



Houston, We Have a Problem

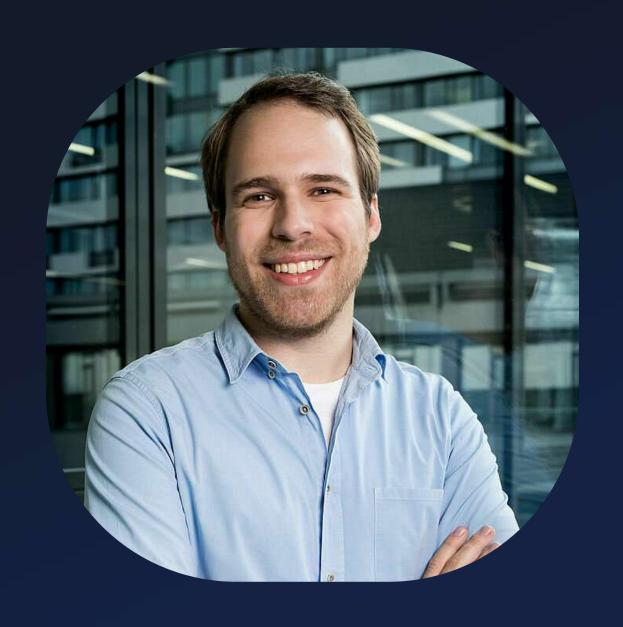
Analyzing the Security of Low Earth Orbit Satellites

Johannes Willbold





\$whoami



- Satellite & Space Systems Security
- Doctoral Student
 - Ruhr University Bochum, DE
- Visiting Researcher
 - Cyber-Defence Campus, CH
- Co-Founder of the SpaceSec
 Workshop

Space Odysséy

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



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 This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.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











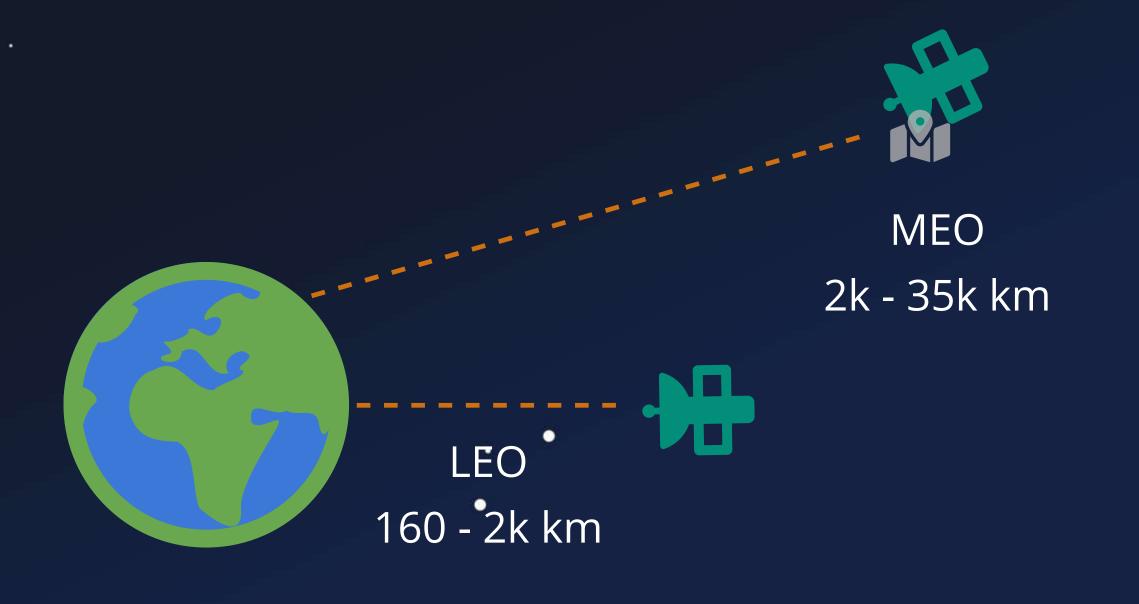


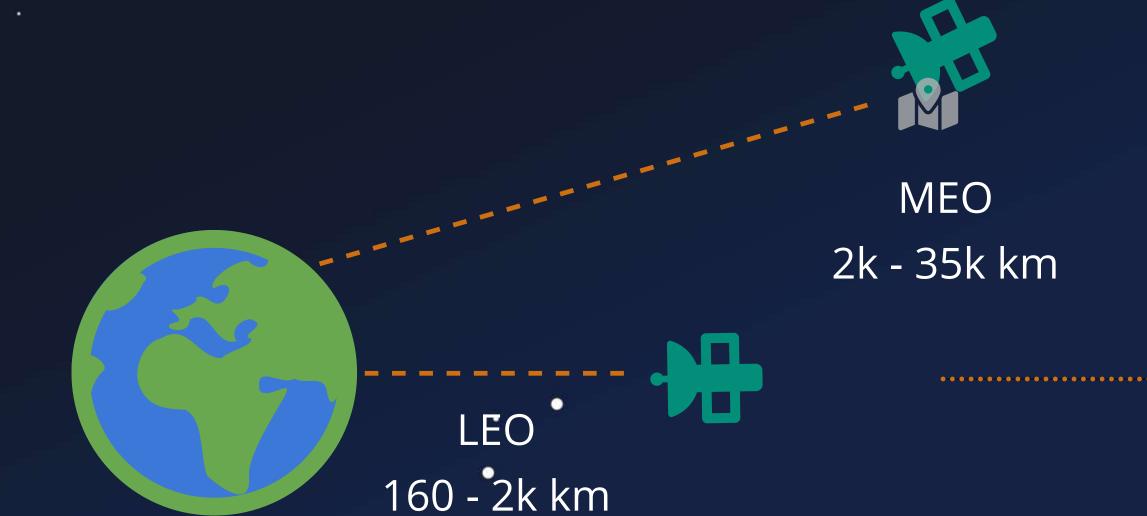


Technology Testing

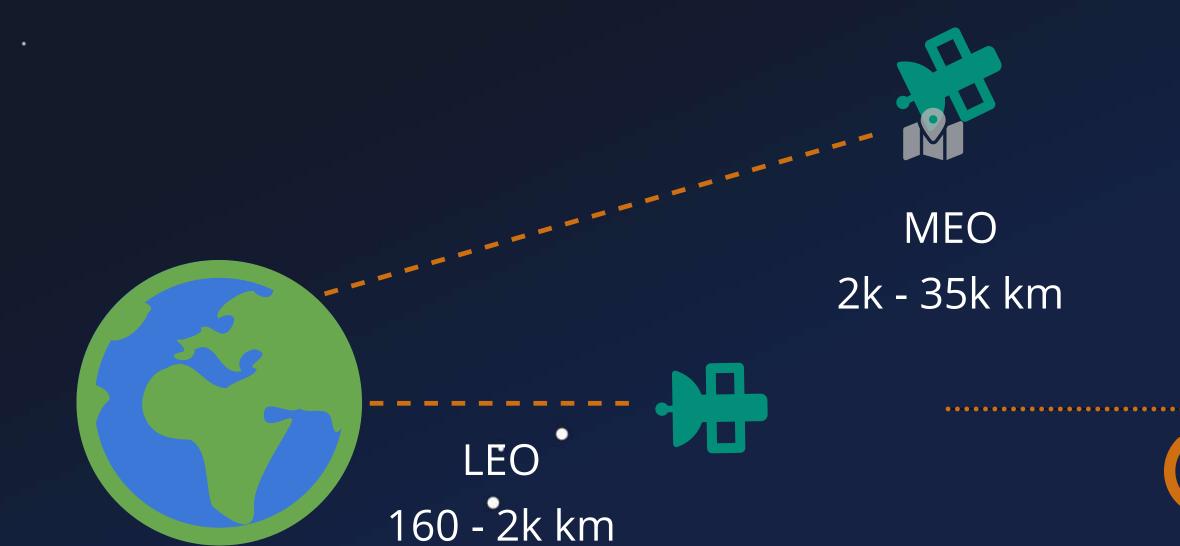








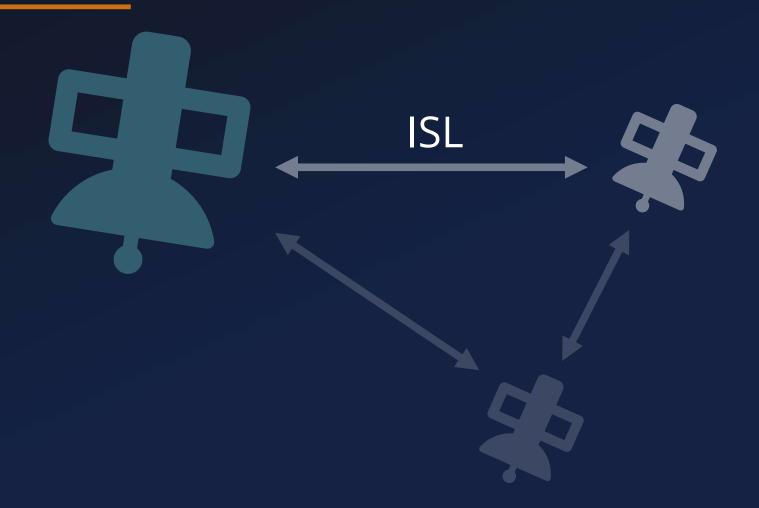




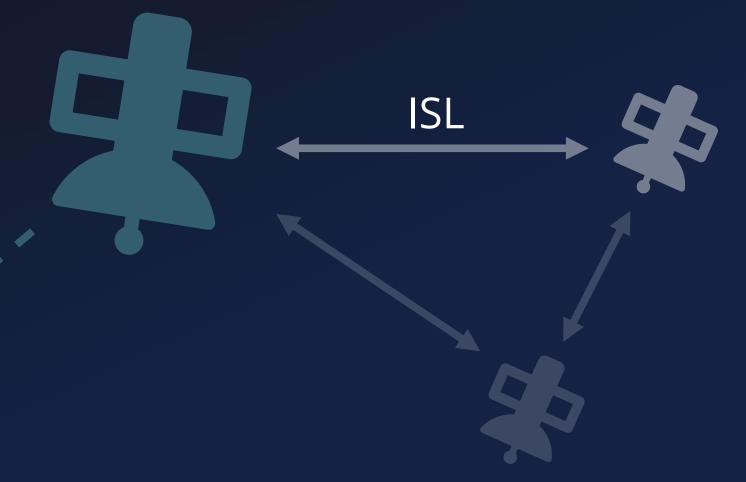


35786 km



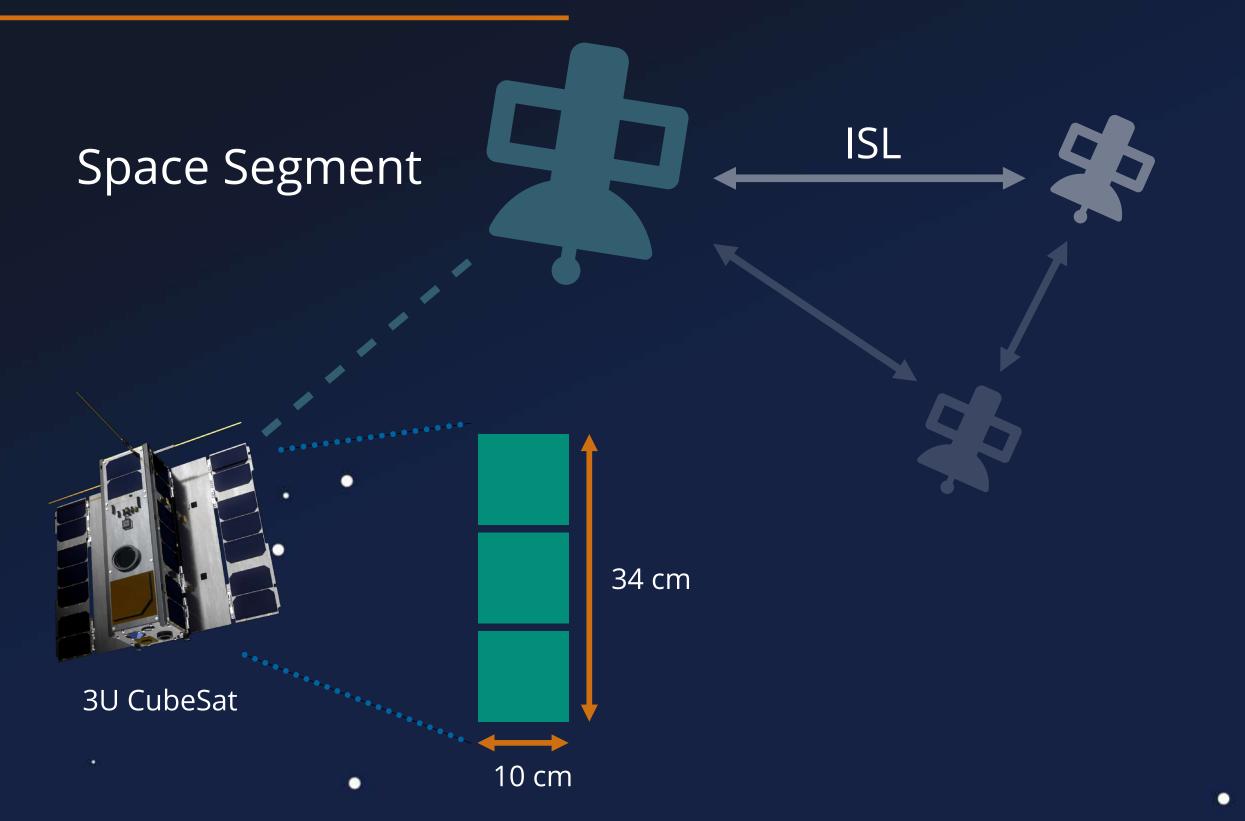


Space Segment



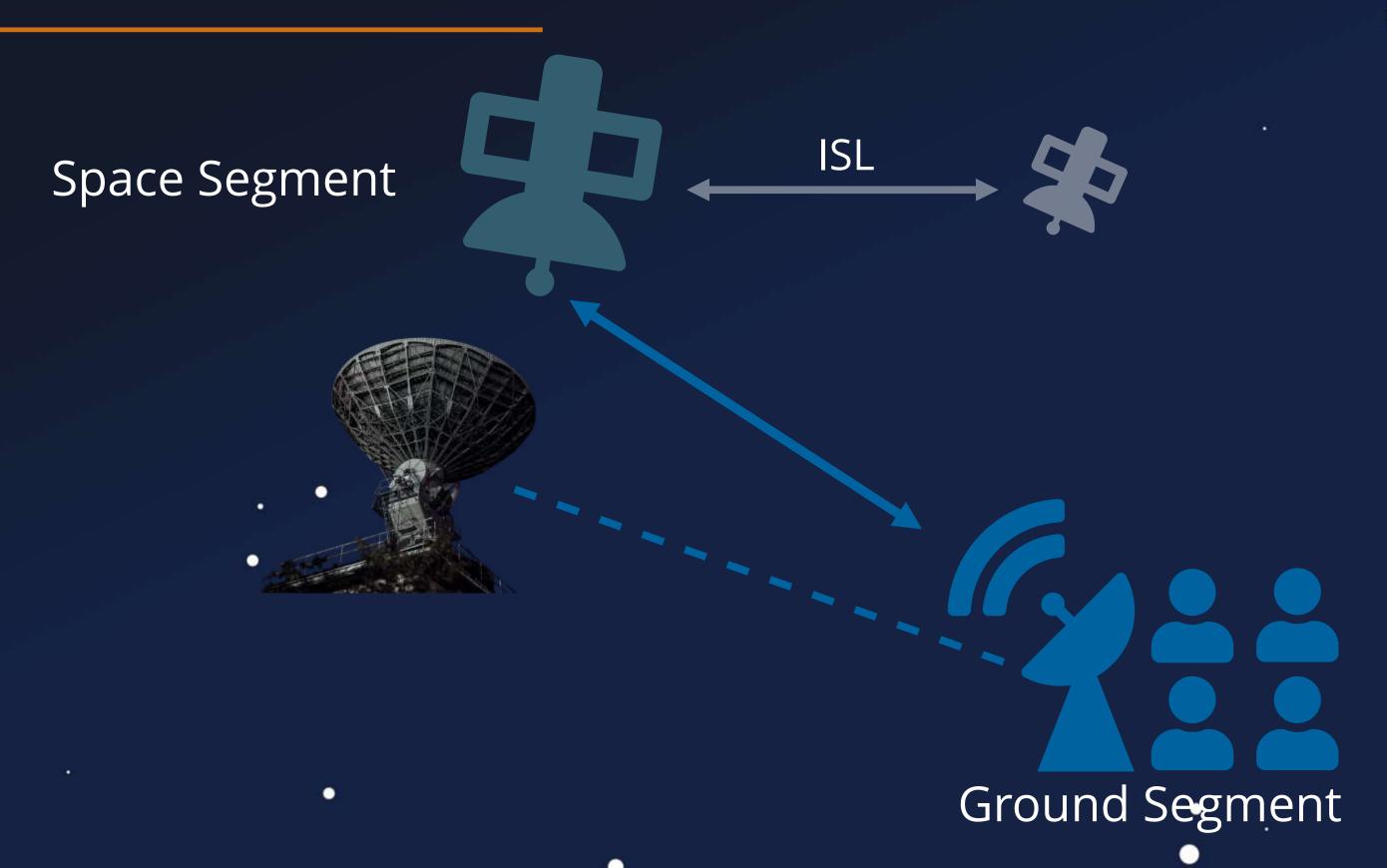


3U CubeSat













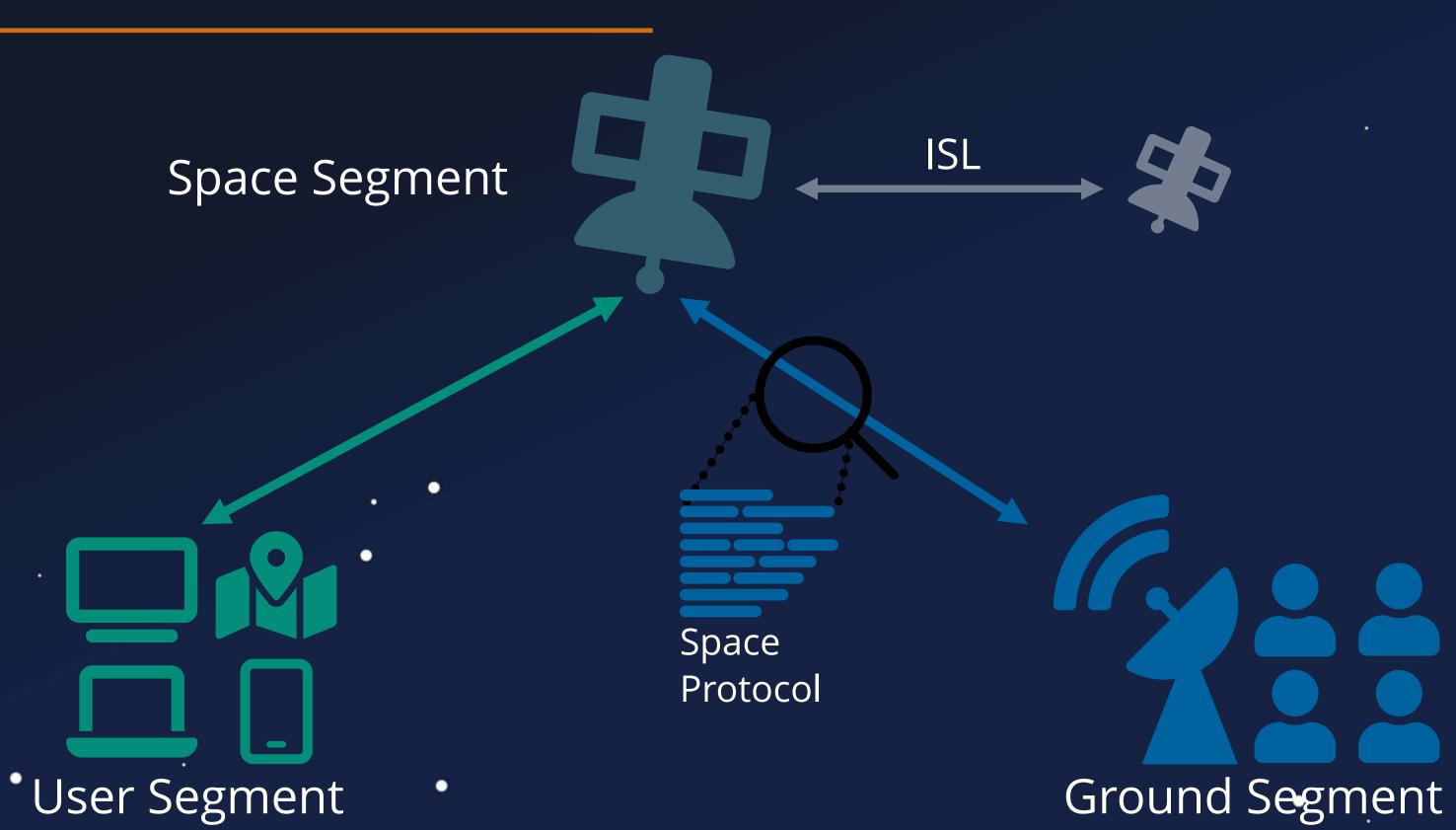
















System Analysis



System Analysis



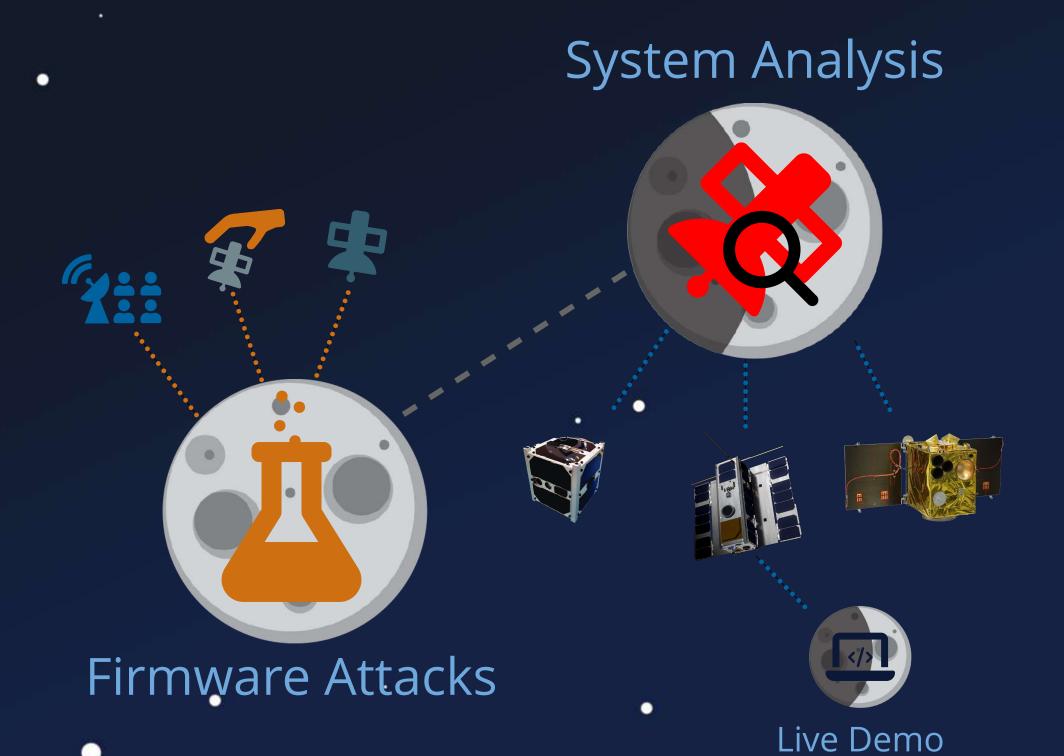
System Analysis

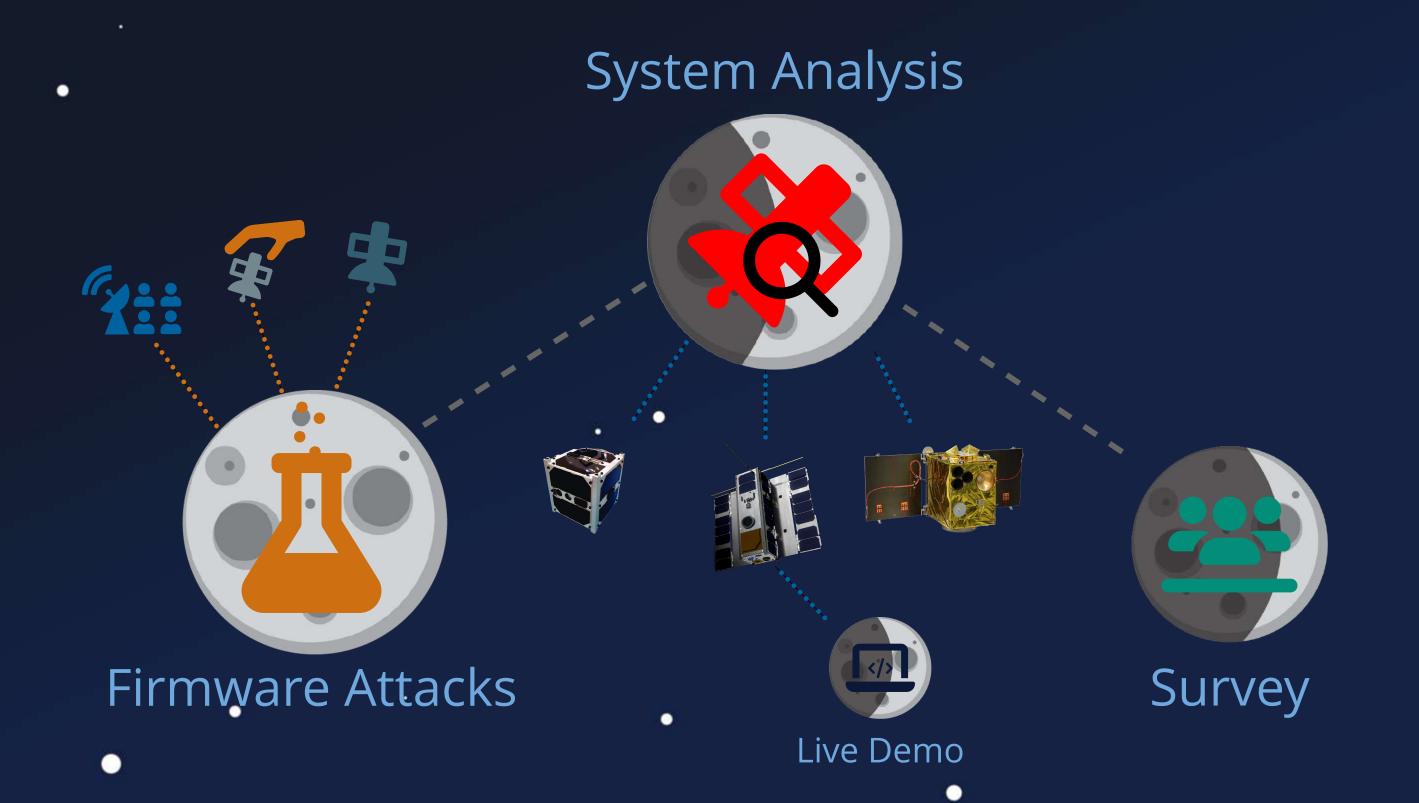


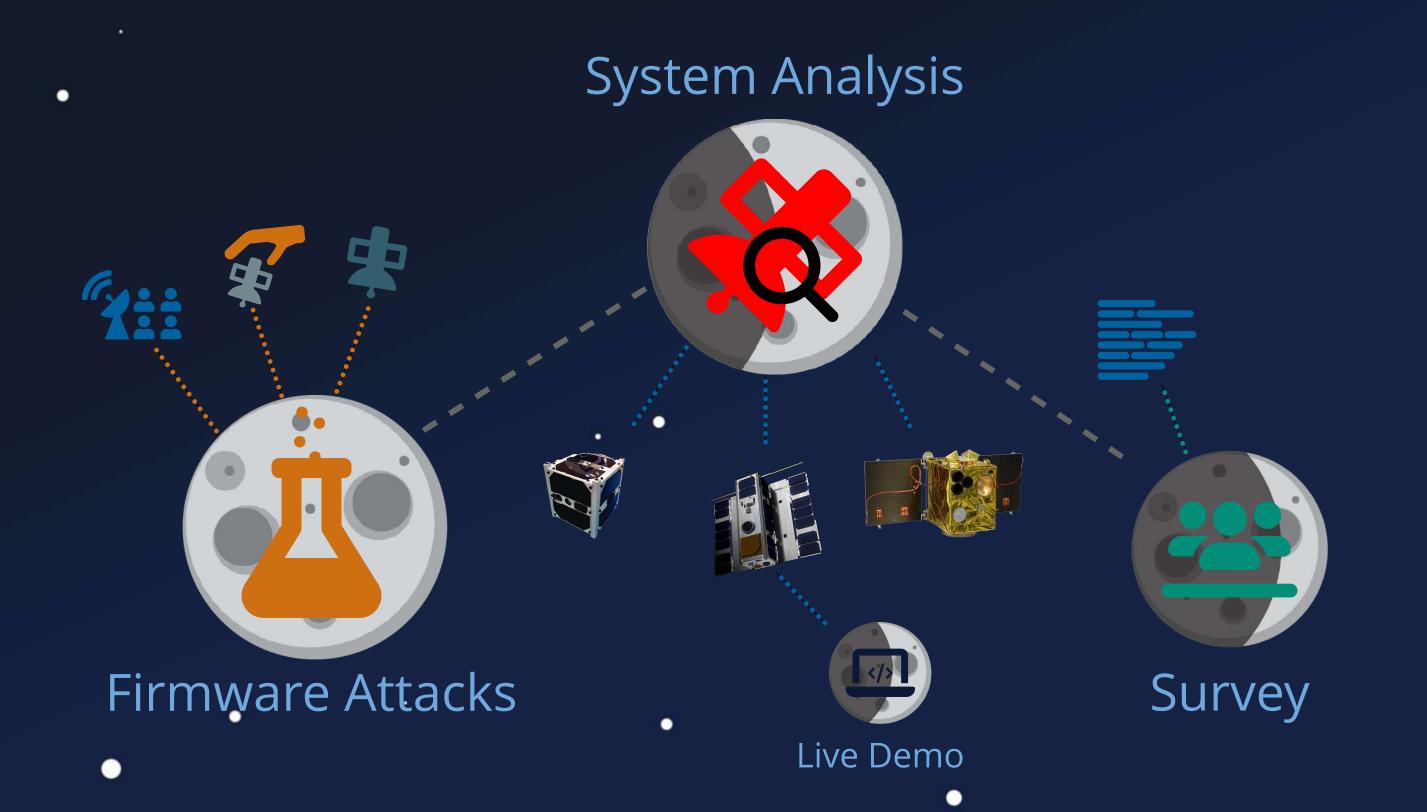
Firmware Attacks

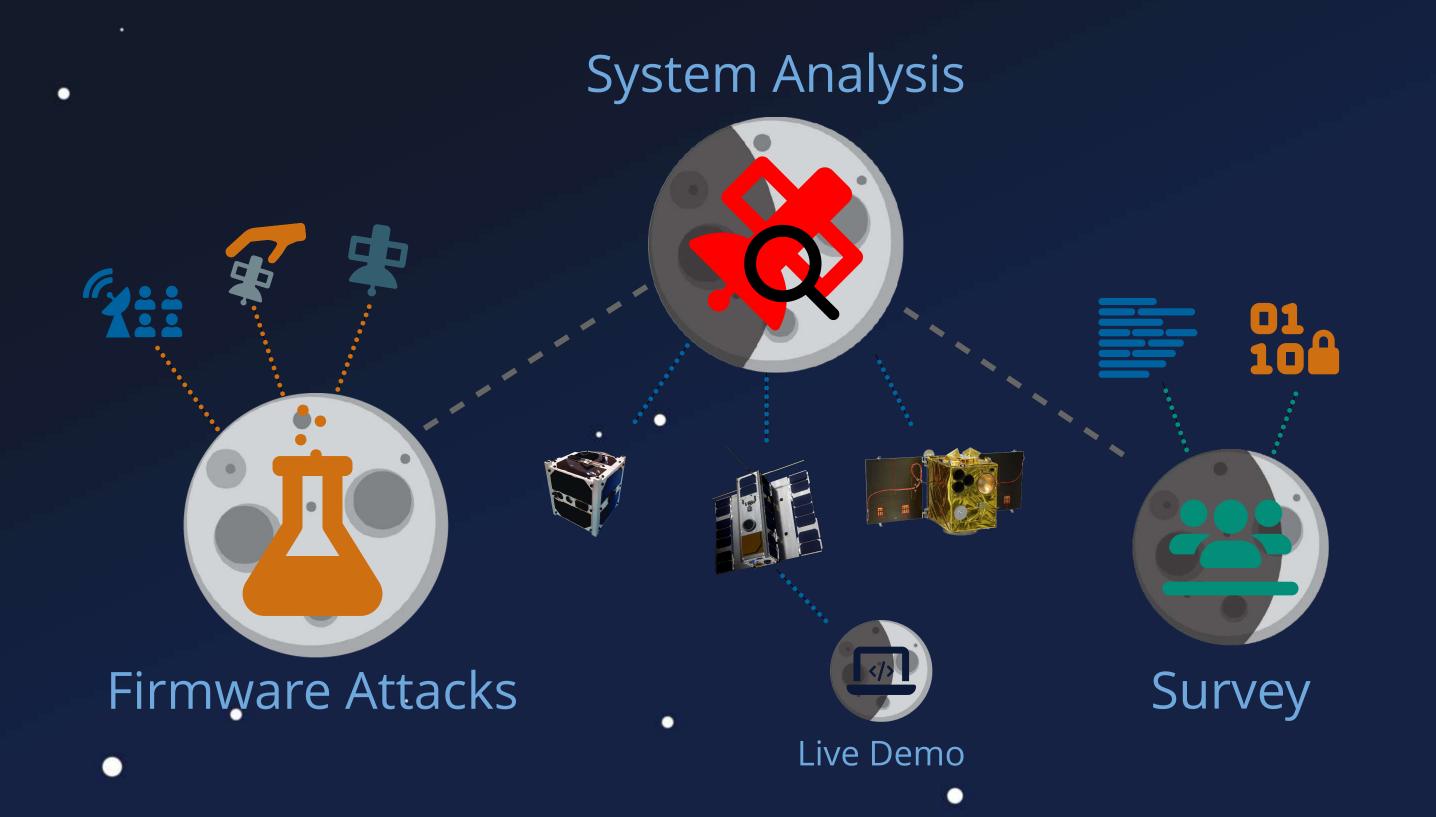
System Analysis

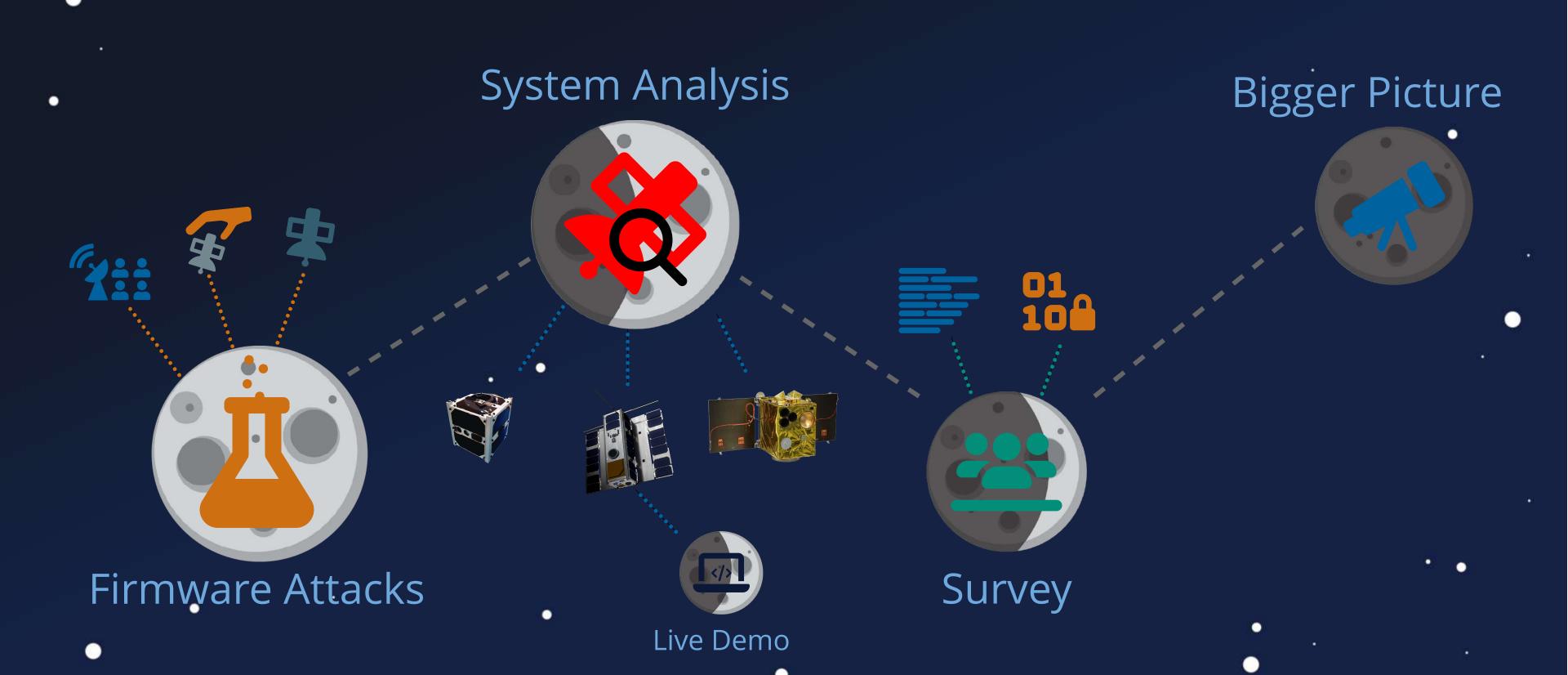




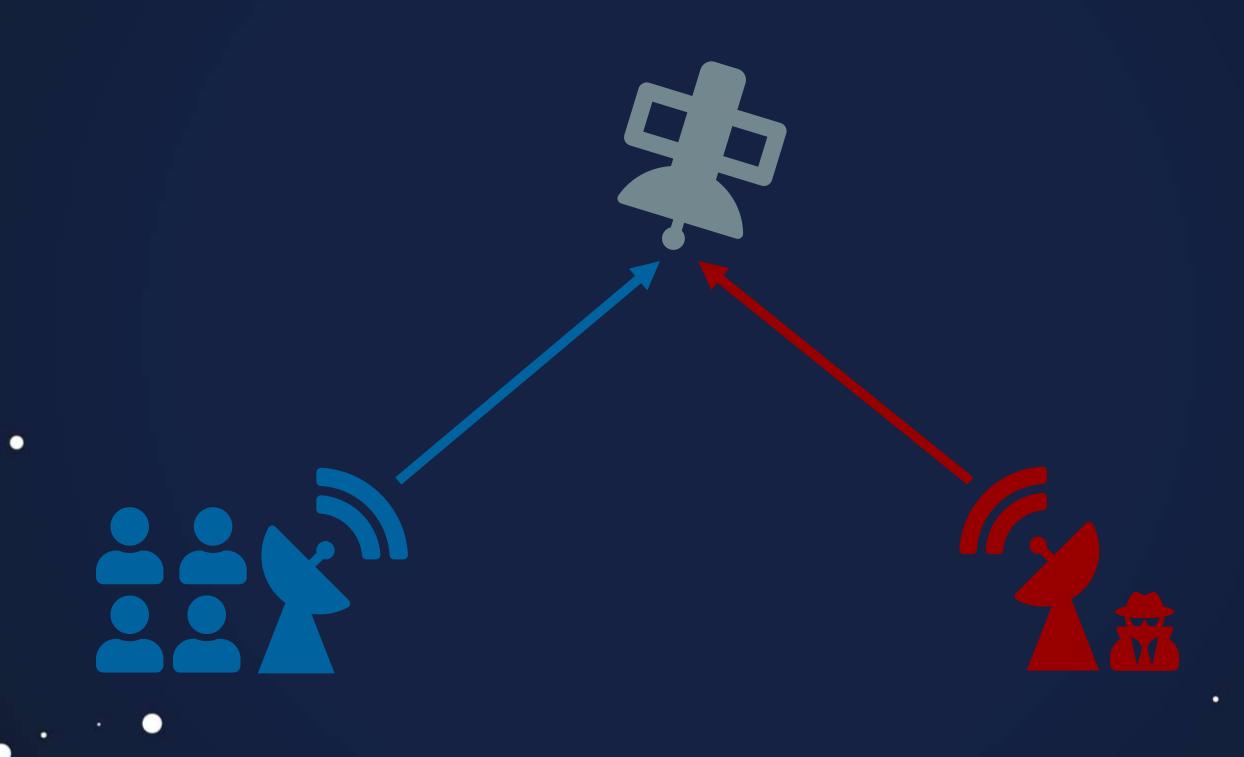




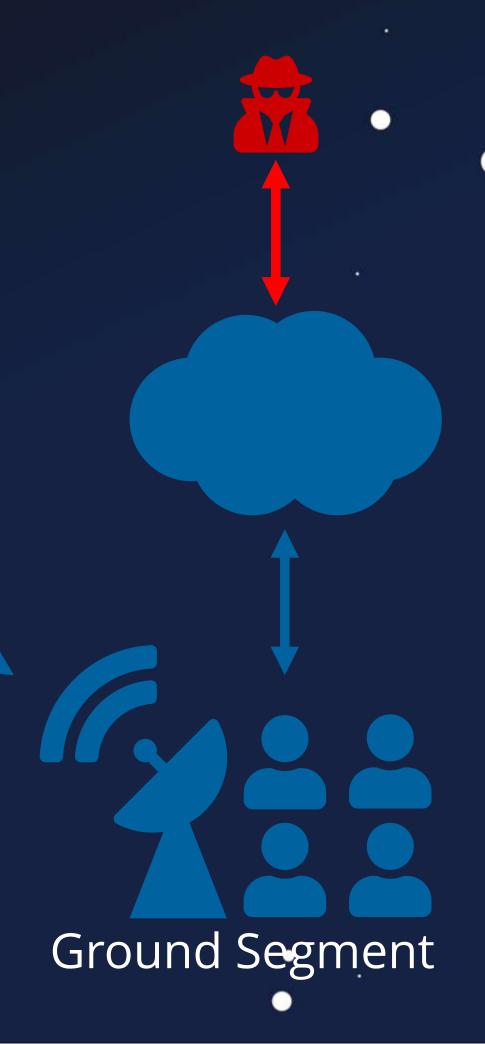


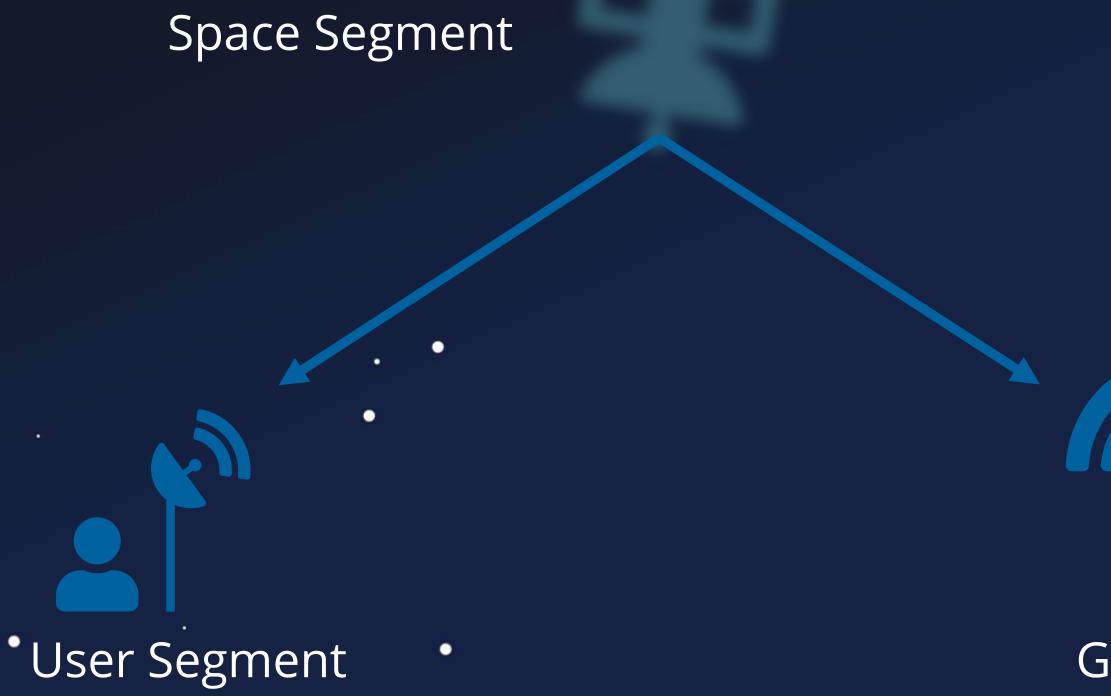


Firmware Attacks









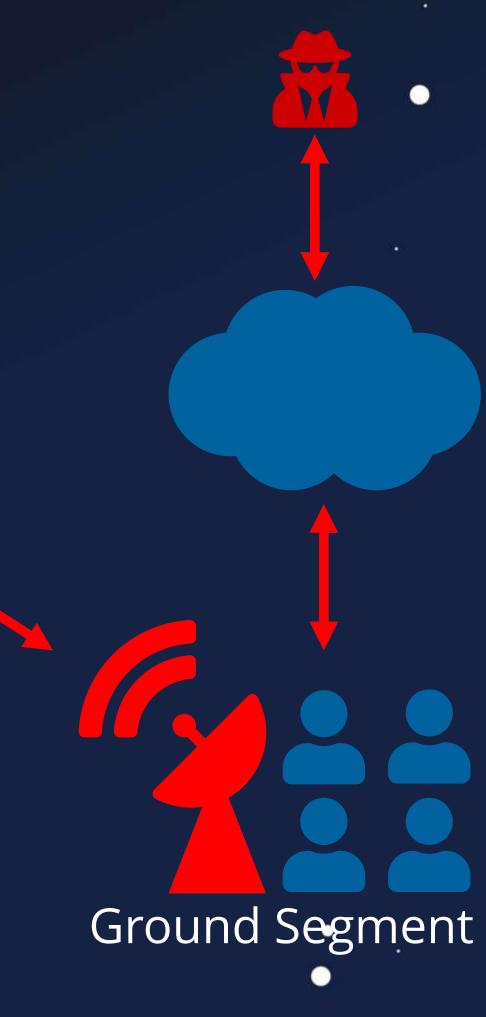


Space Segment

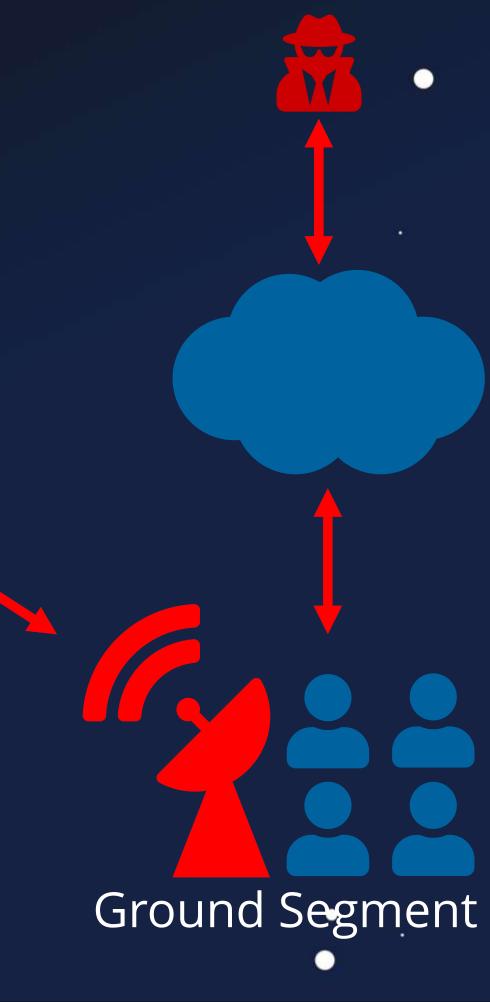


*User Segment

*User Segment

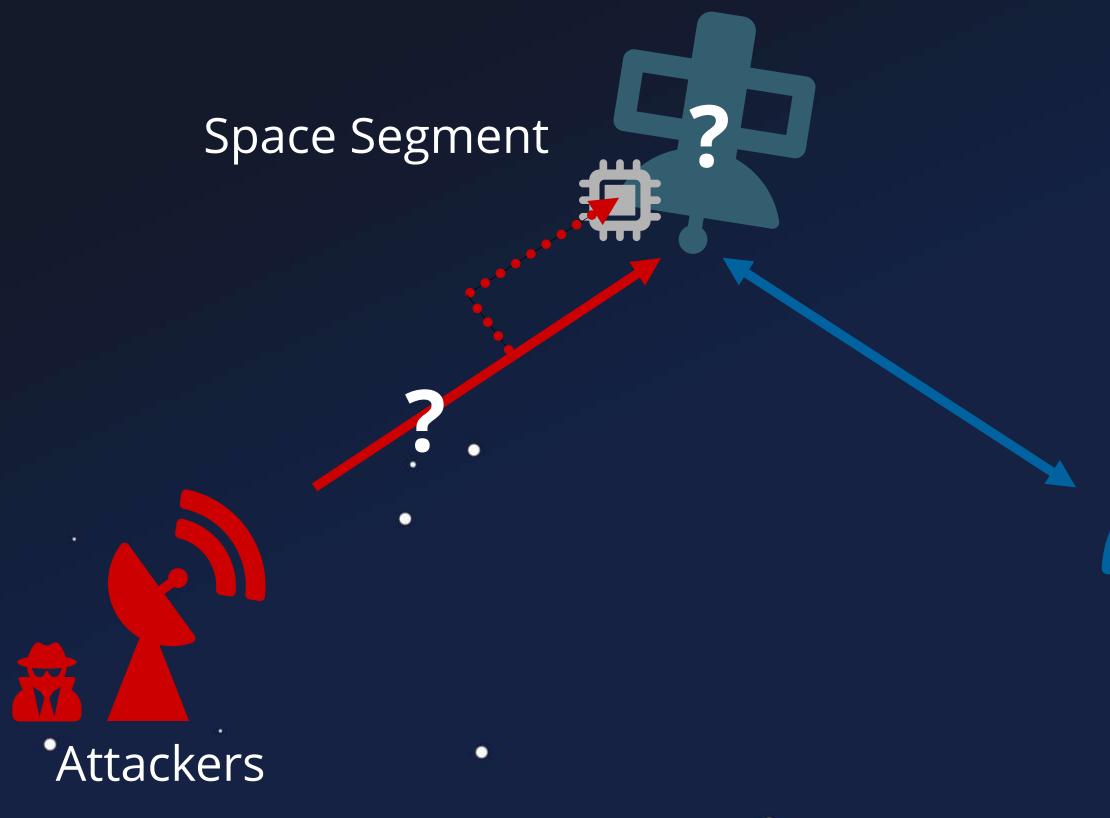


Space Segment



*User Segment

Firmware Attacks





Not so Novė



Report Concerning Space Data System Standards

SECURITY THREATS
AGAINST SPACE
MISSIONS

INFORMATIONAL REPORT

CCSDS 350.1-G-3

GREEN BOOK February 2022



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 intended destination, they might be executed, potentially a case spacecraft represents the result that a spacecraft operations, such as a many a spacecraft re-orientation and the result that a spacecraft is in an unintended orientate to the transmitted of the result that a spacecraft is man unintended orientates the transmitted of the result that a spacecraft is man unintended orientates. It is the reset afficial 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 C THORIZED ACCESS

Applicable to: Space 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 2



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-transmit the intended destination, they might be executed, potentially could result ds are not rejected, they acate spacecraft operations, such as a manand the result that a spacecraft is in an unintended orientate, tumbling pointed in the wrong direction, solar arrays pointed away from the sum, the reset of opportunities of the sum of the reset of the wrong direction.

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.

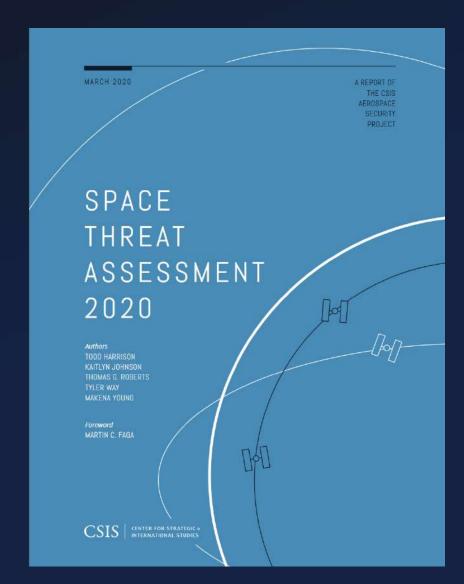
ossible Mission Impact: Software threats could result in loss of data and safety issues loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

THORIZED ACCESS

Applicable to: Spa

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 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 intended destination, they might be spacecraft and they are re-transmit executed, potentially are not rejected, they acate spacecraft operations, such as a maneesuit a made spacecraft operations, such as a mane, a spacecraft re-count the result that a spacecraft is in an unintended orientation of tumbling, pointed in the wrong direction, solar arrays pointed away from the suc

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.

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

THORIZED ACCESS

Applicable to: Spa

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.

used to take control

till pose a cyber threat.

cyberattack on space systems can remunications and permanently damage impossible, because attackers can use a other nations against the attacker. variety of methods to conceal their identity, such as using hijacked servers to

THREAT CHARACTERISTICS

The types of counterspace threats de scribed 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-powere 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.

user terminals that connect to satellites | Counterspace weapons that are reversiare all potential intrusion points for cy- ble, difficult to attribute, and have limited perattacks. Cyberattacks can be used to public awareness are ideally suited for sitmonitor data traffic patterns (i.e., which | uations in which an opponent may want users are communicating), to monitor the to signal resolve, create uncertainty in the data itself, or to insert false or corrupted mind of its opponent, or achieve a fait acdata in the system. While cyberattacks compli without triggering an escalatory require a high degree of understanding of response. For example, an adversary that systems being targeted, they do not | wants to deter the United States from inarily require significant resources | tervening in a situation may believe that duct. Cyberattacks can be contract- such attacks will stay below the threshold to private groups or individuals, for escalation (i.e., not trigger the very neans that a state or non-state act lacks internal cyber capabilities significant operational challenges for the Jnited States that make the prospect of ntervention more costly and protracted. sult in data loss, widespread disruptions, have limited battle damage assessment Conversely, counterspace weapons that and even permanent loss of a satellite. or that risk collateral damage may be less For example, if an adversary can seize useful to adversaries in many situations. control of a satellite through a cyberat-Without reliable battle damage assesstack on its command and control sys- ment, for example, an adversary cannot tem, the attack could shut down all complan operations with the confidence that s counterspace actions have been sucthe satellite by expending its propellant cessful. Furthermore, weapons that prosupply or damaging its electronics and duce collateral damage in space, such as sensors. Accurate and timely attribution of a cyberattack can be difficult, if not

CSIS



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 intended destination, they might be spacecraft and they are re-transmi executed, potentially are not rejected, they acate spacecraft operations, such as a maneesuit a made spacecraft operations, such as a mane, a spacecraft re-count the result that a spacecraft is in an unintended orientation of tumbling, pointed in the wrong direction, solar arrays pointed away from the suc

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.

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

THORIZED ACCESS

Applicable to: Sp

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.

CSIS

used to take control

of a satellite and

till pose a cyber threat. cyberattack on space systems can remunications and permanently damage sensors. Accurate and timely attribution of a cyberattack can be difficult, if not impossible, because attackers can use a other nations against the attacker. variety of methods to conceal their identity, such as using hijacked servers to

THREAT CHARACTERISTICS

The types of counterspace threats de scribed 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-powere 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.

user terminals that connect to satellites | Counterspace weapons that are reversiare all potential intrusion points for cy- ble, difficult to attribute, and have limited perattacks. Cyberattacks can be used to public awareness are ideally suited for sitmonitor data traffic patterns (i.e., which | uations in which an opponent may want users are communicating), to monitor the to signal resolve, create uncertainty in the data itself, or to insert false or corrupted mind of its opponent, or achieve a fait acdata in the system. While cyberattacks compli without triggering an escalatory require a high degree of understanding of response. For example, an adversary that systems being targeted, they do not | wants to deter the United States from inarily require significant resources | tervening in a situation may believe that duct. Cyberattacks can be contract- such attacks will stay below the threshold to private groups or individuals, for escalation (i.e., not trigger the very neans that a state or non-state ac- thing it is trying to prevent) while creating t lacks internal cyber capabilities significant operational challenges for the United States that make the prospect of itervention more costly and protracted. sult in data loss, widespread disruptions, have limited battle damage assessment Conversely, counterspace weapons that and even permanent loss of a satellite. or that risk collateral damage may be less For example, if an adversary can seize useful to adversaries in many situations. control of a satellite through a cyberat- Without reliable battle damage assesstack on its command and control sys- ment, for example, an adversary cannot tem, the attack could shut down all complan operations with the confidence that s counterspace actions have been sucthe satellite by expending its propellant cessful. Furthermore, weapons that prosupply or damaging its electronics and duce collateral damage in space, such as AFROSPACE REPORT NO

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

No Insights <=> No Attacker

** No Insights <=> No Attacker

W No Insights <=> No Attacker



More Developers

More People Involved

W No Insights <=> No Attacker



More Developers

More People Involved



Commercial off-the-Shelf (COTS) Components

We have the sights <=> No Attacker



More Developers

More People Involved



Commercial off-the-Shelf (COTS)

Components



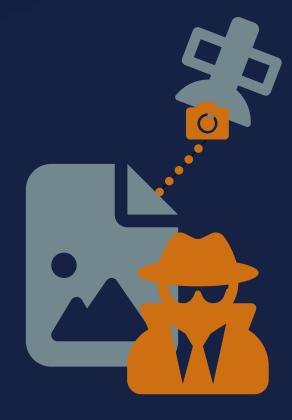
Higher Stakes Critical Infrastructure



Denial of Service



Denial of Service



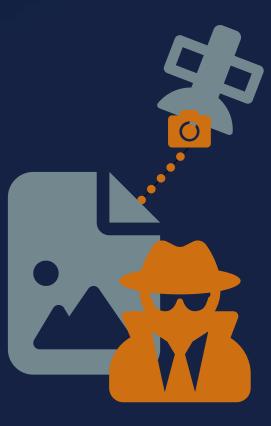
Malicious Data Interaction







Seizure of Control



Malicious Data Interaction



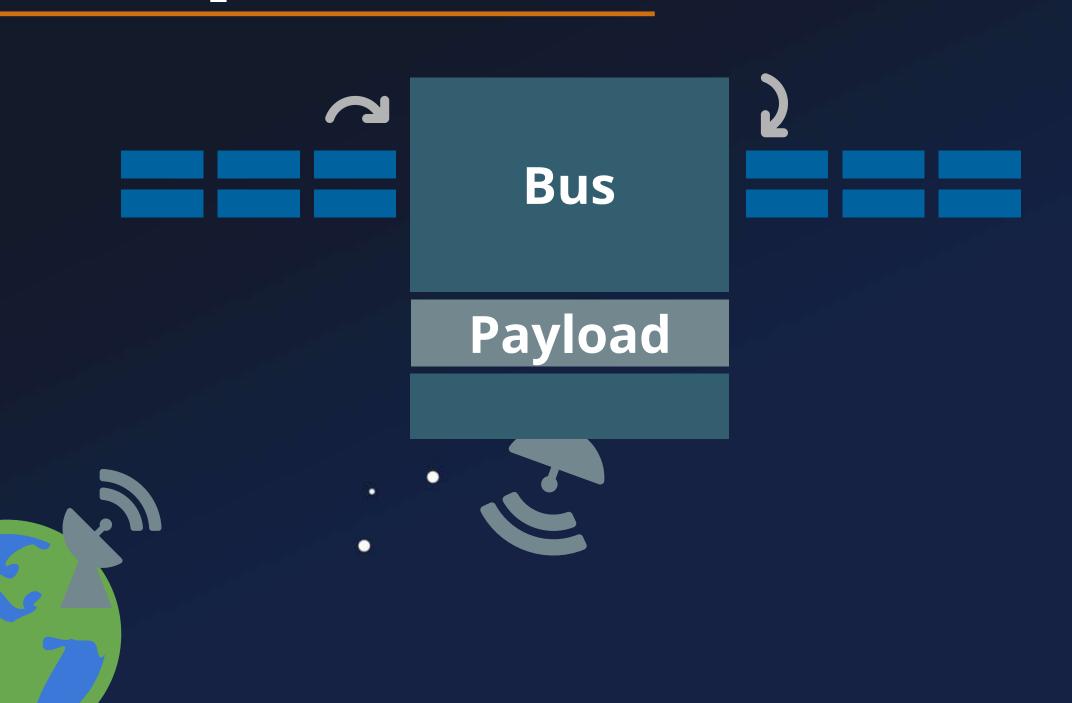


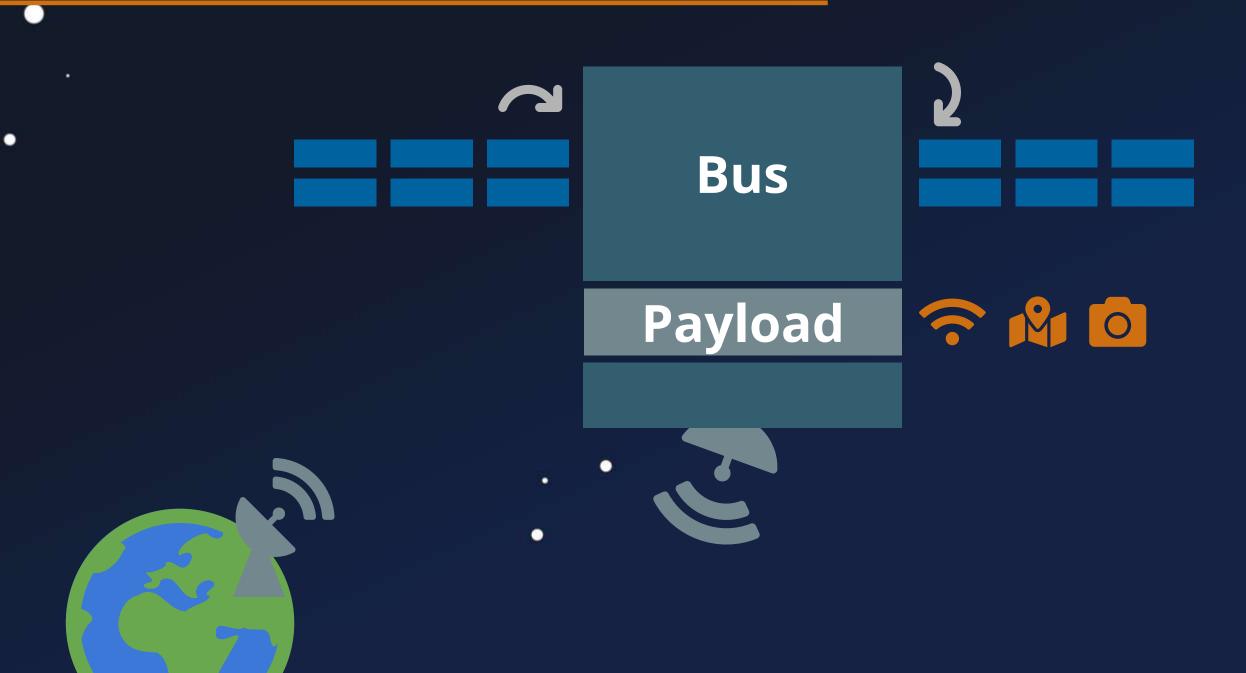
Interaction

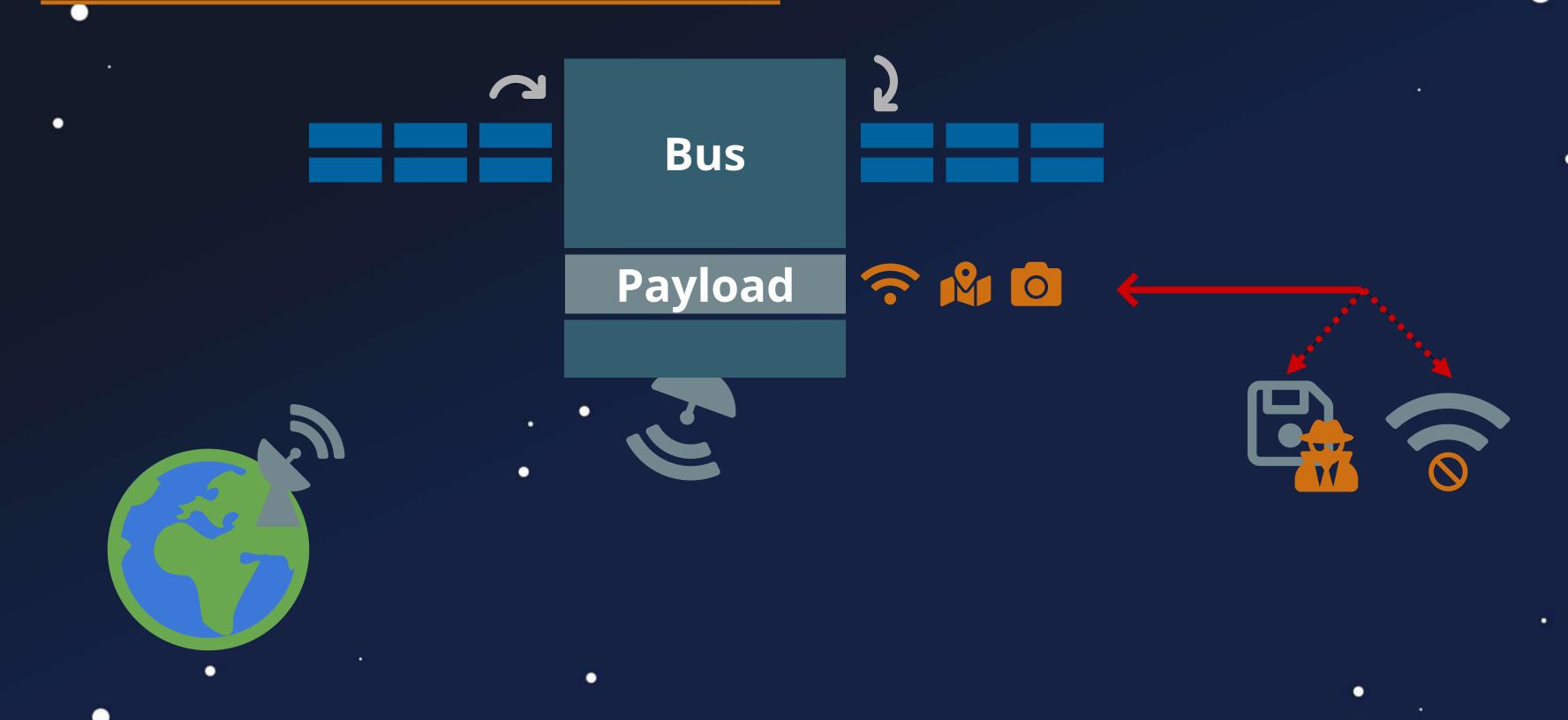


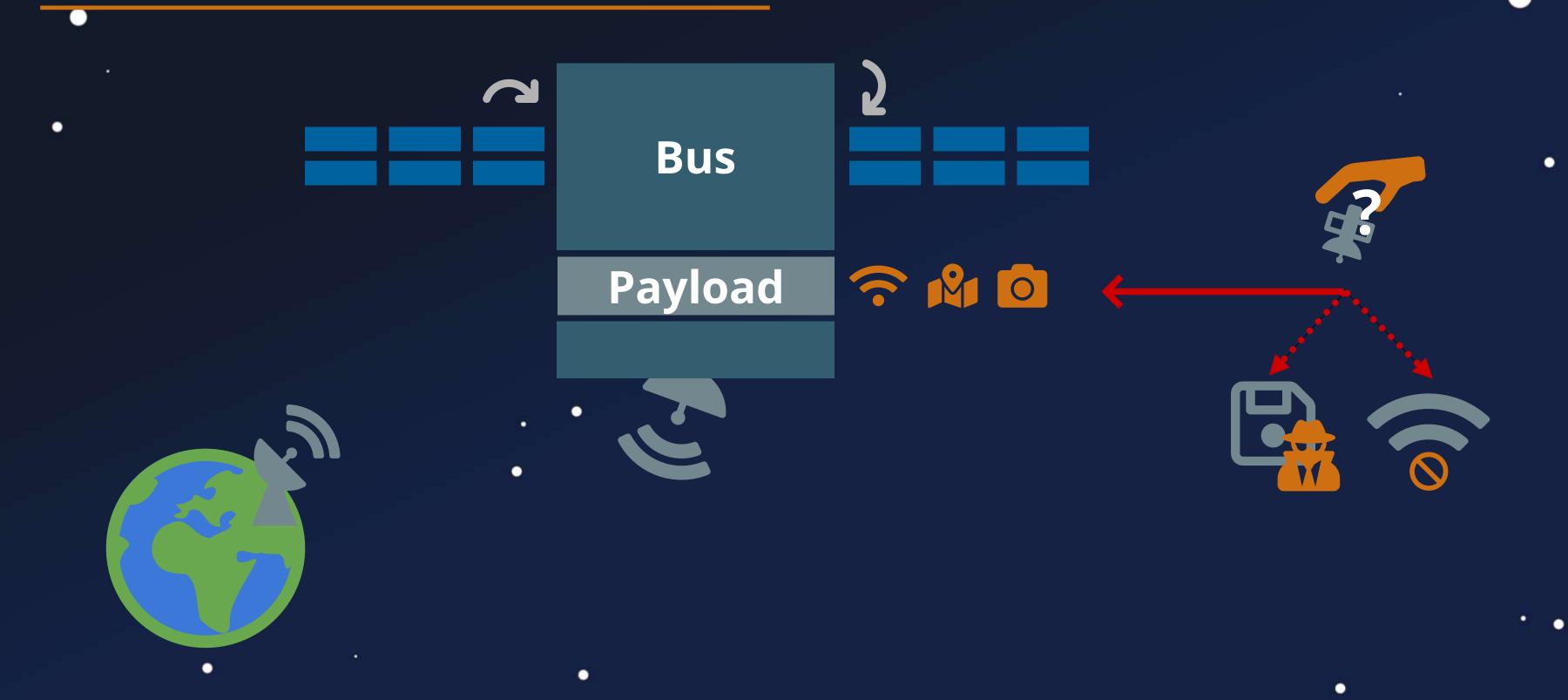
Seizure of Control



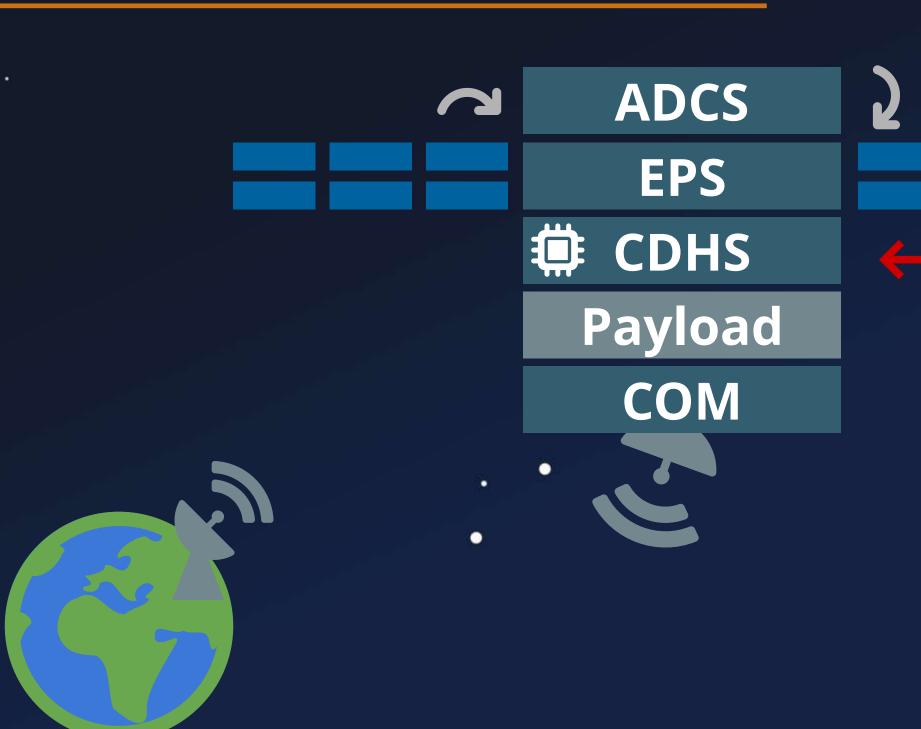














TC/TM Flow



Telecommand (TC)

Telemetry (TM)



- Decode
- Authenticate
- Repackage

ADCS

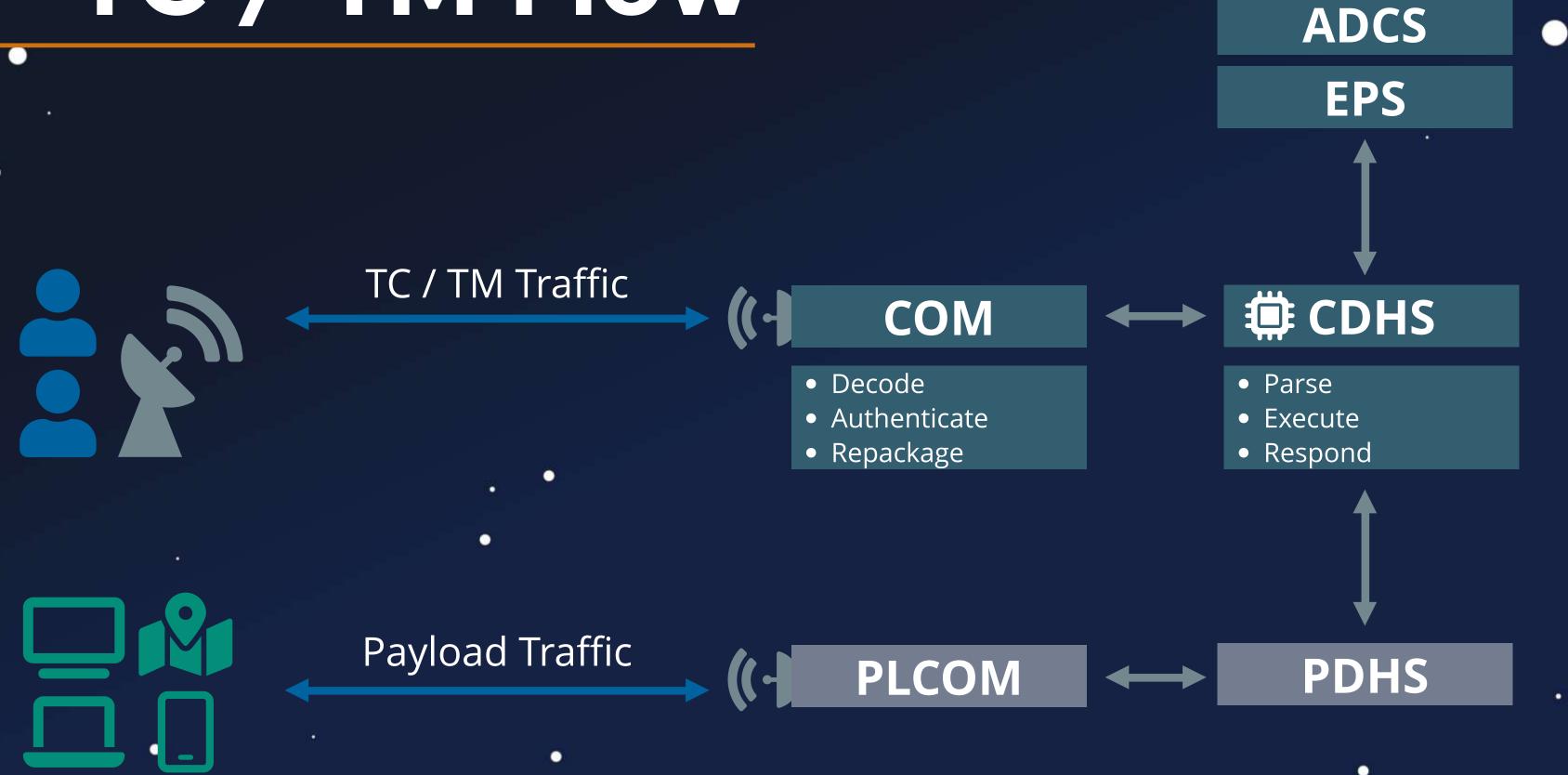
EPS

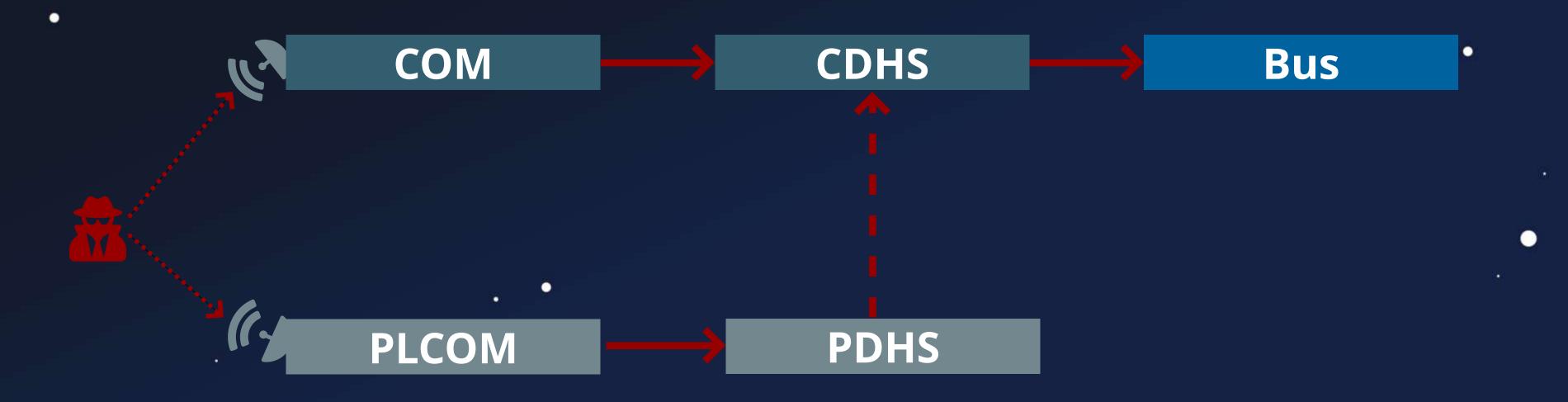


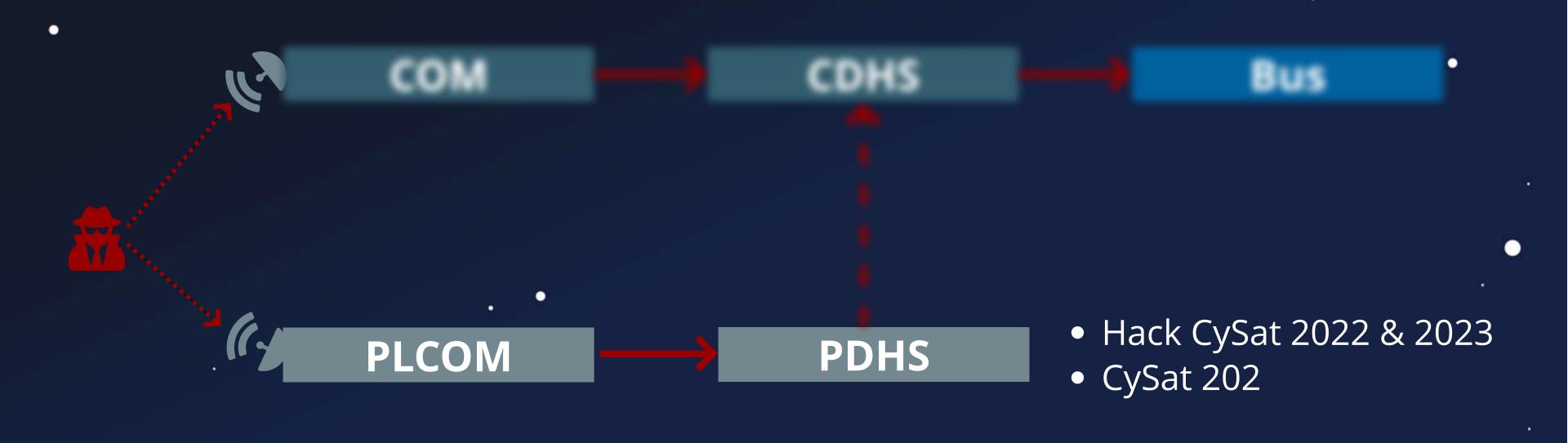
- Parse
- Execute
- Respond

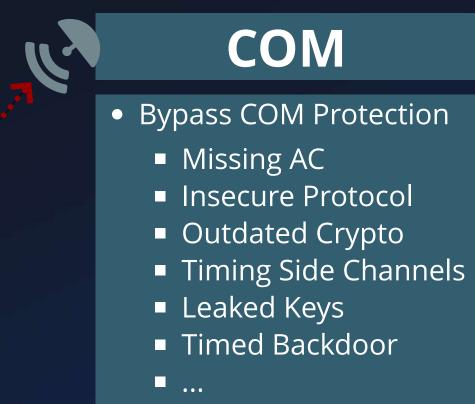
Payload

TC/TMFlow









CDHS



COM

- Bypass COM Protection
 - **[...]**

CDHS

- Deploy Attacker Payload
 - Firmware Update
 - Signed Image
 - Slow Upload
 - Complex System



COM

- Bypass COM Protection
 - **[...]**

CDHS

- Deploy Attacker Payload
 - Firmware Update
 - Dangerous TC
 - Vulnerable TC



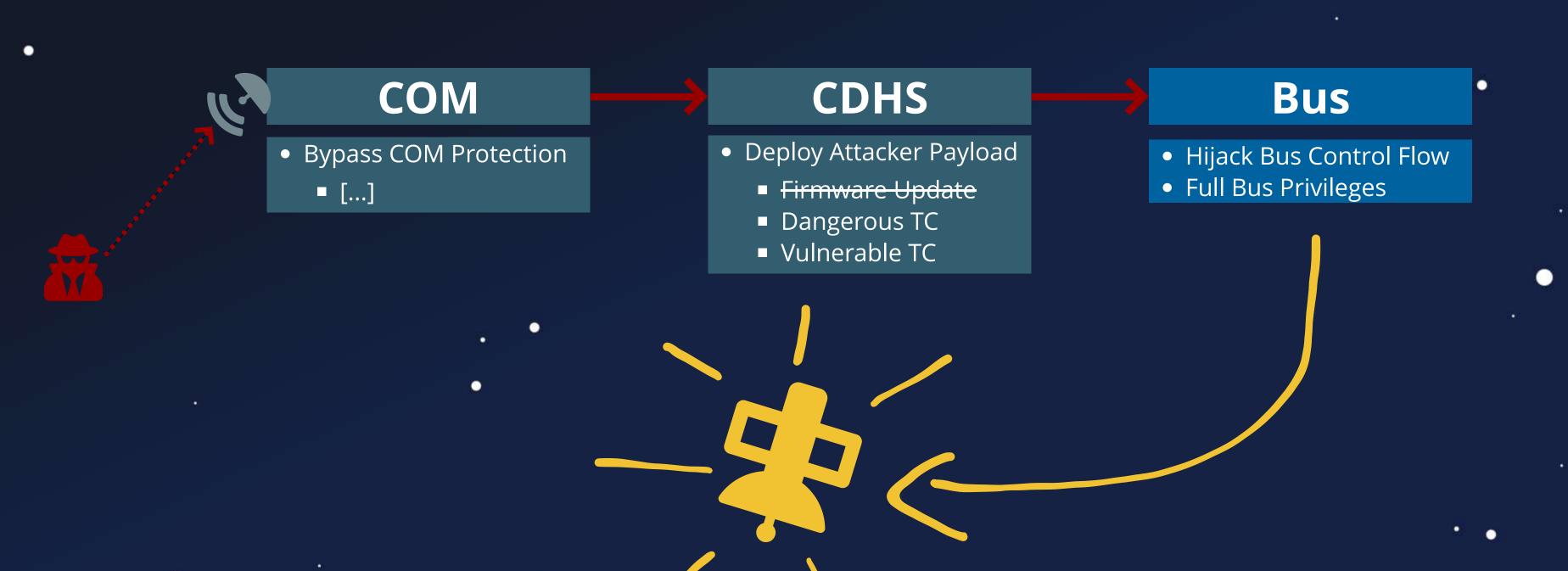
COM

- Bypass COM Protection
 - **[...]**

CDHS

- Deploy Attacker Payload
 - Firmware Update
 - Dangerous TC
 - Vulnerable TC

- Hijack Bus Control Flow
- Full Bus Privileges



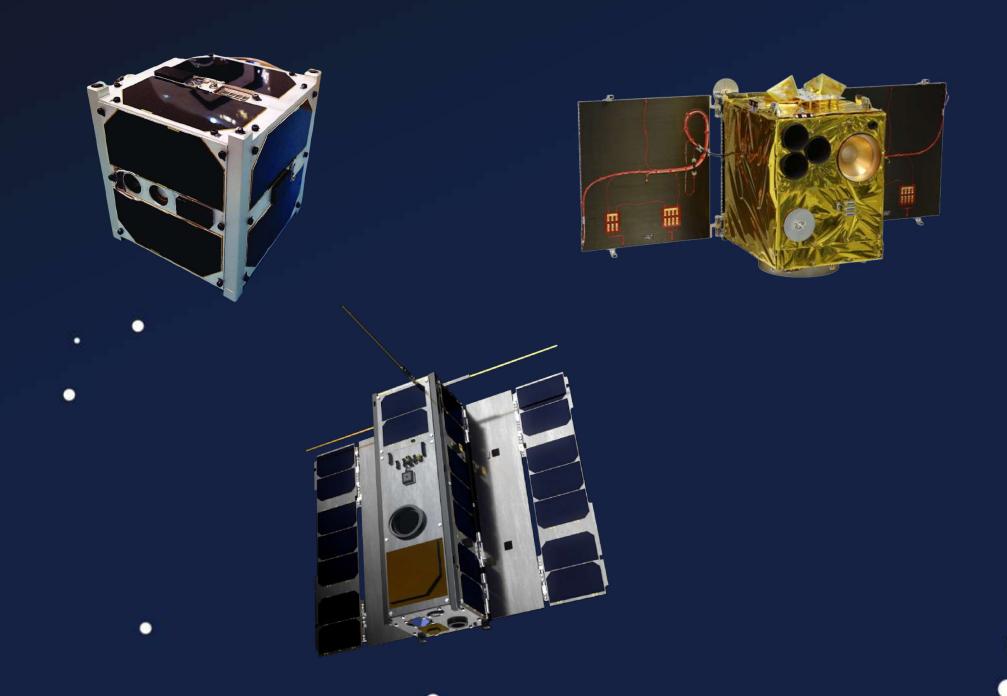
Objectives





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

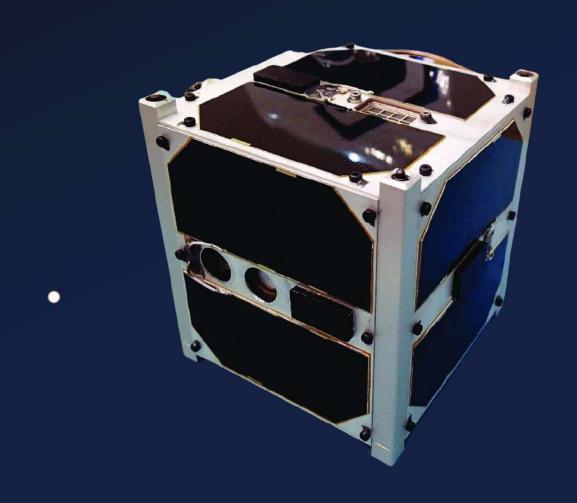
Satellite Case Studies



Approach



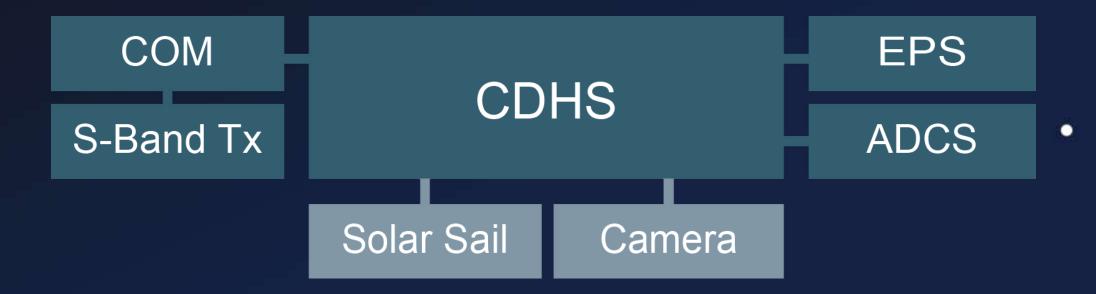
ESTCube-1



ESTCube-1



Developed by University of Tartau



E-Sail (Electric Solar Wind Sail) Proplsion

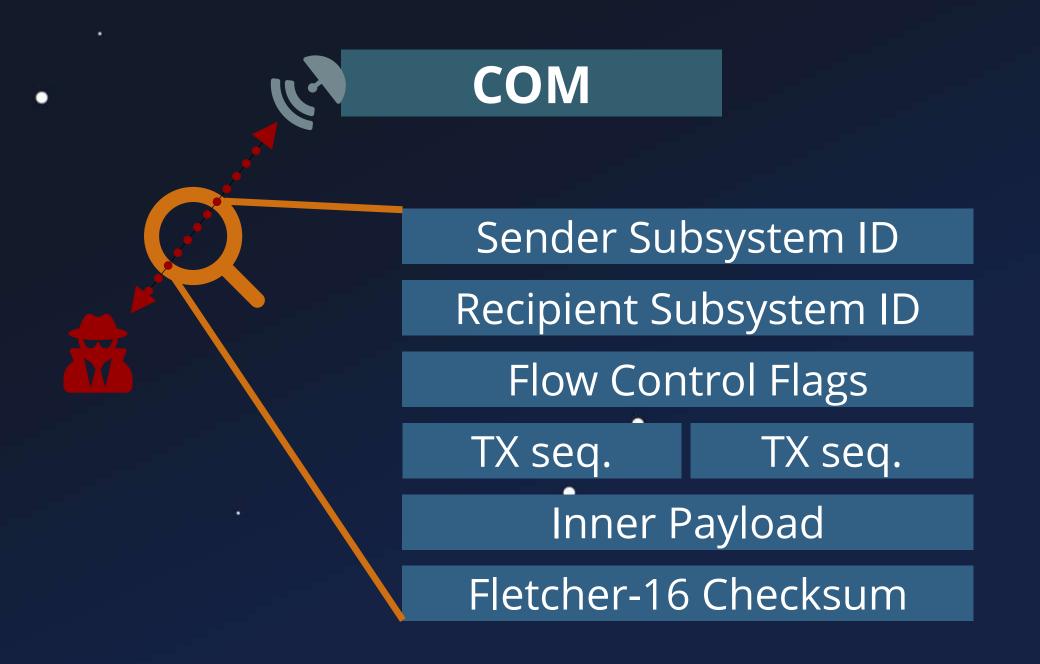
Peripherals

ARM STM32

Payload Platform

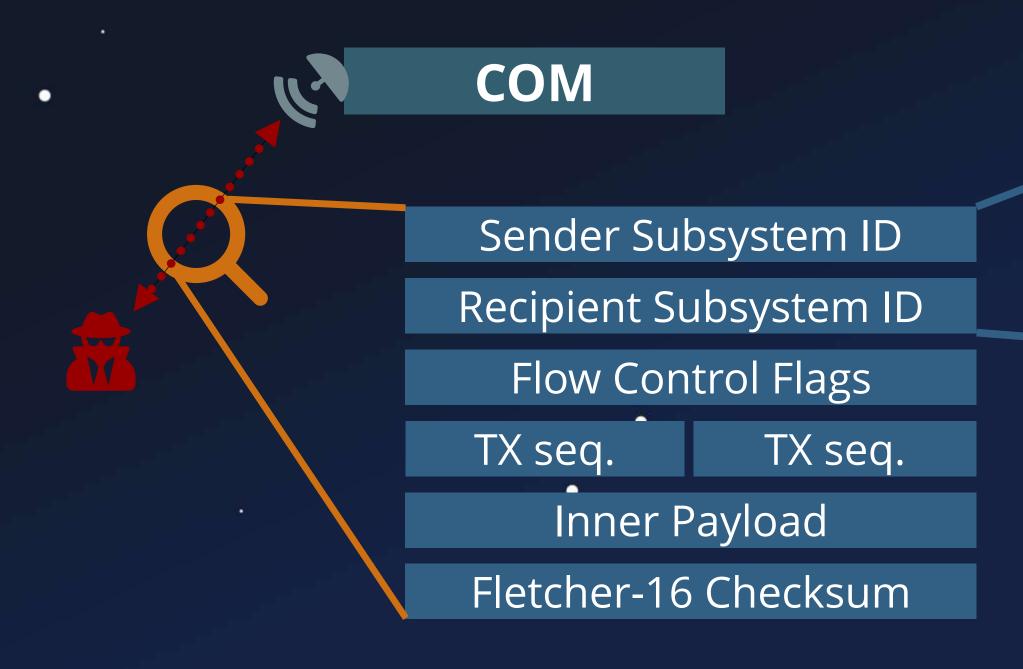
Custom Protocol





Custom Protocol

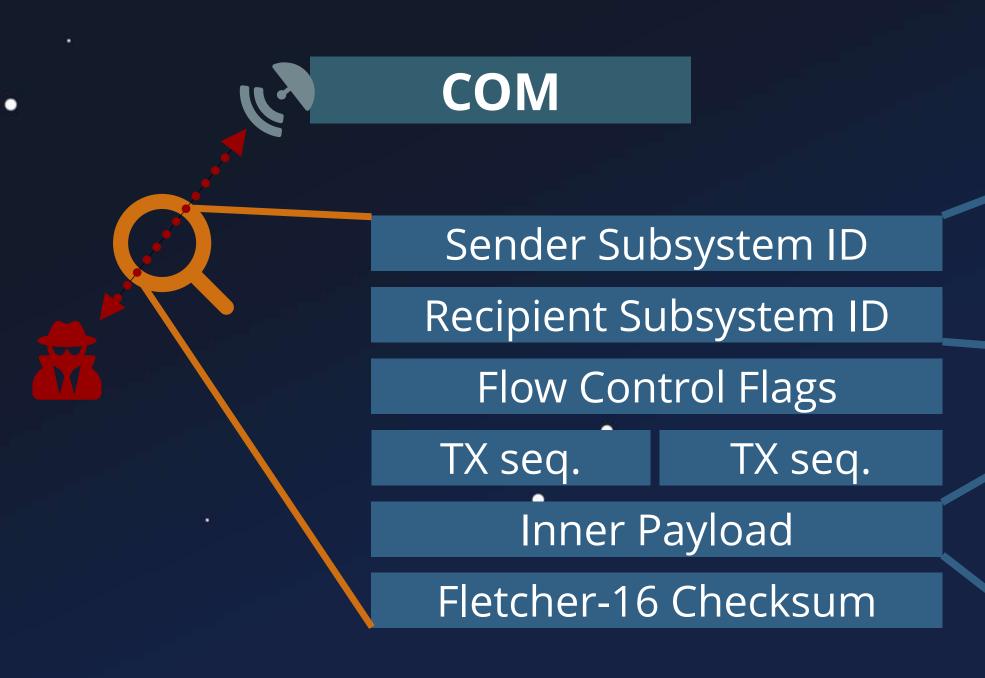




ID	Subsystem
0	EPS
1	COM
2	CDHS
•••	
5	Ground Station

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		Sou	ırce		Block ID										
Byte 3		Length													
•••		Args													





COM

- Bypass COM Protection
 - Missing TC Protection

	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				Le	n,	gth									
•••		Args													

```
int sch_handle_command(scheduler_packed_cmd_t *pCmd) {
   //! simplified!
   sch_unpack_command(&g_command, pCmd);
   //...
   handler_func = &handler_table[g_command.handler_func_index];
   //...
   retval = (*handler_func) (&g_command);
}
```



COM

- Bypass COM Protection
 - Missing TC Protection

The state of the s

	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				L	er	ngth									
•••		Args													

```
int sch_handle_command(scheduler_packed_cmd_t *pCmd) {
   //! simplified!
   sch_unpack_command(&g_command, pCmd);
   // ...
   handler_func = &handler_table[g_command.handler_func_index];
   // ...
   retval (*nandler_func) (&g_command);
}
```





- Bypass COM Protection
 - Missing TC Protection

```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
     char* pWriteData;
     if (pAddr) {
       if (g sch exec mode != 1 ) {
         /* exception and return */
       char* pWriteData = &pAddr->start of data buf;
       if (pAddr->filesystem target) {
10
11
12
       } else {
13
         memcpy(pAddr->targetAddr,
14
                &pAddr->start_of_data_buf,
                pAddr->writeLength);
15
16
17
18
19 }
```





COM

- Bypass COM Protection
 - Missing TC Protection

```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
     char* pWriteData;
     if (pAddr) {
       if (g sch exec mode != 1 ) {
       char* pWriteData = &pAddr->start of data buf;
       if (pAddr->filesystem target) {
         memcpy(pAddr->targetAddr,
13
14
                &pAddr->start_of_data_buf,
                pAddr->writeLength);
15
19 }
```

Real-World Test





- Deploy Attacker Payload
 - Dangerous TC

Real-World Test

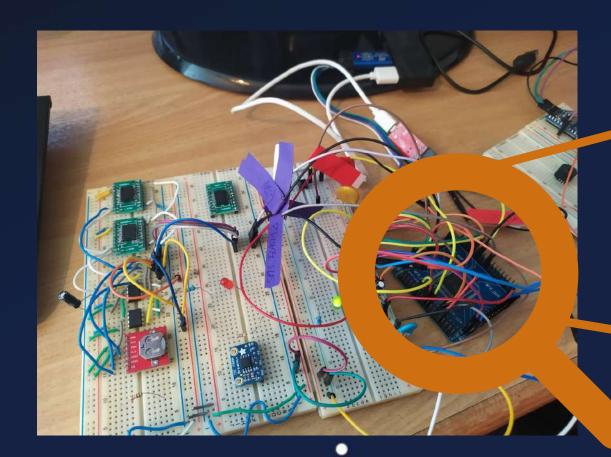


COM

- Bypass COM Protection
 - Missing TC Protection

CDHS

- Deploy Attacker Payload
 - Dangerous TC



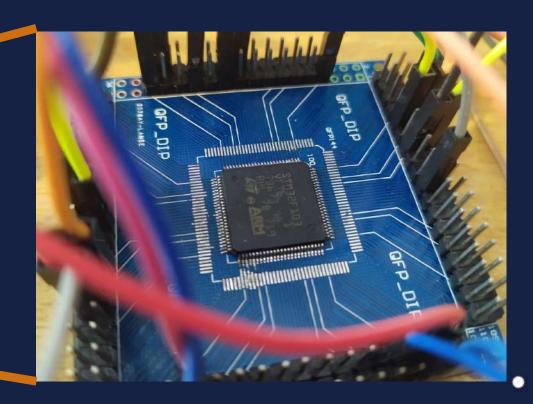


Image Source: Maximilian Gerhardt, Reverse Engineering Satellite Firmware for Security Evaluation, 13. Dec. 2021

OPS-Sat

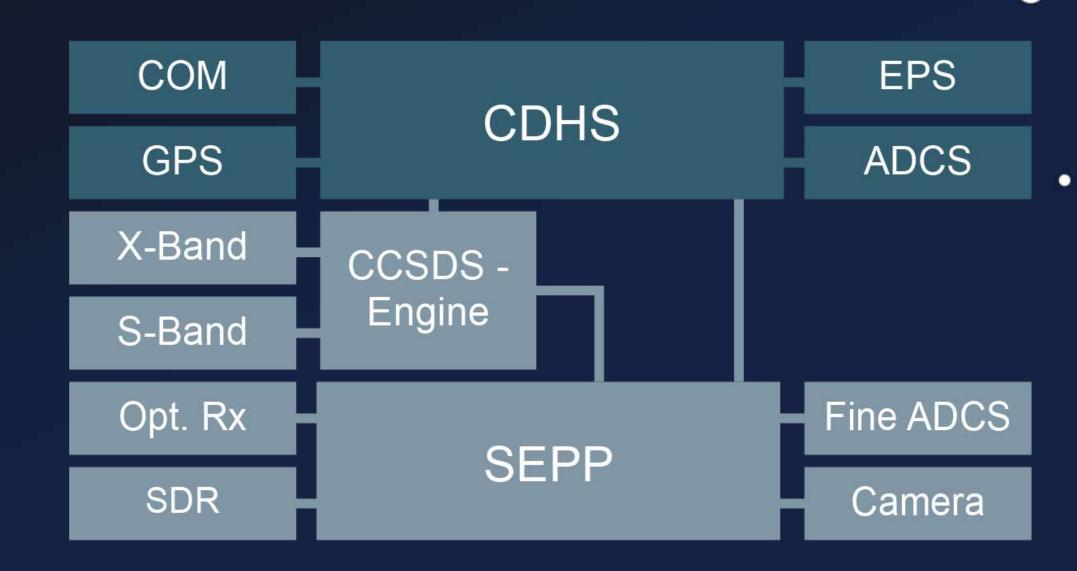




Experimenter

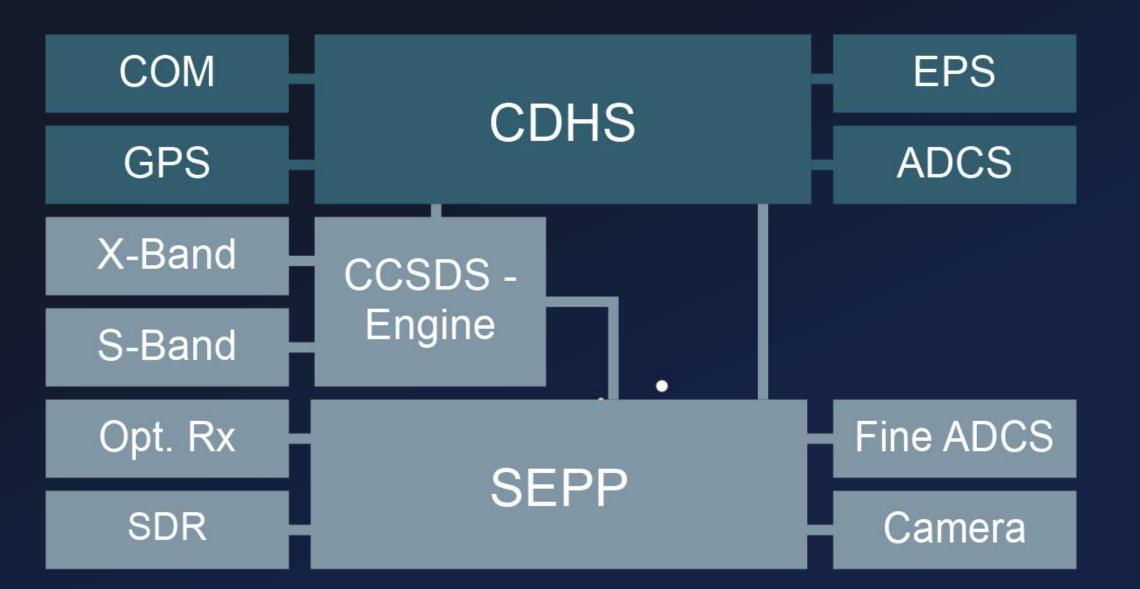
Operated by ESA

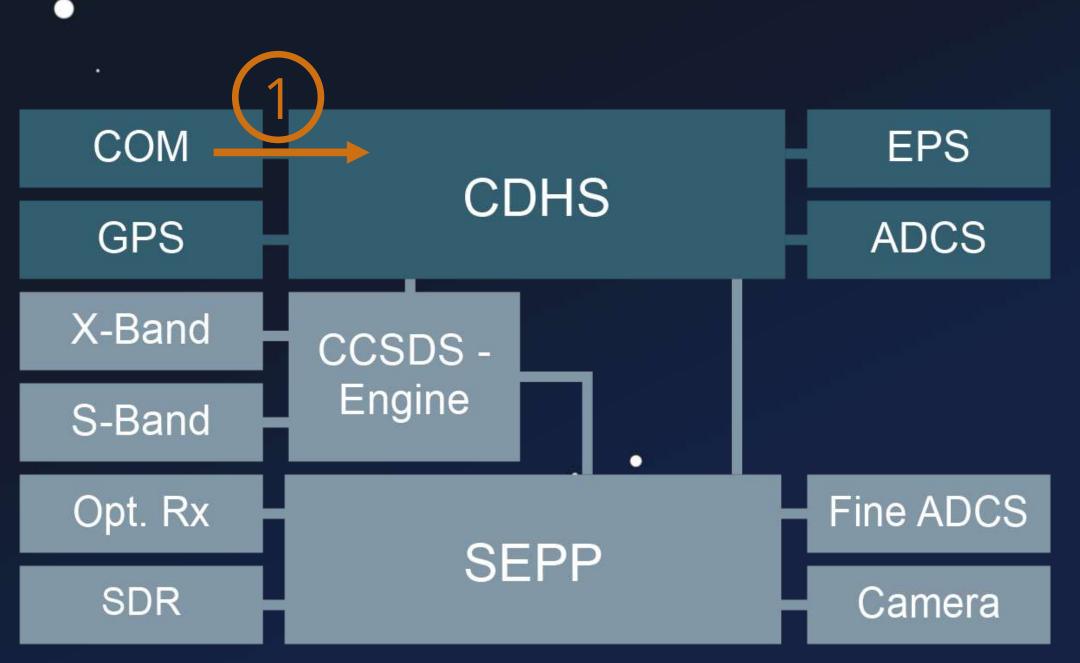
Open for Research



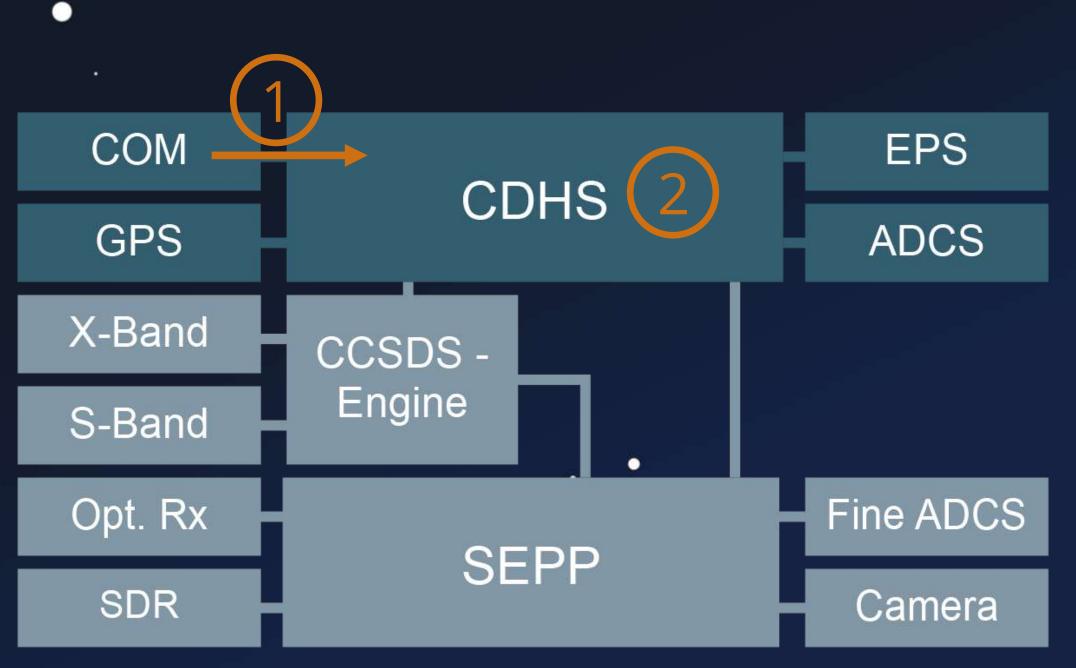
S-/X-Band, SDR, Optical Rx., Camera, ...

Peripherals



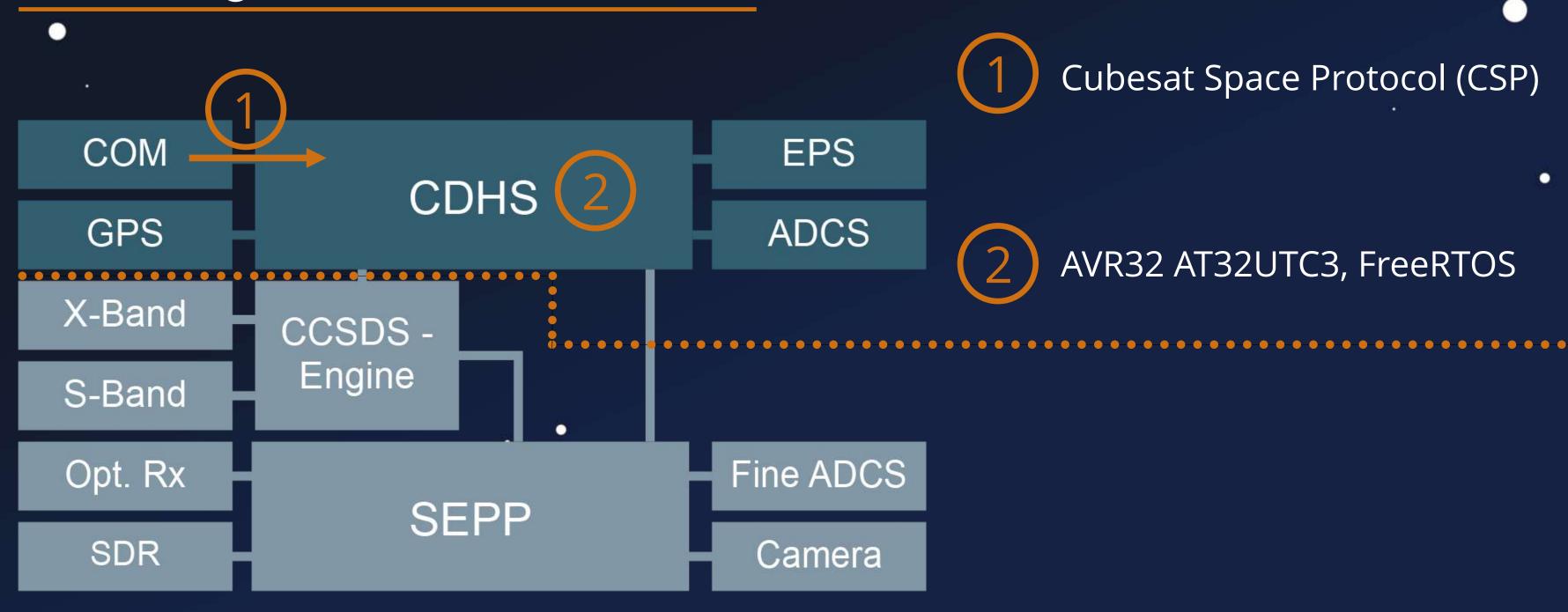


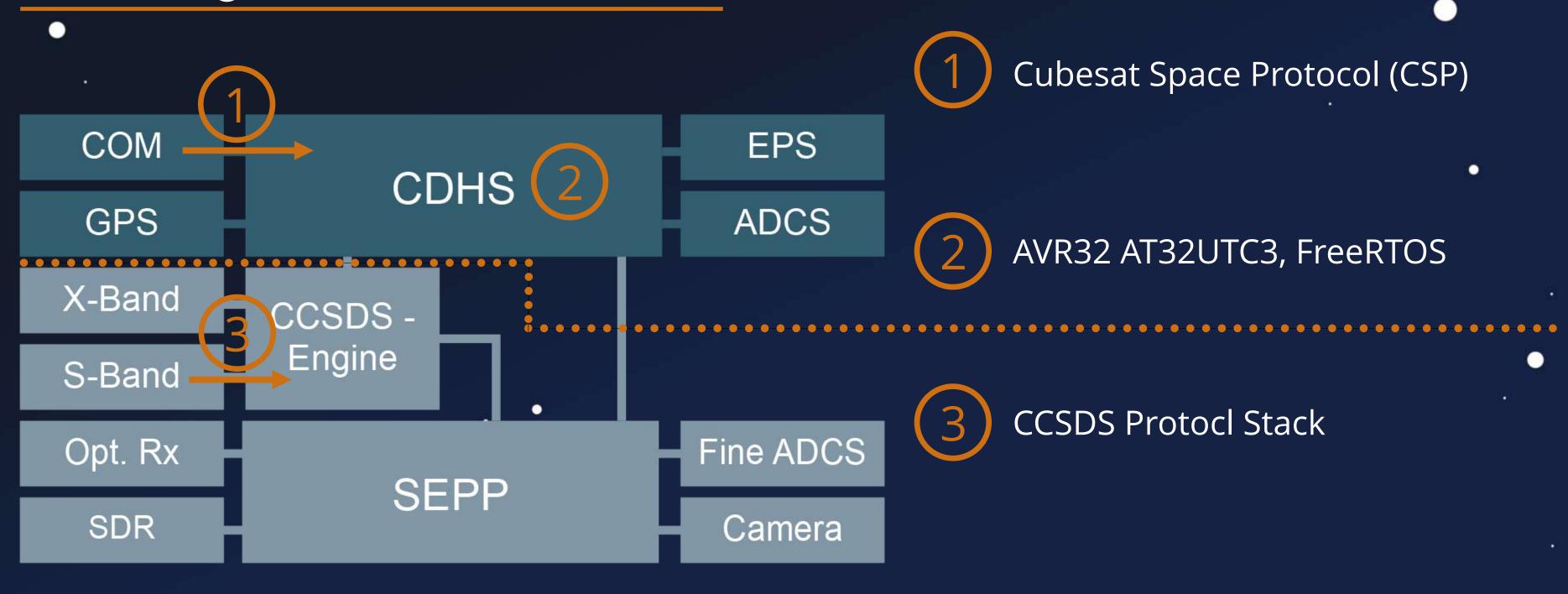
1 Cubesat Space Protocol (CSP)

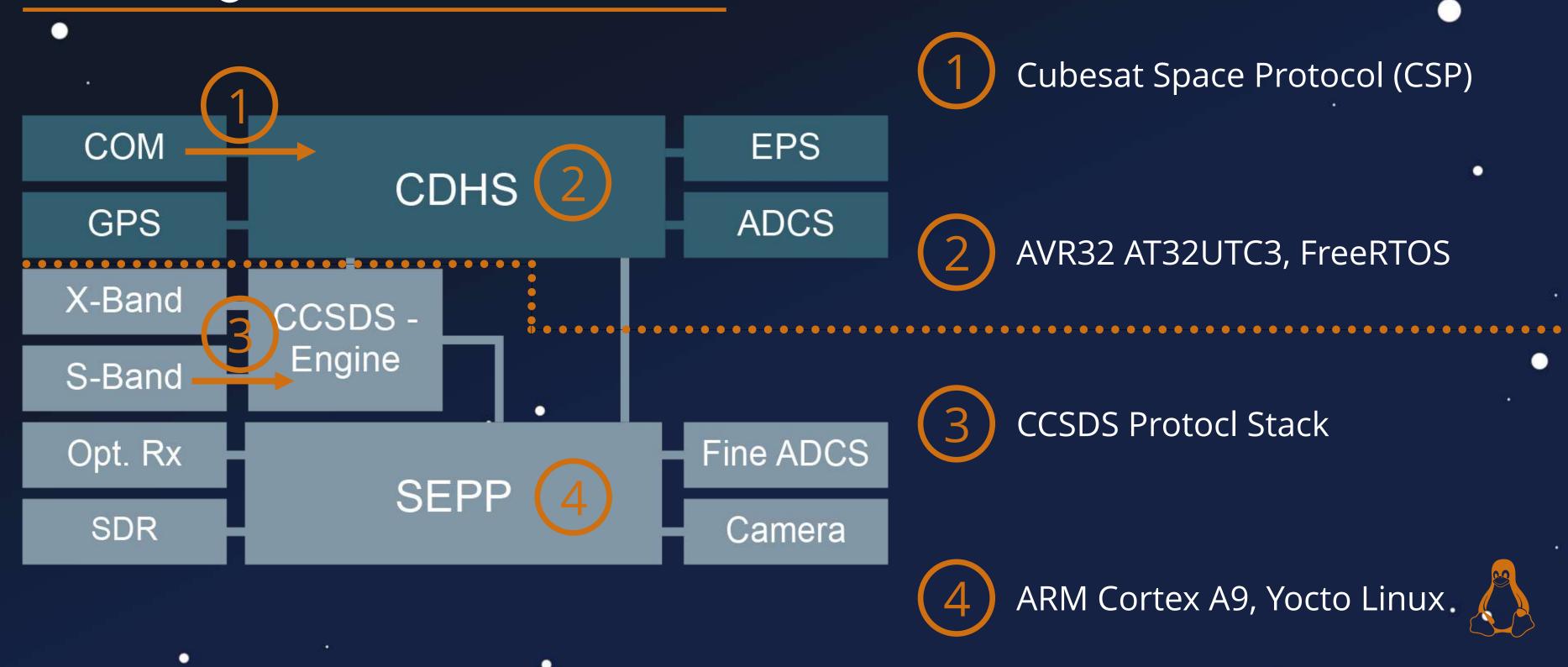


1 Cubesat Space Protocol (CSP)

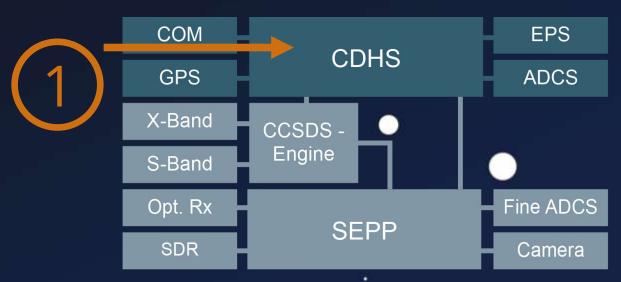
2 AVR32 AT32UTC3, FreeRTOS







UHF-Stack



Cubesat Space Protocol (CSP) v1

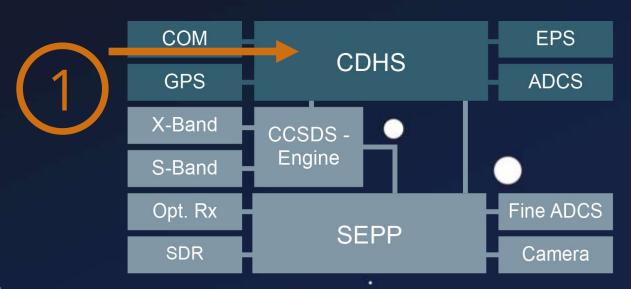


	CSP Header 1.x																															
Bit offset	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	Pric	ority		s	ourc	æ			Des	stina	tion		19 18 17 16 15 14 Destination Port					Source Port					F	Rese	erved	d	H M A C	X T E A	R D P	C R C		
32	32 Data (0 – 65,535 bytes)																															

Source: 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

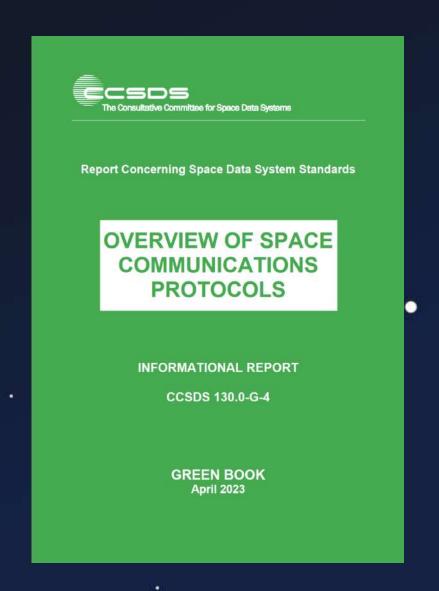
- 1. MAC comparison leaks timing data #44
 - memcmp to compare the digest
- 2. HMAC doesn't protect headers #45
 - Same problem for the CRC checks
- 3. XTEA encrypt packet nonce too predictable #162
 - const uint32_t nonce = (uint32_t)rand();

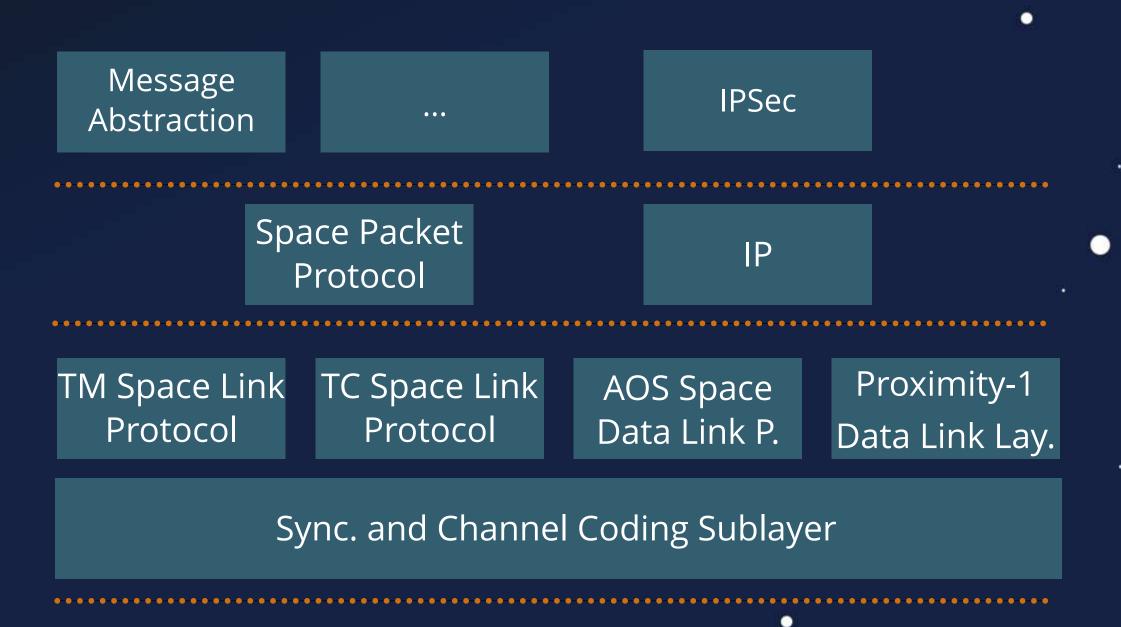
Authors: Issues fixed in libcsp v2

S-Band Stack

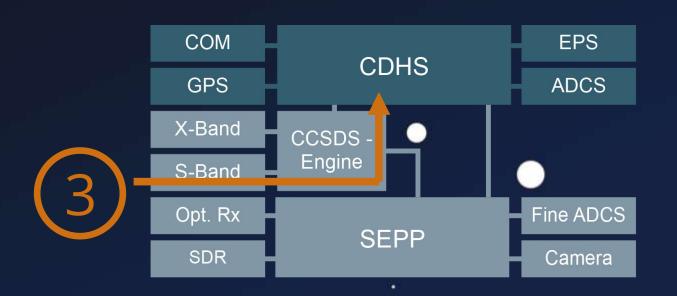


CCSDS - Protocol Stack

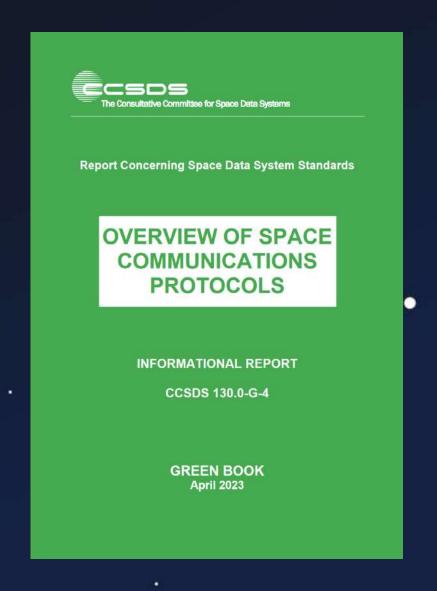


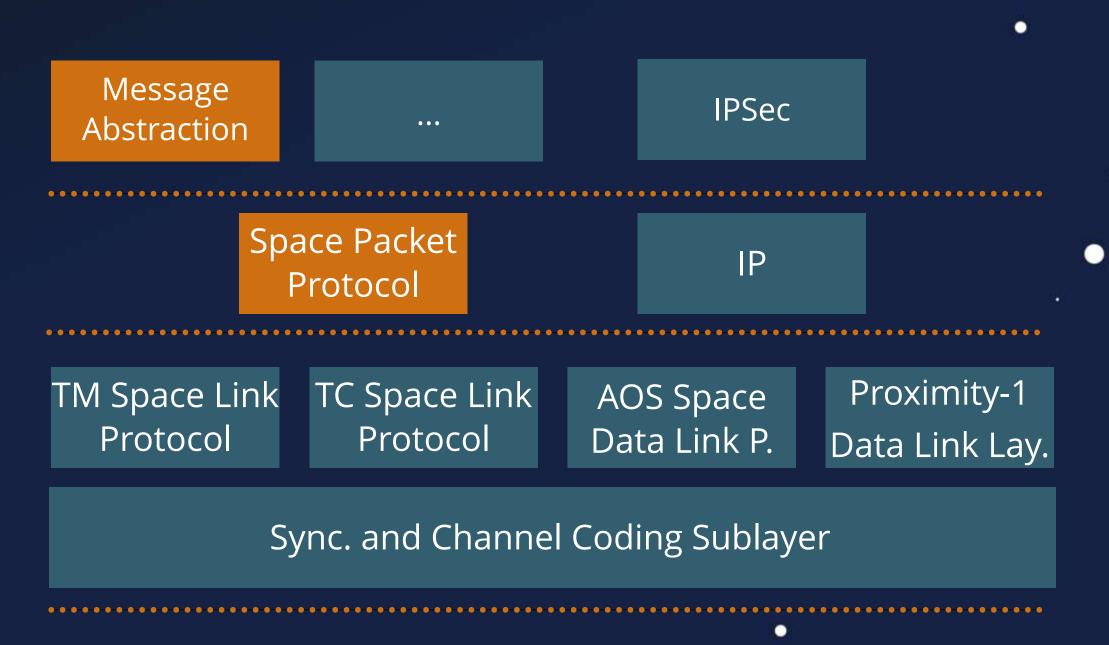


S-Band Stack



CCSDS - Protocol Stack



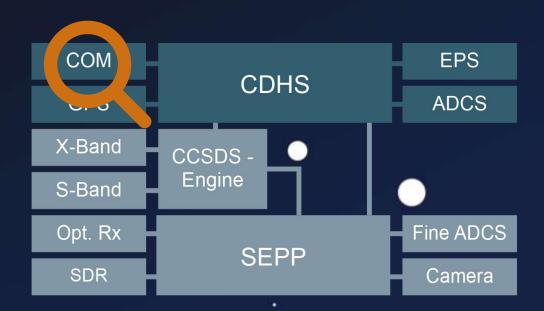


Unprotected TCs

COM

```
int csp_route_security_chek(...) {
  if (packet->id.flags & CSP_FXTEA) {
    csp_log_error("Received XTEA encrypted packet, but CSP was compiled without XTEA support. Discarding packet");
  }
  // ...
  if (packet->id.flags & CSP_FHMAC) {
    csp_log_error("Received packet with HMAC, but CSP was compiled without HMAC support. Discarding packet");
  }
}

// ...
// ...
// ...
// ...
// ...
```



Unprotected TCs



COM

- Bypass COM Protection
 - Missing TC Protection

```
1 int sch_handler_set_raw_memory(scheduler_cmd_t* pCmd) {
     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
     char* pWriteData;
     if (pAddr) {
       if (g_sch_exec_mode != 1 ) {
         /* exception and return */
       char* pWriteData = &pAddr->start of data buf;
       if (pAddr->filesystem_target) {
       } else {
         memcpy(pAddr->targetAddr,
                &pAddr->start of data buf,
15
                pAddr->writeLength);
19 }
```

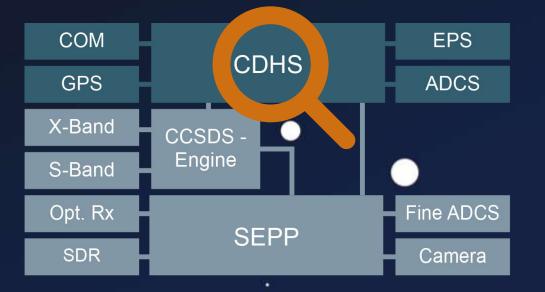
Unprotected TCs

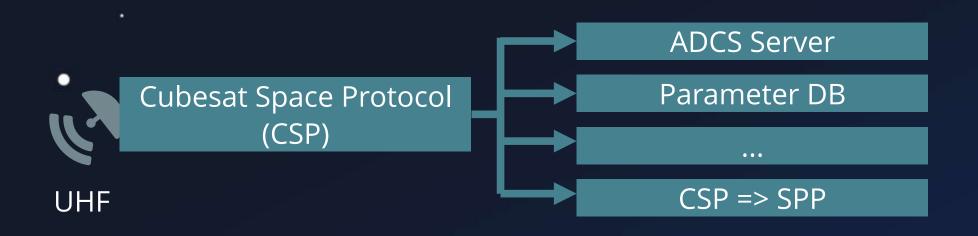


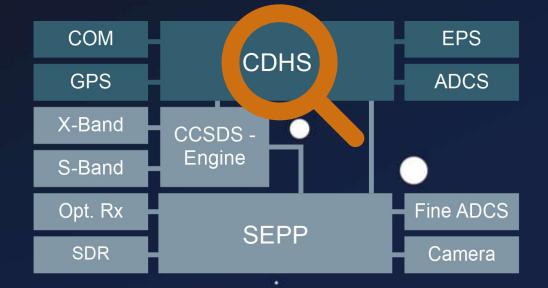
COM

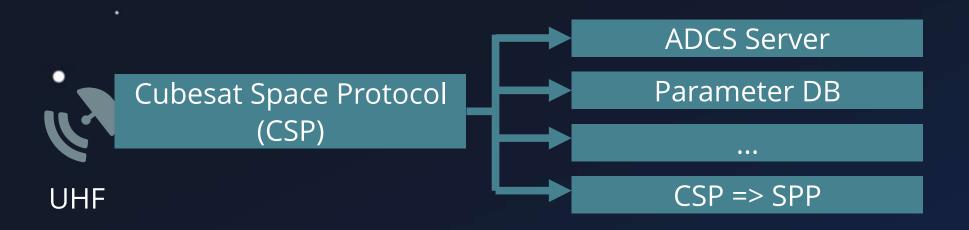
- Bypass COM Protection
 - Missing TC Protection

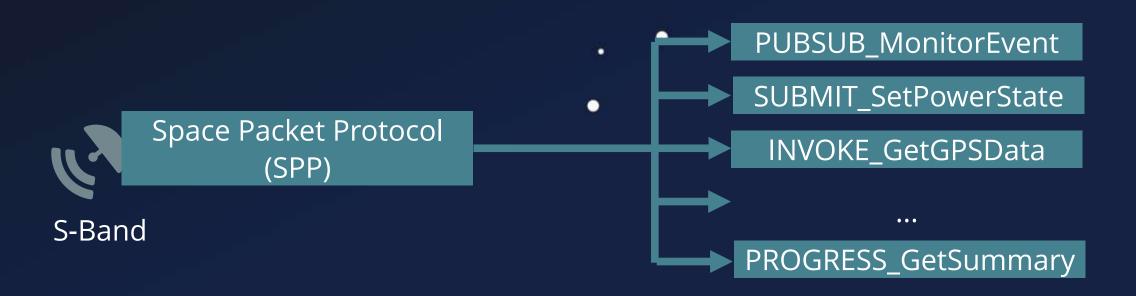
```
1 int sch handler set raw memory(scheduler cmd t* pCmd) {
     raw_mem_access_cmd_t* pAddr = pCmd->pCmdArgs;
     char* pWriteData;
     if (pAddr) {
       if (g_sch_exec_mode != 1 ) {
       char* pWriteData = &pAddr->start of data buf;
       if (pAddr->filesystem_target) {
         memcpy(pAddr->targetAddr,
13
                &pAddr->start of data buf,
14
15
                pAddr->writeLength);
```

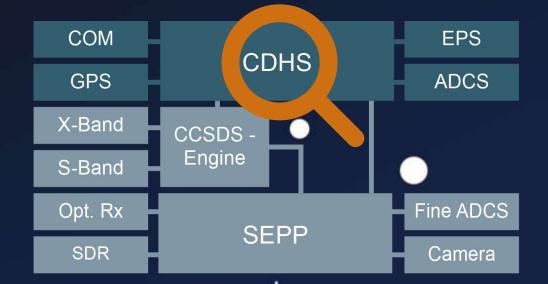


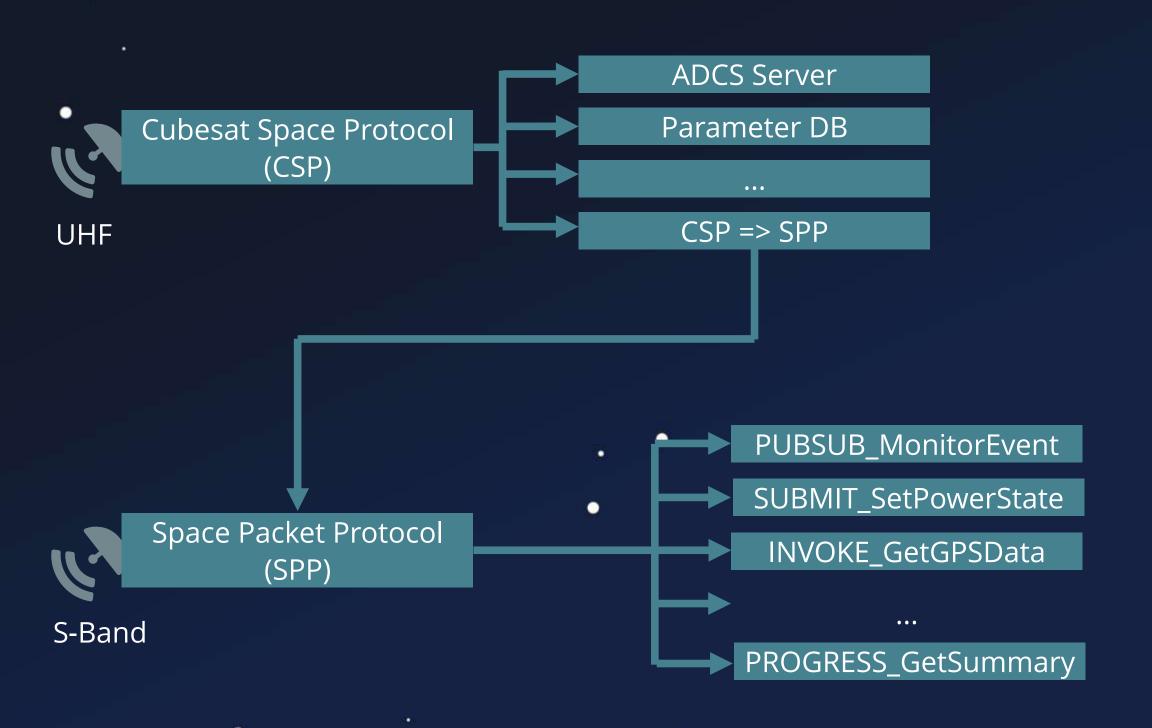


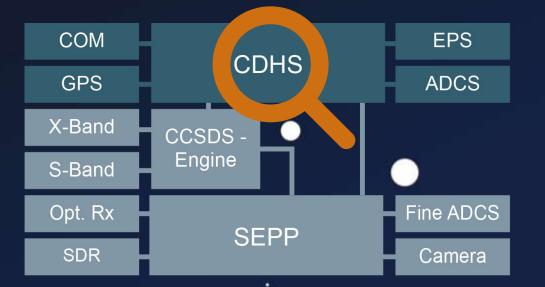


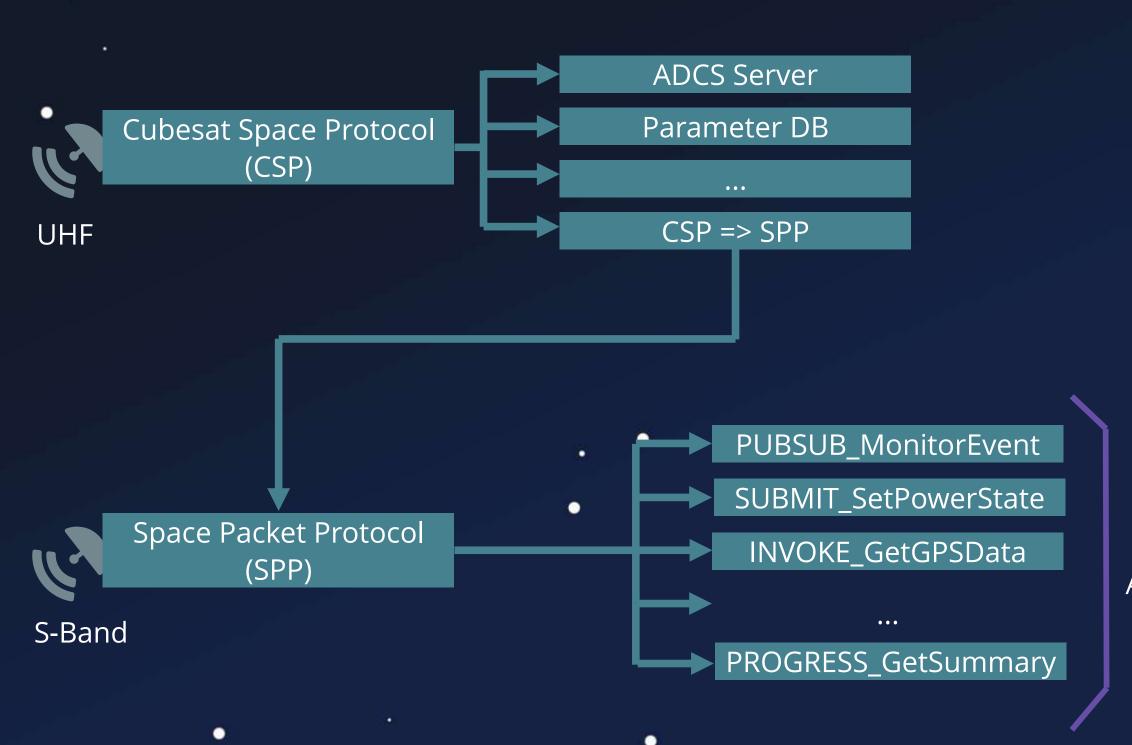


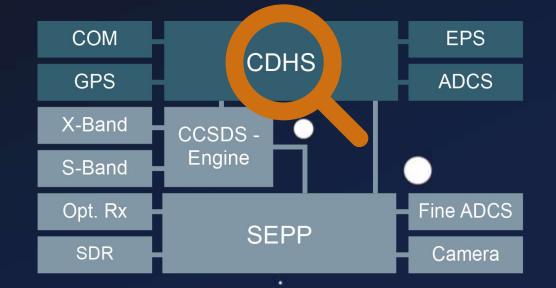








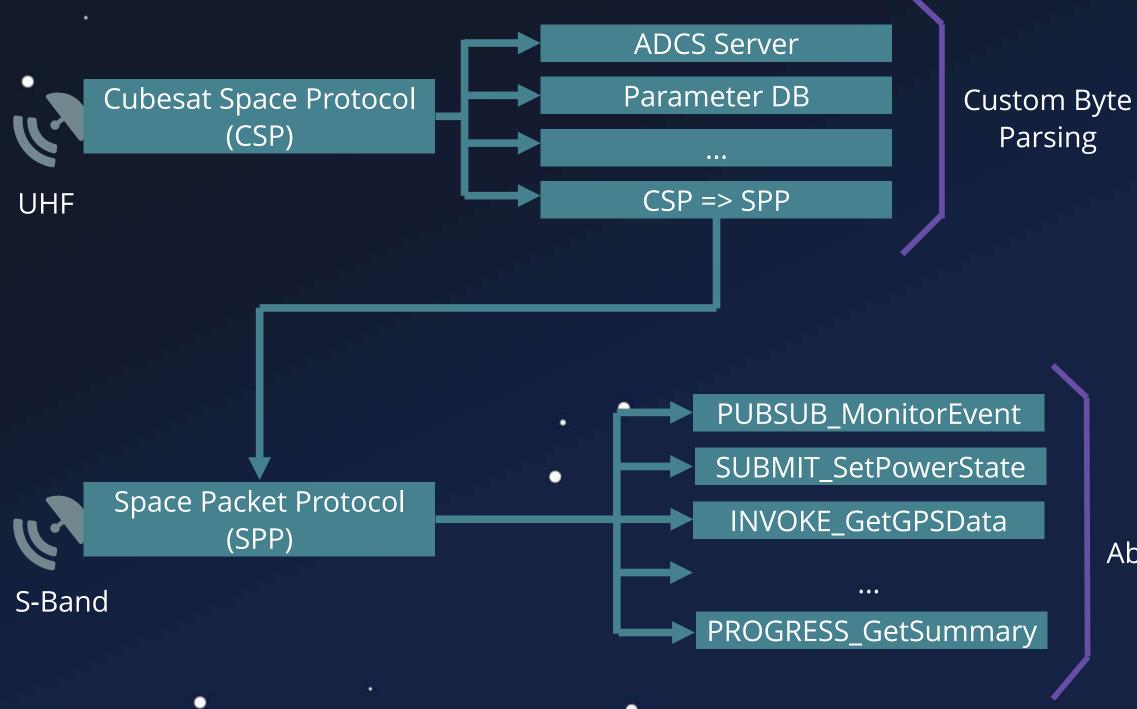


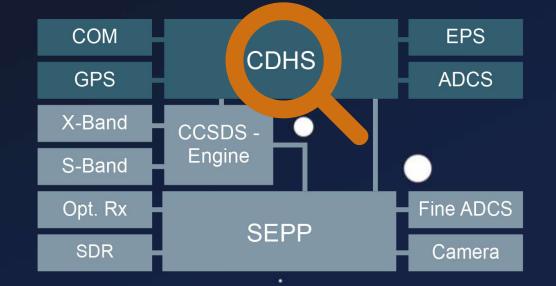


Message Abstraction Layer (MAL) Message Abstraction

Space Packet Protocol



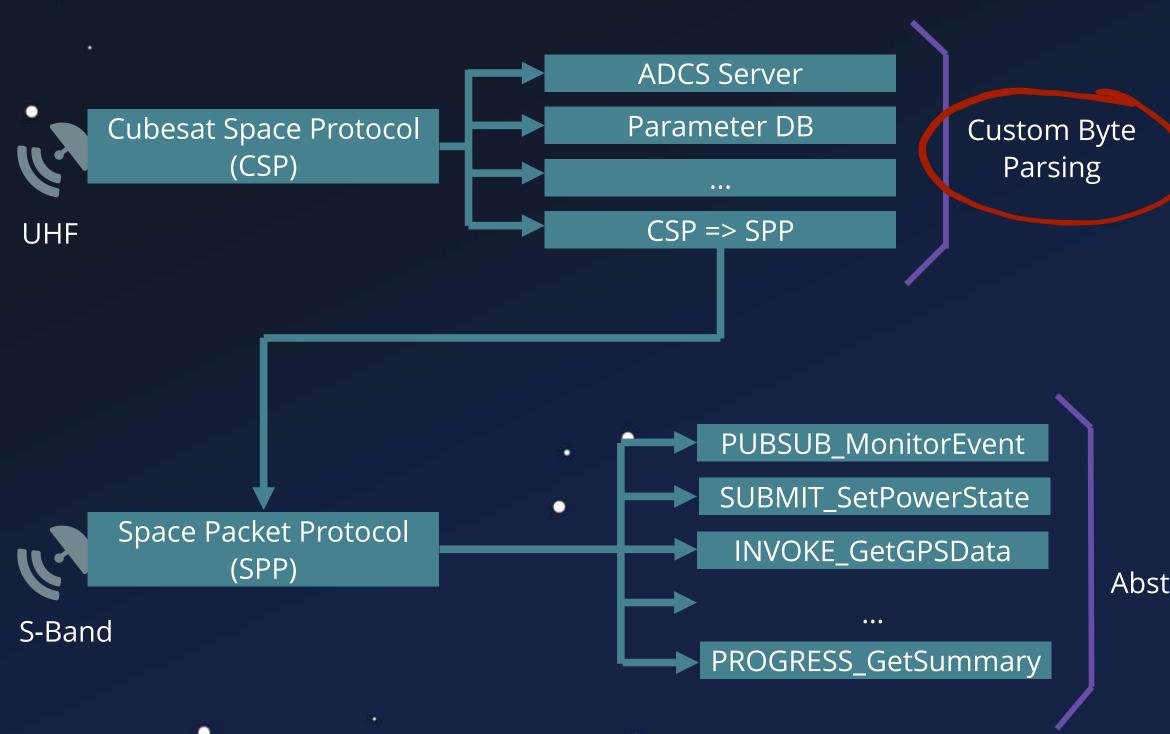


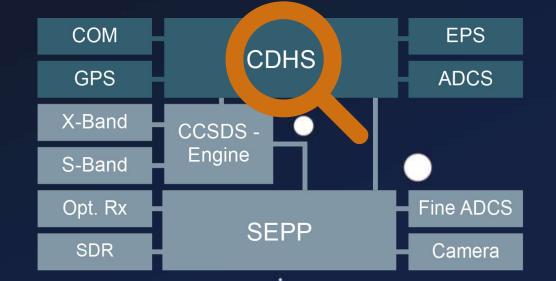


Message Abstraction Layer (MAL) Message Abstraction

Space Packet Protocol







Message
Abstraction Layer

(MAL)

Space Packet Protocol The Cornulative Committee for Space Data Systems

Report Concerning Space Data System Standards

OVERVIEW OF SPACE COMMUNICATIONS PROTOCOLS

INFORMATIONAL REPORT

CCSDS 130.0-G-4

GREEN BOOK

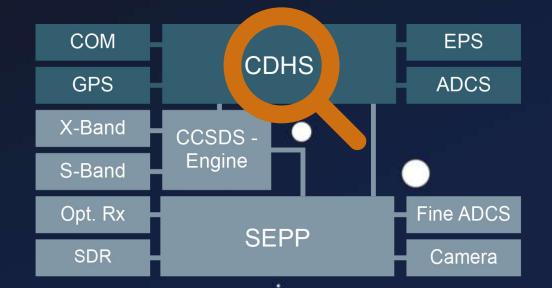
April 2023

Vulnerable TC

Cubesat Space Protocol (CSP)

ADCS Server

```
1 void task_adcs_servr() {
      char log_file_name [32];
      csp_listen(socket, 10);
      csp_bind(socket, port);
  6
      do {
        do {
  9
          conn = csp accept(socket, 0xff);
 10
         } while (do wait for conn);
 11
        packet = csp_read(conn, 10);
 12
        if (packet) {
 13
 14
          packet data = packet->data;
          switch(*packet_data) {
 15
 16
 17
            case SET LOGFILE: {
              packet_data = packet->data + 0xf;
 18
               log_file_name[0] = '\0';
 19
               strcat(log_file_name,packet_data);
 20
 21
 22
 23
 24
_25
```

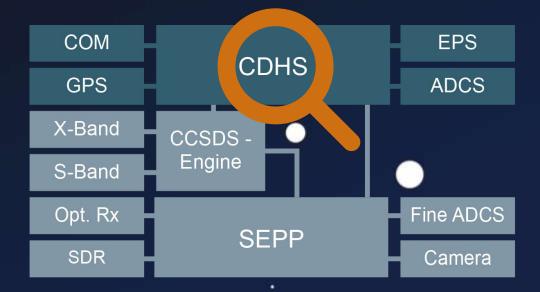


Vulnerable TC

Cubesat Space Protocol (CSP)

ADCS Server

```
1 void task_adcs_servr() {
     char log_file_name [32];
     csp_listen(socket, 10);
     csp_bind(socket, port);
       do {
 9
         conn = csp accept(socket, 0xff);
       } while (do wait for conn);
10
11
       packet = csp_read(conn, 10);
12
       if (packet) {
         packet data = packet->data;
         switch(*packet_data) {
           case SET LOGFILE: {
             packet data = packet->data + 0xf;
             log file name[0] = ' \setminus 0';
             strcat(log_file_name,packet_data);
```

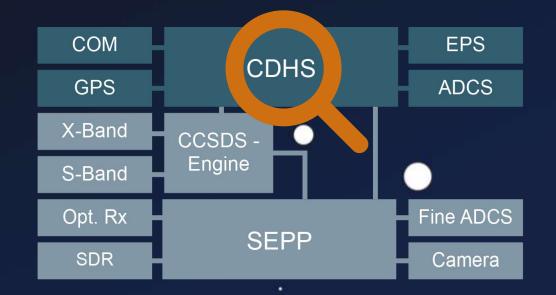


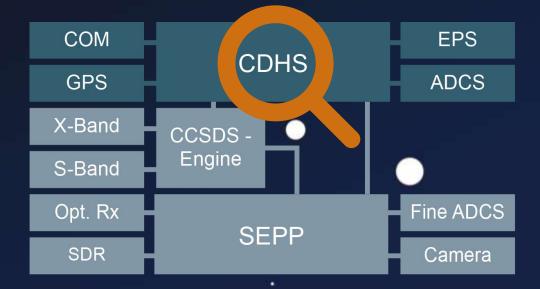
Vulnerable TC

Cubesat Space Protocol (CSP)

ADCS Server

```
1 void task_adcs_servr() {
     char log_file_name [32];
     csp_listen(socket, 10);
     csp_bind(socket, port);
         conn = csp_accept(socket, 0xff);
       } while (do wait for conn);
       packet = csp read(conn, 10);
       if (packet) {
         packet data = packet->data;
         switch(*packet_data) {
           case SET LOGFILE: {
             packet data = packet->data + 0xf;
18
             log_file_name[0] = '\0';
19
             strcat(log_file_name,packet_data);
20
```





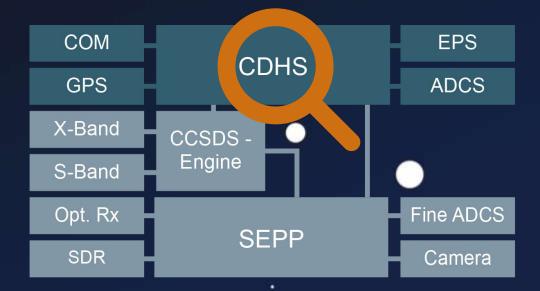
COM

- Bypass COM Protection
 - Missing TC Protection

CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus



COM

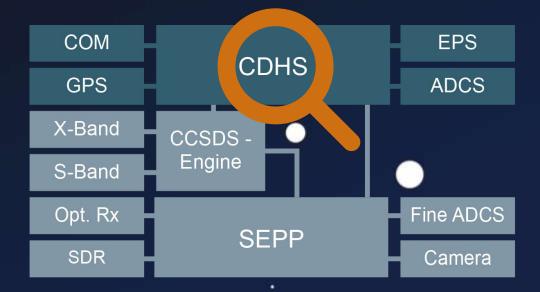
- Bypass COM Protection
 - Missing TC Protection

CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus

Hijack Bus Control Flow



COM

- Bypass COM Protection
 - Missing TC Protection

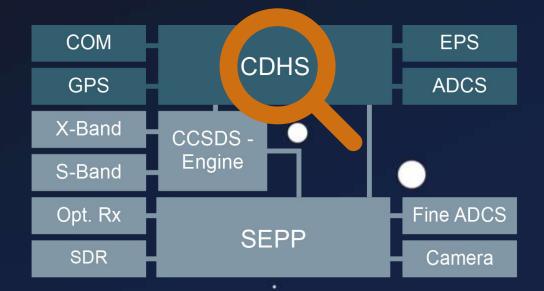
CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus

Hijack Bus Control Flow

- No OS-Defenses
 - ASLR*
 - NX Stack



COM

- Bypass COM Protection
 - Missing TC Protection

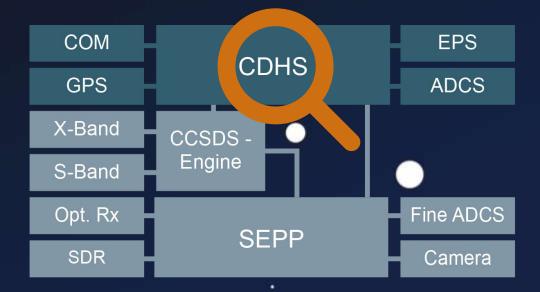
CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus

Hijack Bus Control Flow

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



COM

- Bypass COM Protection
 - Missing TC Protection

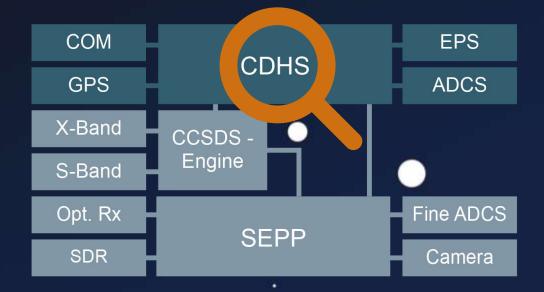
CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus

- Hijack Bus Control Flow
- Full Bus Privileges

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



COM

- Bypass COM Protection
 - Missing TC Protection

CDHS

- Deploy Attacker Payload
 - Vulnerable TC

Bus

- Hijack Bus Control Flow
- Full Bus Privileges

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

Privilege-free RTOS

Demo Setup

Emulation Overview

TC Handlers

Sensors

Simulation

Agent

OBSW

AVR32

Emulation Ovierview

TC Handlers

OBSW

AVR32

QEMU

UHF

Simulation Sensors Agent

Telecommand

TCP

Telemtry



Emulation Ovierview

UHF Telecommand **TC Handlers** Simulation TCP **Telemtry** Sensors **OBSW** Sensor Values AVR32 Agent TCP Flight Manuvers **QEMU**

AVR32-QEMU

404 - AVR32 Not Found

AVR32

AVR32-QEMU

404 - AVR32 Not Found

RUHR UNIVERSITÄT BOCHUM



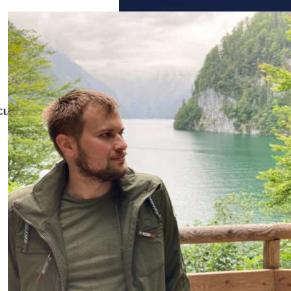
RUHR-UNIVERSITÄT BOCHUM

Hacking the Stars: A Fuzzing Based Security Assessment of CubeSat Firmware

Florian Göhler

Master's Thesis - December 22, 2022. Chair for System Security.

1st Supervisor: Prof. Dr. Thorsten Holz 2nd Supervisor: M.Sc. Johannes Willbold





AVR32

AVR32-QEMU

404 - AVR32 Not Found

RUHR UNIVERSITÄT BOCHUM



RUHR-UNIVERSITÄT BOCHUM

Hacking the Stars: A Fuzzing Based Secu Assessment of CubeSat Firmware

Florian Göhler

Master's Thesis - December 22, 2022 Chair for System Security.

1st Supervisor: Prof. Dr. Thorsten Holz 2nd Supervisor: M.Sc. Johannes Willbold





AVR32

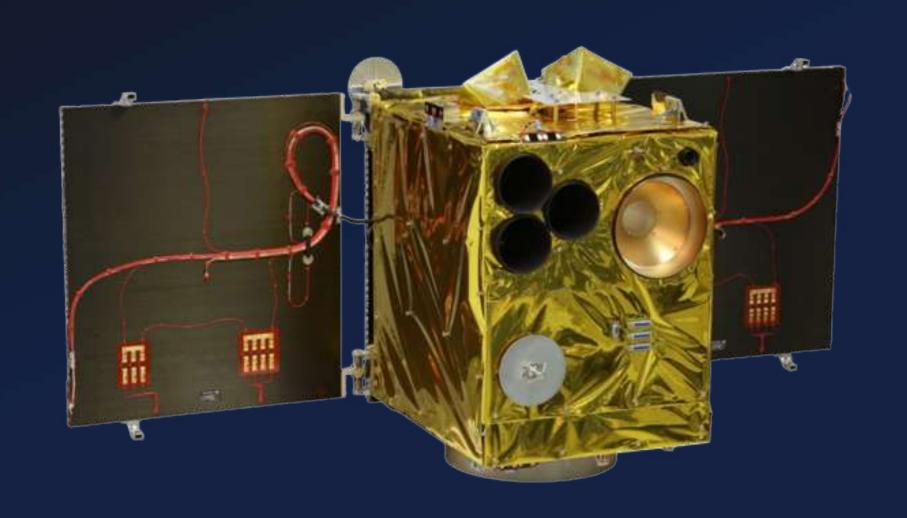
- Florian Göhler
- AVR32 in QEMU from Scratch
- Incl. I2C, SPI, PDCA, etc.
- Blog:
 - How to add a new architecture to QEMU - Part 1-4

Live Demo

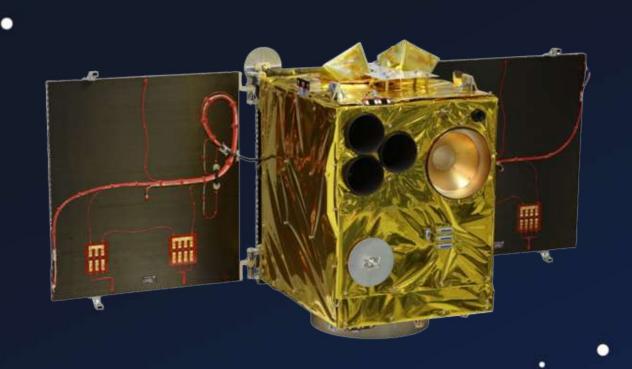


```
1 $> ./access-satellite.
2 [*] Uploading TC ...
3 [*] Deploying payload ...
4 [*] Payload written to flash ...
5 [*] Rebooting ...
6 [*] $$$
```

Flying Laptop

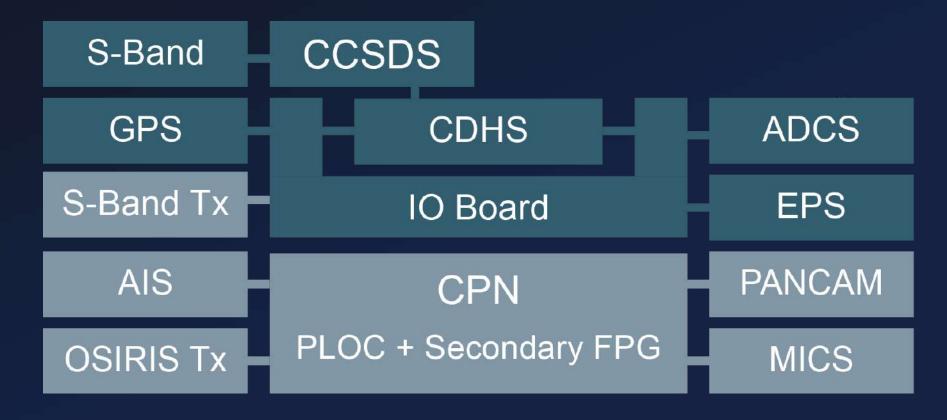


Flying Laptop



Technology Tester

Co-Developed by Airbus Space & Defense



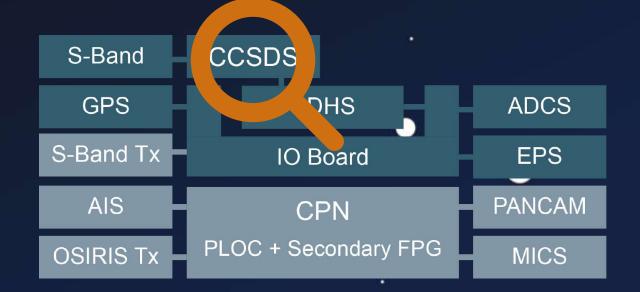
De-orbit mechanism, AIS, Camera, etc...

Peripherals

SPARC LEON 3 - OBC from Airbus S&D

Bus Platform

CCSDS



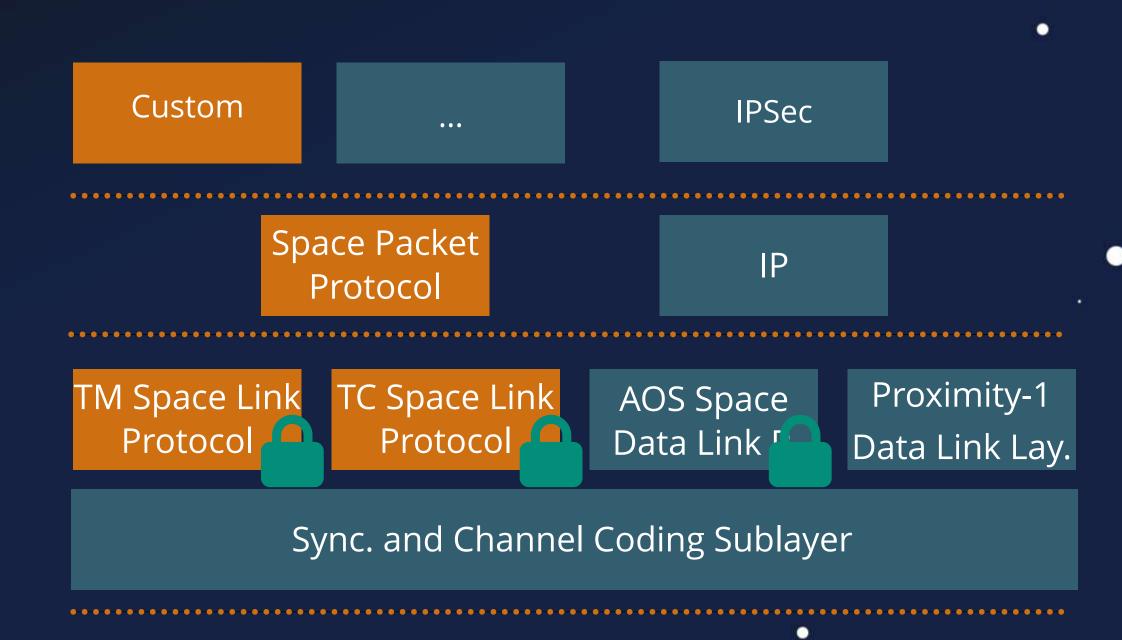
The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

OVERVIEW OF SPACE
COMMUNICATIONS
PROTOCOLS

INFORMATIONAL REPORT
CCSDS 130.0-G-4

GREEN BOOK April 2023



CCSDS - SDLP





Recommendation for Space Data System Standards

SPACE DATA LINK SECURITY PROTOCOL

RECOMMENDED STANDARD

CCSDS 355.0-B-2

BLUE BOOK July 2022 Space Link Protocol Header

Frame Data

Space Link
Protocol Trailer

CCSDS - SDLS





Recommendation for Space Data System Standards

SPACE DATA LINK SECURITY PROTOCOL

RECOMMENDED STANDARD

CCSDS 355.0-B-2

BLUE BOOK July 2022 Space Link Protocol Header

Security Header Frame Data

Security Trailer Space Link
Protocol Trailer

Bigger Picture

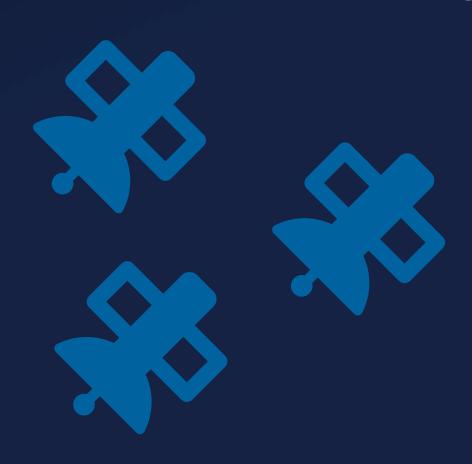


"But it's different for [...] satellites.

"But it's different for [...] satellites, right?

Developer Survey







•	Custom	Standard	Weight
			~ 1.3 kg
			~ 5.4 kg
			~ 120 kg
			Weight ≈ Money

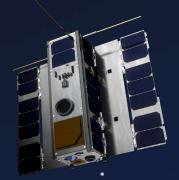


Custom /
Standard



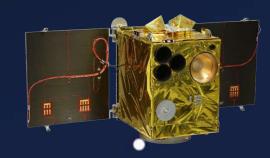
















	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
Σ	10	2	5

Weight ≈ Money

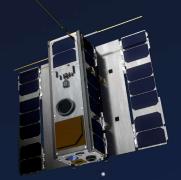


Custom /
Standard



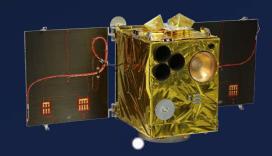














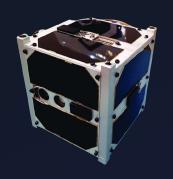


	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	0
Abstains	3	0	1
Σ	10	2	5

Weight ≈ Money



Custom /
Standard



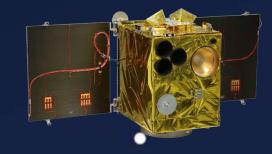
















	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	U
Abstains	3	0	1
Σ	10	2	5

Weight ≈ Money

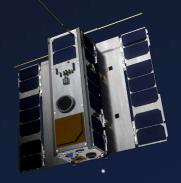


Custom /
Standard







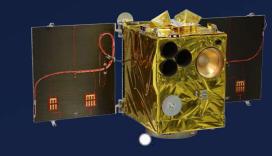






	1-50 kg	50-100 kg	> 100 kg
Standard	1	1	4
Custom	6	1	U
Abstains	3	0	1
Σ	10	2	5

Weight ≈ Money







=> Inaccessible Standard

TC Protection

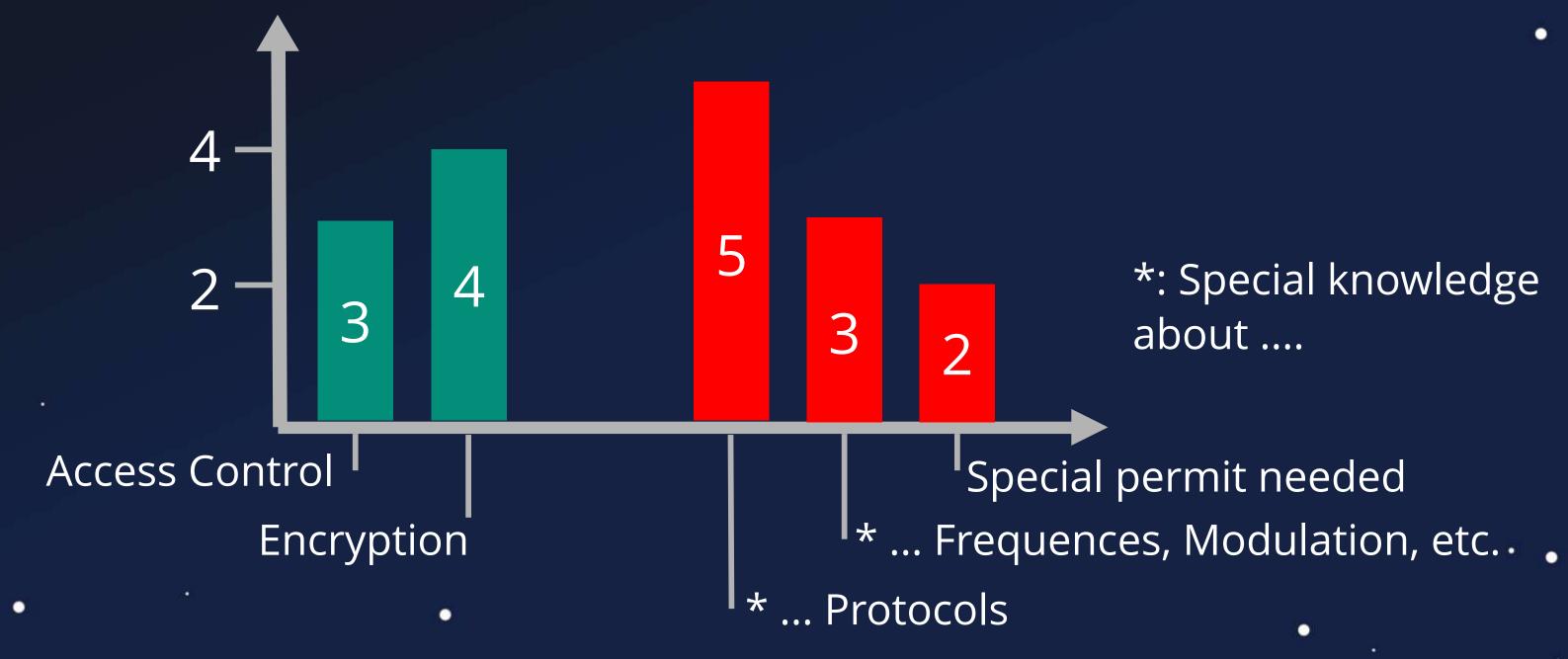


Question: Are any measures deployed to prevent 3rd parties from controlling your satellite? Unknown*: Prefer not to say / Don't know Unknown* No Yes

TC Obscurity



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



But it's different for *my* satellite

Impact



1. Hack a Satellite

???

Scenarios



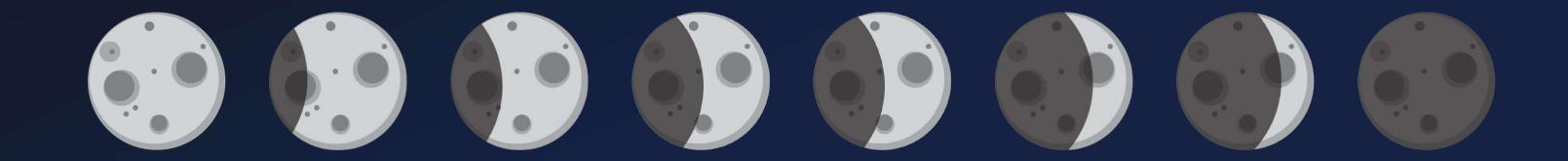
Orbital Access

1 Attacking Inter-Sat Links

2 Orbital Traffic Interception

3 Kessler Syndrome

Lesson Learnt



Lessons Learnt



Firmware Attacks on Satellites are a thing



ViaSat Incident != Satellite Firmware Attack



Common Sat Protocols lack Security

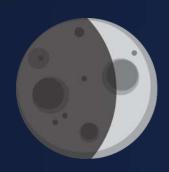


Security by Obscurity

Lessons Learnt



Missing TC Protection



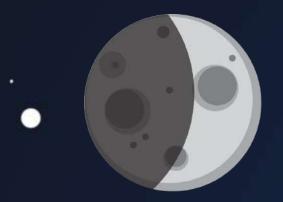
Missing State-of-the-Art Defenses



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





Johannes Willbold - 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

[3] Flying Laptop Image: https://www.irs.uni-stuttgart.de/en/research/satellitetechnology-and-instruments/smallsatelliteprogram/flying-laptop/