Problem Domain

Additive Manufacturing--also known as “3D printing”--is the process of manufacturing three-dimensional objects from a digital model by depositing or solidifying material via a computer-controlled system. While Additive Manufacturing has a robust hobbyist community, it has also become increasingly important in industrial production processes; today, 3D printed parts have been put in the skies by Boeing and into space by SpaceX. However, as the prevalence of Additive Manufacturing grows in these complex and critical contexts, so too does the threat posed by compromise of these cyber-physical systems.

Perhaps the most famous hack of a cyber-physical system was the Stuxnet virus, which wreaked havoc on Iran's nuclear program by causing centrifuges to spin at their resonant frequencies until they ripped themselves apart in dramatic failure. Compromise of an Additive Manufacturing system has the potential to be far more insidious: structural weaknesses maliciously introduced into a 3D printed part may be small and escape notice at time of production, and yet have devastating consequences if they induce failure in the part while it is in use [1]. Approaches to protecting against Additive Manufacturing attacks include using external analog sensors to validate machine behavior [2][3].

[1] Logan D. Sturm, Christopher B. Williams, Jamie A. Camelio, Jules White, Robert Parker, “Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects”, in Journal of Manufacturing Systems, vol. 44, no. 1, pp. 18-25, 2017, doi: 10.1016/j.jmsy.2017.05007.

[2] S. Rokka Chhetri and M. A. Al Faruque, "Side Channels of Cyber-Physical Systems: Case Study in Additive Manufacturing," in IEEE Design & Test, vol. 34, no. 4, pp. 18-25, Aug. 2017, doi: 10.1109/MDAT.2017.2682225.

[3] Shih-Yuan Yu, Arnav Vaibhav Malawade, Mohammad Abdullah Al Faruque, “Multi-Modal Attack Detection for Cyber-Physical Additive Manufacturing”, in TC-CPS Newsletter, vol. 5, no. 1, Mar. 2020.

Threat Model

STRIDE model

Spoofing	● n/a (since manufactured parts are fungible by nature, “authenticity” attacks are equivalent to tampering)
Tampering	● Sabotage via introducing defects in manufactured parts

Repudiation	● Attacks not traceable via software logging (e.g., interacting directly with machine hardware)
Information disclosure	● Obtaining IP via: ○ Compromising any program in the process chain (CAD software, slicer, machine firmware) ○ Information leaked through side channels (acoustic, magnetic, power)
Denial of service	● Destroying machine via commands to operate outside safe parameters (may not be possible, depending on machine) ● Running machine without authorization to exhaust supplies of raw materials ● Bricking machine via malicious firmware
Elevation of privilege	● Using machine and supplies to produce parts without authorization

Attack tree