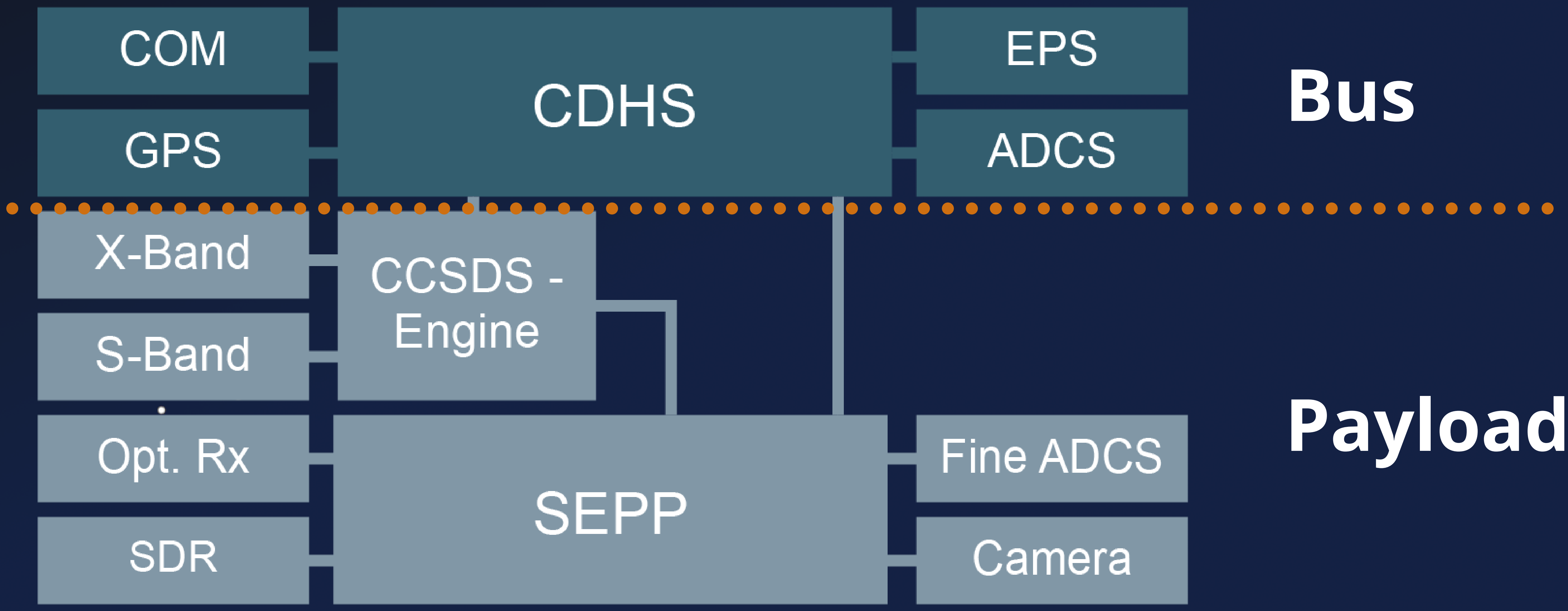
OPS-Sat

①

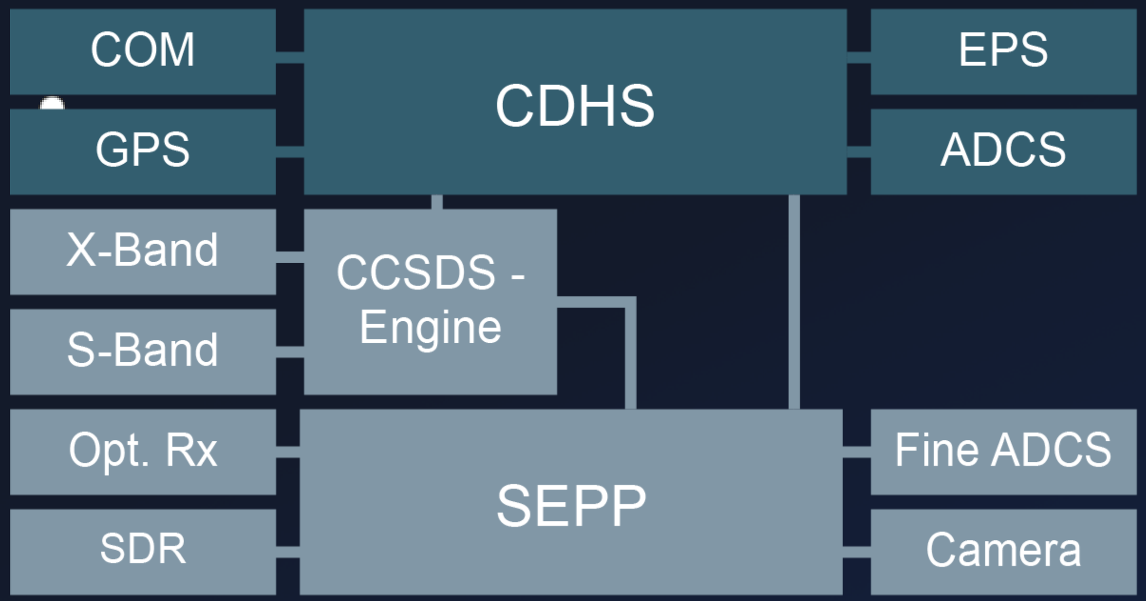
②

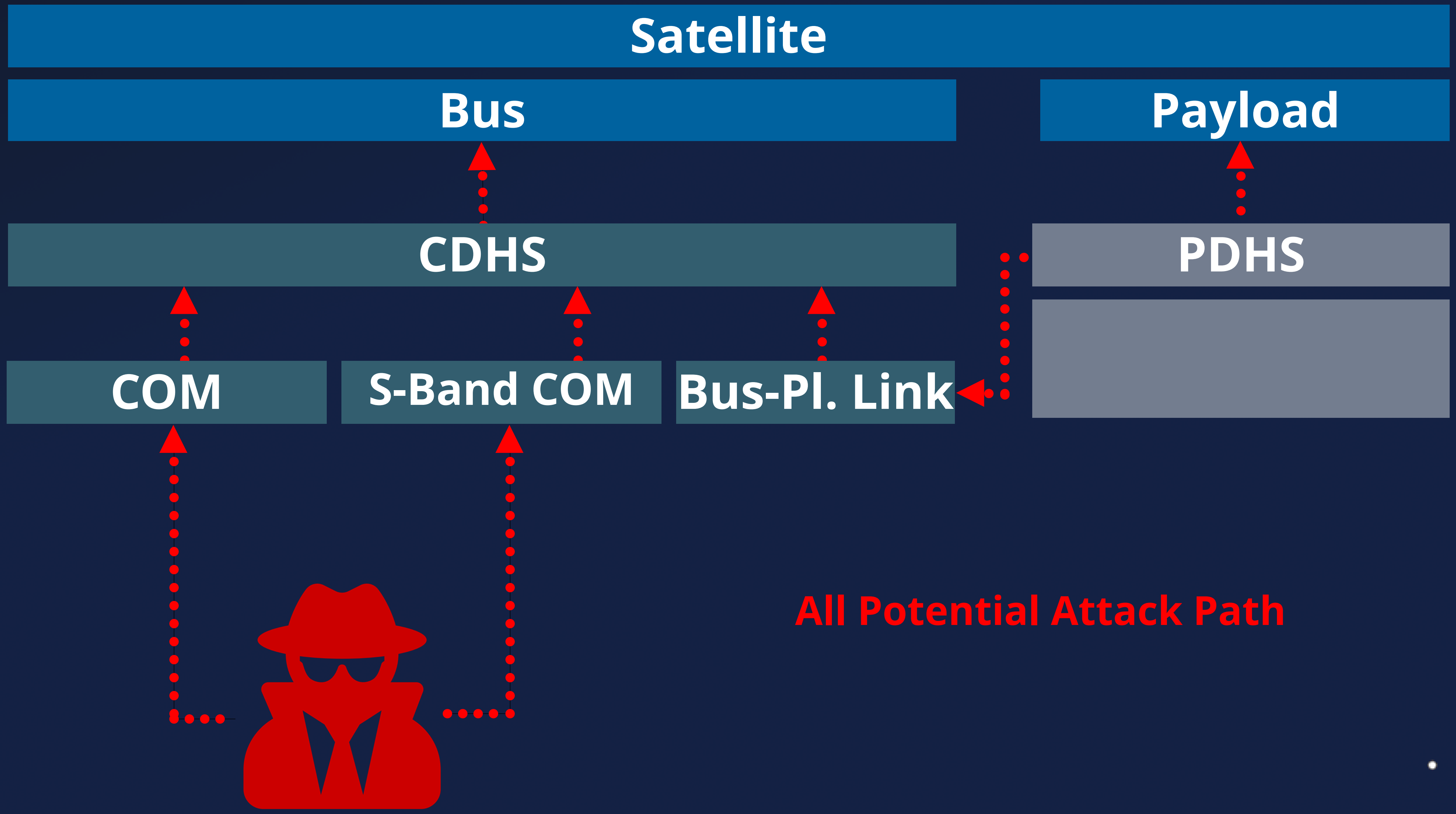
③

OPS-Sat


COM
GPS
CDHS
EPS
ADCS
Bus
X-Band
S-Band
CCSDS - Engine
Opt. Rx
SDR
SEPP
Fine ADCS
Camera
Payload

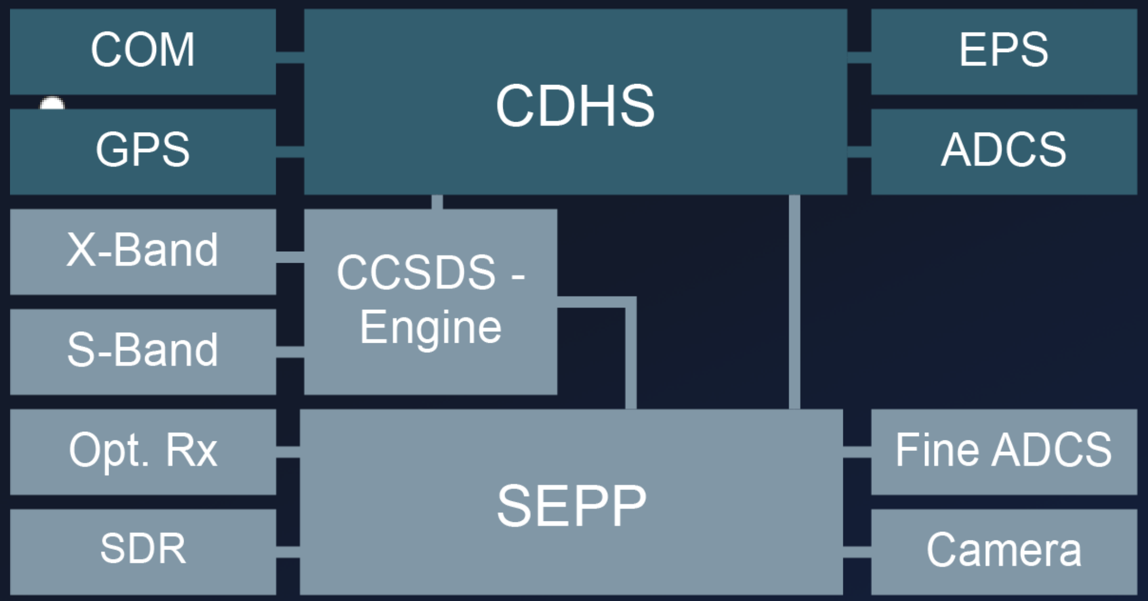
OPS-Sat

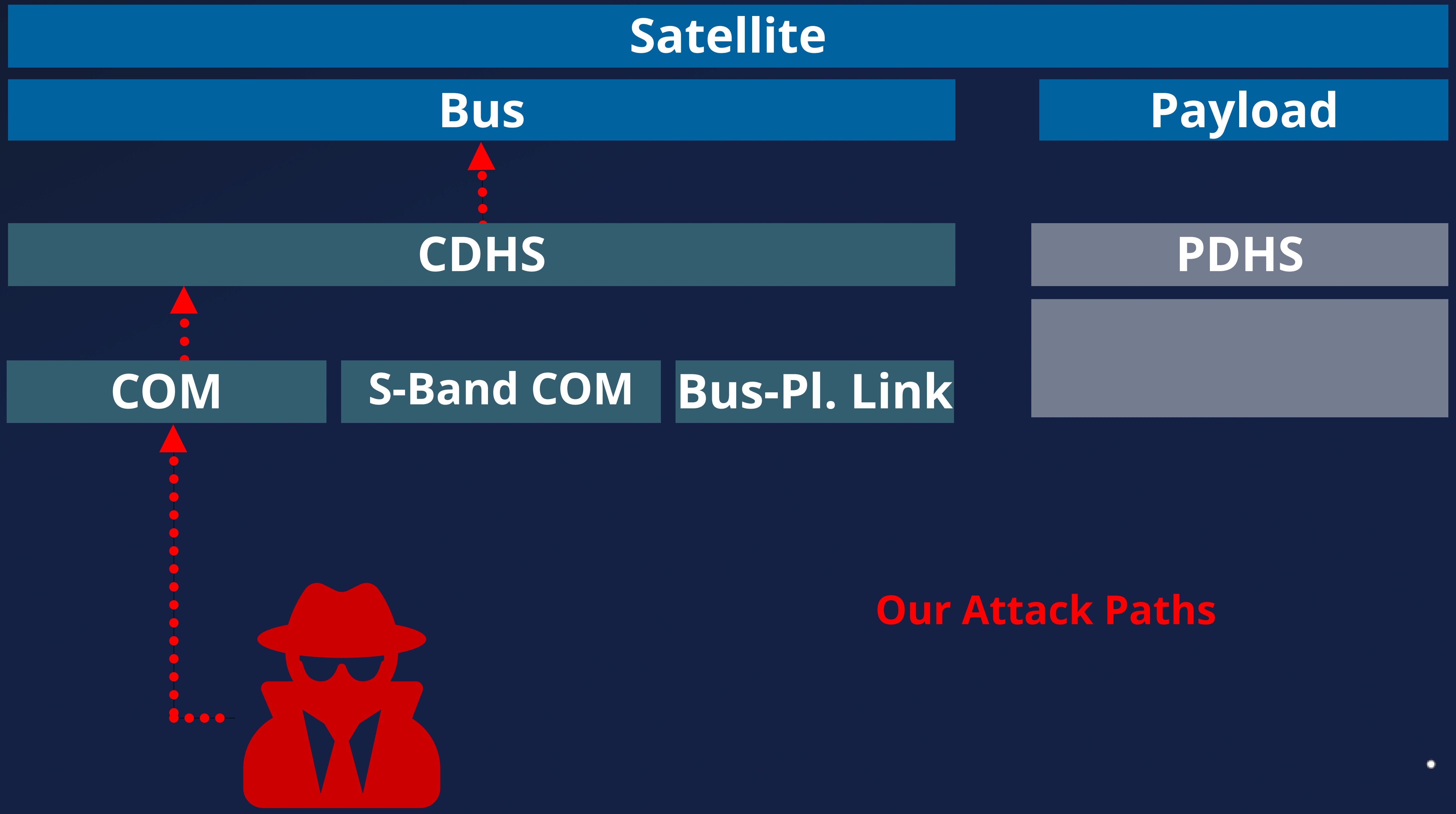




All Potential Attack Path

OPS-Sat





Our Attack Paths

OPS-Sat

COM

- Bypass Access Control
  - Missing Access Control

CDHS

- Vulnerable TC
  - Stack Buffer Overflow

Bus

- Arbitrary Code Execution
  - Missing OS Defenses

Satellite

OPS-Sat

COM

- Bypass Access Control
  - Missing Access Control

CDHS

- Vulnerable TC
  - Stack Buffer Overflow

Bus

- Arbitrary Code Execution
  - Missing OS Defenses

Satellite

Mission accomplished: Control seized

Survey

Space Agencies
Universities
Companies
19
Professionals

Survey

Space Agencies

Universities

Companies

19
Professionals

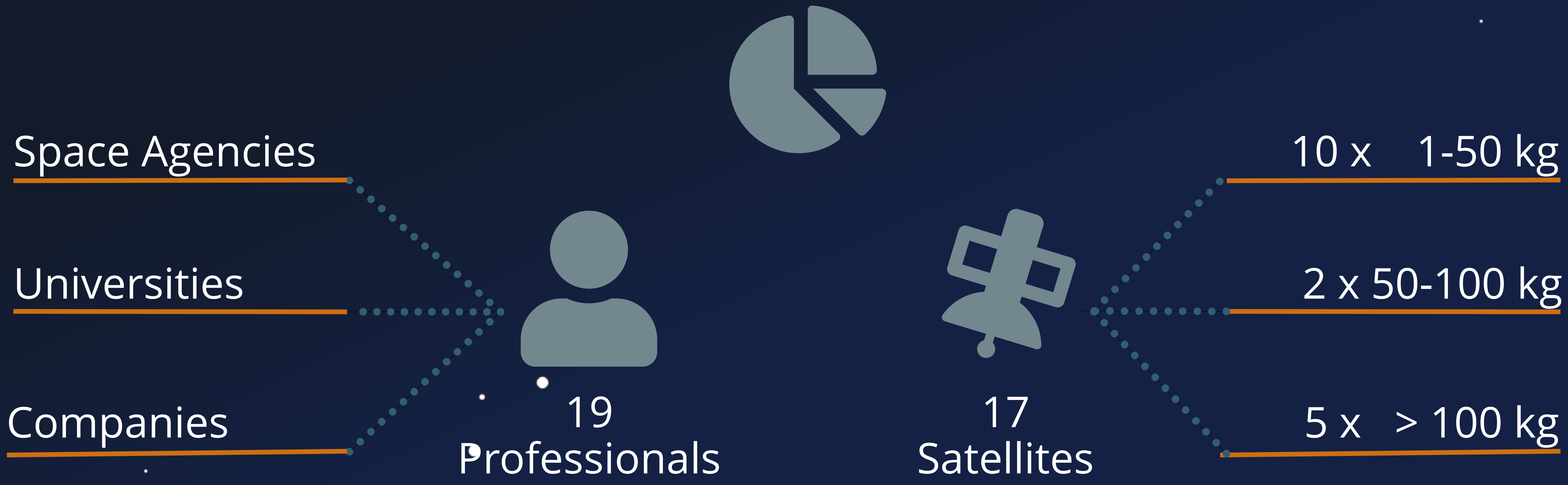
17
Satellites

10 x 1-50 kg

2 x 50-100 kg

5 x > 100 kg

Survey



Space Agencies

Universities

Companies

19 Professionals

17 Satellites

10 x 1-50 kg

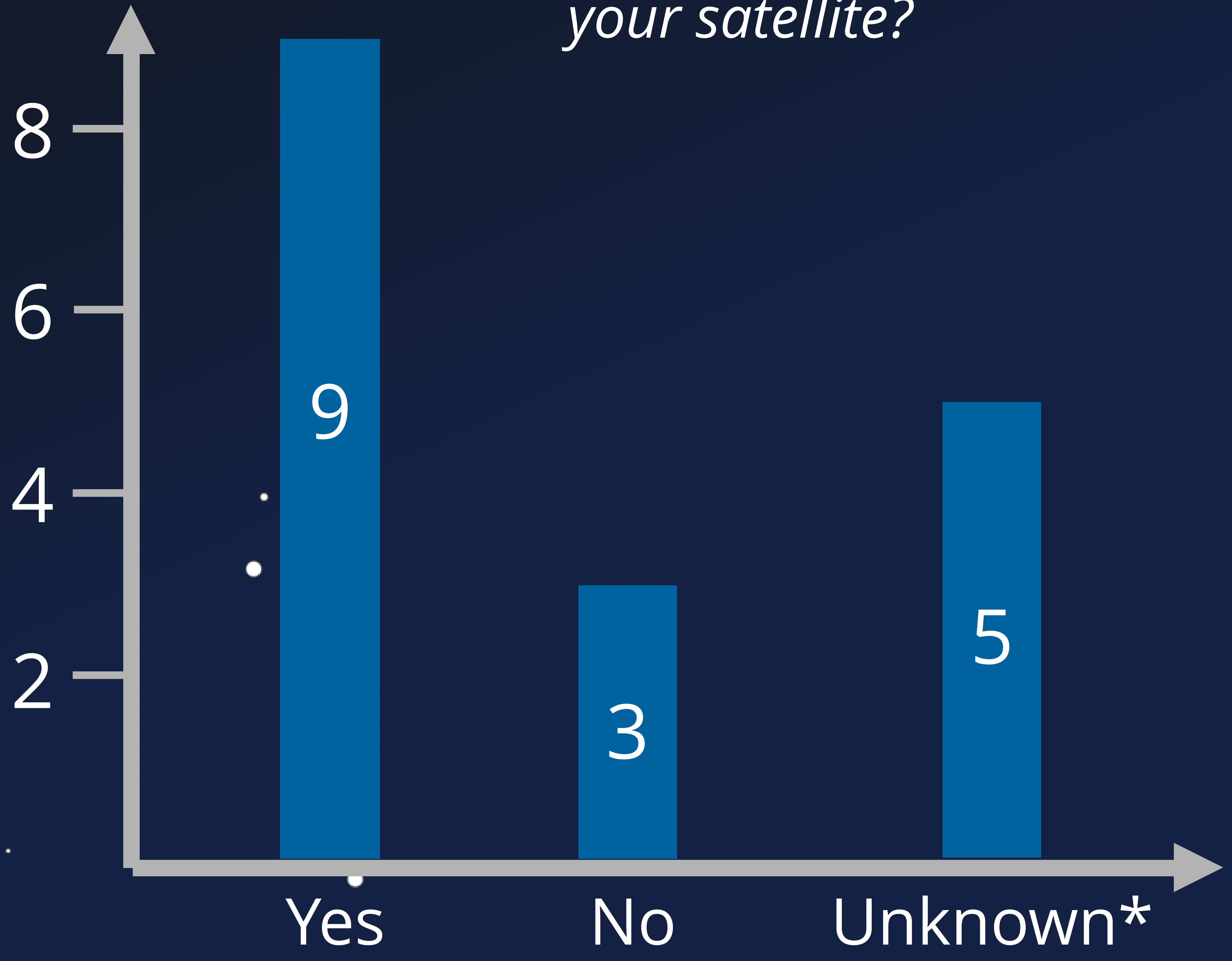
2 x 50-100 kg

5 x > 100 kg

Fully Anonymous

TC Protection

Question: *Are **any measures deployed** to prevent 3rd parties from controlling your satellite?*

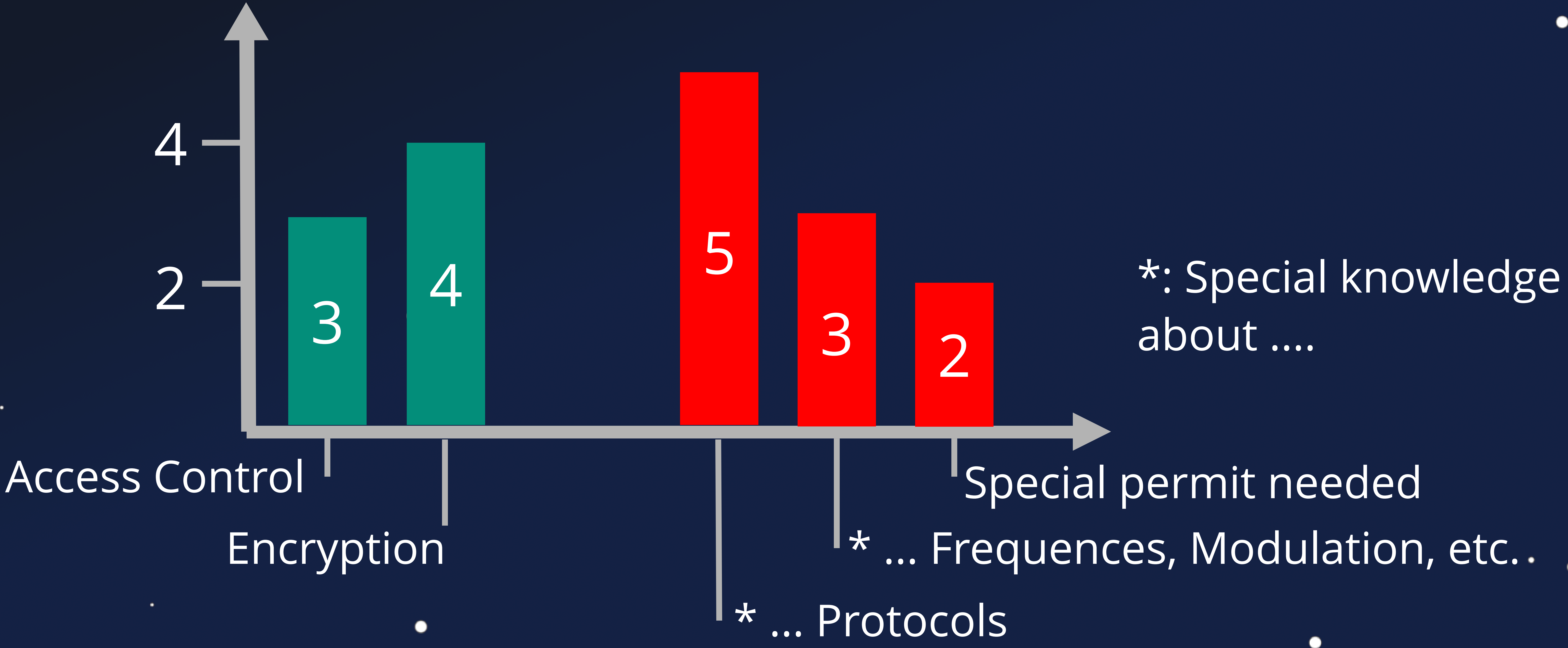


Unknown*:

Prefer not to say / Don't know

TC Obscurity

Question: ***What measures** are deployed to prevent 3rd parties from controlling your satellite? (Multiple Answers)*



Conclusion

Satellite Threat Taxonomy

Security Analysis of 3 Satellites

Survey amongst Professionals

Thanks!

- Satellite Threat Taxonomy
  - External Attacker → COM → CDHS → Seizure of Control
- Security Analysis of 3 Satellites
  - Successful exploitation of several vulnerabilities
  - Missing state-of-the-art defenses
- Survey amongst professionals
  - Supports our results
  - Security-by-obscurity prevails

@jwillbold

/jwillbold

@jwillbold

Johannes Willbold - johannes.willbold@rub.de