Hackathon Problem: Digital manufacturing cybersecurity strategies for protecting valuable information in design files

Problem Statement

A digital manufacturing (DM) process chain requires the use of computers, network connectivity, and cloud systems. Industry 4.0 continues to evolve towards the digital transformation of manufacturing, leading to concerns of hacking for sabotage and intellectual property protection. The unique threats faced by DM are side-channel attacks, direct sabotage, reverse engineering, and counterfeit production.

The objective of this hackathon problem is to assess the robustness of security strategies to hide information in the design files for DM and stimulate the critical thinking process. An STL file of a model will be provided, and participants are to complete the objective by gathering as much evidence from the provided files to prove their conclusion. Teams would be required to present their solution approaches for completing each benchmark to a panel of judges.

Challenges

- How can security strategies be developed and incorporated into a DM cyber-physical system? [1]
- What is the optimal approach to test the effectiveness of developing security strategies and to account for every classification of attacks in the DM supply chain? [2]
- How can the cybersecurity threats be minimized in digital manufacturing?
- Is current 3D printing technology safe from threats?

Objective

You and your friends are traveling across the globe to multiple locations for summer vacation. One day, you discovered that your passport was missing, and you received a mysterious email containing a file. The anonymous sender requires you to solve the puzzle in the attachments to be able to find where your passport is located. You and your friends are only given 24 hours to locate your passport.

The STL file shows a 3D model of an object and there are five hints that are hidden throughout the files. Each hint that you can decode will get you closer to the location of the lost passport. Teams will receive points based on how many puzzles they can decode correctly and their method of solving the challenges.

Results submission table:

Hint #	The location provided by the hint	Brief description of the hint and solution method
1	?	
2	?	
3	?	
4	?	
5	?	

Judgment Criteria

Category	**Criteria**	**Scoring**
Results (60%): Output solution	• The objective is achieved by determining the exact GPS location of the passport • Clear and concise explanation of obtaining solution	Correctly determining: 12 points for each clue
Creativity (20%): A new direction in the field to approach the problem	• Derived solution through critical thinking • The approach is a major departure from other submissions • Team demonstrates creativity in solving each puzzle • Use of appropriate software to aide in problem solving	Excellent (9-10 pts) Very good (7-8 pts) Good (5-6 pts) Limited (3-4 pts) Poor (1-2 pts)

Overall presentation (20%): Organization, structure, and message conveying	• Title, headings, labels: Appropriate size, location, spelling, and content • The demonstration of teamwork • Structure and Clarity	Excellent (9-10 pts) Very good (7-8 pts) Good (5-6 pts) Limited (3-4 pts) Poor (1-2 pts)

Submission

1. The presentation slides describing the overall approach to obtain the solution for each benchmark and outlining the difficulties faced.
2. Each team will submit a zip file containing:
    a. A detailed word document which includes:
        i. The completed submission table from above
        ii. A description of the brainstorming process and each clue
        iii. A summary of any other approach attempted that may not have been successful to provide insight into your effort level and thought process.
    b. Any supplementary file to support your report (CAD/STL files, programming scripts, images)

Sample Data Set

Click for sample data set

References

1. Mahesh, P., et al., *A Survey of Cybersecurity of Digital Manufacturing.* Proceedings of the IEEE, 2021. **109**(4): p. 495-516.
2. Linares, M., et al. *HACK3D: Crowdsourcing the Assessment of Cybersecurity in Digital Manufacturing*. 2020. arXiv:2005.04368.
3. Practice problems and previous challenges are available at: https://www.csaw.io/hack3d

Subject Matter Experts and Mentors:

Nikhil Gupta, Professor, Department of Mechanical and Aerospace Engineering, New York University

Gary Mac, Ph.D. Candidate in Mechanical Engineering, Department of Mechanical and Aerospace Engineering, New York University

Hammond Pearce Postdoctoral Associate, Department of Mechanical and Aerospace Engineering, New York University