Solid Freeform Fabrication 2021: Proceedings of the 32nd Annual International Solid Freeform Fabrication Symposium – An Additive Manufacturing Conference
Reviewed Paper

Evaluation of a Cyber-Physical Attack Effectiveness in Metal Additive Manufacturing by Selectively Modifying Build Layer Thickness

*Patricio E. Carrion[1, 2], Lynne M. Graves[3], Mark Yampolskiy[1, 4, 5], Nima Shamsaei[1, 2, *]*

[1]National Center for Additive Manufacturing Excellence (NCAME), Auburn University, Auburn, AL 36849, USA

[2]Department of Mechanical Engineering, Auburn University, Auburn, AL 36849, USA

[3]School of Computing, University of South Alabama, Mobile, AL 36688, USA

[4]Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA

[5]Auburn Cyber Research Center (ACRC), Auburn University, Auburn, AL 36849, USA

*Corresponding author: shamsaei@auburn.edu

Abstract

To produce functional parts satisfying required functional characteristics, Additive Manufacturing (AM) process maintains a combination of numerous parameters within material-dependent ranges; these include power density, scanning speed, hatch distance, and layer thickness. Unintentional misconfiguration of these parameters is easily detectable as it impacts the entire build. In this paper, however, we consider the case of a deliberate sabotage attack which causes misconfiguration localized to only few strategically selected layers. We propose a method on how such targeted misconfigurations can be executed without hacking into the firmware. Specifically, we altered a build file to mimic localized layer thickness modification by disabling laser beam exposure, while maintaining geometrical and visual part integrity. For two distinct laser powder bed fusion (L-PBF) systems and two metal alloys, we validated empirically the impact of such attack on part quality and demonstrated that it can avoid detection by non-destructive techniques (NDT). The conducted attack illustrates susceptibility of AM to deliberate sabotage attacks and motivates the need of security solutions for this increasingly adopted manufacturing technology.

Keywords: Additive Manufacturing; Laser Powder Bed Fusion; AM security, Cyber-Physical Attack; Sabotage.

Introduction

Additive Manufacturing (AM) has numerous advantages, such as ability to manufacture parts of complex geometry, reduced lead times and material waste, and on-demand manufacturing of spare parts at a location where they are needed [1–3]. Therefore, AM is increasingly adopted by various industries, including the aerospace, defense, and biomedical sectors.

NIST classifies AM as a Direct Digital Manufacturing (DDM) technology, meaning that it fabricates physical objects from a digital design file using computer-controlled processes with little to no human intervention [4]. Because it relies so heavily on digital input files, in addition to the

digital control systems operating the AM machine itself, its security has been identified as a critical gap [4,5]. Security issues include *technical data theft*, *sabotage*, and *illegal part manufacturing* [6].

This paper focuses specifically on cyber-physical sabotage attacks, i.e., attacks which originate as a manipulation in the cyber domain and cause effects in the physical domain [7]. It should be noted that the effects of interest to an adversary are rarely achieved immediately but are rather a product of a complex causal chain of effect propagations [8]. In the AM context, sabotage attacks can target properties of manufactured parts (and thus of systems into which they are integrated), the AM machine itself, or the manufacturing environment [9]. The dr0wned study [10] has demonstrated that sabotage of a part is rather a means and not the end goal per see; in the study, a sabotaged propeller broke after a brief operation time causing fall and destruction of the quadcopter UAV on which it was installed.

Sabotage attacks are of especial importance for metal parts, because they are used in safety-critical systems. Currently, the most dominant AM process to manufacture net shape metal parts is Laser Powder Bed Fusion (L-PBF). Part sabotage on a L-PBF is the focus of this paper. We propose a novel method on how layer thickness, an essential PBF process parameter, can be modified locally without the need to compromise the 3D printer firmware. We employ this method to simulate an attack that selectively modifies a part's layer thickness using two difference L-PBF systems with different powder feedstocks, 316L and 17-4PH Stainless Steel (SS). We then verify both the ability of this attack to remain undetected by an X-ray computer tomography (CT) and to degrade part's tensile strength. Finally, we discuss the implications of the studied attack on the security posture in AM.

Related Work

Several publications survey the state of AM Security field as a whole [6,11,12]. Analysis of software, firmware, and communication protocols used by desktop 3D printers has identified numerous vulnerabilities that can be exploited for their compromise [13]. It has been demonstrated externally that external attackers can compromise manufacturing environment [10], run a malware on a compromised computer [14], hijack network communication with 3D printer [15], or compromise firmware of a 3D printer [16,17]. When compromised, any of these elements can then be used to conduct a broad variety of cyber- and cyber-physical attacks. Furthermore, several studies identified that the attack methods available to sabotage AM parts exceed those available for traditional manufacturing methods [18,19].

Most AM sabotage attacks has been performed on Fused Deposition Modeling (FDM) [6], an AM process that is predominantly used with polymers and widely adopted in low-cost desktop 3D printers. Introduction of random voids into a design file [14], selective substitution of print material through support structure material [20], manual modification of the design file [10], varying print orientation [20,21], changes of the extruded filament amount [17] or temperature [16], or even on-the-fly substitution of one print through an entirely different [17] – these are representative examples of methods used in part sabotage. All these attacks are of cyber-physical nature, i.e., manipulations in cyber domain case effect in physical domain[7]. The above-mentioned works focused on identification of new categories of attack methods that would lead to the degradation of part's tensile strength or fatigue life. For composite material parts it has been shown that sabotage attacks can also be optimized to minimize deviations from the original design while achieving the performance degradation level set by an adversary [22].

Only few publications have investigated sabotage attacks of metal AM. Several theoretical analysis papers identified direct attack methods for sabotaging parts manufactured with L-PBF. These include manipulation of numerous process parameters [21], disturbance of network communication timing [23], and fluctuations of power supply to 3D printer [18]. In our related work [24], we investigated how manipulations of the Powder Delivery System (PDS) can be used to sabotage parts and verified experimentally that such attacks can degrade part's fatigue life. Manipulation of L-PBF scanning characteristics (laser power and scan speed) has been used to define a part's failure point [25]. For the L-PBF systems integrating in-situ monitoring in a closed control loop to adjust laser power, it has been shown that manipulation of the sensor data can be used to impair the part's quality indirectly [26].

Experimental Set-up

Selective layer thickness via build file manipulation

Simulation and validation of the proposed method (i.e., localized layer thickness modification) was performed by fabricating and mechanically testing a set of round tensile specimens based ASTM standard E8 [27]. The geometry and dimensions of the tensile specimen is presented in **Figure 1**(a). The specimen can be destructively tested to experimentally evaluate the impact of the introduced layer thickness defect on function-related mechanical properties such as ultimate tensile strength and ductility (a detailed account of the tensile properties obtained is presented in the *Test methodologies* section).

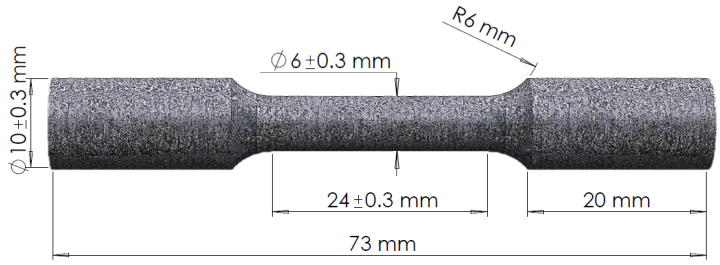
To introduce the layer thickness defect, we split the design of the specimen in three parts, top, bottom, and the cross-section located between the aforementioned parts (see **Figure 1**(b)). Since technically the design now consists of three individual parts stacked on top of each other, the process parameters for these parts can be selected/modified individually. We kept the default process parameters, including layer thickness, for both bottom and top parts. For the cross-section part, only the core laser exposure was set to zero power, meaning that the laser will still take time to traverse the scanning path while being turned off, therefore not melting powder. To conceal the attack and provide the appearance of a successful layer deposition, the contouring laser pass of the cross-section part was still performed with the recommended laser parameters. Furthermore, to maintain the overall specimen length (indicated in **Figure 1**(a)) while varying the cross-section part thickness, the bottom part size was kept constant while the top part was reduced in length. As a result, the specimen's critical location was targeted using the cross-section part, which may contain an arbitrary number of layers of unmelted powder.

Build layout design & specimen fabrication

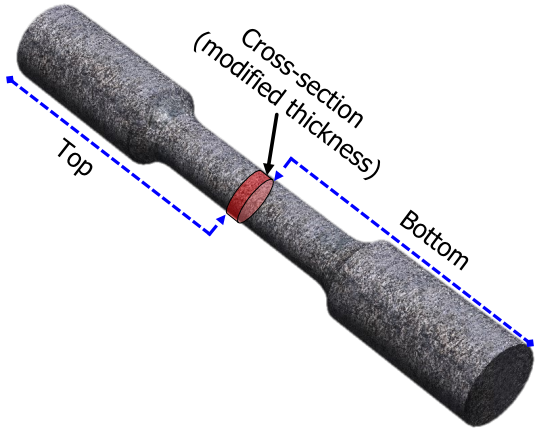
To test the impact of the layer thickness defect on mechanical performance, we used three categories of specimen modification: (i) single part design, hereinafter referred to as "default", (ii) a three part specimen design (discussed in the previous section and shown in **Figure 1**(b)) with a cross-section length corresponding to one layer thickness per the recommended process parameters of the powder feedstock being used, hereinafter referred to as "1-layer", and (iii) a three part specimen design with a cross-section length corresponding to two times the layer thickness of the recommended process parameters, hereinafter referred to as "2-layer". The former (default specimen) is used establish baseline mechanical properties. The latter two (1-layer and 2-layer) are used to study impact of the introduced layer thickness defect.

The build file created was used to fabricate specimens using two L-PBF systems, a dual-laser GE Concept Laser M2 (GE M2), and a single-laser EOS M290. Furthermore, two metal

powders were selected for each machine, 3l6L and 17-7PH stainless steel (SS), respectively. Both materials had similar powder size distributions ranging between 15–45µm and the same recommended layer thickness of 40µm. Extra details on other process parameters and powder feedstock properties maybe found in [24]. The specimens were manufactured vertically, using previously recycled metal powder. The recycling/reconditioning procedure used may be found in [28]. Schematics of the build layout, including the recoater arm direction and inter gas flow with respect to specimen location, for the GE M2 and EOS M290 systems are presented in **Figure 2**(a) and (b), respectively. Additionally, as can be seen in **Figure 2**(a), the specimens were divided in two groups, front (green colored) which were fabricated using one laser, while the ones located on the back (red colored), were fabricated with the secondary laser. For specimens fabricated with EOS M290, shown in **Figure 2**(a), the build layout was kept the same and it can be seen that the recoater direction and niter gas flow are perpendicular to each other.



(a)



(b)

Figure 1. (a) Round tensile specimen size and geometry designed based on ASTM standard E8 [27]. (b) Three-part split of the original design to simulate the selective layer thickness defect (i.e., layer skip location).

After fabrication and built plate removal, the 316L SS specimens were tested without any post-processing, i.e., as-built surface condition. The 17-4 PH SS specimens were subjected to a CA-H1025 heat treatment procedure after we removed them from the built plate. This heat-treatment was selected to increase the strength of the material, which will provide a comparison between a ductile (316L SS) and brittle (17-4PH SS) material behavior [24]. No further processing

was performed after heat treatment; hence, 17-4 PH SS specimens were tested in the as-built surface condition.

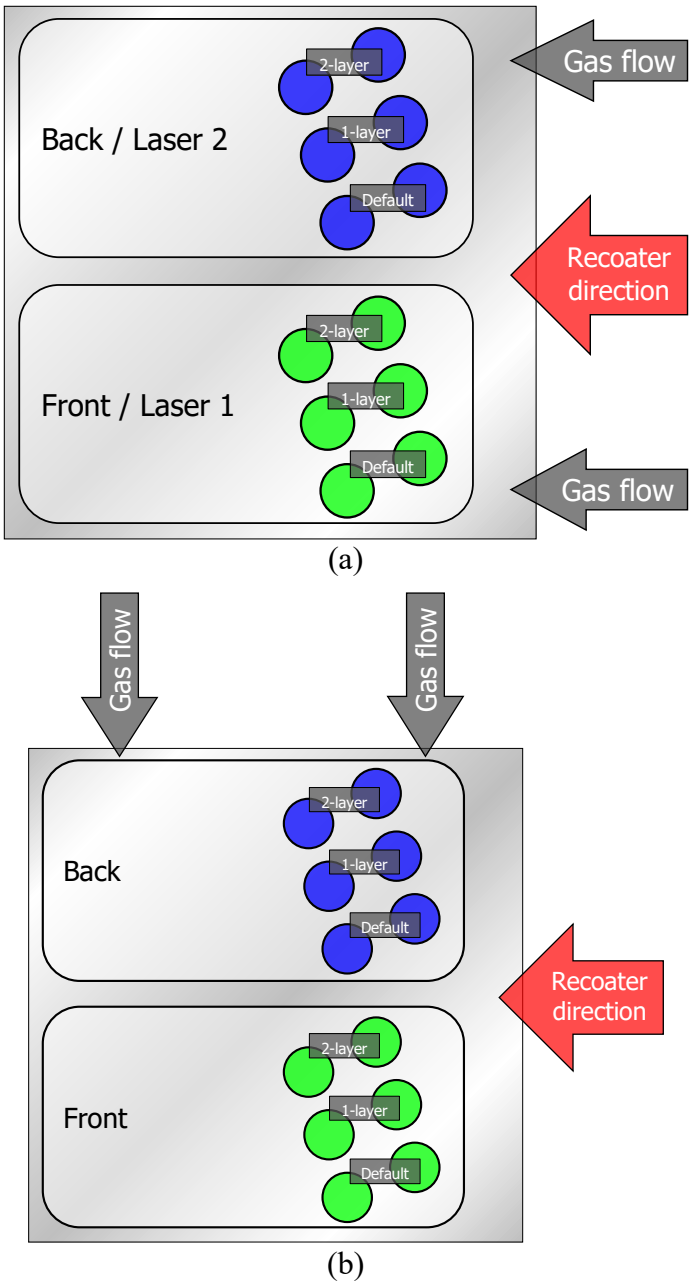


Figure 2. Schematic of build layout indicating specimen location with respect to the recoater arm and inert gas flow direction for the fabrications using (a) GE M2 with 316L SS and (b) EOS M290 with 17-4PH SS. The three specimen modifications are also indicated (default, 1-layer, and 2-layer).

Test methodologies

Monotonic tensile tests were performed according to ASTM standard E8 [27] and using an MTS Landmark servohydraulic system. All tests were conducted in displacement control mode at a rate of 0.012 mm/s; an extensometer with a 12 mm gage length was employed to record strain deformation up to 0.05 mm/mm. Two test per L-PBF system and specimen category (default, 1-

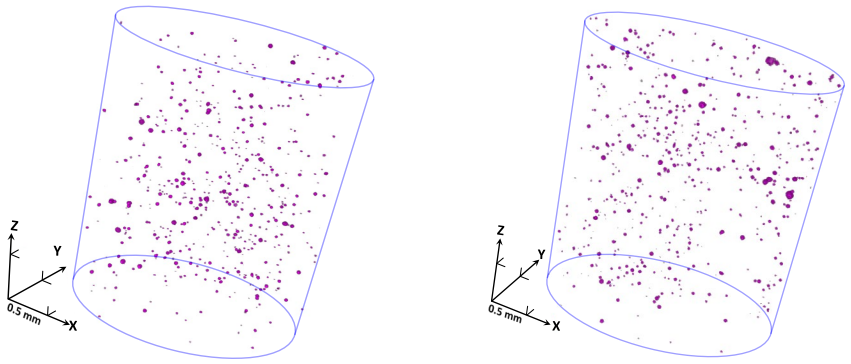
layer, 2-layer) were conducted. A tabulated summary including the feedstock material (316L/17-4PH SS), specimen category, built plate location (front or back), and test results is presented in **Table 1**. The results include, the ultimate tensile strength, *UTS*, 0.2% offset yield strength, *0.2%YS*, modulus of elasticity, *E*, percent area reduction, *RA*, and elongation to failure, ε_f.

Results and Discussion

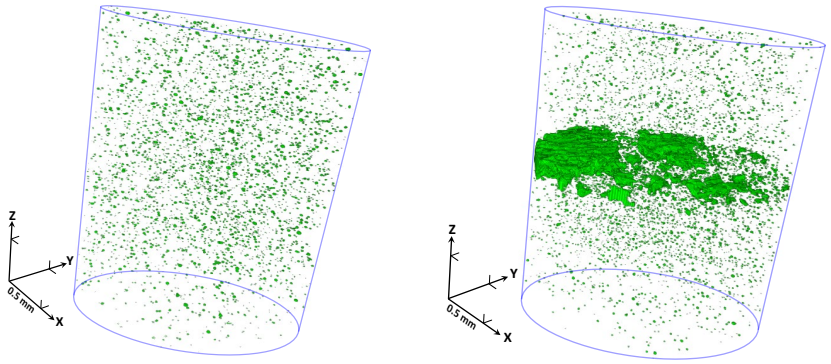
Specimen comparison

After fabrication, the efficacy of the cyber-attack was evaluated to see if it could go undetected by non-destructive inspection such as X-ray imaging. Comparison of X-ray reconstruction images of the default and 2-layer specimens at the area around the cross-section region, shown in **Figure 3**(a) – (d), demonstrate the different levels of severity of the cyber-attack. It can be observed in **Figure 3**(a) and (c) that default specimens have internal defects that are characteristic to AM parts, but in the case of the 2-layer thickness modified 17-4PH SS specimen (see **Figure 3**(c)), the defects are unmistakably visible. Contrary to the aforementioned results, shown in **Figure 3**(b), the 2-layer thickness modified 316L SS specimen does have clear indications that the part has been compromised, but it was observed that defects were generally larger within the scanned area (in comparison to the "default" counterpart) and some were agglomerated near/at the modified layers.

These results indicate that quality inspection of AM parts quality should be more rigorous and versatile since is seems that effectiveness and detectability (via non-destructive evaluations like X-ray tomography) of this type of attacks hinge on the AM system and material properties. The reason being that for a given AM system, the melt pool depth prescribed by the manufacturer's recommended processes parameters vary from material to material, leading to different laser power and layer thickness requirements [24,29]. Finally, it should be emphasized that the precise location of the modified layer(s) was known as well the specimen size being relatively small in comparison the actual parts. In realistic applications these conditions will most likely not hold, thus significantly reducing the probability of the attack detection.



(a) (b)



(c) (d)

Figure 3. X-ray tomography images comparing the internal porosity of a (a) default and (b) 2-layer modified thickness 316L SS specimen, as well as (c) default and (d) 2-layer modified thickness 17-4PH SS specimen near/at the cross-section volume [24].

Tensile behavior

The stress-displacement response of L-PBF 316L SS default, 1-layer, 2-layer specimens are presented in **Figure 4.** Since specimens were manufactured using a GE M2 dual laser AM system, specimens fabricated with laser 1 (i.e., front specimens) are denoted with the solid lines while specimens fabricated with laser 2 (i.e., back specimens) are denoted with dashed lines. The linear portion of the curves (which are related to the modulus of elasticity, E) do not vary from each other regardless of specimen category (i.e., default, 1-layer, 2-layer). This was further corroborated by comparing the modulus of elasticity, E, values from each test, presented in **Table 1**, where it was observed that values were similar (< 5 GPa difference). However, after yielding the specimens fabricated with laser 1 had higher yield stresses in comparison to those fabricated with laser 2, regardless of specimen category. Moreover, the effect of the attack was only evident after specimen failure, where it was observed that the area reduction, RA, and elongation to failure, ε_f, of 1-layer and 2-layer thickness specimens were considerably lower than the default specimens. Hence, the attack significantly affected the ductility of the part. The reduced ductility of 1-layer and 2-layer thickness specimens was confirmed to be due to the cyber-attack rather than other variables because the failure occurred exclusively at cross-section region, while for the default specimens occurred elsewhere along the specimens reduced section.

In the case of the default, 1-layer, 2-layer L-PBF 17-4PH SS specimens, presented in **Figure 5**(a) and (b), the influence of the attack was immediately evident as both specimen categories (1-layer and 2-layer) failed prematurely and before reaching yield. As can be seen in the close-up view of the stress-displacement curves shown in **Figure 5**(b), 1-layer and 2-layer specimens did not surpass a stress value of 600MPa, which is close to half the yield stress of the material. Moreover, it is observed that the stress-displacement curves of the 1-layer and 2-layer specimens are not similar to those of the default specimens; thus, indicating that the stiffness of the parts were affected as well, i.e., the modulus of elasticity was lower (see **Table 1**). Finally, it is important to mention that these tensile properties of the default specimens were in agreement

with similar studies on the mechanical behavior of vertically fabricated L-PBF 3l6L and 17-4 PH SS parts [30,31].

Table 1. Summary of test parameters and tensile properties evaluated in this study.

Specimen Category	Location	UTS	0.2% YS	E	RA	ε_f
		MPa	MPa	GPa	%	%
316L SS						
Default	Front	560	407	155	46	50
Default	Back	564	427	166	49	43
1-layer	Front	560	407	153	32	32
1-layer	Back	551	424	162	29	18
2-layer	Front	555	407	159	34	40
2-layer	Back	553	412	162	29	23
17-4PH SS						
Default	Front	1171	1137	197	29	22
Default	Back	1169	1137	197	26	14
1-layer	Front	425	-	192	3	1
1-layer	Back	434	-	197	3	2
2-layer	Front	612	-	197	2	5
2-layer	Back	239	-	192	3	2

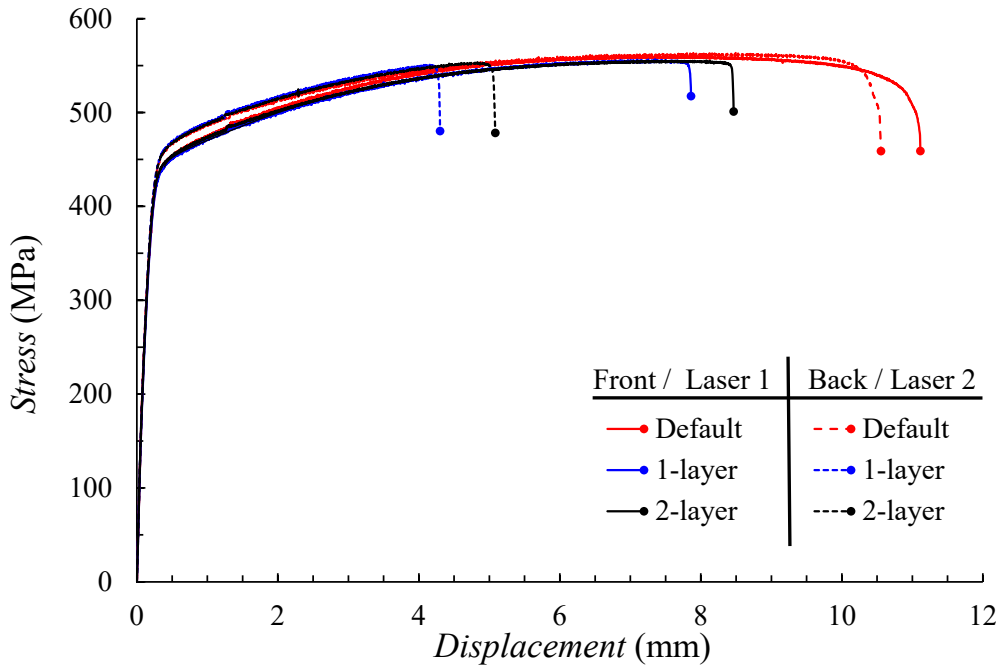


Figure 4. Stress vs. displacement curves comparing the tensile deformation behavior of default, 1-layer, and 2-layer L-PBF 316L stainless steel specimens fabricated using a GE Concept Laser M2 dual laser AM system.

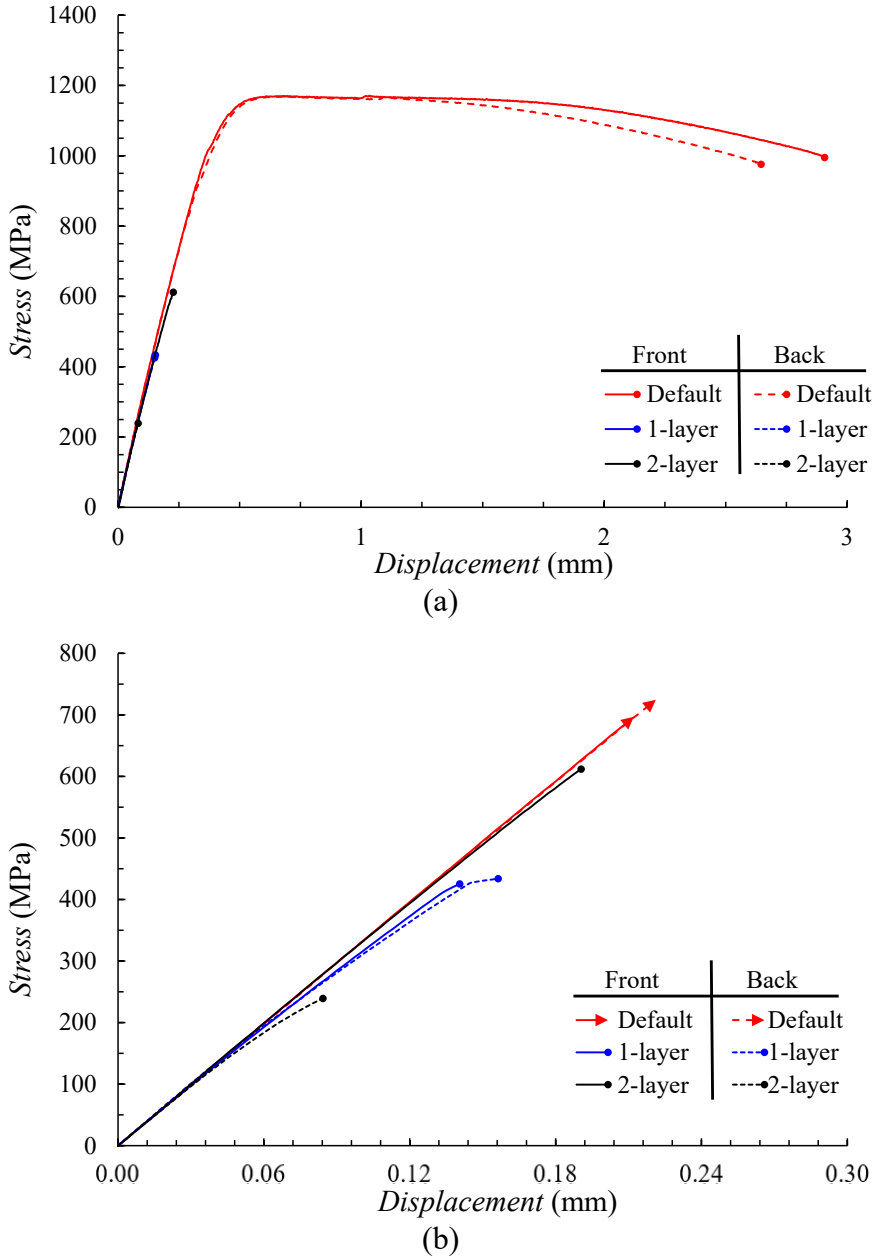


Figure 5. (a)Stress vs. displacement curves, as well as an (c) enhanced view plot comparing the tensile deformation behavior of default, 1-layer, and 2-layer L-PBF 17-4PH stainless steel specimens fabricated using a EOS M290 AM system.

Discussion of security implications

The experimental results clearly verify our assumption that the proposed method to introduce the layer thickness defect can be used in cyber-physical sabotage attacks on metal AM parts. We also demonstrated that this category of attacks can be implemented by simple modification of the build design files, which significantly lowers the technical sophistication needed and consequently increases the potential exposure to such attacks. We have also shown that both the impact of such attacks and their detectability are material dependent. From the

security perspective, it means that indiscriminately attacks might not necessarily yield significant impact, while targeted attacks would require participation of a subject matter expert and substantial knowledge about a part to be sabotaged – factors that reduce the security exposure. Lastly, at least on the designed specimens, this attack can be readily identified during quality inspection if the region of interest is known (see **Figure 3**). This means that even though material and time have been expended on the attacked build, the potential impact on the target system in which the part should be integrated can be easily averted.

Conclusion and Future Work

Additive Manufacturing (AM) is increasingly adopted, while its degree of computerization exposes it to a variety of cyber- and cyber-physical attacks. The study of such attacks and their characteristics is a necessary prerequisite for the development of efficient countermeasures.

In this paper, we focused on sabotage attacks against metal AM parts manufactured on a L-PBF machine. Specifically, we proposed a novel method to selectively modify process parameters at the layer thickness granularity. We demonstrated how this attack can be executed by simple modification of design file. We also evaluated the impact of the attack on a part's function by conducting tensile destructive tests on specimens manufactured with two different SS alloys, 316L and 17-4 PH. The experimental evaluation clearly shows that the attack is very effective in degrading the part's performance by at least factor of 6 when comparing the ductile properties of 17-4PH SS.

While we have expected that the defect size (or heights of the cross-section impacting the modified layer thickness) will have a direct proportionate impact on the failure characteristic, the results presented show that it is not necessarily the case. For example, for both 316L and 17-4PH materials, the 2-layer specimens were relatively more ductile than the 1-layer, which is counterintuitive as it was expected that thicker layers will lead to more defects. The underlying mechanisms leading to these results will need further future investigation.

The sabotage attacks modifying AM process parameters have, so far, relied on compromised firmware; however, the technical sophistication needed to compromising firmware is higher. The attack presented in this paper can be conducted via compromised computer or computer network. As hacking into computer systems and hijacking computer network communication can be conducted by readily available exploits and tools, the technical entry level of the considered attack is fairly low. To counter this, well-established cyber-security measures should be used to ensure the integrity of the design and build files.

In our future work we plan to investigate how the proposed approach can be used to introduce different modification of the manufacturing process parameters at the layer granularity. While our primary objective for this paper was to study a specific sabotage attack, a similar method can be used to introduce layer graded microstructural characteristics – a goal that might be of interest to benign applications as well.

Acknowledgments

This work was funded in part by the U.S. Department of the Navy, Office of Naval Research under Grant N00014-18-1-2488, in part by the U.S. Department of Commerce, National Institute of Standards and Technology under Grant NIST-70NANB19H170, and partially supported by the National Science Foundation (NSF) under grant #1919818

References

[1] Shamsaei N, Yadollahi A, Bian L, Thompson SM. An overview of Direct Laser Deposition for additive manufacturing; Part II: Mechanical behavior, process parameter optimization and control. Addit Manuf 2015;8:12–35. https://doi.org/10.1016/j.addma.2015.07.002.

[2] Yadollahi A, Shamsaei N. Additive manufacturing of fatigue resistant materials: Challenges and opportunities. Int J Fatigue 2017;98:14–31. https://doi.org/10.1016/j.ijfatigue.2017.01.001.

[3] Seifi M, Gorelik M, Waller J, Hrabe N, Shamsaei N, Daniewicz S, et al. Progress towards metal additive manufacturing standardization to support qualification and certification. Jom 2017;69:439–55.

[4] Paulsen C. Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium. National Institute of Standards and Technology; 2015. https://doi.org/10.6028/NIST.IR.8041.

[5] ASTM International. ASTM AM Data Management and Schema Workshop - Strategic Guide: Findings and Path Forward. 2019.

[6] Yampolskiy M, King WE, Gatlin J, Belikovetsky S, Brown A, Skjellum A, et al. Security of additive manufacturing: Attack taxonomy and survey. Addit Manuf 2018;21:431–57. https://doi.org/10.1016/j.addma.2018.03.015.

[7] Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J. Taxonomy for description of cross-domain attacks on CPS. Proc. 2nd ACM Int. Conf. High Confid. Networked Syst., New York, NY, USA: Association for Computing Machinery; 2013, p. 135–42. https://doi.org/10.1145/2461446.2461465.

[8] Yampolskiy M, Horváth P, Koutsoukos XD, Xue Y, Sztipanovits J. A language for describing attacks on cyber-physical systems. Int J Crit Infrastruct Prot 2015;8:40–52. https://doi.org/10.1016/j.ijcip.2014.09.003.

[9] Yampolskiy M, Skjellum A, Kretzschmar M, Overfelt RA, Sloan KR, Yasinsac A. Using 3D printers as weapons. Int J Crit Infrastruct Prot 2016;14:58–71. https://doi.org/10.1016/j.ijcip.2015.12.004.

[10] Belikovetsky S, Yampolskiy M, Toh J, Gatlin J, Elovici Y. dr0wned – Cyber-Physical Attack with Additive Manufacturing, 2017.

[11] Prinsloo J, Sinha S, von Solms B. A review of industry 4.0 manufacturing process security risks. Appl Sci 2019;9:5105.

[12] Mahesh P, Tiwari A, Jin C, Kumar PR, Reddy AN, Bukkapatanam ST, et al. A Survey of Cybersecurity of Digital Manufacturing. Proc IEEE 2020.

[13] Moore S, Armstrong P, McDonald T, Yampolskiy M. Vulnerability analysis of desktop 3D printer software. 2016 Resil. Week RWS, 2016, p. 46–51. https://doi.org/10.1109/RWEEK.2016.7573305.

[14] Sturm L, Williams C, Camelio A, White J, Parker R. Cyber-physical vunerabilities in additive manufacturing systems 2014.

[15] Do Q, Martini B, Choo K-KR. A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers. IEEE Trans Inf Forensics Secur 2016;11:2174–86. https://doi.org/10.1109/TIFS.2016.2578285.

[16] Xiao C. Security Attack to 3D Printing 2013.

[17] Moore SB, Glisson WB, Yampolskiy M. Implications of malicious 3D printer firmware 2017.

[18] Yampolskiy M, King W, Pope G, Belikovetsky S, Elovici Y. Evaluation of additive and substractive manufacturing from the security perspective. In: Rice M, Shenoi S, editors. Crit.

Infrastruct. Prot. XI, Cham: Springer International Publishing; 2017, p. 23–44. https://doi.org/10.1007/978-3-319-70395-4_2.
[19]Graves LMG, Lubell J, King W, Yampolskiy M. Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives. IEEE Access 2019;7:103833–53. https://doi.org/10.1109/ACCESS.2019.2931738.
[20]Zeltmann SE, Gupta N, Tsoutsos NG, Maniatakos M, Rajendran J, Karri R. Manufacturing and Security Challenges in 3D Printing. JOM 2016;68:1872–81. https://doi.org/10.1007/s11837-016-1937-7.
[21]Yampolskiy M, Schutzle L, Vaidya U, Yasinsac A. Security Challenges of Additive Manufacturing with Metals and Alloys. In: Rice M, Shenoi S, editors. Crit. Infrastruct. Prot. IX, Cham: Springer International Publishing; 2015, p. 169–83. https://doi.org/10.1007/978-3-319-26567-4_11.
[22]Ranabhat B, Clements J, Gatlin J, Hsiao K-T, Yampolskiy M. Optimal sabotage attack on composite material parts. Int J Crit Infrastruct Prot 2019;26:100301. https://doi.org/10.1016/j.ijcip.2019.05.004.
[23]Pope G, Yampolskiy M. A hazard analysis technique for additive manufacturing. ArXiv Prepr ArXiv170600497 2017.
[24]Graves L, King W, Carrion P, Shao S, Shamsaei N, Yampolskiy M. Sabotaging Metal Additive Manufacturing: Powder Delivery System Manipulation and Material-Dependent Effects. Addit Manuf 2021:102029. https://doi.org/10.1016/j.addma.2021.102029.
[25]Ilie A, Ali H, Mumtaz K. In-built customised mechanical failure of 316L components fabricated using selective laser melting. Technologies 2017;5:9.
[26]Slaughter A, Yampolskiy M, Matthews M, King WE, Guss G, Elovici Y. How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective. Proc. 12th Int. Conf. Availab. Reliab. Secur., 2017, p. 1–10.
[27]ASTM E8/E8M-21 Standard Test Methods for Tension Testing of Metallic Materials, ASTM International, West Conshohocken, PA, 2021, https://doi.org/10.1520/E0008_E0008M-21 2021.
[28]Carrion PE, Soltani-Tehrani A, Phan N, Shamsaei N. Powder Recycling Effects on the Tensile and Fatigue Behavior of Additively Manufactured Ti-6Al-4V Parts. JOM 2019;71:963–73. https://doi.org/10.1007/s11837-018-3248-7.
[29]du Plessis A, Yadroitsava I, Yadroitsev I. Effects of defects on mechanical properties in metal additive manufacturing: A review focusing on X-ray tomography insights. Mater Des 2020;187:108385.
[30]Nezhadfar PD, Shrestha R, Phan N, Shamsaei N. Fatigue behavior of additively manufactured 17-4 PH stainless steel: Synergistic effects of surface roughness and heat treatment. Int J Fatigue 2019;124:188–204.
[31]Shrestha R, Simsiriwong J, Shamsaei N. Fatigue behavior of additive manufactured 316L stainless steel parts: Effects of layer orientation and surface roughness. Addit Manuf 2019;28:23–38. https://doi.org/10.1016/j.addma.2019.04.011.