



Department of Mechanical and Aerospace Engineering  
FALL 2023

**ME-GY 6453: Security in Additive Manufacturing**

**Thursday, 5-7:30 pm (2 MTC 803)**

The course will cover the topics of security strategies in additive manufacturing (AM). A completely digital process chain is exposed to significant cybersecurity risks from internal or external malicious players for sabotage and intellectual property (IP) theft. Also, product counterfeiting is possible by reverse engineering. Such concerns require new security strategies that are unique to AM process chain. The course will cover threat models, security strategies and industrial scenarios related to security in AM. The course is divided into three modules.

The course is designed for MS students from MAE, ECE and CS departments, who are interested in AM or cybersecurity.

Week		Topic
		<b>Module 1: AM Threat Models and Attack Vectors</b>
Week 1	09/13	Introduction to Additive Manufacturing digital process chain
Week 2	09/20	Sabotage: IP theft and product sabotage
Week 3	09/27	Case study: product sabotage – detection of sabotaged designs
Week 4	10/4	Threat model development: aviation, defense, energy and medical sectors
<b>Week 5</b>	<b>10/12</b>	<b>Midterm exam/project 1: Threat model and solutions case study</b>
		<b>Module 2: Cybersecurity Tools in AM Process Chain and Supply Chain</b>
Week 6	10/18	Encryption, integrity
Week 7	10/25	Authentication
Week 8	11/1	Side channel information leakage
Week 9	11/8	Attend CSAW presentations
<b>Week 10</b>	<b>11/15</b>	<b>Midterm 2: Hack3D Challenge</b>
		<b>Module 3: Design-Based Approaches to AM Security</b>
Week 11	11/22	Design based security method
Week 12	11/29	Secure product design, printing, testing
Week 13	12/6	Embedded codes in AM parts, obfuscation and reading techniques
Week 14	12/13	Encryption of design files
<b>Week 15</b>	<b>12/20</b>	<b>Final project and presentation: Part design hacking and authentication</b>

The course prerequisite is graduate status. Undergraduate seniors may take it as elective with the permission from their undergraduate advisor and the instructor.

For more information, contact: Prof. Nikhil Gupta ([ngupta@nyu.edu](mailto:ngupta@nyu.edu))  
Prof. Ramesh Karri ([rkarri@nyu.edu](mailto:rkarri@nyu.edu))