Spooky Manufacturing: Probabilistic Sabotage Attack in Metal AM using Shielding Gas Flow Control

Theo Zinner
Department of Computer Science and Software Engineering Auburn University
Auburn, Alabama, USA
tvz@auburn.edu

Grant Parker
Department of Computer Science and Software Engineering Auburn University
Auburn, Alabama, USA
gap0014@auburn.edu

Nima Shamsaei
Department of Mechanical Engineering Auburn University
Auburn, Alabama, USA
nzs0058@auburn.edu

Wayne King
The Barnes Global Advisors
USA
wayne@barnesglobaladvisors.com

Mark Yampolskiy
Department of Computer Science and Software Engineering Auburn University
Auburn, Alabama, USA
mark.yampolskiy@auburn.edu

ABSTRACT

Metal Additive Manufacturing (AM) is increasingly utilized for functional parts, often used in safety-critical applications such as jet engine components. For these applications, it is imperative that the fit, form, and function are not compromised. However, it has been shown that numerous intentional sabotage attacks are possible. Understanding how sabotage attacks can be conducted is a prerequisite for their prevention and detection.

This work focuses on Laser Beam Powder Bed Fusion (LB-PBF), an AM machine type dominant in the manufacturing of net-shape metal parts, and its subsystem controlling the shielding gas flow. We analyze how this essential subsystem can be manipulated to sabotage AM part performance. Our analysis shows that such sabotage attacks will be probabilistic, as opposed to the deterministic attacks previously discussed in the research literature. While this introduces issues with performance degradation and control over it, it is likely to also complicate the determination of intent and investigation of its root cause.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

Additive Manufacturing, Powder Bed Fusion, AM Security, Sabotage, Environmental Controls in Additive Manufacturing.

AMSec '22, November 11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9883-1/22/11…$15.00
https://doi.org/10.1145/3560833.3563565

ACM Reference Format:
Theo Zinner, Grant Parker, Nima Shamsaei, Wayne King, and Mark Yampolskiy. 2022. Spooky Manufacturing: Probabilistic Sabotage Attack in Metal AM using Shielding Gas Flow Control. In *Proceedings of the 2022 ACM CCS Workshop on Additive Manufacturing (3D Printing) Security (AMSec '22), November 11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3560833.3563565

1 INTRODUCTION

Additive Manufacturing (AM) is used in a wide array of industries due to the inherent advantages it offers. These include complex internal geometries in net-shape parts, rapid prototyping, and on-demand manufacturing [50]. AM is already being used to produce safety-critical parts. Prime examples include jet engine nozzles produced by General Electric [28], turbofan engine bearing housings from Honeywell Aerospace [25], and the main oxidizer valve body for the Space X Falcon 9 rocket [42]. In addition to the aerospace industry, AM has also rapidly gained popularity in the automotive and medical industries [50]. The average annual growth rate in revenue across AM industries has been 20.8% over the last four years [50]. AM offers opportunities for innovation and improvements upon existing technologies. However, reliance on AM exposes the AM industry and its customers to various security threats.

Security is vital to ensure success and the adoption of any technology, including AM. The need for security is especially critical in the case when dealing with safety-critical parts. While AM is closely related to traditional subtractive manufacturing, it has numerous unique characteristics that require a different approach to security [20]. Even the classical cyber-security CIA model[1] is only conditionally applicable to AM [51]. Instead, the security threats of technical data theft, illegal or unauthorized part manufacturing, steganographic covert channels, and sabotage must be considered [52, 53]. In this paper, we focus exclusively on the latter.

While we are unaware of any reports describing real-world attacks on AM manufactured parts or machines, many works have already demonstrated the feasibility of AM sabotage. Belikovetsky et al. [3] demonstrated the entire attack chain from the compromise of

[1] CIA stands for Confidentiality, Integrity, and Availability.

a computer controlling AM equipment to the physical destruction of a quadcopter due to sabotage of one of its AM-produced propellers. This attack was carried out on a consumer desktop 3D printer using polymers; however, the same principles apply. Thus a similar attack could be carried out on metal AM equipment producing safety-critical parts. This assertion is supported by many other works studying ability to compromise AM systems [12, 17, 23, 35, 40] and to sabotage AM parts [3, 19, 35, 55].

The intent and ability to conduct sabotage attacks in the broader context of Cyber-Physical Systems has been first demonstrated by the Stuxnet attack [13], followed by the alleged "arms race" between the world's major cyber powers. Therefore, it is only a matter of time before AM sabotage attacks become a reality. Understanding how such attacks can be conducted is a prerequisite for their prevention and detection.

Threat Model: In this work, we exclusively focus on sabotage of metal AM parts manufacturing using Laser Beam Powder Bed Fusion (LB-PBF). LB-PBF is an AM process currently dominant in manufacturing net-shape metal parts for safety-critical systems [50]. Furthermore, we restrict our investigation to its single but essential subsystem controlling shielding gas flow. As AM machines are often assembled using components and subsystems manufactured by third parties, compromising and manipulating a single subsystem is a realistic attack vector [19]. Other security threats (e.g., technical data theft) or different types of sabotage (e.g., AM machine sabotage or part sabotage using a different subsystem) are explicitly out of scope.

2 BACKGROUND

This section is dedicated to the cyber-security experts who may not be familiar with AM. It will provide specifics necessary to understand the remaining discussion in the paper.

In AM, 3D objects are produced incrementally by repeatably depositing and fusing thin layers of materials [48]. AM relies on a part's 3D digital design, commonly specified in a Computer-Aided Design (CAD) file format such as Stereolithography (STL). The 3D design is first "sliced" in thin horizontal layers. For each such slice, a toolpath is created that prescribes how actuators (specific to the AM process) should act to produce the geometry of the layer. The American Society for Testing and Materials (ASTM) defines seven distinct AM processes. In this paper, we focus on LB-PBF, which is dominant in manufacturing net-shape metal parts and some high-end polymer parts.

An LB-PBF machine uses source material (commonly referred to as feedstock) in powder form. For a new layer to be produced, a portion of the source material is allocated by raising the powder cell and spreading the powder across the build plate using the recoater (see Figure 1). This results in a thin uniform layer of feedstock spread across the entire build plate, which covers the previously manufactured layer. Afterward, a laser melts or sinters the powder to produce a single layer of the part, adhering it to the underlying layer. Repeating this process builds a part one layer at a time.

When exposed to oxygen, the metal powders used in LB-PBF can cause harmful effects such as oxide inclusions [11]. Additionally, some metal powders can combust when exposed to oxygen and the heat from the laser [39]. Prevention of this effect involves using

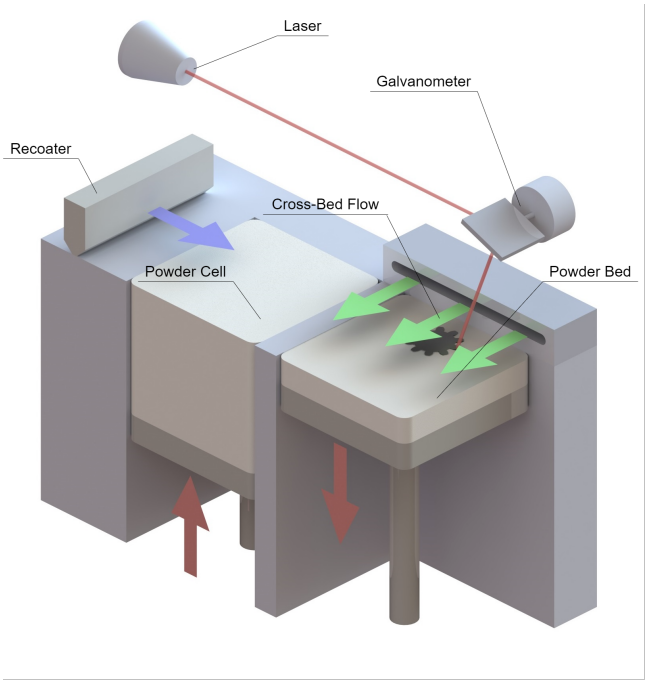

Figure 1: Schematic of a LB-PBF Machine.

an inert gas such as argon or nitrogen to shield the melt pool; the build chamber of the machine is flooded with the inert gas to keep the oxygen content under a certain threshold, typically 0.3 percent [38]

The high temperatures generated by the laser cause some metals to reach their boiling point, creating a vapor plume above the melt pool [29]; the vaporized metal quickly condensates and forms tiny particles, orders of magnitude smaller than the base powder. Different from metal vapor, spatter can be generated by numerous factors and comes in various forms. The spatter can also land on the surface of the part's profile (before or after melting) and lead to several defects. Young et al. [56] observed five different spatter types and identified them as follows: solid spatter, metallic jet spatter, agglomeration spatter, entrainment melting spatter, and defect-induced spatter.

A solid spatter results from base powder being swept up toward the vapor plume by an inward gas flow. It is then ejected before it can be melted [33]. Metallic jet spatter results from instability due to rapid expansion of the depression zone leading to high recoil pressure around the boundaries of the melt pool. This causes droplets of molten material to be ejected at high speed [56, 58]. Spatter can also be made up of multiple particles agglomerating together, producing spatter larger than the base powder. This is known as powder agglomeration spatter, created when molten particles near the melt pool are pushed outward by the vapor plume. These particles can pick up either melted or unmelted powder along the way. It can be characterized as a "snowballing" effect [56]. Similar to solid and powder agglomeration spatter, entrainment melting spatter is picked up by the inward gas flow toward the vapor plume. However, the critical difference is that the laser melts

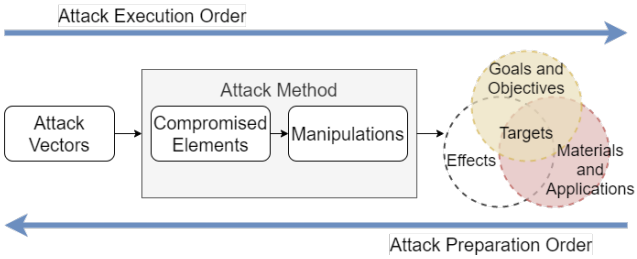

Figure 2: Using Attack Analysis Framework for Indentification of Sabotage Attacks in AM (based on [19, 53, 55]).

the base powder particles before being ejected. Additionally, while in molten form, these particles can coalesce with one another - increasing their size. Defect-induced spatter is generated when the laser interacts with existing defects in the part, such as porosity. In this instance, molten droplets are violently ejected from the melt pool. This effect could result from trapped gas or a rapid change of absorbed energy [56].

Each of these spatter types has different characteristics, such as size and initial ejection velocity, which depend on many more factors such as the base material, scanning speed, and the size of the depression in the melt pool. However, fully or partially melted spatter generally tends to be larger than the base powder [30, 31, 56]. While solid spatter or entrained spatter (i.e., powder swept into the vapor plume caused by an inward gas flow) is of a similar size to the base powder [33].

A constant flow of shielding gas must be maintained in the build chamber of an LB-PBF machine to carry away byproducts from the melting process that could interfere with the laser. Therefore, a subsystem controlling and maintaining the shielding gas flow is an indispensable component of every LB-PBF machine.

3 ANALYSIS

To identify the sabotage attacks that a single subsystem can be conducted, we use an approach proposed by Graves et al. [19]. The method is based on reverse traversal of the attack analysis framework originally introduced by Yampolskiy et al. [53, 55]. When "traversed" from left to right, the framework (depicted in Figure 2) describes the chronological order of an attack execution. However, the same framework can be traversed in the opposite direction for attack identification and preparation. The elements of the framework are described in chronological order below.

Attack Vectors represent different avenues the adversary can use to compromise a system involved in the AM. A classic example is a spear-phishing attack enabling compromised and, in some cases, remote control of a computer controlling the 3D printing process [3].

Compromised Elements specify the relevant element that is compromised; examples shown in the research literature include a controller storing design files [3, 49], controller workstation [3], a Wi-Fi network session between a workstation and 3D printer [12], and firmware controlling the AM machine [23, 35, 40].

Depending on the role that these elements play in the manufacturing process and the degree of control the adversary has over them, a variety of manipulations can be introduced in this process. Research literature shows a modification of design files [3, 49], toolpath [57], manufacturing process parameters [19, 23, 55], data monitoring in closed-loop process controls [47], and substitution of a print [12, 35]. Some *manipulations* can be semantically identical even when exercised by different compromised elements, e.g., changes of geometry via *manipulations* of design files on a computer or of the corresponding toolpath on a computer or network session; these are known as *Attack Methods* [53].

Manipulations (or *Attack Methods*) introduced in the manufacturing process could produce various effects. In general, these depend on several factors, such as the AM process and the material used. Necessary for our discussion, not all achievable *Effects* are also of interest to an adversary. Exemplary of this, manipulating a design (and thus violating of its integrity) instead of part sabotage could lead to improved part performance [51]. Those effects that that coincide with adversarial goals and objectives can be seen as *Attack Targets* [53].

In this work, we explicitly focus on part sabotage as an attack target, i.e., impact on one or more of its three F's: Fit, Form, and Function [16]. While we are explicitly focused on analyzing a new type of sabotage attack, for completeness, we need to note that an actual attack would try to optimize various properties while achieving a stated goal. For example, reducing a part's tensile strength to 90% of the operational load while minimizing deviations from the original design decreases probability of attack detection [43].

3.1 Effects and Manipulations

It is well known that misconfiguration of shielding gas flow can negatively impact the quality of parts produced with LB-PBF [1, 14, 29, 44]. The alloy and powder characteristics determine the window where gas flow parameters can vary without affecting manufacturing part quality [46]. Independent of the exact boundaries of the window, we can distinguish misconfiguration to be either above the upper bound or below the lower bound of the window.

Figure 3 depicts the qualitative relationships between the events when gas flow is outside window, as mentioned earlier. While the existing literature focuses on identifying the window and handles individual defects as motivation for determining the window boundary, we compiled this figure as a roadmap for intentional sabotage attacks with LB-PBF. It is important to note that while AM literature assumes that the same misconfiguration is present through the entire build, in the case of a sabotage attack, these can be introduced during strategically chosen layers.

We describe the individual causalities in more detail below, distinguishing between the three significant effects that can lead to reduced part quality. These include laser beam attenuation, spatter deposition, and powder layer disturbance. All of which can result from the either insufficient or excessive gas flow.

3.1.1 Laser Beam Attenuation. Spatter and the vapor plume are ejected from the melt pool as byproducts of the melting or sintering process and dispersed into the air above, expanding outward. Under normal operating conditions, the cross-bed flow is responsible for removing these byproducts. However, in the case of insufficient gas flow, these byproducts can interfere with the laser beam by either absorbing its incident energy or scattering the beam [4, 14, 29, 44]

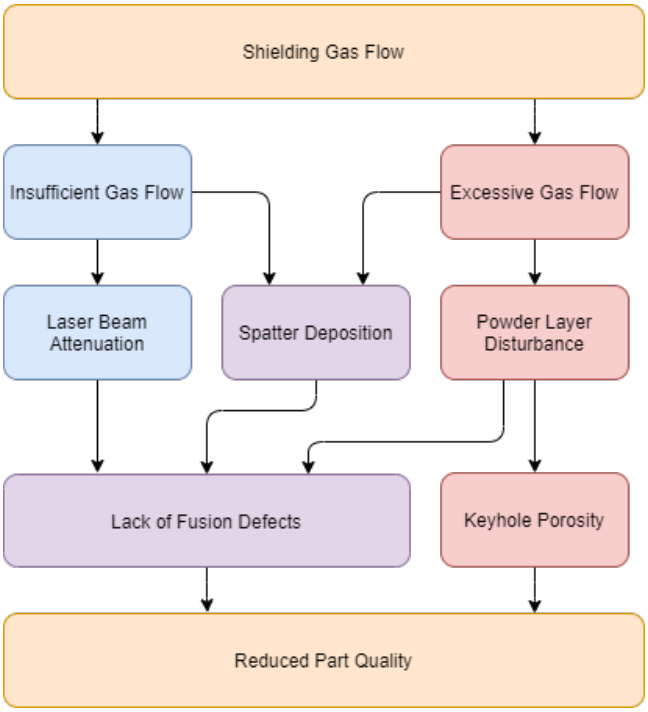

Figure 3: Shielding Gas Flow Defects.

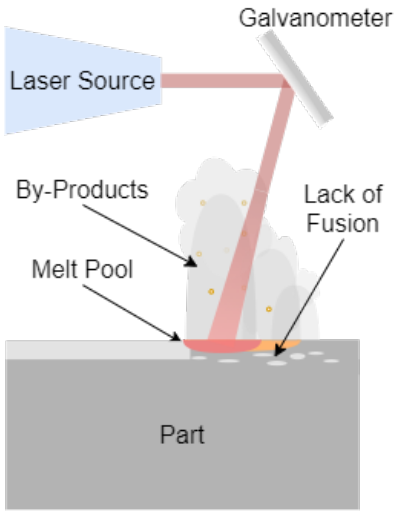

Figure 4: Laser Beam Attenuation.

(see Figure 4). The reduced amount of laser energy exerted on the powder can lead to lack of fusion defects [4, 14, 21, 29, 44]. The defects can be characterized by poor adhesion to previous layers as the laser does not exert enough energy to penetrate previously deposited layers fully. Insufficient laser energy can lead to balling, in which the molten pool agglomerates to a spherical body driven by surface tension, leaving the molten pool to form a disjointed body on the surface as a coarsened "ball" [21, 29]].

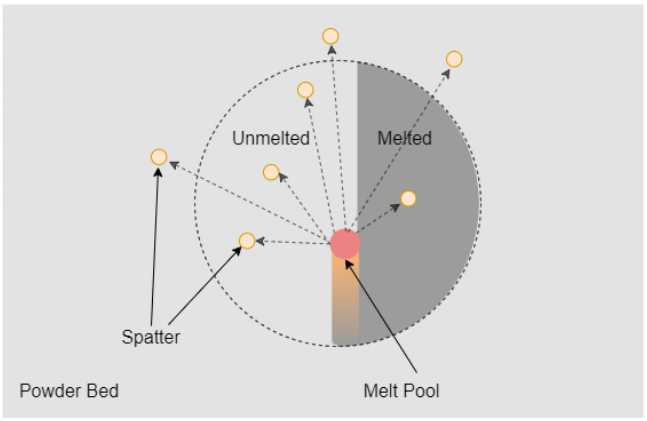

Figure 5: Spatter Deposition.

3.1.2 Spatter Deposition. As indicated above, spatter can interfere with the laser beam, causing attenuation of the laser. However, spatter causes a more significant negative effect when it lands on the part (see Figure 5). Here, we distinguish between the following two cases where spatter can lead to defects. First, spatter can land on an unmelted region of the part. Second, spatter can land on an already melted section of the part.

In the former case, when spatter lands on an unmelted region of the part, it can cause locally increased layer thickness, possibly leading to lack of fusion defects (see Figure 6). When a larger spatter particle is in the path of the laser, the laser may not properly melt the powder below the spatter, leaving unmelted powder within the layer and poor connection. Additionally, the poor connection to the previous layer can lead to a balling effect, similar to the result of laser beam attenuation, in which there is a disjointed "ball" just above the layer [29].

In the latter case, when molten spatter lands on an already melted section of the part, spatter can be partially welded to the part. If it is large enough, it can cause a similar balling effect as previously mentioned. However, in more extreme cases, the spatter can be pulled off by the recoater during powder distribution, leaving behind a pit (see Figure 6). If small enough, this pit can be trapped under subsequent layers as a defect. It can also be filled with powder, causing a localized increase in layer thickness for the next layer, thus, causing further defects [18].

3.1.3 Powder Layer Disturbance. In LB-PBF, it is imperative that the powder layer is uniform to ensure consistent melting characteristics across the build platform. However, in the case of excessive gas flow, the powder particles can be picked up in the cross-bed flow and either removed or redeposited on different regions of the powder layer [46] (see Figure 7). This process creates localized areas in which layer thickness is reduced and other areas in which it is increased.

Several factors can amplify each other in areas where layer thickness is reduced. While the laser exerts the same amount of energy in areas with reduced layer thickness, less fresh powder is melted than expected, corresponding to the case where laser power is excessive. It is well-known that excessive laser energy can lead to melt pool

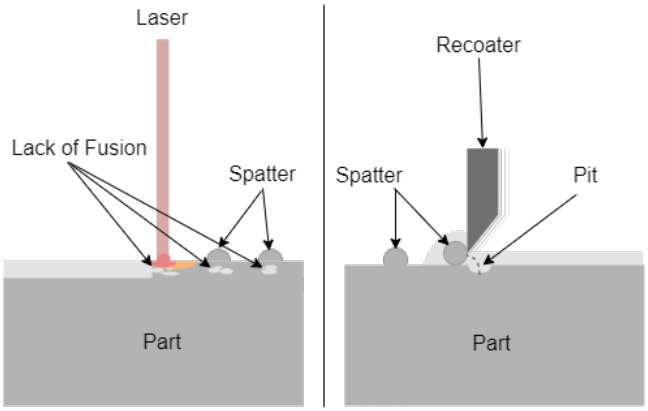

Figure 6: Spatter Deposition.

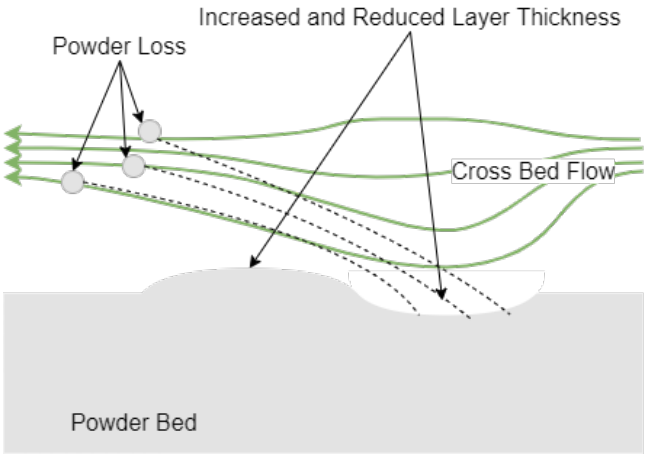

Figure 7: Particle Pickup.

turbulence and metallic jet spatter [34, 45]. Together, these factors can lead to the formation of Keyhole Porosity defects [7, 27], which also can cause defect-induced spatter [56]. This, in turn, can lead to reduced part quality, such as decreased tensile strength or fatigue life [30]. Shen et al. [46] conducted an experiment in which the powder bed experienced particle pickup. After five to ten layers, the part suffered significant visible shape defects. In addition, occasional powder thickness fluctuations can lead to defects hidden within the part.

3.2 Part Targeting with Effects

All sabotage attacks previously studied in the AM security literature were deterministic, i.e., manipulations such as design changes would lead to a predictable degradation of part performance. Furthermore, design changes would automatically apply to all parts manufacturing using modified design. However, neither of them applies to the category of manipulations analyzed in this paper. Instead, effects caused by misconfigured shielding gas flow and their characteristics experience stochastic fluctuations. Furthermore, in addition to the degree of misconfigurations, the effects also have a

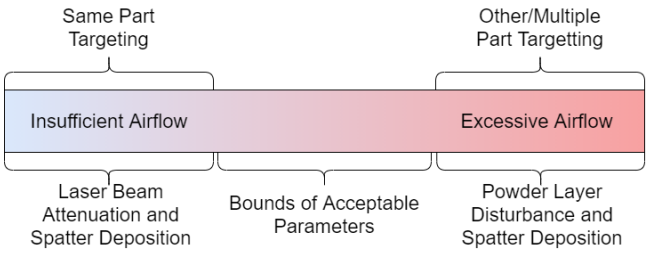

Figure 8: Gas Flow Targeting.

localized dependency, i.e., depend on the distance from and direction of the melt pool while shielding gas flow was manipulated.

A probabilistic approach is needed for a successful sabotage attack when dealing with stochastic variations. For example, spatter will only cause adverse effects when it lands on the part. Therefore, an estimate of this event's probability must be considered.

First, however, we need to understand what can be targeted using these effects. We must distinguish between the following three cases for targeting through gas flow manipulation (see Figure 8). First, in the case of insufficient gas flow, byproducts ejected from the melt pool can interfere with the laser, impacting the part they originate from. Second, spatter can be used to target the part it derives from as well as other parts within the build chamber. Depending on factors such as the size of an individual part or the distance between parts, this can be achieved with either insufficient or excessive gas flow. Third, excessive gas flow can change the profile of the powder layer, potentially impacting multiple affected parts.

3.2.1 Targeting Laser Beam Attenuation. Laser beam attenuation can occur above any part on the build platform. For targeting purposes, the cross-bed flow should be either reduced or increased to the extent that the byproducts can interfere with the laser during the melting process. The effect level is relative to the overlap between the laser's path and the area the byproducts occupy.

The overlap depends on a multitude of factors such as the volume of byproducts produced, scanning strategy, and speed of the laser [1, 4] to name few. For example, under normal operating conditions, the laser scanning speed and gas flow velocity work in conjunction to prevent overlap; however, this may no longer be the case with gas flow outside of its intended parameters. Furthermore, insufficient gas flow can also lead to spatter deposition on the same part. Thus, the two effects can be used in combination with one another to sabotage a single part.

3.2.2 Targeting: Spatter Deposition. Multiple considerations must be made for targeting a part with spatter deposition, such as the trajectory and size of the spatter. Additionally, when targeting other parts, the number, distance, and relative location between parts and their profile geometry at a particular layer have to be taken into account.

The trajectory of the spatter is influenced by several factors other than the shielding gas flow velocity. Different combinations of scanning speed and laser power have been shown to shift the initial ejection angle from the front of the melt pool to the back [4]. For example, a lower scanning speed will eject spatter particles in the direction of the scanning path, while a higher speed will

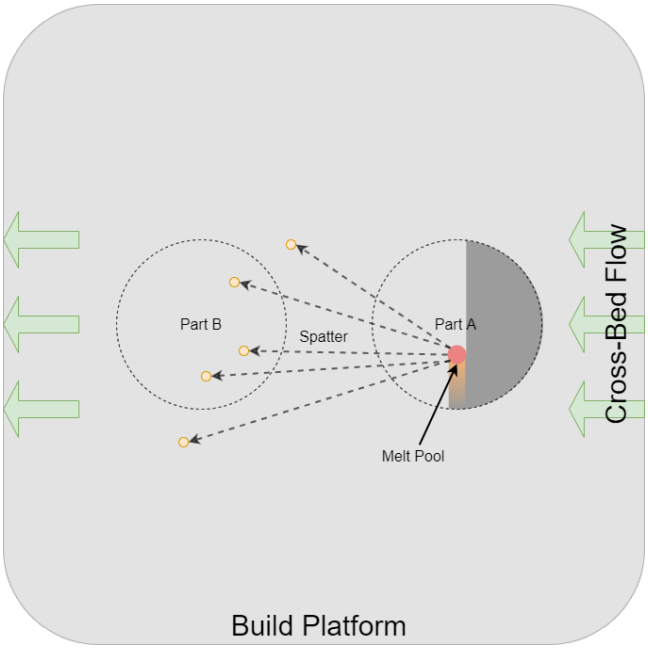

Figure 9: Cross Part Spatter Deposition.

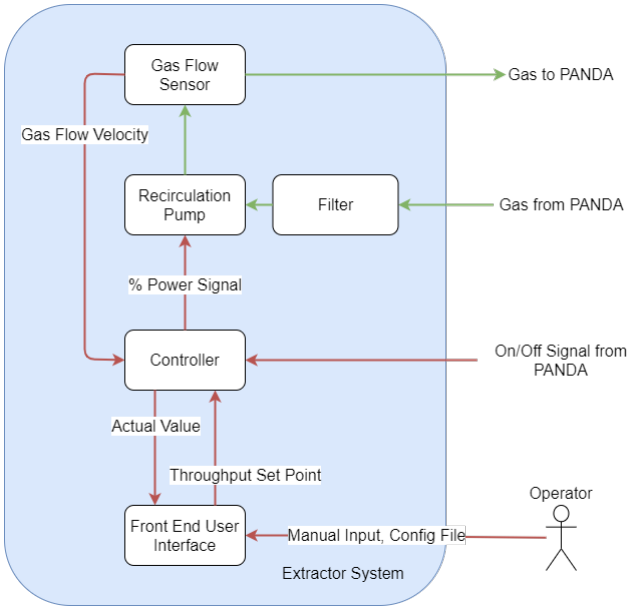

Figure 10: Extractor System.

eject them in the opposite direction [4]. Additionally, the amount of droplet spatter generated is affected by the scanning speed. Lower scanning speed can result in higher recoil pressure causing more spatter to be ejected from the melt pool [59].

The shielding gas flow velocity impacts the trajectory and distance spatter travels. After the spatter is ejected from the melt pool, it can be picked up by the cross-bed flow. The distance it travels is then dependent on the ejection vector, gas flow velocity, and other factors such as mass, size, and shape [2]. Increasing or decreasing the gas flow will change the area and probability distribution of where the spatter is likely to land; this can be used to target both the part it originates from or another part within the build chamber (see figure 9). In general, targeting the exact part that spatter originates from requires insufficient gas flow, while excessive gas flow can be used to target other parts.

A particular case of manufacturing multiple parts is when one or more functional parts are produced alongside complementary specimens that undergo destructive testing [34]. This case could be used for targeting in two different ways. First, by targeting the specimens that undergo destructive testing, parts will fail quality checks – reducing the yield. More dangerous still, by using spatter from the test specimens to target the production part(s), defects can go unnoticed because only the production part(s) will contain them.

3.2.3 Targeting: Powder Layer Disturbance. For targeting using powder layer disturbance, there are several factors at play. For instance, the characteristics of the powder itself, such as the size, shape, density, and flowability, influence the degree to which the gas flow velocity can change the powder layer profile [26, 46]. Additionally, the distance between the part and the gas inlet will determine the gas flow velocity above the part. Both parameters in combination determine whether or not the change of the shielding gas velocity will be sufficient to achieve the desired effect. Therefore, as the distance from the inlet to the part increases, so does the required gas flow velocity. Furthermore, the maximum attainable gas flow velocity is machine-dependent. These factors limit what can be targeted with powder layer disturbance to the gas outlet's immediate area.

3.3 Compromised Elements

Upon identification of shielding gas flow manipulations that can lead to part defects, we need to identify which elements in an LB-PBF system can be misused to exercise these manipulations. While this is machine-specific, we selected Open Additive PANDA for this analysis to demonstrate the identification approach. This open architecture machine provides access to all its subsystems and allows manipulation of most process parameters without the need to modify the machine's firmware. This, in conjunction with all the documentation available, makes the PANDA a good candidate for our analysis. This resulted in an approach that can be applied to identify the elements on other LB-PBF machines to conduct real attacks.

On the PANDA, the gas circulation is controlled by an external device known as the extractor. The extractor is responsible for maintaining constant flow and filtering out byproducts generated during the manufacturing process. We analyzed the machine's documentation, which included the user manual [38]. The diagram compiling the information of the inner-working of this sub-system, including its essential components and exchanged signals, is presented in Figure 10.

3.3.1 Extractor System in Open Additive PANDA. The cross-bed flow is only needed during the manufacturing process. Before the build process starts, the PANDA sends a signal to turn On the

extractor's Controller. Upon completion of the build, the PANDA sends the Off signal to the Controller. The same applies when the build is interrupted, e.g., by an operator or when a severe error is detected.

The central component of the extractor system is the Recirculation Pump. It pulls gas from the build chamber on one side and reintroduces it back into the chamber on the other side. During the recirculation process, the gas passes through a Filter that removes byproducts of the manufacturing process.

Over time, the Filter gets increasingly clogged, which can restrict the gas flow. For a stable and predictable manufacturing process, it is essential that the shielding gas flow is kept at a constant speed. The Controller, Recirculation Pump, and Gas Flow Sensor form a closed control loop to maintain continuous throughput. The extractor system will automatically adjust to maintain the desired throughput over the Filter's lifespan. The Controller operates based on the set value of throughput represented by $m^3/hour$. The Operator specifies this value through the Front-End User Interface. If the extractor senses that the gas flow dropped below the set value (caused by the Filter becoming clogged and obstructing gas from flowing), the Controller will react by increasing gas flow. However, if the Recirculation Pump cannot achieve the desired throughput, the machine will lower the Set Point to what is achievable with the Filter's current state [38].

3.3.2 Correlation between Components of Shielding Gas Flow Control and Manipulations. Depending on a role of an element in a closed control loop, it can be used to conduct either a direct or state estimate attack [8]. A direct attack is when the adversary uses a controller or control signal to manipulate the physical system. A state estimate attack is when the adversary uses the sensor or sensor data to report false information to the Controller, thus forcing the Controller to make a wrong decision.

Applied to the considered AM machine, Direct attacks can be executed from multiple components within the extractor system: Front-End User Interface, Throughput Set Point, Controller, Power Signal, and On/Off Signal from PANDA. If the Front-End User Interface is compromised, it can be used arbitrarily to change the Throughput Set Point. The Controller will then ensure that the modified throughput value is achieved by sending the corresponding Power Signal to the Recirculation Pump. If the Controller is compromised, it can change the % Power Signal regardless of the Throughput Set Point. Communication between individual elements is usually conducted by a shared bus. If any other compromised element is connected to the same bus through which one of the control signals is transmitted, it can also send a modified value to the receiver.

If the Actual Value reported through the Front-End User Interface does not match the specified Throughput Set Point, the Operator could become suspicious. This is only a problem in the case of direct attacks because they do not necessarily modify the reported sensor readings. To prevent this, attacks could simultaneously falsify the value reported to the Operator.

The State Estimate attacks can be executed from two components within the extractor system, the Gas Flow Sensor and the Gas Flow Velocity signal. The compromise of either of these components will allow an attacker to influence the Controller by providing false information on which it operates. If the Gas Flow Velocity value exceeds the actual value, the Power Signal will decrease and vice versa. Note that attacks by other components on the shared bus via injecting false sensor readings are possible; this, however, can cause a "jitter" between actual and falsified values - a situation that could be detected by a Controller and/or Operator.

In addition to the above-described cyber-physical attacks, attacks can be conducted through a variety of modifications to the physical components of the machine. These can only be performed by a malicious insider. An insider can replace or compromise any component of a system. Even without such a drastic measure, a malicious insider can set false parameters using the Front-End User Interface.

3.4 Attack Vectors

There are several ways to compromise various elements of the extractor system. These include direct action by malicious insiders and modifications of elements within cyber and physical supply chains by other means.

Dissatisfaction, coercion, or bribery can turn a company's employee into what is known as a "malicious insider." The danger is that malicious insiders often have legitimate access to the equipment and either already has or can easily gain knowledge of how it is used. Applied to our scenario, a malicious insider could often manipulate a system without hacking. For example, a malicious insider can modify the config file on the extractor. More dangerous still, but also requiring a higher level of sophistication, a malicious insider can install modified firmware or software on various system components. In this case, it could include the Front-End User Interface, the Controller on the extractor, or even the environmental control software on the PANDA. Given physical access to a machine, a malicious insider can also conduct a variety of physical manipulations. For example, components like the Filter or Recirculation Pump can be damaged, and the Gas Flow Sensor can be replaced by a faulty one.

Another increasingly common vector used to compromise a system is the cyber supply chain. For example, the company developing software for the individual sub-systems can be compromised, thus enabling the integration of malicious code in the software updates distributed to the customers. Supply chain attacks have been proven to be effective even against highly secure facilities [10]. Note that also physical supply chain attacks are possible. For example, the Gas Flow Sensor mentioned above can also be replaced by a compromised one.

Considering that over 73% of the manufacturing companies in the US are small and medium-sized [37], they will likely lack the resources or expertise to implement efficient security measures. Therefore, a direct external attack can compromise the manufacturer's equipment even through less sophisticated and more common attack means, such as spear phishing, automated malware, and remote hacking.

4 DISCUSSION

Several topics are conjectured in the discussion presented in the paper so far. For one, it is the combination of shielding gas manipulations with manipulations of other manufacturing process parameters that can be controlled by other subsystems. Further,

such attack's detectability (or stealthiness) plays an essential role in their potential ramifications.

4.1 Combination of Manipulations

There are a multitude of manufacturing process parameters which simultaneous manipulation together with the shielding gas velocity could further amplify the negative impact on the part function. These include but are not limited to the scanning strategy, the chamber pressure, and composition of the gas in the build chamber.

4.1.1 Additional Manipulations: Scanning Strategy. The laser scanning strategy plays a role in laser beam attenuation and spatter deposition. The scanning direction concerning the gas flow can impact the profile of the heat-affected zone (HAZ) and the cooling rate of the part. Masoomi et al. [32] found that when the gas and the laser move in the same direction, the powder downstream from the laser can be preheated due to forced convection. This can reduce the temperature gradient in the HAZ, leading to a lower cooling rate, reduced residual stress, and increased ductility in the part. Furthermore, increasing the velocity of the gas could augment this effect [32]. Therefore, simultaneous manipulation of the scan direction and the cross-bed flow velocity could be used in part sabotage, e.g., increased cooling speed.

4.1.2 Additional Manipulations: Build Chamber Pressure. The pressure in the build chamber can impact the amount of spatter and the initial direction taken. Lower pressure can lead to more molten spatter [5] and a wider ejection angle from the melt pool [22]. Increased pressure can reduce the total spatter in the build chamber and cause it to be ejected in a direction normal to the surface [22]. Bidare et al. [6] has also shown that working at high pressures (>1 atm/bar) can increase the amount of splatter generated. The compromise of a subsystem controlling this parameter could be used to increase the amount of spatter being deposited on the part, thus simplifying the part targeting and amplifying the impact on its quality.

4.1.3 Additional Manipulations: Shielding Gas Composition . The composition of the shielding gas is critical to the process. The oxygen levels could be increased to introduce oxides into the part. This could be done by compromising the O2 sensor in the machine and allowing some ambient air to enter the build chamber. Additionally, in more extreme cases, oxygen could theoretically be used to cause an explosion of the metal powder [55].

4.1.4 Additional Manipulations: Transition between Flow Profiles. Another aspect that could be considered is the transition between laminar and turbulent flow profiles. LB-PBF systems aim to achieve smooth laminar flow across the build surface which is more predictable and better at removing spatter [36]. Changes to the velocity, inlet profile, or surface of the build area could result in the flow becoming turbulent in some areas of the build volume which could locally affect the heat transfer, spatter removal, and powder denudation.

4.2 Stealth

In the case of functional parts, they are commonly screened with a variety of non-destructive testing (NDT) methods such as digital microscopy and X-ray computer tomography. Additionally, detection from testing coupons or a small punch test could easily be avoided by placing defects outside the elements that will undergo destructive tests. For a sabotage attack to be effective, a defect needs to be stealthy enough to bypass these screening techniques. With the deterministic sabotage attacks, this could have been achieved by strategically placing a defect, e.g., next to intricate internal features. With the probabilistic sabotage attack discussed in this paper, however, the location of the defect is hard to control. Thus such sabotage attack can be considered less stealthy than the deterministic categories.

However, defects introduced through this type of attack are similar if not identical to those naturally occurring in the LB-PBF process. If discovered, it is reasonable to assume that the defects will be attributed to misconfiguration of equipment or negligence on the part of the machine operator rather than intentional sabotage. When detected, this could lead to lengthy and costly investigations (a kind of economic sabotage). In the cases when the defect is not detected, classical effects of a sabotage attack can be the result, e.g., destruction of a part during operation.

5 RELATED WORK

The AM Security research literature has demonstrated numerous ways to compromise various components involved in AM. This includes using a trojan to infect 3D printer software [40], modifying the machine's firmware [23, 35], spear phishing to garner access to the controller PC [3], exploiting insecure network protocols to hijack communication with a 3D printer [12], and negligence to changing the default username and password for remote access [17].

Once compromised, these components can be used to sabotage parts in numerous ways, such as modification of external [23, 35] and internal geometry [3, 49] and change in build orientation [54, 57]. In addition, insertion of foreign material [57] and modification of feedstock characteristics [55] can occur. Furthermore, print jobs can be substituted [35, 40], printer availability can be disrupted [12], and even printer timing interference can occur [41].

Only a few AM security publications address the sabotage of metal parts. To date, all are focused on the PBF process. Slaughter et al. [47] demonstrated the possibility of a state estimate attack on an LB-PBF system implementing a closed control loop. In the closed control loop, laser power is adjusted automatically depending on the melt pool temperature measured by an IR sensor. Compromising the sensor and providing false readings can result in under or overmelting the source material, potentially introducing defects within the generated part. Graves et al. [19] identified individual and compound manipulations using the Powder Delivery System (PDS) of a PBF machine that can be used to degrade a part's mechanical properties. The validity of such an attack was verified experimentally. In addition to control specimens that have been manufactured without any changes, two attack cases have been investigated: the thickness of a single selected layer in the middle of a part was increased by a factor of 2 and 3. Non-destructive testing showed that such attacks could be challenging to detect with conventional methods such as X-Ray CT scans. Nevertheless, destructive testing has demonstrated significant degradation of fatigue life and tensile strength [9, 19]. Numerous process parameters that can be used for sabotage have

been identified in AM by Yampolskiy et al. [54]; these parameters significantly overlap with Frazier's survey [15] for parameters critical to quality control. Optimization of metal AM parameters is a topic widely covered throughout the material science literature. Although not directly security-oriented, such works can be used as a basis for the identification of potential sabotage attacks on AM. For example, Ilie et al. [24] modified process parameters related to laser energy density to introduce porosity defects, highlighting the crucial role process parameters play in various part properties.

6 CONCLUSION

In recent years AM has become prominent across multiple industries for diverse applications, including manufacturing of safety-critical parts. This increases the attractiveness of AM as a target to various malicious actors.

In this paper, we specifically focus on the security threat of sabotage attacks in LB-PBF 3D printers, a technology widely used in metal AM for safety-critical systems.

Specifically, we evaluated the ability to use the shielding gas flow system to conduct such an attack. The scientific contributions of this paper are as follows. We first analyzed how increasing or decreasing the throughput of shielding gas can impact the quality of the manufactured parts. We then identified the various components of this subsystem that can be used to conduct such an attack. We further discussed the common attack vectors a malicious actor could use to compromise these components.

While all prior sabotage attacks demonstrated for AM have been entirely deterministic, to our knowledge, this is the first example of a probabilistic attack. This has numerous consequences. On the one hand, the probabilistic nature reduces the precision of quality degradation and increases complexity of the part targeting. On the other hand, this attack can be used to attack multiple simultaneously. Furthermore, the degraded part performance may not be easily attributed to an intentional sabotage attack. Lastly, the fact that the degradation is not consistent makes the root cause analysis more complex and time-consuming. The latter can be considered a significant advantage from the attacker's perspective, especially when the attacker's goal is to inflict financial damage.

In our future work, we plan to conduct an experimental evaluation of our theoretical analysis presented in this paper. In addition to validating the effectiveness of this attack, we plan to investigate whether established non-destructive techniques can be effectively used to detect such an attack.

ACKNOWLEDGMENTS

This work was funded in part by the U.S. Department of Commerce, National Institute of Standards and Technology under Grants NIST-70NANB19H170 and NIST-70NANB21H121.

REFERENCES

[1] Ahmad Bin Anwar and Quang-Cuong Pham. 2017. Selective laser melting of AlSi10Mg: Effects of scan direction, part placement and inert gas flow velocity on tensile strength. *Journal of Materials Processing Technology* 240 (2017), 388–396.

[2] Ahmad Bin Anwar and Quang-Cuong Pham. 2018. Study of the spatter distribution on the powder bed during selective laser melting. *Additive Manufacturing* 22 (2018), 86–97.

[3] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. 2017. dr0wned–{Cyber-Physical} Attack with Additive Manufacturing. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*.

[4] Prveen Bidare, Ioannis Bitharas, RM Ward, MM Attallah, and Andrew J Moore. 2018. Fluid and particle dynamics in laser powder bed fusion. *Acta Materialia* 142 (2018), 107–120.

[5] PRVEEN Bidare, Ioannis Bitharas, RM Ward, MM Attallah, and Andrew J Moore. 2018. Laser powder bed fusion at sub-atmospheric pressures. *International Journal of Machine Tools and Manufacture* 130 (2018), 65–72.

[6] Prveen Bidare, Ioannis Bitharas, RM Ward, MM Attallah, and Andrew J Moore. 2018. Laser powder bed fusion in high-pressure atmospheres. *The International Journal of Advanced Manufacturing Technology* 99, 1 (2018), 543–555.

[7] MC Brennan, JS Keist, and TA Palmer. 2021. Defects in Metal Additive Manufacturing Processes. *Journal of Materials Engineering and Performance* 30, 7 (2021), 4808–4818.

[8] Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. 2008. Secure control: Towards survivable cyber-physical systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 495–500.

[9] Patricio E Carrion, Lynne M Graves, Mark Yampolskiy, and Nima Shamsaei. 2021. Evaluation of a Cyber-Physical Attack Effectiveness in Metal Additive Manufacturing by Selectively Modifying Build Layer Thickness. In *2021 International Solid Freeform Fabrication Symposium*. University of Texas at Austin.

[10] Microsoft Threat Intelligence Center. 2021. Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit. (2021).

[11] Pu Deng, Mallikarjun Karadge, Raul B Rebak, Vipul K Gupta, Barton C Prorok, and Xiaoyuan Lou. 2020. The origin and formation of oxygen inclusions in austenitic stainless steels manufactured by laser powder bed fusion. *Additive Manufacturing* 35 (2020), 101334.

[12] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2016. A data exfiltration and remote exploitation attack on consumer 3D printers. *IEEE Transactions on Information Forensics and Security* 11, 10 (2016), 2174–2186.

[13] N Falliere. 2011. W32. stuxnet dossier. white paper, Symantec Corp., Security Response 5. (2011).

[14] B Ferrar, L Mullen, E Jones, R Stamp, and CJ Sutcliffe. 2012. Gas flow effects on selective laser melting (SLM) manufacturing performance. *Journal of Materials Processing Technology* 212, 2 (2012), 355–364.

[15] William E Frazier. 2014. Metal additive manufacturing: a review. *Journal of Materials Engineering and performance* 23, 6 (2014), 1917–1928.

[16] Ian Gibson, David Rosen, Brent Stucker, and Mahyar Khorasani. 2021. *Additive manufacturing technologies*. Vol. 17. Springer.

[17] Dominick Glavach, Julia LaSalle-DeSantis, and Scott Zimmerman. 2017. Applying and assessing cybersecurity controls for direct digital manufacturing (ddm) systems. In *Cybersecurity for Industry 4.0*. Springer, 173–194.

[18] Haijun Gong, Khalid Rafi, Thomas Starr, and Brent Stucker. 2013. The effects of processing parameters on defect regularity in Ti-6Al-4V parts fabricated by selective laser melting and electron beam melting. In *2013 International Solid Freeform Fabrication Symposium*. University of Texas at Austin.

[19] L Graves, WE King, P Carrion, S Shao, N Shamsaei, and M Yampolskiy. 2021. Sabotaging metal additive manufacturing: Powder delivery system manipulation and material-dependent effects. *Additive Manufacturing* 46 (2021), 102029.

[20] Lynne MG Graves, Joshua Lubell, Wayne King, and Mark Yampolskiy. 2019. Characteristic aspects of additive manufacturing security from security awareness perspectives. *IEEE Access* 7 (2019), 103833–103853.

[21] Dongdong Gu and Yifu Shen. 2009. Balling phenomena in direct laser sintering of stainless steel powder: Metallurgical mechanisms and control methods. *Materials & Design* 30, 8 (2009), 2903–2910.

[22] Qilin Guo, Cang Zhao, Luis I Escano, Zachary Young, Lianghua Xiong, Kamel Fezzaa, Wes Everhart, Ben Brown, Tao Sun, and Lianyi Chen. 2018. Transient dynamics of powder spattering in laser powder bed fusion additive manufacturing process revealed by in-situ high-speed high-energy x-ray imaging. *Acta Materialia* 151 (2018), 169–180.

[23] Xiao Zi Hang and Claud Xiao. 2013. Security attack to 3D printing. Keynote at XCon2013.

[24] Andrei Ilie, Haider Ali, and Kamran Mumtaz. 2017. In-built customised mechanical failure of 316L components fabricated using selective laser melting. *Technologies* 5, 1 (2017), 9.

[25] Amanda Jensen. 2020. Honeywell achieves FAA certification for first flight-critical engine part built from additive manufacturing. https://aerospace.honeywell.com/us/en/learn/about-us/press-release/2020/08/faa-certification-for-first-flight-critical-engine

[26] Haim Kalman, Andrei Satran, Dikla Meir, and Evgeny Rabinovich. 2005. Pickup (critical) velocity of particles. *Powder technology* 160, 2 (2005), 103–113.

[27] Wayne E King, Holly D Barth, Victor M Castillo, Gilbert F Gallegos, John W Gibbs, Douglas E Hahn, Chandrika Kamath, and Alexander M Rubenchik. 2014. Observation of keyhole-mode laser melting in laser powder-bed fusion additive manufacturing. *Journal of Materials Processing Technology* 214, 12 (2014), 2915–2925.

[28] Amy Kover. 2018. Transformation in 3D: How a walnut-sized part changed the way GE Aviation Builds Jet Engines. https://www.ge.com/news/reports/transformation-3d-walnut-sized-part-changed-way-ge-aviation-builds-jet-engines

[29] Alexander Ladewig, Georg Schlick, Maximilian Fisser, Volker Schulze, and Uwe Glatzel. 2016. Influence of the shielding gas flow on the removal of process by-products in the selective laser melting process. *Additive Manufacturing* 10 (2016), 1–9.

[30] Yang Liu, Yongqiang Yang, Shuzhen Mai, Di Wang, and Changhui Song. 2015. Investigation into spatter behavior during selective laser melting of AISI 316L stainless steel powder. *Materials & Design* 87 (2015), 797–806.

[31] Sonny Ly, Alexander M Rubenchik, Saad A Khairallah, Gabe Guss, and Manyalibo J Matthews. 2017. Metal vapor micro-jet controls material redistribution in laser powder bed fusion additive manufacturing. *Scientific reports* 7, 1 (2017), 1–12.

[32] Mohammad Masoomi, Jonathan W Pegues, Scott M Thompson, and Nima Shamsaei. 2018. A numerical and experimental investigation of convective heat transfer during laser-powder bed fusion. *Additive Manufacturing* 22 (2018), 729–745.

[33] Manyalibo J Matthews, Gabe Guss, Saad A Khairallah, Alexander M Rubenchik, Philip J Depond, and Wayne E King. 2016. Denudation of metal powder layers in laser powder bed fusion processes. *Acta Materialia* 114 (2016), 33–42.

[34] John O Milewski. 2017. Additive manufacturing of metals. *Applied Mechanics and Materials* (2017).

[35] Samuel Bennett Moore, William Bradley Glisson, and Mark Yampolskiy. 2017. Implications of malicious 3D printer firmware. Proceedings of the 50th Hawaii International Conference on System Sciences.

[36] TP Moran, DH Warner, A Soltani-Tehrani, N Shamsaei, and N Phan. 2021. Spatial inhomogeneity of build defects across the build plate in laser powder bed fusion. *Additive Manufacturing* 47 (2021), 102333.

[37] MxD. 2019. STRATEGIC INVESTMENT PLAN 2019.

[38] OpenAdditive. 2019. PANDA_user_manual_V05.

[39] OSHA. 2020. Department of Labor Logo United Statesdepartment of Labor. https://www.osha.gov/otm

[40] Hammond Pearce, Kaushik Yanamandra, Nikhil Gupta, and Ramesh Karri. 2021. FLAW3D: A Trojan-based Cyber Attack on the Physical Outcomes of Additive Manufacturing. *arXiv preprint arXiv:2104.09562* (2021).

[41] Gregory Pope and Mark Yampolskiy. 2017. A hazard analysis technique for additive manufacturing. *arXiv preprint arXiv:1706.00497* (2017).

[42] H Post. 2014. SpaceX Launches 3D-Printed Part to Space, Creates Printed Engine Chamber. *SpaceX website. http://www. spacex. com/news/2014/07/31/spacex-launches-3dprinted-part-space-creates-printed-engine-chamber-crewed* (2014).

[43] Bikash Ranabhat, Joseph Clements, Jacob Gatlin, Kuang-Ting Hsiao, and Mark Yampolskiy. 2019. Optimal sabotage attack on composite material parts. *International Journal of Critical Infrastructure Protection* 26 (2019), 100301.

[44] Joni Reijonen, Alejandro Revuelta, Tuomas Riipinen, Kimmo Ruusuvuori, and Pasi Puukko. 2020. On the effect of shielding gas flow on porosity and melt pool geometry in laser powder bed fusion additive manufacturing. *Additive Manufacturing* 32 (2020), 101030.

[45] Giulia Repossini, Vittorio Laguzza, Marco Grasso, and Bianca Maria Colosimo. 2017. On the use of spatter signature for in-situ monitoring of Laser Powder Bed Fusion. *Additive Manufacturing* 16 (2017), 35–48.

[46] Haopeng Shen, Paul Rometsch, Xinhua Wu, and Aijun Huang. 2020. Influence of gas flow speed on laser plume attenuation and powder bed particle pickup in laser powder bed fusion. *Jom* 72, 3 (2020), 1039–1051.

[47] Andrew Slaughter, Mark Yampolskiy, Manyalibo Matthews, Wayne E King, Gabe Guss, and Yuval Elovici. 2017. How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*. 1–10.

[48] ASTM Standard. 2013. F2792-12a: standard terminology for additive manufacturing technologies (ASTM International, West Conshohocken, PA, 2012). *Procedia Eng* 63 (2013), 4–11.

[49] Logan D Sturm, Christopher B Williams, Jamie A Camelio, Jules White, and Robert Parker. 2017. Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects. *Journal of Manufacturing Systems* 44 (2017), 154–164.

[50] T Wohlers. 2021. Wohlers report 2021: 3d printing and additive manufacturing state of the industry. (2021).

[51] Mark Yampolskiy, Jacob Gatlin, and Moti Yung. 2021. Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. In *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*. 3–9.

[52] Mark Yampolskiy, Lynne Graves, Jacob Gatlin, Anthony Skjellum, and Moti Yung. 2021. What Did You Add to My Additive Manufacturing Data?: Steganographic Attacks on 3D Printing Files. In *24th International Symposium on Research in Attacks, Intrusions and Defenses*. 266–281.

[53] Mark Yampolskiy, Wayne E King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, and Yuval Elovici. 2018. Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing* 21 (2018), 431–457.

[54] Mark Yampolskiy, Lena Schutzle, Uday Vaidya, and Alec Yasinsac. 2015. Security challenges of additive manufacturing with metals and alloys. In *International Conference on Critical Infrastructure Protection*. Springer, 169–183.

[55] Mark Yampolskiy, Anthony Skjellum, Michael Kretzschmar, Ruel A Overfelt, Kenneth R Sloan, and Alec Yasinsac. 2016. Using 3D printers as weapons. *International Journal of Critical Infrastructure Protection* 14 (2016), 58–71.

[56] Zachary A Young, Qilin Guo, Niranjan D Parab, Cang Zhao, Minglei Qu, Luis I Escano, Kamel Fezzaa, Wes Everhart, Tao Sun, and Lianyi Chen. 2020. Types of spatter and their features and formation mechanisms in laser powder bed fusion additive manufacturing process. *Additive Manufacturing* 36 (2020), 101438.

[57] Steven Eric Zeltmann, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. 2016. Manufacturing and security challenges in 3D printing. *Jom* 68, 7 (2016), 1872–1881.

[58] Cang Zhao, Qilin Guo, Xuxiao Li, Niranjan Parab, Kamel Fezzaa, Wenda Tan, Lianyi Chen, and Tao Sun. 2019. Bulk-explosion-induced metal spattering during laser processing. *Physical Review X* 9, 2 (2019), 021052.

[59] Hang Zheng, Huaixue Li, Lihui Lang, Shuili Gong, and Yulong Ge. 2018. Effects of scan speed on vapor plume behavior and spatter generation in laser powder bed fusion additive manufacturing. *Journal of Manufacturing Processes* 36 (2018), 60–67.