

INTRODUCTION

Background

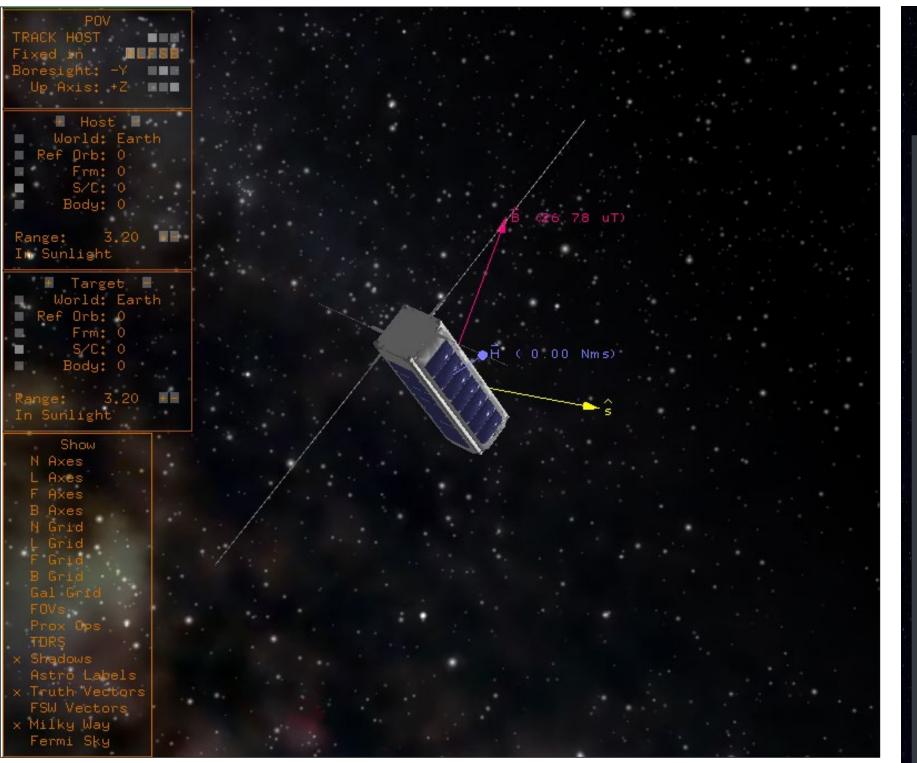
- Cybersecurity protects computers, data, and networks from unau and attacks
- Satellite networks are vulnerable to cyber threats, which can be Deep Packet Inspection (DPI) – Analyzes network traffic granu
- Machine Learning (ML) Detects anomalies and potential cyb

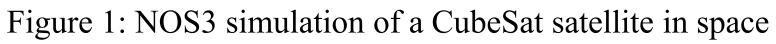
Motivation

- Why study onboard satellite communications?
- Research exists on satellite-to-ground cybersecurity, but much cybersecurity
- Onboard satellite functions produce data that does not reach data could hold a wealth of information that could inform cyb
- Why satellite cyberattacks?
- Satellite cyberattacks can disrupt critical global infrastructure communication, navigation, national security, economic stabi
- Why simulated data?
- As a generally protected/proprietary technology, satellite info publicly accessible
- Simulation is used extensively in space operations for testing because of limited data accessibility.

<u>The Goal</u>

Utilize machine learning models to analyze onboard satellite dat potential cyberattacks, preventing potentially catastrophic impact





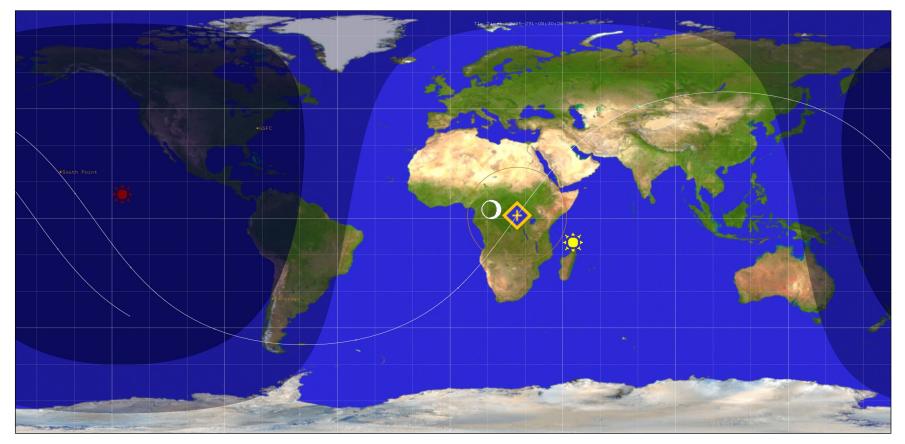


Figure 2: Map of the path for the simulated satellite

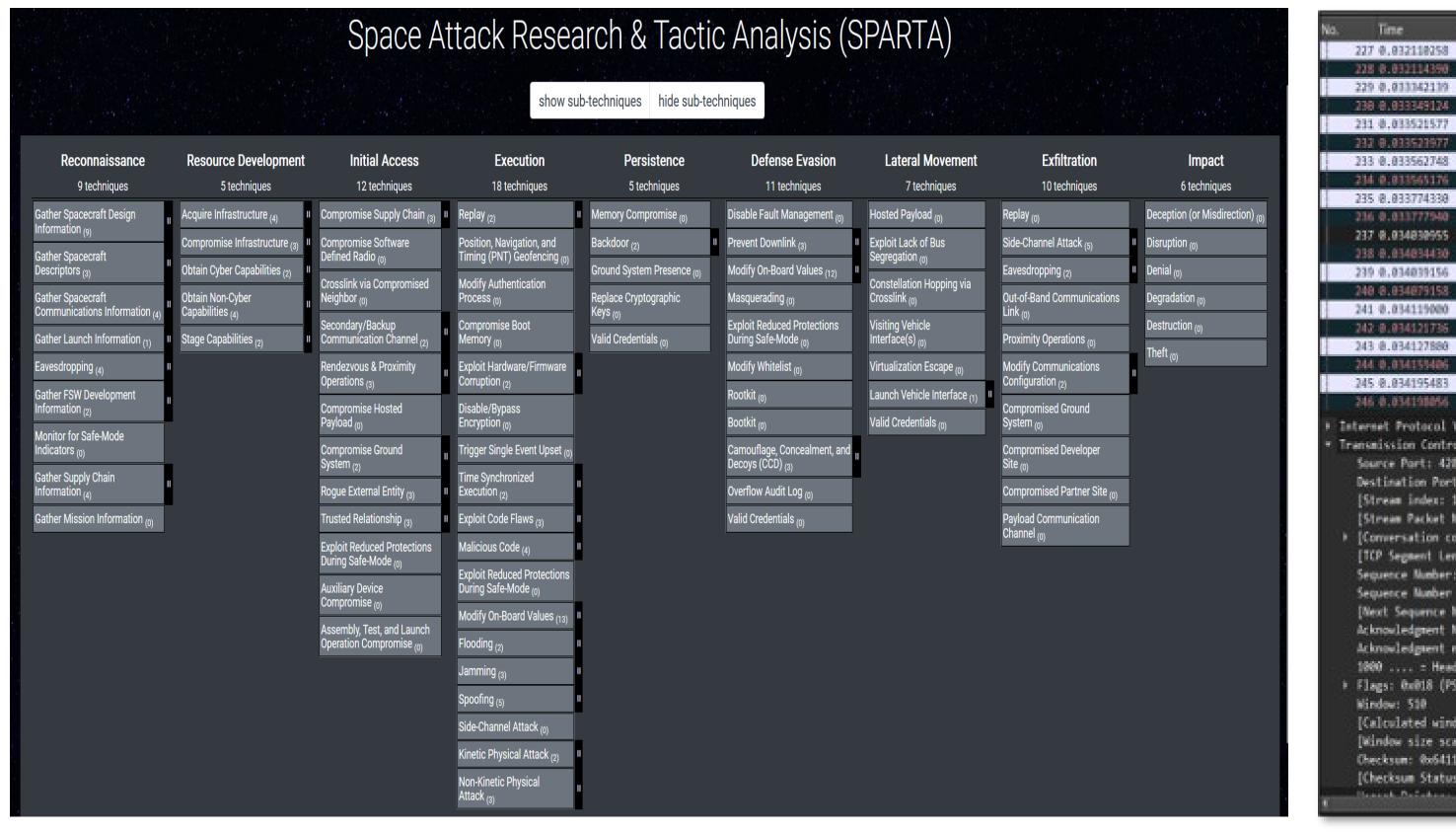


Figure 3: Image of SPARTA Matrix

Acknowledgements: Our team sincerely thanks the following people for supporting our project: Dr. Tomás Peña, Paul Kroszczynski, Dr. Daniel Hirleman, Dr. Mark Daniel Ward, Jessica Jud, Kali Lacy, Mia Sartain, and the collective Data Mine team.

L3Harris: Satellite Cyberattack Detection

Purdue: Shrenick Gannamani, Vanessa Jan, Kabir Jain, Michelle Jyi – TA: Mahima Malhotra UC Colorado Springs: Marlin Jaramillo, Dylan Truesdell CU Boulder: Tate Charboneau, Vraj Patel **MSU Denver: Angela Fleenor**

uthorized access	 Satellite Day-in-the-Life Model Developed a day-in-the-life model representing a type of events and events.
monitored using: ularly	type of small satellite, as displayed in Figure 1) with a reasonable command set
berattacks	 Researched messages/commands commonly s
n less on onboard	 Used SPARTA (Space Attack Research and Tacti a matrix that defines and categorizes different l specifically for satellites, to research common c
the ground. This	 Developed sample use case:
ersecurity	 Determined mission for our simulated satellit attack simulation
e essential for	 Determined possible cyber-attacks that this s real-world scenario
ility, and more	NOS3 Satellite Simulation
	Utilized NOS3, a small satellite simulator development
rmation is not	CubeSat model (Figures 1 and 2)
and modeling	 Studied the space communication protocols use
	 Used our Day-in-the-Life model as a template fo
ta to detect cts.	 Used Tshark, a network traffic analyzer, within N transmission packet data for training a machine

Figure 4: Example of network packet data analyzed using Wireshark

REFERENCES

Cybersecurity framework. NIST. (2024, October 31). https://www.nist.gov/cyberframework Mitre ATT&CK®. MITRE ATT&CK®. (n.d.). https://attack.mitre.org/

Sparta: The Aerospace Corporation.. (n.d.). https://aerospace.org/sparta

He, J., Cheng, Z., & Guo, B. (2022, August 24). Anomaly detection in satellite telemetry data using a sparse feature-based method. MDPI. https://www.mdpi.com/1424-8220/22/17/6358

Artificial Intelligence. NIST. (2024a, September 25). https://www.nist.gov/artificial-intelligehttps://github.com/nasa/nos3/wikince NASA Operational Simulator for Small Satellites (NOS3) Wiki. NASA. (2024, October 21). https://github.com/nasa/nos3/wiki

RESEARCH AND PROJECT WORK

a typical day for a CubeSat (a to help us simulate a satellite

sent between components

- tic Analysis shown in Figure 3), kinds of cyberattacks yberattacks
- te to carry out during cyber-
- satellite may experience in a
- oped by NASA, to simulate our
- sed by NOS3
- or simulating data on NOS3
- NOS3 to capture satellite e learning model

Analysis of Packet Data

- Used Tshark and Wireshark, tools used to a network traffic, to understand and clean d gathered from the NOS3 simulation (show 4), specifically for:
- Scraping packet data to find keywords r satellite commands
- Filtering and organizing packet data bas packet type
- Cleaning the packet dataset by discarding corrupted packets and packets containi irrelevant information

Machine Learning Algorithms

- Researched effective machine learning alg and chose optimal algorithms to analyze s packet data and detect potential cyber three
- Long Short-Term Memory (LSTM) Model effective model for working with time-se and determining cyber anomalies throug temporal (timing) data
- Isolation Forest Model A model well-si finding anomalies in a given set of data
- Utilized data extracted from network traffic the Machine Learning models

Source	Destination	Protocol	Length	inio										
172,18.0,14	172.18.0.3	TCP	68	46270	+ 4245	ACK	Seq-	d Ack	-2999	$[k_{i}^{\prime}]_{i=1}$	0090 1	en-9 TSva	1-342525	3843
172.18.0.14	172.18.0.3	TOP	68	TOP 1	Dup AD	1222	i) 46a	28.4	4245		Segal	458-2999	Min-1985	0-Li
172,15,0,3	172.18.0.11	TEP	522	4227	49570	PIN PIN	ACK	Seq-1	i Aclo	-1 Mir	-510 1	49-454 15	val=41540	7371
172.18.0.3	172.18.0.11	TEP	522	TCP	Roto alto	ales i	a) (a	107 + 1	49578	ESH,	408	Seg-1 Ach	el almes	10 1
172.18.0.11	172.18.8.3	TCP	- 68	49570	+ 4327	ACK	Seq-	d Ack	-455 1	dia-96	68 Les	-0 TSval-	10931327	61.1
172.18.0.11	172.18.0.3	TEP	68	TOP I	Dep AD	2314	495	20 + 1	4227	(ACC)	Secret	Act 455 8	La-9658	Lun
172.18.0.3	172.18.0.16	TEP	238	4234	 43896 	PSH.	ACK	Sequi	1 Acb	-1 Mir	-518 1	.en=178_TS	val-3114	8154
172-18:0:3	172.18.0.16	ICP.	238	TOP I	Ri Ernaldi	and to be de	an (). 42	14 +	11036	254	408 }	Sug-1 Ack	-1 Min-Si	10-1
172.18.0.3	172.18.0.8	TCP	772	9999	• 58298	PSH	ACK	Seq-	1 Acio	-1 Mir	-510-1	en=784 TS	val=1538	8224
172.18.0.3	172,18.0.8	TOP	777	TOP 1	Referance	and the set	a j 99	199 ÷ -	902-04	(P98),	ant)	Seg-1 Ack	el allossi	10 1
172.18.0.3	172.18.0.13	TEP	3866	4281	• 53652	(PSH)	, ACK)	Sequi	2998	Actor 1	Min-51	0 Len-295	8 TSval-	1533
172.18.0.3	172.18.0.13	TCR	3866	TOP I	Retriets	missi	aj o	111 +	5.365.3	PSH,	468]	Seq=3998	Ack-1 Mi	n=53
172.18.0.13	172.18.0.3	10P	68	\$3652	+ 4233	ACK	Seq	4 Ack	-5996	Win-1	0090 L	en-0 TSva	1-232225	4838
172.18.0.13	172.18.0.3	TEP	68	TOP I	Dep AD	2356	1 536	62 ÷ 1	1281	ACC	Sequil	Ark-5996	Min-1089	8 Ls
172.18.0.3	172.18.0.15	TCP	3066	4288	47416	1254	ACX	Seq-	2998	Ack+1	Min-53	10 Len-299	6 TSval-	1740
177.18.0.3	172.18.0.15	TEP	3066	TOP	Reteratio	mittadi	n) (80	47436	PSH,	408]	Seg-2938	Activit with	n=53
172.18.0.15	172.18.0.3	109	68	47416	+ 4286	ACK	Seq	d Ack	-5996	Min-1	10811	envil TSva	1-169280	4.578
172,18,0,15	172.18.0.1	TEP	0	TOP	8ap 140	24.34	() 678	116 • 1	1250	400	Supl	4-1-5996	Min-1101	1.1.1
172.18.0.3	172.18.0.22	TCP	231	4282	• 52386	PSH	ACK	Seq.	164 A	ckel k	dia-518	Let-163	TSvia1-248	8768
172.18.0.3	172.18.0.22	TEP	214	TOP	Retrati	missi	a] ()		2100	UPSH,	ACK]	Seq=164_8	and Mar-	-3:1
l Protocol, Src Port: 1 : 53652 2] umber: 5] mpleteness: Incomplete : 2998 (relative sec (raw): 67235689 umber: 5996 (relati	guence number) ive sequence number)] ack number) W		0 8a 0 31 0 33 0 34 0 55 0 32 0 36 0 36 0 30 0 30	Ga th 10 51 10 10 10 10 10 10 10 10 10 10 10 10 10	38 3a 31 8a 32 32 36 28 35 65 34 39 65 6c	49 4d 14 15 53 43 10 35 2d 35 30 39 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 3	45 20 34 3. 55 36 3. 56 3. 57 3. 58 3. 59 3. 50	2 18 2 8 5d 2 8 5d 3 9 31 2 8 30 3 8 30 3 9 30 30 3 9 30 30 3 9 30 30 30 30 9 30 30 30 9 30 30 30 9 30 30 9 30 30 30 9 30 30 10 30 30 10 30 30 10 30 30 10 30 30 100 30 30 100 30 100 30 100 30 100 30 10000000000	0 32 30 30 32 32 32 32 32 32 32 32 32 32 32 32 32	5 2d 19 73 37 33 11 43 98 29 39 39 39 39 39 39 39 39 39 39 39 39 39	37 35 39 38 38 38	-jT1 1-08-4 3761-5 - 1.28 e-05 2685e-6 637493 J.VeTR 000000 000000 000000 000000 000000	5; 28.005 [[0].Pos 05 142687 8. 607203 38 1.031 30 -07 5C = 0.000	-29 98 875 98 180 190 100 100 100 100 100 100 100 100 10
aw size: 510] ling factor: -1 (wakan [unverified] : Unverified] 2	≫n)]		62 0 35 0 32 0 34	28 3d 37 65 38 34 34 35		2e 30 35 20 65 26 33 36	36 30 32 20 38 30 39 30	2 33 3 e 35 3 5 20 2 3 65 2	5 39 7 34 8 32 8 38	32 31 31 31 2e 39 35 6a	33 35 33 39 35 32 53 43	b = 2.0 57e-05 28488e 445273	6 235921 2 .57411 0 5 -2.9 29 3e-05 5 = 3.78	135 139 62 52

Explore other "Day in the Life" scenarios:

We analyzed anomalies in a satellite whose purpose was to photograph the earth. What would we find if we did the same in a satellite whose purpose was to measure space weather or boost radio communications? Exploring other DITL scenarios would help us understand how our model applies to different scenarios.

<u>Test model on real-world satellite data:</u>

Intra-satellite communications data is not readily available. We utilized simulated data for our project. We could work to gather private intrasatellite communications data. Training or evaluating our model using that data would expand our accuracy or give us further insight into our model's performance.

Explore applicability of model with other types of network traffic:

Currently, our model is designed to analyze the network traffic data of satellites, performing anomaly detection to identify potential satellite cyberattacks. However, satellites are not the only devices susceptible to cyberattacks, and although this is beyond the scope of our project, it could be interesting to explore the applicability of our model to the network traffic data of cellular devices.





	CONCLUSION
analyze ata n in Figure elating to	 Researched what a typical Day- in-the-Life of a small satellite looks like to build a dataset simulating a small satellite in a normal day
sed on ng ng	 Researched common cyberattacks that small satellites are vulnerable to in conjunction with the SPARTA Matrix
gorithms atellite eats: – An eries data gh	 Utilized NOS3 simulator to generate sample CubeSat data for machine learning algorithm training
	 Used Tshark and Wireshark to analyze telemetry data
	 Simulated cyberattack data on NOS3 satellite simulator
c to train	 Trained Isolation Forest and LSTM Machine Learning models

CONCLUSION

FUTURE GOALS