

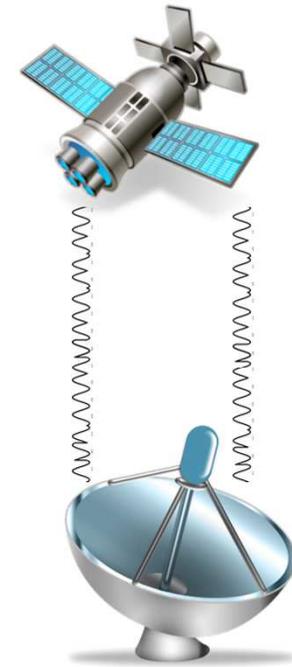
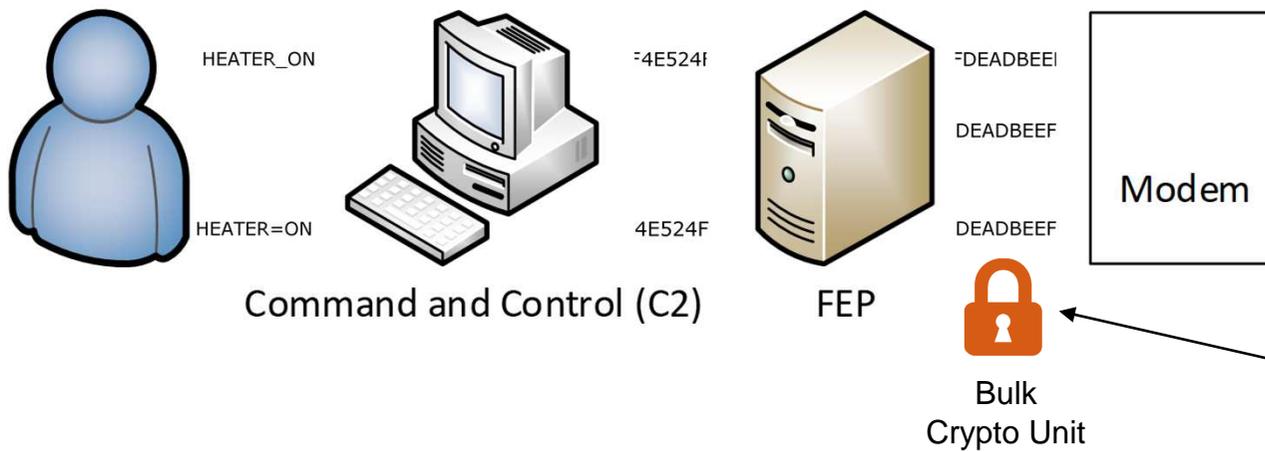
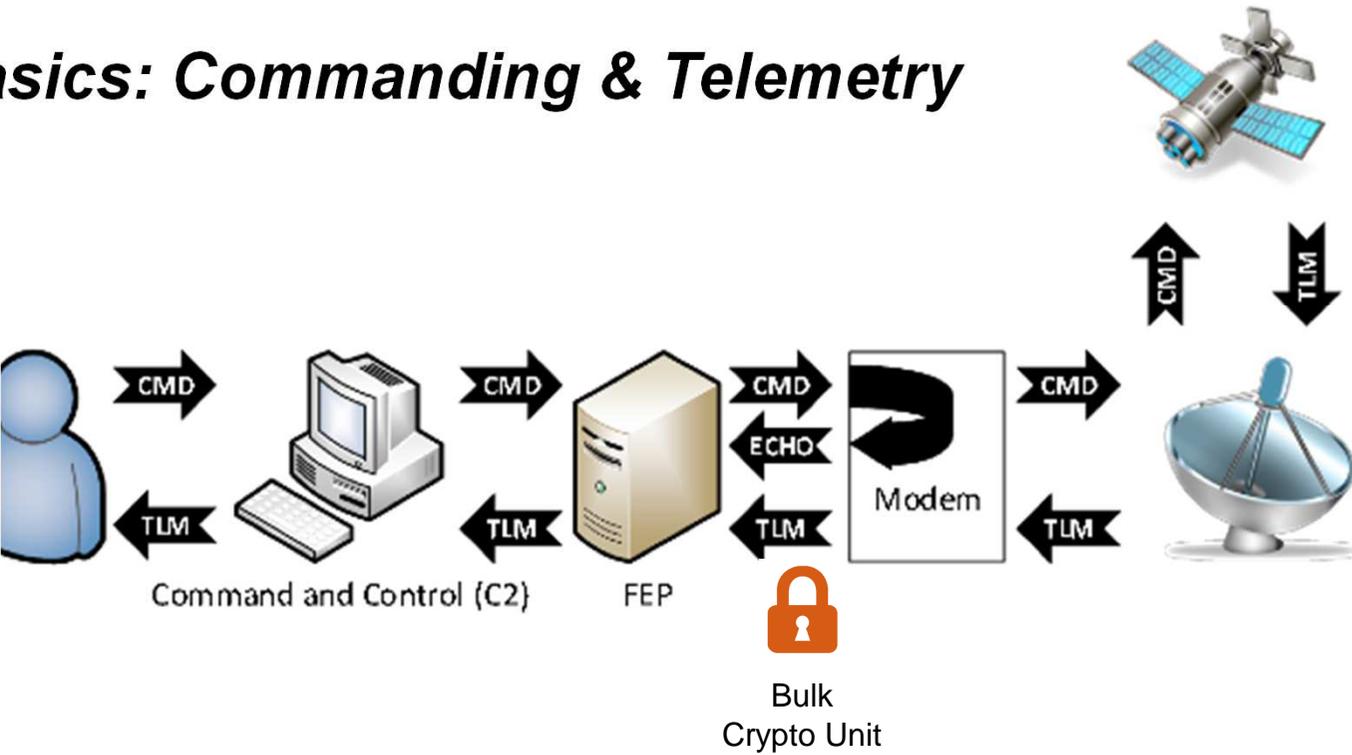
Covert Control: Unveiling Vulnerabilities TT&C to Cyber Attack CYSAT 202



Brandon Bailey, Randi Tinn
*Cybersecurity and Advanced Platforms Subdivision (CA)
Cyber Assessment & Research Dept (CA)
The Aerospace Corporat*

brandon.bailey@a
240.521.4

Basics: Commanding & Telemetry



We got crypto... we good right?

Not So Fast My Friend!!!

Link Crypto Units (BCUs)

Some Features ... according to ChatGPT

Secure Communication Protocols

- Implement secure communication protocols to establish encrypted channels between ground systems and spacecraft. These protocols ensure that data exchanged over the communication link is protected from interception, tampering, and unauthorized access.*

Encryption and Decryption

- Encrypting and decrypting data transmitted between ground systems and spacecraft. They use cryptographic algorithms and keys to transform plaintext data into ciphertext before transmission and vice versa upon reception. Depending on BCU, full frame (including headers) or only payload frame.*

Key Management

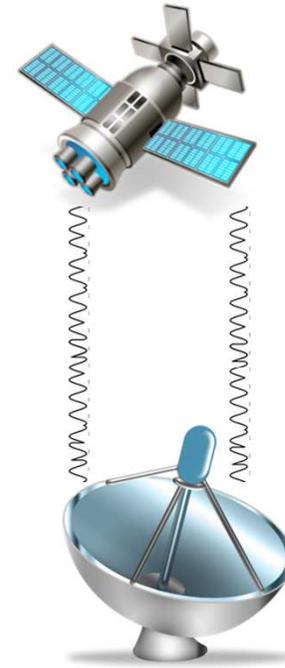
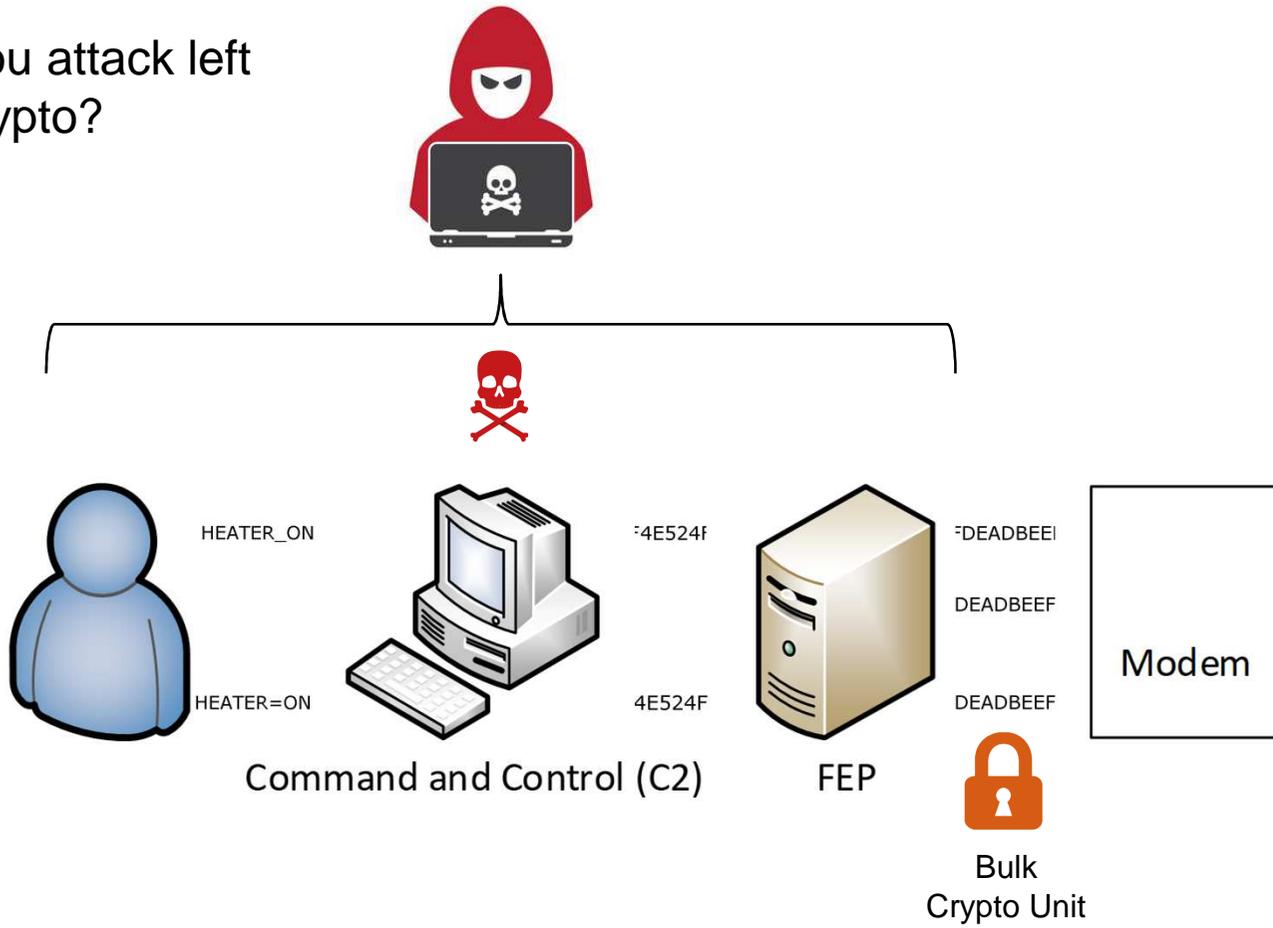
- Manage cryptographic keys used for encryption and decryption. They generate, store, distribute, and update encryption keys securely to ensure the confidentiality and integrity of communications. Key management practices include key generation, key distribution, key rotation, and key revocation.*

Authentication and Integrity Checking

- Authentication and integrity checking to verify the identity of communicating entities and ensure the integrity of transmitted data. Authentication mechanisms authenticate the identities of ground systems and spacecraft, while integrity checks detect any unauthorized modifications to the data during transmission.*

What If....?

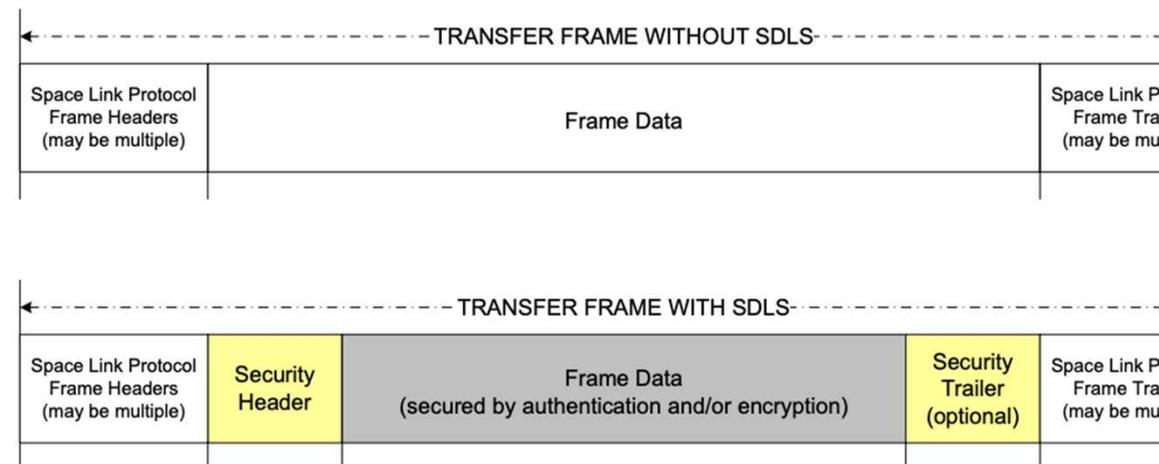
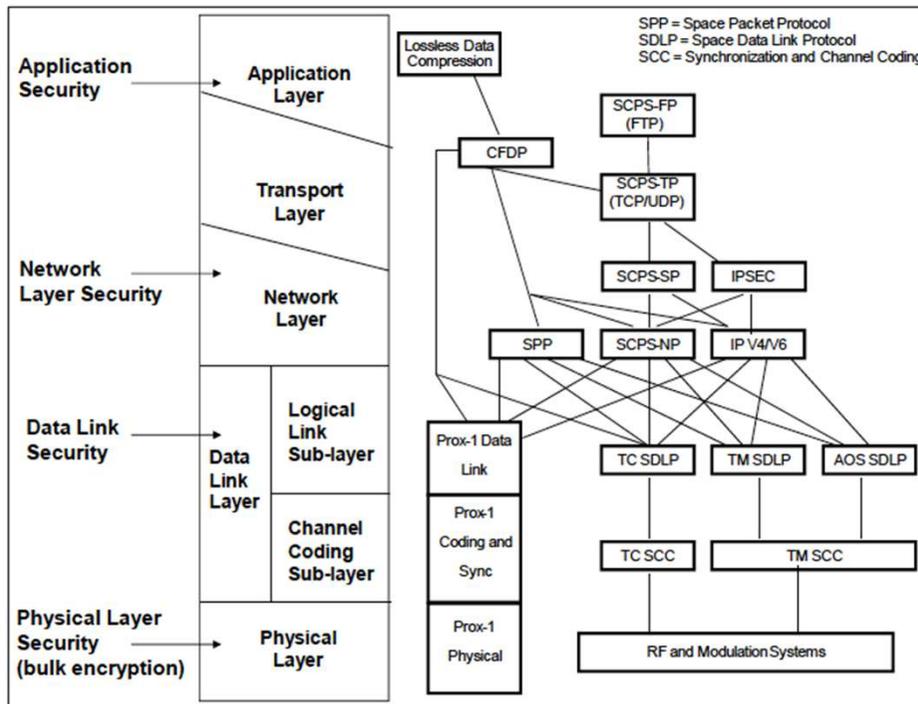
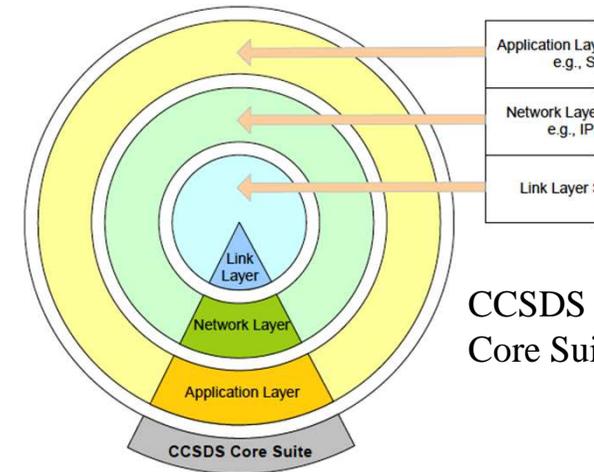
What if you attack left
of bulk crypto?



Space Systems Protocol Overview

Many systems use CCSDS as the space systems protocol – **Not everyone does!!!**

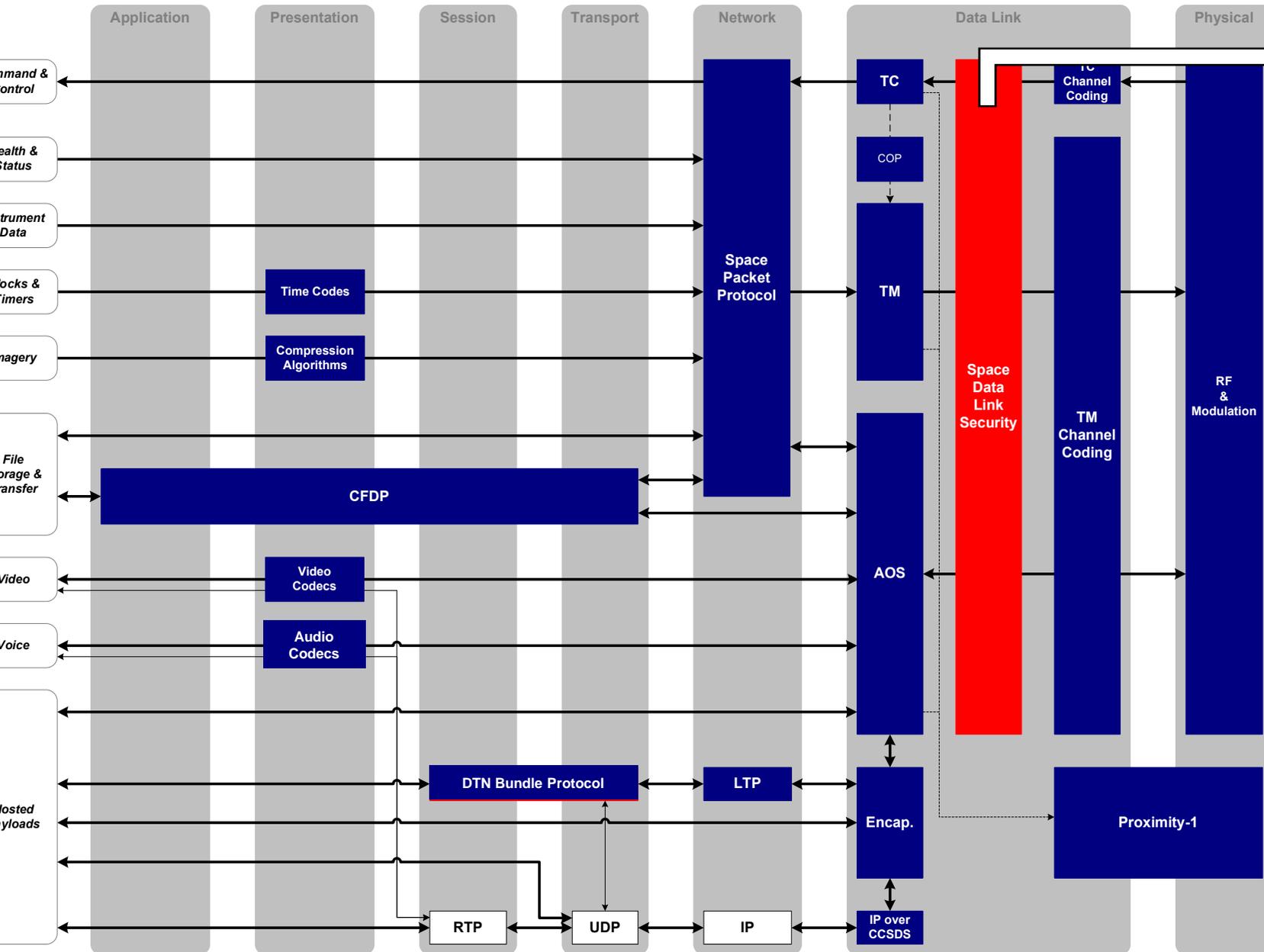
- Protocols are created by the Consultative Committee for Space Data Systems ([CCSDS](https://public.ccsds.org))
- These are recommendations – they are not legally binding
- Protocols exist to allow for collaboration between international agencies
- Some protocol differences between commands and telemetry



CCSDS Space Mission Protocols and Security Options

SDLS Blue Book: <https://public.ccsds.org/Pubs/355x0b2.pdf>

Space-to-Ground: OSI Stack View for CCSDS



Can support encryption and authentication

Demo will show why you must do both!!!

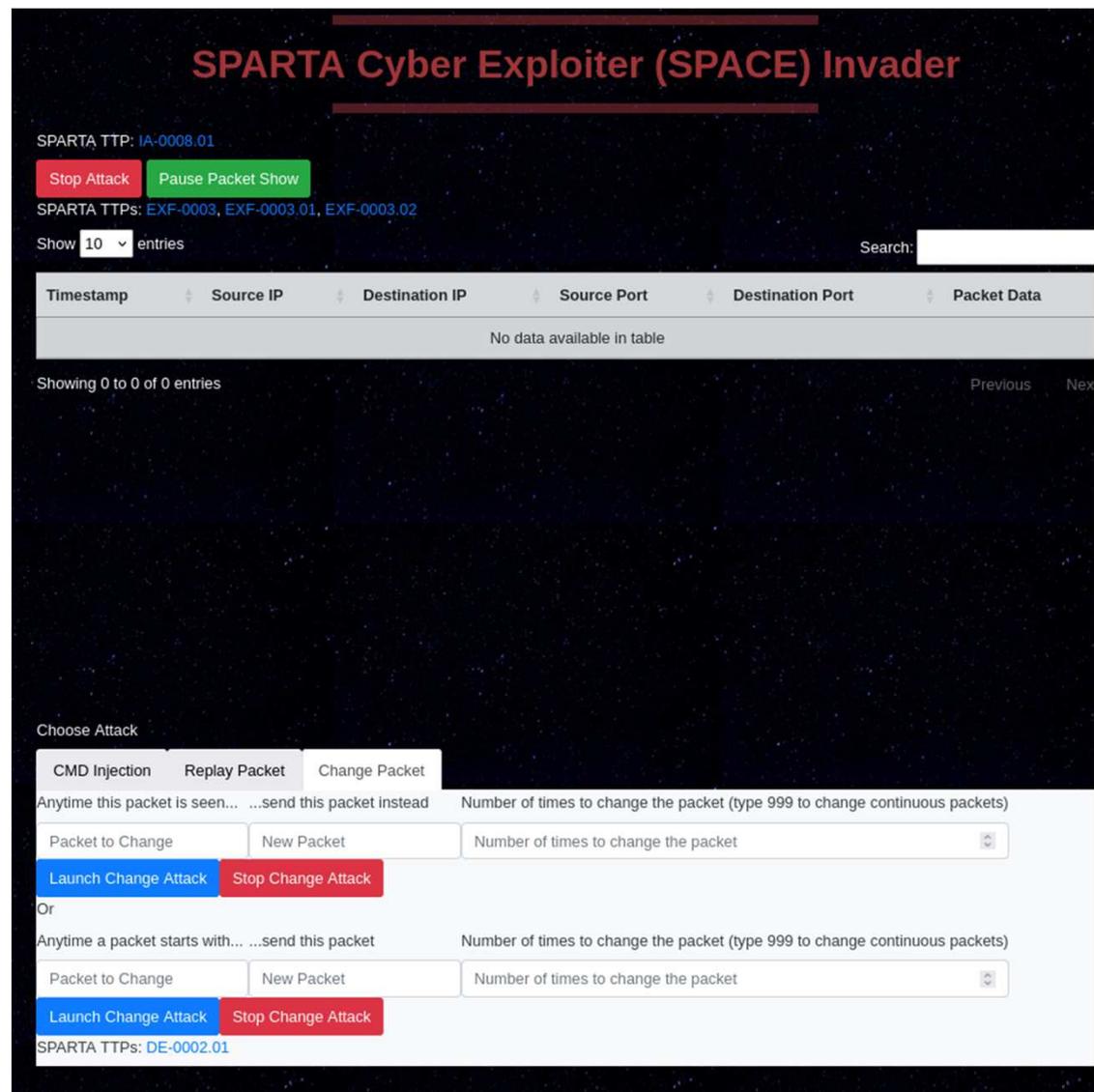
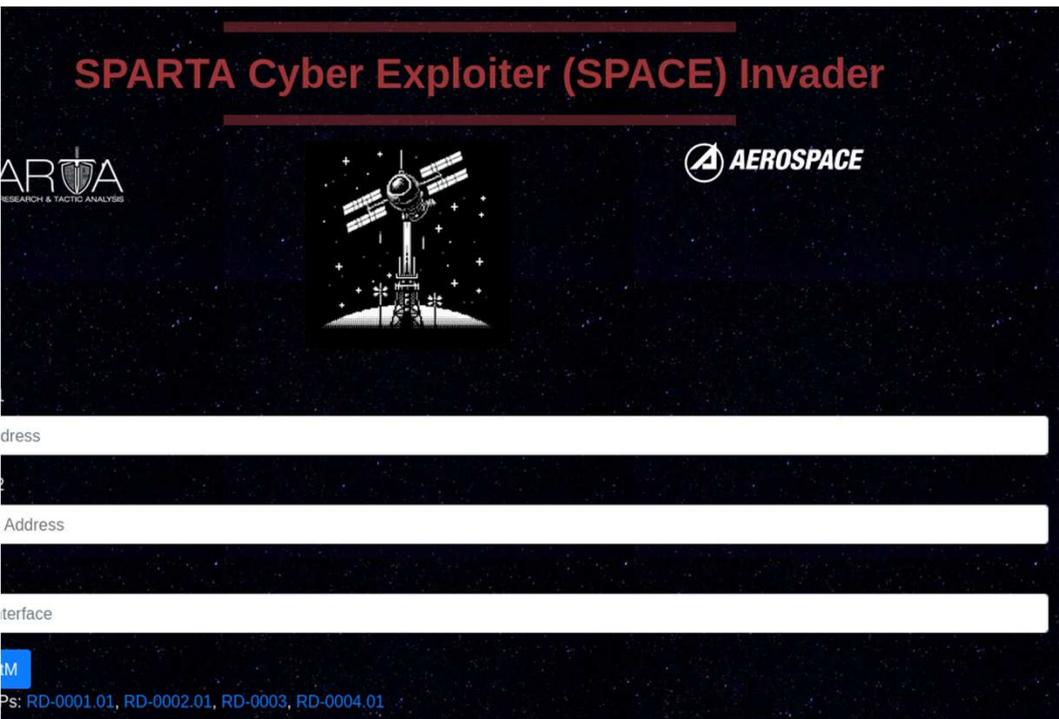
Without data link encryption (e.g., SDL) replay, injection, evasion techniques can be leveraged via Man-in-Middle on the ground

SPACE Invader

MITM Tool / Rogue Ground

SPARTA Cyber Exploiter (SPACE) Invader

- Acts as a rogue ground station or performs MitM attacks
- Currently utilizes 12 SPARTA TTPs
- Parsers for numerous open-source ground station CMD/TLM databases



Scenario #1 – No SDLS (cont.)

Verify Telemetry

MitM the telemetry for the camera to report only two received commands

- SV actually receives many NOOPs but the ground SW receives the wrong data via MitM

SPARTA TTP: IA-0008.01

Stop Attack Start Packet Show

SPARTA TTPs: EXF-0003, EXF-0003.01, EXF-0003.02

Show 10 entries Search: 08c8

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
2024-04-03 17:55:16.844247	10.57.64.223	10.57.64.220	58680	5013	08c8c03300b000000340ccc000000000002
2024-04-03 17:55:19.495495	10.57.64.223	10.57.64.220	58680	5013	08c8c03400b000000350ccc000000000002
2024-04-03 17:55:22.525246	10.57.64.223	10.57.64.220	58680	5013	08c8c03500b000000360ccc000000000002
2024-04-03 17:55:24.899142	10.57.64.223	10.57.64.220	58680	5013	08c8c03600b000000370ccc000000000002
2024-04-03 17:55:27.814349	10.57.64.223	10.57.64.220	58680	5013	08c8c03700b000000380ccc000000000002
2024-04-03 17:55:29.982779	10.57.64.223	10.57.64.220	39938	5111	07e9012300a00120008001f4021c7b057fa3edc149cb55150763a241

Choose Attack

CMD Injection Replay Packet Change Packet

Anytime this packet is seen... send this packet instead Number of times to change the packet (type 999 to change continuous packets)

Packet to Change New Packet Number of times to change the packet

Launch Change Attack Stop Change Attack

Or

Anytime a packet starts with... send this packet Number of times to change the packet (type 999 to change continuous packets)

08c8 0000340ccc000000000002 999

Launch Change Attack Stop Change Attack

SPARTA TTPs: DE-0002.01 Change Attack Stopped

VIEW COS

- PACKET_TIMEFORMATTED *
- RECEIVED_TIMESECONDS *
- RECEIVED_TIMEFORMATTED *
- RECEIVED_COUNT *
- CCSDS_STREAMID
- CCSDS_SEQ_FLAGS
- CCSDS_SEQ_COUNT
- CCSDS_LENGTH
- CCSDS_SECONDS
- CCSDS_SUBSECS
- CCSDS_SPARE
- COMMANDERRORCOUNT
- COMMANDCOUNT

2

Rows per page: 1000 1-14 of 14

```
B Axes  
N Grid  
L Grid  
F Grid  
B Grid  
Gal Grid  
FOVs
```

```
(Slot 1). Disabling  
state = 1  
output enabled for IP 127.0.  
firstID=3, LastID=64, Modifie  
command received  
command received  
enabled  
new state = 1  
completed  
Id 0x1940, pipe ADCS_CMD_PIP
```

Scenario #1 – No SDLS (cont.)

Monitoring the traffic, you see a Camera NOOP go to the SV; what if we change it the next time and every time moving forward?

Show 10 entries Search: 6012

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
2024-04-03 17:27:39.734085	10.57.64.223	10.57.64.220	39064	5111	07e90123000a00120008002040309eb8b5feffbc14cf27092503750414
2024-04-03 17:28:01.161959	10.57.64.220	10.57.64.223	53609	6012	18c8c00000010000

```
NOS3 Flight Software
EVS Port1 42/1/FM 89: Child Task initialization complete
EVS Port1 42/1/RW 1: GENERIC_RW App Initialized. Version: 2000-001-00:00:00.65000 CFE_ES_Main: CFE_ES_Main entered
2000-001-00:00:00.65000 CFE_ES_Main: CFE_ES_Main entered
EVS Port1 42/1/CFE_TIME 21: Stop FLYWHEEL
EVS Port1 42/1/SC 73: RTS Number 001 Started
EVS Port1 42/1/SCH 21: Major Frame Sync too noisy (Slot 1)
EVS Port1 42/1/DS 35: APP STATE command: state = 1
EVS Port1 42/1/TO_LAB_APP 3: TO telemetry output enabled
EVS Port1 42/1/SC 121: Enable RTS group: FirstID=3, LastID=3
EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received
EVS Port1 42/1/SAMPLE 13: SAMPLE: Enable command received
EVS Port1 42/1/SAMPLE 14: SAMPLE: Device enabled
EVS Port1 42/1/SC 86: RTS 001 Execution Completed
EVS Port1 42/1/LC 28: Set LC state command: new state = 1
EVS Port1 42/1/RADIO 31: GENERIC_RADIO: Request device
```

Select Packet
CAM_NOOP_CC
Camera NOOP Command
SEND

EVS Port1 42/1/CAM 3: CAM App: NOOP command

Scenario #1 – No SDLS (cont.)

MitM every time a CAM_NOOP_CC goes across the wire and change it to a CFS ES NOOP

entries Search: 6012

amp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
4-03 9.734085	10.57.64.223	10.57.64.220	39064	5111	07e90123000a00120008002040309eb8b5feffbc14cf27092503750414
4-03 1.161959	10.57.64.220	10.57.64.223	53609	6012	18c8c00000010000

Choose Attack

CMD Injection Replay Packet **Change Packet**

Anytime this packet is seen... ...send this packet instead Number of times to change the packet (type 999 to change continuous p

18c8c00000010000 1806c00000010000 999

Launch Change Attack **Stop Change Attack**

Or

Anytime a packet starts with... ...send this packet Number of times to change the packet (type 999 to change continuous p

Packet to Change New Packet Number of times to change the packet

Launch Change Attack **Stop Change Attack**

DE

COSMOS Command Sender

Scope: DEFAULT

Select Packet: **CAM_NOOP_CC** **SEND**

Camera NOOP Command

ARDUCAM CAM_NOOP_CC") sent.

Command History: (Pressing Enter on the line re-executes the command)

```
ARDUCAM CAM_NOOP_CC" )
```

times to change the packet (type 999 to change continuous packets)

times to change the packet (type 999 to change continuous packets)

times to change the packet

```
EVs Port1 42/1/30-001-MS-001 Execution completed
Re EVs Port1 42/1/LC 28: Set LC state command: new state = 1
Range
In Su
EVs Port1 42/1/CAM 3: CAM App: NOOP command
```


Scenario #1 – No SDLS (cont.)

Can do everything you can do, but better with Rogue Ground Station

Find the command database and load it into the tool

Deploy commands as a normal operator

The image shows a composite screenshot of a Kali Linux environment. On the left, the 'COSMOS CmdTlmServer' web interface is open in a browser. It displays two active interfaces: 'DEBUG' and 'SIM_42_TRUTH_INT', both in a 'CONNECTED' state. Below the interface list, there is a 'Log Messages II' section showing several 'CRITICAL' log entries from 'DEFAULT_INTERFACE_DEBUG' regarding packet length mismatches.

On the right, a 'SPACE Invader' browser window shows a packet capture tool interface. It displays a table of captured packets with columns for time, source IP, destination IP, source port, destination port, and protocol. Below the table, there are tabs for different attack types: 'CMD Injection', 'Replay Packet', 'Change Packet', 'Jamming Attack', 'Flooding Attack', and 'HAVOC'. An 'Upload Command/Telemetry Database' dialog is open, showing an 'Upload' button and a 'Select Database' dropdown menu. Below the dialog, there is a 'Send Raw CMD' button and a 'Choose CMD' button.

At the bottom right, a terminal window displays system logs and telemetry data, including messages like 'TO Lab Initialized. TO Lab DEVELOPMENT BUILD v2.5.0' and 'APP STATE command: state = 1'.

Scenario #2 – With SDLS Using Only Encryption

SPARTA TTP: IA-0008.01

Stop Attack Start Packet Show

SPARTA TTPs: EXF-0003, EXF-0003.01, EXF-0003.02

Show 10 entries Search: 6012

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
2024-04-03 18:07:07.912764	10.57.64.223	10.57.64.220	46384	5013	0941c10123e4040c070b8bc8a7efa19feaed6997dd0088561d624a4edf
2024-04-03 18:07:13.169922	10.57.64.223	10.57.64.220	46384	5013	0941c1012319409eeda4a4f5dab96e5046ca1bbdb80017688f01de919a
2024-04-03 18:07:19.767392	10.57.64.223	10.57.64.220	46384	5013	0945c101234b6a52f99ee01d3655b33b1ade454485069c3960ec1f38fb
2024-04-03 18:07:20.948860	10.57.64.220	10.57.64.223	57616	6012	18c8c001231fd877f40823b0e3f2954afe4adb669e06795e79d071144e

Showing 21 to 24 of 24 entries (filtered from 1,530 total entries)

Data looks different now...

MODE

COSMOS Command Sender

Scope: DEFAULT

Select Packet: CAM_NOOP_CC

SEND

Camera NOOP Command

ARDUCAM CAM_NOOP_CC") sent.

Command History: (Pressing Enter on the line re-executes the command)

"ARDUCAM CAM_NOOP_CC")

UTC 2

TRACK Fixed Bore Up

EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received

EVS Port1 42/1/SAMPLE 13: SAMPLE: Enable command received

EVS Port1 42/1/SAMPLE 14: SAMPLE: Device enabled

EVS Port1 42/1/SC 86: RTS 001 Execution Completed

EVS Port1 42/1/LC 28: Set LC state command: new state = 1

EVS Port1 42/1/CAM 3: CAM App: NOOP command

Range In Su

N A

L A

F Axes

B Axes

N Grid

L Grid

F Grid

B Grid

Gal Grid

EDVs

Scenario #2 – With SDLS Using Only Encryption

Replay Attack Still in Play!!

Without sequencing, command counters, authentication of some sort – replay attacks will still work

Showing 21 to 24 of 24 entries (filtered from 1,530 total entries) Previous 1 2 3 Next

Choose Attack

CMD Injection **Replay Packet** Change Packet

Hex Packet to Replay	Destination IP	Source IP	Destination Port	Source Port
114f4ef47a4525c63ac0569	10.57.64.223	10.57.64.220	6012	56666

Number of times to replay packet (type 999 to send continuous packets)

10

Launch Replay Attack Stop Replay Attack

SPARTA TTPs: [EX-0001.01](#)

```
B Axes
N Grid
L Grid
F Grid
B Grid
Gal Grid
EQVs
```

request device HK reported error

Scenario #3 – With SDLS Using Encryption & Authentication

None of the Previous Attacks Work 😞

Attempt to perform command injection, replay, etc. – nothing works

The screenshot displays the COSMOS Command Sender application interface. At the top, the title bar reads "COSMOS Command Sender" and "Scope DEFAULT". Below the title bar, there is a "Select Packet" dropdown menu set to "CAM_NOOP_CC" and a prominent blue "SEND" button. The interface also shows a "Command History" section with the text "(ARDUCAM CAM_NOOP_CC)" and a terminal window at the bottom right containing a list of grid coordinates: B Axes, N Grid, L Grid, F Grid, B Grid, Gal Grid, and F0Vs. A semi-transparent window in the background shows "Destination Port" (6012) and "Source Port" (5666) fields. The background of the application is a dark space-themed image with a starry sky and a planet's horizon.

Techniques Used >>> SPARTA Countermeasures

<https://sparta.aerospace.org/countermeasures/SPARTA>

Replay

Threat actors recording previously recorded data streams and then resending them at a later time. This attack can be used to fingerprint systems, gain elevated privileges, or even cause a denial of service.

ID: EX-0001

Sub-techniques: EX-0001.01 | EX-0001.02

Notional Risk (H | M | L): 25 | 24 | 21

Related Aerospace Threat IDs: SV-AC-1 | SV-AC-2

Related MITRE ATT&CK TTPs: T0831

Related ESA SPACE-SHIELD TTPs: T2008.006 | T2019.005

Tactic: Execution

Home > Techniques > Eavesdropping

Eavesdropping

Threat actors may seek to capture network communications throughout the ground station and communication channel (i.e. radio frequency, optical) used for uplink and downlink communications.

Subtechniques (2)

ID: EXF-0003

Sub-techniques: EXF-0003.01 | EXF-0003.02

Notional Risk (H | M | L): 23 | 22 | 19

Related Aerospace Threat IDs: SV-AC-7 | SV-CF-1 | SV-CF-2

Related MITRE ATT&CK TTPs: No related MITRE ATT&CK TTPs

Related ESA SPACE-SHIELD TTPs: T2042 | T2042.001 | T1557 | T1557.001 | T2018.001 | T2018.002 | T2018.003 | T2015.003

Tactic: Exfiltration

Created: 2022/10/19

Home > Techniques > Prevent Downlink > Inhibit Ground System Functionality

Prevent Downlink: Inhibit Ground System Functionality

Threat actors may utilize ground-system presence to inhibit the ground system software's ability to process (or display) telemetry, effectively leaving ground controllers unaware of vehicle activity during this time. Telemetry is the only method in which ground controllers can monitor the health and stability of the spacecraft while in orbit. By disabling this downlink, threat actors may be able to stop mitigations from taking place.

Other Subtechniques of Prevent Downlink (3)

ID: DE-0002.01

Sub-technique of: DE-0002

Notional Risk (H | M | L): 21

Related Aerospace Threat IDs: No related Aerospace Threat IDs

Related MITRE ATT&CK TTPs: No related MITRE ATT&CK TTPs

Related ESA SPACE-SHIELD TTPs: No related ESA SPACE-SHIELD TTPs

Tactic: Defense Evasion

Created: 2022/10/19

Last Modified: 2024/02/29

Home > External Entity > Rogue Ground Station

External Entity: Rogue Ground Station

Threat actors may attempt to access a victim spacecraft through the use of a rogue ground system. With this technique, the threat actor does not need access to a legitimate ground station or communication site.

Subtechniques of Rogue External Entity (3)

Countermeasures

ID	Name	Description
CM0002	COMSEC	A component of cyber telecommunications. It is imperative to utilize secure communication protocols with strong cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission. Systems should also maintain the confidentiality and integrity of information during preparation for transmission and during reception. Spacecraft should not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). The cryptographic mechanisms should identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
CM0073	Traffic Flow Analysis	Utilizing techniques to adversary inferences.

Countermeasures

ID	Name	Description	NIST Rev5	D3FEND
CM0002	COMSEC	A component of cybersecurity to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. It is imperative to utilize secure communication protocols with strong cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission. Systems should also maintain the confidentiality and integrity of information during preparation for transmission and during reception. Spacecraft should not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). The cryptographic mechanisms should identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	AC-17 AC-17(1) AC-17(10) AC-17(10) AC-17(2) AC-18 AC-18(1) AC-2(11) AC-3(10) CA-3 IA-4(9) IA-5 IA-5(7) IA-7 PL-8 PL-8(1) SA-8(18) SA-8(19) SA-9(6) SC-10 SC-12 SC-12(1) SC-12(2) SC-12(3) SC-12(6) SC-13 SC-16(3) SC-28(1) SC-28(3) SC-7 SC-7(10) SC-7(11) SC-7(18) SC-7(5) SC-8(1) SC-8(3) SI-10 SI-10(3) SI-10(5) SI-10(6) SI-19(4) SI-3(8)	D3-ET D3-MH D3-MAN D3-MENCR D3-NTF D3-ITF D3-OTF D3-CH D3-DTP D3-NTA D3-CAA D3-DNSTA D3-IPCTA D3-NTCD D3-RTS D3-PHDURA D3-PMAD D3-

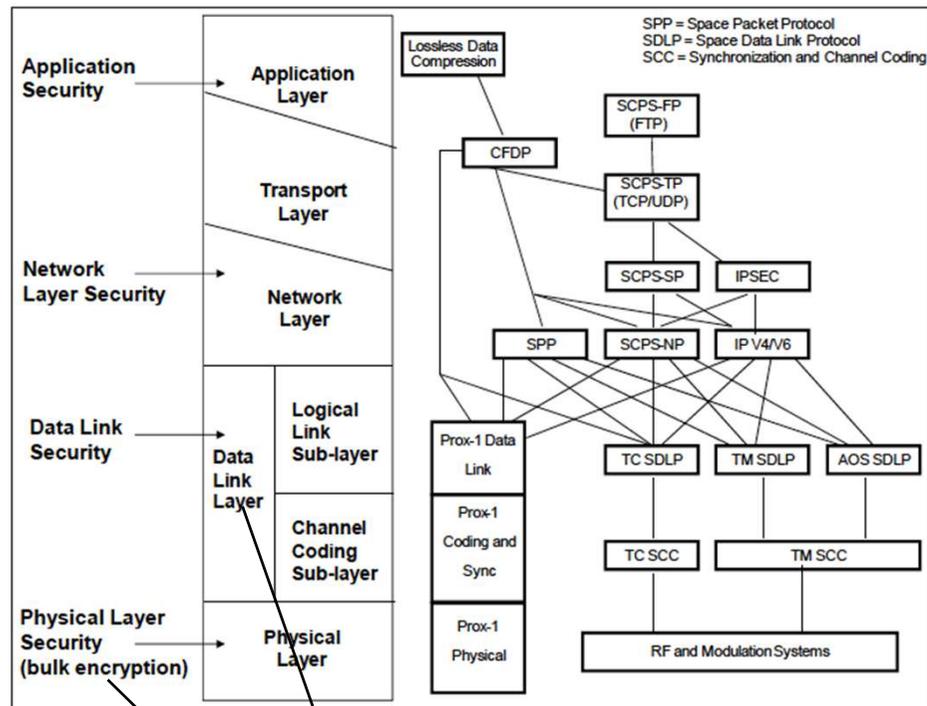
Summary

Both is Good – Both is Better!!!

According to [SPARTA Notional Risk Scores](#)

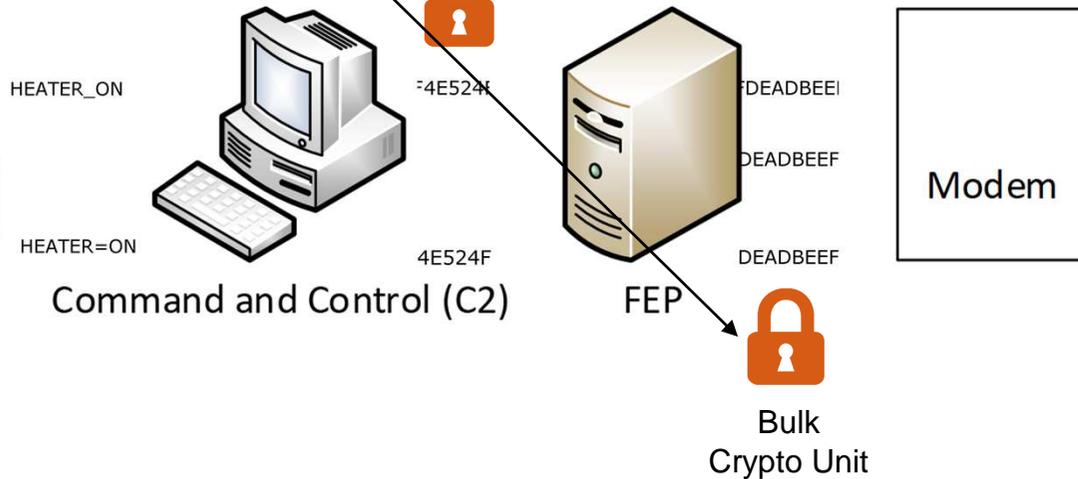
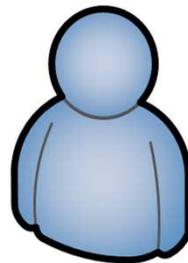
Compromised ground is one of the highest risks to the SV

SPARTA Techniques/Sub-Techniques	Notional Risk (HIGH Criticality Systems)
IA-0004.01 - Ground Station	25
IA-0008.01 - Rogue Ground Station	25
PER-0003 - Ground System Presence	25
EXF-0007 - Compromised Ground System	25
IA-0007 - Compromise Ground System	24

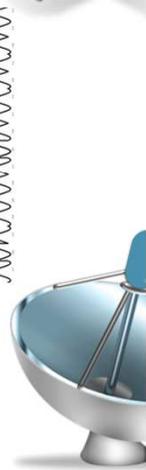


Adding defense-in-depth is key!!!

- If using CCSDS (TC/TM/AOS) [SDLS](#) improves security immensely and mitigates many known TTPs
 - [SDLS Extended Procedures](#) are also available



The purpose of this Recommended Standard is to specify the Space Data Link Security (SDLS) Protocol Extended Procedures (EP). It defines the Key Management, Security Association Management, SDLS Monitoring and Control Services, and data structures required to operate the SDLS protocol over a space link. Further, it defines the interfaces and required data structures for proper interaction with the Space Data Link (SDL) protocols and security function status reporting mechanism.



<https://sparta.aerospace.org>



Space Attack Research & Tactic Analysis (SPARTA)

show sub-techniques | hide sub-techniques

Reconnaissance 9 techniques	Resource Development 5 techniques	Initial Access 12 techniques	Execution 18 techniques	Persistence 5 techniques	Defense Evasion 11 techniques	Lateral Movement 7 techniques	Exfiltration 10 techniques	Impact 6 techniques
Gather Spacecraft Design Information (1)	Acquire Infrastructure (4)	Compromise Supply Chain (2)	Replay (2)	Memory Compromise (2)	Disable Fault Management (2)	Hosted Payload (2)	Replay (2)	Reception (or Misdirection) (2)
Gather Spacecraft Descriptors (2)	Compromise Infrastructure (2)	Compromise Software Defined Radio (2)	Position, Navigation, and Timing (PNT) Geofencing (2)	Backdoor (2)	Prevent Downlink (2)	Exploit Lack of Bus Segregation (2)	Side-Channel Attack (2)	Disruption (2)
Gather Spacecraft Communications Information (2)	Obtain Cyber Capabilities (2)	Crosslink via Compromised Neighbor (2)	Crosslink via Compromised Neighbor (2)	Ground System Presence (2)	Modify On-Board Values (2)	Constellation Hopping via Crosslink (2)	Eavesdropping (2)	Denial (2)
Gather Launch Information (2)	Obtain Non-Cyber Capabilities (2)	Secondary/Backup Communication Channel (2)	Compromise Boot Memory (2)	Replace Cryptographic Keys (2)	Masquerading (2)	Visiting Vehicle Interface (2)	Out-of-Band Communications Link (2)	Degradation (2)
Eavesdropping (2)	Stage Capabilities (2)	Rendezvous & Proximity Operations (2)	Exploit Hardware/Firmware Corruption (2)	Valid Credentials (2)	Exploit Reduced Protections During Safe-Mode (2)	Virtualization Escape (2)	Proximity Operations (2)	Destruction (2)
Gather FSW Development Information (2)	Compromise Hosted Payload (2)	Compromise Hosted Payload (2)	Disable/Bypass Encryption (2)		Modify Whitelist (2)	Launch Vehicle Interface (2)	Modify Communications Configuration (2)	Theft (2)
Monitor for Safe-Mode Indicators (2)	Compromise Ground System (2)	Compromise Ground System (2)	Trigger Single Event Upset (2)		Rootkit (2)	Valid Credentials (2)	Compromised Ground System (2)	
Gather Supply Chain Information (2)	Rogue External Entity (2)	Rogue External Entity (2)	Time Synchronized Execution (2)		Camouflage, Concealment, and Decoy (CCD) (2)		Compromised Developer Site (2)	
Gather Mission Information (2)	Trusted Relationship (2)	Trusted Relationship (2)	Exploit Code Flaws (2)		Overflow Audit Log (2)		Compromised Partner Site (2)	
	Exploit Reduced Protections During Safe-Mode (2)	Exploit Reduced Protections During Safe-Mode (2)	Malicious Code (2)		Valid Credentials (2)		Payload Communication Channel (2)	
	Auxiliary Device Compromise (2)	Auxiliary Device Compromise (2)	Exploit Reduced Protections During Safe-Mode (2)					
	Assembly, Test, and Launch Operation Compromise (2)	Assembly, Test, and Launch Operation Compromise (2)	Modify On-Board Values (2)					
			Flooding (2)					
			Jamming (2)					
			SpooFing (2)					
			Side-Channel Attack (2)					
			Kinetic Physical Attack (2)					
			Non-Kinetic Physical Attack (2)					

Popular Media Links:

- <https://cyberscoop.com/space-satellite-cybersecurity-sparta/>
- <https://www.darkreading.com/ics-ot/space-race-defenses-satellite-operations-attacks>
- <https://thecyberwire.com/podcasts/daily-podcast/1715/notes> &
- <https://thecyberwire.com/newsletters/signals-and-space/6/21>

Overview Briefings:

- [Using SPARTA to Conduct Space Vehicle Cyber Assessments](#) (February 2024)
- [DEF CON 31: Building Space Attack Chains using SPARTA](#) (August 2023)
- [Hacking Spacecraft using Space Attack Research & Tactic Analysis | Video](#) (April 2023)
- [In-depth Overview - Space Attack Research & Tactic Analysis](#) (November 2022)

SPARTA Links:

- Getting Started with SPARTA: <https://sparta.aerospace.org/resources/getting-started> | <https://sparta.aerospace.org/resources/understanding-space-cyber-ttps-with-the-sparta-matrix>
- Understanding Space-Cyber TTPs with the SPARTA Matrix: <https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix>
- Leveraging the SPARTA Matrix: <https://aerospace.org/article/leveraging-sparta-matrix>
- Use Case w/ PCspooF:
 - <https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c>
 - <https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed>
- FAQ: <https://sparta.aerospace.org/resources/faq>
- Matrix: <https://sparta.aerospace.org>
- Navigator: <https://sparta.aerospace.org/navigator> | Countermeasure Mapper: <https://sparta.aerospace.org/countermeasures/mapper>
- Notional Risk Scores on 5x5: <https://sparta.aerospace.org/notional-risk-scores>
- Related Work: <https://sparta.aerospace.org/related-work/did-space> with ties into [TOR 2021-01333 REV A](#)

Other Papers and Resources

CYSAT '23:

<https://www.youtube.com/watch?v=l9nezXxO3iE>



<https://sparta.aerospace.org/resources/>

DEF CON Presentations:

- [DEF CON 2020: Exploiting Spacecraft](#)
- [DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities](#)
- [DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins](#)
- [DEF CON 2023: Building Space Attack Chains using SPARTA](#)



AEROSPACE
VILLAGE

Papers/Articles: <https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368>

- 2019: [Defending Spacecraft in the Cyber Domain](#)
- 2020: [Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices](#)
- 2021: [Cybersecurity Protections for Spacecraft: A Threat Based Approach](#)
- 2021: [The Value of Space](#)
- 2021: [Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles](#)
- 2022: [Protecting Space Systems from Cyber Attack](#)
- 2022: [An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action](#)

July 2022 Testimony: Space and Aeronautics Subcommittee Hearing - Exploring Cyber Space: Cybersecurity for Civil and Commercial Space Systems

- Video: <https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964>
- Written Testimony: https://republicans-science.house.gov/_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf

