ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35681

Threat Vector Analysis - Finding Fault in the Pile

Mr. Caleb Ian-Watson Beckwith, CUNY New York City College of Technology

I am a Senior in mechanical engineering at the New York City College of Technology in Brooklyn New York. Over the past three years, I have worked with my school and several others both inside and outside of the US in order to research and learn more about Additive Manufacturing and how it is incorporated with the engineering supply chain and design process. This includes working with NYU over the summer as part of their NSF IRES summer research program with students from India to learn how cyber security plays a role in AM and how machine learning can be used to combat cyber/physical attacks,

ASEE Fall 2021 Middle Atlantic Conference
November 12-13, 2021

Threat Vector Analysis - Finding Fault in the Pile

Caleb Beckwith[1], Harsh Sankar Naicker[2], Svara Mehta[3], Viba R Udupa[4], Nghia Tri Nim[5], Varun Gadre[6], Hammond Pearce[7], Gary Mac[7]

1. NYC College of Technology, 300 Jay St, Brooklyn, NY 11201
2. Vellore Institute of Technology, Kelambakkam - Vandalur Rd, Rajan Nagar, Chennai, Tamil Nadu 600127, India
3. Indian Institute of Technology, Goa Engineering College Campus, Farmagudi, Ponda, Goa 403401, India
4. National Institute of Technology NH 66, Srinivasnagar, Surathkal, Mangalore, Karnataka 575025, India
5. New York University Abu Dhabi, Abu Dhabi, UAE.
6. Indian Institute of Technology Kanpur, Kanpur, Uttar Pradesh 208016, India.
7. New York University Tandon School of Engineering, 6 MetroTech Center, Brooklyn, NY 11201

Background

In the additive manufacturing (AM) supply chain, there are numerous factors that may allow malicious third parties to negatively influence the specific outcomes of a given product. These factors are known as threat vectors, and commonly include avenues for counterfeiting, information leakage, and sabotage.

For AM one such case where this applies is with G-Code files, and through machine learning, malicious files can be detected through feature recognition seeing how the altered ones deviate from the acceptable ones thus finding the fault(s) in the pile.

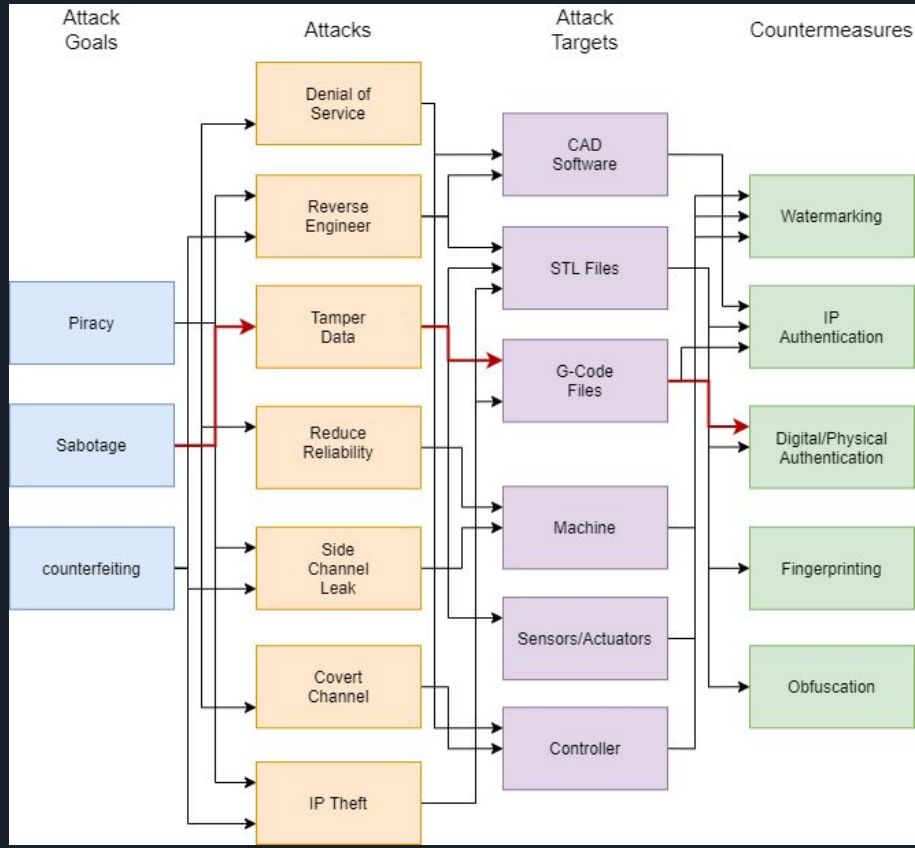

Figure 1: Threat vectors in additive manufacturing

Method of Attack

Two data sets of g-code files were prepared for the students to examine and find the defected files within.

The first dataset was composed of 180 files, two of which were compromised. The files were each rotated 1 degree from the original starting point about the Y-axis.

The Second dataset was composed of 4230 files, 60 of which were compromised. The model used was a bracket sliced in Ultimaker Cura.

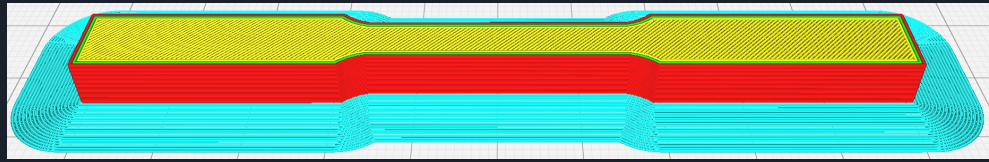

Figure 2. Tensile test specimen

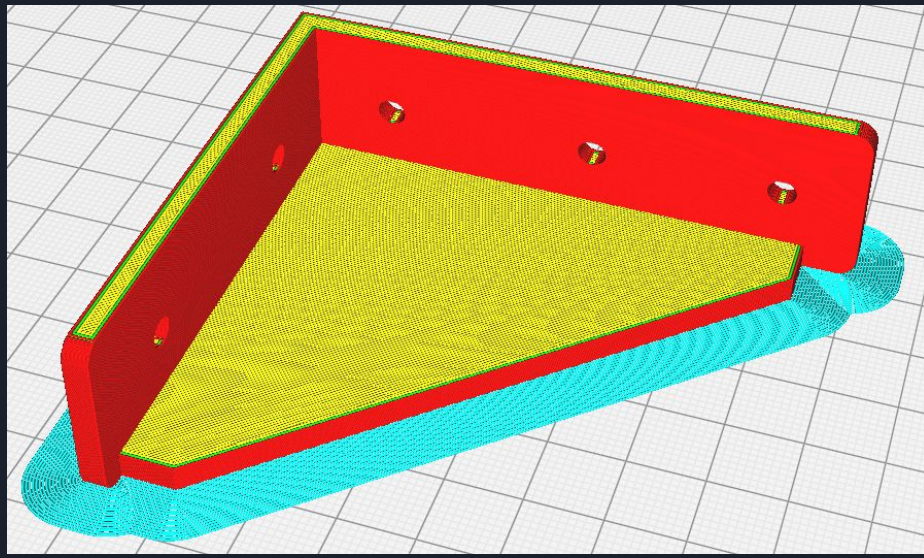

Figure 3. Bracket

Fault in the pile 180 codes

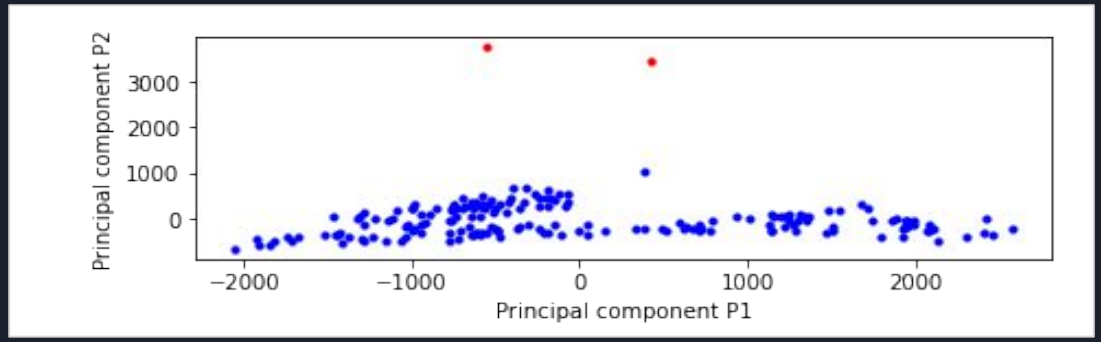

Figure 4. Scatter plot for Gcode showing principle component outliers

Three methods were created to find the faulty files:

- **Statistical Analysis Approach:** Broke the G-code into the individual commands and examined the count of each command as well as the decimal range of each input associated with the command.
- **Machine Learning Approach:** Used python to break down the data set and then performed principal component analysis to cluster the files to find outliers.
- **Combination Method:** Examined the files in much of the same way as the first two methods, finding the faulty files statistically and validating the files with machine learning using DBSCAN.

Fault in the pile 4320 codes

- Pure statistical analysis method was able to flag 50 files as potentially tempered. 29 of these files were shown to be correctly identified, and 21 were false positives.
- Pure machine learning method only detected 35 files, where 28 of those were correctly identified.
- Combined method detected 50 files correctly, DBSCAN validated the found files and ruled out potential false flags.

  Overall 50 out of the 60 damaged files were found.

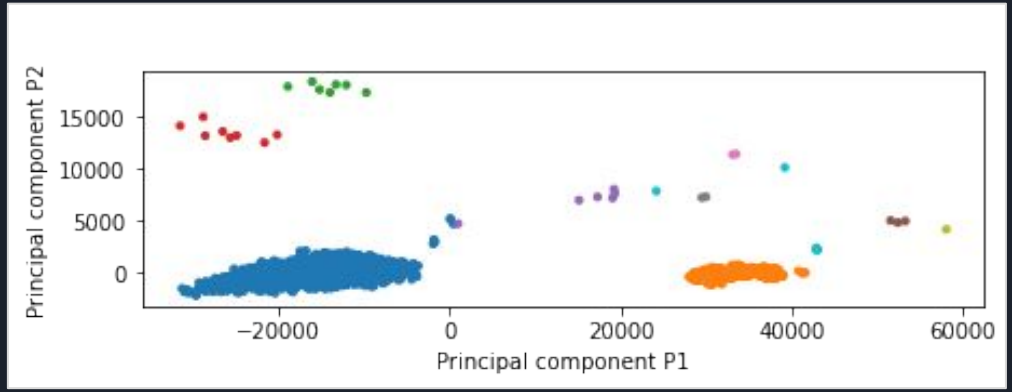

Figure 5. Principal component break down for sample set of 4320 files

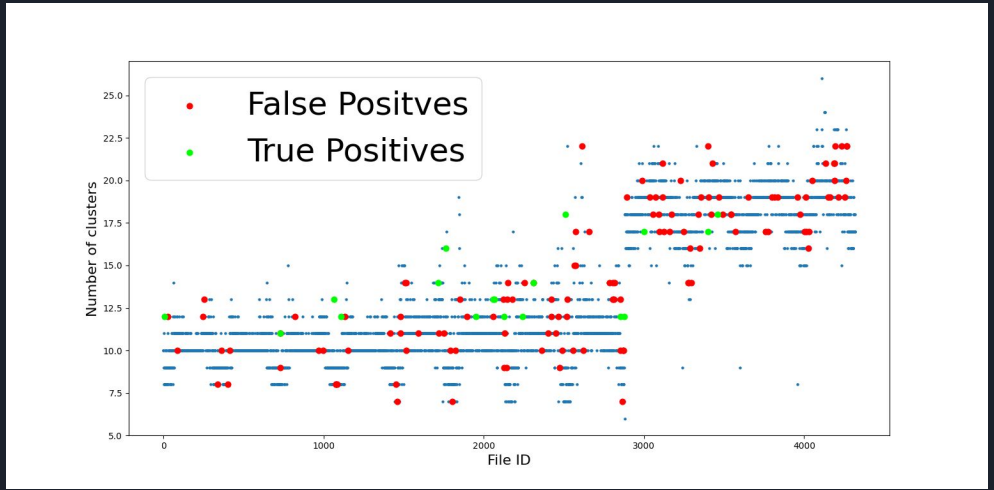

Figure 6. DBSCAN for 4320 files

Conclusion

Interdisciplinary undergraduate researchers were able to demonstrate methods of detecting faulty files through statistical analysis and machine learning such that it can be further developed and implemented as a method of cyber security for companies.

The methods used were able to correctly identify defects for small datasets but experienced difficulty scaling up to larger datasets with broader defect types.

Acknowledgments & Resources

Thank you to NYU Tandon as well as The National Science Foundation and the International Research Experience for Students (IRES) program for sponsoring this research and the students from outside of the USA to attend. The authors thank the professors and doctoral students who aided this research in providing information and resources for us to learn with.

1. Belikovetsky, Sofia, et al. “Cyber-Physical Attack with Additive Manufacturing.” *arXiv.org*, 2016, https://arxiv.org/abs/1609.00133. Accessed 31 07 2021.
2. Yampolskiya, Mark, et al. “Security of Additive Manufacturing: Attack Taxonomy and Survey.” Additive Manufacturing, 2018. https://www.osti.gov/servlets/purl/1502040.
3. Chen, Fei, et al. “Security Features Embedded in Computer Aided Design (CAD) Solid Models for Additive Manufacturing.” *Science Direct* , doi:https://doi.org/10.1016/j.matdes.2017.04.078.
4. N. Gupta, A. Tiwari, S. T. S. Bukkapatnam and R. Karri, "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks," in IEEE Access, vol. 8, pp. 47322-47333, 2020, doi: 10.1109/ACCESS.2020.2978815.
5. S. Zafeiriou, A. Tefas and I. Pitas, "Blind robust watermarking schemes for copyright protection of 3D mesh objects," in IEEE Transactions on Visualization and Computer Graphics, vol. 11, no. 5, pp. 596-607, Sept.-Oct. 2005, doi: 10.1109/TVCG.2005.71.

NSF

NYU Center for Cybersecurity

iRES