



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@ae
240.521.4

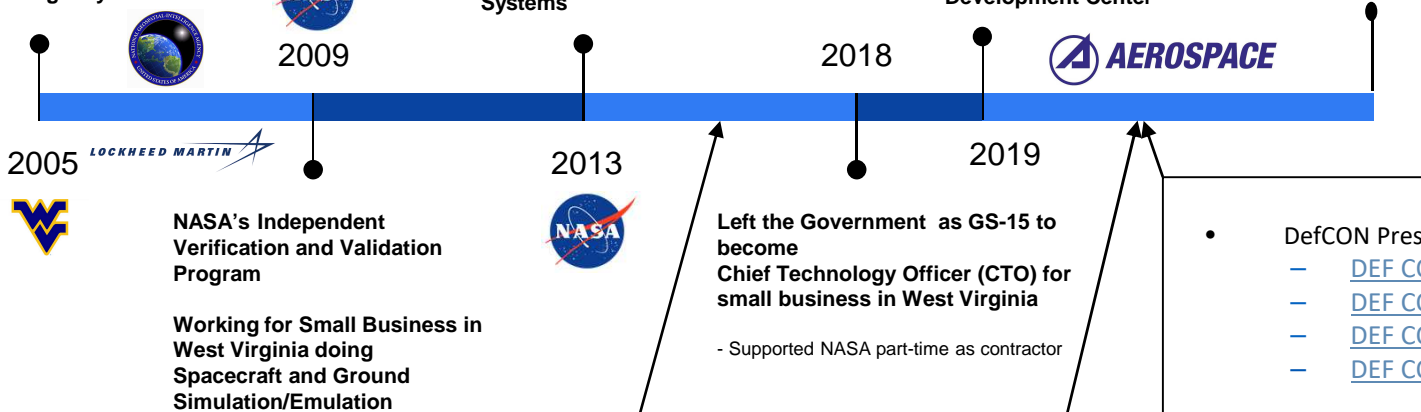
Andon Bailey

Current Job: Principal Engineer, Cybersecurity and Advanced Platforms Subdivision (CAPS), at The Aerospace Corporation

- Developing cyber labs for training, perform penetration testing & vulnerability assessments {Ethical Hacking!}
- Performing cybersecurity research on ground systems and spacecraft systems to better position the federal government with respect to protection of our critical space infrastructure.

Electrical Engineering
University of Virginia

Lockheed Martin Supporting
Geospatial
Space Agency



Tested / "Ethically Hacked" Space Systems

2013-2024

Mars' Rovers (MER & MSL) & Deep Space Network (DSN) at JPL
Hubble Space Telescope (HST) at GSFC
Closed IONet (CIONet) within NASCOM at GSFC
Space Network (SN) at the White Sands Complex (WSC)
KSC Ground Systems Development and Operations (GSDO) Kennedy Ground Control System (KGCS) and Launch Control System (LCS)
James Webb Space Telescope (JWST) Ground System at the Space Telescope Science Institute (STScI) in Baltimore
Huntsville Operations Support Center (HOSC) at Marshall Space Flight Center
Near Earth Network (NEN) at Wallops Flight Facility
ISS Mission Control Center (MCC) at Johnson Space Center
Wind tunnels at Glenn Research Center
Hypersonic Environment at Langley Research Center
NOAA's Joint Polar Satellite System (JPSS)

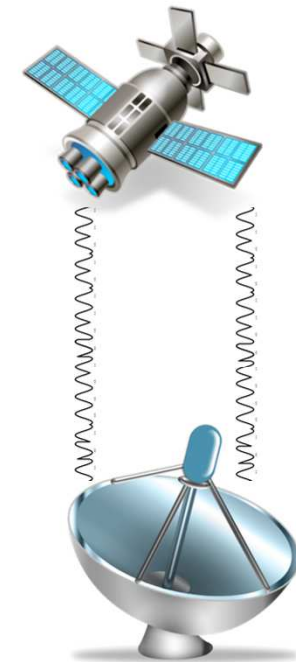
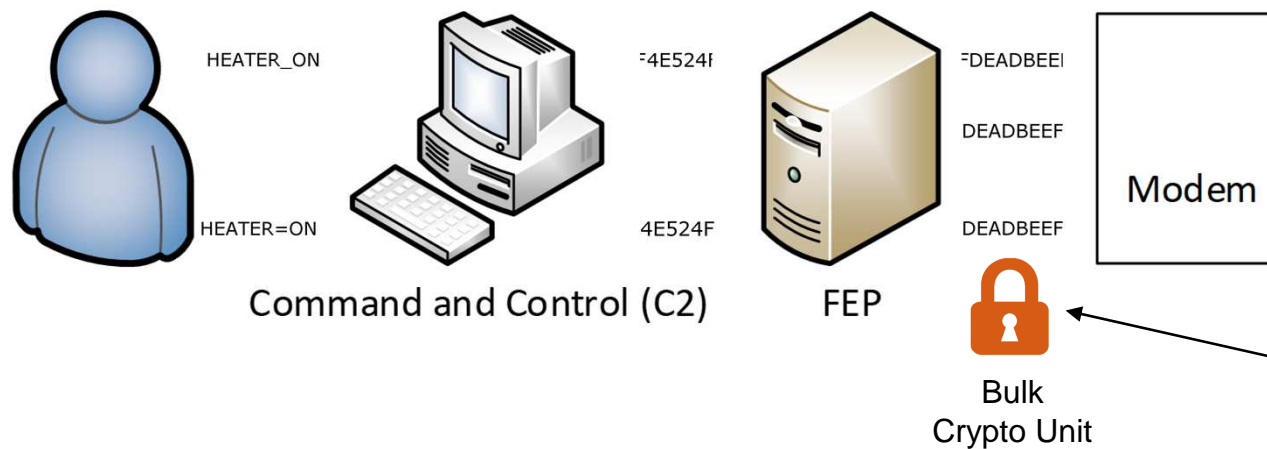
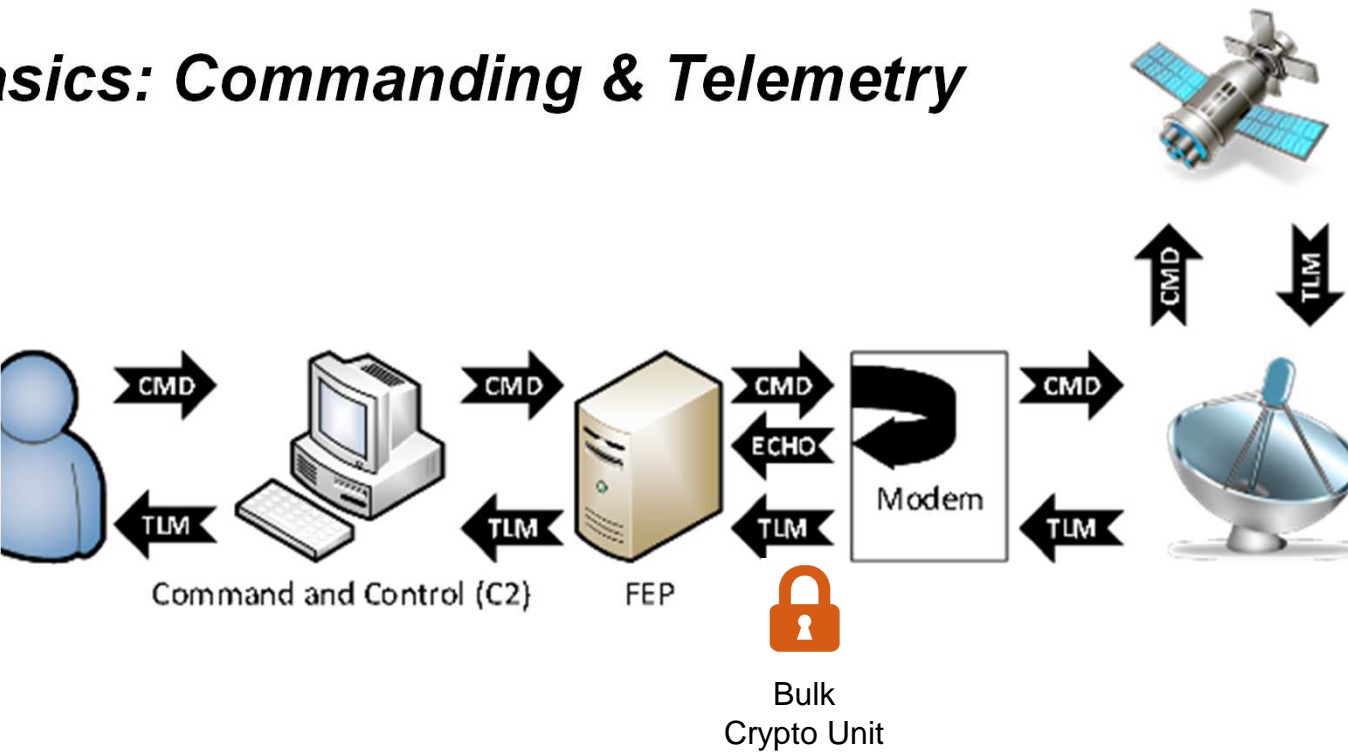


NASA's Exceptional Service Medal (2019) for "groundbreaking" cyber work

- DefCON 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](#)
- Papers/Articles:
 - 2019: [Defending Spacecraft in the Cyber Domain](#)
 - 2020: [Establishing Space Cybersecurity Policy, Standards, & Risk Management](#)
 - 2021: [Cybersecurity Protections for Spacecraft: A Threat Based Approach](#)
 - 2021: [Translating Space Cybersecurity Policy into Actionable Guidance for Space Vendors](#)
 - 2022: [Protecting Space Systems from Cyber Attack](#)
- July 2022 Congressional Testimony:
 - Video: <https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964>
 - Written Testimony: <https://republicans-science.house.gov/cache/files/2/9/290176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.20220727090000/bailey-testimony.pdf>
- SPARTA Launched
 - <https://sparta.aerospace.org>



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

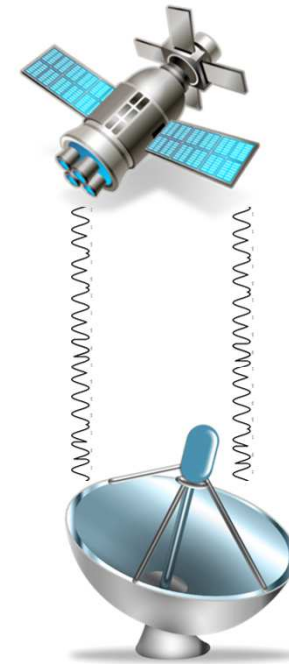
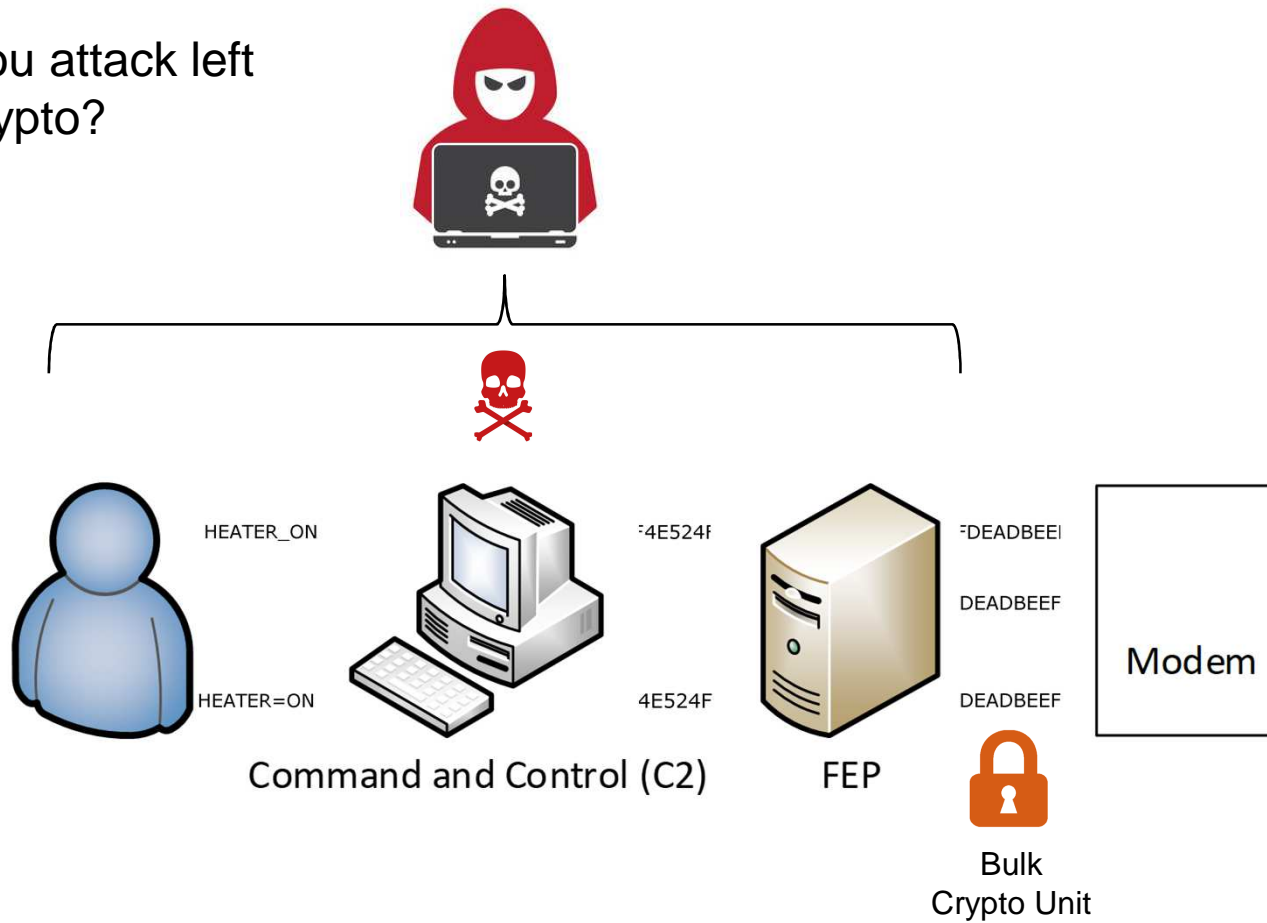
- *Manage cryptographic keys used for encryption and decryption. They generate, store, distribute, and update encryption keys securely to ensure the confidentiality and integrity of communications. Key management practices include key generation, key distribution, key rotation, and key revocation.*

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....?

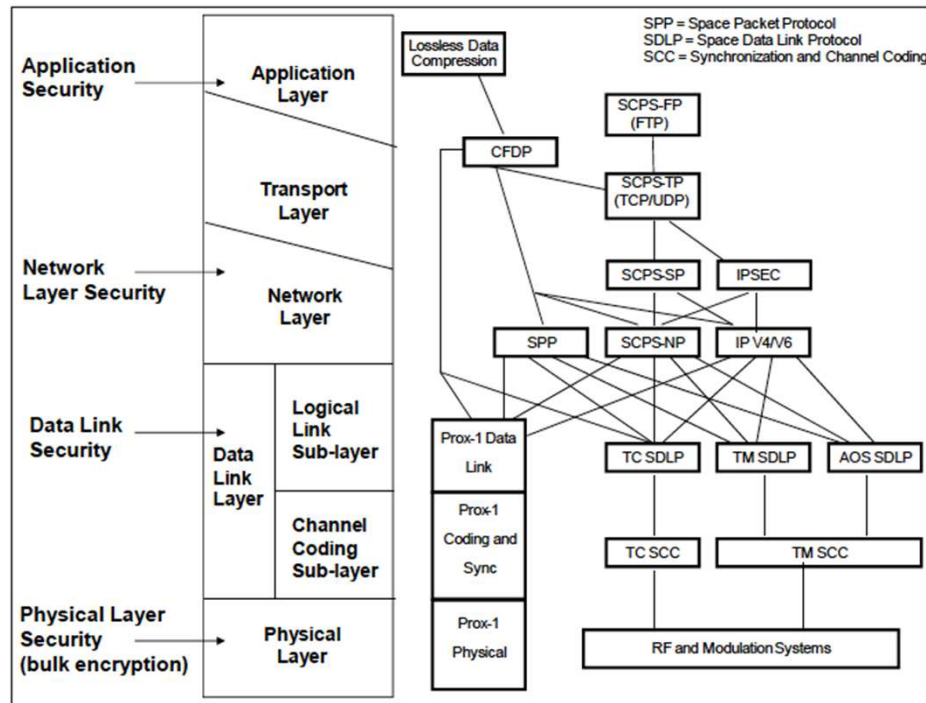
What if you attack left
of bulk crypto?



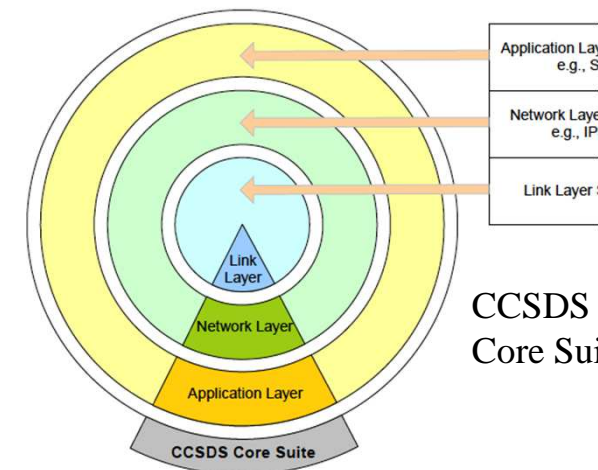
Space Systems Protocol Overview

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

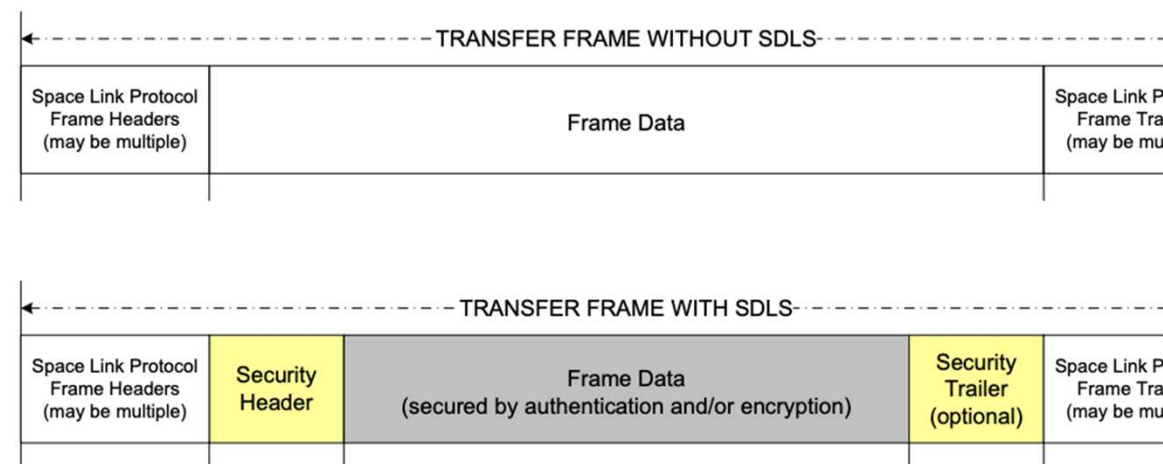
- Protocols are created by the Consultative Committee for Space Data Systems ([CCSDS](https://public.ccsds.org/))
- These are recommendations – they are not legally binding
- Protocols exist to allow for collaboration between international agencies
- Some protocol differences between commands and telemetry



CCSDS Space Mission Protocols and Security Options

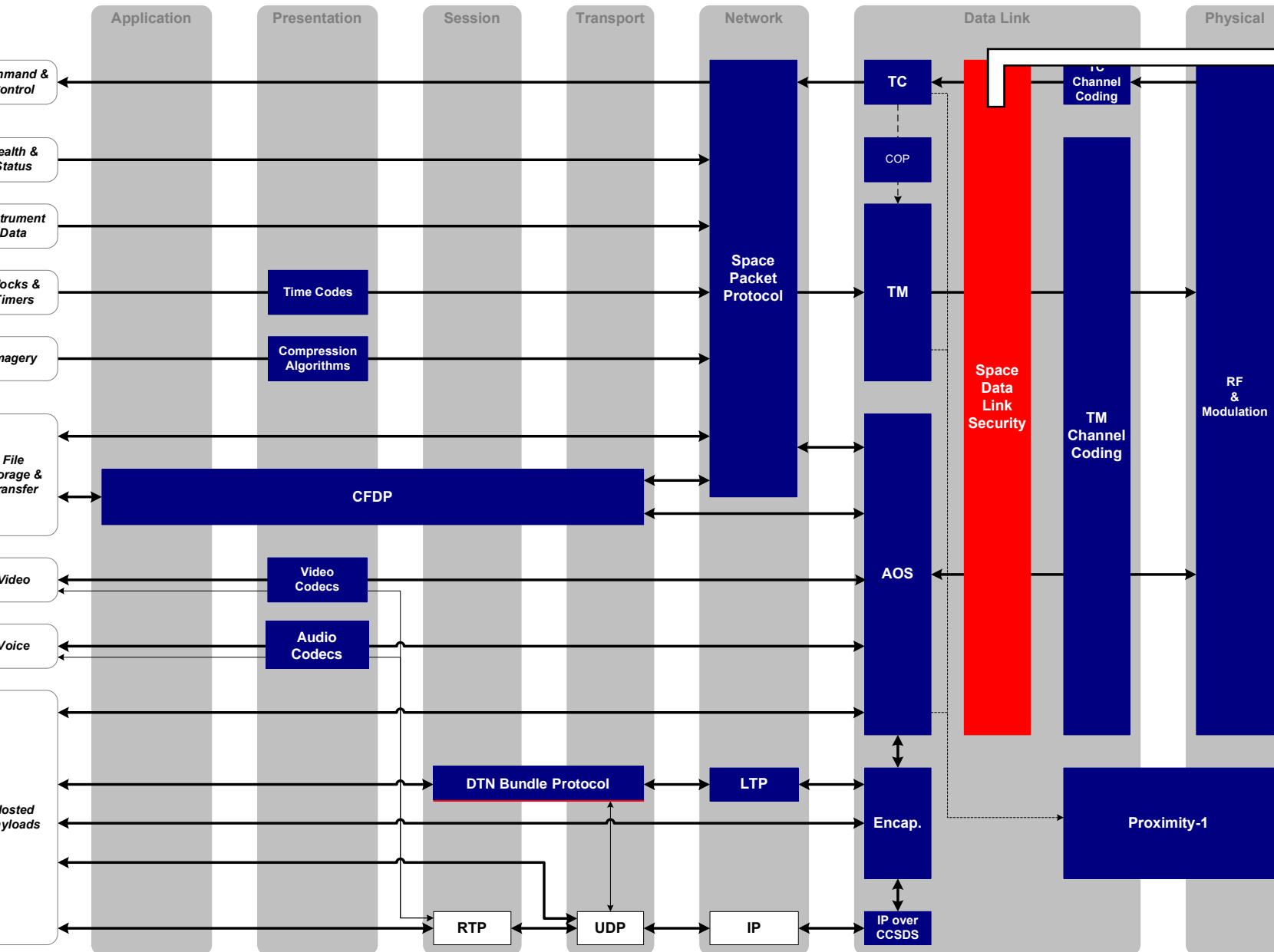


CCSDS Core Suite



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

Space-to-Ground: OSI Stack View for CCSDS



Can support encryption and authentication

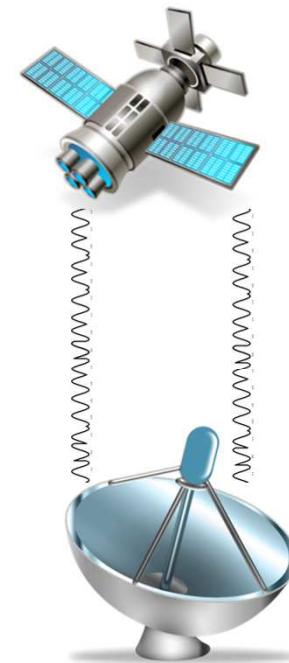
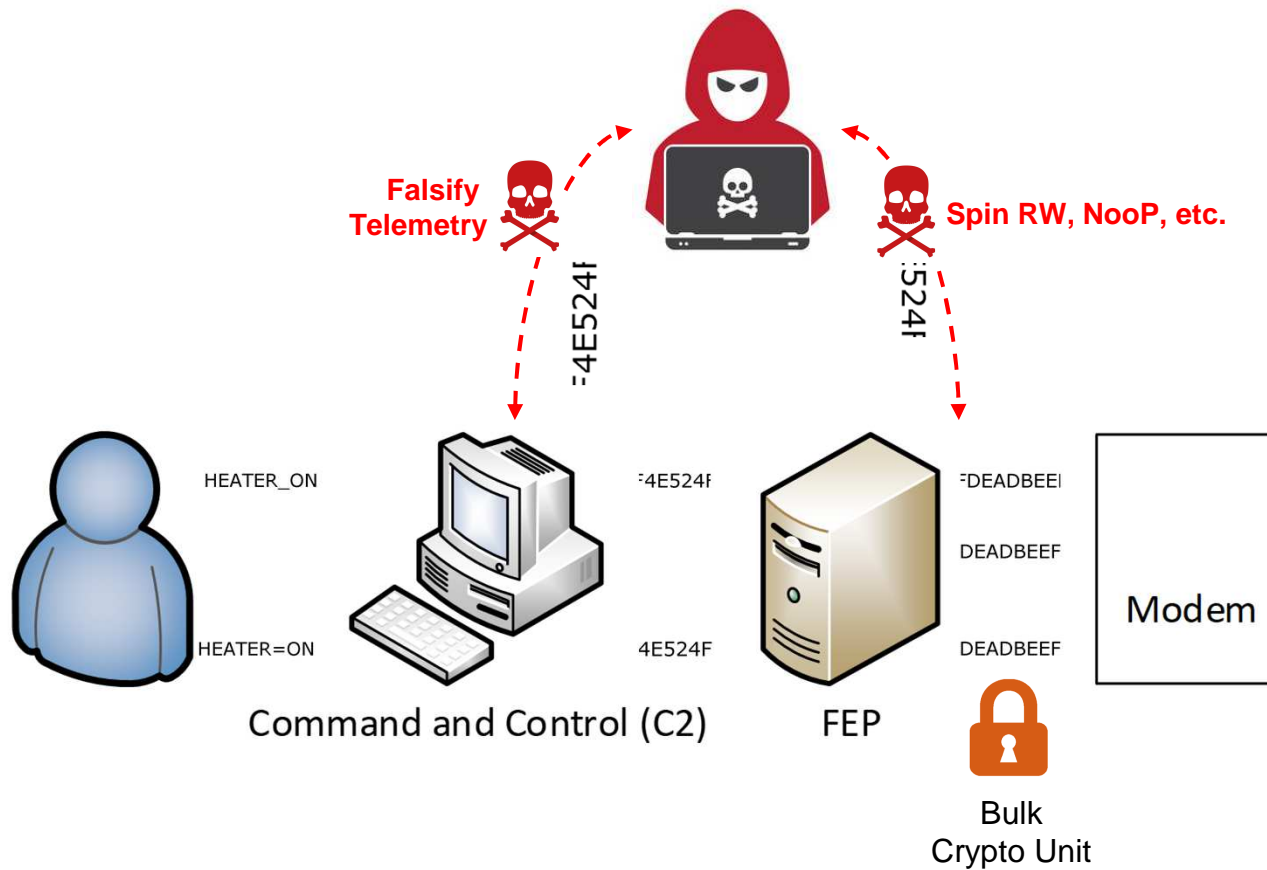
Demo will show why you must do both!!!

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

performing the MitM



SPARTA Cyber Exploiter (SPACE) Invader

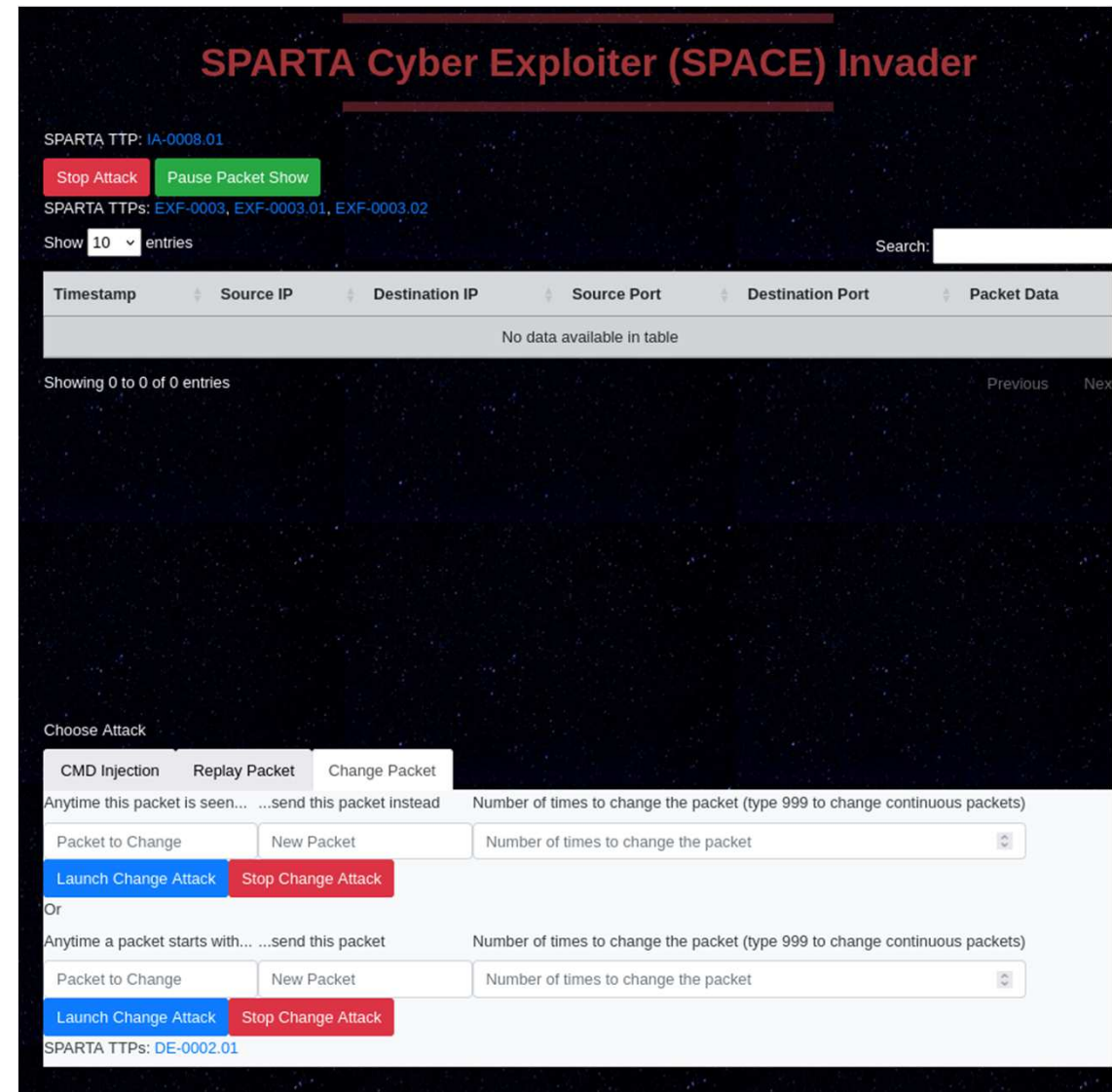
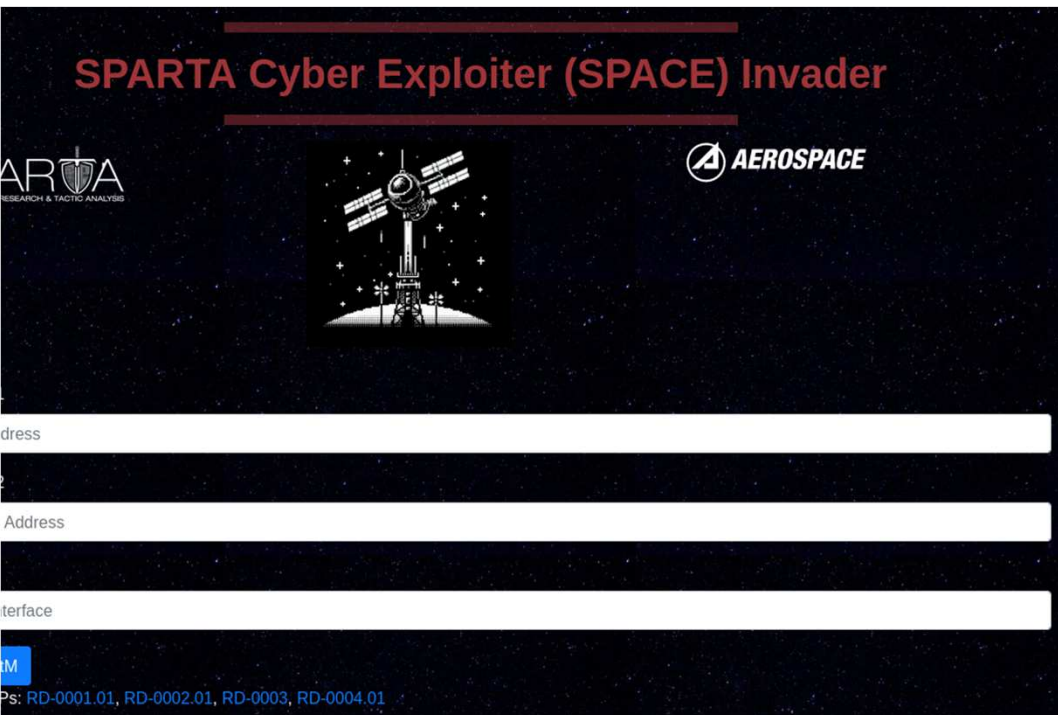


SPACE Invader

M 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



Types of attacks available (for now)

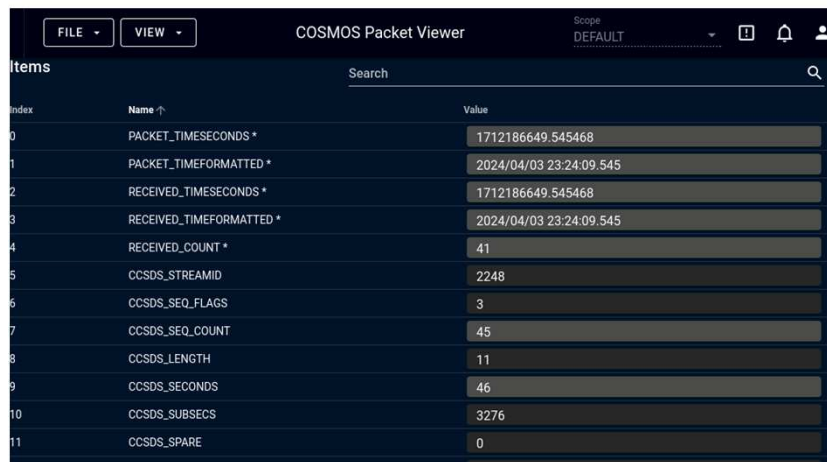
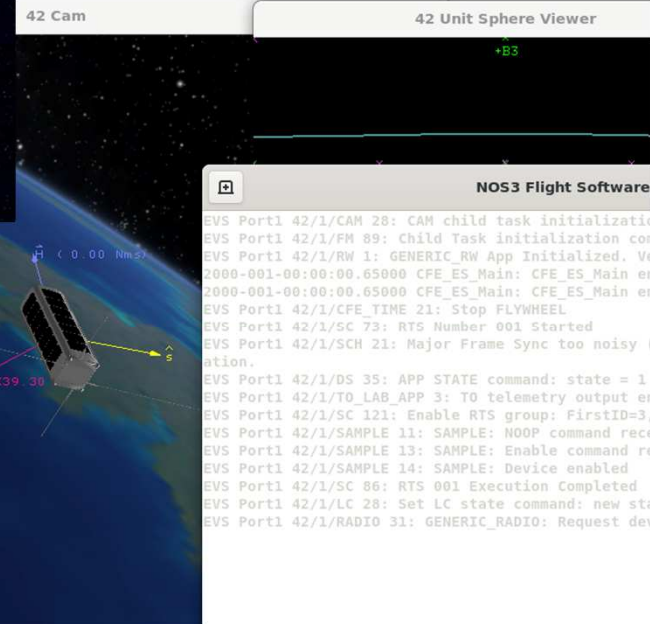
Falsify telemetry

Ability to send commands

Flooding

Rogue Flight Application

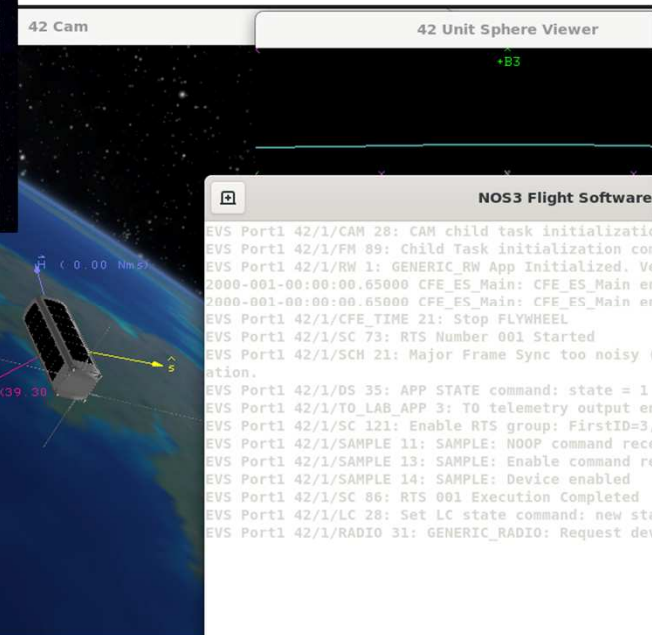
Etc.



No Time!!!

<https://github.com/nasa/nos>

- Exfiltrating data
- Falsify telemetry
- Ability to replay commands
- Ability to send commands
- Etc.



Scenario #1 – No SDLS (cont.)

Simplify 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

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

2024-04-03 17:55:27.814349	10.57.64.223	10.57.64.220	58680		
2024-04-03 17:55:29.982779	10.57.64.223	10.57.64.220	39938	5111	07e90123000a00120008001f4021c7b057ffa3edc149cb55150763a241

CMD Injection

Replay Packet

Change Packet

Anytime this packet is seen... send this packet instead

Packet to Change

New Packet

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

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-0002.01Change Attack Stopped

2

Rows per page: 1000 1-14 of 14

B Axes
N Grid
L Grid
F Grid
B Grid
Gal Grid
ENVs

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	08c8c033000b000000340ccc000000000002
2024-04-03 17:55:19.495495	10.57.64.223	10.57.64.220	58680	5013	08c8c034000b000000350ccc000000000002
2024-04-03 17:55:22.525246	10.57.64.223	10.57.64.220	58680	5013	08c8c035000b000000360ccc000000000002
2024-04-03 17:55:24.899142	10.57.64.223	10.57.64.220	58680	5013	08c8c036000b000000370ccc000000000002
2024-04-03 17:55:27.814349	10.57.64.223	10.57.64.220	58680	5013	08c8c037000b000000380ccc000000000002
2024-04-03 17:55:29.982779	10.57.64.223	10.57.64.220	39938	5111	07e90123000a00120008001f4021c7b057ffa3edc149cb55150763a241

CMD Injection

Replay Packet

Change Packet

Anytime this packet is seen... send this packet instead

Packet to Change

New Packet

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

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-0002.01Change Attack Stopped

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

Select Packet
CAM_NOOP_CC

Camera NOOP Command

SEND

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 enter
2000-001-00:00:00.65000 CFE_ES_Main: CFE_ES_Main enter
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
ation.
EVS Port1 42/1/DS 35: APP STATE command: state = 1
EVS Port1 42/1/TO_LAB_APP 3: TO telemetry output enable
EVS Port1 42/1/SC 121: Enable RTS group: FirstID=3, Las
EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received
EVS Port1 42/1/SAMPLE 13: SAMPLE: Enable command receiv
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 =
EVS Port1 42/1/RADIO 31: GENERIC_RADIO: Request device
```

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

0 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

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")

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)

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 packets)

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

Launch Change Attack Stop Change Attack

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/LC 28: Set LC state command: new state = 1

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

N A
L A
F Axes
B Axes
N Grid
L Grid
F Grid
B Grid
Gal Grid
EDVs

Scenario #1 – No SDLS (cont.)

NOOPs Are Fun....but Let's Make It Spin!!!

MitM the next CAM_NOOP_CC to spin the reaction wheels to cause an uncontrollable spin

Source IP	Destination IP	Source Port	Destination Port	Packet Data
10.57.64.223	10.57.64.220	39064	5111	07e90123000a00120008002040309eb8b5feffbc14cf27092503750414
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 packets)

18c8c00000010000 1992c00000040300006400 1

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)

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

Launch Change Attack Stop Change Attack

SPARTA TTPs: DE-0002.01Change Attack Launched

COSMOS Command Sender

Scope: DEFAULT

Select Packet: CAM_NOOP_CC

SEND

Camera NOOP Command

ARDUCAM CAM_NOOP_CC") sent. (5)

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

"ARDUCAM CAM_NOOP_CC")

UTC 291-08:31:10.89

POV

TRACK HOST

Fixed in: [] [] [] [] [] [] [] [] [] []

Boresight: -Y [] [] [] [] [] [] [] [] [] []

Up Axis: +Z [] [] [] [] [] [] [] [] [] []

Host

World: Earth

Ref Orb: 0

Frm: 0

S/C: 0

Body: 0

Range: 3.20

In Sunlight

Target

World: Earth

Ref Orb: 0

Frm: 0

S/C: 0

Body: 0

Range: 3.20

In Sunlight

Show

N Axes

L Axes

F Axes

B Axes

N Grid

L Grid

F Grid

B Grid

Gal Grid

Top

+X -X

+Y -Y

+Z -Z

Center

+X -X

+Y -Y

+Z -Z

Center

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 screenshot displays two web-based interfaces used for satellite command and telemetry management.

COSMOS CmdTlmServer (Left Panel):

- Interfaces:** Shows two interfaces: **DEBUG** and **SIM_42_TRUTH_INT**. Both are **CONNECTED**. The **DEBUG** interface has 0 clients, 0 Tx Q, 0 Rx Q, 1682 Tx Bytes, and 1557542 Rx Bytes. The **SIM_42_TRUTH_INT** interface has 0 clients, 0 Tx Q, 0 Rx Q, 0 Tx Bytes, and 8844906 Rx Bytes.
- Log Messages II:** A table of log messages with columns: Time, Log Level, Source, and Message. The log level is filtered to **NORMAL**. The messages are critical and show errors related to packet lengths and command reception.

SPACE Invader (Right Panel):

- Attack Selection:** A dropdown menu shows **Choose Attack** with options: **CMD Injection**, **Replay Packet**, **Change Packet**, **Jamming Attack**, **Flooding Attack**, and **HAVOC**.
- Upload Command/Telemetry Database:** A button labeled **Upload** is visible.
- Select Database:** A dropdown menu shows **Select Database** with the option **SPARTA TTP: REC-0003.02**.
- Send Raw CMD / Choose CMD:** Buttons for sending raw commands or choosing from a database.
- Log Output:** A text area showing the output of the tool, including messages like "Log writer out of order time detected", "CFS CFE_EVS_TLM_PKT received with actual packet length of 22 but defined length of 160", and "CFS CFE_EVS_TLM_PKT received with actual packet length of 22 but defined length of 160".

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	0941c1012319409eeda4a4f5dab96e5046ca1bbdb80017688f01de9194
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	18c8c001231fd877f40823b0e3f2954afe4adb669e06795e79d07114f4e

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 Bores 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

Range In Su

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

END

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

The screenshot shows a network tool interface with a dark background. At the top, it says "Showing 21 to 24 of 24 entries (filtered from 1,530 total entries)". Below this, there are three tabs: "CMD Injection", "Replay Packet", and "Change Packet". The "Replay Packet" tab is selected. Under this tab, there are five input fields: "Hex Packet to Replay" (containing "114f4ef47a4525c63ac0569"), "Destination IP" (containing "10.57.64.223"), "Source IP" (containing "10.57.64.220"), "Destination Port" (containing "6012"), and "Source Port" (containing "56666"). Below these fields is a label "Number of times to replay packet (type 999 to send continuous packets)" and a dropdown menu set to "10". At the bottom of the configuration area, there are two buttons: "Launch Replay Attack" (blue) and "Stop Replay Attack" (red). Below the buttons, it says "SPARTA TTPs: [EX-0001.01](#)". On the right side of the interface, there is a terminal window showing the text "request device HK reported error". At the bottom of the interface, there is a list of grid names: "B Axes", "N Grid", "L Grid", "F Grid", "B Grid", "Gal Grid", and "FOWs".

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](#)

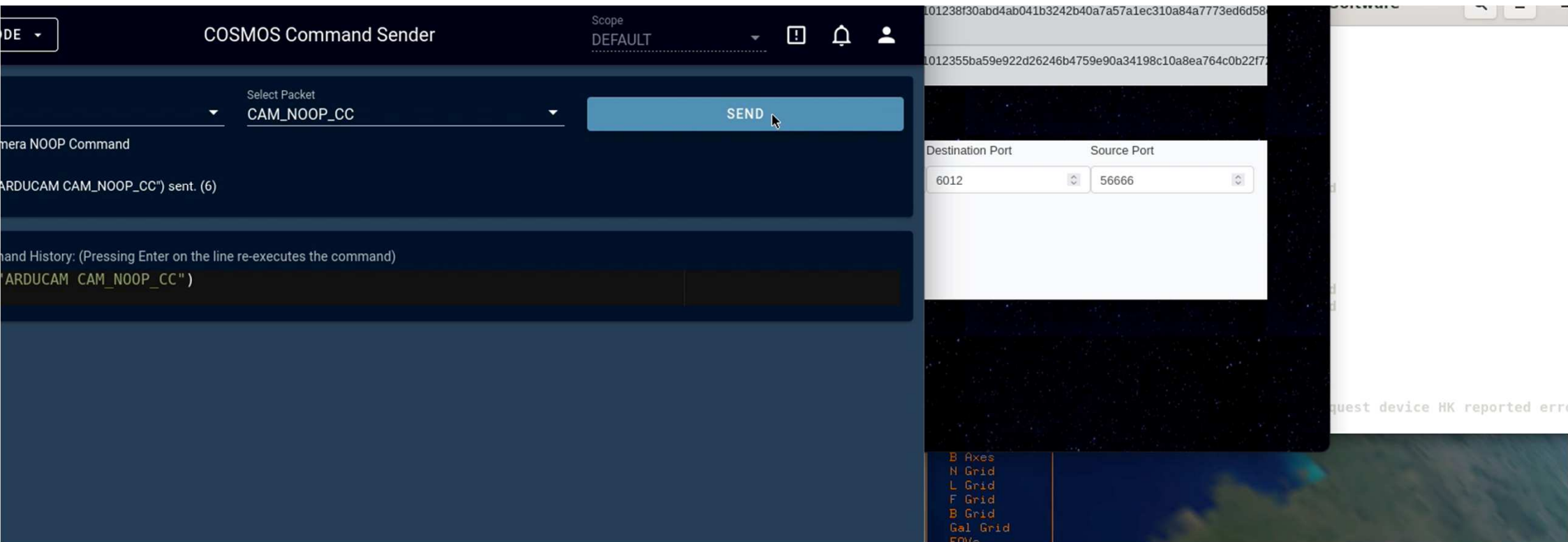
request device HK reported error

B Axes
N Grid
L Grid
F Grid
B Grid
Gal Grid
FOWs

Scenario #3 – With SDLS Using Encryption & Authentication

None of the Previous Attacks Work 😞

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



Techniques Used >>> SPARTA Countermeasures

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.

Subtechniques (2)

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

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

Countermeasures

	Description
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.
Authentication	Authenticate all communication sessions (crosslink and ground stations) for all commands before establishing remote bidirectional authentication that is cryptographically based. Adding authentication on the spacecraft bus and communication links is also recommended.
Relay Protection	Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections over the bus.
Traffic Flow	Utilizing techniques to assure traffic flow security and confidentiality to mitigate or defeat traffic analysis attacks or reduce the effectiveness of such attacks.

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

Countermeasures

ID	Name	Description
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.
CM0073	Traffic Flow Analysis	Utilizing techniques to assure traffic flow security and confidentiality to mitigate or defeat traffic analysis attacks or reduce the effectiveness of such attacks.

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: SV-AC-1
Related MITRE ATT&CK TTPs: T0831
Related ESA SPACE-SHIELD TTPs: T2008.006 | T2019.005
Tactic: Defense Evasion
Created: 2022/10/19
Last Modified: 2024/02/29

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](#)

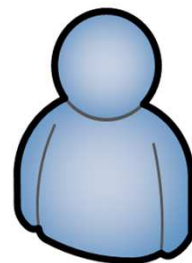
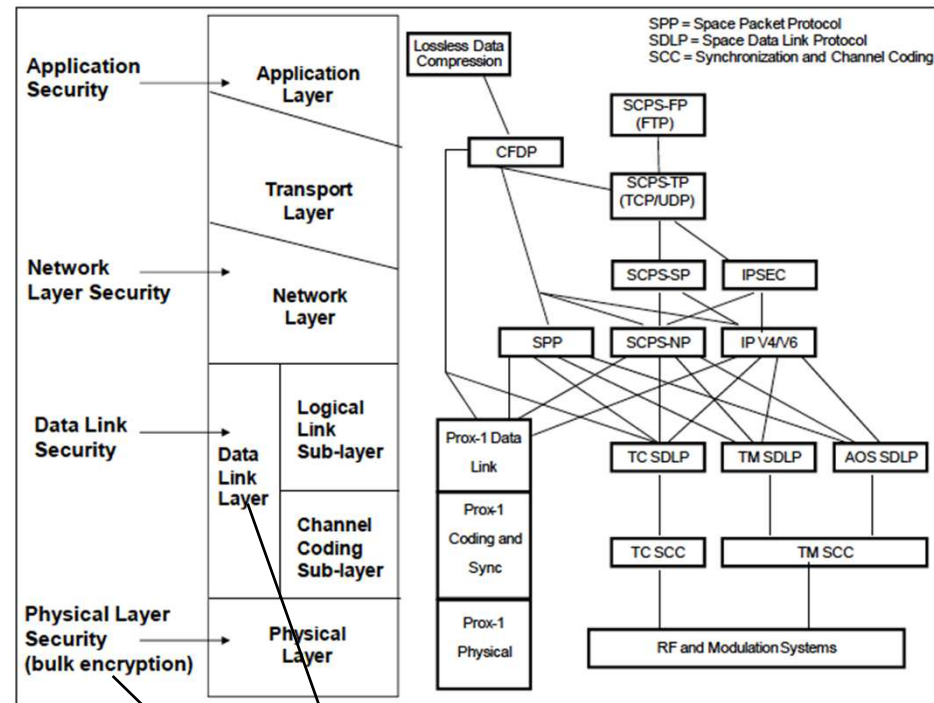
Compromised ground is one of the highest risks to the SV

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!!!

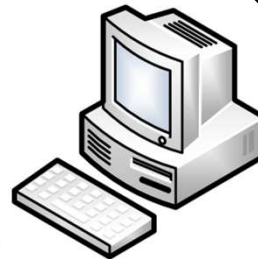
- If using CCSDS (TC/TM/AOS) [SDLS](#) improves security immensely and mitigates many known TTPs
 - [SDLS Extended Procedures](#) are also available

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.



HEATER_ON

HEATER=ON



Command and Control (C2)

4E524F

4E524F



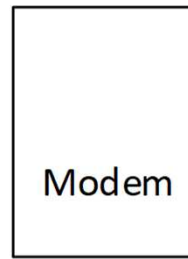
FEP

DEADBEEF

DEADBEEF

DEADBEEF

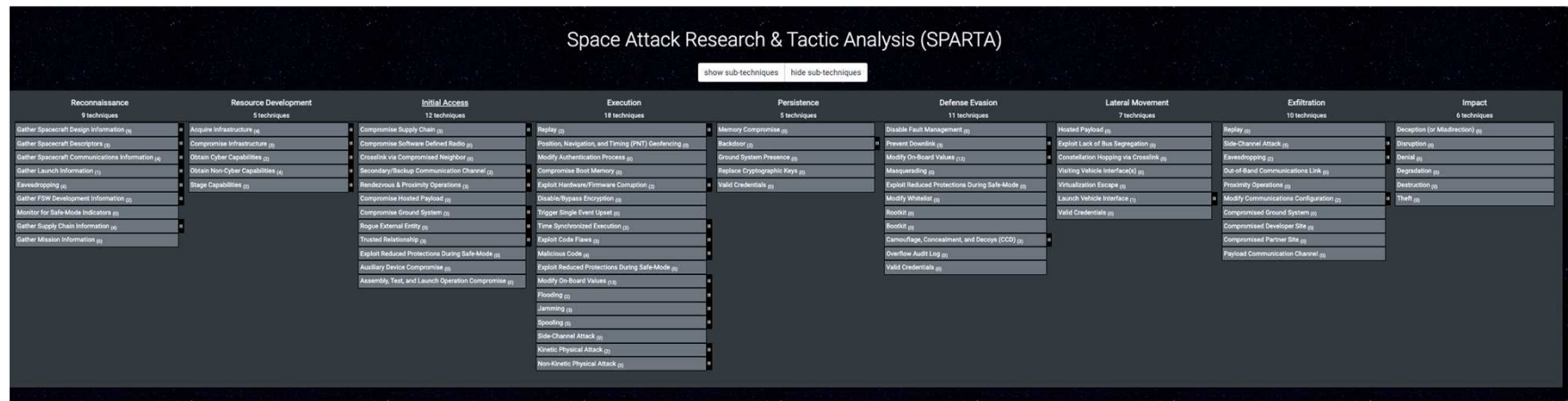
Bulk
Crypto Unit



Modem



<https://sparta.aerospace.org>



More Media Links:

<https://cyberscoop.com/space-satellite-cybersecurity-sparta/>
<https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks>
<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

