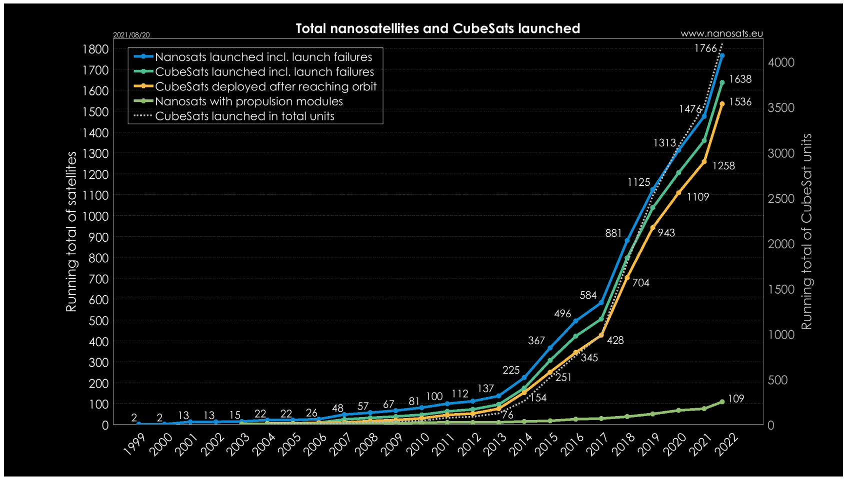
Safety and Security of Small Satellites in Low Earth Orbit (LEO): Small Satellite Workshop @ UTD

Kangkook Jee

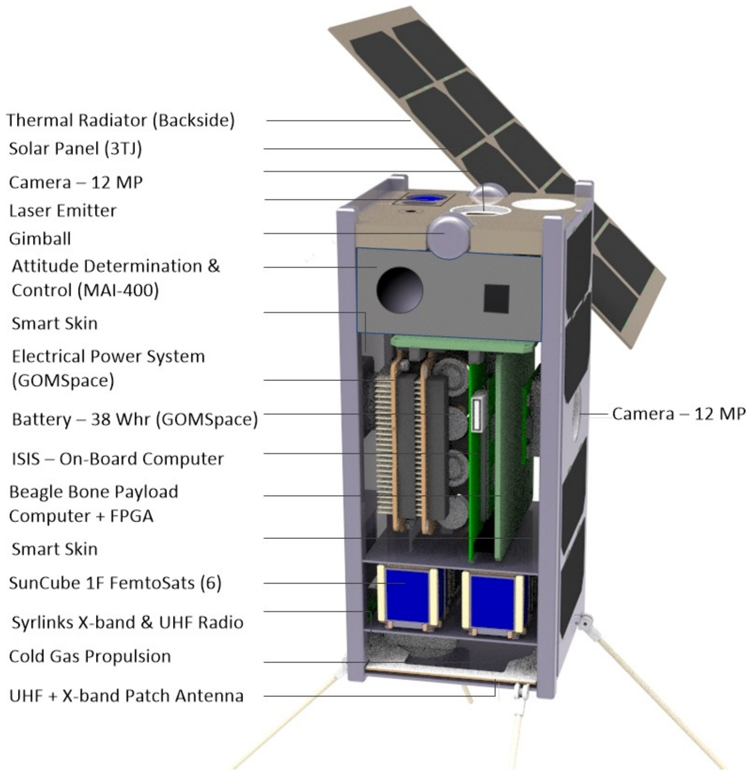
July 7, 2025

New Space Era

- Two Enablers
  - Re-usable booter technologies
  - Ever-shrinking size of technologies



Total count of CubeSats launched as of August 2021



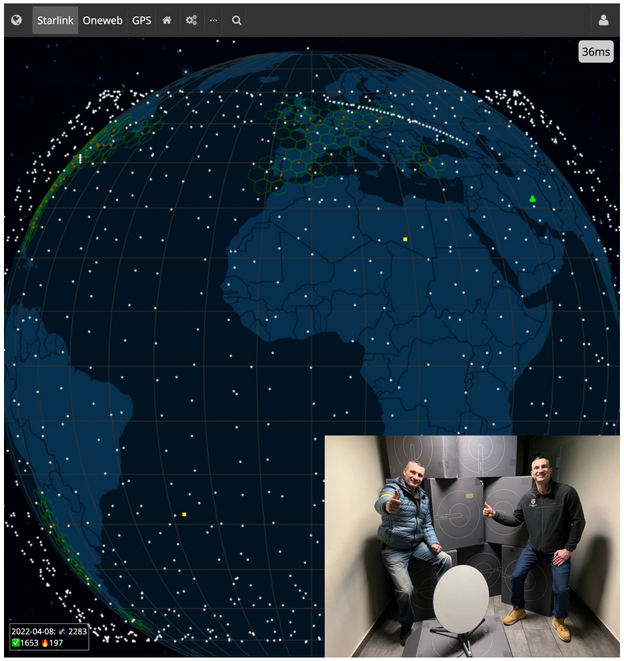
Standard 2U CubeSat
(1U: 10 cm × 10 cm × 11.35 cm)

Starlink@Ukraine

- Starlink aims to be a world-wide Internet ISP
  - Constellation with ~2000 on LEO (Low Earth Orbit)
  - ~3000 more on their ways

- Ukraine has been winning a propaganda campaign

- If you were Putin, what would you do?

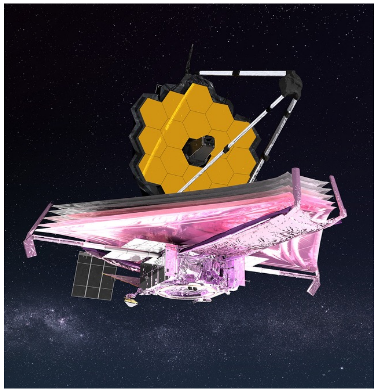


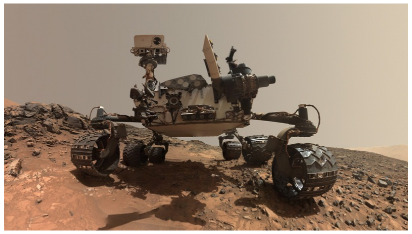
Starlink satellite map - https://satellitemap.space/

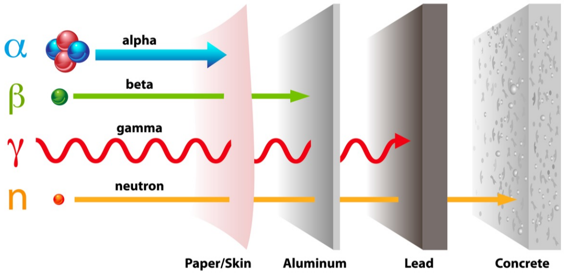
"Traditional" Space Electronics

- Confirmed by a rigorous process
  - E.g., Rad-hardening, ruggedized components

Image source: BAE systems

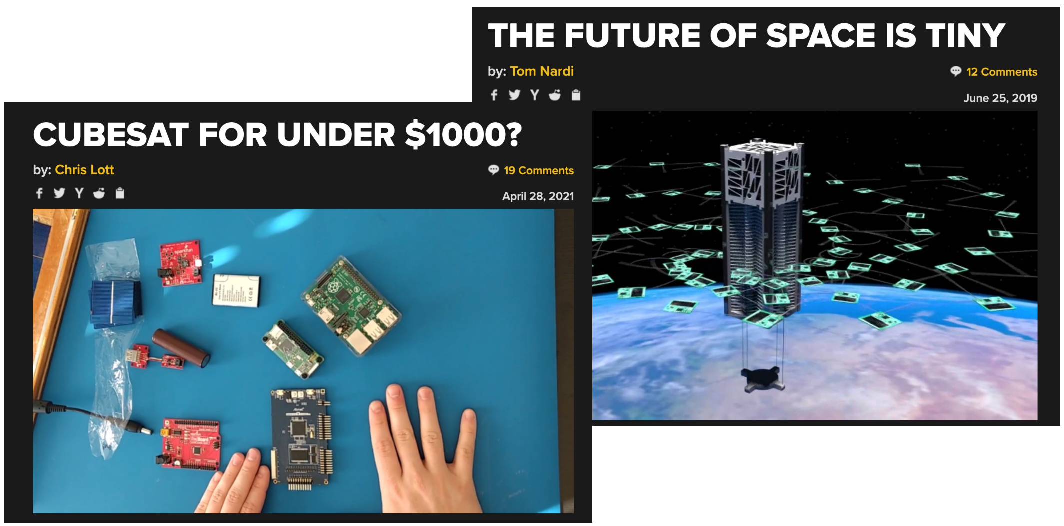






The Game is Turning into a New Phase

- $2M to put your CubeSat on LEO
- Big business for sweeping space debris



Space + Cyber Security

This is historical material "frozen in time". The website is no longer updated and links to external websites and some internal pages may not work.

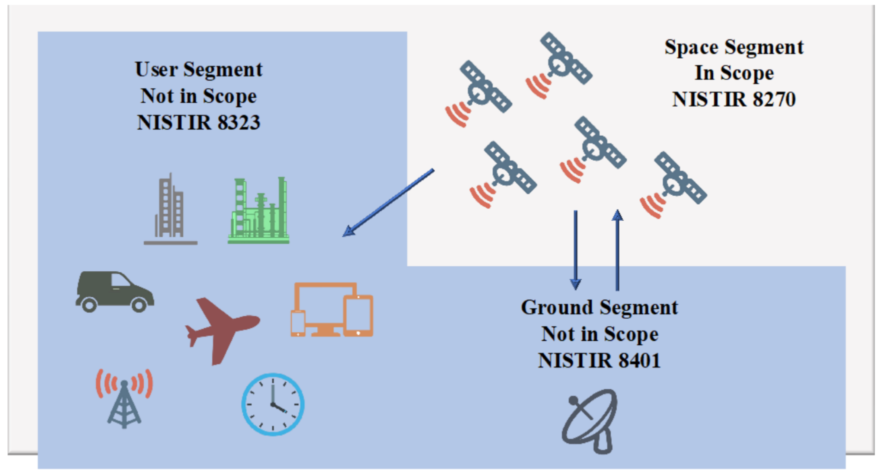
PRESIDENTIAL MEMORANDA

Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems

NATIONAL SECURITY & DEFENSE

Issued on: September 4, 2020

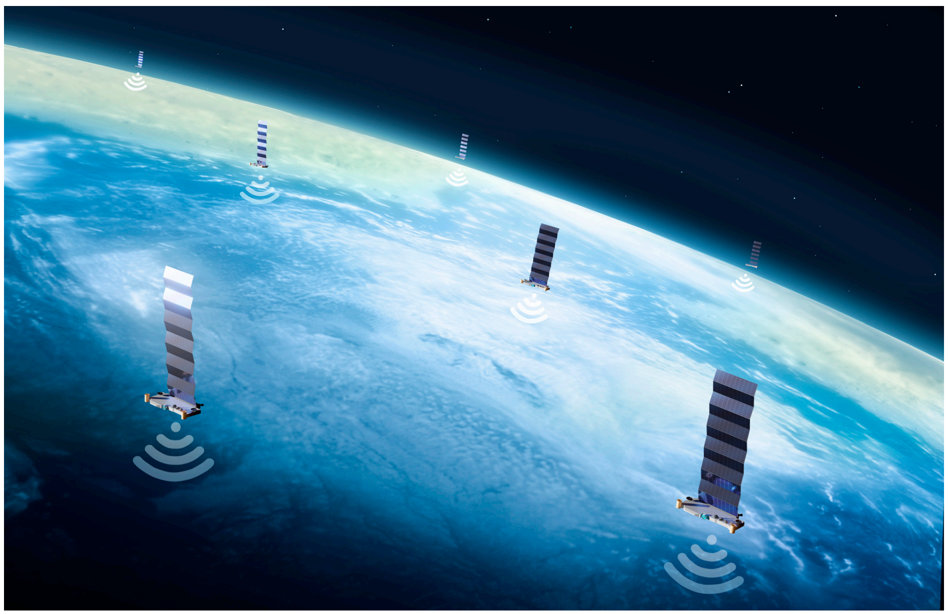
[memorandum on space policy direct 5]

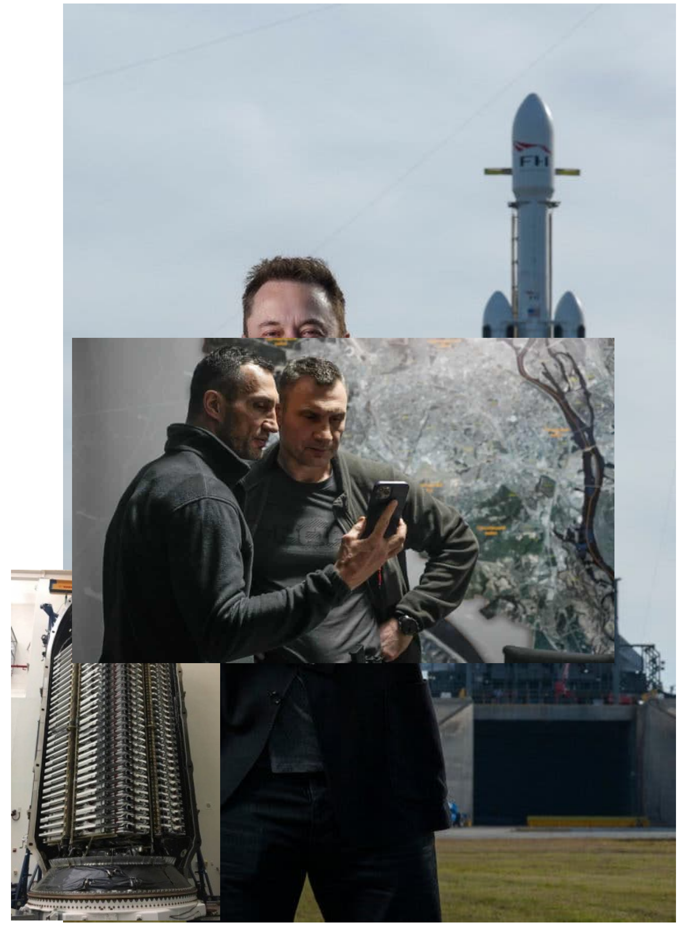


- NIST-IR 8270: Introduction to Cybersecurity for Commercial Satellite Operations
- NIST-IR 8323: Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
- NIST-IR 8401:Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control
- NIST-IR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Starlink@Ukraine

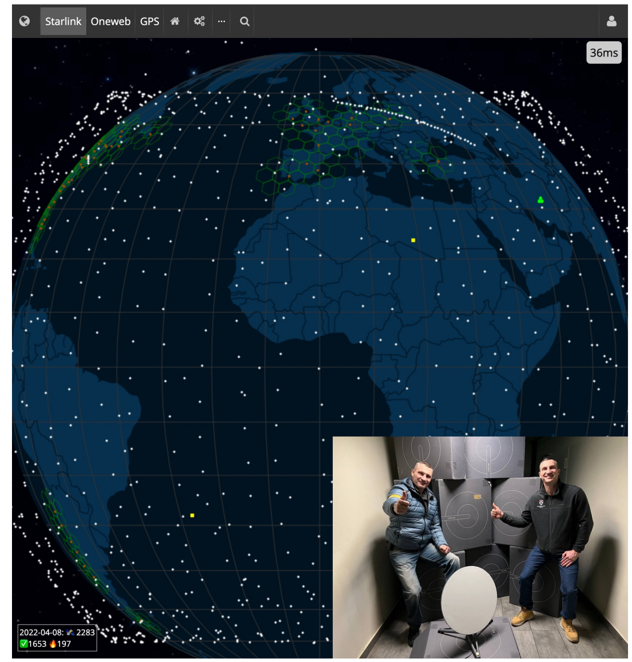
- People are still connected amongst war





Starlink@Ukraine

- Starlink aims to be a world-wide Internet ISP
  - Constellation with ~2000 on LEO (Low Earth Orbit)
  - ~3000 more on their ways
- Ukraine has been winning a propaganda campaign
- If you were Putin, what would you do?



Starlink satellite map - https://satellitemap.space/

Disclaimer

- This is a failure story
  - 4+ years of endeavor without producing concrete outcomes

- Safety and security of small satellites (or CubeSats) in LEO
  - Space has many segments
  - LEO, MEO, GEO, and deep space
  - Private, public sectors, and *academic and research communities*

Who Am I?

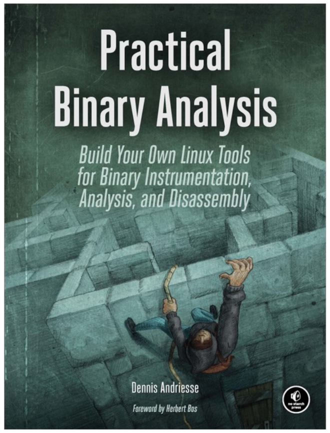
- 10 years of industry experience
  - IBM Korea, NEC Laboratory in America
  - OS/JVM engineer
  - EDR research, Pen-testing, and security analysis
- Joined UT Dallas in 2019
  - Specialized in system security
  - Teaching binary reversing (CTF) courses

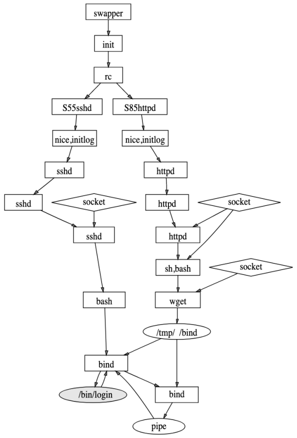
Who Am I?

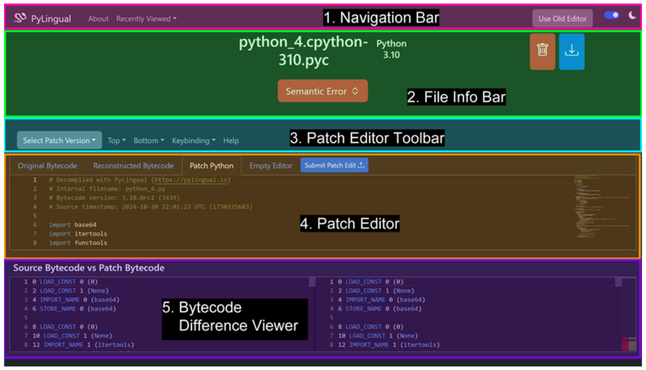
- System security researcher
  - Binary-level information flow tracking: [libdft]
  - Static and dynamic program (binary) analysis

- Leveraging ML-techniques to automate security analysis
  - Data-driven security research with large security graphs
    - EDR, system provenance
  - Decompilation of High-level Dynamic Languages (HDLs)
    - [PyLingual]

- Why SPCACE?



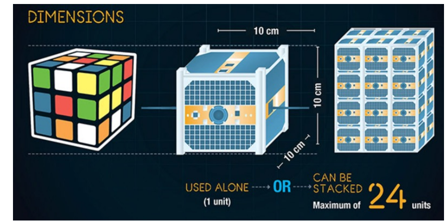




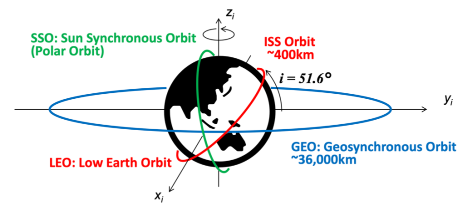
My Space Journey

- How a system security researcher come to be a space enthusiast?
- Lucky to have a chance to participate satellite project (6U CubeSat)
  - 1 year in preparation stage, 2 years of operation
  - Planned to run various cybersecurity research
  - Couldn't say it was quite successful …
- Still working on space
  - Gap between cyber and aerospace communities
  - Research opportunities
  - Optimistic (or Naive) about space
- This talk will be about …

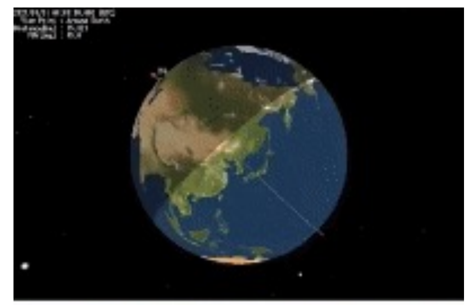
Context Reminder: CubeSat in LEO

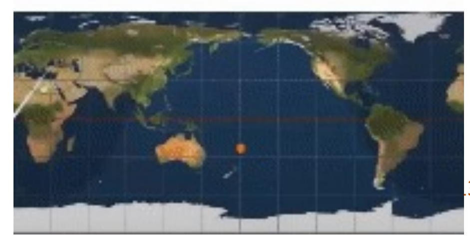


- CubeSat
  - Mico- or nanosatellites (~ 10 kg)
  - For amateur and hobbyists (You may not find it super-relevant)



- Low Earth Orbit (LEO)
  - Popular destination among recent spacecraft projects (e.g., Starlink, ISS)
  - Pros
    - Inexpensive launch cost
    - Short latency for terrestrial communication
  - Cons
    - Circle the earth every 7 ~ 9 hours
    - Under close gravity interference
    - Space debris



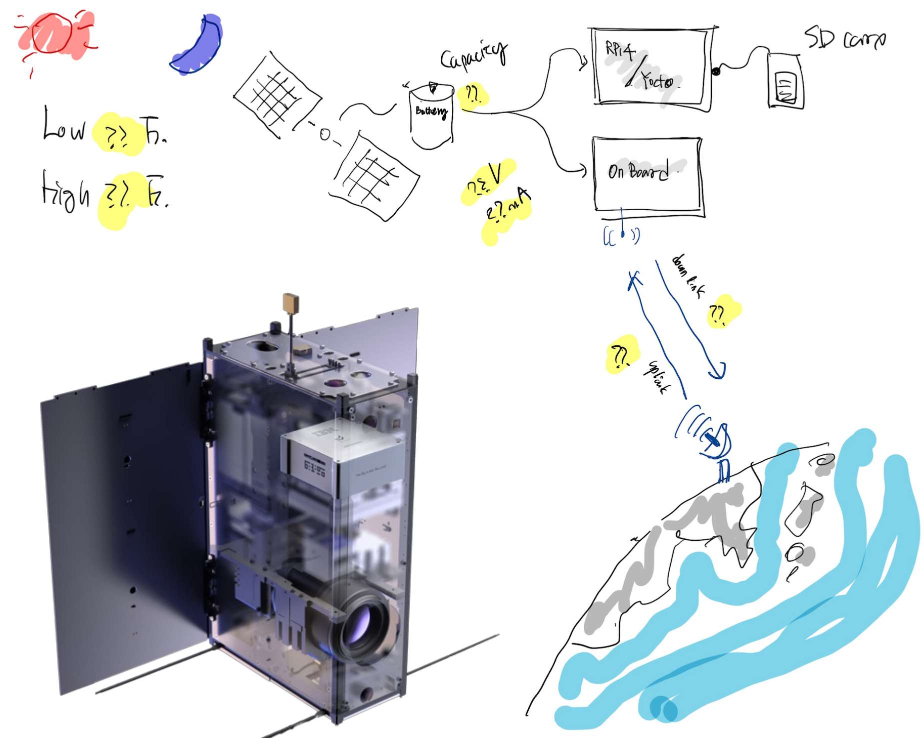


UTD + IBM Space Collaboration

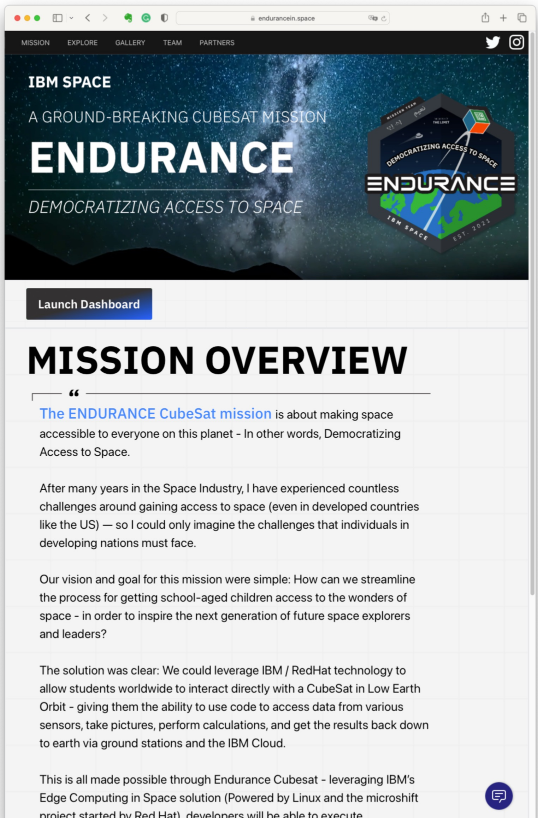
- Endurance CubeSat mission
  - A new and exciting topic
- Aim to make scientific contributions
- Safety and Security

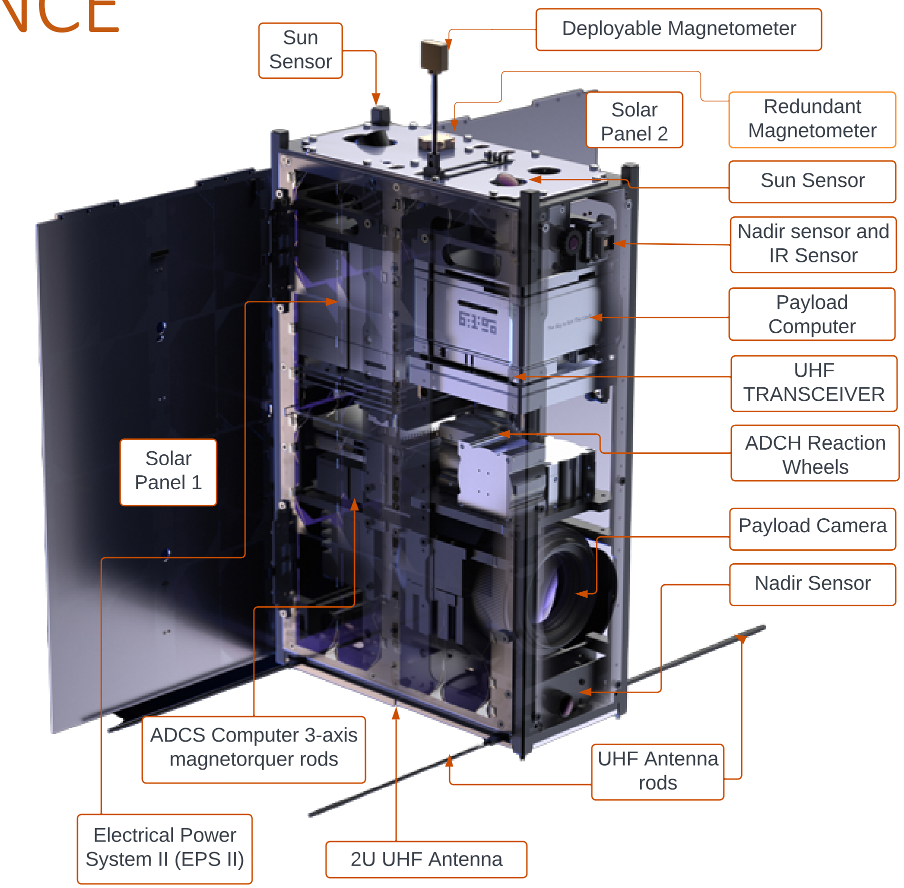
UTD + IBM Space Collaboration

- CubeSat on LEO
  - Low-Earth-Orbit (LEO)
  - A unique testbed for safety and security using consumer grade electric device
- IBM Space Tech + academic research collaboration
- Unconventional use-case of edge-cloud computing model
  - Different physics for space computing



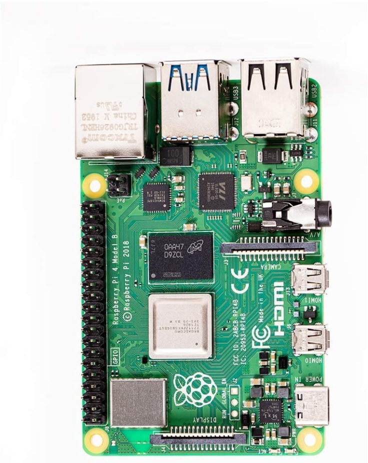
IBM Space: ENDURANCE



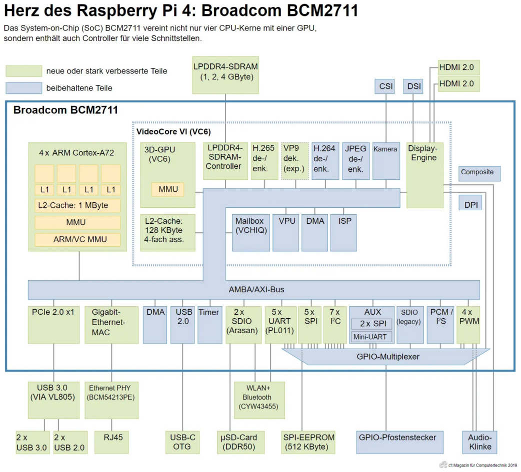


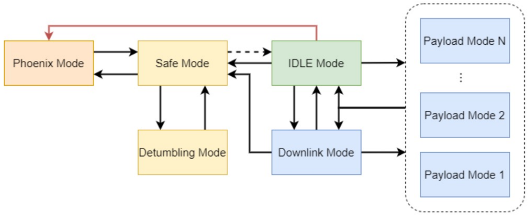
IBM Endurance

- Raspberry Pi 4 (BCM 2711)
  - Yoko Linux image customized for satellite operation
  - Minimal power consumption
  - Fast / seamless recovery
- CubeSat Onboard Computer (OBC)
  - Microcontroller (MCU) -based computer for payload operation
  - Mainly concerns about Satellite operation + ground communications

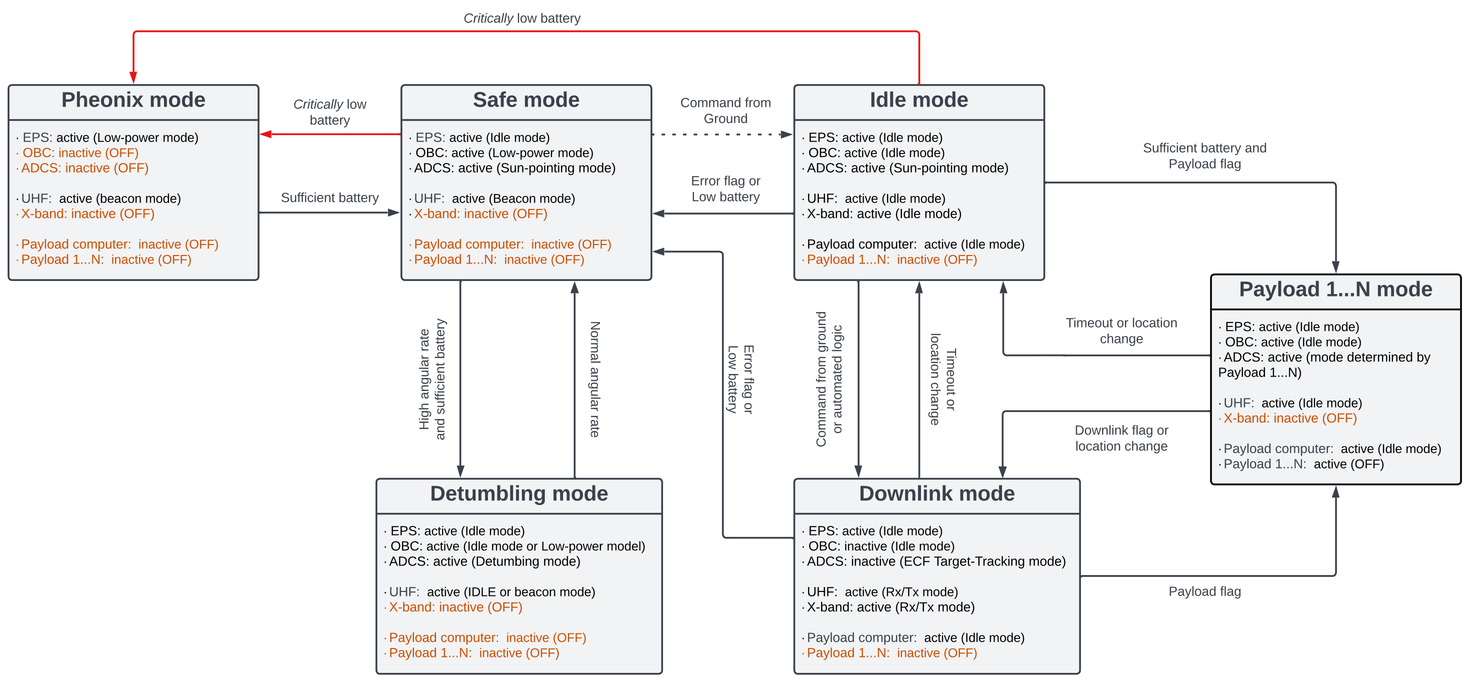


Payload (Rpi4)





Endurance CubeSat OBC State Diagram



* Custom (in-house) control software

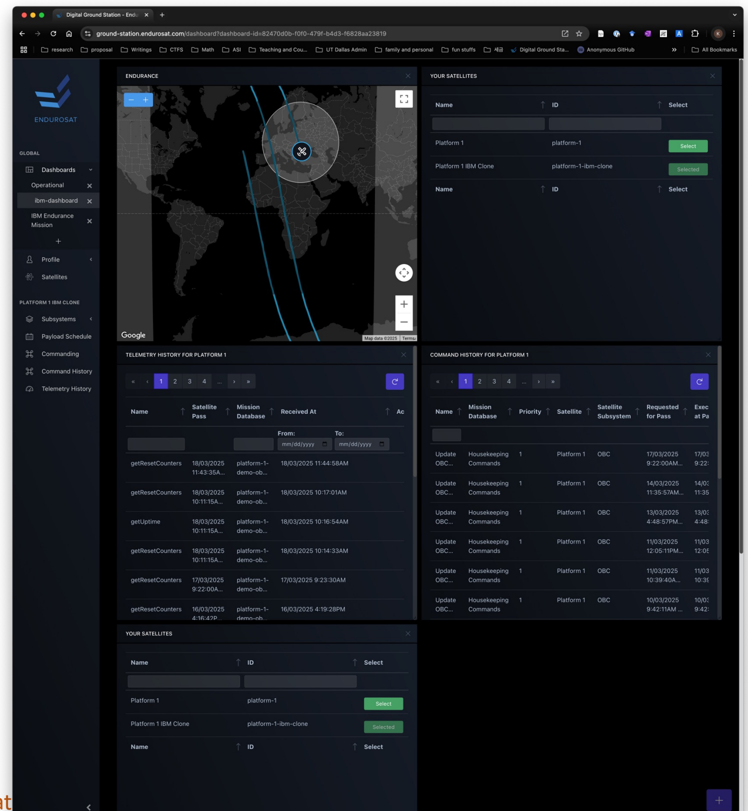
IBM Endurance Telemetry

Image source: EndureSat

Components	Data field	Data width	Type	Granularity
Attitude Determination and Control System (ADCS)	Magnetic Field Vector	6	int16_t MagFieldVec[3]	Formatted value in [uT] = MagFieldVec[x] * 0.01
	Coarse Sun Vector	6	int16_t CoarseSunVec[3]	Formatted value = CoarseSunVec[x] / 10000.0
	Fine Sun Vector	6	int16_t FineSunVec[3]	Formatted value = FineSunVec[x] / 10000.0
	Nadir Vector	6	int16_t NadirVec[3]	Formatted value = NadirVec[x] / 10000.0
	Rate Sensor Rates	6	int16_t AngRateArr[3]	Formatted value [deg/s]= AngRateArr[x] * 0.01
	Wheel Speed	6	int16_t WheelSpeedArr[3]	-
	Star{1..3}† Body Vector	6	int16_t Star{1..3}BVec[3]	Formatted value = Star{1..3}BVec[x] / 10000.0
	Star{1..3}† Orbit Vector	6	int16_t Star{1..3}OVec[3]	Formatted value = Star{1..3}OVec[x] / 10000.0
	Estimated Angular Rates	6	int16_t EstAngRateArr[3]	Formatted value [deg/s] = EstAngRate[x] * 0.01
	Estimated Quaternion Set	6	int16_t EstQArr[3]	-
	Satellite Position in ECI Frame	6	int16_t SatPosECI[3]	Formatted value [km] = SatPosECI[x] * 0.25
	Satellite Velocity in ECI Frame	6	int16_t SatVelECI[3]	Formatted value [m/s] = SatVelECI[x] * 0.25
Electronic Power System (EPS)	Battery [Capacity, Voltage, Current, Temperature]	[4, 4, 4, 4]	int32_t[4] battery_stats	-
6U Dove Solar Panel {1,2}‡	MCU Temperature	2	int16_t SunDataTemp	Formatted value [degC] = SunDataTemp * 0.1
	Main Temperature	2	int16_t TmpDataMain	Formatted value [degC] = SunDataTemp * 0.1
	External1 Temperature	2	int16_t TmpDataExt1	Formatted value [degC] = SunDataTemp * 0.1
	External2 Temperature	2	int16_t TmpDataExt2	Formatted value [degC] = SunDataTemp * 0.1

How My First Mission Crashed

- Could not schedule and run the experiments
  - Unstable communication, hard to schedule an experiment
  - Time synchronization problem
- No common bases for payload operations
  - Ad-hoc implementation for per-mission basis
  - Found many non-sensual design decisions
- And many many more …

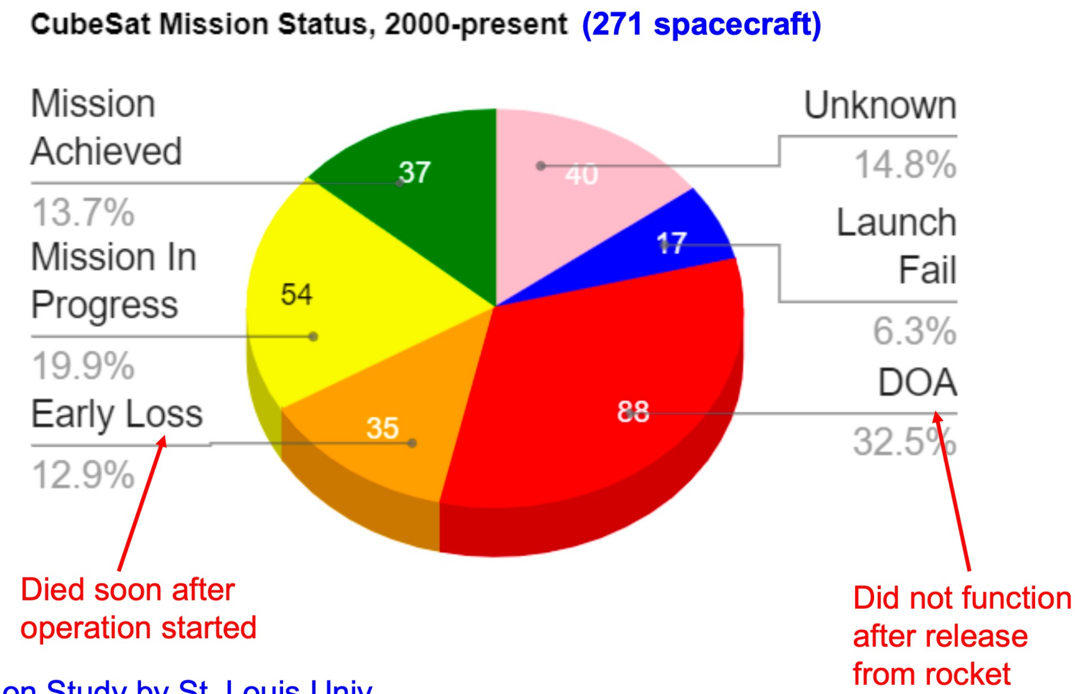


How My First Mission Crashed

- Communication is very thin and unstable
  - Return rate 10 % ~ 20 %
  - High frequency band communication are sensitive and power greedy
    - X-band communication not activated
- Powers are very scarce
  - Short charging time; insufficient battery capacity
  - Need to budget wisely among: ADCS, communication, and payload operation
- Difficult (almost impossible) maintenance operation
  - OBC software mostly in-house and ecosystem is largely fragment
  - Open-source solutions are too heavy-weighted or not well maintained
    - E.g., NASA cFS

This is a Community Issue

Failure rate is about 50%



Based on Study by St. Louis Univ.
https://sites.google.com/a/slu.edu/swartwout/cubesat-database

Space Research Opportunities

- Launch cost dropped (and will drop) over time
- COTS components and open-source software stacks
- Unclear legal and regulatory guidelines
  - Many recommendations but few enforcements
- What will be the killer application for space (or LEO)?

Two Research Ideas

1. Small Satellites Under Space Influence
   - Small satellites built with COTS components + open-source software stacks

2. Security and privacy of RF communications for satellites using amateur bands
   - Telemetry (downlink) and telecommands (uplink) communications cannot be obfuscated (or encrypted)
   - Due to outdated assumptions on amateur band users

CHAPTER VI – Provisions for services and stations RR25-1

ARTICLE 25

Amateur services

Section I – Amateur service

25.1 § 1 Radiocommunication between amateur stations of different countries shall be permitted unless the administration of one of the countries concerned has notified that it objects to such radiocommunications. (WRC-03)

25.2 § 2 1) Transmissions between amateur stations of different countries shall be limited to communications incidental to the purposes of the amateur service, as defined in No. **1.56** and to remarks of a personal character. (WRC-03)

25.2A 1A) Transmissions between amateur stations of different countries shall not be encoded for the purpose of obscuring their meaning, except for control signals exchanged between earth command stations and space stations in the amateur-satellite service. (WRC-03)

1.ITU-RR Article 25.2A (International Telecommunication Union Radio Regulations — binding worldwide)

LII Legal Information Institute About LII ▸ Get the law ▸ Lawyer directory

(iii) A control operator may accept compensation as an incident of a teaching position during periods of time when an amateur station is used by that teacher as a part of classroom instruction at an educational institution.

(iv) The control operator of a club station may accept compensation for the periods of time when the station is transmitting telegraphy practice or information bulletins, provided that the station transmits such telegraphy practice and bulletins for at least 40 hours per week; schedules operations on at least six amateur service MF and HF bands using reasonable measures to maximize coverage; where the schedule of normal operating times and frequencies is published at least 30 days in advance of the actual transmissions; and where the control operator does not accept any direct or indirect compensation for any other service as a control operator.

(4) Music using a phone emission except as specifically provided elsewhere in this section; communications intended to facilitate a criminal act; messages encoded for the purpose of obscuring their meaning, except as otherwise provided herein; obscene or indecent words or language; or false or deceptive messages, signals or identification.

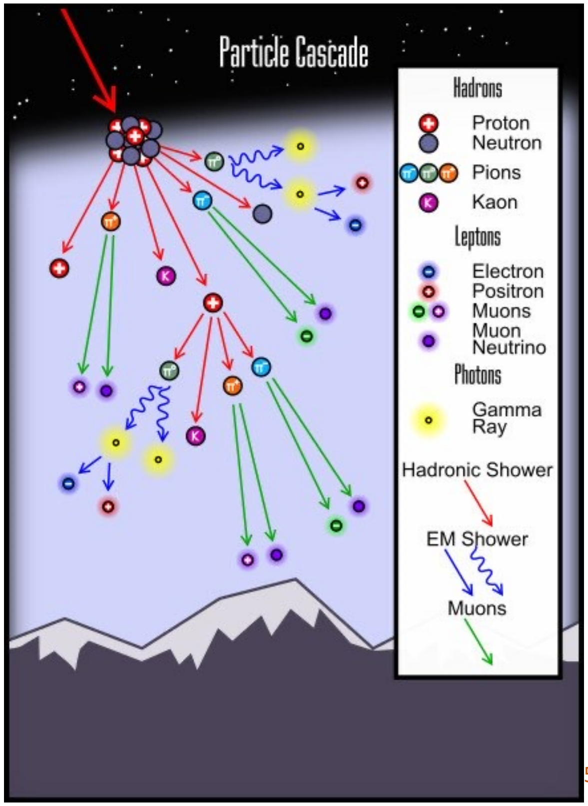
(5) Communications, on a regular basis, which could reasonably be furnished alternatively through other radio services.

2. FCC Part 97.113(a)(4) in the US

Small Satellites Under Space Influence

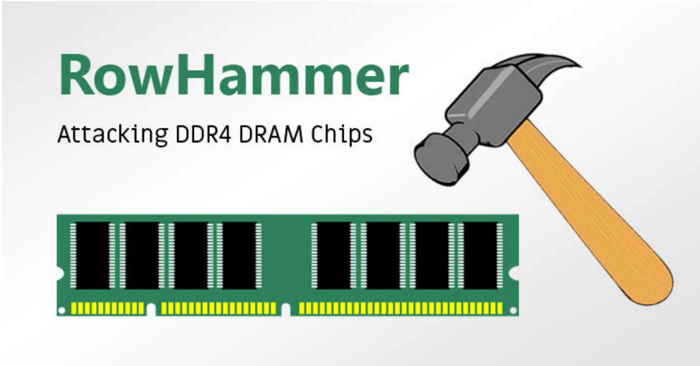
- Confirm and verify our assumptions cyber/digital components
  - DRAM?, SoC?, SD Cards?, HWRNG?
  - Open-source software stacks

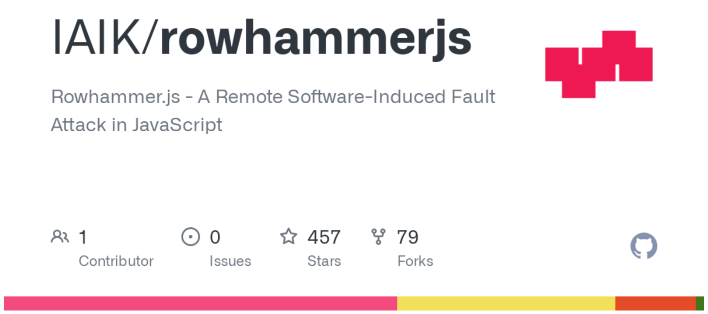
- CubeSat model for cyber security research
  - Running space software – e.g., NASA cFS framework
  - Emulating space mission tasks
  - End-to-end experiments and testing



RowHammer Attack

- First proposed by researchers in 2014
  - Kim et al. ICSA 2014
- One of prominent HW attack vectors
  - Spectre, MeltDown and RowHammer
- Google Project Zero actualized the attack 2015
  - Gain kernel privileges
  - Hypervisor escape
- Created high-severity practical threats
  - Javascript level attack from the browser
  - Mobile phone take over
  - ….





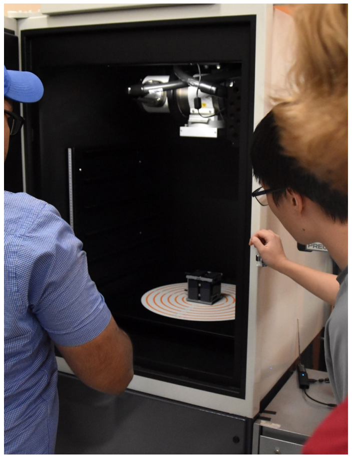
Robustness and Stability of COTS Components

- Evolving space practice
  - Based on heritage components + COTS components
  - Based on COTS components + specially-designed/mission-specific devices

- Security-sensitive CPU features need to e tested
  - HWRNG: Hardware Random Number Generators
  - Crypto co-processors
  - CPU performance counters

Small Satellites Under Space Influence

- Space RQs
  - Q1: How can we emulate space influences?
  - Q2: What components would break first?
    - What would be the recipe to impact certain components?
    - What would be the recipe to trigger *software errors* (e.g., bitflips, SEU) while not taking permanent damages to the HW components
- What would be distribution of the software errors?
  - Are space software are designed and written to be resilient against such errors?



Satellite Communication

- UTD Ground stations
  - Operational and participating [crowdsourcing ground station network]
- Collecting downlink RF signals in Amateur bands aiming to
  - Improving demodulation performance
  - Decode/understand satellite telemetry items

UHF/VHF Ground station at residential area		
Frequency range	432~438 MHz	144~146 MHz
Gain	13.3 dBic	9.2 dBic
Polarization	Circular R.H./L.H	
VSWR	1.1	1.1
Front-to-Back (F/B)	15 dB	16 dB
Beamwidth	42°	60°
Impedance	50 Ω	
Power Rating	1000 W	
Weight	Approx. 8.7 kg (2 Antennas+Stacking Boom)	
Length	1.6 m	1.7 m
Radius of Rotation	1.7 m	
Connector	N-type	

(a) Ground station at residential area specification.

UHF/VHF Ground station at UTD Campus		
Frequency range	420~440 MHz	144~146 MHz
Gain	15.2 dBic	13 dBic
Polarization	Circular R.H/L.H	
VSWR	1.5 (Measured: 1.9)	1.5 (Measured: 1.8)
Front-to-Back (F/B)	20 dB	20 dB
Beamwidth	25°	32°
Impedance	50 Ω	
Power Rating	250 W	
Weight	Approx. 12 kg (2 Antennas+Stacking Boom)	
Length	4.45 m	5.7 m
Radius of Rotation	3.9 m	
Connector	N-type	

(b) Ground station at UTD Campus specification.

Satellite Communication

- RF communications
  - De facto route open to user and the attacker
  - Channel between ground station and spacecraft
- Private bands are expensive and limited
  - Public frequencies reserved for amateurs and research groups
  - Cannot obfuscate (or encrypt) the traffic by regulation
- May contain information (telemetry) critical for satellite operations

Components	Data field	Data width	Type	Granularity
Attitude Determination and Control System (ADCS)	Magnetic Field Vector	6	int16_t MagFieldVec[3]	Formatted value in [uT] = MagFieldVec[x] * 0.01
	Coarse Sun Vector	6	int16_t CoarseSunVec[3]	Formatted value = CoarseSunVec[x] / 10000.0
	Fine Sun Vector	6	int16_t FineSunVec[3]	Formatted value = FineSunVec[x] / 10000.0
	Nadir Vector	6	int16_t NadirVec[3]	Formatted value = NadirVec[x] / 10000.0
	Rate Sensor Rates	6	int16_t AngRateArr[3]	Formatted value [deg/s]= AngRateArr[x] * 0.01
	Wheel Speed	6	int16_t WheelSpeedArr[3]	-
	Star{1..3}† Body Vector	6	int16_t Star{1..3}BVec[3]	Formatted value = Star{1..3}BVec[x] / 10000.0
	Star{1..3}† Orbit Vector	6	int16_t Star{1..3}OVec[3]	Formatted value = Star{1..3}OVec[x] / 10000.0
	Estimated Angular Rates	6	int16_t EstAngRateArr[3]	Formatted value [deg/s] = EstAngRate[x] * 0.01
	Estimated Quaternion Set	6	int16_t EstQArr[3]	-
	Satellite Position in ECI Frame	6	int16_t SatPosECI[3]	Formatted value [km] = SatPosECI[x] * 0.25
	Satellite Velocity in ECI Frame	6	int16_t SatVelECI[3]	Formatted value [m/s] = SatVelECI[x] * 0.25
Electronic Power System (EPS)	Battery [Capacity, Voltage, Current, Temperature]	[4, 4, 4, 4]	int32_t[4] battery_stats	-
6U Dove Solar Panel {1,2}‡	MCU Temperature	2	int16_t SunDataTemp	Formatted value [degC] = SunDataTemp * 0.1
	Main Temperature	2	int16_t TmpDataMain	Formatted value [degC] = SunDataTemp * 0.1
	External1 Temperature	2	int16_t TmpDataExt1	Formatted value [degC] = SunDataTemp * 0.1
	External2 Temperature	2	int16_t TmpDataExt2	Formatted value [degC] = SunDataTemp * 0.1

Small Satellite + Cybersecurity

- European Space Agency (ESA) is actively engaging in cybersecurity
  - Compared to NASA

2023 IEEE Symposium on Security and Privacy (SP)

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

2023 IEEE Symposium on Security and Privacy (SP) | 978-1-6654-9336-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/SP46215.2023.10351029

***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 against satellite firmware. We then conduct an experimental security analysis of three real-world satellite firmware images. We base our analysis on a set of real-world attacker models and find several security-critical vulnerabilities in all analyzed firmware images. The results of our experimental security assessment show that modern in-orbit satellites suffer from different software security vulnerabilities and often a lack of proper access protection mechanisms. They also underline the need to overcome prevailing but obsolete assumptions. To substantiate our observations, we also performed a survey of 19 professional satellite developers to obtain a comprehensive picture of the satellite security landscape.

***Index Terms*—satellites, satellite security, space segment, satellite firmware, threat taxonomy, software security**

1. Introduction

Satellites are sophisticated technical devices that are placed in outer space for research purposes or to provide terrestrial applications with services that leverage the coverage of the Earth's surface. While the first satellite, *Sputnik*, dates back to 1957, we are in the midst of a renaissance of spaceflight referred to as *New Space Era* [1]. Especially in recent years, we have observed an enormous growth in the number of earth-orbiting satellites. According to the United Nations Office for Outer Space Affairs (UNOOSA), their number has almost doubled from 4,867 in 2019 to 9,350 in 2022 [2]. The vast majority of these satellites form mega-constellations like *Starlink*, which plans to launch more than 40,000 satellites in the coming years [3].

Small satellites [4] are at the heart of this *New Space Era* as their size and the widespread use of Commercial off-the-shelf (COTS) components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications (like Earth observation, machine-to-machine communication, and Internet services) to research applications, such as technology testing, weather and earthquake forecasting, and even interplanetary missions [5]–[8].

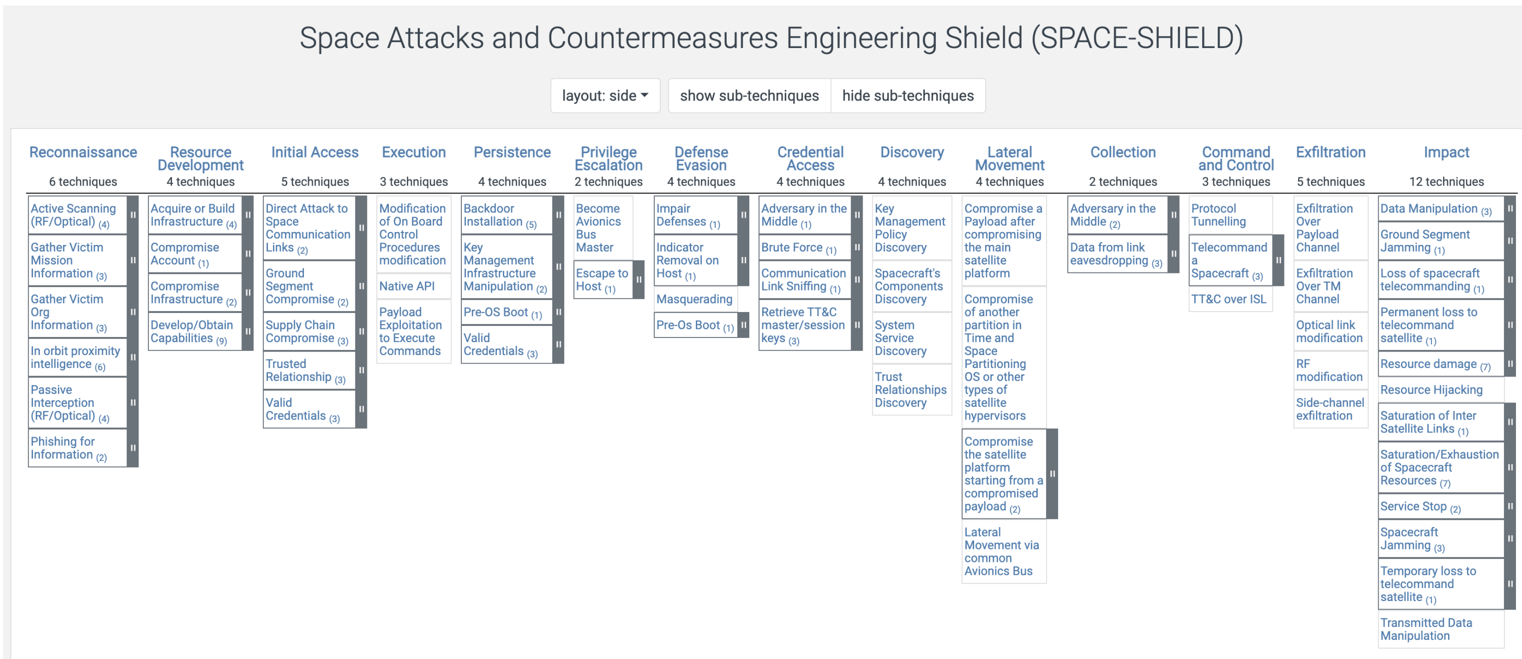
Although their applications vary widely, small satellites commonly consist of radio equipment and microcontroller boards. Hence—in the broadest sense—they are computer systems connected to a ground station on Earth and, sometimes, even to other satellites. Because they rely on wireless connections for command and control and use microcontrollers, they are potentially as vulnerable to attacks as any other connected IT platform on Earth.

This issue has not been very relevant in the past, since access to ground stations was expensive and limited to large satellite operators. However, the situation changed fundamentally in recent years. Nowadays, ground stations are even affordable for private individuals and with the emergence of Ground Station as a Service (GSaaS) models, such as those offered by *Amazon Web Services* [9] and *Microsoft Azure* [10], the entry barrier becomes even lower. We have seen in the mobile network security domain how the providers' assumption that the radio equipment required for attacks would be too costly and out of reach for attackers was ultimately disproved by technological advances [11]. Similarly, affordable ground stations create a novel attack surface, where adversaries can communicate with satellites and take advantage of software vulnerabilities. If they successfully compromise the satellite's firmware, they can access the satellite and potentially take complete control of the system.

Despite warnings being made early [12], little has been done to address this problem for several reasons, as Falco [13] points out. While the lack of security standards

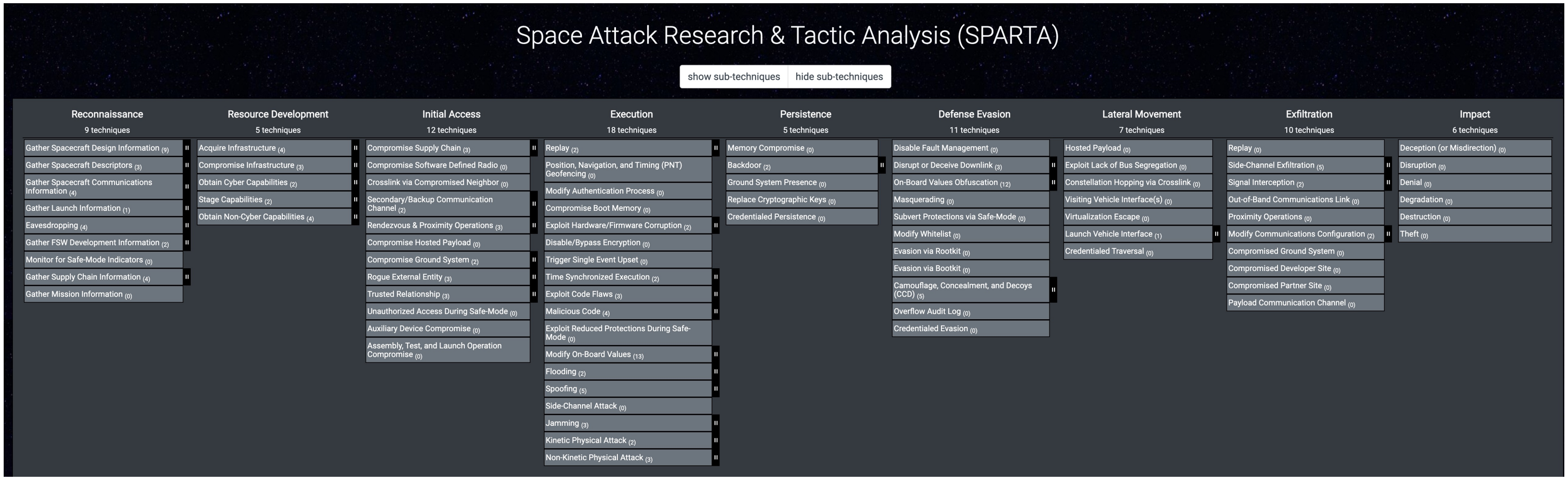
DOI 10.1109/SP46215.2023.00131

Space Attack Vectors (SPACE-SHIELD)



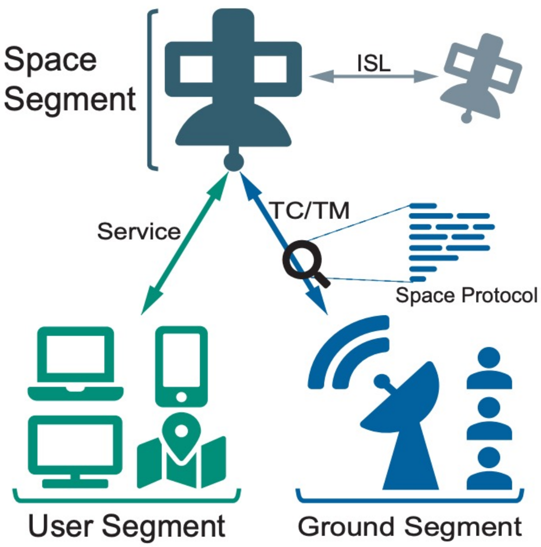
https://spaceshield.esa.int/

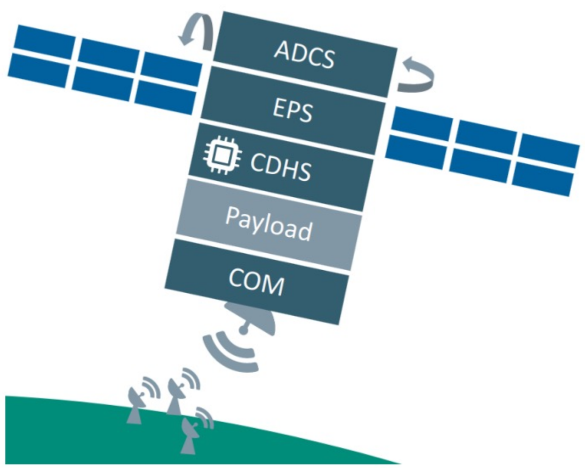
Space Attack Research and Tactic Analysis (SPARTA)



https://sparta.aerospace.org/

Space Security In Action





Research Objectives

- New space era, new operational practices
  - Widespread use of COTS components and open-source software stacks.
  - Are these systems secure and resilient against space-related challenges?
- RF communication as a critical attack surface
  - RF communication is vital for spacecraft operations.
  - However, its security and safety remain insufficiently verified.
- Testbed environment for small satellite research
  - UTD's ongoing efforts focus on building expertise and establishing a comprehensive space testbed environment.

Thoughts on Space Threat Modeling

- Bridging aerospace and cyber communities
  - Difficult in U.S.: cultural reasons, security clearances
- Highly inter-disciplinary research
  - Collaborative effort is must
- Different views to see the research problems
  - Similar to old days of computing
    - Micro computers vs. mainframe
    - Early days of Internet
- Can't think of *killer*-applications

Conclusion

- Space is expanding
  - Rapidly dropping launch cost, shrinking technology
  - Increasing privatization of space activities
- Gap between aerospace and cyber security sectors
  - Aerospace remains cautious in adopting new technologies
- The UTD team's commitment to space and security research
  - Development of the IBM Endurance CubeSat.
  - Establishment of UHF/VHF ground stations.
  - NSF-supported small satellite workshop.

Backup

Small Satellite Workshop

- Three-day program with 19 participants
  - 17 UTD students from diverse backgrounds
  - 2 graduate students from KAIST
  - University press release
  - Workshop website

- Supported by NSF (#2321117)
  - “CyberTraining:Pilot:CyberTraining for Space CI in Low Earth Orbit (LEO)”

- Interdisciplinary effort
  - Cybersecurity, material science, computational algorithm

Day 1 Schedule

Time	Sessions	Description
Day 1: Monday, June 10, 2024, **Location:** FO 2.208		
08:30 – 10:00 AM	Session 1	Opening remark and workshop logistics (8:30 ~ 9:00 AM) • Dr. Ovidiu Daescu & Dr. Kangkook Jee Guest lecture (9:00 ~ 10:00 AM) • Speaker: Kuang-Han Ke (Gran Systems CEO) • Title: The Road to Mass-produced CubeSat - Lessons Learned from our Mission
10:30 – 11:00 AM	Break	
11:00 – 12:30 AM	Session 2	Introduction to small satellite in LEO (Dr. Kangkook Jee) • Introduction to basic concepts • Small satellite operational lifecycles
12:30 – 1:30 PM	Lunch	
1:30 – 3:00 PM	Session 3	Small satellite components (Dr. Kangkook Jee) • CubeSat design and specification overview • Basic components for small satellite (CubeSat)
3:00 – 3:30 PM	Break	
3:30 – 5:00 PM	Session 4	[Hands-on] Building your own CubeSat I (Jaehyun Park, Ron Dang) • CubeSatSim v1.3 o Introduction (building guide) o Hardware component assembly o Software image installation

- Student group
  - 6 groups 3 ~ 4 students per group
- Basic concept intro
- Start hands-on building

Day 2 Schedule

Time	Sessions	Description
Day 2: Tuesday, June 11, 2024, **Location:** FO 2.208		

08:30 – 10:00 AM	Session 1	Guest speaker: Jessica Thompson, US Space Force
		
		[Hands-on] Building your own CubeSat II
		• Ground station set-up
		  ○ Hardware component assembly
		  ○ Software Image setup
		• RF Communication between CubeSatSim and Ground station

10:30 – 11:00 AM	Break	
11:00 – 12:30 AM	Session 2	Satellite software and programming interface (Dr. Kangkook Jee) • On-Board Computer (OBC) and ground system overview and programing interface • Commercial and open-source solutions • **Lab challenge 1, 2, 3**
12:30 – 1:30 PM	Lunch	
1:30 – 3:00 PM	Session 3	Basic RF transmission and antenna theory (Dr. Kangkook Jee) • Modulation and Demodulation • Space RF communication • SDR programming intro
3:00 – 3:30 PM	Break	
3:30 – 5:00 PM	Session 4	[Hands-on] CubsatSim communication competition • **Lab challenge 4**

- Guest lecture: Jessica Thompson, US Space Force
- Finish building CubeSatSim
  - Conduct lab challenges
- Session on
  - Satellite software systems
  - RF communication

Day 3 Schedule

Time	Sessions	Description
-	Day 3: Wednesday, June 12, 2024, **Location:** NSERL, RL 3.204 (Session 1), FO 2.208 (Session 3, 4)	
08:30 – 10:00 AM	Session 1	Introduction to CHESS research (Dr. Manuel Quevedo-Lopez) Physical and structural considerations (Dr. Francisco Aguirre) • Small satellite form factors o Shielding and insulations • Launcher and launch time considerations
10:30 – 11:00 AM	Break	
11:00 – 12:30 AM	Session 2	[Hands-on] Experimenting CubeSatSim under X-ray radiations
12:30 – 1:30 PM	Lunch (ROW)	
1:30 – 3:00 PM	Session 3	Space debris and De-orbit systems (Dr. Ovidiu Daescu) • Space and orbital debris • Space governance • De-orbit systems
3:00 – 3:30 PM	Break	
3:30 – 5:00 PM	Session 4	Workshop closing (Dr. Kangkook Jee) • Student discussion • Participant survey • Closing remarks

- Different location NSERL @ ROW building
- Physical and structural considerations
- Session environmental influences on spacecraft
  - E.g., temperature variation, excessive radio exposures
- Session on space debris and de-orbiting mechanisms

Participants

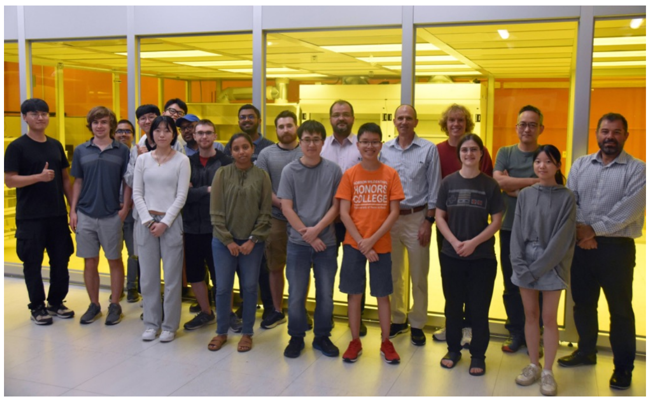
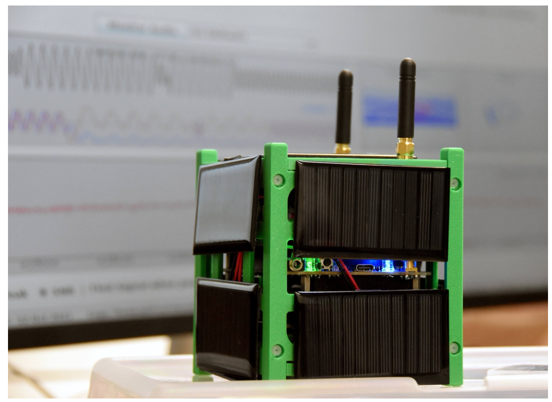
- Student demographics

Program	Female	Male	Sum
Biomedical engineering	1		1
BS Mechanical Engineering, MS Systems Engineering & Management	1		1
Computer Engineering	1		1
Computer Science	1	9	10
Electrical Engineering		1	1
Materials Science and Engineering		2	2
Physics		1	1
Software Engineering		1	1
Telecommunication Engineering	1		1
Total	5	12	19

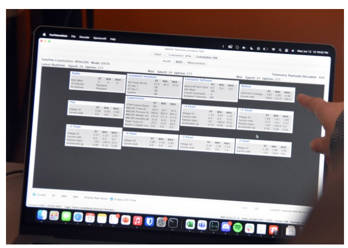
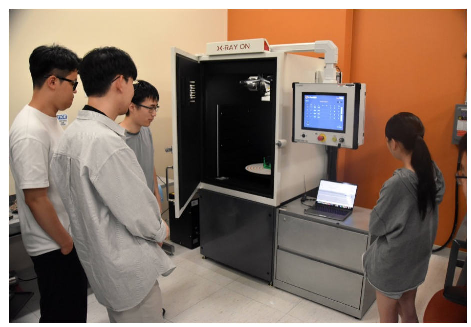
Program	Bachelor	Master	Ph.D.	Sum
Biomedical engineering	1			1
BS Mechanical Engineering, MS Systems Engineering & Management		1		1
Computer Engineering	1			1
Computer Science	5	4	1	8
Electrical Engineering			1	1
Materials Science and Engineering		1	1	2
Physics			1	1
Software Engineering	1			1
Telecommunication Engineering			1	1
Grand Total	8	6	5	19

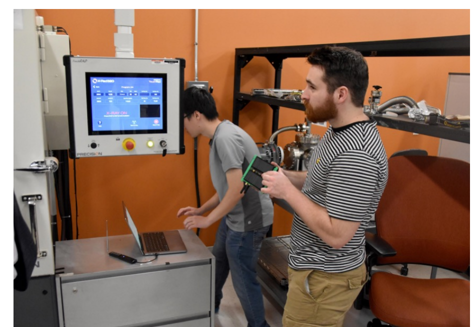
- Two International participants!

Small Satellite Workshop





Workshop Outcomes and Plan

- Resources and infrastructures
  - CubeSat Model
    - Extending AMSAT's CubeSatSim
  - Research and education/training infrastructure
    - UHF/VHF Ground stations
    - X-ray radiation chamber
  - Education/Training materials
- Future plan
  - Annual space *security* workshop
  - Course design
  - Community outreaches

Research Problems

- Proper testbed environment*
  - In-orbit (preferred) or terrestrial
  - Small satellites/CubeSats are toys
- Conferences/Workshop support
  - Between cyber and aerospace communities
  - Strict requirements for citizenship and security clearance
- Access to space computing devices and testing environment
  - Legacy software and hardware components
  - Radiation testing environment