Instructor:

Gregory Falco, Assistant Professor, Department of Civil & Systems Engineering, Institute for Assured Autonomy, falco@jhu.edu, cell: 917-494-1053

Office Hours:

By appointment, as indicated in class, or Virtual on Wednesday 9PM

Response Policy:

Students can expect a response to email within 24 hours. Alternatively, if urgent, students may text me at the above number with a quick question or request a call. I will respond upon checking my phone.

Course Goal

To identify and describe current challenges specific to space systems in the context of its cybersecurity and then apply mitigation techniques that are realistic within the constraints of space assets and their supporting infrastructure to help enable the security of space system operations.

Course Objectives

By the end of the course, students should be able to:

- Engineer an attack against a space system using methods and frameworks discussed in class.
- Explain the motivations of attackers, the unique security challenges of space systems and the expansive space system surface areas that attackers are interested in as both targets and vectors.
- Identify opportunities to infuse practical, implementable low-hanging fruit security practices into space system development processes.
- Articulate future space system capabilities and propose how these assets and their services will need to be secured.
- When This Course is Typically Offered
- This course is typically offered in the fall term at the Homewood campus as a Virtual Live class, where there is an option to participate remotely.

Course Outline

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
1	Sept 1	Who cares about space systems?	In this module we introduce the appeal of space	By the end of this module you will be able to:	Falco, Gregory. "Cybersecurity principles for

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
			systems to attackers. Then we describe the various threat actors for space systems. I’ll conclude by describing why space system security is different than IT security or other practices of cybersecurity.	1.1. Discuss threat actors and their motivations 1.2. Articulate why space system security is unique from IT security 1.3. Apply your understanding of threat actors by identifying and summarizing a potential type of attack against space systems	space systems." Journal of Aerospace Information Systems 16.2 (2019): 61-70.
2	Sept 8	Cyber 101	In this module we introduce key terminology in cybersecurity. Then we describe the broader cybersecurity landscape. We will conclude with a discussion of parallel industries of concern for cyber.	By the end of this module you will be able to: 1.4. Discuss some of the general challenges of cyber security 1.5. Articulate the systemic nature of cyber risk 1.6. Apply your understanding of space system issues in the context of other sectors’ technologies.	Visner, Samuel S., and Scott Kordella. "Cyber Best Practices for Small Satellites." ASCEND 2020. 2020. 4013.
3	Sept 15	What can be attacked?	In this module we introduce the various ways that attackers can disrupt space systems. Then we describe the surface area of attack for space systems. We will conclude with a discussion of attack vectors and targets.	By the end of this module you will be able to: 1.7. Discuss harms that can be caused to space systems due to cyber incidents 1.8. Articulate the architectural components of space systems	CENTRA Technology Inc. “Cyber Content of Satellites." 2017.

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
				and their appeal for attack 1.9. Apply your understanding of space system attack surfaces by identifying relevant attack vectors	
4	Sept 22	What cybersecurity standards and resources exist?	In this module we introduce the NIST cybersecurity framework. Then we discuss vulnerabilities and weaknesses for digital assets. We will conclude with a discussion on the applicability to space systems.	By the end of this module you will be able to: 1.10. Describe the nature of the NIST cybersecurity framework. 1.11. Articulate how one engages with vulnerability and weakness databases. 1.12. Apply your understanding of space systems and describe what existing cybersecurity standards apply and what do not.	Shackelford, Scott J., et al. "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices." Tex. Int'l LJ 50 (2015): 305. APA
5	Sept 29	How do hackers think?	In this module we introduce attack methodology. Then we describe frameworks available to describe attacks against systems. We will conclude by introducing tools to enumerate attack methods.	By the end of this module you will be able to: 1.13. Discuss attack strategy and an attacker’s approach 1.14. Articulate how the various security technical frameworks apply (or don’t) to space systems 1.15. Apply your understanding of space system	Schneier, Bruce. "Attack trees." Dr. Dobb’s journal 24.12 (1999): 21-29.

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
				attack methods by using the available tools	
6	Oct 6	What guidance is out there for space?	In this module we introduce space system security policy guidance in place today. Then we describe applicable standards. We will conclude by introducing policy recommendations on space systems.	By the end of this module you will be able to: 1.16. Discuss existing mechanisms to encourage space system security 1.17. Articulate some of the gaps in existing cybersecurity guidance 1.18. Apply your understanding of space system standards by identifying its interventive use	The White House. “Space Policy Directive –5 Cybersecurity Principles for Space Systems.” 2020.
7	Oct 13	Midterm Presentations	In this module we will learn about a unique space cybersecurity challenge from peers as part of the midterm oral report.	By the end of this module you will be able to: 1.19. Discuss a space cybersecurity issue in depth	N/A
8	Oct 20	Why does management matter for space system cybersecurity?	In this module we introduce the various stakeholder engaged in space systems that could impact the security. Then we discuss the supply chain of components of a space system. We conclude with an overview of supply chain threats to space systems.	By the end of this module you will be able to: 1.20. Discuss why space cybersecurity is not only a technical problem 1.21. Articulate who the stakeholders are that engage with space systems 1.22. Apply your understanding of	Falco, Gregory. "Job one for space force: Space asset cybersecurity." *Belfer Center, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School* 79 (2018).

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
				space system supply chain operations to deduce the security issues therein	
9	Oct 27	What are the ground segment threats?	In this module we introduce the merits of attacking a ground station. Then we discuss the components of a ground station that are vulnerable. We conclude with an overview of remediation techniques.	By the end of this module you will be able to: 1.23. Discuss why ground stations are attractive targets 1.24. Articulate the most vulnerable components of a ground station 1.25. Apply your understanding of security frameworks to ground stations	Manulis, M., et al. "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges." *International Journal of Information Security* (2020): 1-25.
10	Nov 3	What are the communication signal threats?	In this module we introduce the merits of attacking a communications signal. Then we discuss the components of a communication signal that are vulnerable. We conclude with an overview of remediation techniques.	By the end of this module you will be able to: 1.26. Discuss why communication signals are attractive targets 1.27. Articulate the most vulnerable components of a communications signal 1.28. Apply your understanding of security frameworks to communications signals	Pavur, James, and Ivan Martinovic. "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space." *2019 11th International Conference on Cyber Conflict (CyCon)*. Vol. 900. IEEE, 2019.

Module #	**Date**	**Module Title**	**Module Overview**	**Module Learning Objectives**	**Module Resources**
11	Nov 10	What are the space vehicle threats?	In this module we introduce the merits of attacking a space vehicle. Then we discuss the components of a space vehicle that are vulnerable. We conclude with an overview of remediation techniques.	By the end of this module you will be able to: 1.29. Discuss why space vehicles are attractive targets 1.30. Articulate the most vulnerable components of a space vehicle 1.31. Apply your understanding of security frameworks to space vehicles	Falco, Gregory. "When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience." *ASCEND 2020*. 2020. 4014.
12	Nov 17	What is the reality for space security implementation?	In this module we introduce the highly diverse approaches taken to security across civil, commercial and military space systems. Then we discuss limitations of security on certain systems. We conclude with describing incentives and disincentives for security on space systems.	By the end of this module you will be able to: 1.32. Discuss some of the current challenges to aligning security interests for space users 1.33. Articulate the limitations of space system security 1.34. Apply your understanding of security value propositions to evaluate security incentives	Bailey. B. et al. Defending Spacecraft in the Cyber Domain. Aerospace Corporation. 2019.
13	Dec 1	What are future threats?	In this module we will introduce emergent trends in space systems. Then we will discuss these trends in the context of their cyber threats. We will conclude with a guest lecture on this topic describing	By the end of this module you will be able to: 1.35. Discuss what is on the horizon for space system technology development	Baker, Cameron, and Hisham A. Kholidy. "Cyber Security Advantages of Optical Communications in SATCOM Networks." (2020).

Module #	Date	Module Title	Module Overview	Module Learning Objectives	Module Resources
			some highly practical examples of how the course content could be applied.	1.36. Articulate the potential security concerns of these future developments 1.37. Apply your understanding of security risk management to extrapolate how to pre-empt these future security risks	
14	Dec 15	Final Oral Report	In this module we will learn about a unique space cybersecurity challenge from peers as part of the midterm oral report.	By the end of this module you will be able to: 1.38. Discuss a space cybersecurity issue in depth	N/A

Student Assessment Criteria

Midterm Project	**30%**
Final Project	**40%**
Reflection Assessment	**10%**
Weekly Discussion Blog	**10%**
Course Participation	**10%**

Assignments

Two major projects – one at the midpoint of the course (Module 7) and one at the end of the course (Module 14). Students will be required to work in teams to effectively apply the tools and techniques presented in each half of the course. (70% of total grade / 30% for midterm, 40% for final project)

The midterm involves selecting a space systems security problem (after approval of the instructor) and conducting an exhaustive literature review on the topic. This will be presented to the class in a 10-minute oral presentation.

The final involves documenting a typical space system architecture, plot an attack against the space system (based on the midpoint project) and propose interventive measures to enable a resilient space system operations. The final report submission will include a block diagram and associated attack/defense tree associated with a 1-page memo describing the attack and resilience interventions. There will also be a 10-minute oral presentation of your memo and a 5-minute instructional video clip that you will be required to make and post online.

“Did You Know?” (Reflection Assessment)- Each module will contain a pass/fail 30-second “did you know” assignment where students will need to create a short video clip with something they learned/read over the week that was interesting about space system security and distinct from what their peers post. (10% of total grade)

Weekly discussion activities - students will be asked to participate in asynchronous weekly discussions on topics related to the module learning objectives on the class blog spacesecurity.ai. (10% of total grade)

Course Participation a brief summary of individual contribution to your midterm and final group projects. (10% of total grade)

Computer and Technical Requirements

Basic knowledge of either cybersecurity or space system components is highly recommended.

Participation Expectations

This is a highly interactive course where I aim to get to know each of my students through class discussions. I have had the privilege to help shape space cybersecurity guidance in the U.S. and I hope to bring much of the unique experiences I've had along the way to life in the classroom. I expect you to bring your own interesting stories and anecdotes to contribute to our discussions. While the course is highly participative, the majority of the course grade is composed of the midterm presentation/report and the final presentation/report both done in teams.

Late work

Late work will not be accepted unless an extension was granted. If an extension is needed, please set expectations appropriately and be reasonable with your request. Extensions should be requested ***before*** the due date. No extensions are permitted on the midterm or final assignment.