

# Interstellar Intruders

---

Hijacking Satellites through Firmware Vulnerabilities

Johannes Willbold



# \$whoami

---

RUHR  
UNIVERSITÄT  
BOCHUM

RUB



- Satellite & Space Systems Security
- Doctoral Student
  - Ruhr University Bochum, DE
- Visiting Researcher
  - Cyber-Defence Campus, CH
- General Chair @ SpaceSec Workshop
- Subgroup Chair @ IEEE SA Space System Cybersecurity Working Group
- Hack-a-Sat 2 & 4 Finals

# Space Odyssey

## Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold\*, Moritz Schloegel\*<sup>‡</sup>, Manuel Vögele\*, Maximilian Gerhardt\*,  
Thorsten Holz<sup>‡</sup>, Ali Abbasi<sup>‡</sup>

\*Ruhr University Bochum, *firstname.lastname@rub.de*

<sup>‡</sup>CISPA Helmholtz Center for Information Security, *lastname@cispa.de*



**Distinguished  
Paper Award**

**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 This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.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].

44th IEEE Symposium on Security and Privacy (S&P)



# Applications

---



Telecommunications



Global Positioning



Earth Observation



Research



Technology Testing



# Context

---

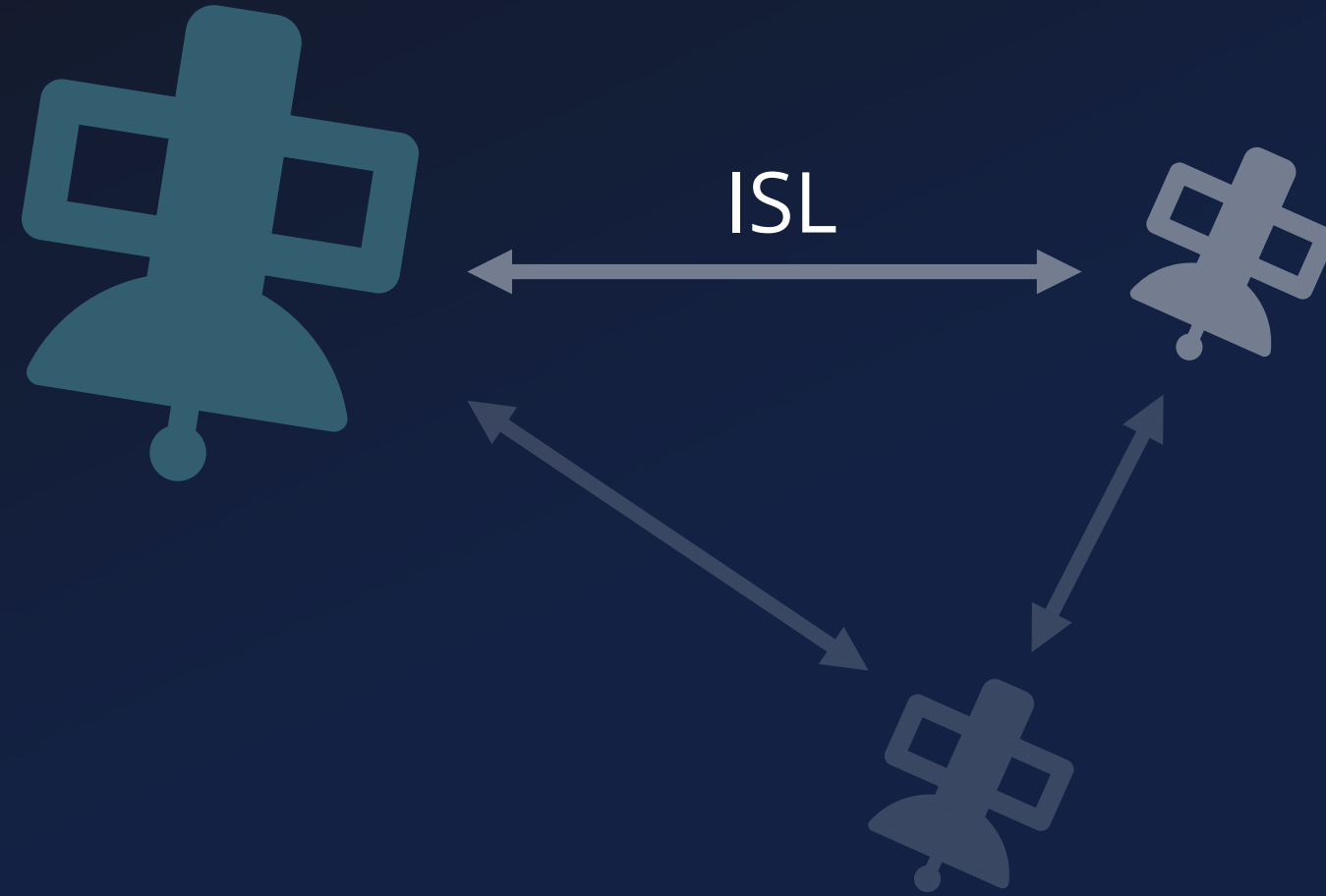
Space Segment



# Context

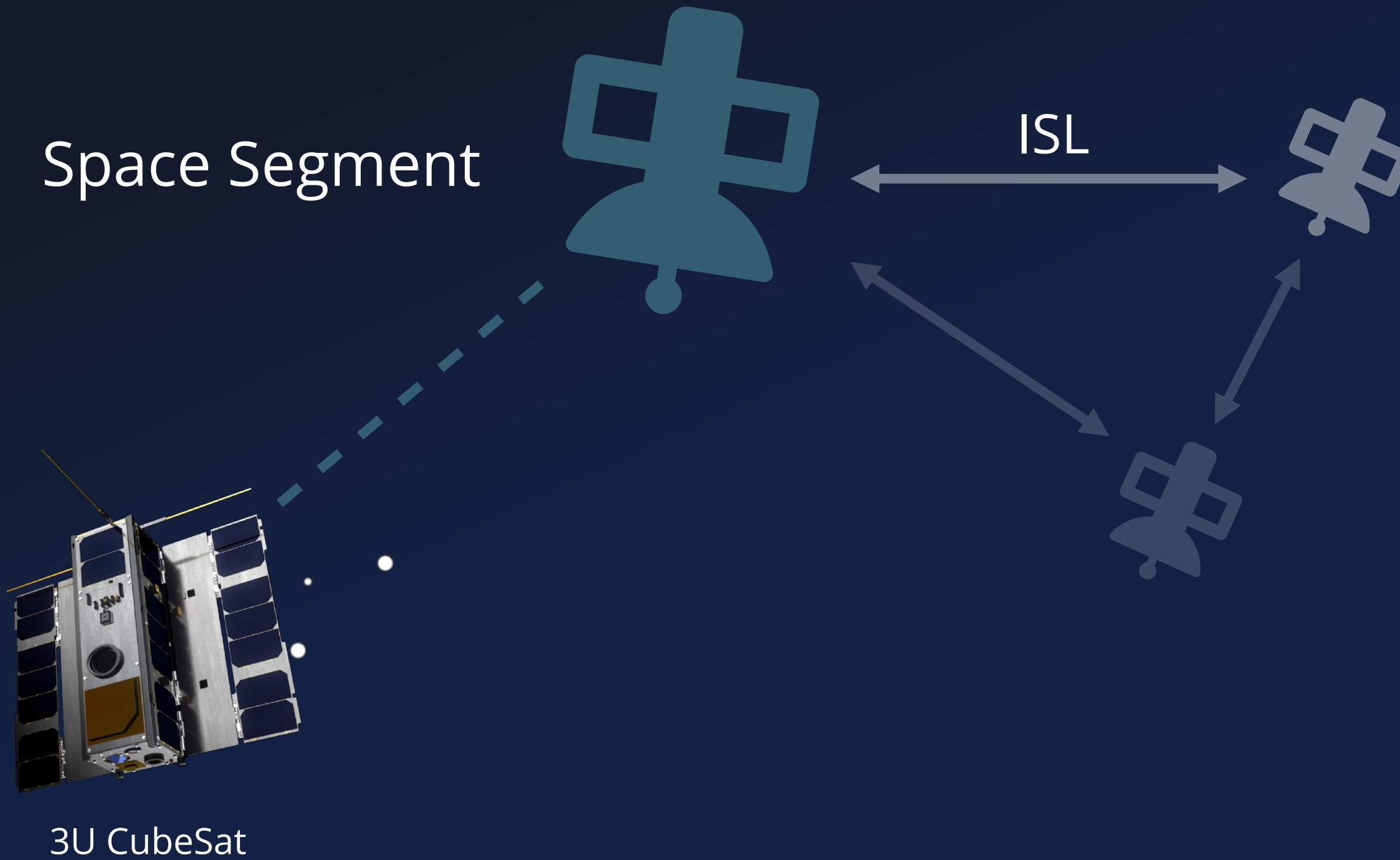
---

Space Segment



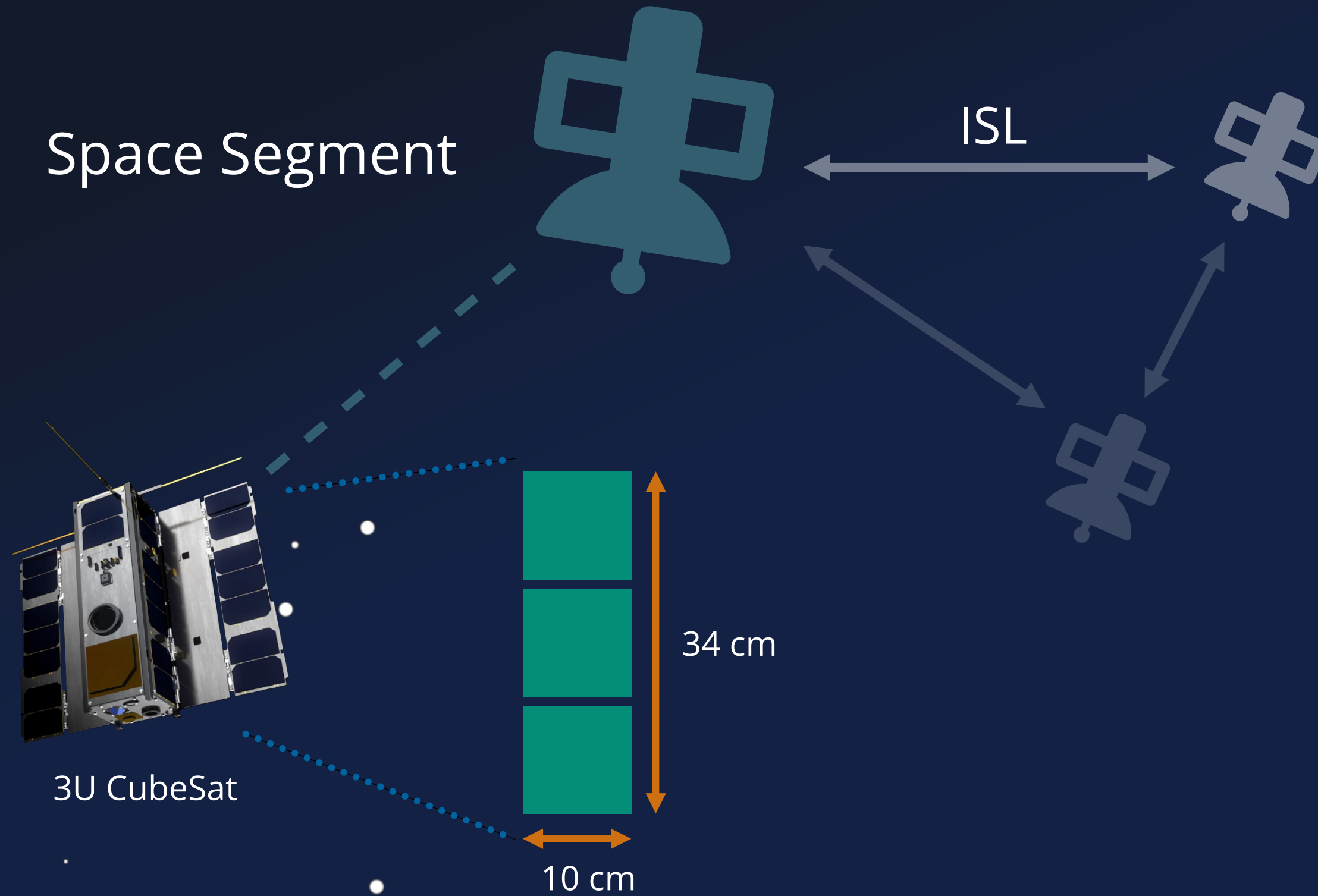
# Context

---



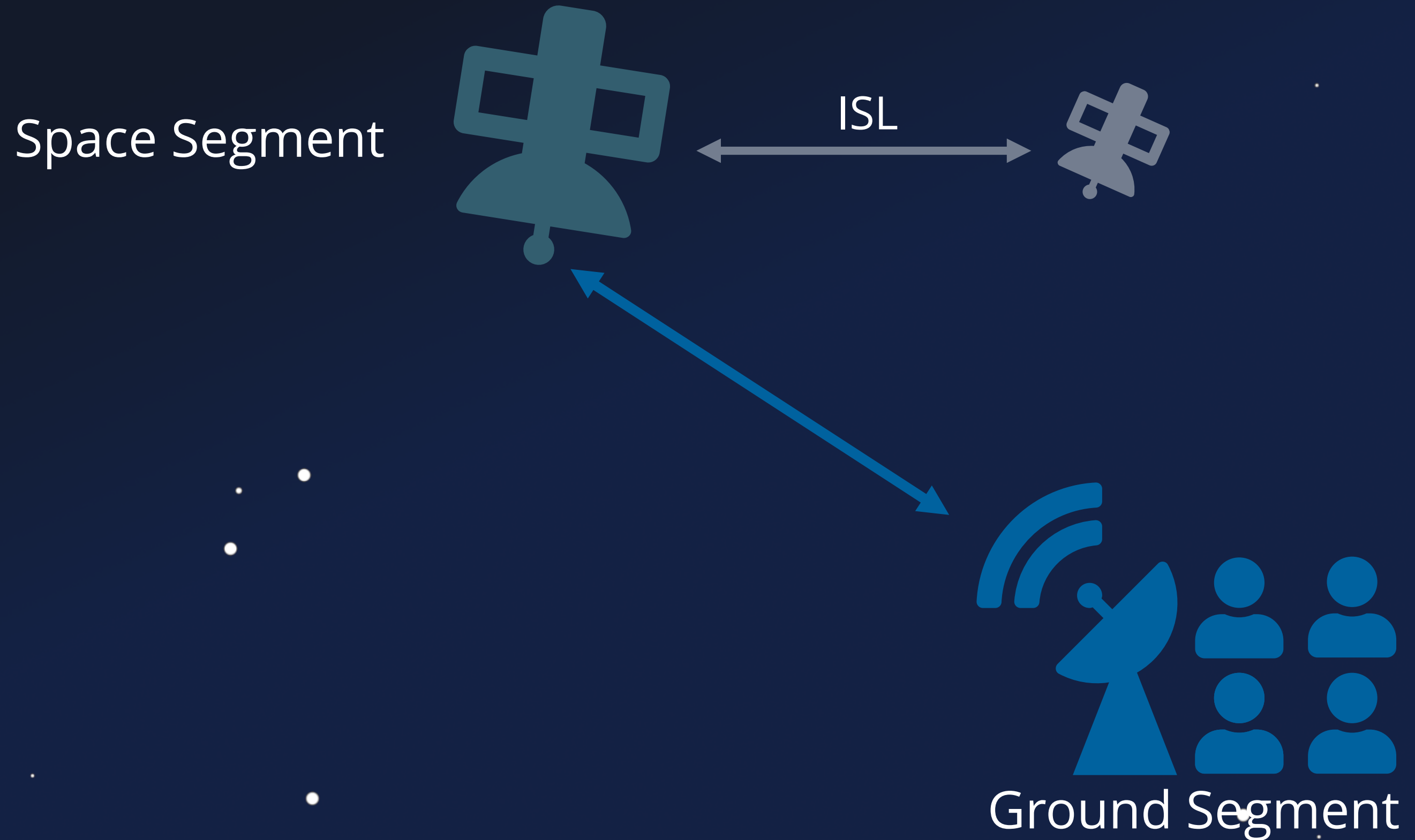


# Context



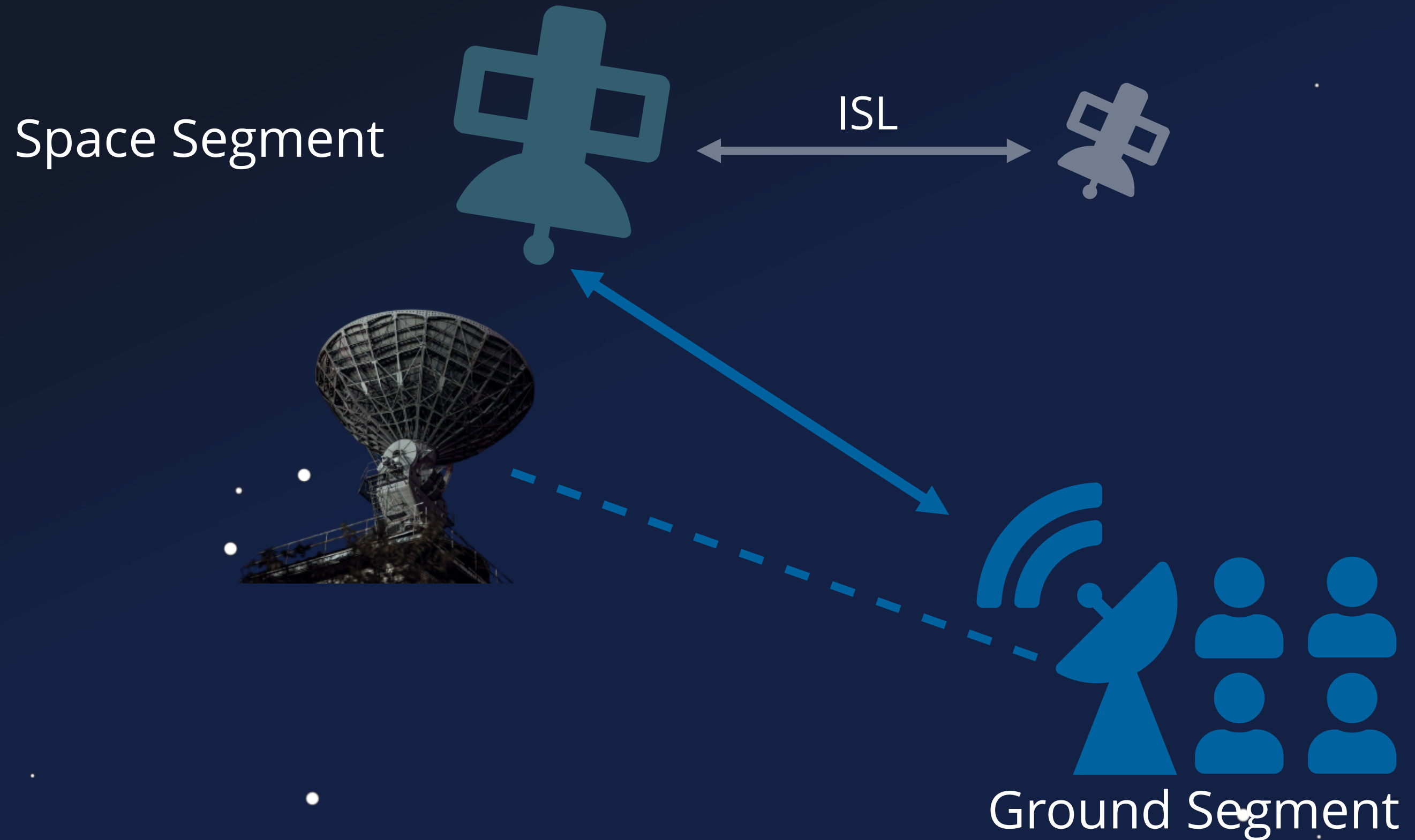
# Context

---



# Context

---





# Context

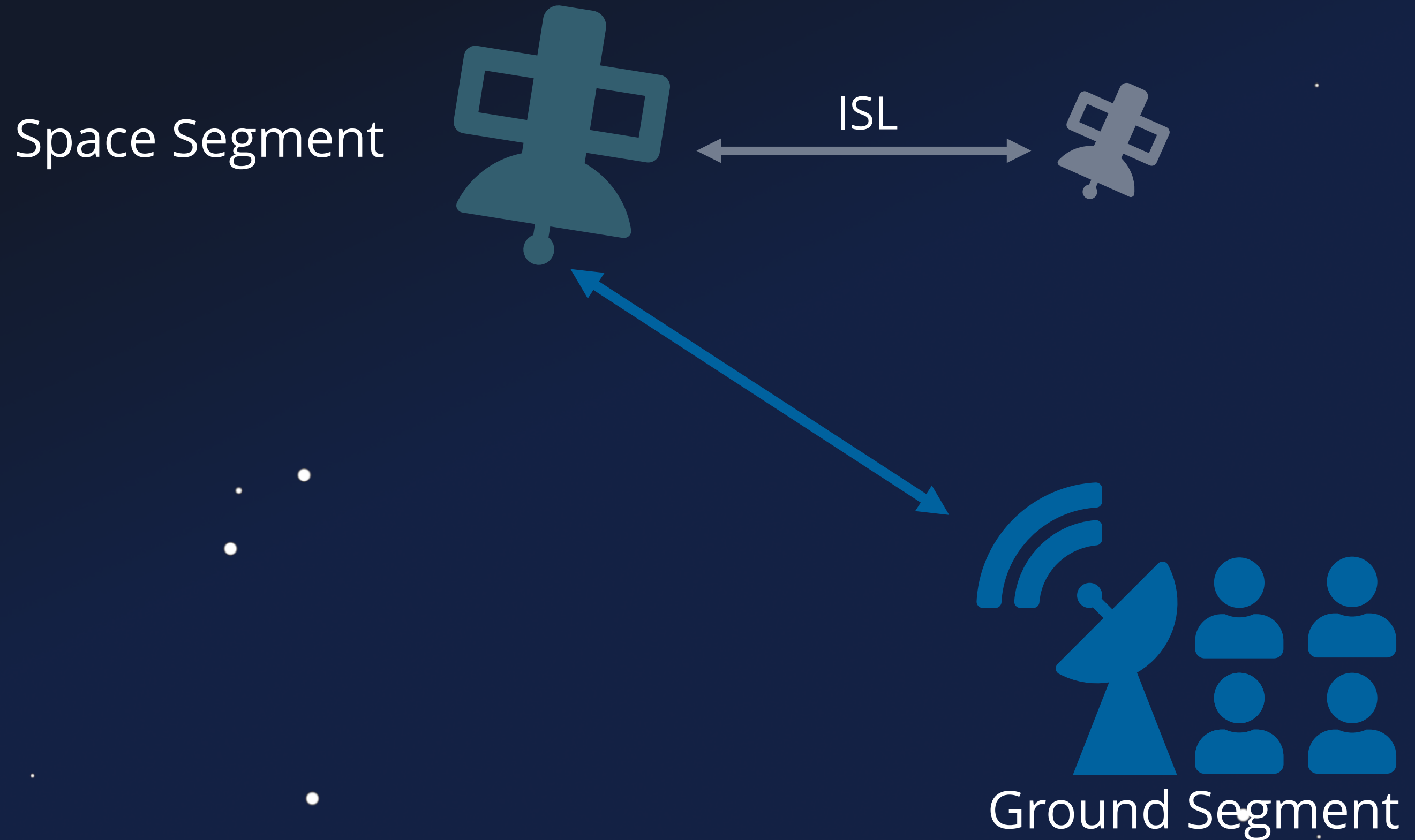
Space Segment



Ground Segment

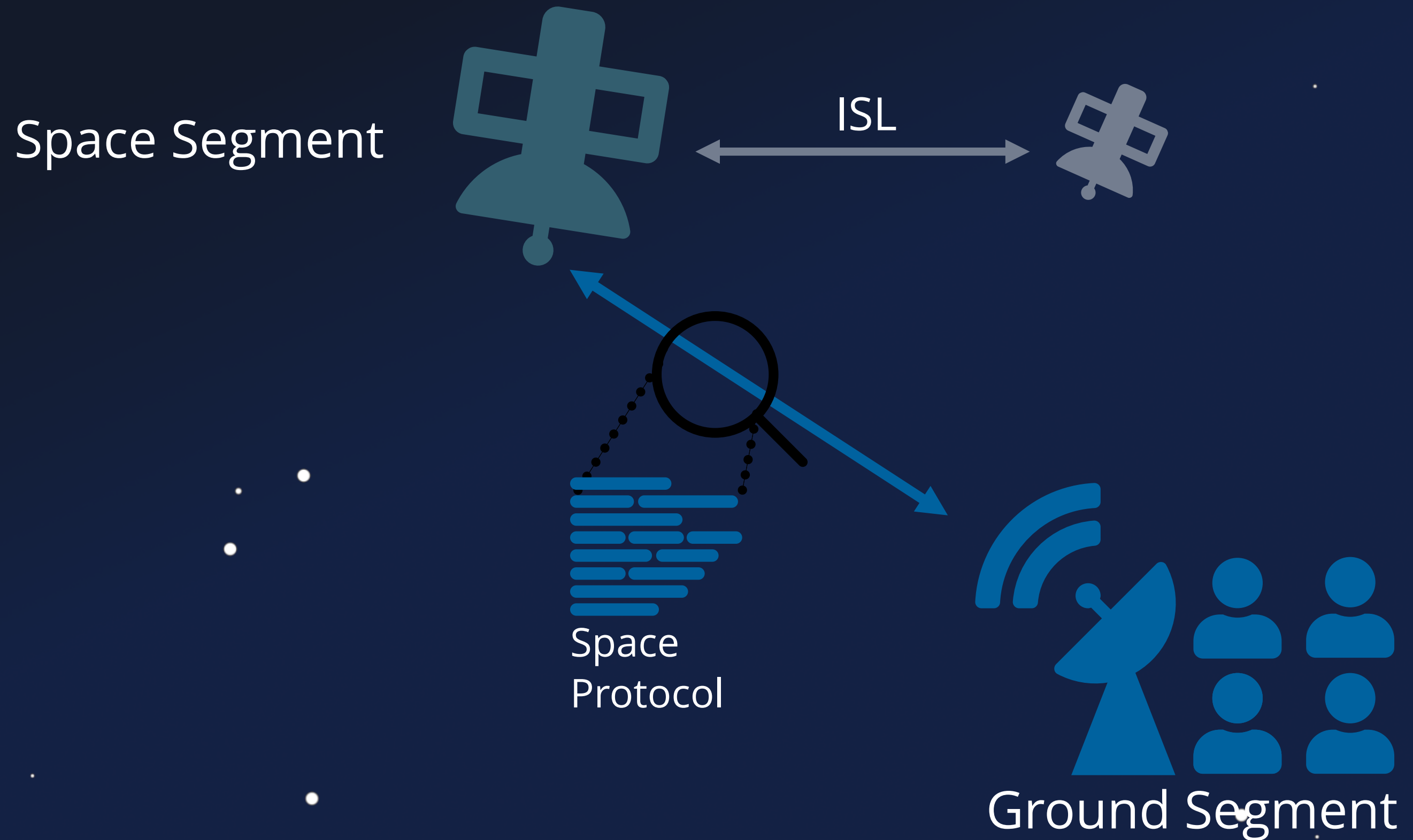
# Context

---



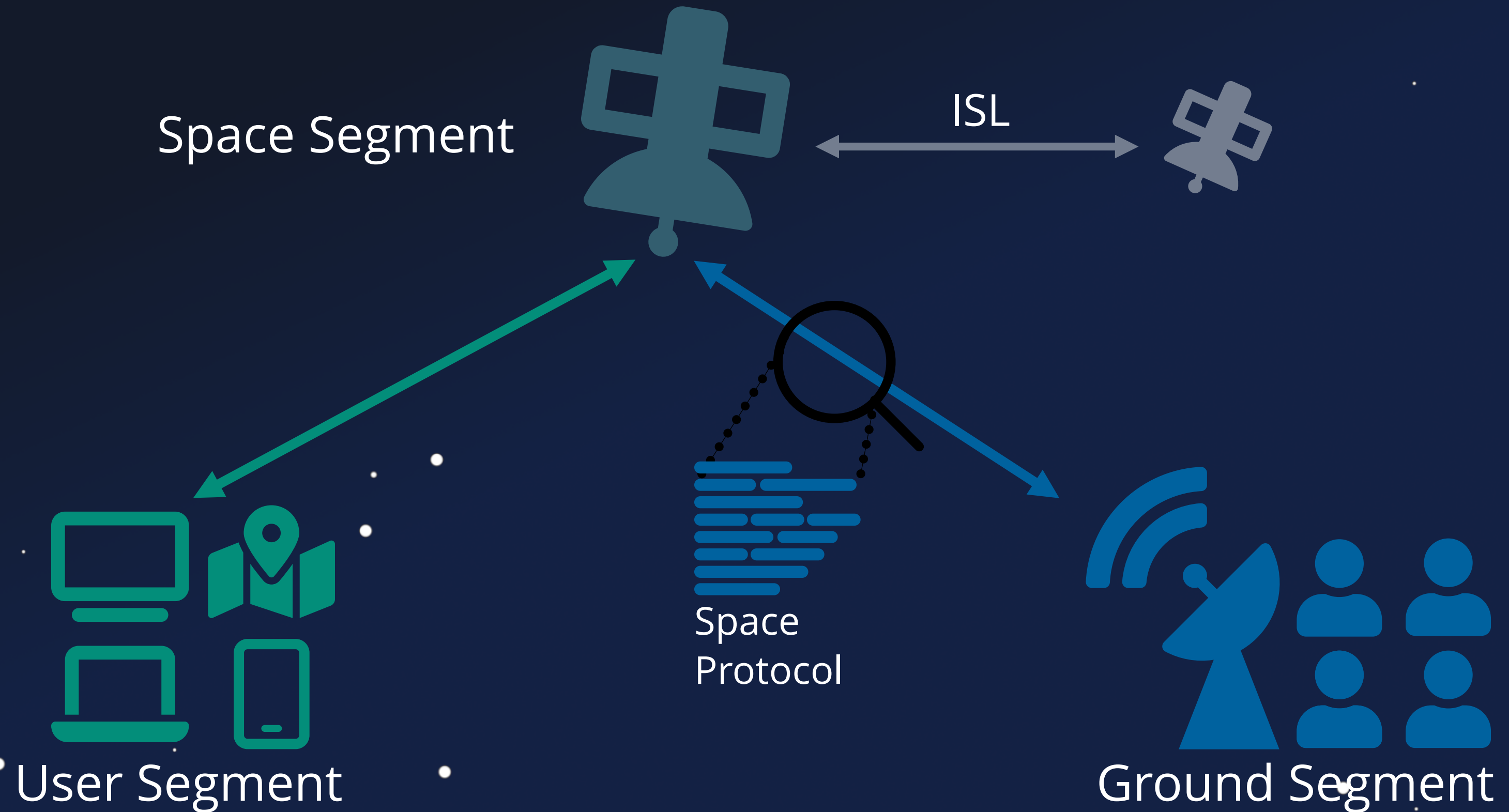
# Context

---





# Context



# Our Journey ...

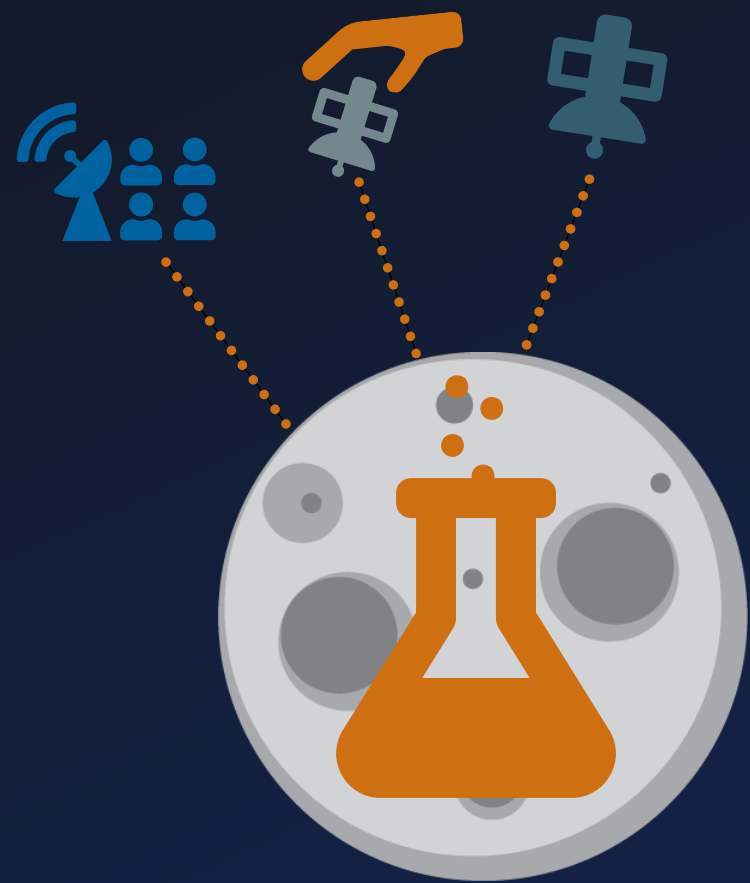
---



Firmware Attacks

# Our Journey ...

---



Firmware Attacks



# Our Journey ...

---

System Analysis



Firmware Attacks

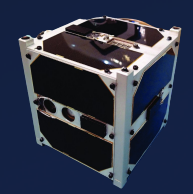
# Our Journey ...

---

System Analysis



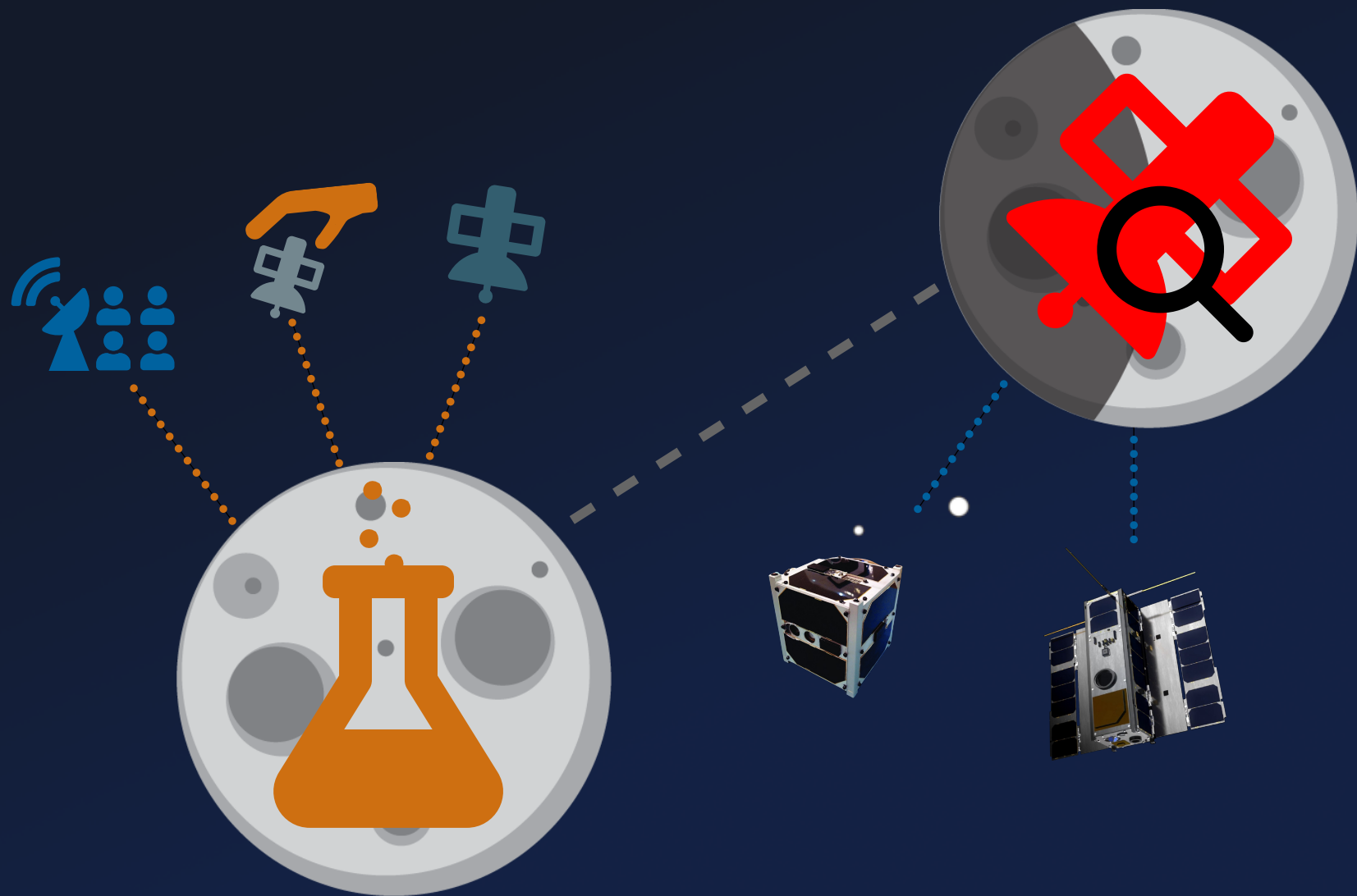
Firmware Attacks



# Our Journey ...

---

System Analysis



Firmware Attacks

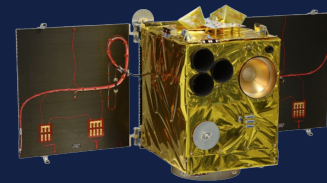
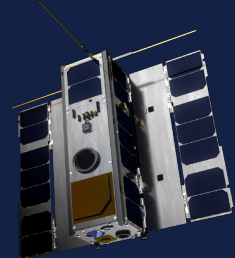
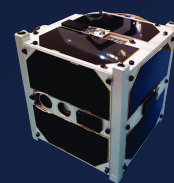
# Our Journey ...

---

System Analysis



Firmware Attacks





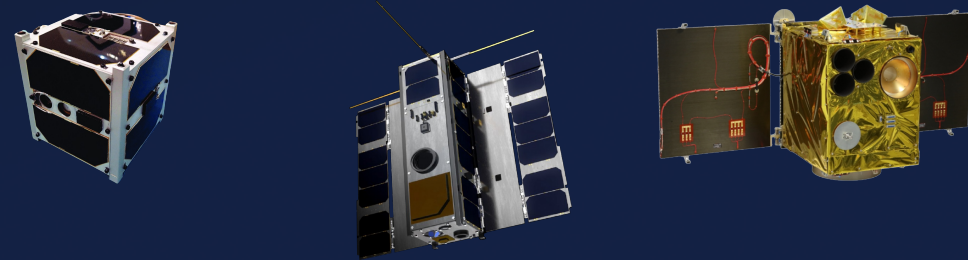
# Our Journey ...

---

System Analysis



Firmware Attacks



Survey

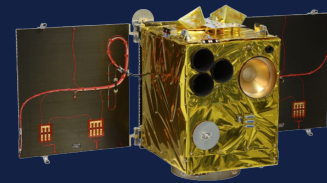
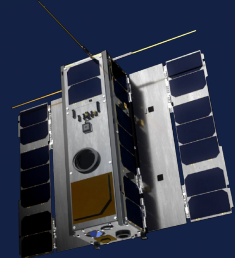
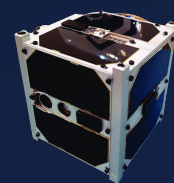
# Our Journey ...

---

System Analysis



Firmware Attacks



Survey

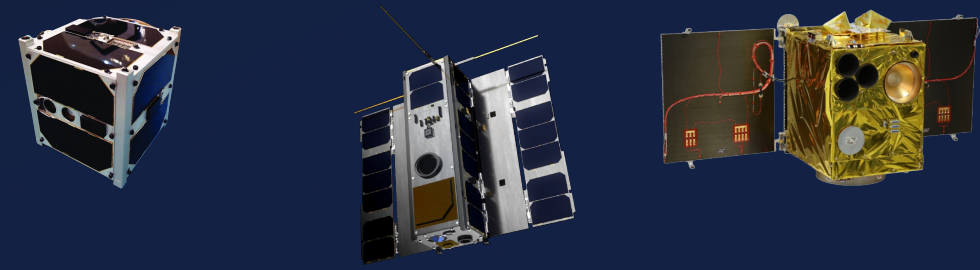
# Our Journey ...

---

## System Analysis



Firmware Attacks

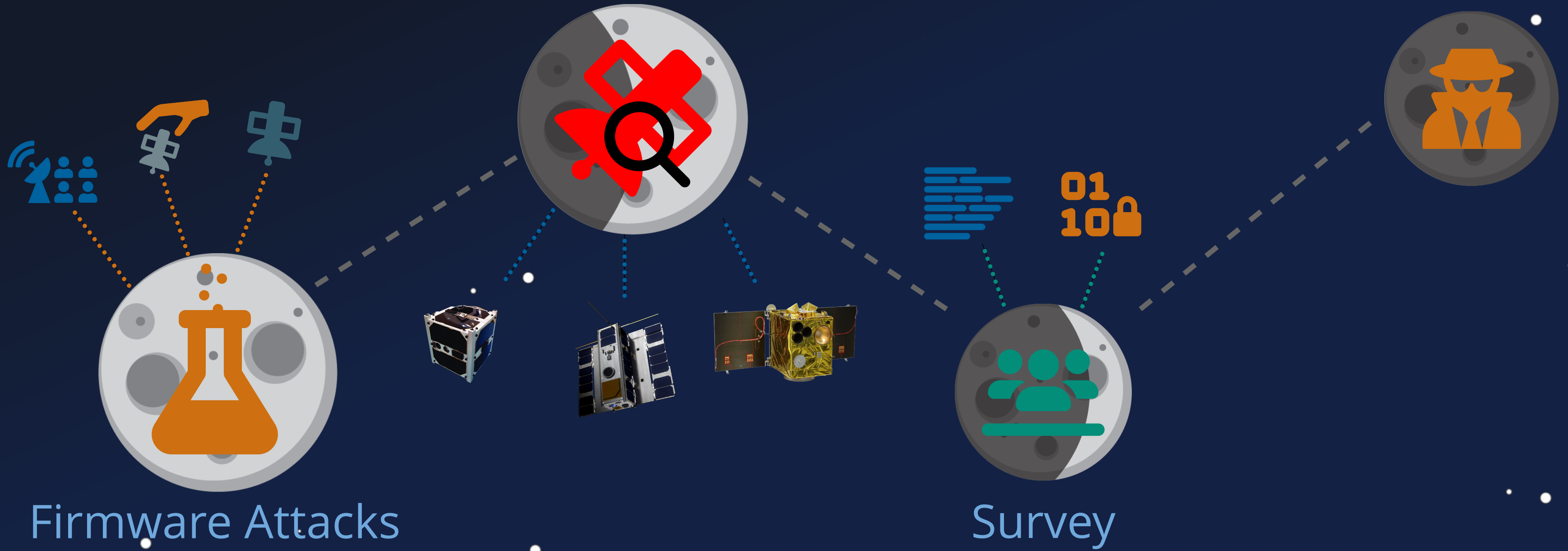


Survey

# Our Journey ...

System Analysis

Attacker Perspective

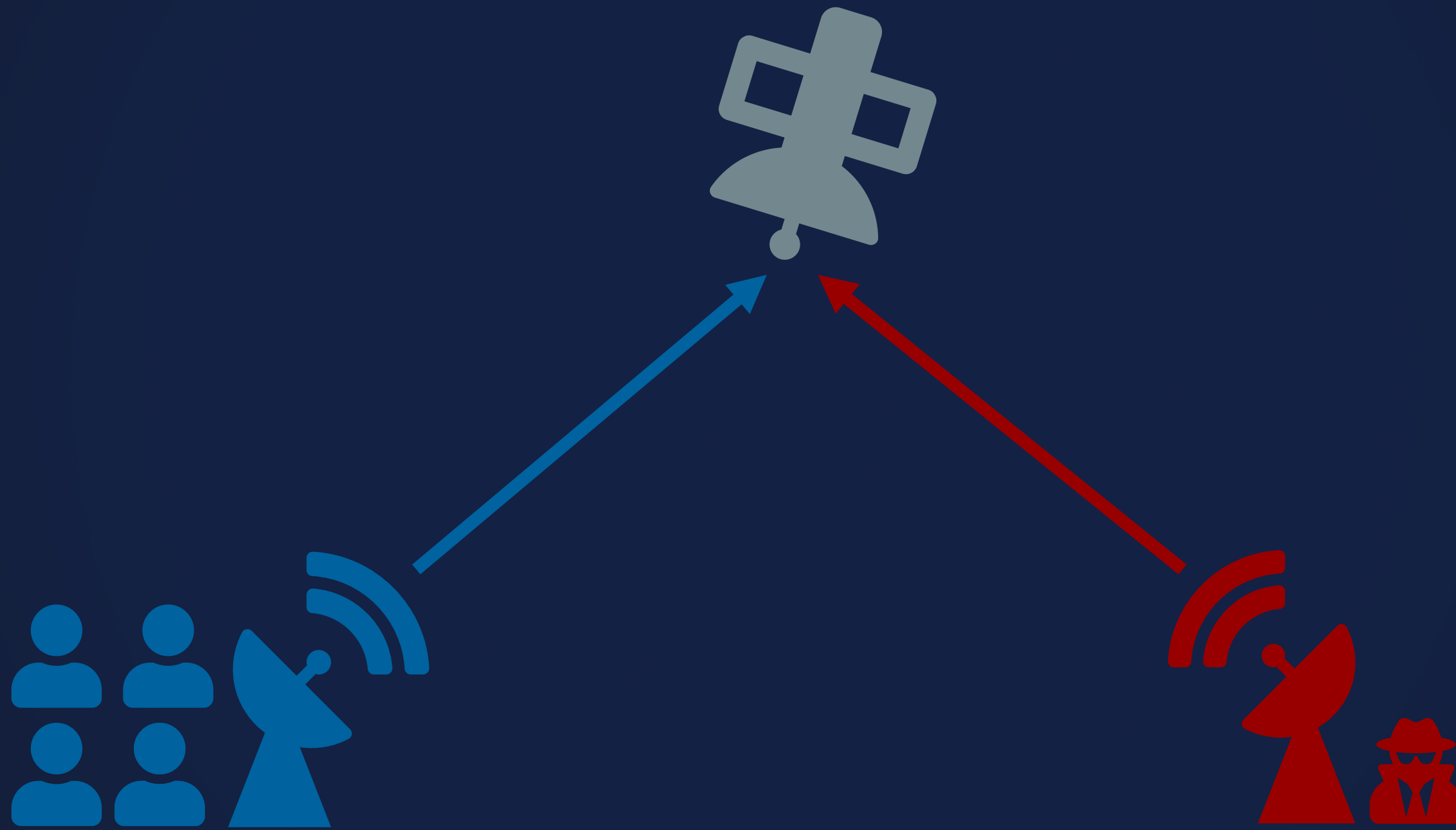


Firmware Attacks

Survey

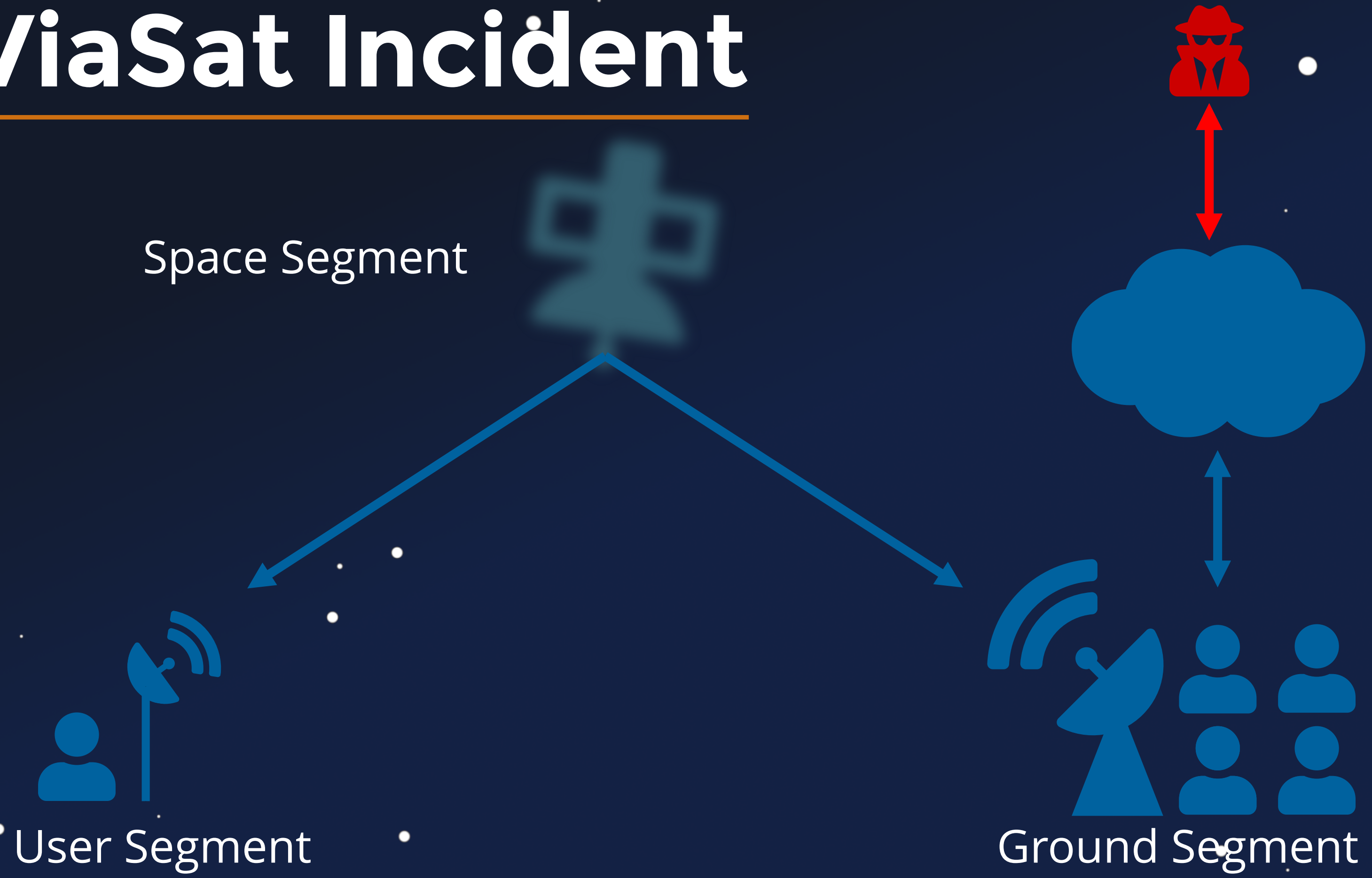


# Firmware Attacks



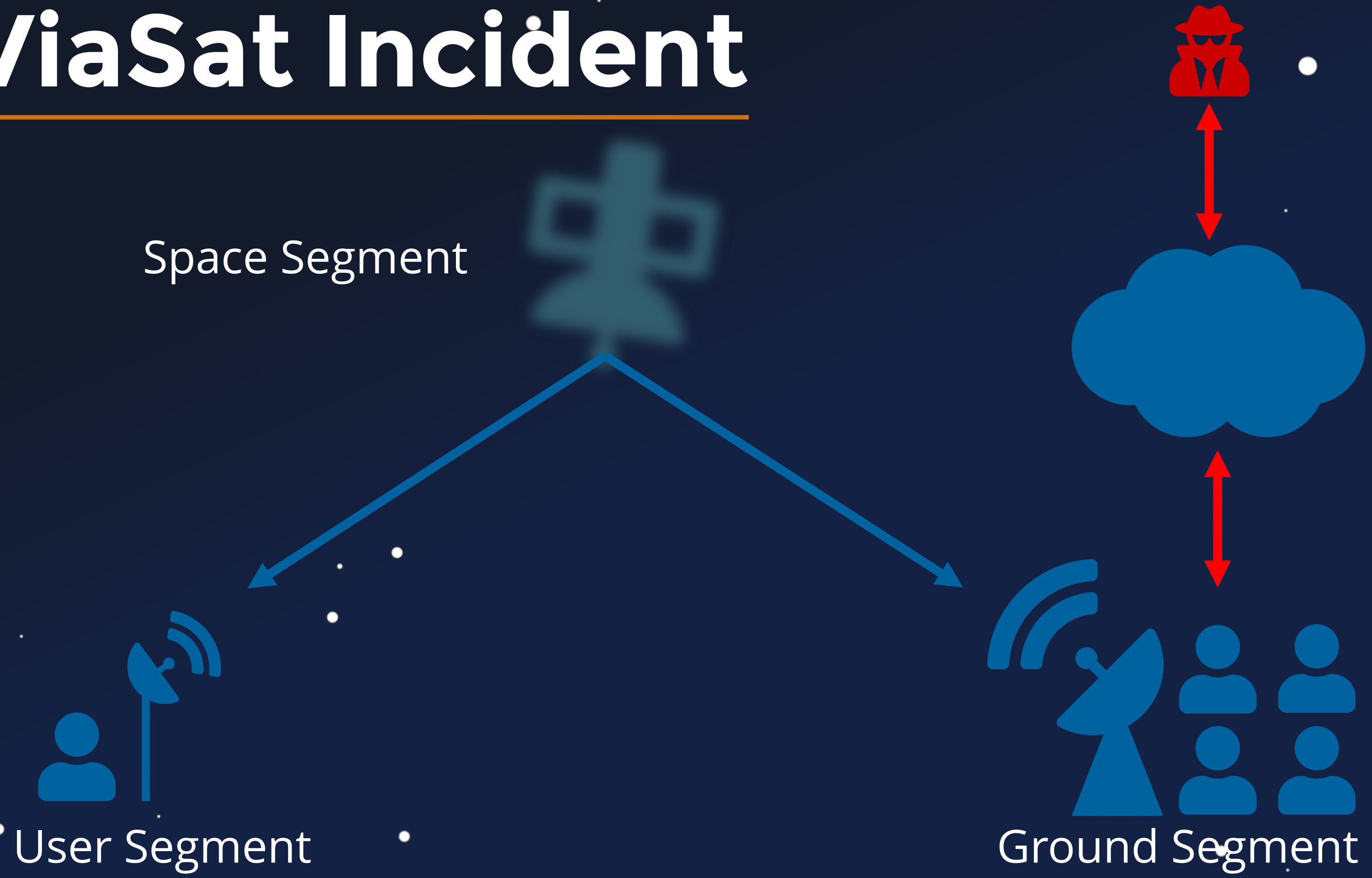
# ViaSat Incident

---



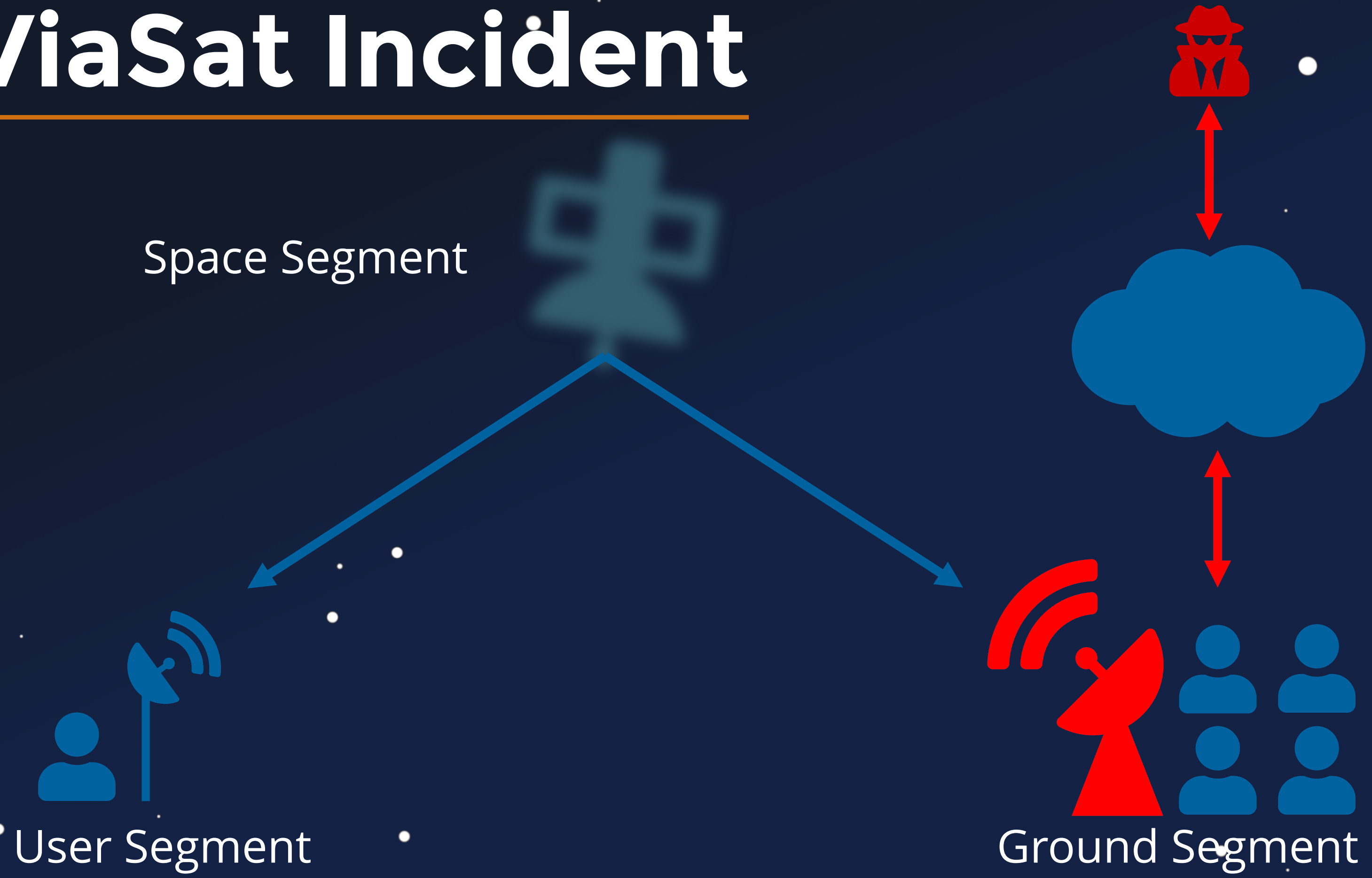
# ViaSat Incident

---



# ViaSat Incident

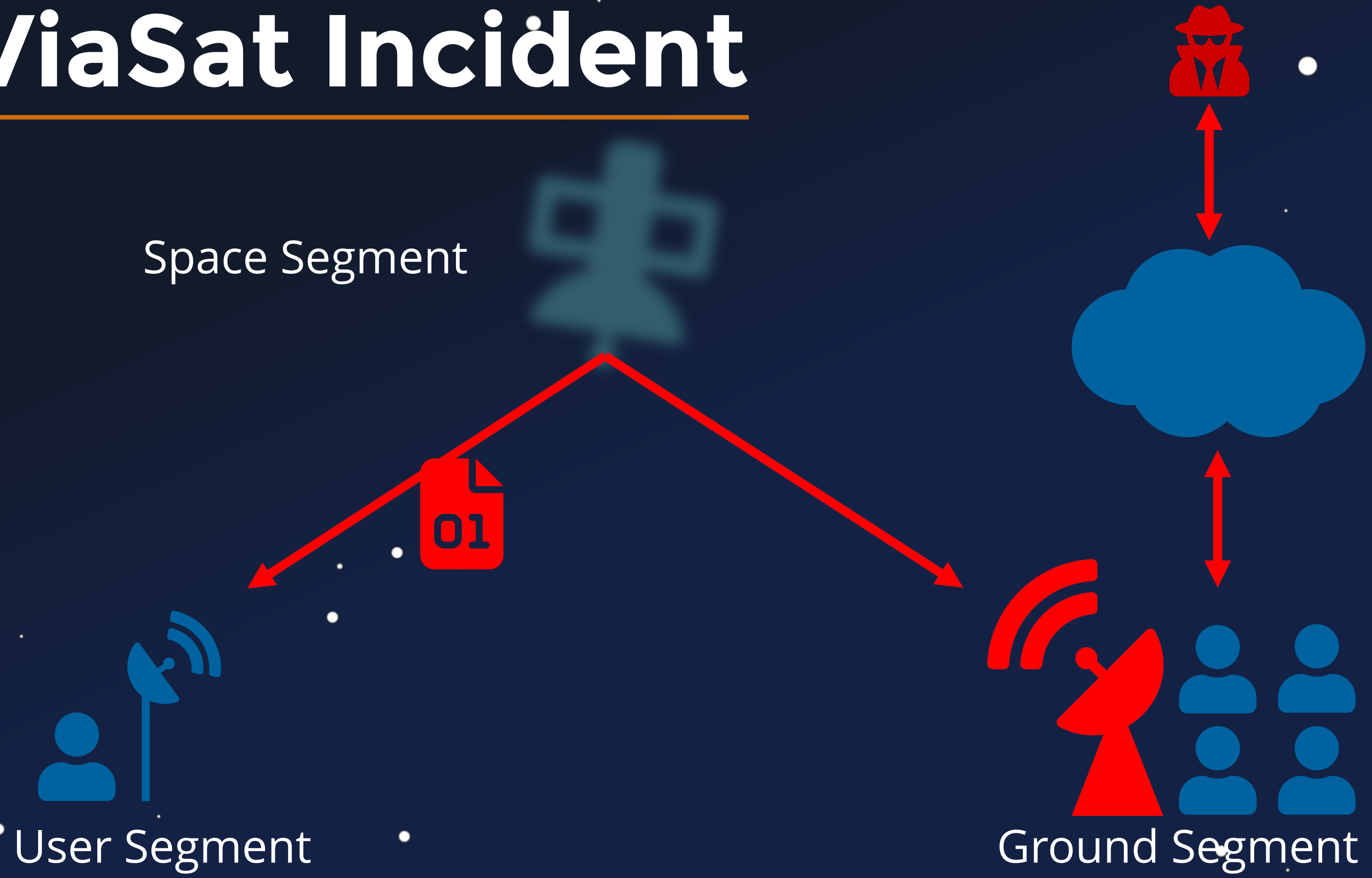
---





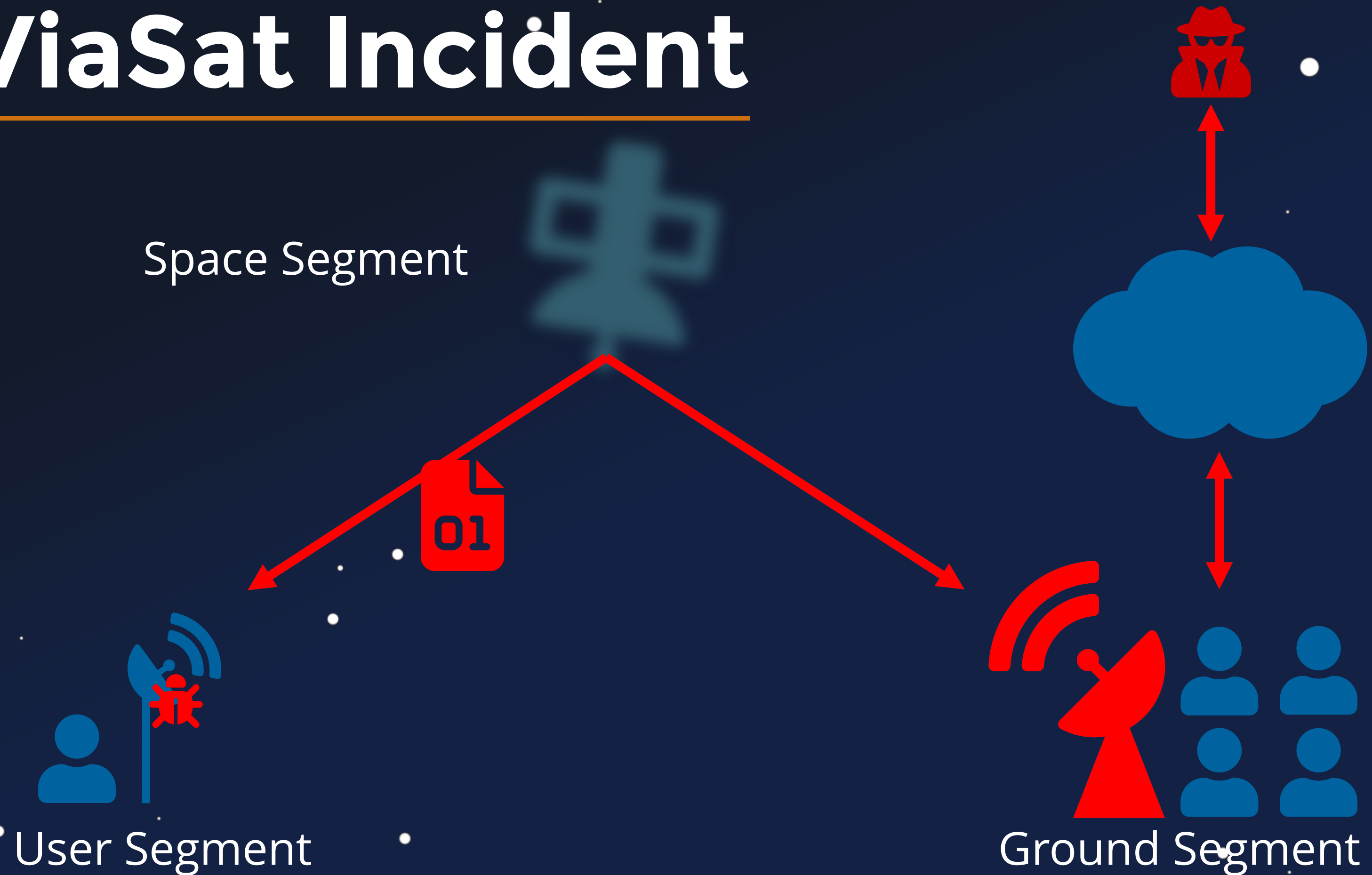
# ViaSat Incident

---



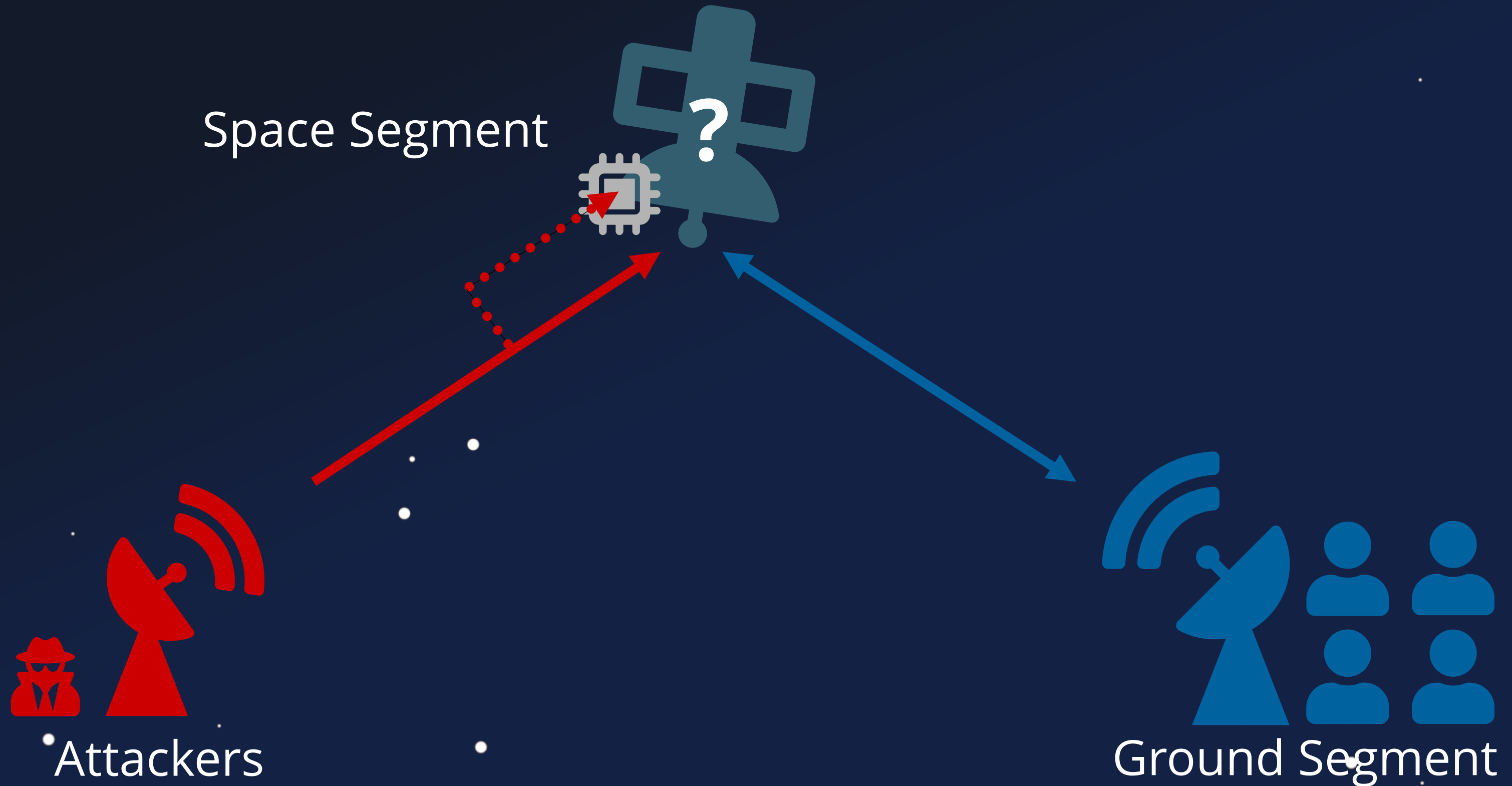
# ViaSat Incident

---



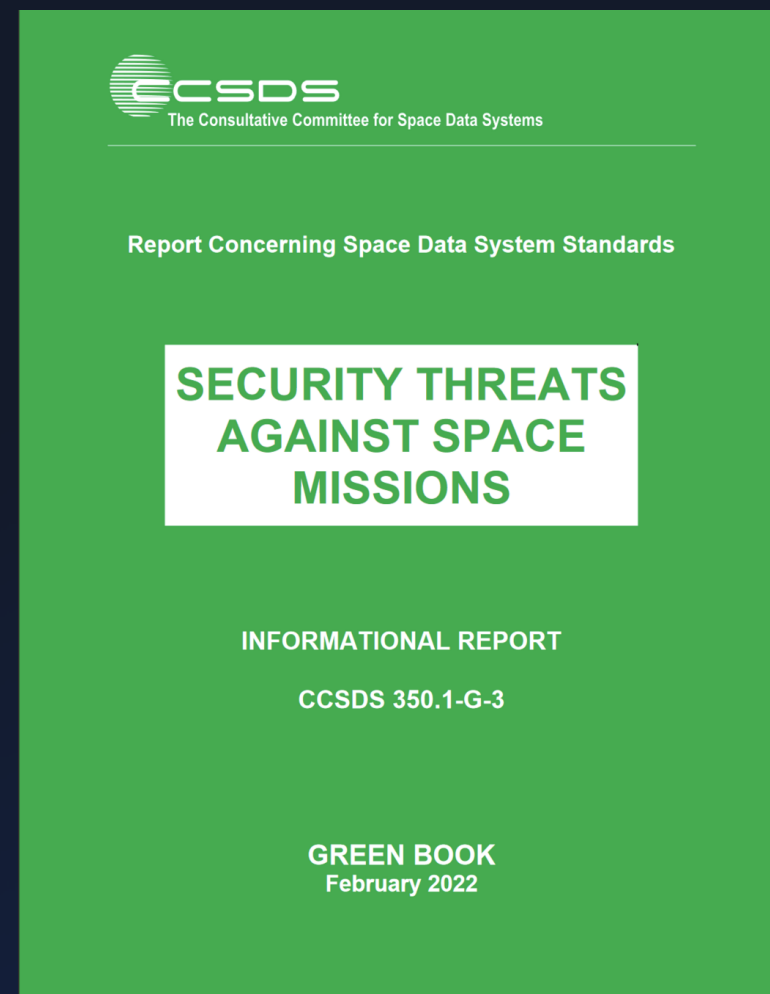
# Firmware Attacks

---



# Not so Novel

---





# Not so Novel

## 3.4.8 REPLAY

**Applicable to:** Space Segment, Ground Segment, Space-Link Communication.

**Description:** Transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

**Possible Mission Impact:** If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to the originally intended destination, they might be executed, potentially at a later time. If the replayed commands are not rejected, they could result in duplicate spacecraft operations, such as a maneuver of a spacecraft re-orientation, with the result that a spacecraft is in an unintended orientation (e.g., tumbling, antennas pointed in the wrong direction, solar arrays pointed away from the sun, the reset of critical onboard parameters).

## 3.4.9 SOFTWARE THREATS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or unvetted software that might contain bugs, viruses, or spyware, which could result in system instability. System operators might misconfigure a system resulting in security weaknesses. Programmers may introduce logic or implementation errors that could result in system vulnerabilities, or instability/reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

**Possible Mission Impact:** Software threats could result in loss of data and safety issues, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

## 3.4.10 UNAUTHORIZED ACCESS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

**Possible Mission Impact:** An access control breach would allow an unauthorized entity to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, execute unauthorized commands aboard a crewed mission, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.

# Not so Novel

CCSDS REPORT CONCERNING SECURITY THREATS AGAINST SPACE MISSIONS

3.4.8 REPLAY

**Applicable to:** Space Segment, Ground Segment, Space-Link Communication.

**Description:** Transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

**Possible Mission Impact:** If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to the spacecraft at an unintended destination, they might be executed, potentially at a later time. If the replayed commands are not rejected, they could result in duplicate spacecraft operations, such as a maneuver of a spacecraft re-orientation, with the result that a spacecraft is in an unintended orientation (e.g., tumbling, antennas pointed in the wrong direction, solar arrays pointed away from the sun, the reset of critical onboard parameters).

3.4.9 SOFTWARE THREATS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or unvetted software that might contain bugs, viruses, or spyware, which could result in system instability. System operators might misconfigure a system resulting in security weaknesses. Programmers may introduce logic or implementation errors that could result in system vulnerabilities, or instability/reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

**Possible Mission Impact:** Software threats could result in loss of data and safety issues, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

3.4.10 UNAUTHORIZED ACCESS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

**Possible Mission Impact:** An access control breach would allow an unauthorized entity to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, execute unauthorized commands aboard a crewed mission, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.

CCSDS 350.1-G-3 Page 3-8 February 2022

MARCH 2020

A REPORT OF  
THE CSIS  
AEROSPACE  
SECURITY  
PROJECT

## SPACE THREAT ASSESSMENT 2020

**Authors**  
TODD HARRISON  
KAITLYN JOHNSON  
THOMAS G. ROBERTS  
TYLER WAY  
MAKENA YOUNG

**Foreword**  
MARTIN C. FAGA

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

# Not so Novel

### 3.4.8 REPLAY

**Applicable to:** Space Segment, Ground Segment, Space-Link Communication.

**Description:** Transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

**Possible Mission Impact:** If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to the spacecraft, they might be executed, potentially at a later time. If the replayed commands are not rejected, they could result in duplicate spacecraft operations, such as a maneuver or a spacecraft re-orientation, with the result that a spacecraft is in an unintended orientation, tumbling, and/or pointed in the wrong direction, solar arrays pointed away from the sun, or the reset of critical onboard parameters).

### 3.4.9 SOFTWARE THREATS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or unvetted software that might contain bugs, viruses, or spyware, which could result in system instability. System operators might misconfigure a system resulting in security weaknesses. Programmers may introduce logic or implementation errors that could result in system vulnerabilities, or instability/reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

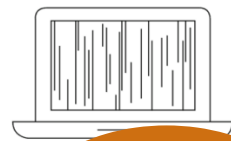
**Possible Mission Impact:** Software threats could result in loss of data and safety issues, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

### 3.4.10 UNAUTHORIZED ACCESS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

**Possible Mission Impact:** An access control breach would allow an unauthorized entity to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, execute unauthorized commands aboard a crewed mission, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.



**Illustration**  
Cyberattacks can be used to take control of a satellite and damage or destroy it.

user terminals that connect to satellites are all potential intrusion points for cyberattacks. Cyberattacks can be used to monitor data traffic patterns (i.e., which users are communicating), to monitor the data itself, or to insert false or corrupted data in the system. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. Cyberattacks can be contracted to private groups or individuals, which means that a state or non-state actor that lacks internal cyber capabilities still pose a cyber threat.<sup>9</sup>

A cyberattack on space systems can result in data loss, widespread disruptions, and even permanent loss of a satellite. For example, if an adversary can seize control of a satellite through a cyberattack on its command and control system, the attack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

### THREAT CHARACTERISTICS

The types of counterspace threats described above have distinctly different characteristics that make them more suitable for use in some scenarios than others. As shown in Table 1, some types of counterspace threats are difficult to attribute or have fully reversible effects, such as mobile jammers. High-powered lasers, for example, are “silent” and can carry out an attack with little public awareness that anything has happened. Other types of counterspace weapons produce effects that make it difficult for the attacker to know if the attack was successful, and some produce collateral damage that can affect space systems other than the one being targeted.

Counterspace weapons that are reversible, difficult to attribute, and have limited public awareness are ideally suited for situations in which an opponent may want to signal resolve, create uncertainty in the mind of its opponent, or achieve a fait accompli without triggering an escalatory response. For example, an adversary that wants to deter the United States from intervening in a situation may believe that such attacks will stay below the threshold for escalation (i.e., not trigger the very thing it is trying to prevent) while creating significant operational challenges for the United States that make the prospect of intervention more costly and protracted. Conversely, counterspace weapons that have limited battle damage assessment or that risk collateral damage may be less useful to adversaries in many situations. Without reliable battle damage assessment, for example, an adversary cannot plan operations with the confidence that its counterspace actions have been successful. Furthermore, weapons that produce collateral damage in space, such as large amounts of space debris, run the risk of escalating a conflict and turning other nations against the attacker.

SP  
TH  
AS  
20

Authors  
TODD HAR  
KAITLYN JI  
THOMAS G  
TYLER WA  
MAKENA Y

Foreword  
MARTIN C

CSIS



# Not so Novel

### 3.4.8 REPLAY

**Applicable to:** Space Segment, Ground Segment, Space-Link Communication.

**Description:** Transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

**Possible Mission Impact:** If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to the spacecraft, they might be executed, potentially at a later time. If the replayed commands are not rejected, they could result in duplicate spacecraft operations, such as a maneuver or a spacecraft re-orientation, with the result that a spacecraft is in an unintended orientation, tumbling, and/or pointed in the wrong direction, solar arrays pointed away from the sun, or the reset of critical onboard parameters).

### 3.4.9 SOFTWARE THREATS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or unvetted software that might contain bugs, viruses, or spyware, which could result in system instability. System operators might misconfigure a system resulting in security weaknesses. Programmers may introduce logic or implementation errors that could result in system vulnerabilities, or instability/reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

**Possible Mission Impact:** Software threats could result in loss of data and safety issues, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

### 3.4.10 UNAUTHORIZED ACCESS

**Applicable to:** Space Segment, Ground Segment.

**Description:** Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

**Possible Mission Impact:** An access control breach would allow an unauthorized entity to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, execute unauthorized commands aboard a crewed mission, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.



**Illustration**  
Cyberattacks can be used to take control of a satellite and damage or destroy it.

user terminals that connect to satellites are all potential intrusion points for cyberattacks. Cyberattacks can be used to monitor data traffic patterns (i.e., which users are communicating), to monitor the data itself, or to insert false or corrupted data in the system. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. Cyberattacks can be contracted to private groups or individuals, which means that a state or non-state actor that lacks internal cyber capabilities still pose a cyber threat.<sup>9</sup>

Cyberattacks on space systems can result in data loss, widespread disruptions, and even permanent loss of a satellite. For example, if an adversary can seize control of a satellite through a cyberattack on its command and control system, the attack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

### THREAT CHARACTERISTICS

The types of counterspace threats described above have distinctly different characteristics that make them more suitable for use in some scenarios than others. As shown in Table 1, some types of counterspace threats are difficult to attribute or have fully reversible effects, such as mobile jammers. High-powered lasers, for example, are "silent" and can carry out an attack with little public awareness that anything has happened. Other types of counterspace weapons produce effects that make it difficult for the attacker to know if the attack was successful, and some produce collateral damage that can affect space systems other than the one being targeted.

Counterspace weapons that are reversible, difficult to attribute, and have limited public awareness are ideally suited for situations in which an opponent may want to signal resolve, create uncertainty in the mind of its opponent, or achieve a fait accompli without triggering an escalatory response. For example, an adversary that wants to deter the United States from intervening in a situation may believe that such attacks will stay below the threshold for escalation (i.e., not trigger the very thing it is trying to prevent) while creating significant operational challenges for the United States that make the prospect of intervention more costly and protracted. Conversely, counterspace weapons that have limited battle damage assessment or that risk collateral damage may be less useful to adversaries in many situations. Without reliable battle damage assessment, for example, an adversary cannot plan operations with the confidence that its counterspace actions have been successful. Furthermore, weapons that produce collateral damage in space, such as large amounts of space debris, run the risk of escalating a conflict and turning other nations against the attacker.

## Cybersecurity Protections for Spacecraft: A Threat Based Approach

April 29, 2021

Brandon Bailey  
Cyber Assessment and Research Department (CARD)  
Cybersecurity Subdivision (CSS)

Prepared for:  
U.S. GOVERNMENT AGENCY

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

**Distribution Statement A:** Distribution Statement A: Approved for public release; distribution unlimited.



# Outdated Assumptions





# Myth of Inaccessibility

---



\$\$\$ → \$

Affordable  
Ground Stations

# Myth of Inaccessibility

---



\$\$\$ → \$

Affordable  
Ground Stations



Ground Station as a Service  
GSaaS

# Myth of Inaccessibility

---

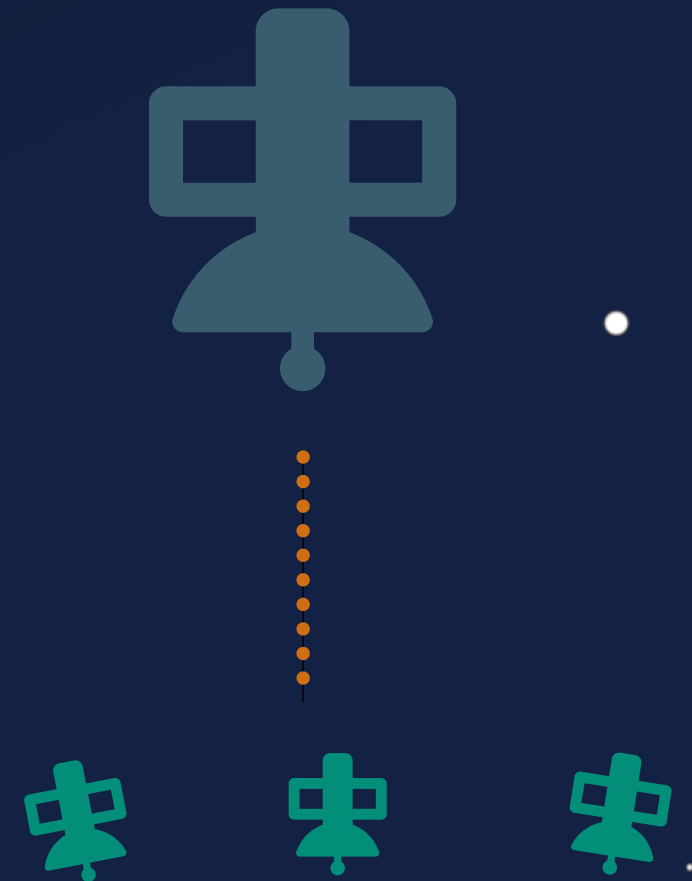


\$\$\$ → \$

Affordable  
Ground Stations



Ground Station as a Service  
GSaaS



More Satellites  
GEO → LEO

# Security by Obscurity

---

// *No Insights  $\Leftrightarrow$  No Attacker*

# Security by Obscurity

---

// ~~No Insights  $\leftrightarrow$  No Attacker~~



# Security by Obscurity

---

// ~~No Insights  $\leftrightarrow$  No Attacker~~



More Developers  
More People Involved

# Security by Obscurity

---

// ~~No Insights~~  $\leftrightarrow$  ~~No Attacker~~



More Developers  
More People Involved



Commercial off-the-Shelf  
(COTS)  
Components

# Security by Obscurity

---

// ~~No Insights~~  $\leftrightarrow$  ~~No Attacker~~



More Developers  
More People Involved



Commercial off-the-Shelf  
(COTS)  
Components



Higher Stakes  
Critical Infrastructure

# Attacker Goals

---



Denial of Service

# Attacker Goals

---



Denial of Service



Malicious Data Interaction



# Attacker Goals

---



Denial of Service



Seizure of Control



Malicious Data Interaction

# Attacker Goals

---



Denial of Service



Seizure of Control



Malicious Data Interaction

# Attacker Goals

---



Seizure of Control

# Attacker Goals

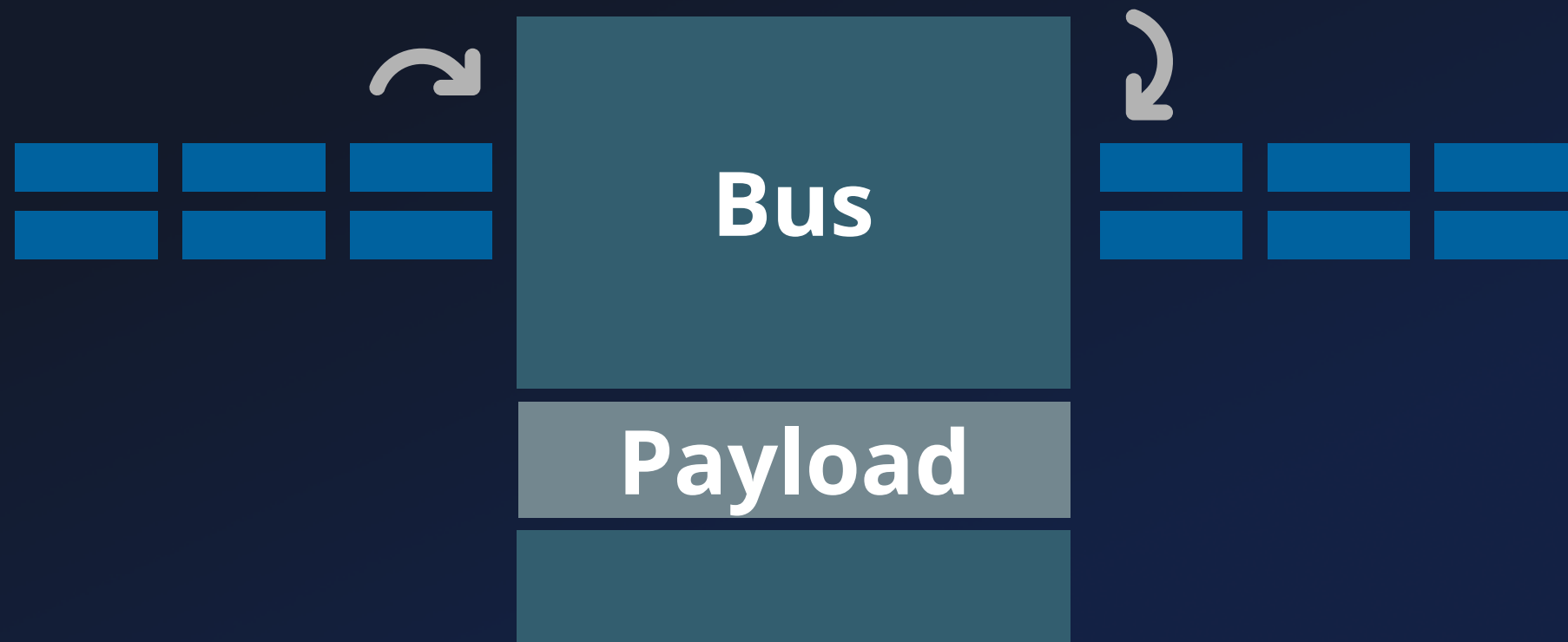
---



Seizure of Control

# Components

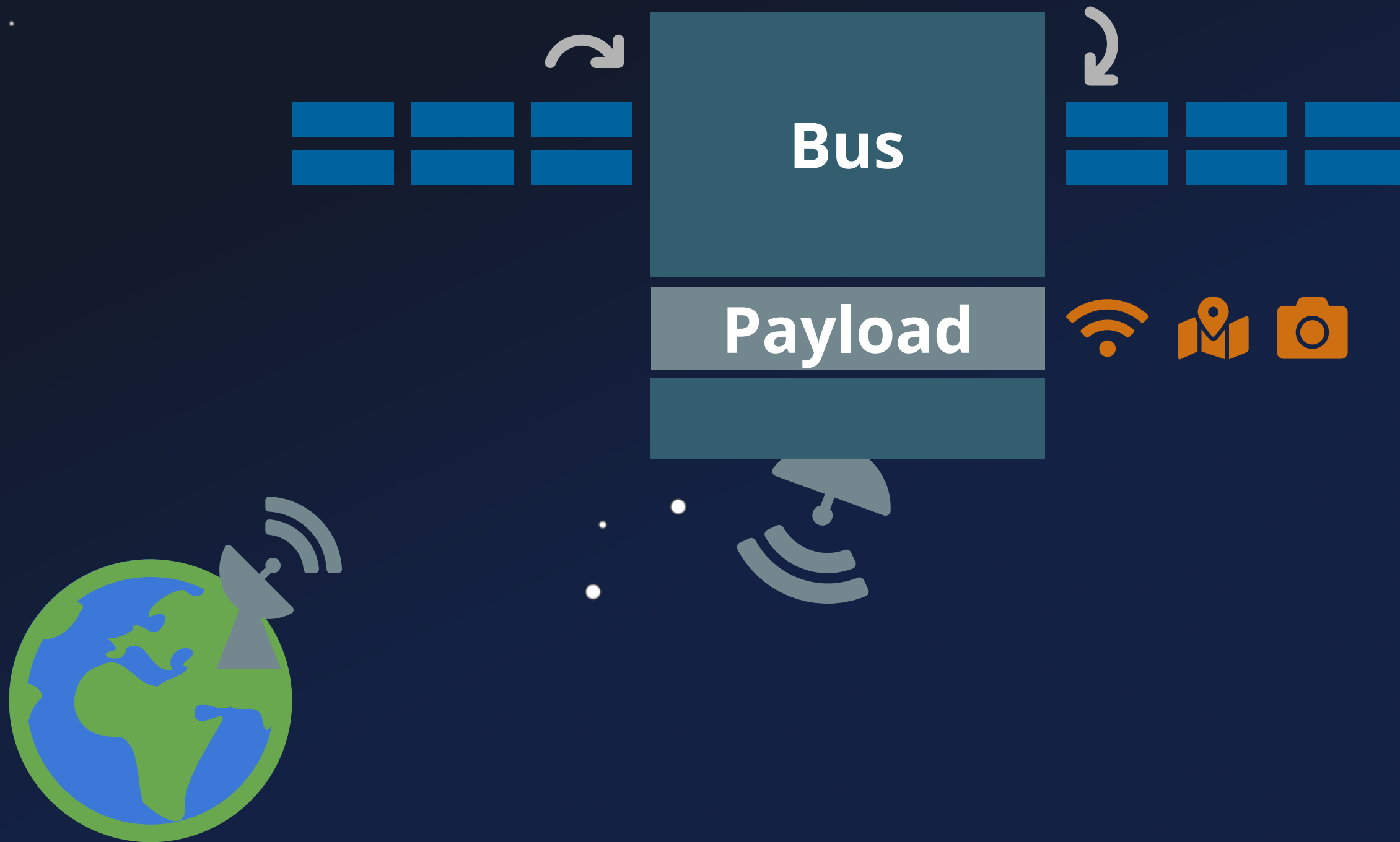
---



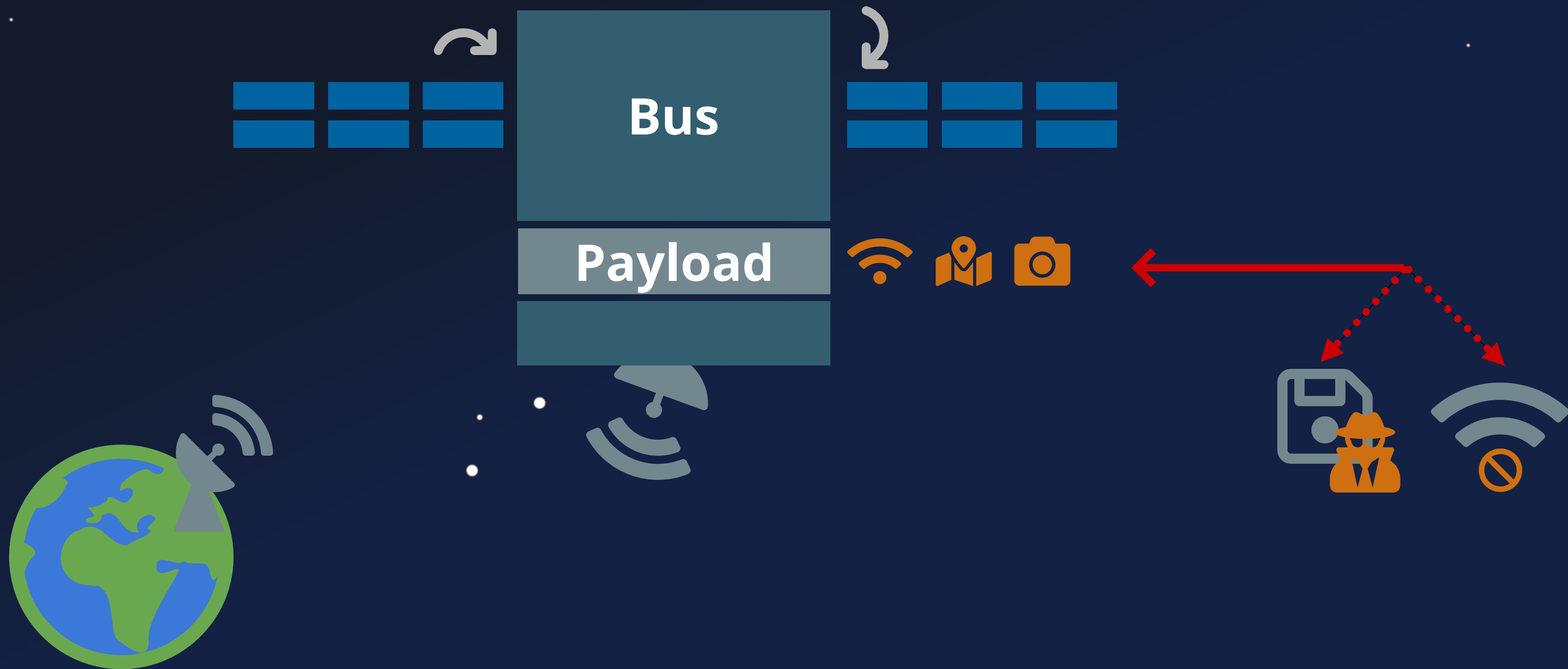


# Components

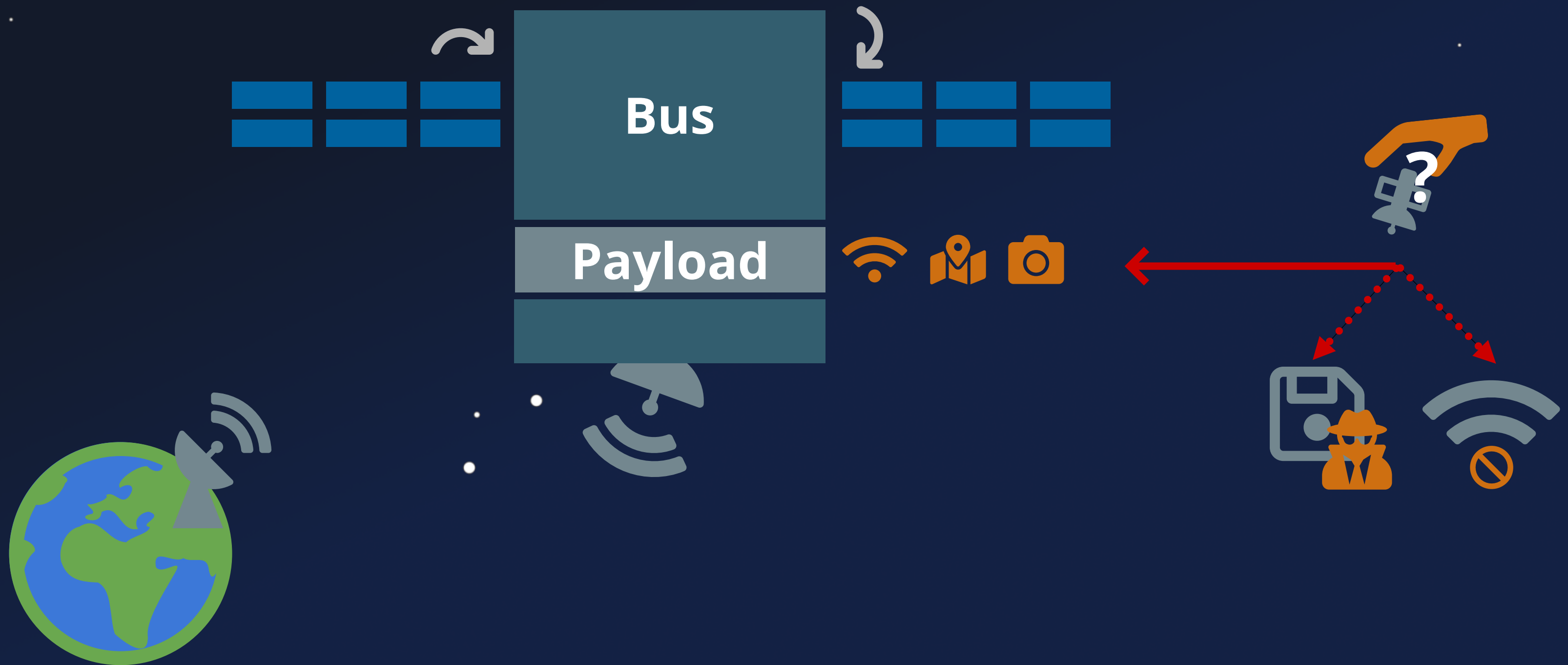
---



# Components

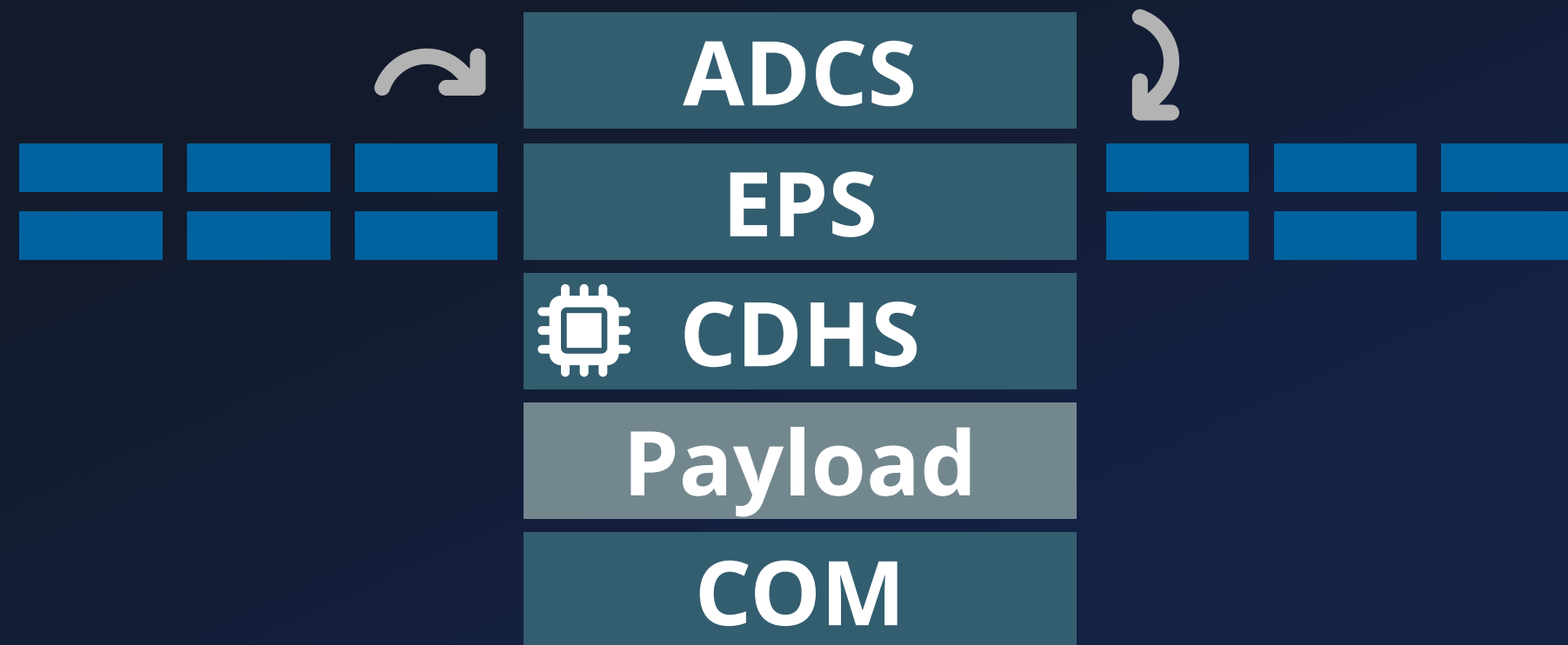


# Components

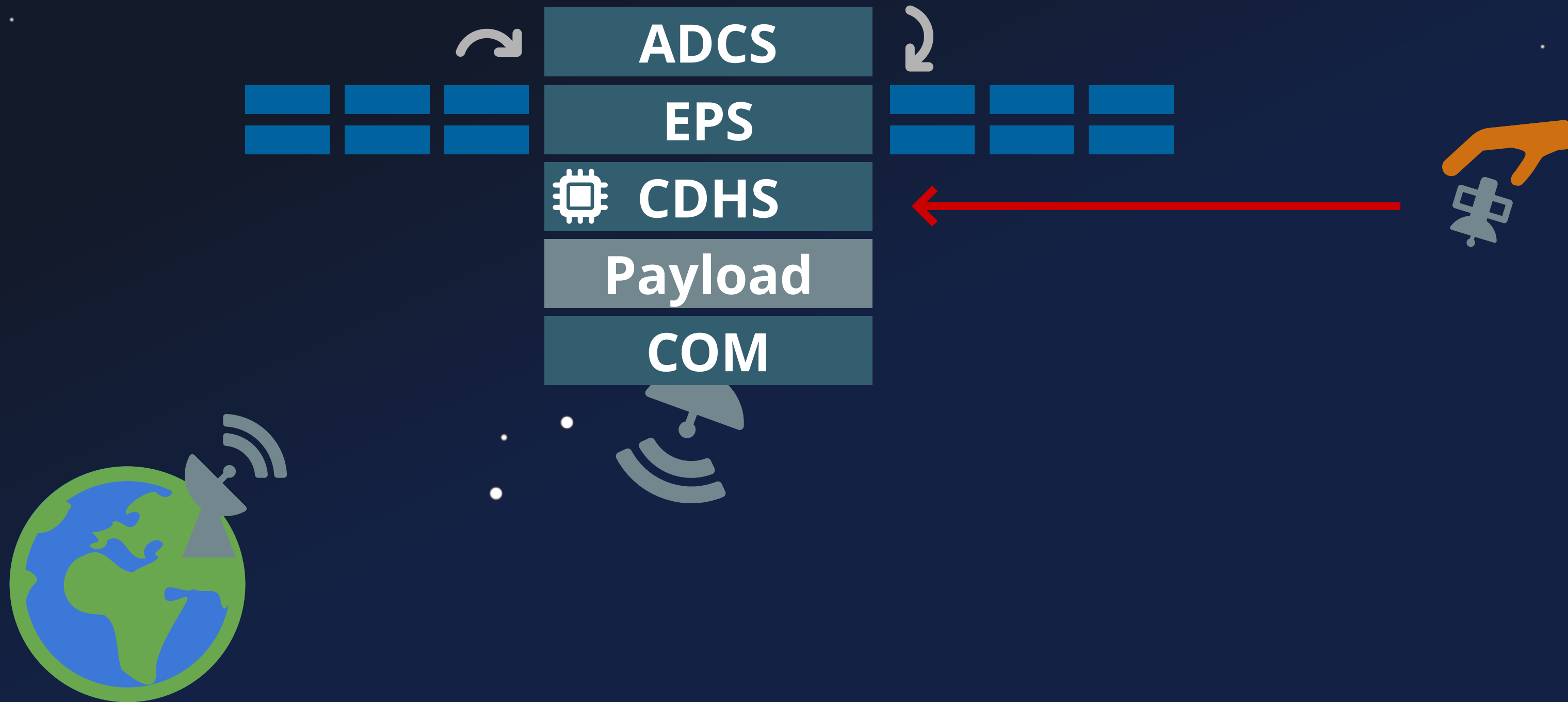


# Components

---

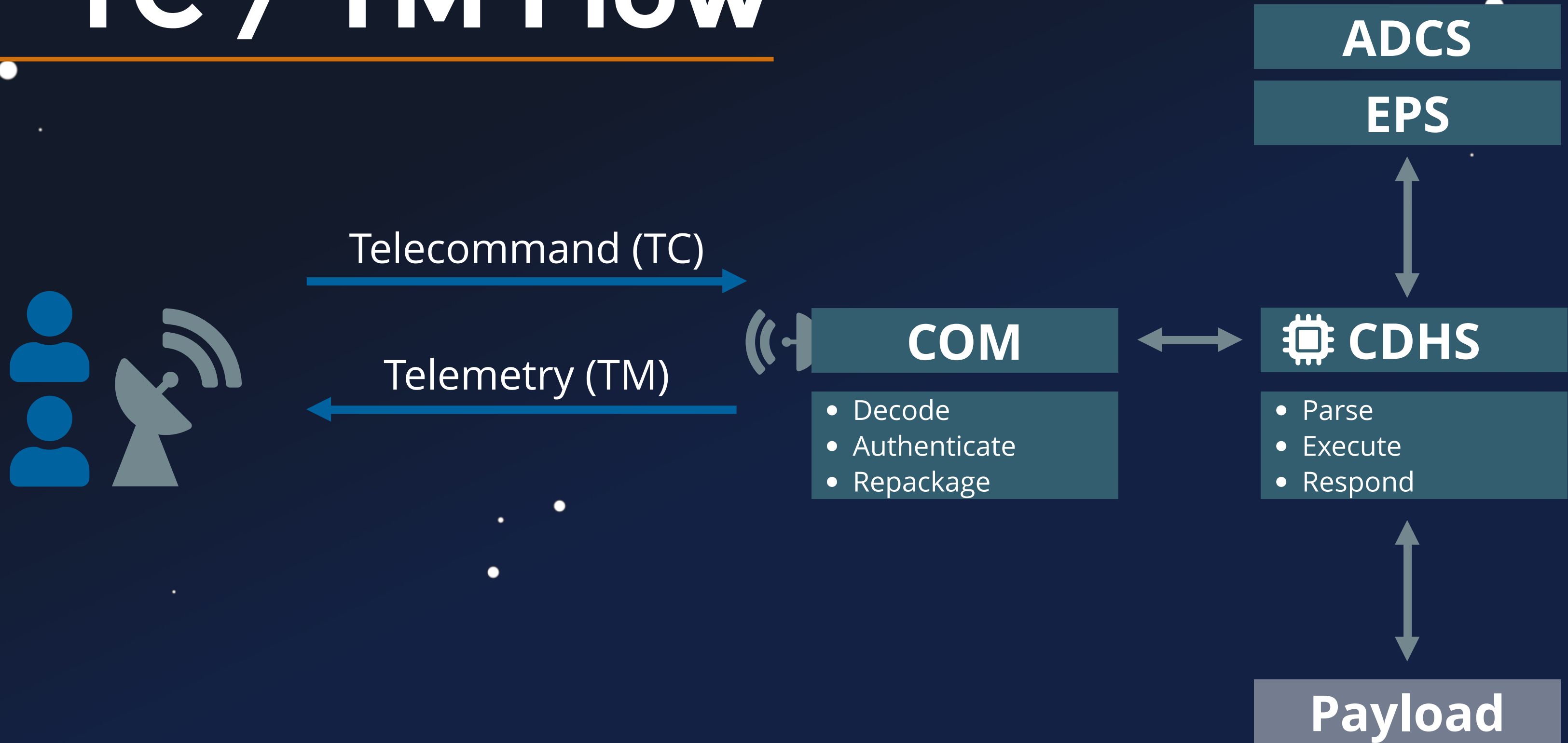


# Components

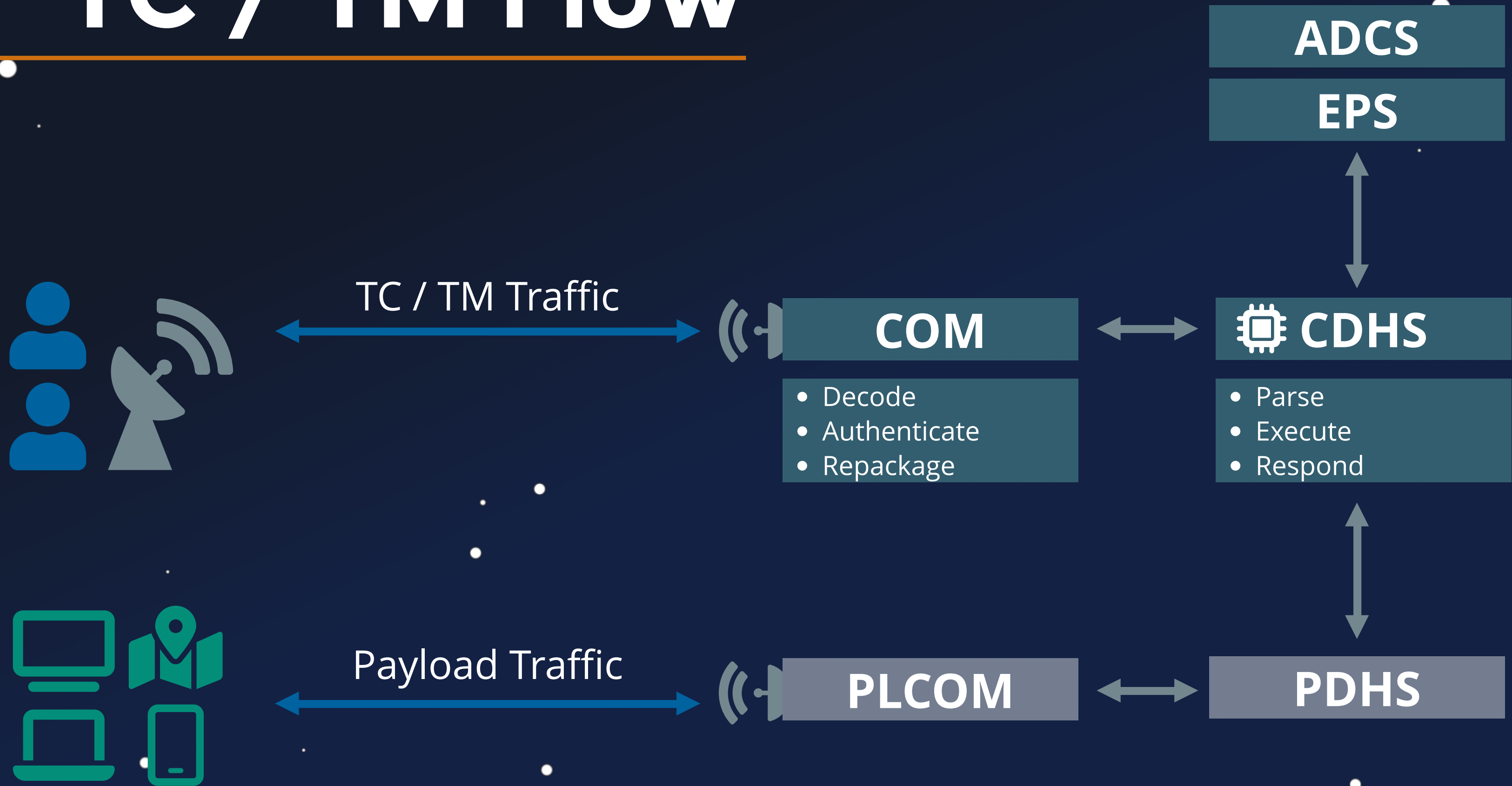




# TC / TM Flow

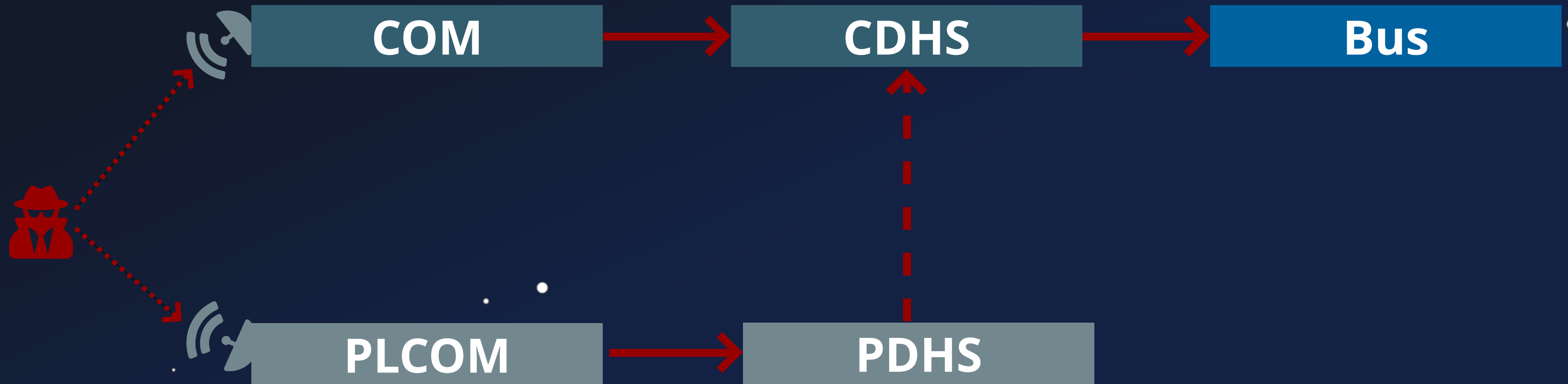


# TC / TM Flow



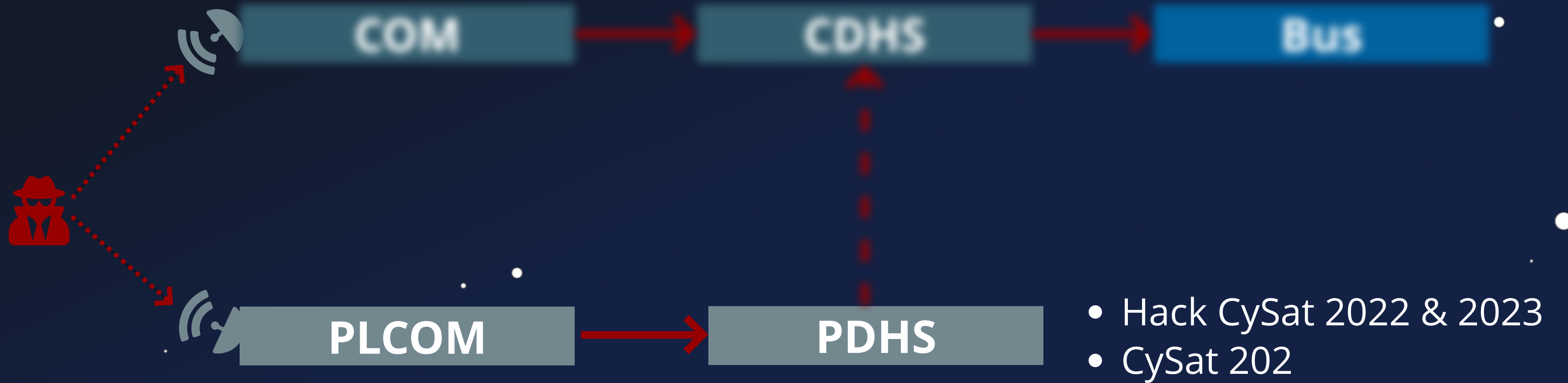
# Attack Path

---



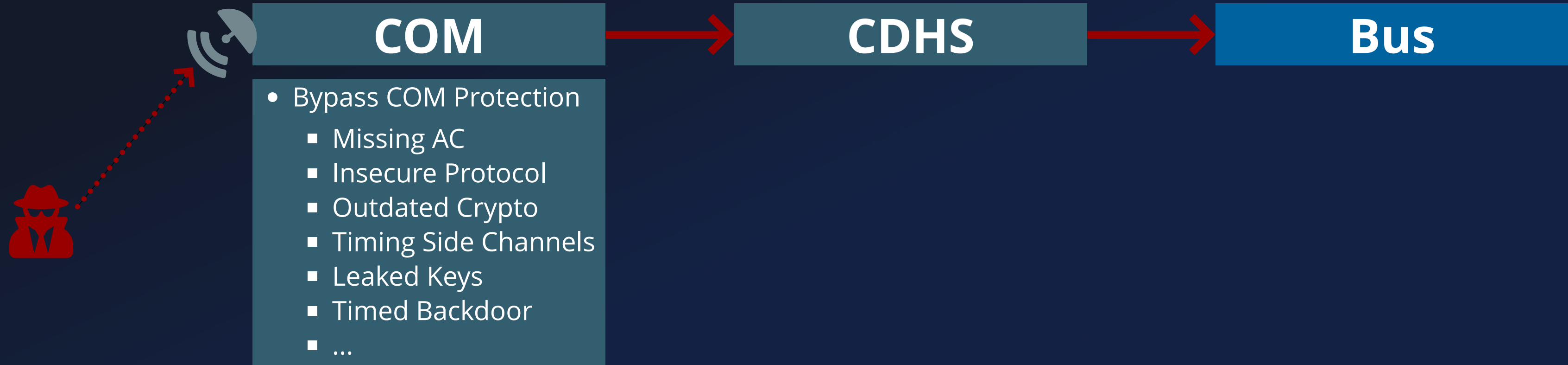
# Attack Path

---



# Attack Path

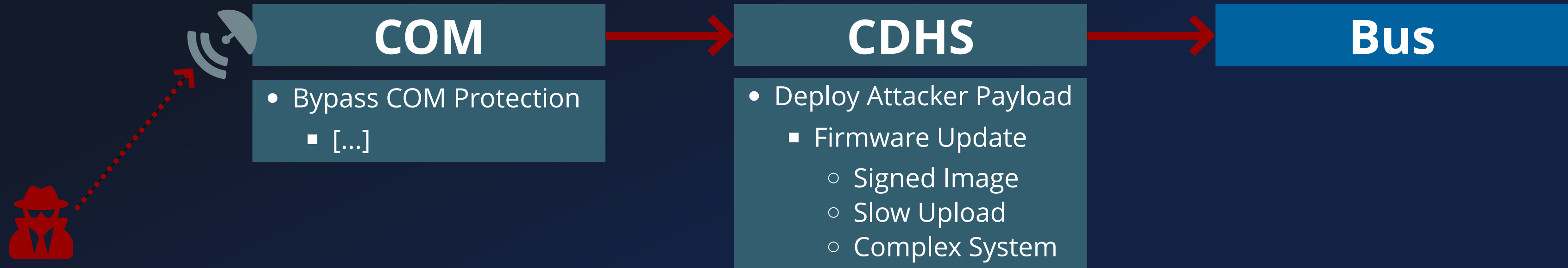
---





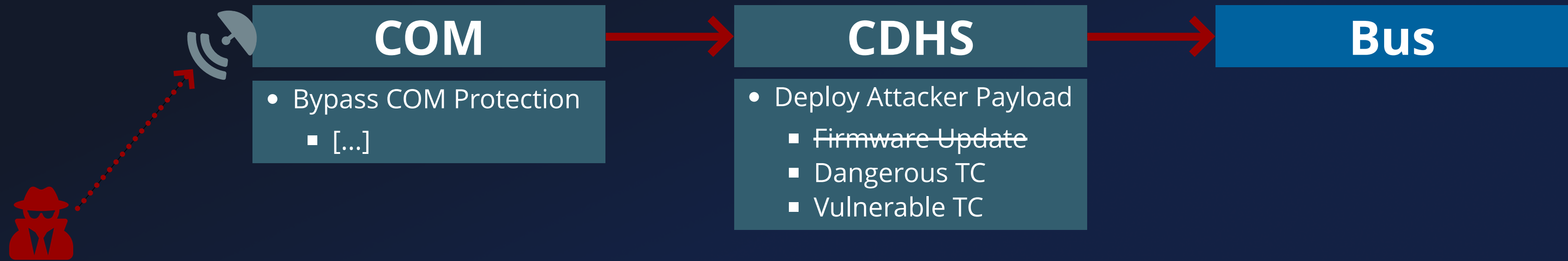
# Attack Path

---



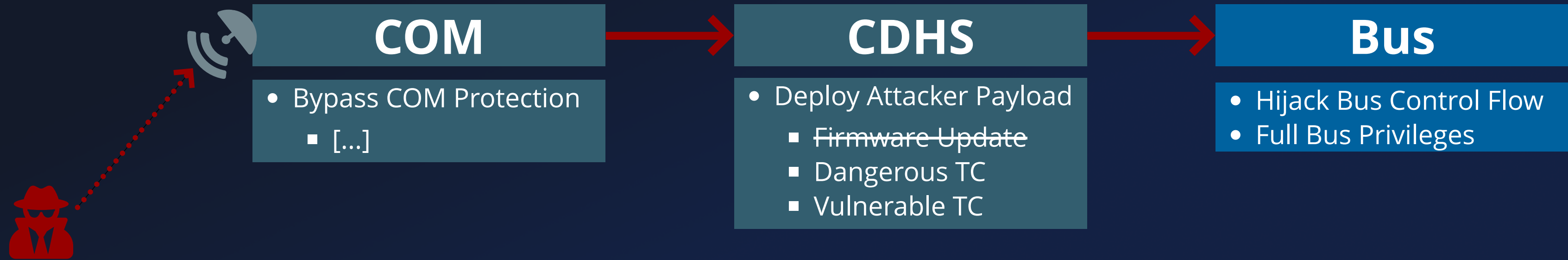
# Attack Path

---

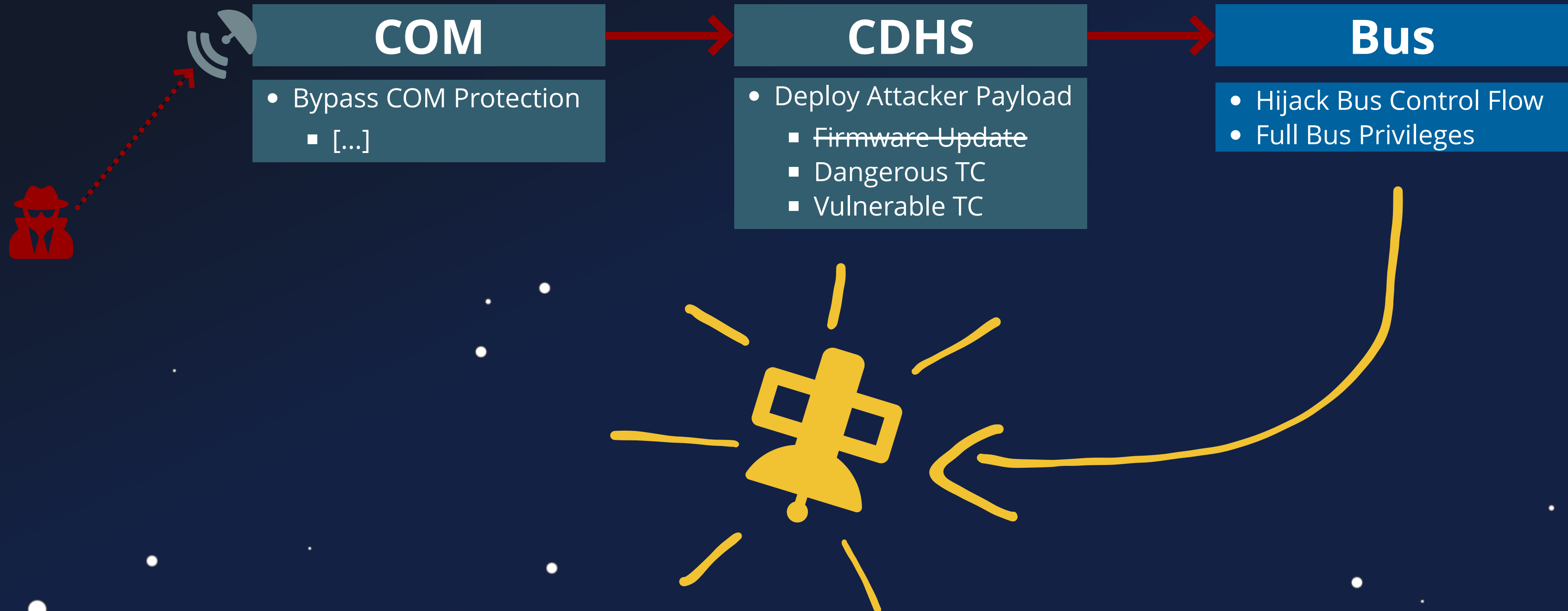


# Attack Path

---

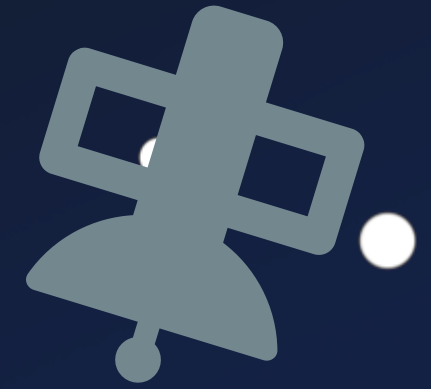


# Attack Path



# Objectives

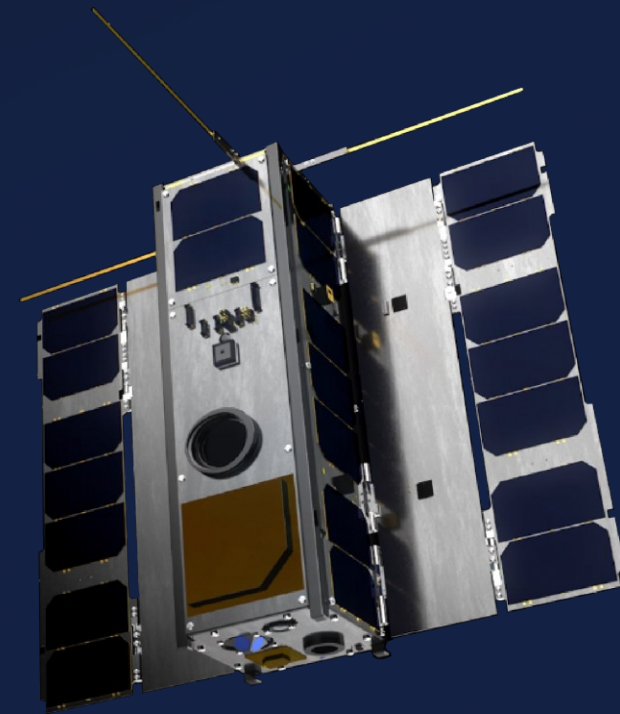
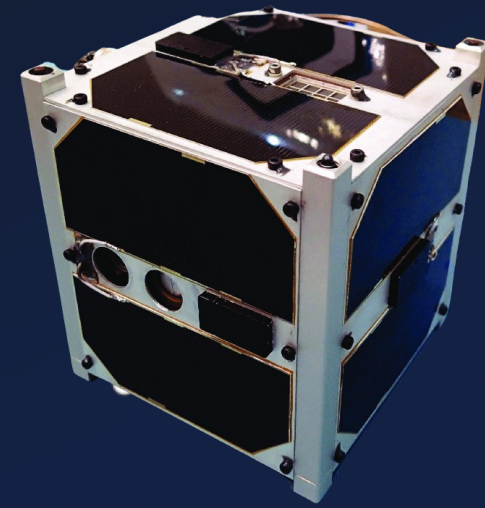
---



- ① Bypass COM Protection
- ② Dangerous / Vulnerable TC
- ③ Hijack Bus Control Flow
- ④ Full Bus Privileges



# Satellite Case Studies



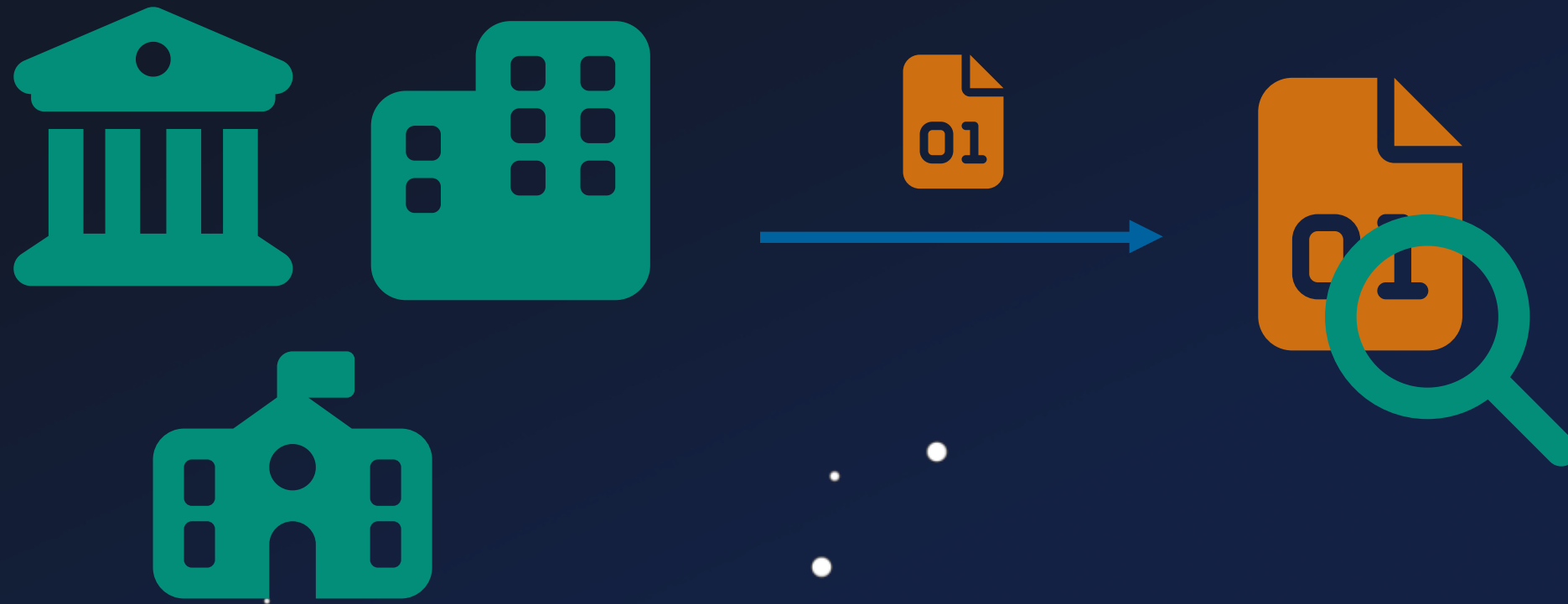
# Approach

---



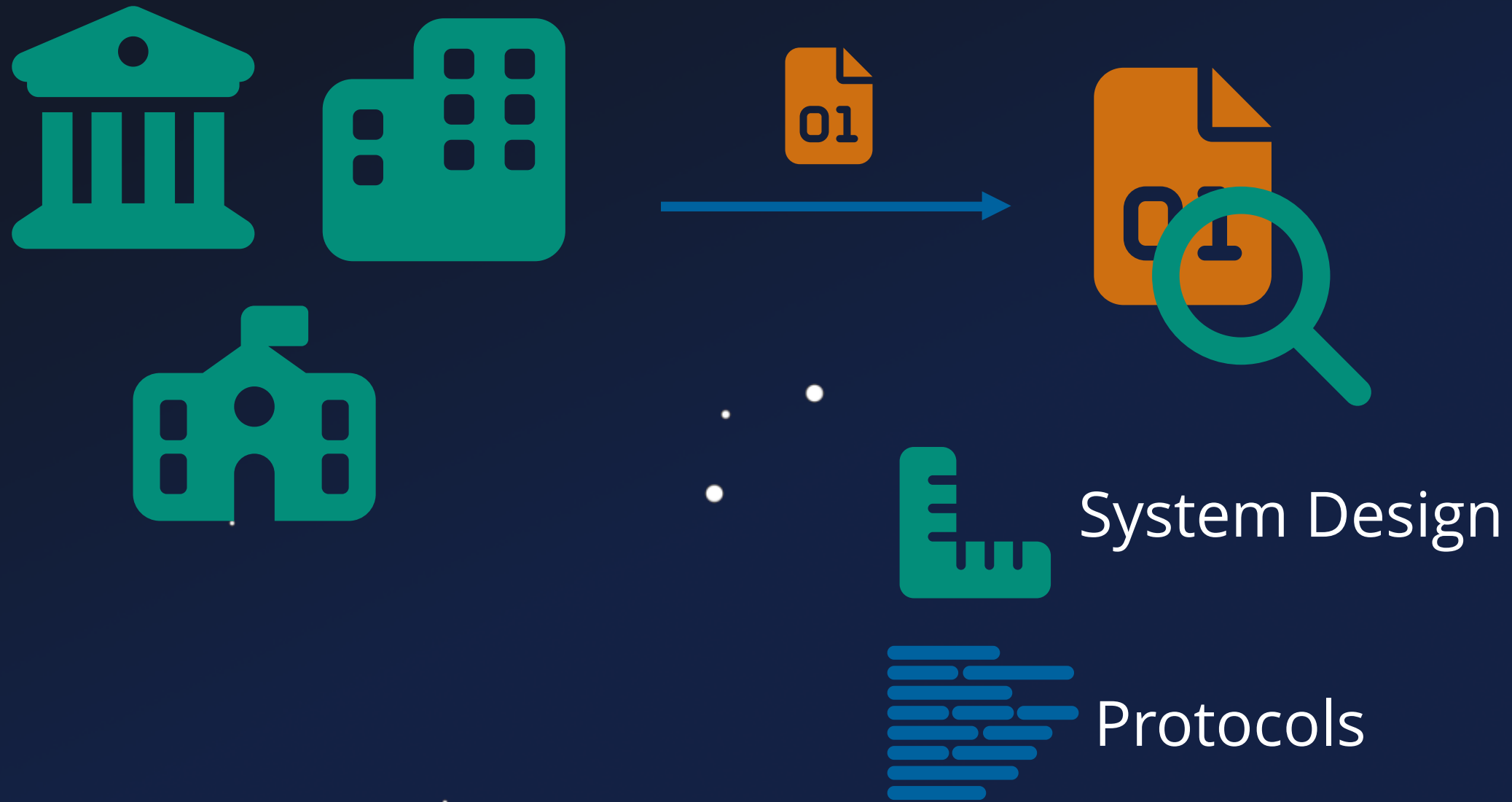
# Approach

---



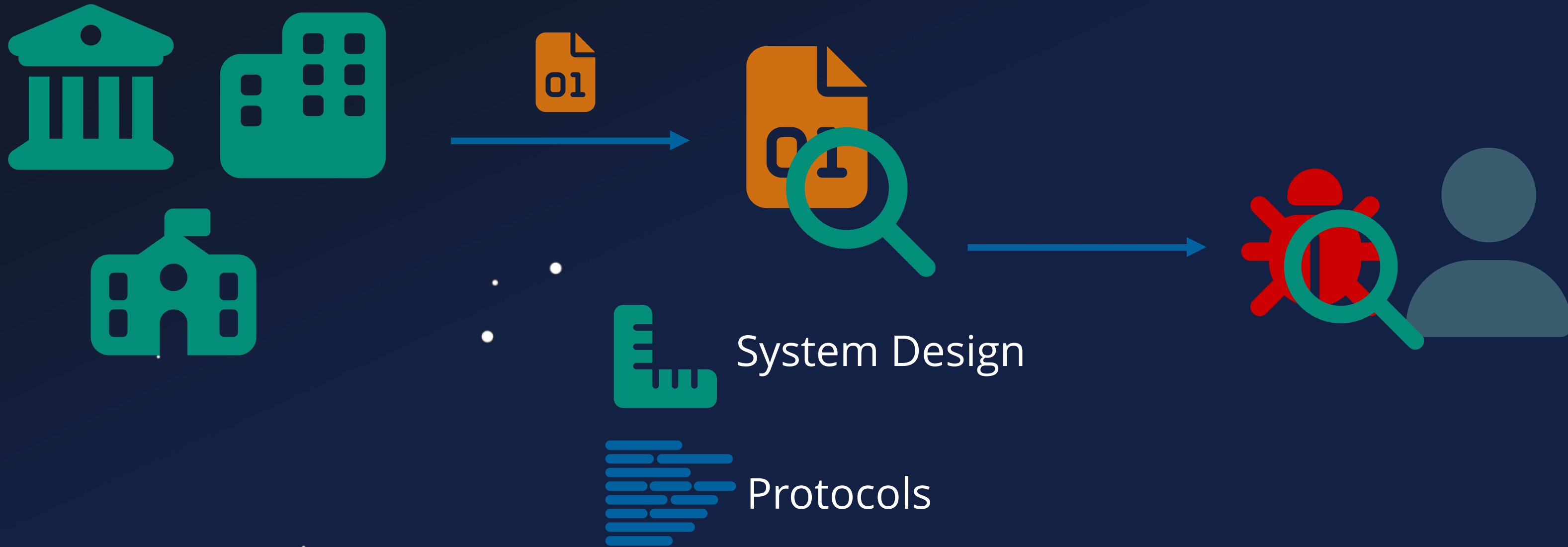
# Approach

---



# Approach

---



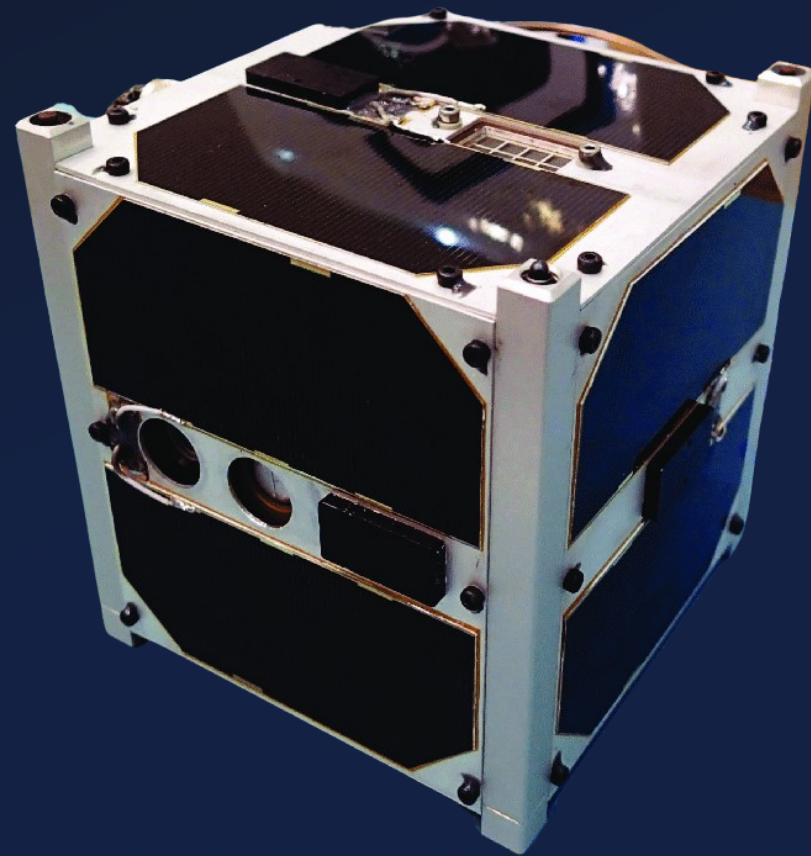


# Approach

---

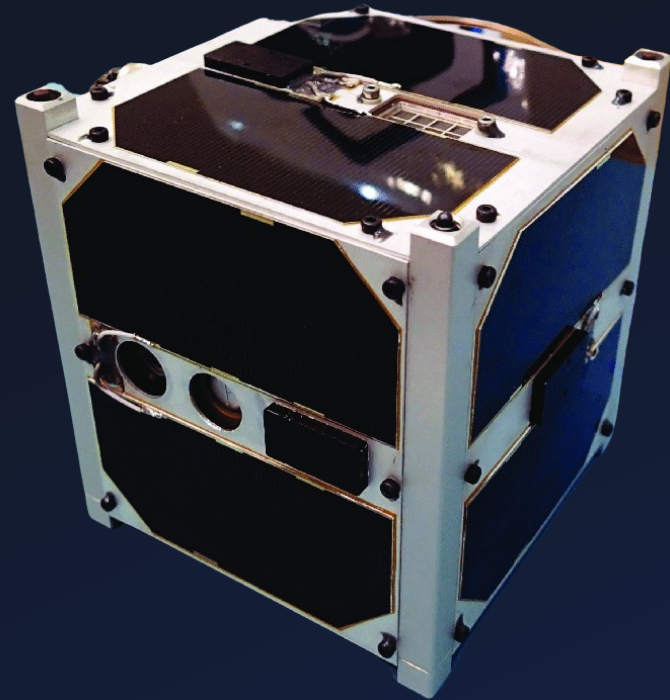


# ESTCube-1



# ESTCube-1

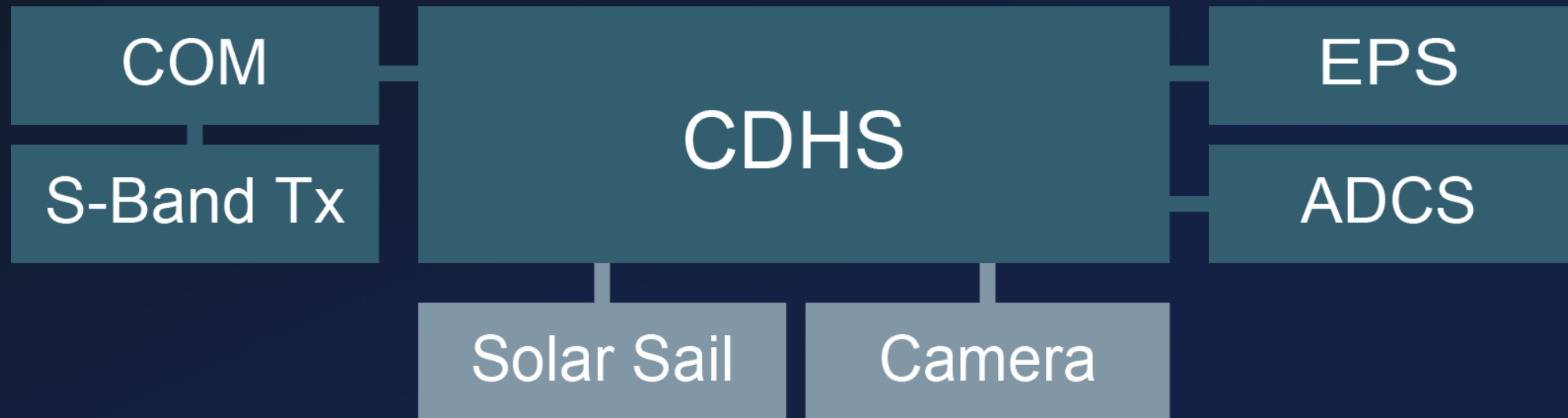
---



## ESTCube-1

---

Developed by  
University of Tartu



E-Sail (E. Solar Wind Sail) Propulsion

---

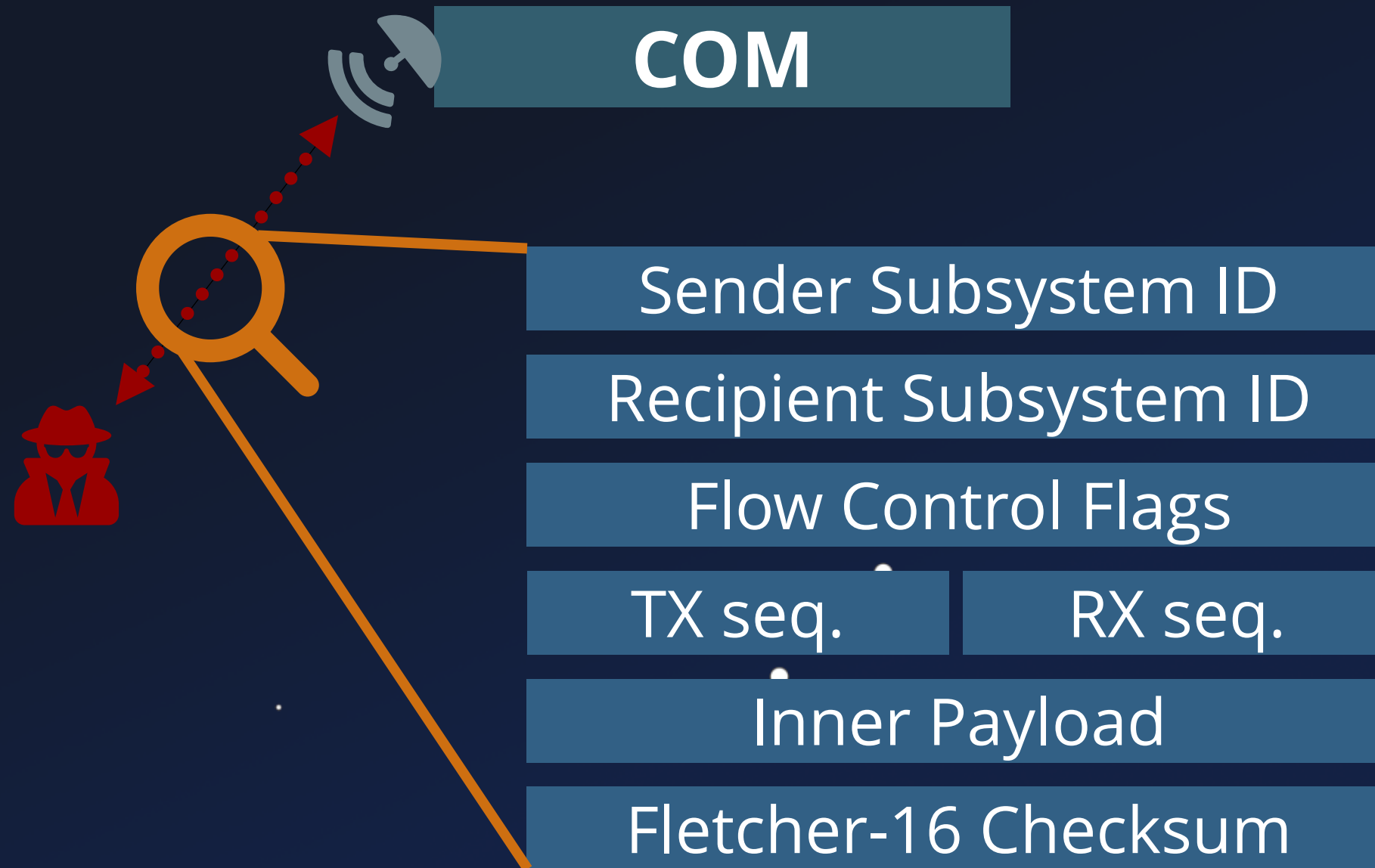
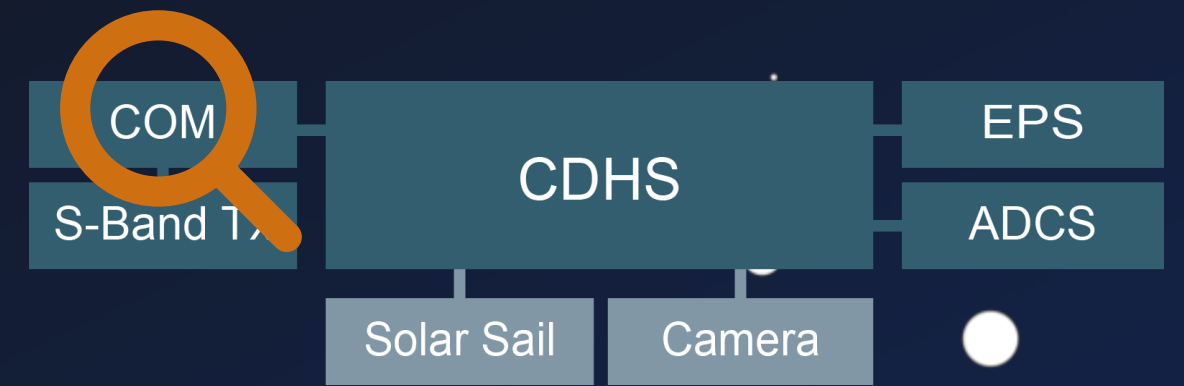
Peripherals

ARM STM32

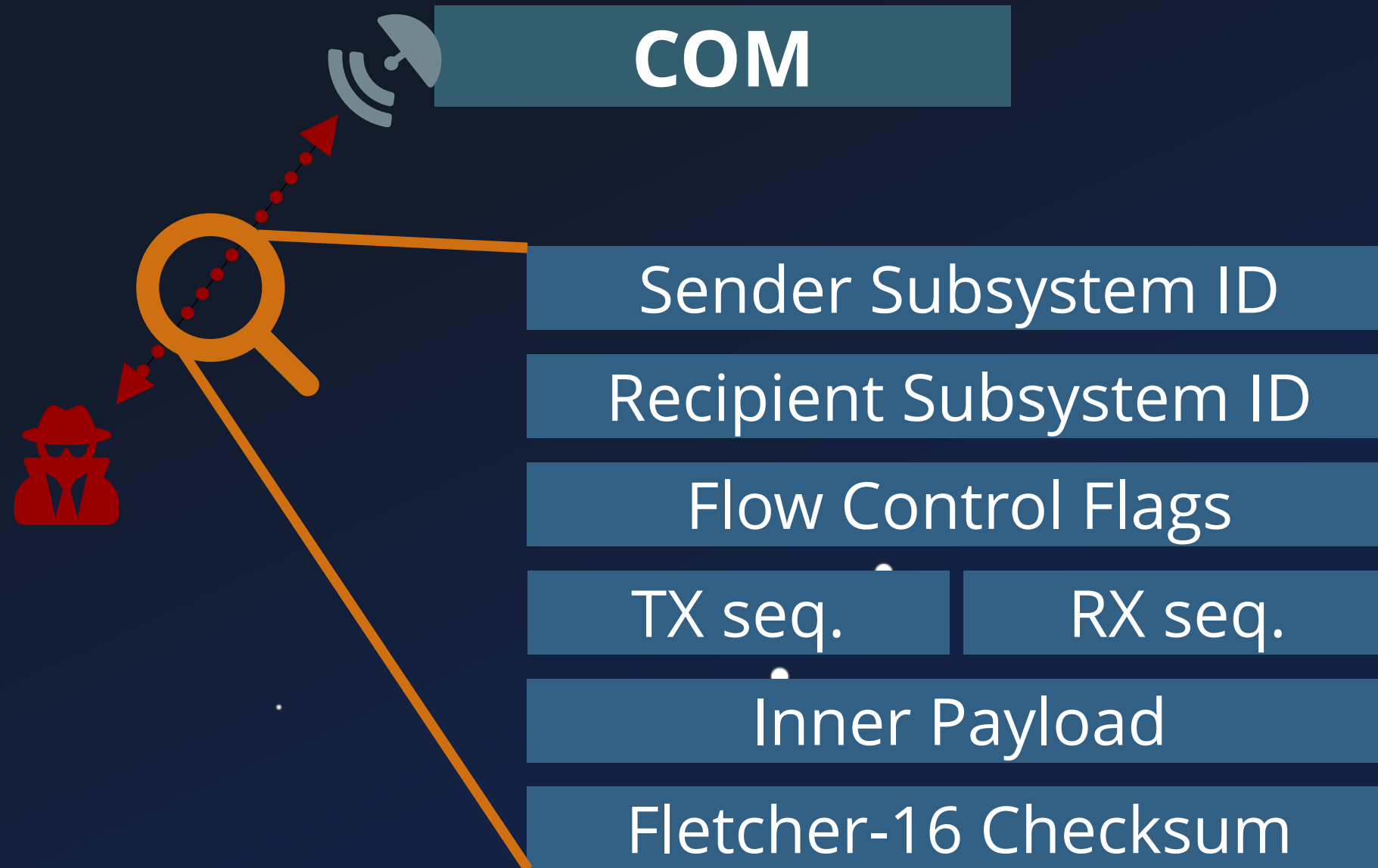
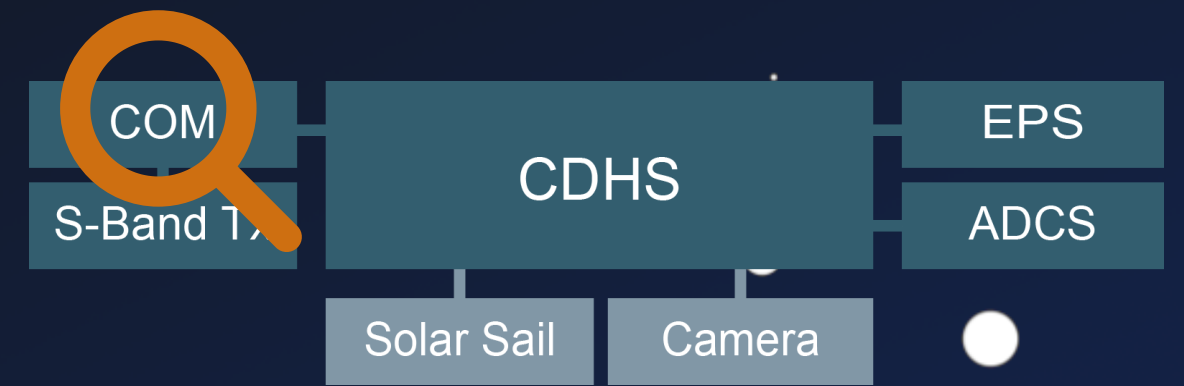
---

Bus Platform

# Custom Protocol



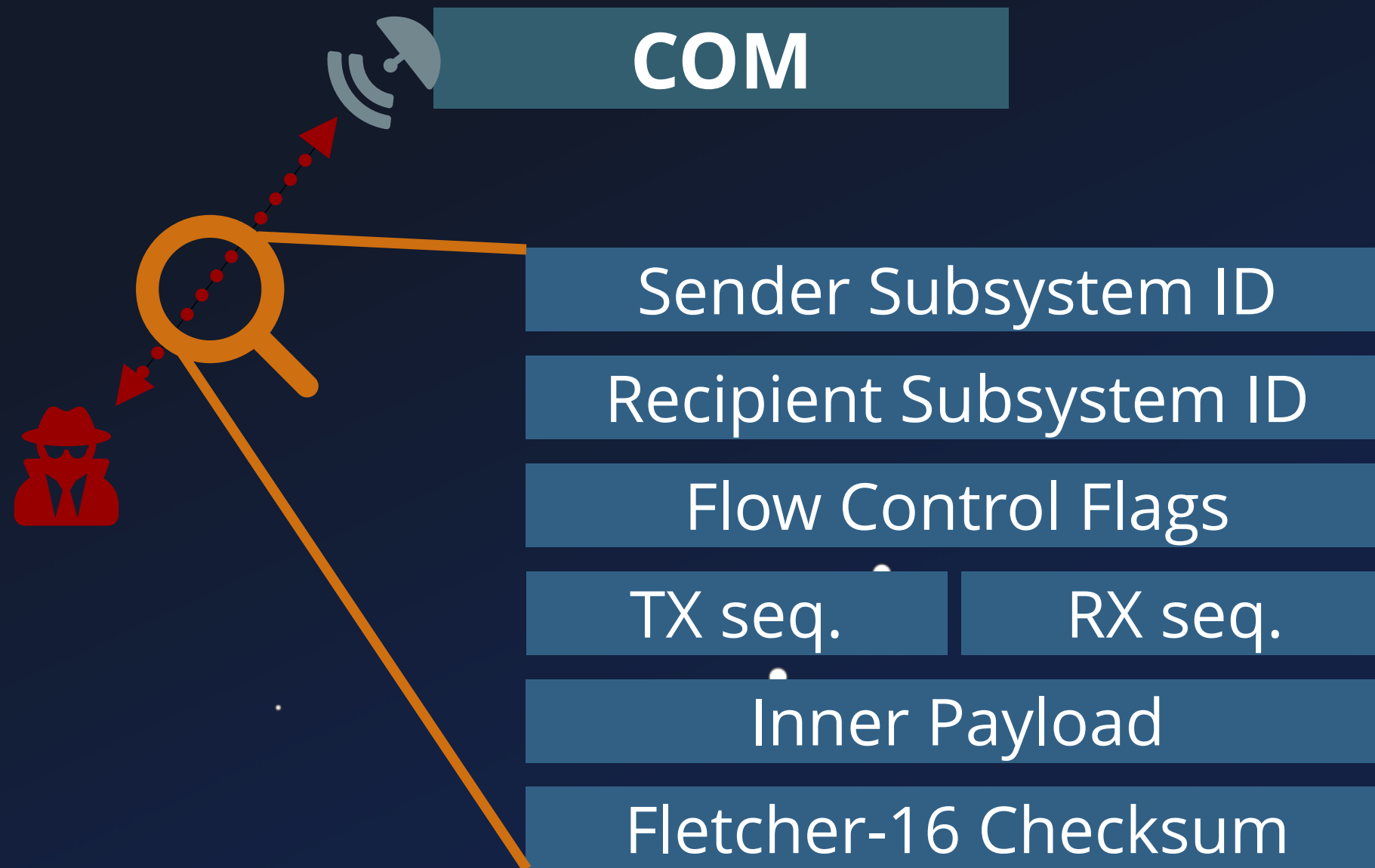
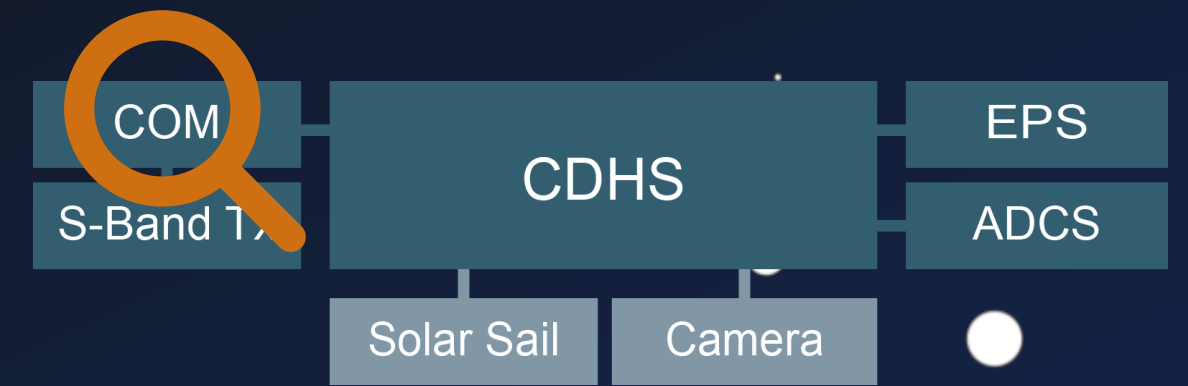
# Custom Protocol



ID	Subsystem
0	EPS
1	COM
2	CDHS
...	
5	Ground Station



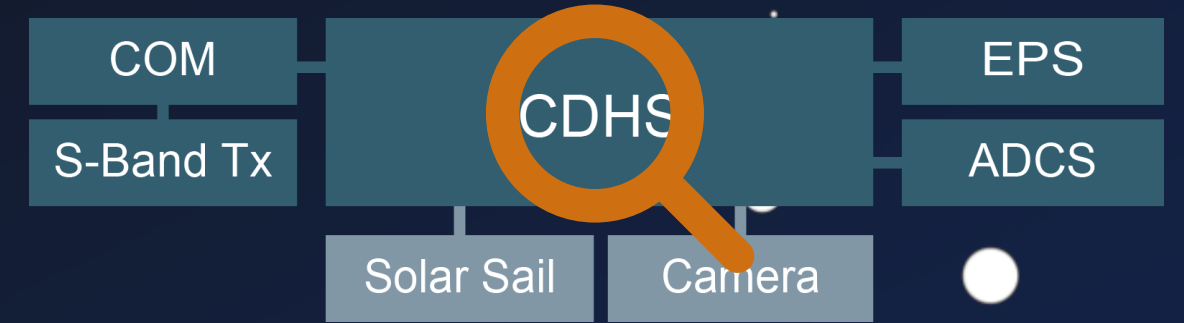
# Custom Protocol



ID	Subsystem
0	EPS
1	COM
2	CDHS
...	
5	Ground Station

	bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
Byte 0	Command Identifier (MSB)							
Byte 1	Command Identifier (LSB)							
Byte 2	Source				Block ID			
Byte 3	Length							
...	Args							

# Security Analysis

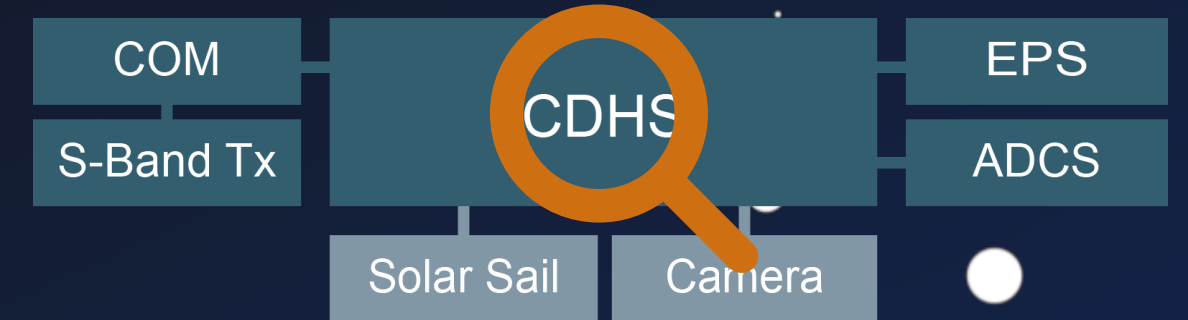


- Bypass COM Protection
  - Missing TC Protection

01  
10



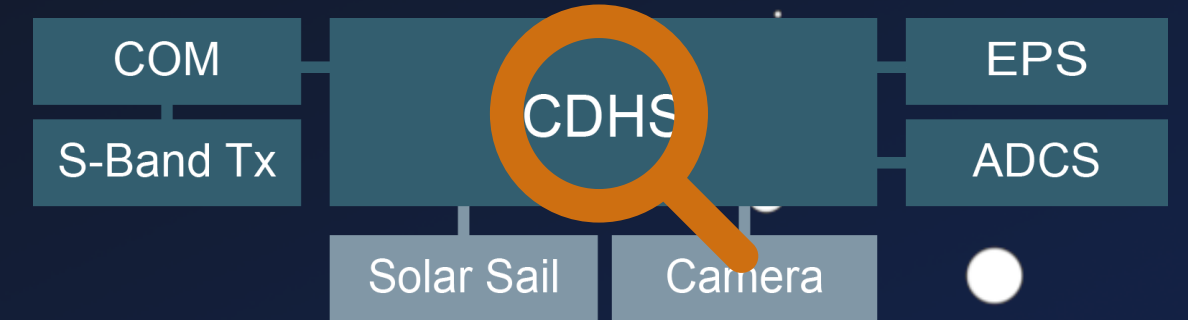
# Security Analysis



- Bypass COM Protection
  - Missing TC Protection

```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
2   raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
3   char* pWriteData;
4
5   if (pAddr) {
6     if (g_sch_exec_mode != 1) {
7       /* exception and return */
8     }
9     char* pWriteData = &pAddr->start_of_data_buf;
10    if (pAddr->filesystem_target) {
11      // [...]
12    } else {
13      memcpy(pAddr->targetAddr,
14            &pAddr->start_of_data_buf,
15            pAddr->writeLength);
16    }
17  }
18  // ...
19 }
```

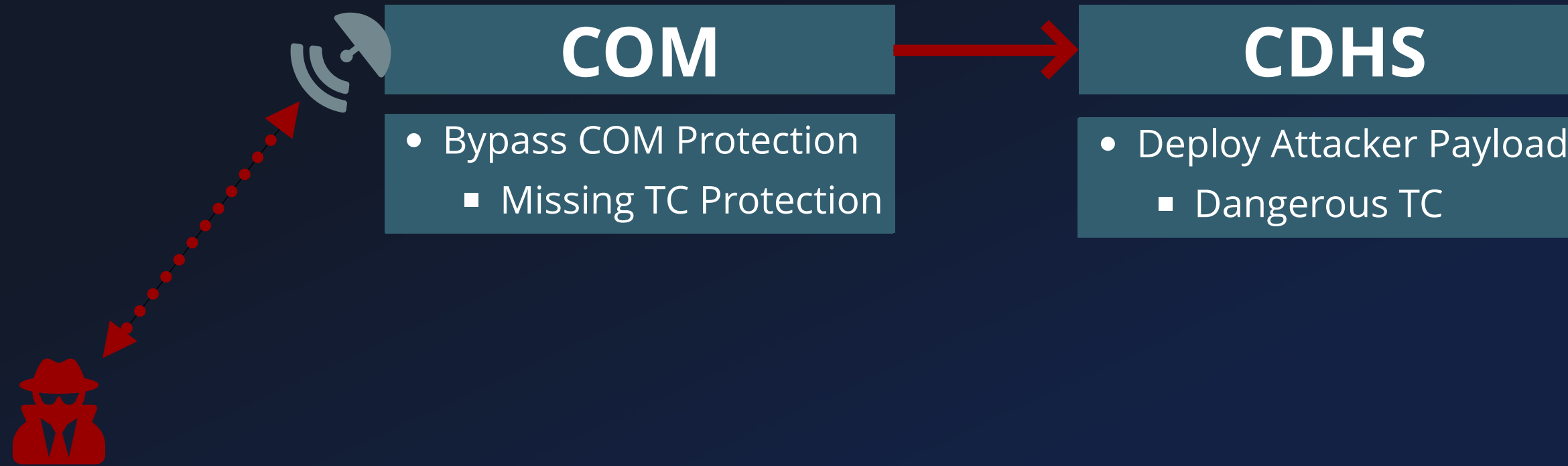
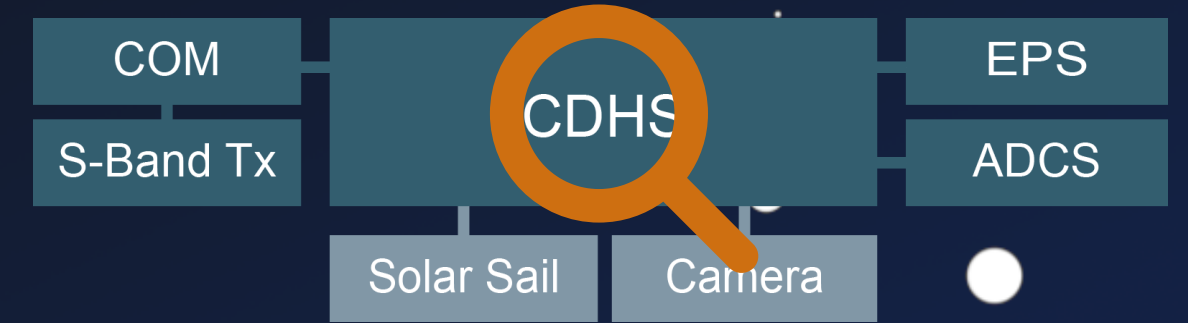
# Security Analysis



- Bypass COM Protection
  - Missing TC Protection

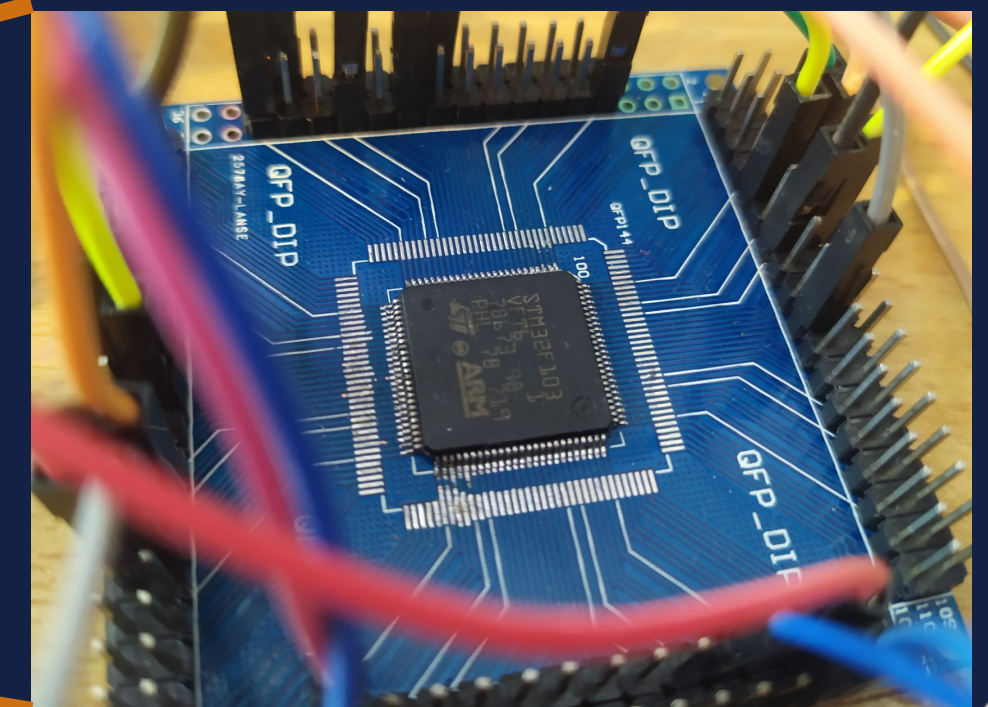
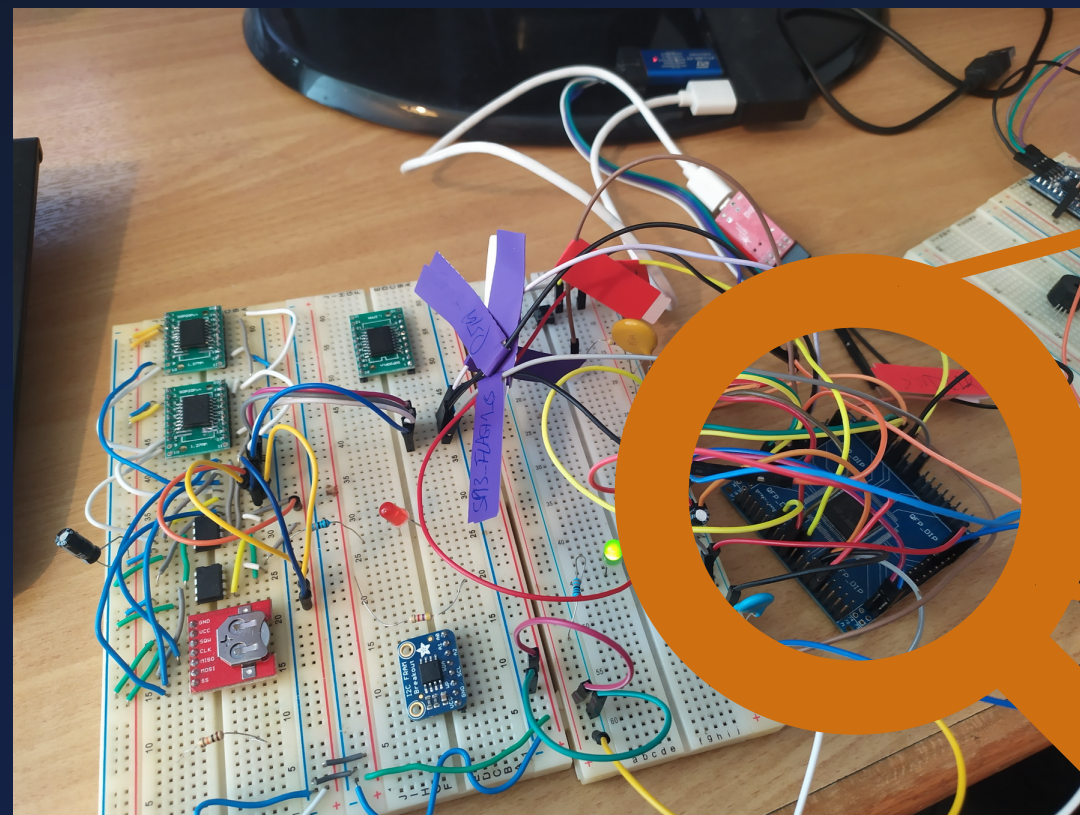
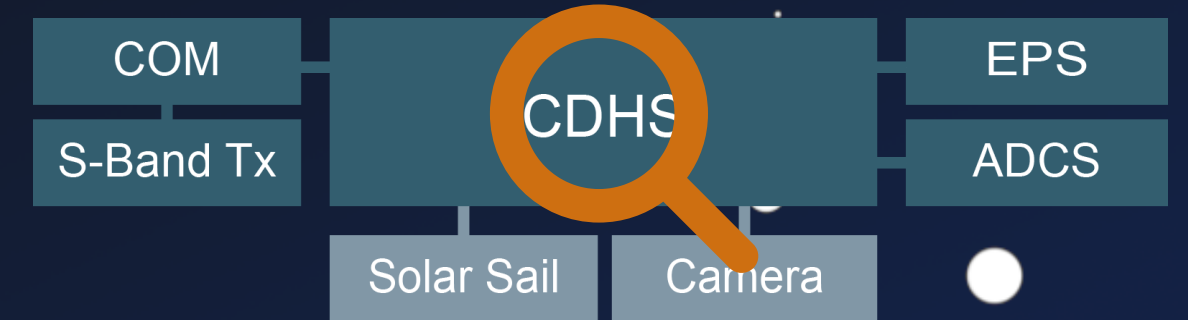
```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
2   raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
3   char* pWriteData;
4
5   if (pAddr) {
6     if (g_sch_exec_mode != 1) {
7       /* exception and return */
8     }
9     char* pWriteData = &pAddr->start_of_data_buf;
10    if (pAddr->filesystem_target) {
11      // [...]
12    } else {
13      memcpy(pAddr->targetAddr,
14            &pAddr->start_of_data_buf,
15            pAddr->writeLength);
16    }
17  }
18  // ...
19 }
```

# Real-World Test

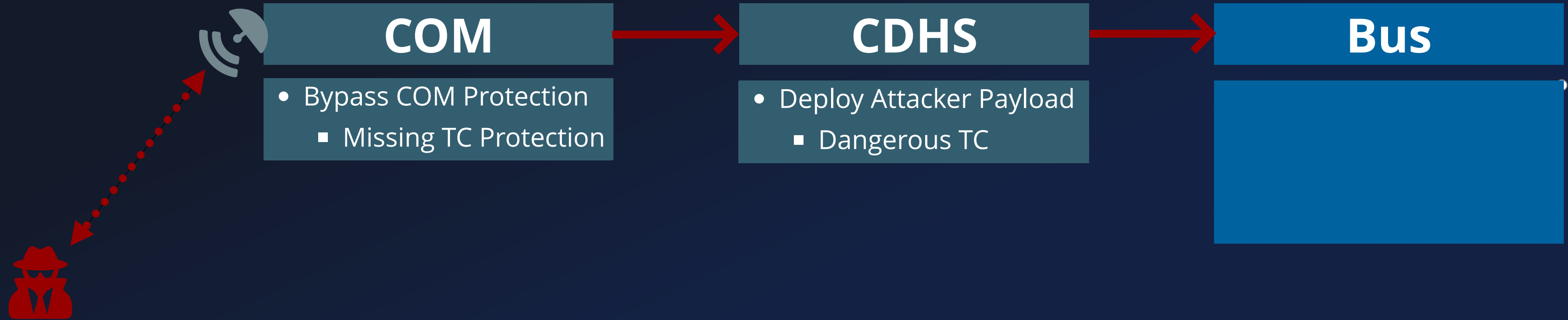
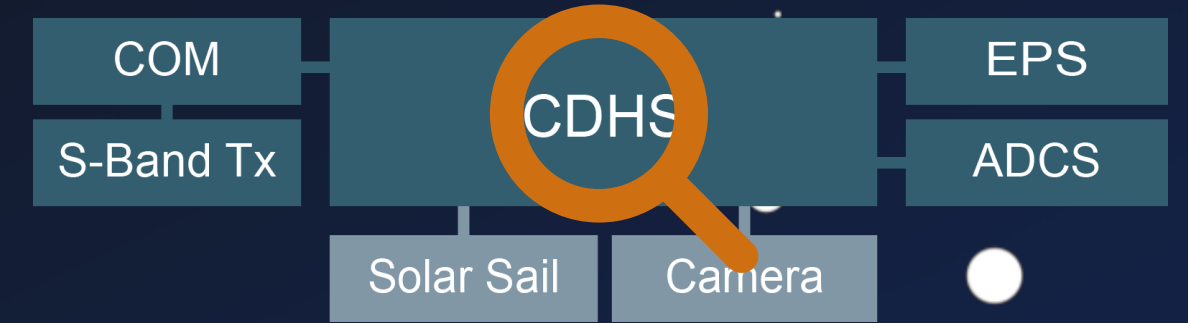




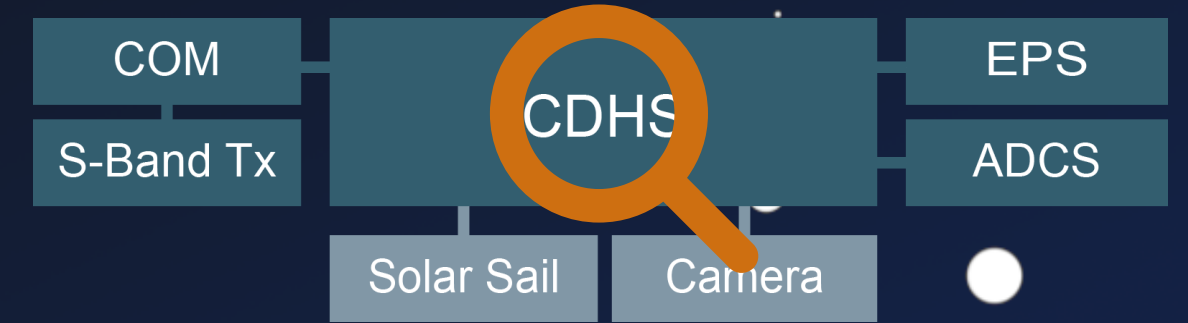
# Real-World Test



# Real-World Test

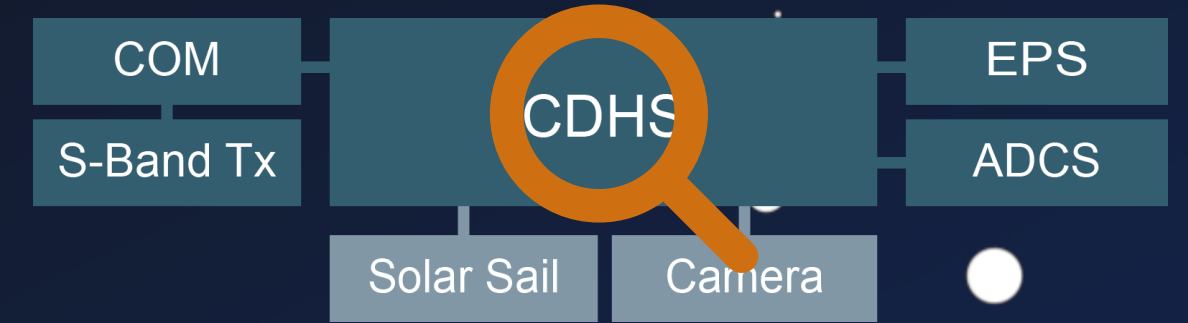


# Real-World Test





# Real-World Test

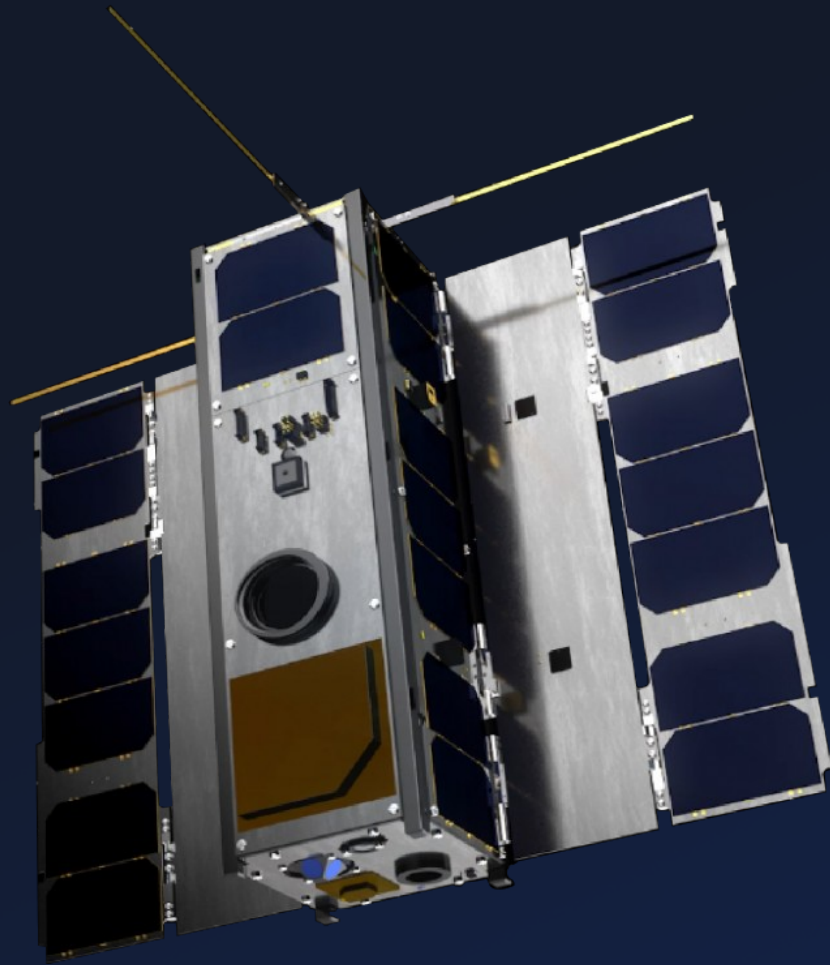


# OPS-Sat





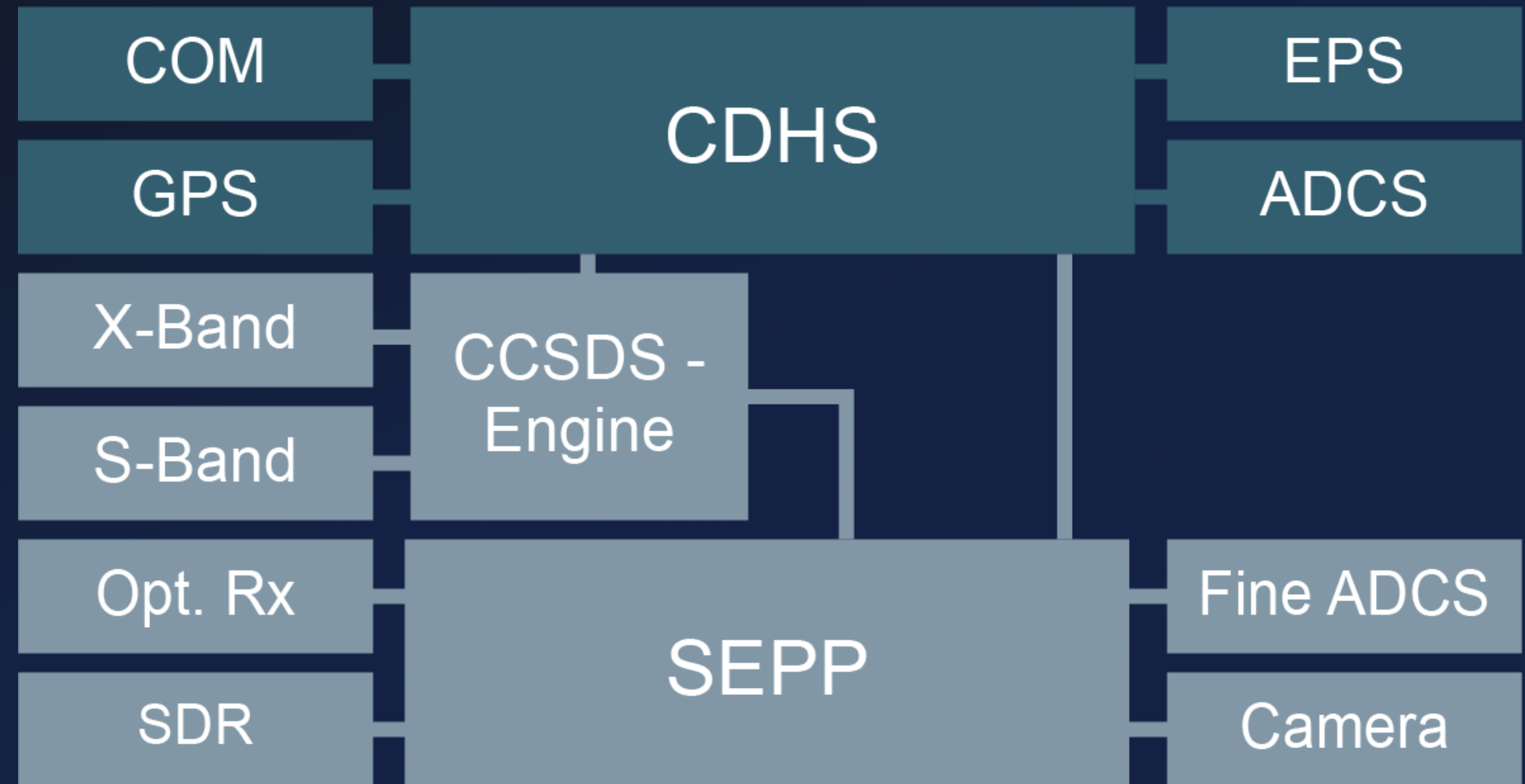
# System Chart



## Experimenter

Operated by ESA

Open for Research

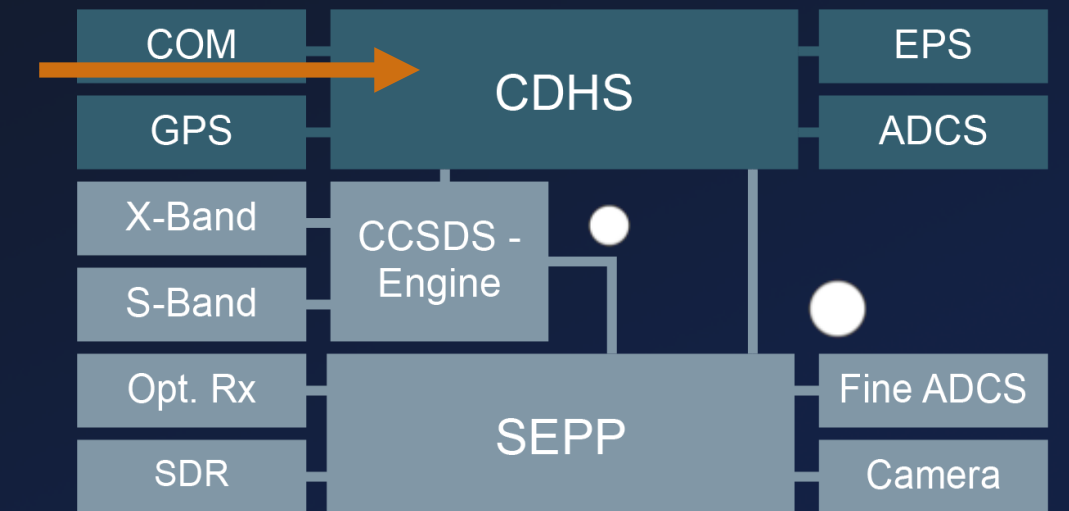


S-/X-Band, SDR, Optical Rx., Camera, ...

Peripherals

# UHF-Stack

## Cubesat Space Protocol (CSP) v1

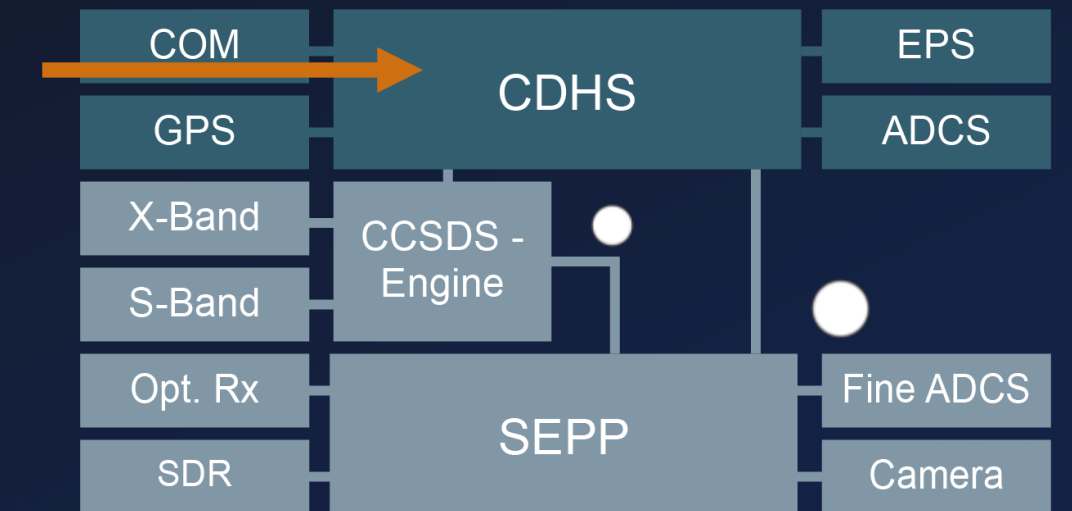


 TCP/IP Oriented Design

CSP Header 1.x																																
Bit offset	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	Priority		Source				Destination				Destination Port				Source Port				Reserved				H	X	R	C						
32	Data (0 – 65,535 bytes)																															

Source: [https://en.wikipedia.org/wiki/Cubesat\\_Space\\_Protocol](https://en.wikipedia.org/wiki/Cubesat_Space_Protocol)

# UHF-Stack

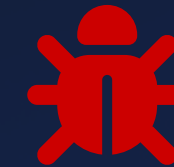


## Cubesat Space Protocol (CSP) v1



### Security Features

- HMAC-SHA1 Authentication
- XTEA Encryption Support

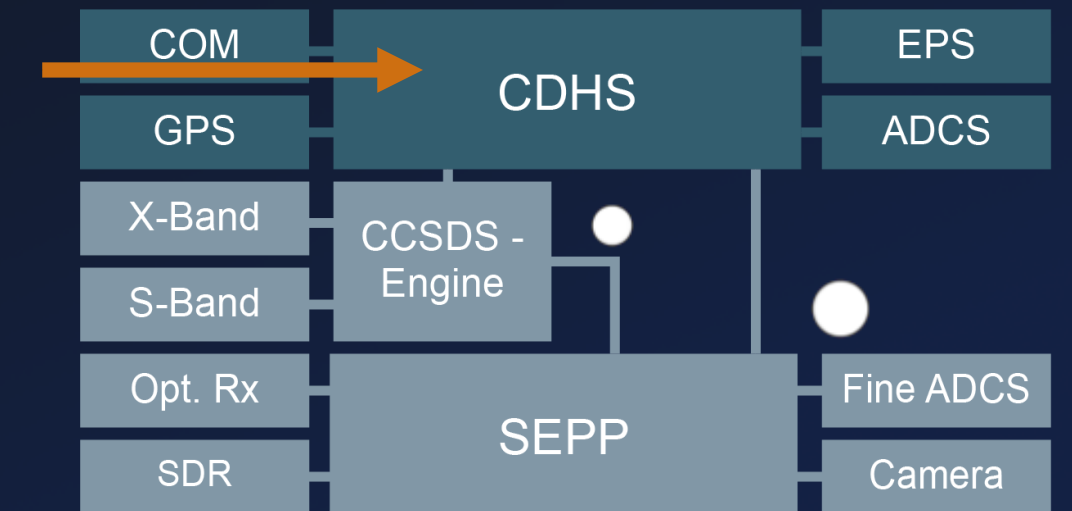


### Security Issues

1. MAC comparison leaks timing data #44
  - memcmp to compare the digest
2. HMAC doesn't protect headers #45
  - Same problem for the CRC checks
3. XTEA encrypt packet nonce too predictable #162
  - `const uint32_t nonce = (uint32_t)rand();`

*Authors: Issues fixed in libcsp v2*

# UHF-Stack

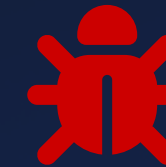


## Cubesat Space Protocol (CSP) v1



### Security Features

- HMAC-SHA1 Authentication
- XTEA Encryption Support

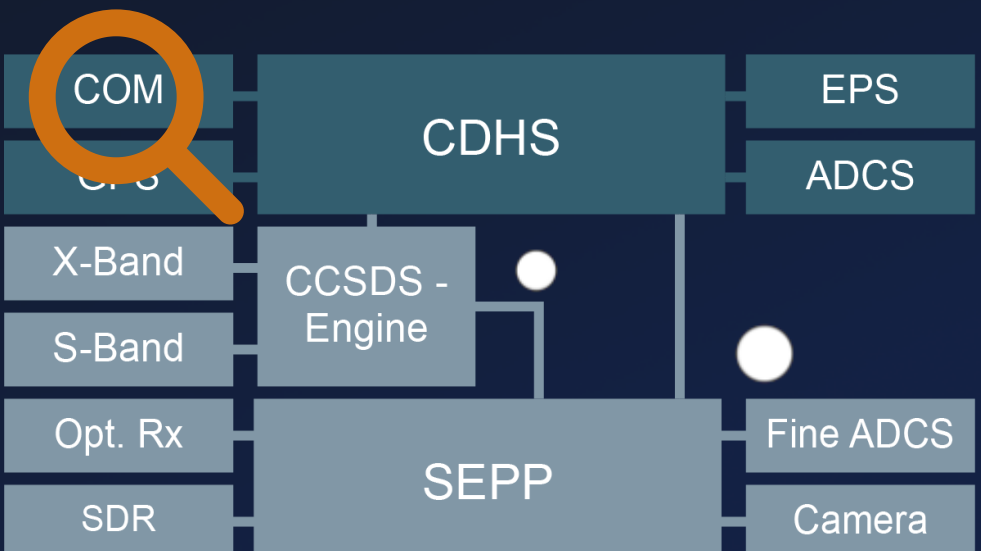


### Security Issues

1. MAC comparison leaks timing data #44
  - memcmp to compare the digest
2. HMAC doesn't protect headers #45
  - Same problem for the CRC checks
3. XTEA encrypt packet nonce too predictable #162
  - `const uint32_t nonce = (uint32_t)rand();`

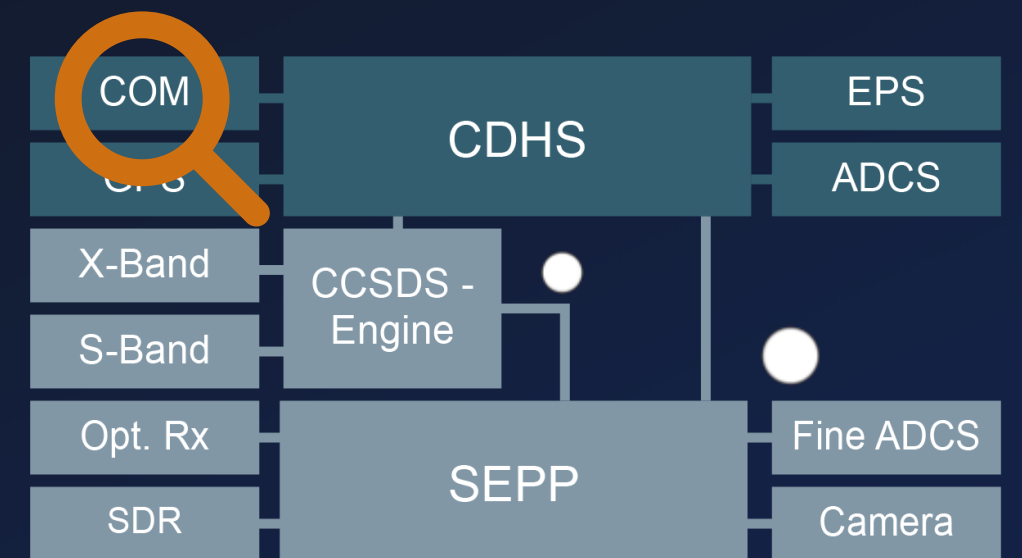
*Authors: Issues fixed in libcsp v2*

# Unprotected TCS



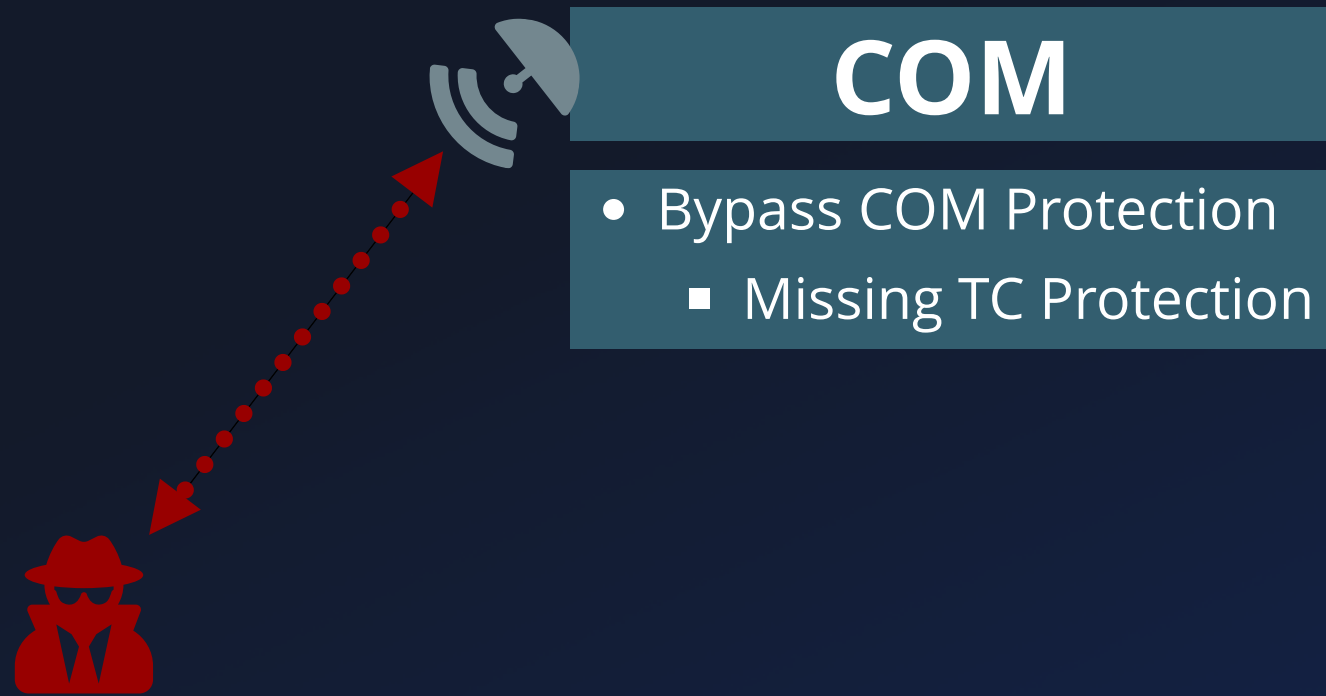


# Unprotected TCs



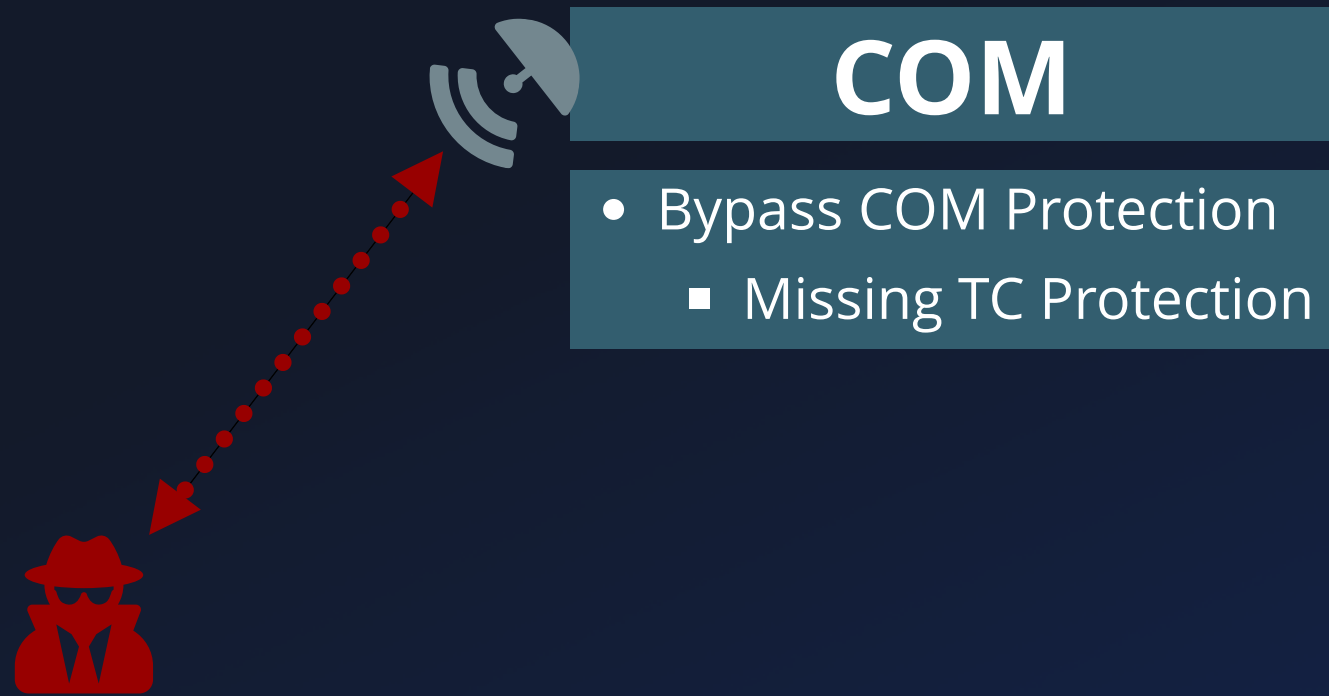
```
1 int csp_route_security_chek(...) {
2     if (packet->id.flags & CSP_FXTEA) {
3         csp_log_error("Received XTEA encrypted packet, but CSP
4         was compiled without XTEA support. Discarding packet");
5     }
6     // ...
7
8     if (packet->id.flags & CSP_FHMAC) {
9         csp_log_error("Received packet with HMAC, but CSP was
10        compiled without HMAC support. Discarding packet");
11    }
12    // ...
13 }
```

# Unprotected TCs



```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
2     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
3     char* pWriteData;
4
5     if (pAddr) {
6         if (g_sch_exec_mode != 1 ) {
7             /* exception and return */
8         }
9         char* pWriteData = &pAddr->start_of_data_buf;
10        if (pAddr->filesystem_target) {
11            // [...]
12        } else {
13            memcpy(pAddr->targetAddr,
14                  &pAddr->start_of_data_buf,
15                  pAddr->writeLength);
16        }
17    }
18    // ...
19 }
```

# Unprotected TCs



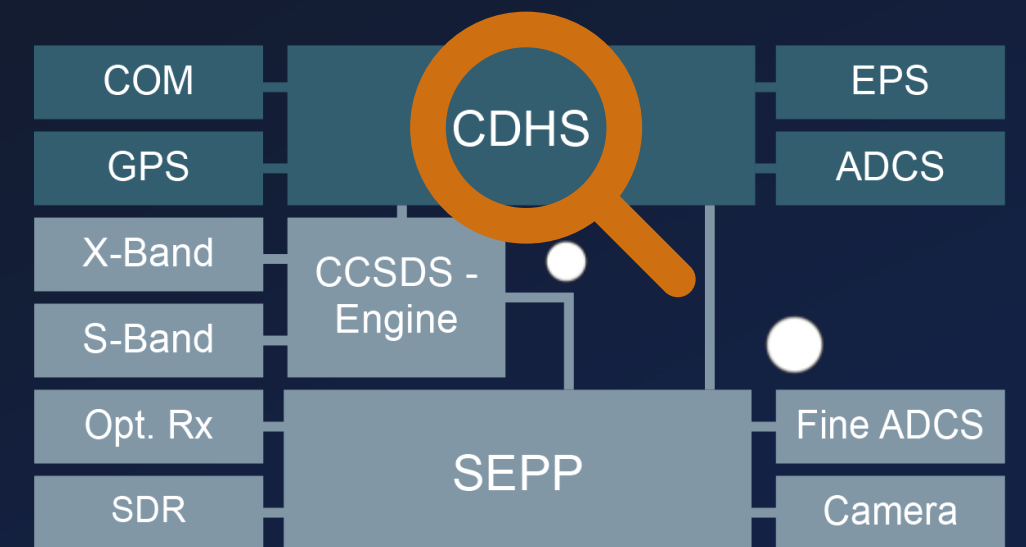
```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
2     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
3     char* pWriteData;
4
5     if (pAddr) {
6         if (g_sch_exec_mode != 1 ) {
7             /* exception and return */
8         }
9         char* pWriteData = &pAddr->start_of_data_buf;
10        if (pAddr->filesystem_target) {
11            // [...]
12        } else {
13            memcpy(pAddr->targetAddr,
14                  &pAddr->start_of_data_buf,
15                  pAddr->writeLength);
16        }
17    }
18    // ...
19 }
```

# Vulnerable TC

Cubesat Space Protocol (CSP)

ADCS Server

```
1 void task_adcs_servr() {
2   char log_file_name [32];
3
4   csp_listen(socket, 10);
5   csp_bind(socket, port);
6
7   do {
8     do {
9       conn = csp_accept(socket, 0xff);
10    } while (do_wait_for_conn);
11
12    packet = csp_read(conn, 10);
13    if (packet) {
14      packet_data = packet->data;
15      switch(*packet_data) {
16        // [...]
17        case SET_LOGFILE: {
18          packet_data = packet->data + 0xf;
19          log_file_name[0] = '\0';
20          strcat(log_file_name, packet_data);
21          // ...
22        }
23      }
24    }
25  }
```

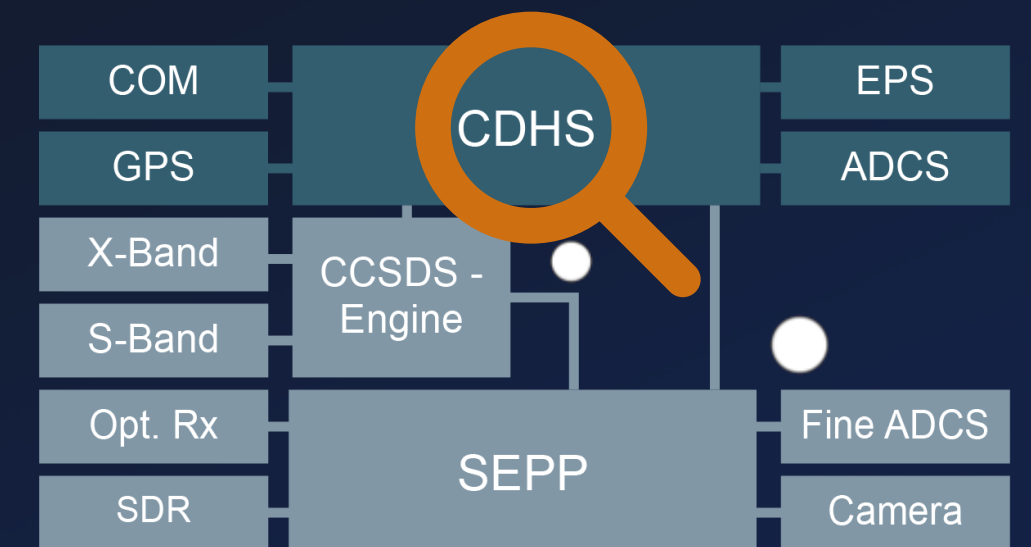


# Vulnerable TC

Cubesat Space Protocol (CSP)

ADCS Server

```
1 void task_adcs_servr() {
2   char log_file_name [32];
3
4   csp_listen(socket, 10);
5   csp_bind(socket, port);
6
7   do {
8     do {
9       conn = csp_accept(socket, 0xff);
10    } while (do_wait_for_conn);
11
12    packet = csp_read(conn, 10);
13    if (packet) {
14      packet_data = packet->data;
15      switch(*packet_data) {
16        // [...]
17        case SET_LOGFILE: {
18          packet_data = packet->data + 0xf;
19          log_file_name[0] = '\0';
20          strcat(log_file_name, packet_data);
21          // ...
22        }
23      }
24    }
25  }
```



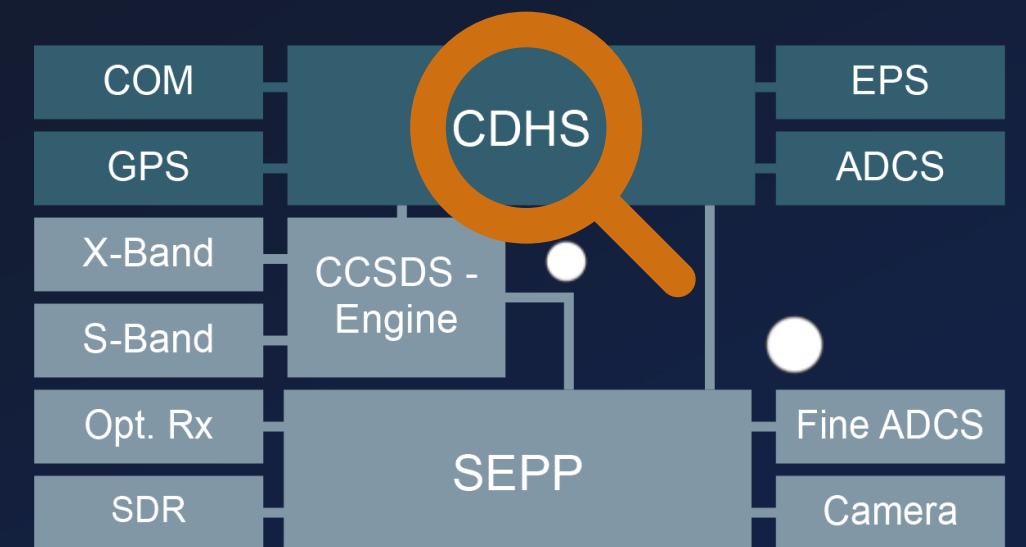


# Vulnerable TC

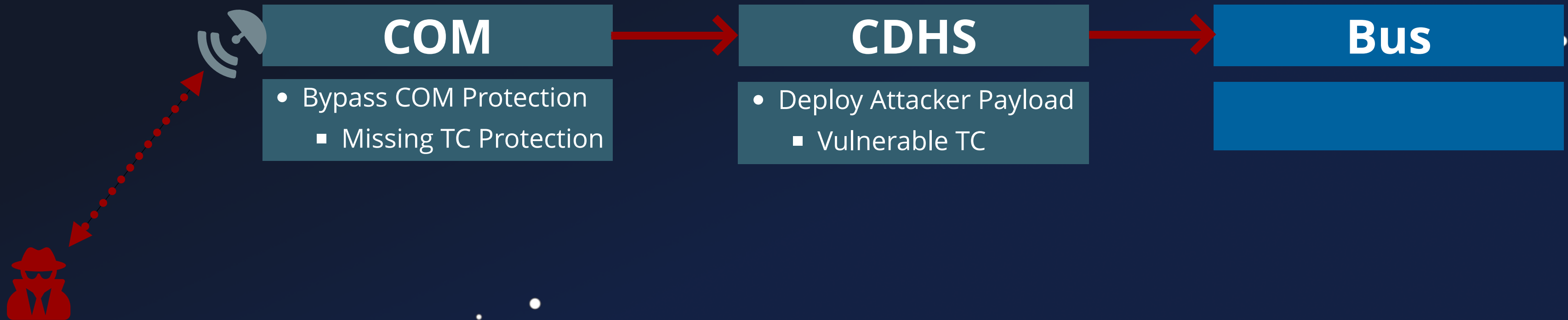
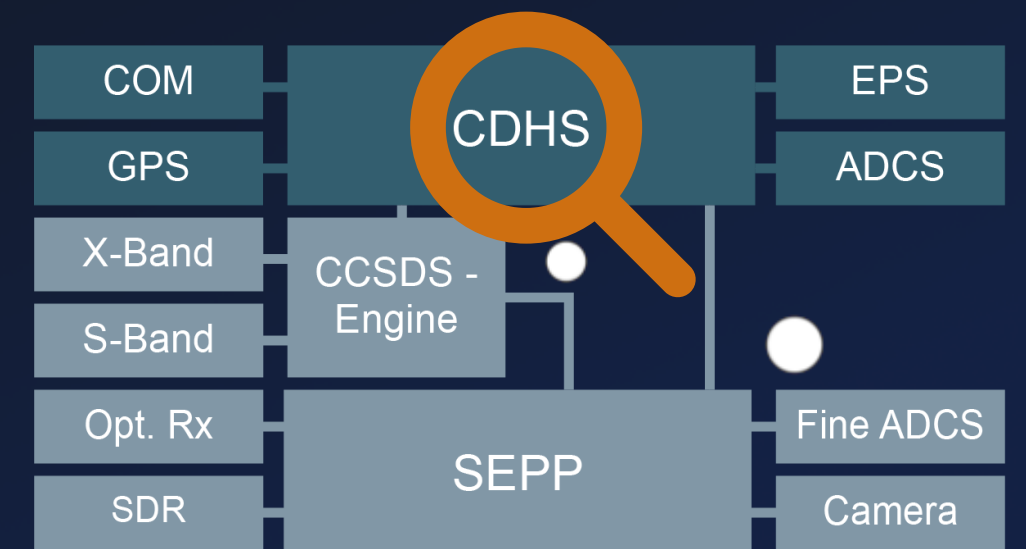
Cubesat Space Protocol (CSP)

ADCS Server

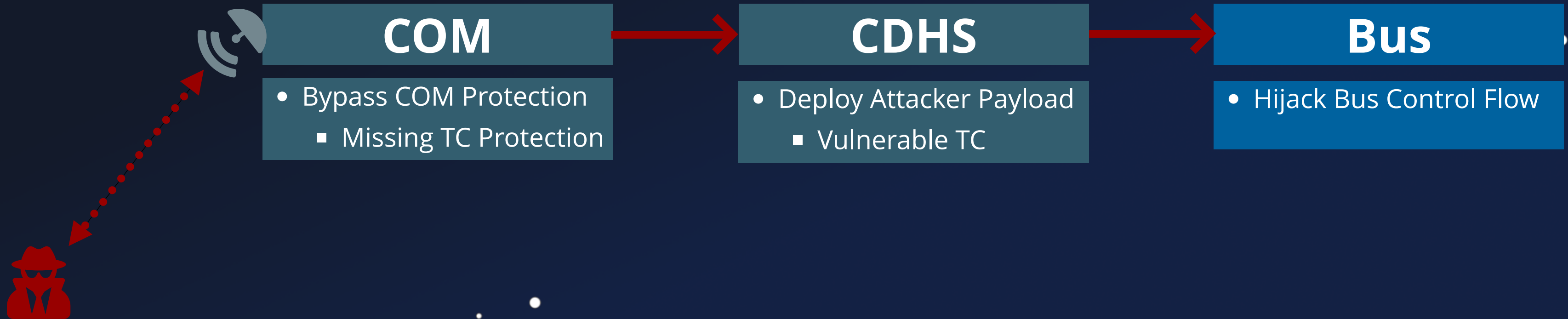
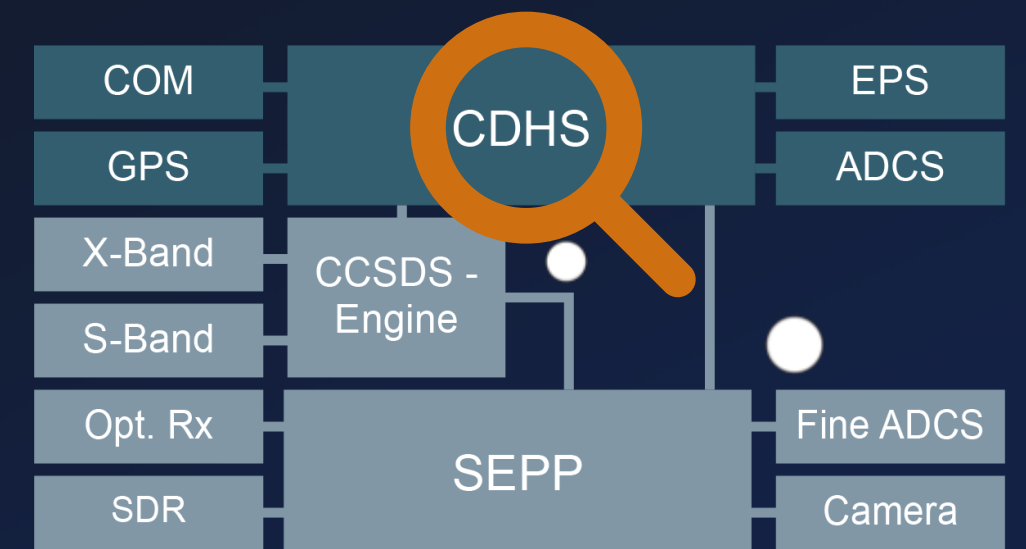
```
1 void task_adcs_servr() {
2   char log_file_name [32];
3
4   csp_listen(socket, 10);
5   csp_bind(socket, port);
6
7   do {
8     do {
9       conn = csp_accept(socket, 0xff);
10    } while (do_wait_for_conn);
11
12    packet = csp_read(conn, 10);
13    if (packet) {
14      packet_data = packet->data;
15      switch(*packet_data) {
16        // [...]
17        case SET_LOGFILE: {
18          packet_data = packet->data + 0xf;
19          log_file_name[0] = '\0';
20          strcat(log_file_name, packet_data);
21          // ...
22        }
23      }
24    }
25  }
```



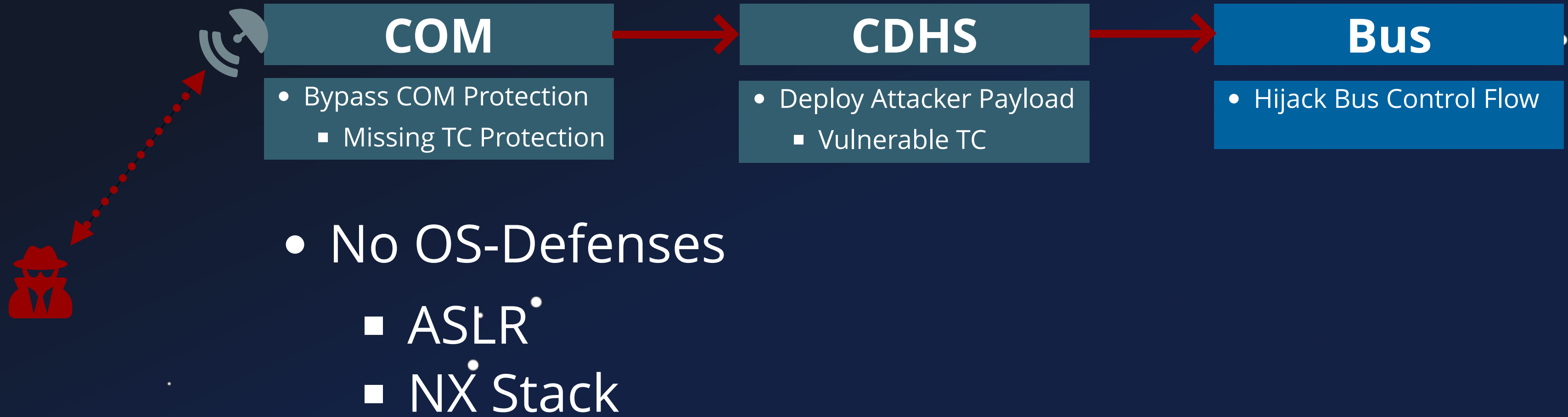
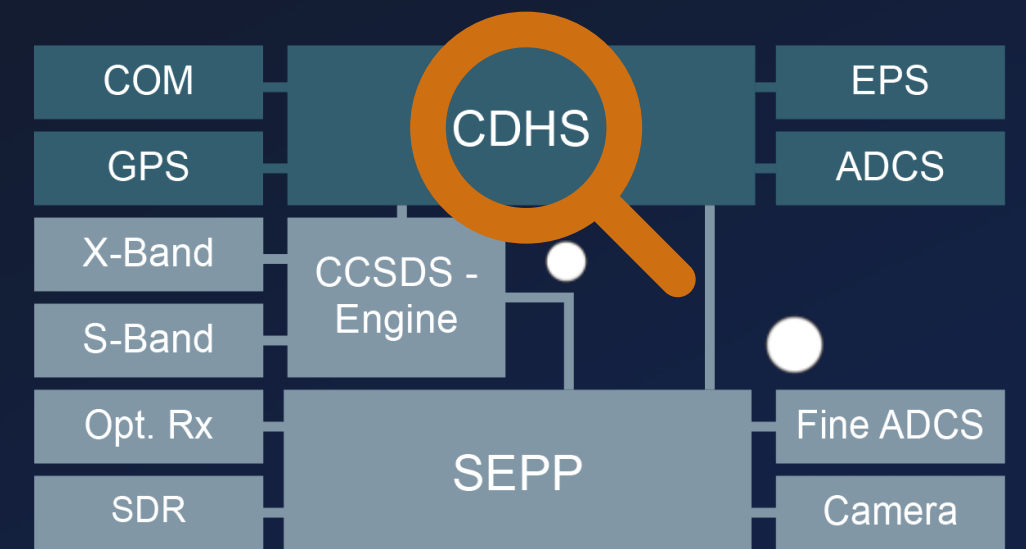
# Defenses - 404?



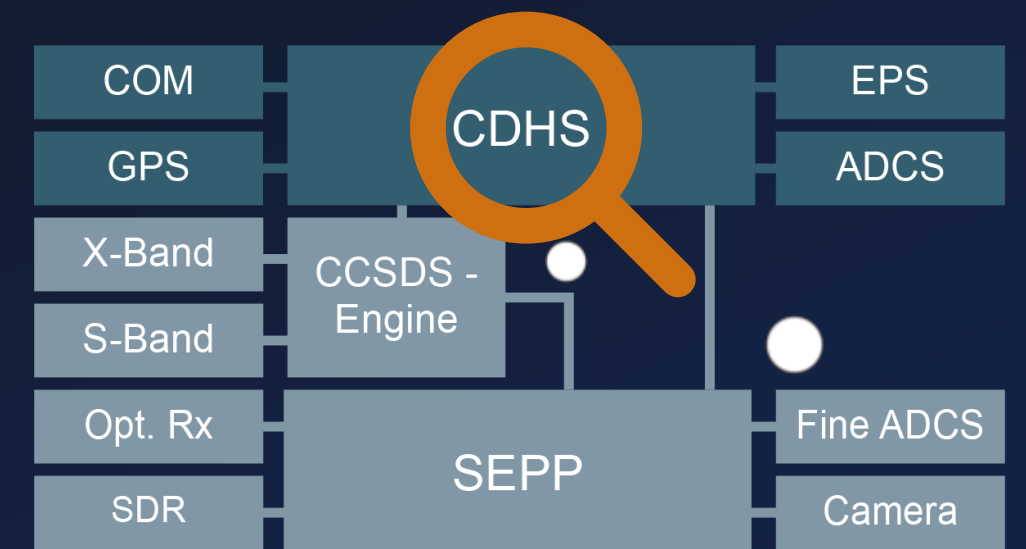
# Defenses - 404?



# Defenses - 404?



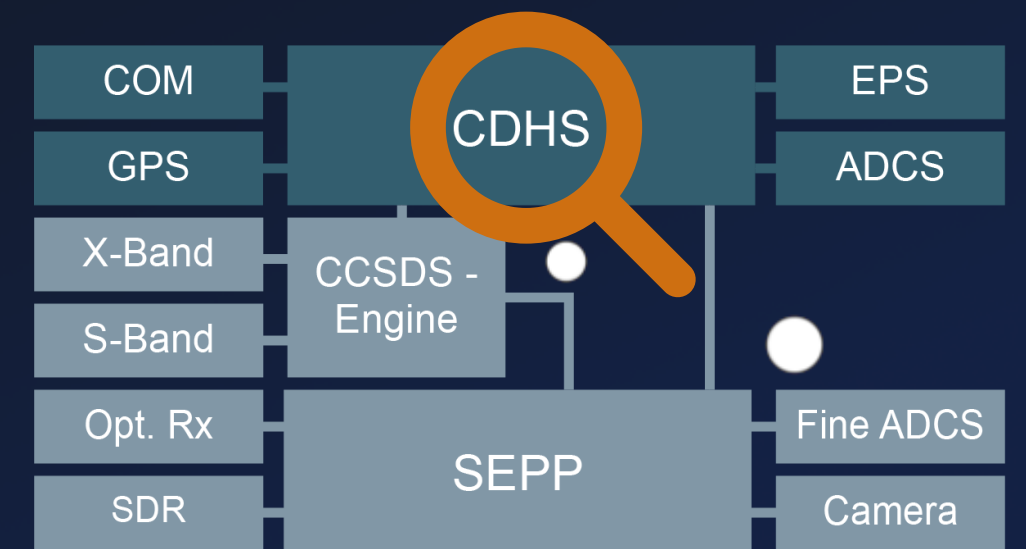
# Defenses - 404?



- No OS-Defenses
  - ASLR
  - NX Stack
- No SW-Defenses
  - Stack Cookies

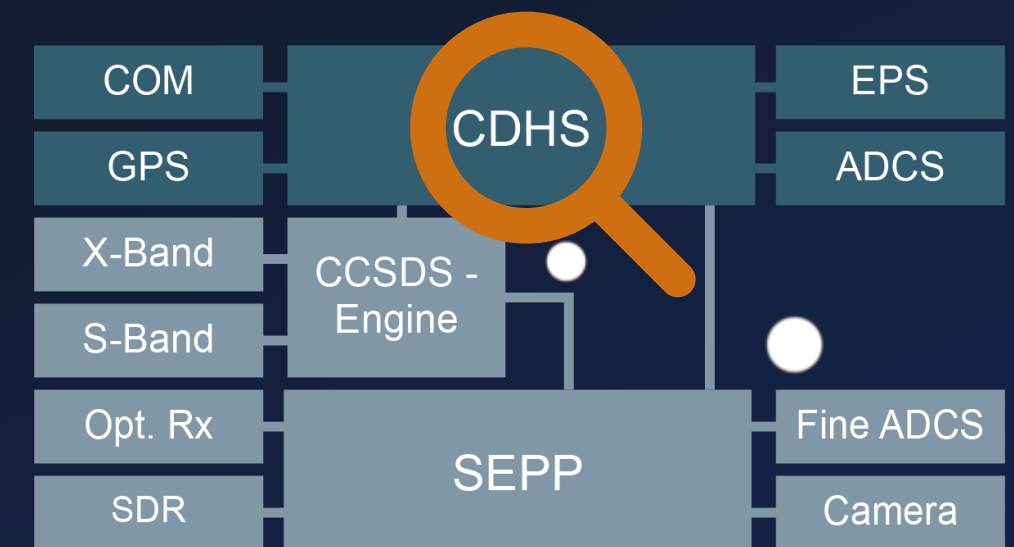


# Defenses - 404?



- No OS-Defenses
  - ASLR
  - NX Stack
- No SW-Defenses
  - Stack Cookies

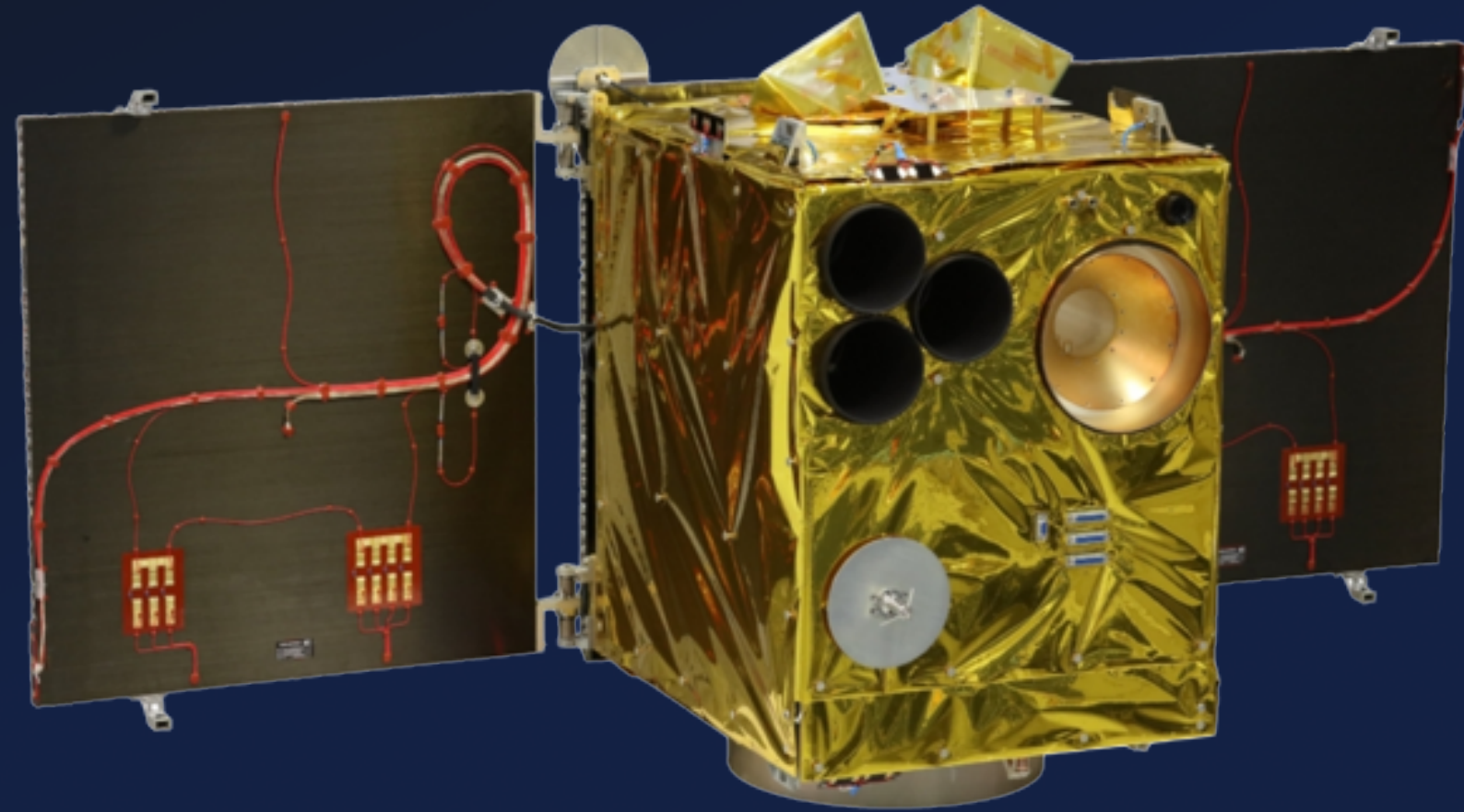
# Defenses - 404?



- No OS-Defenses
  - ASLR
  - NX Stack
- No SW-Defenses
  - Stack Cookies

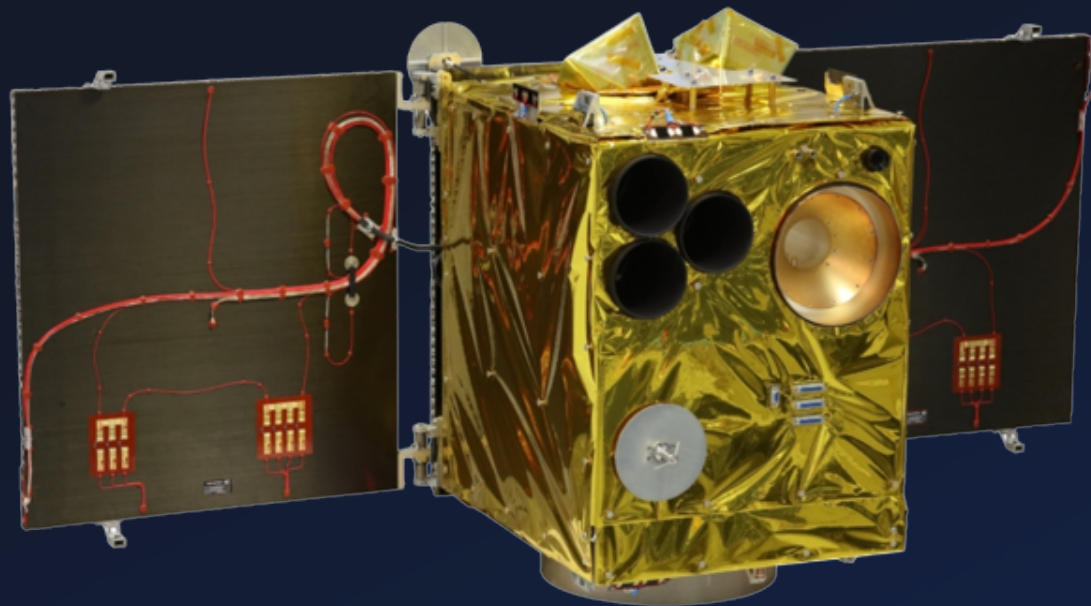
- Privilege-free RTOS

# Flying Laptop



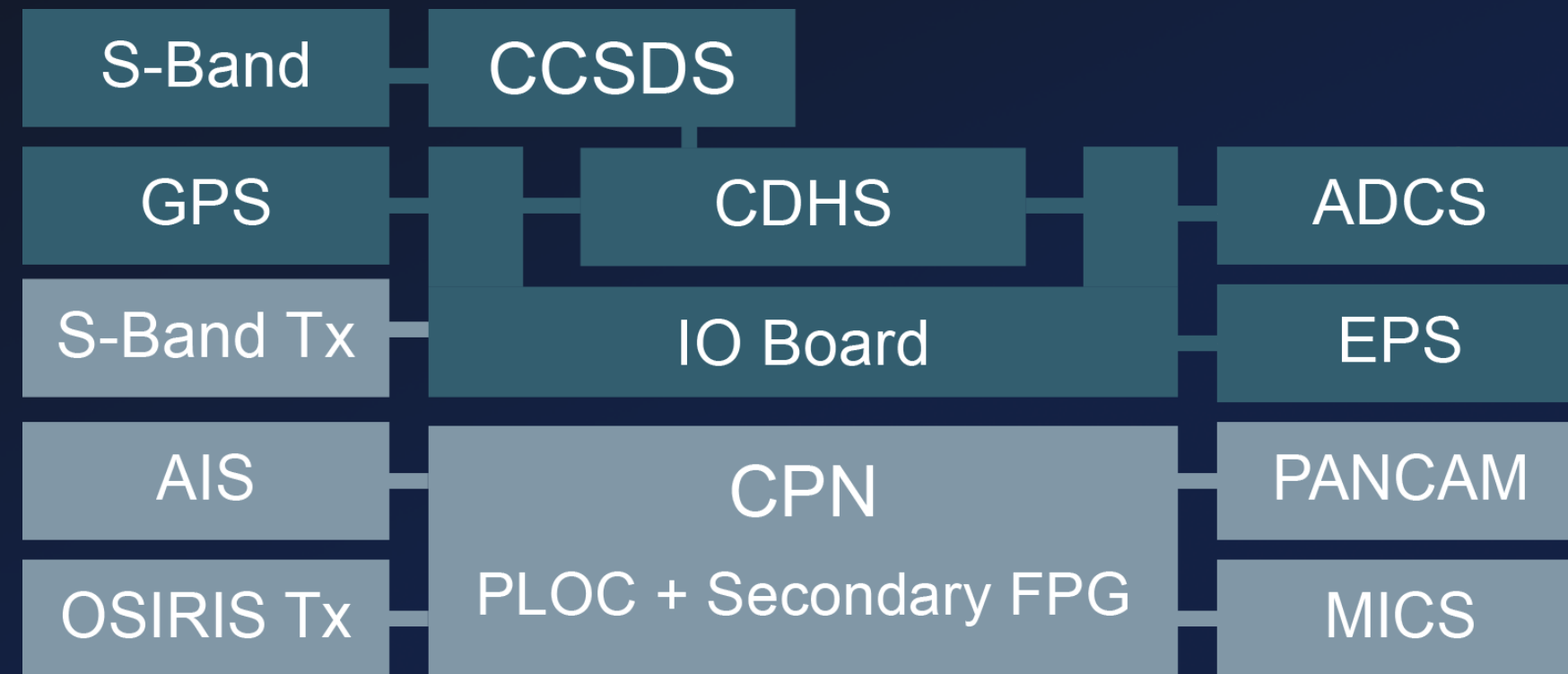


# Flying Laptop



## Technology Tester

Co-Developed by  
Airbus Space & Defense



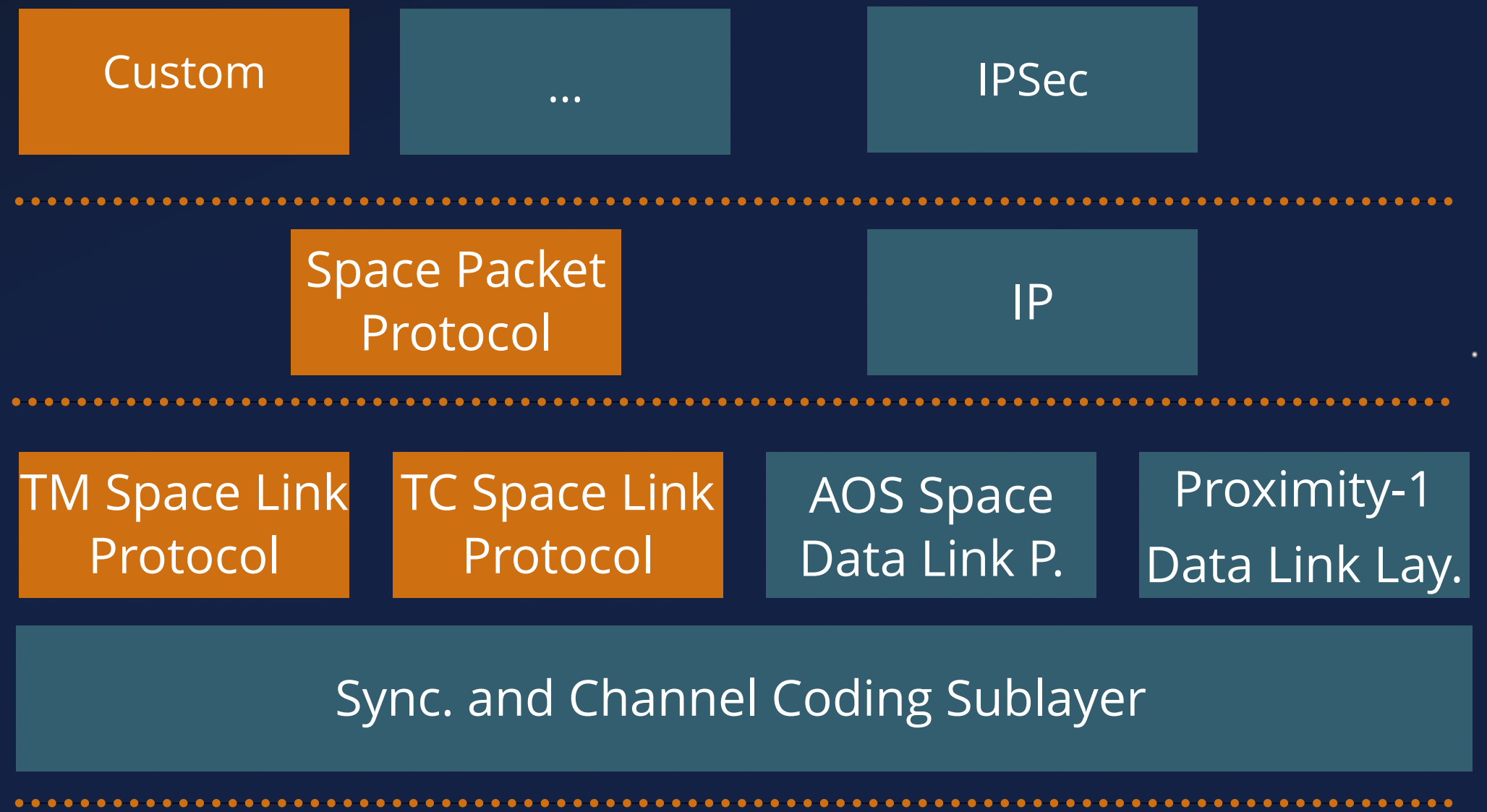
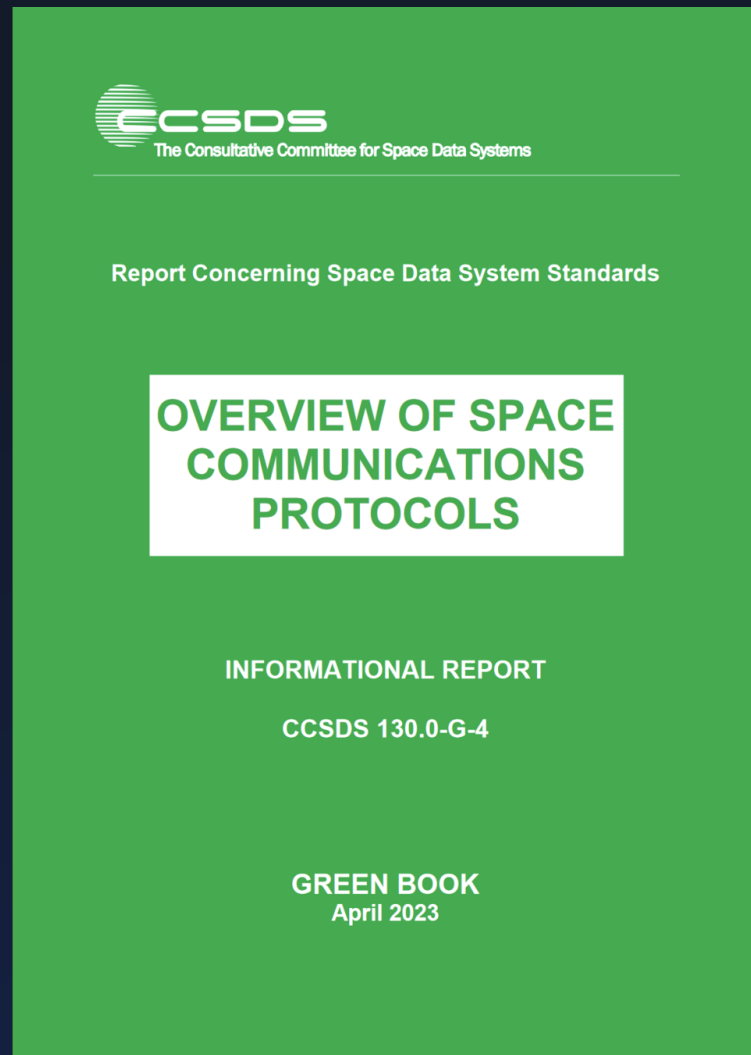
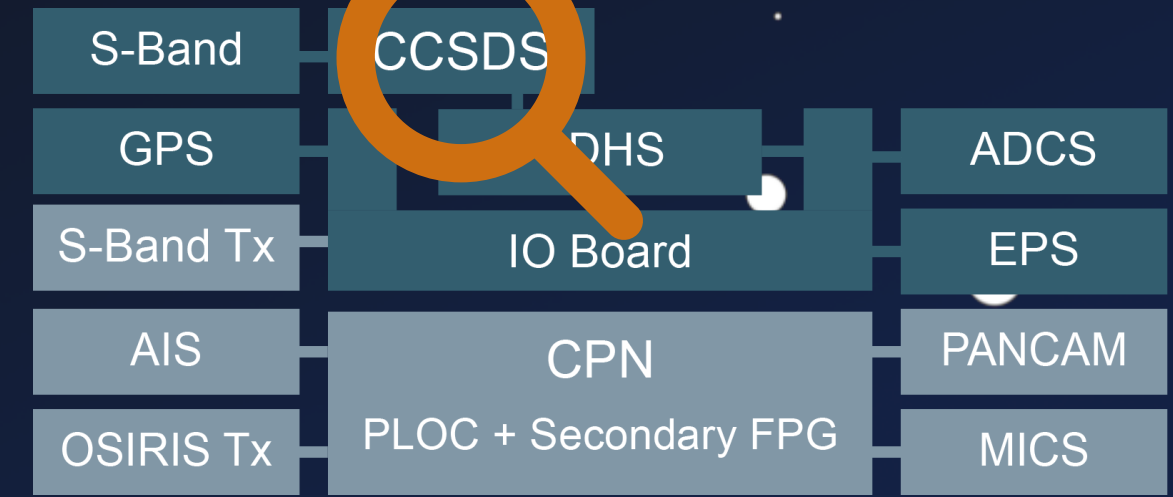
De-orbit mechanism, AIS, Camera, etc...

Peripherals

SPARC LEON 3 - OBC from Airbus S&D

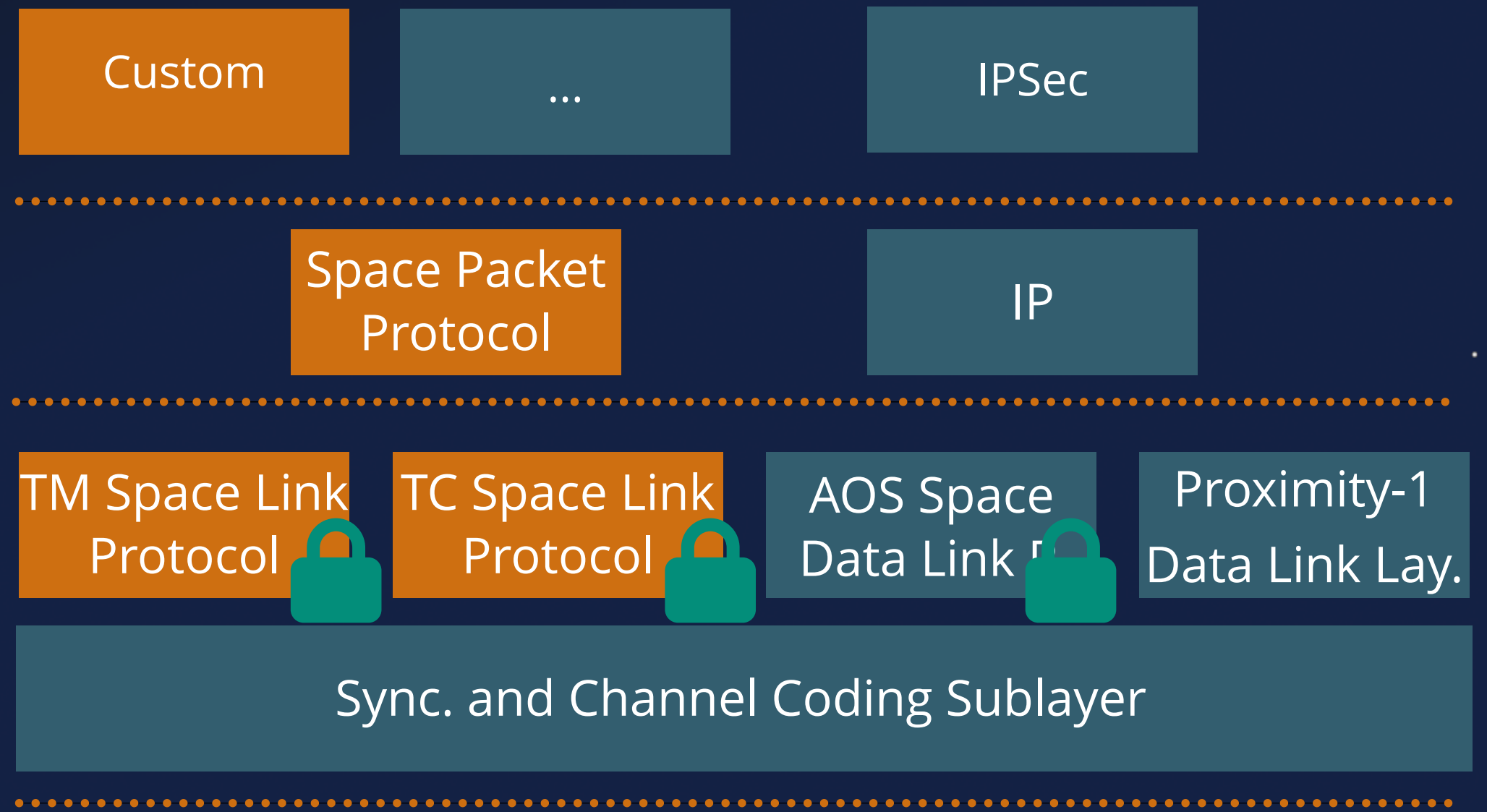
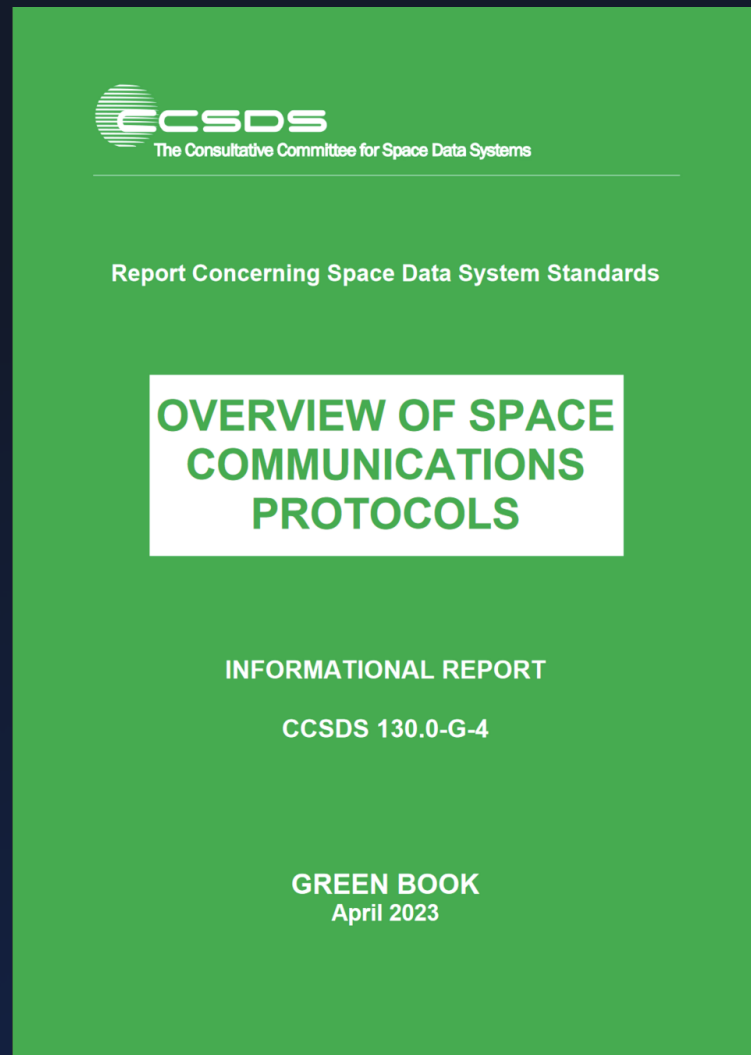
Bus Platform

# CCSDS





# CCSDS



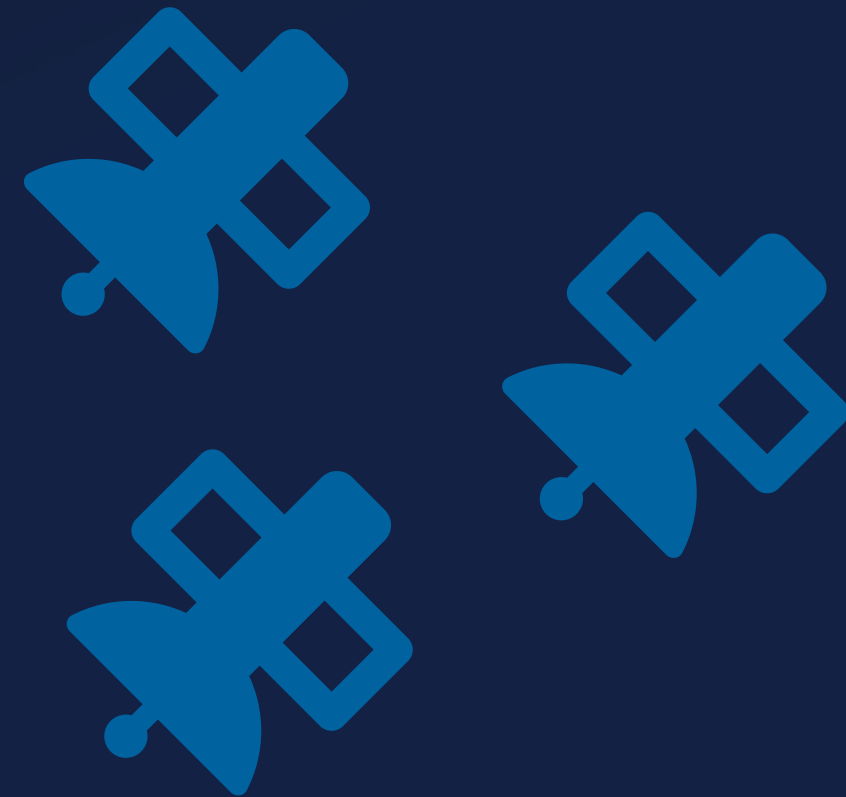
# Bigger Picture



***"But it's different for  
[...] satellites."***

***“ But it's different for  
[...] satellites,  
.... right?”***

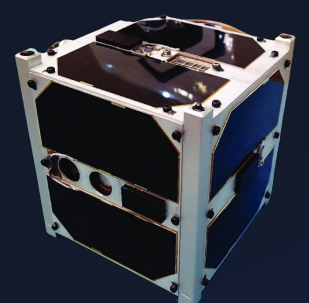
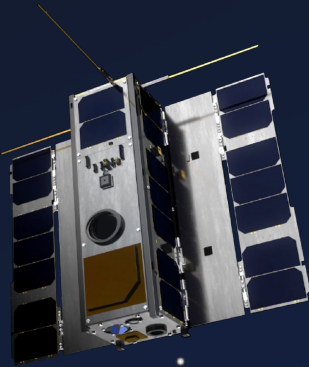
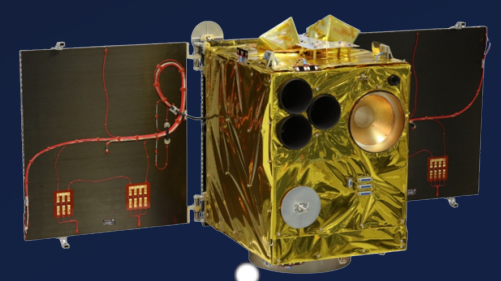
# Developer Survey





# TC Protocols



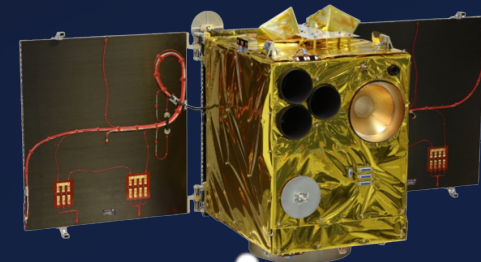
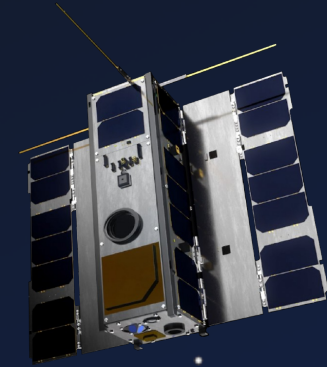
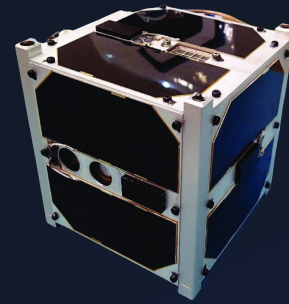
	Custom	Standard	Weight
	✓	✗	~ 1.3 kg
	~	✓	~ 5.4 kg
	✗	✓	~ 120 kg

Weight ≈ Money

# TC Protocols



Custom /  
Standard



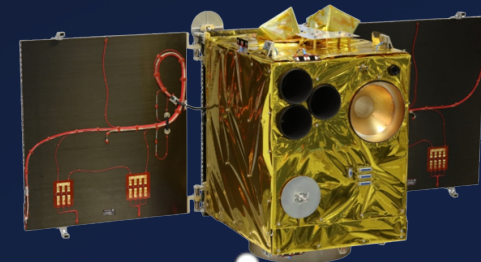
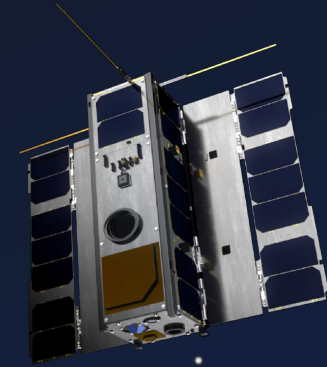
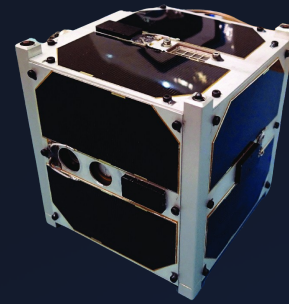
	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
$\Sigma$	10	2	5

Weight  $\approx$  Money

# TC Protocols



Custom /  
Standard



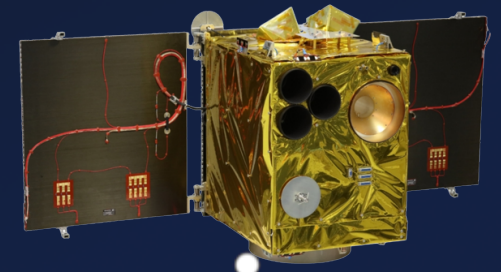
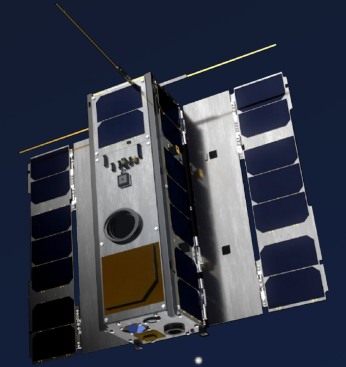
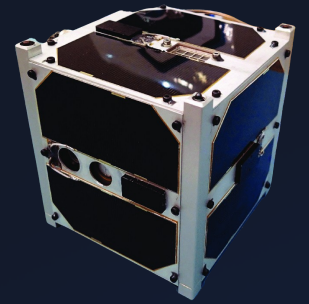
	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
$\Sigma$	10	2	5

Weight  $\approx$  Money

# TC Protocols



Custom /  
Standard



	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
$\Sigma$	10	2	5

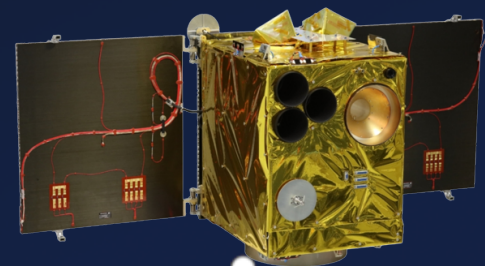
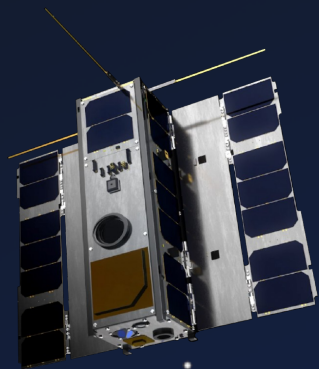
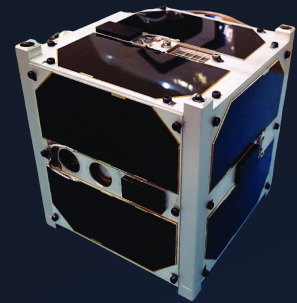
Weight  $\approx$  Money



# TC Protocols



Custom /  
Standard



	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
$\Sigma$	10	2	5

Weight  $\approx$  Money

=> Inaccessible Standard



# TC Protocols

---



*// Inaccessible Standard*

# TC Protocols

---



*// Inaccessible Standard*



Grown over  
Decades

# TC Protocols

---



*// Inaccessible Standard*



Grown over  
Decades



- Unknown Requirements

# TC Protocols

---



*// Inaccessible Standard*



Grown over  
Decades



• Unknown  
• Requirements



No Best  
Practices

# TC Protocols

---



*// Inaccessible Standard*



Grown over  
Decades



• Unknown  
Requirements



No Best  
Practices



Few Open-Source  
Implementations



# TC Protocols

---



*// Inaccessible Standard*



Grown over  
Decades



- Unknown Requirements



No Best  
Practices



Few Open-Source  
Implementations

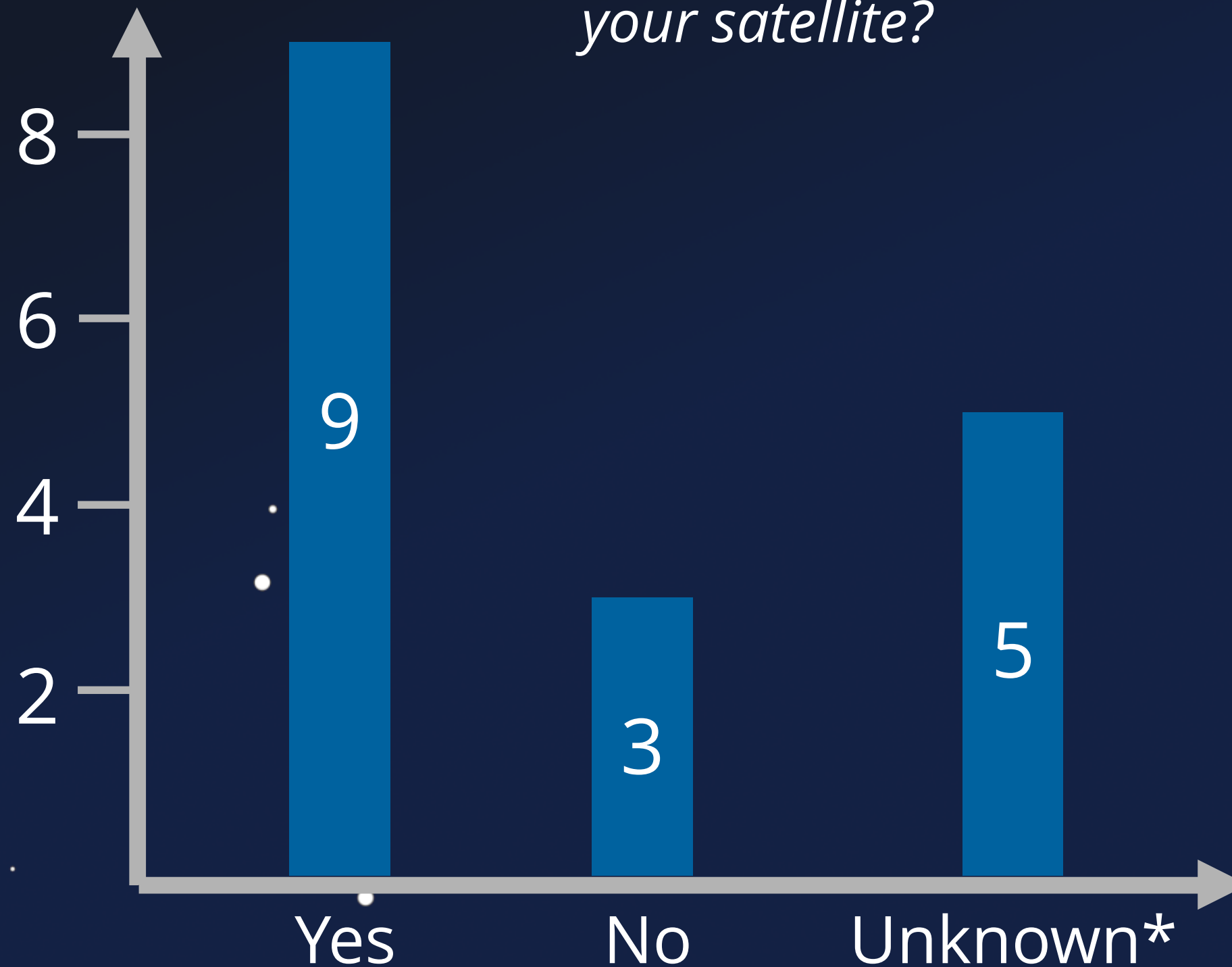


"Guideline" Standards

# TC Protection



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

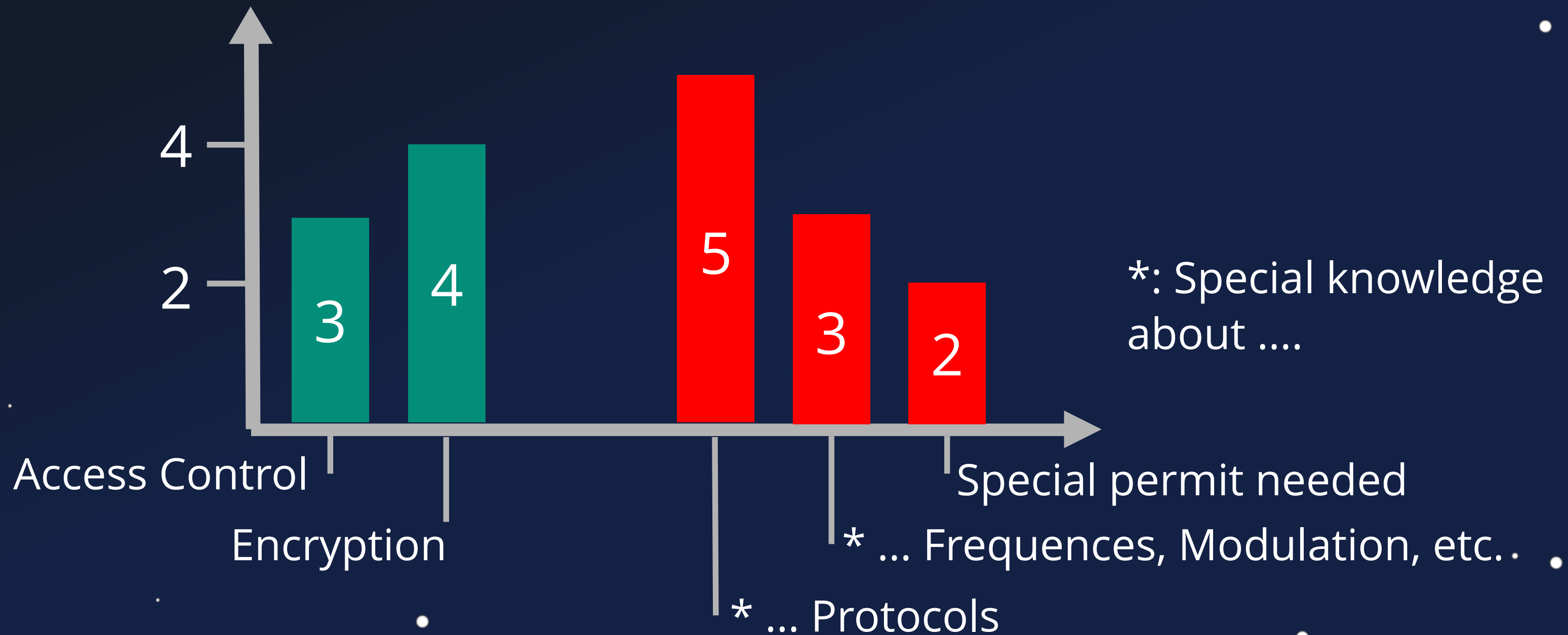


Unknown\*:  
Prefer not to say /  
Don't know

# TC Obscurity



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



# Security by Obscurity

---



// ~~No Insights  $\leftrightarrow$  No Attacker~~



More Developers  
More People Involved



Commercial off-the-Shelf  
(COTS)  
Components

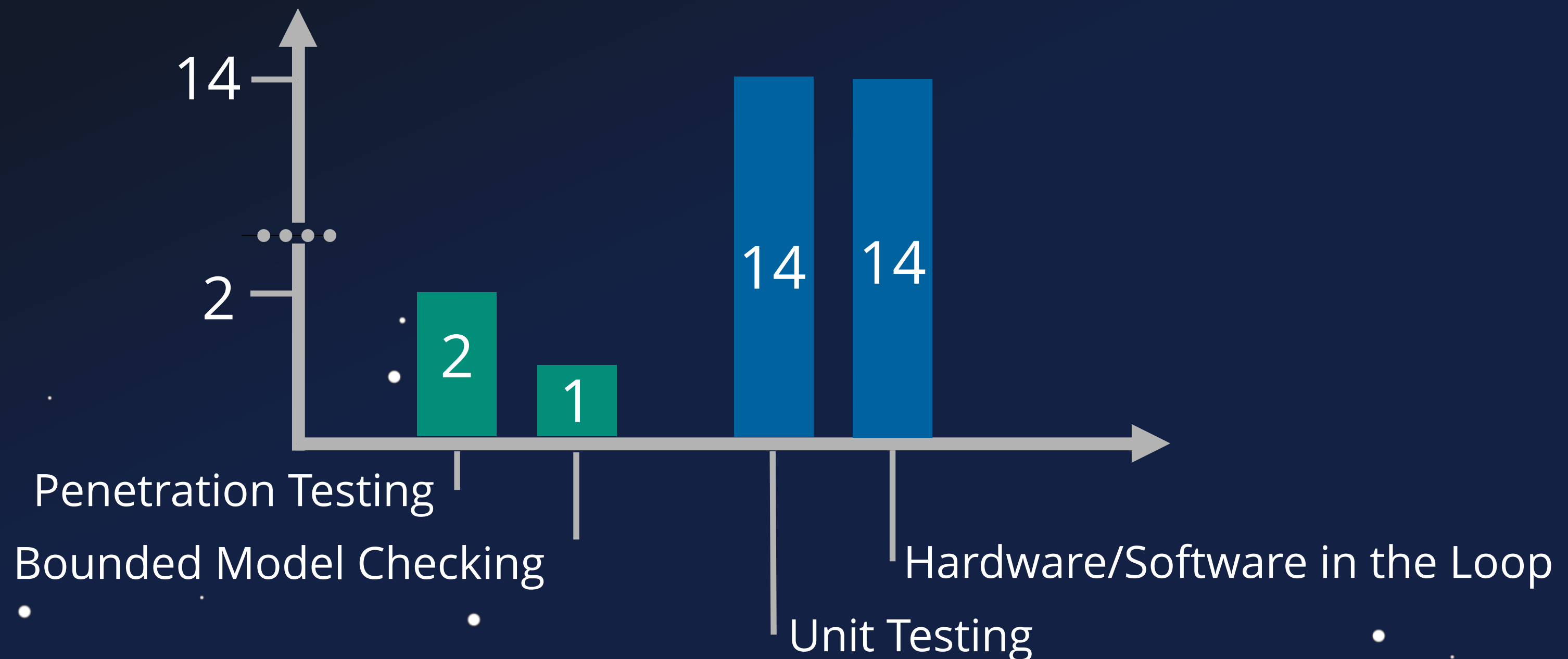


Higher Stakes  
Critical Infrastructure

# Security Testing



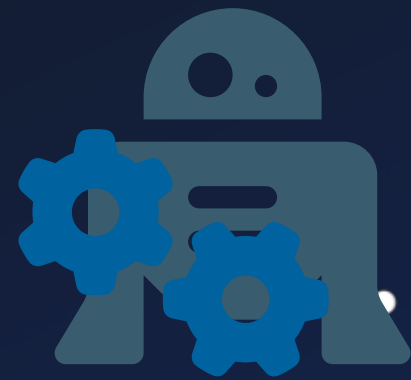
Question: **Which, if any, methods, tools or techniques** were used to ensure/improve code quality? (Multiple Answers Possible)





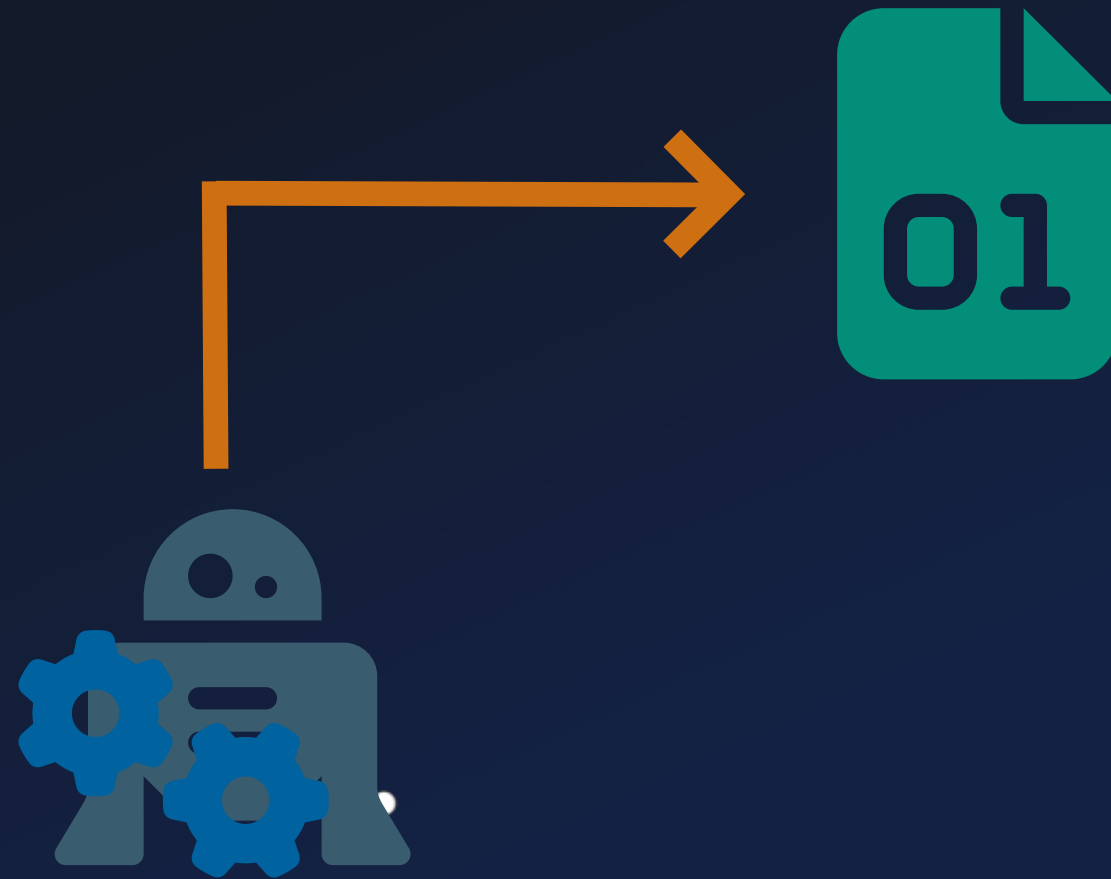
# Fuzzing

---



# Fuzzing

---



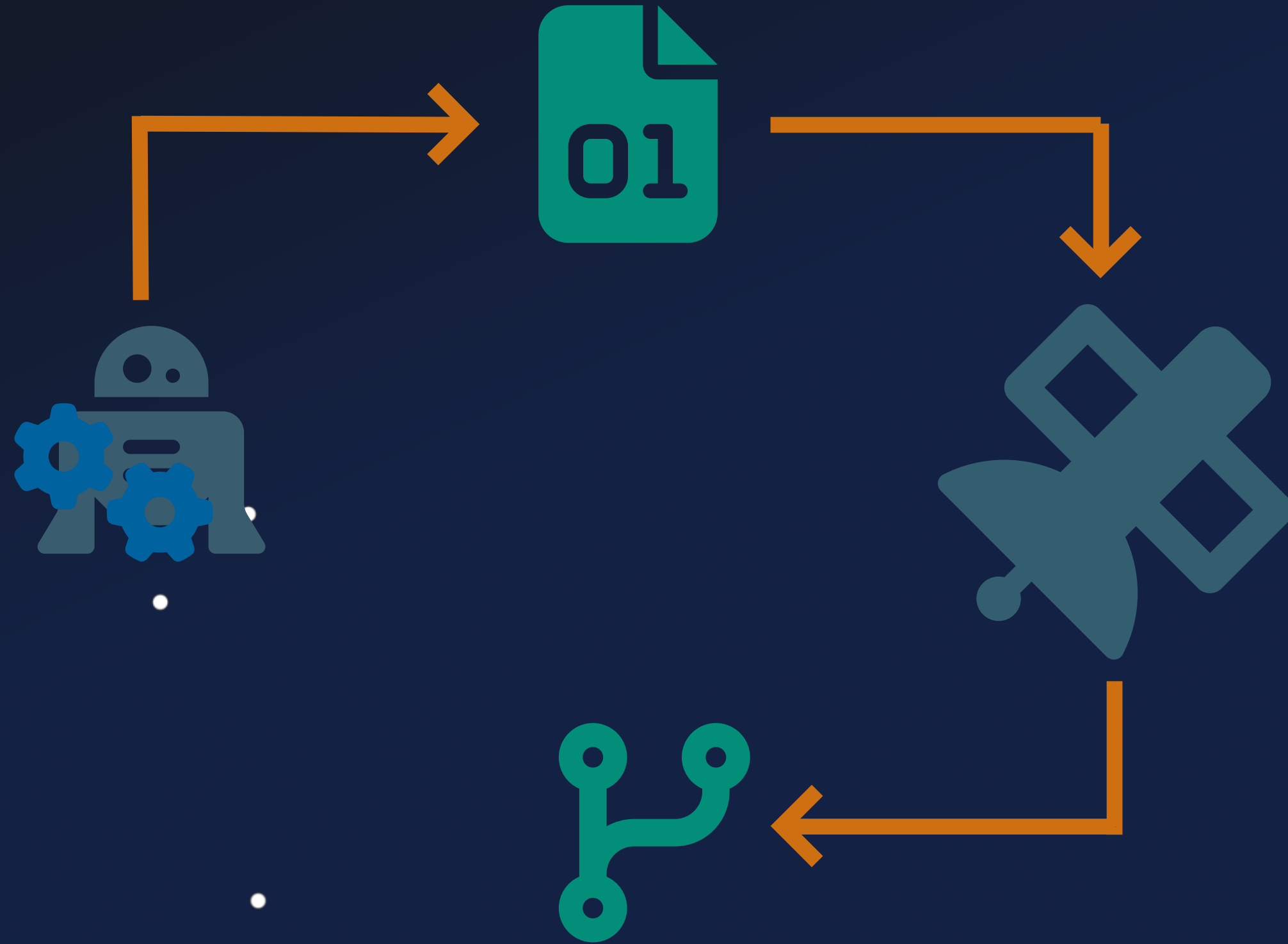
# Fuzzing

---



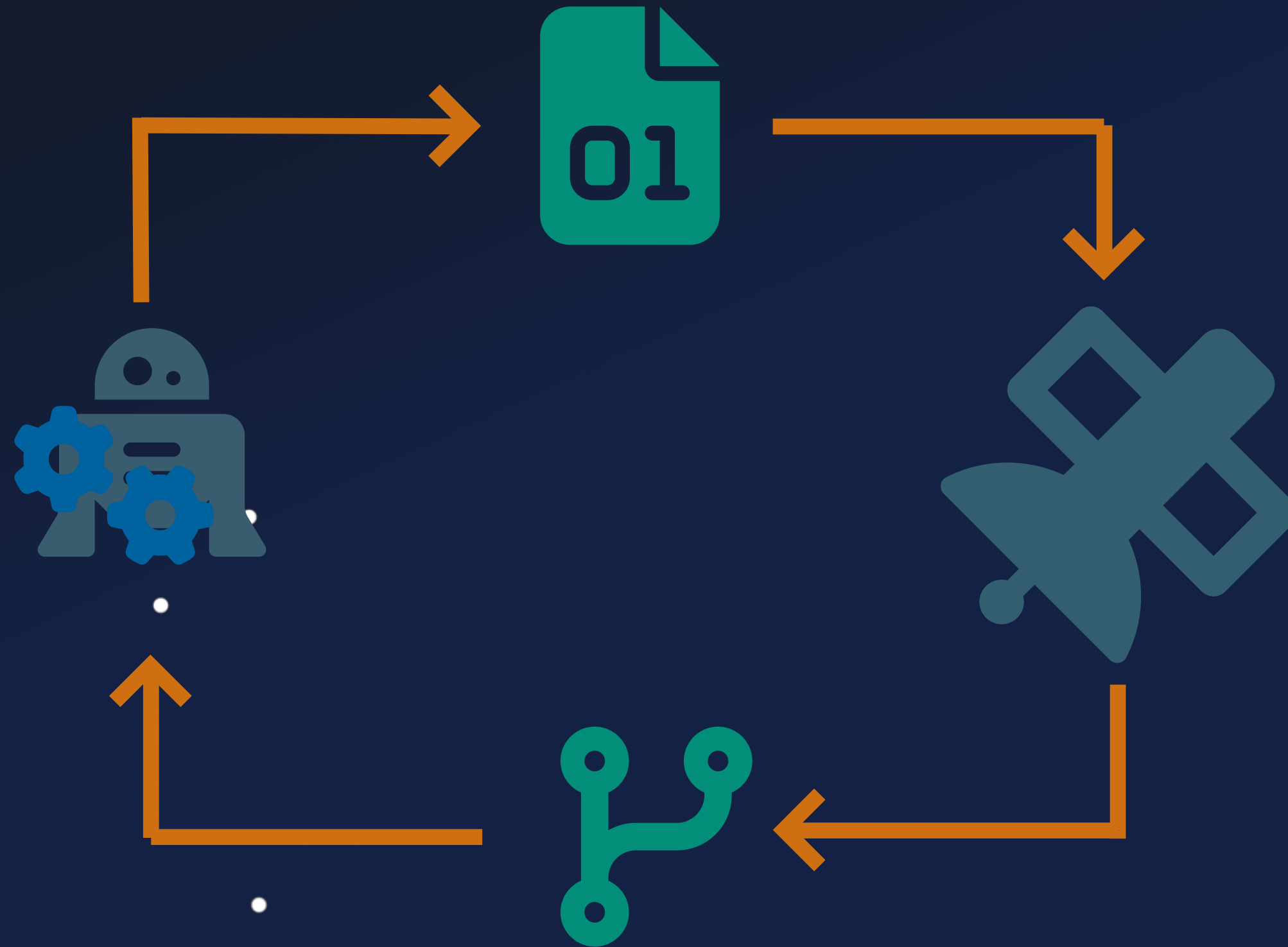
# Fuzzing

---



# Fuzzing

---





*" But it's different for  
\*my\* satellite*

# Impact



1. Hack a Satellite



2. ???



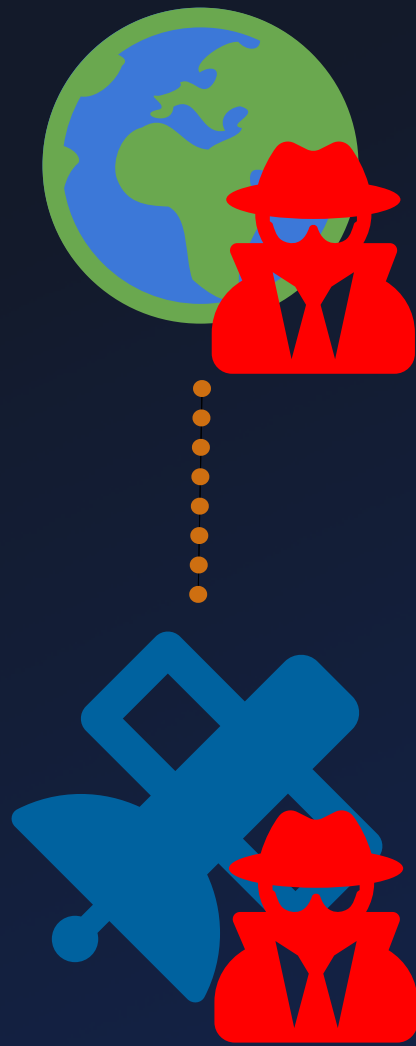
# Scenariós

---



# Scenariós

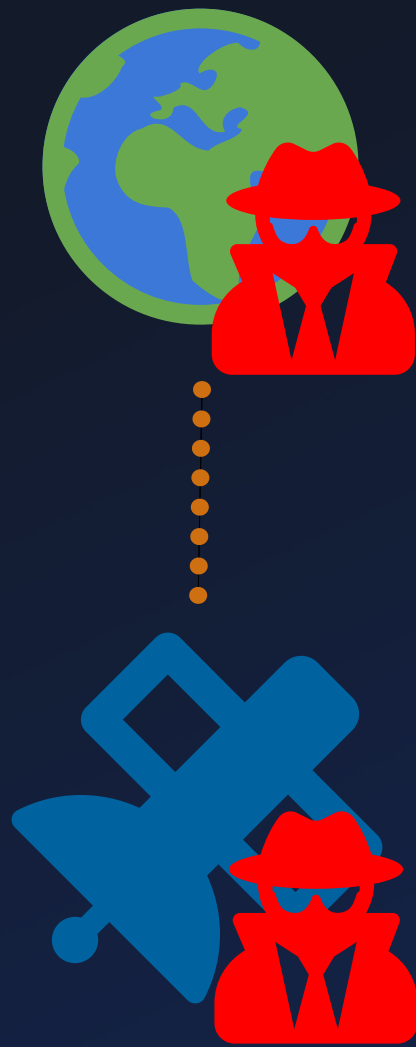
---



Orbital Access

# Scenarios

---



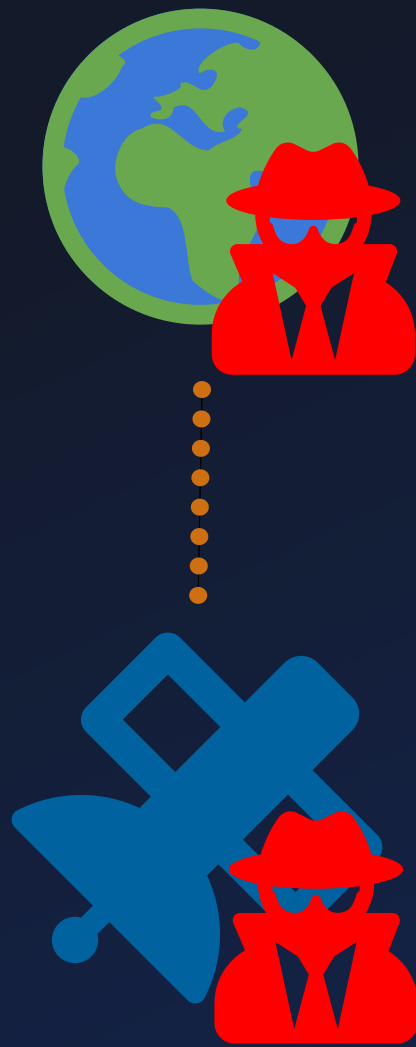
Orbital Access

- ① Attacking Inter-Sat Links



# Scenarios

---

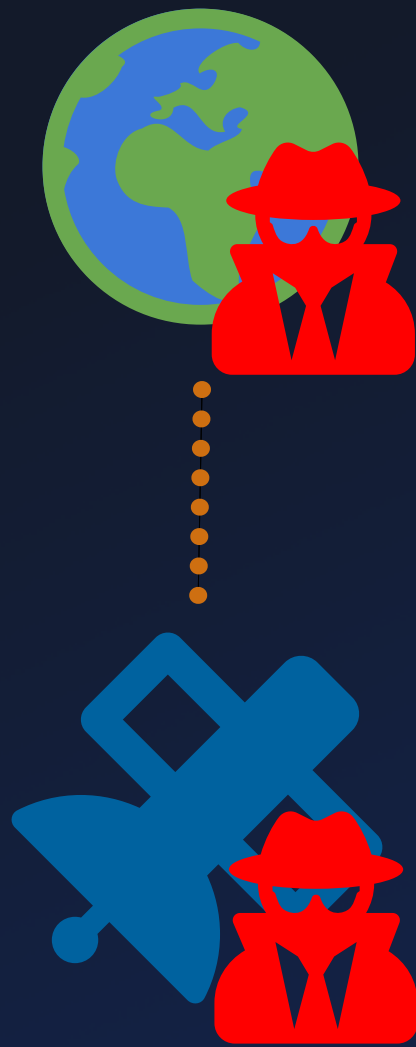


Orbital Access

- ① Attacking Inter-Sat Links
- ② Orbital Traffic Interception

# Scenarios

---

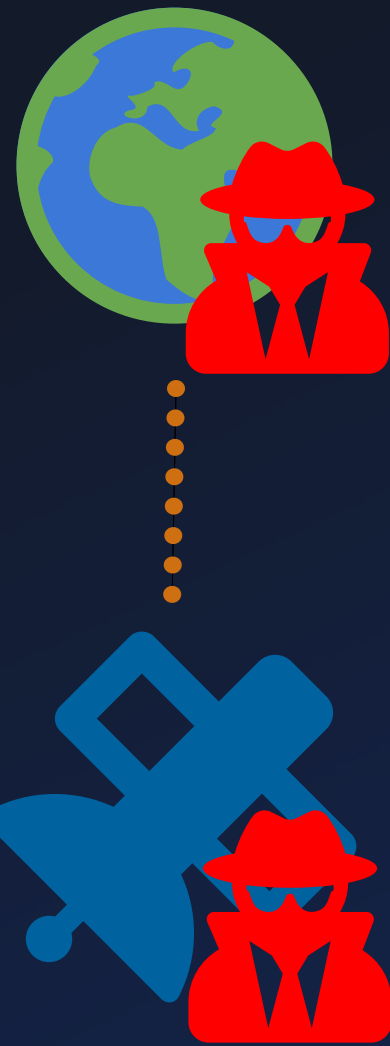


Orbital Access

- ① Attacking Inter-Sat Links
- ② Orbital Traffic Interception
- ③ Orbital Denial-of-Service

# Scenarios

---



Orbital Access

- ① Attacking Inter-Sat Links
- ② Orbital Traffic Interception
- ③ Orbital Denial-of-Service
- ④ Kessler Syndrome

# Attacker Perspective



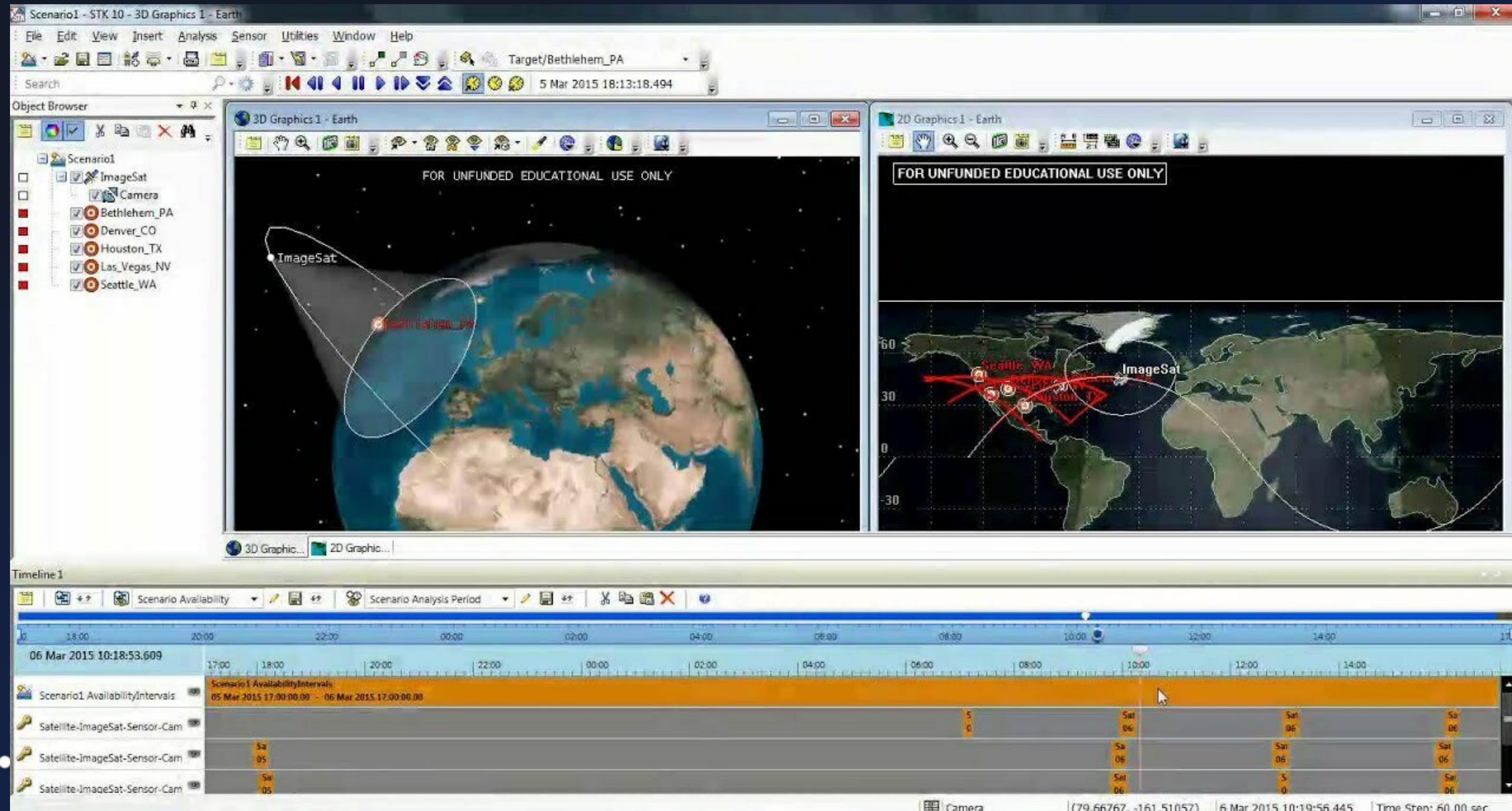
# Hack-a-Sat

---





# Math? Math!





# HACK-A-SAT CONTACT WINDOW TIMELINE

▲ Contact Window Deadline for Team Submissions

◆ Overnight Deadline for Team Submissions

□ Contact Window

■ Game Hours

■ Off Hours

■ ACS

FRI GAME START 9AM

FRI GAME STOP 7PM

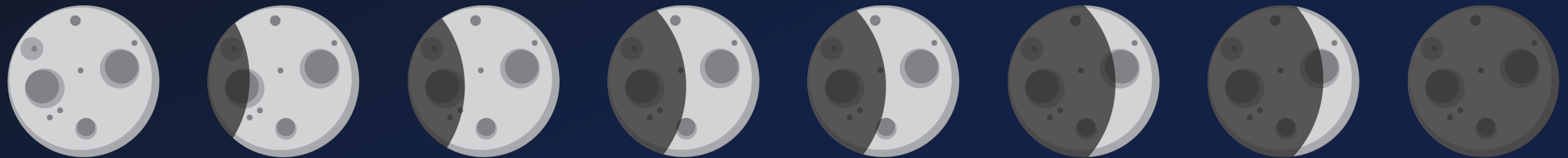
SAT GAME START 10AM

SAT GAME STOP 6PM



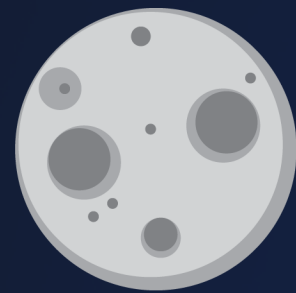


# Lesson Learnt

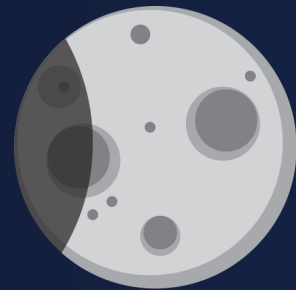


# Lessons Learnt

---



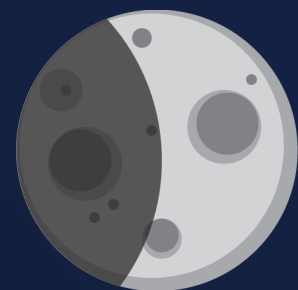
Firmware Attacks on Satellites are a Thing



ViaSat Incident != Satellite Firmware Attack



Common Sat Protocols lack Security



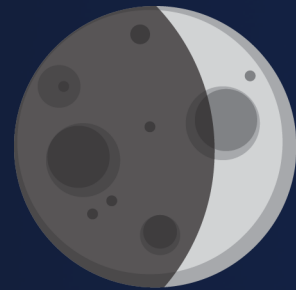
Security by Obscurity

# Lessons Learnt

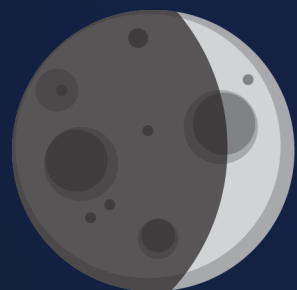
---



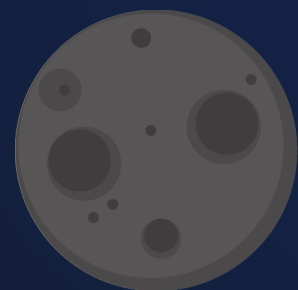
Missing TC Protection



Missing State-of-the-Art Defenses



Attacker Access to Orbit as Staging Ground



Unknown Consequences





# Thanks!

---



- Firmware Attacks on Satellite
- Satellite Exploitation Objectives
- Three Satellite Case Studies
- Satellite Developer Survey
- Impact beyond Vulnerable Satellites



@jwillbold



/jwillbold

Johannes Willbold - [johannes.willbold@rub.de](mailto:johannes.willbold@rub.de)

[1] ESTCube-1 Image: <https://www.eoportal.org/satellite-missions/estcube-1>

[2] OPS-Sat Image: [https://www.esa.int/ESA\\_Multimedia/Videos/2019/12/OPS-SAT\\_ESA\\_s\\_flying\\_lab\\_open\\_to\\_all](https://www.esa.int/ESA_Multimedia/Videos/2019/12/OPS-SAT_ESA_s_flying_lab_open_to_all)