How to Ensure Bad Quality in Metal Additive Manufacturing: *In-Situ* Infrared Thermography from the Security Perspective

Andrew Slaughter
University of South Alabama
150 Jaguar Dr.
Mobile, AL 36688
aes1425@jagmail.southalabama.edu

Mark Yampolskiy
University of South Alabama
150 Jaguar Dr.
Mobile, AL 36688
yampolskiy@southalabama.edu

Manyalibo Matthews
Lawrence Livermore National
Laboratory
7000 East Ave
Livermore, CA 94550
matthews11@llnl.gov

Wayne E. King
Lawrence Livermore National
Laboratory
7000 East Ave
Livermore, CA 94550
king17@llnl.gov

Gabe Guss
Lawrence Livermore National
Laboratory
7000 East Ave
Livermore, CA 94550
guss2@llnl.gov

Yuval Elovici
Ben-Gurion University of the Negev,
Singapore University of Technology
and Design
P.O. Box 653
Beer-Sheva, Israel 84105
yuval_elovici@sutd.edu.sg

ABSTRACT

Additive Manufacturing, a.k.a. 3D Printing, is increasingly used to manufacture functional parts, including components of safety critical systems. Therefore, assuring part quality has become of paramount importance. *In-situ* infrared (IR) imaging systems are a promising solution to increase final build quality and minimize time-consuming and costly post processing and characterization. However, it also raises novel security concerns. We argue that, if compromised, the same in-situ quality control can be abused to sabotage manufactured parts. As a basis for our discussion, we first detail how IR thermography is used in open-loop and, experimentally, in closed-loop quality control for powder bed fusion (PBF) systems. We then identify malicious manipulations that an adversary can perform. We discuss the consequences of the manipulations on the manufactured part's quality. For selected attacks, we also provide experimental proof of the identified manipulations and their consequences.

CCS CONCEPTS

•Applied computing → Computer-aided manufacturing;

KEYWORDS

Additive Manufacturing, Powder Bed Fusion, Infrared Thermography, Security, Tampering, Sabotage, Safety

ACM Reference format:

Andrew Slaughter, Mark Yampolskiy, Manyalibo Matthews, Wayne E. King, Gabe Guss, and Yuval Elovici. 2017. How to Ensure Bad Quality in Metal

ACM acknowledges that this contribution was authored or co-authored by an employee, or contractor of the national government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only. Permission to make digital or hard copies for personal or classroom use is granted. Copies must bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. To copy otherwise, distribute, republish, or post, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ARES '17, Reggio Calabria, Italy

© 2017 ACM. 978-1-4503-5257-4/17/08...\$15.00

DOI: 10.1145/3098954.3107011

Additive Manufacturing: *In-Situ* Infrared Thermography from the Security Perspective. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017*, 11 pages.

DOI: 10.1145/3098954.3107011

1 INTRODUCTION

Metal Additive Manufacturing (AM), a.k.a. 3D Printing, is a rapidly growing multibillion dollar industry. One recent example of AM adoption is GE's fuel nozzle for the next generation LEAP jet engine [31, 38]. Through part consolidation, GE has used AM to create a part five times more durable and being 25% lighter than was possible with typical subtractive manufacturing processes.

Even with its ever-increasing popularity, AM faces many challenges it must overcome before rivaling traditional subtractive manufacturing processes. One of the most crucial limitations is the lack of *in-situ* quality control methods [21]. Most current quality control methods are not usable in-process and involve costly and time-consuming post-processing nondestructive and selective destructive evaluation. This extends manufacturing time, leading to lower production rates and higher cost-per-part. Everton et al. provides a comprehensive list of currently viable and speculative *in-situ* process control methods [11]. While infrared (IR) imaging systems have yet to see widespread use in commercial additive manufacturing, the study and implementation of such systems is important to the worldwide commercial acceptance and competitiveness of metal AM.

To date, very little if any work has been done in terms of a security analysis of this method. This paper offers an analysis of possible attacks associated with implementing *in-situ* infrared thermography as a method of quality assurance.

The remainder of this paper is structured as follows. After discussing related work on AM security in Section 2, we provide background on metal AM and IR thermography in Section 3. We present our security analysis of this system and its impact on manufactured parts quality in Section 4. For selected attacks, we provide

experimental proof of the identified manipulations and their consequences in Section 5. We conclude this paper with a short discussion of our findings in Section 6 and an outline of planned future work in Section 7.

2 RELATED WORK

Security of additive manufacturing is a fairly new research area. Threats to AM have been dichotomized into two primary threat categories: (1) Sabotage and (2) Intellectual Property (IP) violations. Sabotage attacks aim to inflict physical damage, either by compromising part quality or by harm to the actual AM equipment. IP violation attacks aim to illegally replicate 3D objects or the manufacturing process itself. For this paper, only sabotage is relevant.

A growing body of publications discusses how a manufactured part's quality can be compromised in a cyber-physical sabotage attack. The first proof of concept for a sabotage-style attack on an additive manufacturing device was presented by Xiao [40]. It was shown that the attack can modify "printing results" such as the dimensions, positioning, and integrability of the components, among others. Sturm et al. [35] used malware pre-installed on a computer to automate manipulations of .stl files, and provided an empirical demonstration that a part's tensile strength could be degraded by introducing volumetric defects such as voids. By using a material with significantly different stiffness values, Zeltmann et al. [44] used finite element analysis to show that the introduction of these "pseudo-voids" which were beneath the detection limit of their ultrasonic quality control tools greatly reduced the strength of the printed part. An attack that inserts voids with geometry leading to a stress concentration and reduced fatigue life was proposed and empirically demonstrated by Belikovetsky et al. [6]. A phishing attack was used to install a backdoor that enabled the targeted insertion of rectangular voids into the design files for a drone quadcopter propeller by a remote adversary. The manipulated part was then printed and then flight tested. After only a few minutes the manipulated part experienced a catastrophic failure at the site of the void, leading to the loss of the drone.

Yampolskiy et al. [42] argued that the anisotropy that is characteristic of additively manufactured components can be misused to degrade part quality. The effect of misoriented printing on mechanical properties has been shown by Zeltmann et al. [44] for polymers using the FDM process, where the tensile properties were reduced by over 20 percent using a printing orientation perpendicular to that of the control. For metal-based AM, Yampolskiy et al. [42] also argued that both scanning speed and strategy as well as the amplitude of the heat source can greatly sabotage the quality of parts produced by powder bed fusion.

Yampolskiy et al. [43] proposed a framework for analyzing attacks on or with AM. According to this framework, a variety of *attack vectors* can be used to compromise one or more elements of the AM workflow. The *compromised element(s)*, their roles in the workflow, and the degree to which an adversary can control these element(s) determine which *manipulations* an adversary can perform. These manipulations, in conjunction with the type of AM equipment, source materials, and object application area, determine the achievable *effects*. Only a fraction of the achievable

Figure 1: A PBF utilizing a windowed IR camera system.

effects intersect with the adversary's goals. The authors identify the intersection of attack effects and adversarial goals as *attack targets* (or *threats*).

Several analyses have been performed on the possibility of compromising AM equipment. Moore et al. [24] analyzed open source software that is commonly used with desktop 3D printers, namely Marlin firmware and three GUI applications that communicate with the printer via G-code: Cura 3D, ReplicatorG, and Repetier-Host. Their static analysis of the source code, along with dynamic analysis of the communication protocols between the 3D printer and the computer revealed numerous vulnerabilities that could be exploited in a malicious attack. Do et al. [10] analyzed a wireless communication protocol employed by a desktop 3D printer. Their analysis found vulnerabilities that could be exploited to stop current and submit a new prints. Moore et al. [25] empirically demonstrated that a malicious 3D printer firmware can arbitrarily manipulate manufacturing parameters, and modify or even completely replace the printed object.

3 BACKGROUND

In this section, we first outline the general Powder Bed Fusion (PBF) process and then discuss in detail how a typical IR thermography system is incorporated into the build process. Both provide information necessary to the security discussion that we present in Section 4.

3.1 Powder Bed Fusion (PBF)

While AM can be used with a broad (and ever increasing) variety of source materials, metal-based AM is being applied predominately for aerospace and medical applications. One of the most popular metal AM methods is powder bed fusion (PBF), a process in which a build plate is coated with a thin layer of metal powder which is then selectively melted. This process is repeated layer-by-layer to

completion. Laser based systems use an inert gas such as argon to fill the build chamber, whereas electron beam melting (EBM) systems require a vacuum [14].

Numerous parameters of the process can influence the manufactured part's mechanical properties. Gibson et al. [14] states that process parameters fit into one of four categories: laser-related parameters, scan-related parameters, powder-related parameters, and temperature-related parameters. Laser-related parameters include parameters such as laser power and spot size. Scan-related parameters include scan speed, hatch spacing, and scan strategy. Particle shape, size, and packing density fall under the powder-related parameters, whereas temperature-related parameters are typically a function of powder bed temperature and laser parameters. Some PBF parameters are strongly correlated. For example, a lower powder bed temperature and powder energy absorption rate would lead to a necessary increase the beam power.

In a typical production process, these parameters maintain a fixed value throughout the duration of the build; however, due to the inherent complexities associated with PBF, this static manufacturing method can be detrimental to final part quality [36]. An example of the necessity to alter parameters during manufacture is when creating a part with complex geometries such as overhanging surfaces [37]. Process parameters must be constantly adjusted as the part is manufactured. Various research efforts have focused on these parameters, particularly what effect each one has on final part build quality and how to best measure the effects of these parameters in-situ to allow for the purposeful manipulation of the process parameters to improve final build quality [21].

As current in-situ quality control methods cannot prevent issues like porosity, complicated post-processing procedures are applied to remedy the potential problems. In the case of PBF, hot isostatic pressing (HIP) is a post-processing method. HIP is a costly and time consuming process in which an object is placed into a high pressure, high temperature environment in order to alleviate various problems associated with this (and other) AM methods, primarily porosity [12]. However, HIP can also reduce yield strength due to the formation of undesirable microstructures [16]. The part will then go through further nondestructive evaluations to ensure that it is of acceptable quality.

3.2 Thermography in AM

The primary intent of IR thermographic in situ monitoring in AM is to detect, and evaluate the formation of voids in the manufactured object, referred to as porosity. Pores are voids formed in the object in its initial creation, either from an increase in heat leading to excessive melt pool turbulence and evaporation [9] or from an insufficient energy density leading to incomplete powder melting [4]. Another problem IR thermography aims to detect is non-uniformity in build temperature. Non-uniform object temperatures can lead to thermal stress and to undesirable microstructural variations in the object. This is a highly problematic outcome that can lead to a host of problems with the final quality of an object, such as strong anisotropic effects and reduction of tensile strength [45, 46].

IR thermographic monitoring systems entail the use of one or multiple IR and/or near IR cameras and often include single-point

IR pyrometers (e.g., fiber-coupled). These cameras are placed either behind a window looking directly into the build chamber, or are optically coupled into the imaging system of the build laser to obtain a coaxial view. In windowed setups, the window is made of a material suitable for high transmittance of infrared wavelengths such as germanium, as typical silica-based glass has unsuitably low transmittance in the wavelength range of most IR cameras (3-12 μm) [28]. In some systems, particularly EBM, a mechanical shutter system and/or protective film is also put in place to prevent damage to the window from the harsh environment of the build chamber, predominantly metallization that can occur from the melting of metal powder particles [33]. In this setup, the shutter is closed during operation of the laser or electron beam and briefly opens after the pass is finished to allow the IR camera to capture temperature data, particularly that of the melt pool. Camera data is processed by a software solution which can then, in the case of closed-loop systems, alter build parameters accordingly. This software solution uses computationally intensive image processing to allow for temperature stabilization and the detection of voids, the latter typically done by comparing captured image data to previously acquired example images of defective parts fabricated with PBF [23]. Accurate temperature readings are primarily dependent upon accurate calibration data [32].

Current experimental methods require workarounds for a lack of an application programming interface (API) for the control software; however, as in-situ process control methods mature they will likely be integrated by manufacturers.

3.2.1 Calibration. Quality control and assurance relies extensively on accurate sensor data. Calibration of IR imaging systems is of the utmost importance in the acquisition of temperature measurements precise enough to be used in an autonomous system. The accuracy of a thermal imaging system is dependent on the effect of environmental conditions (reflectivity) and surface properties (emissivity). The radiant energy emitted by an object is determined by its temperature, spectral emissivity (the object's ability to radiate energy), radiation from the surrounding enclosure, and atmospheric transmission. Rodriguez et al. [32] have shown that the main sources of thermographic disturbance are the ambient, reflecting sources, and the target's emissivity.

Several different readings must be taken to accurately calibrate the readings from inside the build chamber. A transmission value for the protective window through which the thermal camera looks must be recorded. This is done by heating a blackbody calibration source and comparing temperature readings from thermocouples to those given by the camera both with and without the window in place.

Ambient surface radiation is determined from the enclosure's material properties and mean radiant temperature. This involves taking temperature readings from all surfaces in an enclosure while at operating temperature and factoring these readings into the surface type of each wall, giving an accurate model for surface radiation emitted by the enclosure itself.

Most importantly, the emissivity of the material being used in manufacturing must be known. Commonly a blackbody cavity will be used for this purpose. Determination of the emissivity of a particular material involves fabrication of a blackbody cavity from

that material using the process that is being evaluated. This cavity is then thoroughly cleaned of any loose powder and heated. The blackbody design's emissivity is used as the default setting for the thermal camera. The absolute surface temperature given by thermocouples attached to the radiator is then compared to the thermal camera readings. The emissivity value used by the camera is then manually modified until its temperature reading is the same as the thermocouples'. The resulting emissivity value is the value assigned to the (solid) material in question. A similar process is then used to determine the emissivity of the unmelted powder present in the powder bed, whereby a thermocouple is embedded into a part and used to compare temperature readings with the camera [32].

3.2.2 Open-Loop Systems. Most currently implemented IR solutions are purely open-loop; that is, they exist solely for an operator to manually verify that a part is being manufactured correctly. In an open-loop system IR cameras are typically separate from the direct manufacturing process; that is, there exists an air-gap between the manufacturing and the quality control systems. IR data captured in open-loop systems is typically examined after the part has been manufactured as to gauge porosity in the final part as well as to ensure that the manufacturing process operated within specification. The open-loop process is heavily dependent upon traditional destructive evaluation techniques to certify part quality. If a part fails inspection, the IR imagery captured during production is used to enhance postmortem analysis of the failure. The trail-and-error necessitated by the use of an open loop system can increase costs and part turnaround times as compared to a closed loop system. However, an open loop system is significantly easier to design and operate, as well as requiring lower upfront costs.

3.2.3 Closed-Loop Systems. In a closed-loop system, the IR imaging system is expected to be integrated with the manufacturing control system to allow sufficiently fast feedback using programmable logic controllers (PLCs) or field-programmable gate arrays (FPGAs). IR camera(s) are used to measure the ongoing production process such that readings can be used to autonomously or semi-autonomously correct defects and keep process parameters within accepted operational ranges. Depending on the defect size and type, different actions are taken. Generated defects such as void formation can be actively monitored during a build and dealt with in-process through a combination of rescanning porous areas and increasing or decreasing energy densities proactively in order to prevent further void formation. Porosity can also be used as a measure to halt production or to flag a part for more rigorous post processing and qualification [22].

4 SECURITY ANALYSIS

In this section, we discuss how malicious manipulations on the IR thermography can be introduced via different attack vectors, and how each attack can affect final build quality.

4.1 Adversary Model

Section 2 outlines several AM-related attacks discussed in the research literature. The majority of these attacks contain classical cyber-security components. These include installation of malware [35] or a backdoor [6] on a controller PC, substitution of 3D

printer firmware with a malicious version [25], or exploitation of weaknesses in wireless communication protocols [10]. All these enable adversaries to tamper with digital blueprints in their various representations, e.g., STL files. While being very potent, these avenues of attack are obvious to cyber-security experts. Classical cyber-security means can be employed to effectively combat such attacks, e.g., by digitally signing a cryptographic hash value of a file. An increased awareness of potential cyber-security issues is motivating a push to employ various cyber-security means in the AM environment [3].

Industrial-grade AM machines consist of numerous diverse sub-systems. When these are compromised, attacks which are not limited to the controller PC, firmware, and networks can be staged. The situation becomes even more complicated for additive manufacturing because of its inherently *cyber-physical* nature. Sabotage attacks might not only change a part's 3D geometry, but also its microstructural properties [42]. Furthermore, such attacks can be performed not only directly, but also by more exotic means such as disturbing communication timing or impairing power supply [27, 41].

Cardenas et al. [7] identified tampering with sensor information a way to influence the behavior of a cyber-physical system (CPS) employing control loops. We apply this concept to a metal AM machine, focusing on *in-situ* IR thermography. In this paper, we assume that an adversary can manipulate any aspect of IR thermography, and focus solely on manipulations and their impacts on manufactured part quality. Specifically, we investigate whether and to what extent IR thermography alone can be used to perform sabotage attacks.

For this paper, we consider the motivation of an adversary to perform an attack via IR thermography to be out of scope. As an exemplary reason, this approach might minimize the probability of an attack being detected.

Similarly, we consider attack vectors which compromise components of IR thermography out of scope. Just to give an example, a supply chain attack can be used to compromise an IR camera's firmware or hardware. Introduced hardware Trojans can employ complex triggers that will prevent their detection during functional testing [29]; detecting Trojans via side-channel analysis might be limited by the Trojan's relative size [2].

4.2 Attack Methods

4.2.1 Calibration Data. Even when properly calibrated, obtaining true temperature readings from IR cameras is nearly impossible [26]. Thus, the alteration of any of the various data points which constitute this calibration data could influence the manufacturing process and thus have a dire impact on part quality. As stated in Section 3.2.1, these data points can include the transmission value of the window, emissivity of an object, emissivity of unmelted powder, reflection from the build chamber, and the camera's own internal diagnostic calibrations. The alteration of any one of these would introduce significant inaccuracies to the system's estimation of the melt pool and/or absolute skin temperature of the object.

In a closed-loop system, an attack that manipulates calibration data has the capability of directly impacting manufactured part quality. If the object is shown to be cooler than that of the actual temperature, the system will attempt compensation in the form

Figure 2: Causal chain resulting of an attack on calibration data in a closed-loop system.

of increased power densities, possibly far greater than nominal. This can lead to melt pool turbulence and evaporation of material, which in turn leads to both an increase in porosity and a negative change in grain structure growth, given a high enough temperature differential [19, 34].

Conversely, if the system is deceived into estimating that the object or melt pool is hotter than what is accurate, energy densities would be lowered dramatically. Depending on the temperature difference between the actual melt pool and the modified readings, the system would drastically lower energy densities. The direct consequences would include a significant amount of unmelted powder particles present in the part and a large increase of porosity. In addition, a large temperature differential between layers can lead to a large increase in porosity due to lack of fusion between layers. This is primarily due to the creation of a much shallower, less stable melt pool which does not adequately remelt lower layers to allow for proper fusion between layers [1]. Figure 2 shows a causal chain in the event of an attack.

While open-loop calibration data can be altered essentially the same way as closed-loop data, the consequences of such an attack do not directly affect the quality of the built part. Instead, an attacker has the capability of disrupting post-production quality control. In this case, compromised thermal imaging data could obscure generated part defects, possibly leading to a substandard part passing quality control. On the other end of the spectrum, an attacker also has the capability of disqualifying parts that are within specification, leading to either unnecessary post processing or total rejection of the part.

It is important to note that, in both open- and closed-loop systems, manipulations of calibration process will have a direct and identical effect on every layer of manufactured parts. Therefore, such attacks can be comparatively easily detected even via NDT testing of selected parts, including microscopy and subsequent morphology of last layer. A malware that periodically manipulates calibration data should be able to evade detection for a longer period of time, because only a fraction of parts will be manufacturing using corrupted calibration data.

4.2.2 Thermal Camera. Another element that can be compromised by an attack is the thermal camera itself. This attack affects both open-loop and closed-loop systems in similar ways, yet with a

couple of key differences. Aside from the obvious physical tampering of the camera, an inconspicuous and damaging attack would be to force the camera to remain on constantly. IR cameras are capable of logging immense amounts of data, and leaving one on all the time could fill the hard drive or saturate a network connection, forcing the system offline or creating errors in the analysis of data [26]. Another consequence of this action is the dramatic increase in processor and memory usage as all the image data is cataloged and analyzed.

In the case of a closed-loop system where processing power, primary, and possibly even secondary memory may be shared between the quality assurance and manufacturing systems, this could be very disruptive to the build process in ways that equipment manufacturers may have little to no safeguard for. Even if the processing subsystems are separate, a closed-loop system will be forced to enter some sort of “fail-safe” mode if the quality control system were to be brought offline. This would lead to a part that has very little guarantee of being defect-free and would have to be further examined before acceptance.

4.2.3 Reference Data. As part defects are detected by comparing captured image data to preexisting reference data, any alteration to the computational parameters used by the algorithm, or the images themselves could be an avenue of attack for a potential adversary. If an attacker increased the allowed computed tolerances or disabled the computation altogether between the two data sets, especially in association with attacks on other parts of the system, part defect generation could far exceed operational limits. Alternatively, a secondary attack could be performed in which the alteration of the reference process is not a direct attack on part quality but rather is used to effectively disable the system’s ability to detect the effects of attacks from other attack vectors. Such a surreptitious strategy could allow an attack to subsist much longer than another, more obvious attack. The effects of compromised reference data are principally identical in closed-loop and open-loop systems.

4.2.4 Shutter Mechanism. Another novel attack vector is an attack on the shutter mechanism. In electron beam based production systems, forcing the shutter to remain open for longer than it should, or even permanently, would cause the glass to become appreciably metalized; this would lead to a drastic decrease in the

Defect	Description	Effects on part quality	Example
Pores	Voids either within a layer or between layers caused by lack-of-fusion or gas entrapment, typically due to improper energy densities.	Decreased ultimate tensile strength Decreased yield strength Decreased elongation Increased fatigue crack initiation Increased anisotropic effects
Lack of fusion	Unfused powder in final object caused by improper energy densities, primarily very low energy densities.	Decreased ultimate tensile strength Decreased yield strength Decreased elongation Increased fatigue crack initiation Increased anisotropic effects Difficult to detect using standard nondestructive evaluation methods
Cracks	Cracks formed inside an object, typically from residual stress due to the complex heating/cooling cycles experienced	Decreased high and low cycle fatigue performance

Table 1: Defects possible through attacks on IR thermography based PBF systems

window's ability to pass IR radiation through to the camera it protects. This decrease in transmittance would effectively cripple the camera by reducing the blackbody radiation reaching the sensor and therefore the computed temperature values. This would lead to the false conclusion that increased energy densities would be necessary to maintain optimal operational temperatures. Another prospective attack is to force the shutter to activate much on a different period as compared to the exact frequency needed to capture the images at the given framerate, interrupting image capture when the time periods overlap. This would induce an effect in which the amount of time the sensor is exposed for each picture and, as a result, temperature estimates would fluctuate wildly as a function of time.

4.2.5 Control Loop. The previously described attacks are indiscriminate and, therefore, can be easily detected. Attacks on the control loop itself, on the contrary, can be both targeted and potentially stealthy. Cardenas et al. [7] identify that in a control loop governed cyber-physical system, both controller and its associated communication channels (from sensors to controller, and from controller to actuators) can be compromised; additionally, communication channels can be interrupted. Pope et al. [27] further argue that the disruption of communication timing (even without altering

commands and sensor information) might result in disruption of AM process.

If any of these manipulations can be introduced arbitrarily into a control loop, an adversary can achieve a selective impact on a sub-set of part's layer. This might drastically reduce detectability of an attack using NDT. False IR sensor information will lead to overreactions described above and summarized in Figure 2. The effects of communication interruption might vary between different equipment; it can include a fail-safe stop of manufacturing process, or continuation of the process based on the latest received data. Disruption of communication timing will lead to skipped adjustments for few layers and then to overreaction for several subsequent layers. The affected layers may show effects like increased porosity and others described above (summarized in Table 1).

Even more powerful is an amplification of feedback, in turn forcing an overreaction from the control system. This has the possibility of forcing a runaway reaction where the system oscillates wildly, leading to any number of undesirable behaviors. This could include the effects of any of the aforementioned attacks.

Alteration of environmental variables within the build chamber would have a devastating effect on both part viability and manufacturing equipment. In electron beam-based systems, where manufacture takes place in a vacuum, and laser-based systems, where the build chamber is filled with an inert gas during production,

Figure 3: Metal AM equipment used in experiments

increasing the amount of ambient air present in the build chamber can lead to oxidation in the part and lower energy beam efficiencies [30]. Another consequence of higher-than-optimal ambient air ratios is the possibility of a fire or explosion when combustible materials around or above their flashpoint mix with oxygen from the ambient air.

An attacker could also use a denial-of-service attack to attempt to disrupt the controller (or controlling computer), thus halting production and requiring a re-establishment of the melt pool or proper operating conditions within the build chamber.

5 EXPERIMENTAL EVALUATION

In this section we present experimental evaluation of cyber attacks on a laser driven temperature control loop. Current commercial machines do not incorporate pyrometer or thermal camera based feedback to stabilize the melt pool temperatures in powder bed AM machines, so an experimental control loop was setup in a research AM machine. Here we present evidence recorded using our experimental control loop that cyber attacks can modify the quality of laser welds when the laser power is controlled by a feed back loop.

5.1 Experimental Environment

The AM machine used for powder bed fusion research (see Figure 3) is split into two basic parts: the optical arm and the chamber for powder spreading. The optical arm consists of a 400 W, 1070 nm wavelength laser, synchronized to a 3-axis galvanometer scanning system. The chamber consists of a piston with an attached substrate plate, that powder is spread over. In this experiment no powder was used and the substrate plate, made of 316L stainless steel was directly exposed to the laser. The laser forms a liquid melt pool of 200 μm diameter, larger than the 100 μm beam diameter. The temperature of the melt pool is above 1700 C and incandesces in the near IR. Traveling backwards through the scanner opposite the laser light the incandescence is directed onto a pyrometer through a dichroic mirror (see Figure 4). The pyrometer signal varies monotonically with the temperature of the melt pool. It is aligned to

Figure 4: Layout of used IR thermography system

average the signal originating from an area that covers the entire melt pool.

Closed loop control was implemented by splitting the analog signal that normally adjusts the laser power synchronously with mirror positions. The signal from the scanner mirror controller was treated as the temperature setpoint, by multiplying by a factor of 10. Hence a commanded 200 W laser weld was interpreted as a 2000 C laser weld. Open loop recordings of the pyrometer signal were captured at laser powers between 50 and 350 W. The signal was observed to vary linearly with a slope of 0.00275 V/W in the range of 50 to 200 W. Above 200 W the slope changes due to the onset of boiling. An approximate calibration was created assuming the change to boiling at 200 W occurred at 3000 C. The linear calibration constant was nominally 5500 C/V, but was changed to 7000 C/V to simulate an attack that exploits changing a temperature calibration. LabVIEW was used to program a digital acquisition device, to read in the setpoint and melt pool temperature, and to implement a PI feed back loop that outputs another analog signal to adjust the power of the laser. This last signal closes the gap formed by splitting the original signal from the scanner mirror controller that controls the laser power. Tuning of the proportional and integral constants was achieved, by creating weld tracks on the substrate plate while recording the system response to a change in the melt pool setpoint. The first constant was $1.5\text{e-}4$ and the second $3\text{e-}6$. The time step used for integration was based on the chosen control loop rate.

Besides the calibration attack, two other attacks were tested. The control loop was operated nominally at 20 kHz, but reduced to 1 kHz in order to simulate a denial-of-service attack, or other resource consuming attack that slows the control loops response time. The final attack tested adds signal to the pyrometer signal before entering the feed back loop. This simulates a NIR light source being placed in the optical train, or any other form of electromagnetic based attack on the pyrometer signal. The false signal function, implemented in LabVIEW, randomly picks a new temperature offset in the range -500 C to 500 C and adds it to the scaled pyrometer signal for 200 loop cycles or 10 ms.

Figure 5: Plot of the temperature of the melt-pool input to the control loop (top) and the laser power output of the control loop (bottom) as a function of time. Data taken during a 15 mm weld at 150 mm/s with a melt-pool temperature setpoint of 2000 C. No attack (solid) compared with a calibration attack (dots), loop rate attack (dashes) and false signal attack (small dots).

Figure 6: Composite image showing a height map and optical image of the weld tracks created under four different attack scenarios: no attack (A) compared with a calibration attack (B), loop rate attack (C) and false signal attack (D).

5.2 Experimental Evaluation

The response of the control system for each laser weld is evaluated by plotting the melt-pool temperature which is the process variable and the laser power which is the control loop output as a function of time. If the feedback loop is correctly tuned the melt-pool temperature will follow the setpoint, while the laser power varies to compensate for changing response of the interaction between the laser and the melt-pool. Figure 5 shows a plot of the control loop signals for 15 mm long, weld tracks created on a stainless steel substrate plate. Each track was scanned at a speed of 150 mm/s and required 0.1 s to complete. The control loop was held at a melt-pool

setpoint of 2000 C. It's clear that all of the pyrometer measurements centered around the setpoint indicating the control loop was closed and reasonably tuned, with the laser power varying to compensate for unexpected changes in temperature or due to a simulated cyber attack.

Comparing the control and calibration attack traces, it appears both are stable. The only difference is the output power dropped from an average of 150 W during the control trace to 125 W during the calibration attack. This makes a calibration attack particularly hard to detect by reviewing the control loop response while it's running. Of course part quality would be significantly effected

due to the lower scanning power, which may result in lack of fusion defects, or at low levels will result in layer delamination and eventual print loss. Since the calibration file is generally read only at system start up, the quality of the print can not be varied in time, to prevent detection.

The control loop speed must be faster than the physical response of the system, which is the amount of time it takes for the melt pool temperature to increase or decrease after a change in laser power. This can be estimated by calculating the time it takes the beam to travel one beam width, after which it's heating a new spot on the substrate and given a different power will result in a different melt-pool temperature. For 150 mm/s and 100 μm beam size the response is 666 μs . Running the control loop at 20 kHz is fast enough to adequately control the melt pool temperature for most conditions expected in a typical machine, but 1 kHz is not. Looking again at the control loop plot, it's clear the reduction in loop rate drove the control loop into deep oscillation. This is the most dramatic of the four attacks tested, and would be the easiest to detect. The response of the control loop to false sensor data is the same as it's response to real sensor data. At 0.04 s, a large positive offset in the pyrometer signal for the false data trace is observed. At this point, the false sensor data function added 500 C to the measured temperature. The response of the control loop is to reduce the laser output power to compensate which can be seen in the laser power trace. This has a similar effect to the calibration attack, but can vary in time making it more difficult to detect, as it may be assumed to be a real correction to unexpected changes in the melt pool temperature.

A height map and optical image of the weld tracks is shown in Figure 6. Track B which was created with the increased calibration constant has a reduced height compared to track A with the lower calibration constant. This also indicates a shallower melt pool depth which could lead to lack of fusion during powder welding. The loop rate attack, track C, shows the strong laser power modulation both in width and height. The tracks were scanned left to right in the image and the point where the height changes in track D (about 1/3 of the total distance), corresponds to the time 0.04 when the large positive false data attack occurred.

6 DISCUSSION

As PBF relies on a number of interrelated process parameters, any change to any particular parameter can influence final part quality and performance. Kamath et al. [18] have found that the most important process parameters are laser speed and power. Thus, any attack that either directly or indirectly alters one or both parameters is exceptionally dangerous.

Perhaps the easiest defect to impart on an object through an attack on the production process is an increase in porosity. Galaraga, et al., concludes that porosity has a negative effect on tensile properties such as ultimate tensile strength, yield strength, and elongation [13]. Also noted is the presence of unmelted powder particles as crack nucleation sites, reducing mechanical properties and having a significant impact on cyclic load performance [20, 39]. In scenarios in which a part will be subjected to high cyclic loads, porosity will lead to a dramatically reduced lifespan, if not a total failure of the part.

An attacker wishing for a more surreptitious attack will force low energy density levels in order to create lack of fusion defects, leading to pores filled with unmelted or partially melted powder particles. These defects are much harder to diagnose using nondestructive evaluation techniques such as the widely-used Archimedes method suggested by ASTM [15, 17]. As a result, the best way to be truly sure a part is within specifications is by using destructive testing methods such as microscopy and strength testing. Effects on part strength are equivalent to those from voids.

The defensive options against the presented sabotage attacks via IR thermography are worrisome. Current cyber-security solutions are not built to analyze the IR camera's firmware (or its behavior); it is further unlikely that existing antivirus software will be able to distinguish between malicious and non-malicious firmware updates for the camera. Acoustic side-channel-based approaches proposed by Chhetri et al. [8] and Belikovetsky et al. [5], while showing very good results on FDM technology, cannot be applied to detect the presented attacks due to significant differences with PBF. Among the main factors, the proposed attacks will not impact the behavior of any mechanical parts, thus avoiding differences in generated sound.

7 CONCLUSION

The use of additive manufacturing has grown dramatically both in consumer and industrial sectors in recent years. Barriers to its widespread adoption still exist, primarily due to a lack of *in-situ* quality control methods and intellectual property protection. However, significant progress continues to be made towards the ultimate goal of an additive manufacturing sector competitive with traditional subtractive manufacturing. With the increasing use of additive processes comes the corresponding increase of attention by malicious actors to subvert these processes. To date, the necessary installation of closed-loop control systems to the additive manufacturing process has not been studied as an attack surface by these adversarial actors. We have found that the addition of *in-situ* quality assurance systems built upon infrared thermography present a number of novel attack vectors. Such an attack has the potential to be devastating, as processing parameters in PBF are so interrelated that the ability to indirectly manipulate just one process parameter has the capability to invalidate an entire production cycle.

In the future, we plan to quantify the exact correlations between various IR thermography parameters, their impact on the process parameters, and final part quality. Conversely, research must take place on how to best defend against such indirect attacks.

ACKNOWLEDGMENTS

This work was partially funded through a Laboratory Directed Research and Development grant 15-ERD-037 and performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344.

This work was supported by the Alabama Cyber Research Consortium (ALCRC).

REFERENCES

- [1] Arcam AB. 2016. Electron Beam Melting - EBM Process, Additive Manufacturing. (2016). <http://www.arcam.com/technology/electron-beam-melting/> Accessed: 2017-03-08.
- [2] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. 2007. Trojan detection using IC fingerprinting. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 296–310.
- [3] America Makes & ANSI Additive Manufacturing Standardization Collaborative (AMSC). 2017. *AMSC Standardization Roadmap for Additive Manufacturing*. Technical Report.
- [4] Hooyar Attar, Mariana Calin, LC Zhang, Sergio Scudino, and Jürgen Eckert. 2014. Manufacture by selective laser melting and mechanical behavior of commercially pure titanium. *Materials Science and Engineering: A* 593 (2014), 170–177.
- [5] Sofia Belikovetsky, Yosef Solewicz, Mark Yampolskiy, Jinghui Toh, and Yuval Elovici. 2017. Detecting Cyber-Physical Attacks in Additive Manufacturing using Digital Audio Signing. *arXiv preprint arXiv:1705.06454* (2017).
- [6] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, and Yuval Elovici. 2016. dr0wned-Cyber-Physical Attack with Additive Manufacturing. *arXiv preprint arXiv:1609.00133* (2016).
- [7] Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. 2008. Secure control: Towards survivable cyber-physical systems. In *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 495–500.
- [8] Sujit Rokka Chhetri, Arquimedes Canedo, and Mohammad Abdullah Al Faruque. 2016. KCAD: Kinetic Cyber Attack Detection Method for Cyber-Physical Additive Manufacturing Systems. In *Proceedings of the 35th International Conference on Computer-Aided Design*. ACM, 74.
- [9] Stijn Clijsters, Tom Craeghs, Sam Buls, Karolien Kempen, and J-P Kruth. 2014. In situ quality control of the selective laser melting process using a high-speed, real-time melt pool monitoring system. *The International Journal of Advanced Manufacturing Technology* 75, 5-8 (2014), 1089–1101.
- [10] 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.
- [11] Sarah K Everton, Matthias Hirsch, Petros Stravroulakis, Richard K Leach, and Adam T Clare. 2016. Review of in-situ process monitoring and in-situ metrology for metal additive manufacturing. *Materials & Design* 95 (2016), 431–445.
- [12] William E Frazier. 2014. Metal additive manufacturing: a review. *Journal of Materials Engineering and Performance* 23, 6 (2014), 1917–1928.
- [13] Haize Galarraga, Diana A Lados, Ryan R Dehoff, Michael M Kirka, and Peeyush Nandwana. 2016. Effects of the microstructure and porosity on properties of Ti-6Al-4V ELI alloy fabricated by electron beam melting (EBM). *Additive Manufacturing* 10 (2016), 47–57.
- [14] Ian Gibson, David W Rosen, Brent Stucker, et al. 2010. *Additive manufacturing technologies*. Vol. 238. Springer.
- [15] Haijun Gong, Khalid Rafi, Hengfeng Gu, GD Janaki Ram, Thomas Starr, and Brent Stucker. 2015. Influence of defects on mechanical properties of Ti-6Al-4V components produced by selective laser melting and electron beam melting. *Materials & Design* 86 (2015), 545–554.
- [16] Sean Gribbin, Jonathan Bicknell, Luke Jorgensen, Igor Tsukrov, and Marko Knezevic. 2016. Low cycle fatigue behavior of direct metal laser sintered Inconel alloy 718. *International Journal of Fatigue* 93 (2016), 156–167.
- [17] ASTM International. 2015. ASTM B962-15, Standard Test Methods for Density of Compacted or Sintered Powder Metallurgy (PM) Products Using Archimedes' Principle. (2015). www.astm.org
- [18] Chandrika Kamath, Bassem El-dasher, Gilbert F Gallegos, Wayne E King, and Aaron Sisto. 2014. Density of additively-manufactured, 316L SS parts using laser powder-bed fusion at powers up to 400 W. *The International Journal of Advanced Manufacturing Technology* 74, 1-4 (2014), 65–78.
- [19] Saad A Khairallah, Andrew T Anderson, Alexander Rubenchik, and Wayne E King. 2016. Laser powder-bed fusion additive manufacturing: physics of complex melt flow and formation mechanisms of pores, spatter, and denudation zones. *Acta Materialia* 108 (2016), 36–45.
- [20] Qian Chu Liu, Joe Elambasseril, Shou Jin Sun, Martin Leary, Milan Brandt, and Peter Khan Sharp. 2014. The effect of manufacturing defects on the fatigue behaviour of Ti-6Al-4V specimens fabricated using selective laser melting. In *Advanced Materials Research*, Vol. 891. Trans Tech Publ, 1519–1524.
- [21] Mahesh Mani, Brandon Lane, Alkan Donmez, Shaw Feng, Shawn Moylan, and Ronnie Feserman. 2015. Measurement science needs for real-time control of additive manufacturing powder bed fusion processes. *National Institute of Standards and Technology, Gaithersburg, MD, Standard No. NISTIR 8036* (2015).
- [22] Jorge Mireles, Shakerur Ridwan, Philip A Morton, Alejandro Hinojos, and Ryan B Wicker. 2015. Analysis and correction of defects within parts fabricated using powder bed fusion technology. *Surface Topography: Metrology and Properties* 3, 3 (2015), 034002.
- [23] Jorge Mireles, Cesar Terrazas, Sara M Gaytan, David A Roberson, and Ryan B Wicker. 2015. Closed-loop automatic feedback control in electron beam melting. *The International Journal of Advanced Manufacturing Technology* 78, 5-8 (2015), 1193–1199.
- [24] Samuel Moore, Phillip Armstrong, Todd McDonald, and Mark Yampolskiy. 2016. Vulnerability analysis of desktop 3D printer software. In *Resilience Week (RWS), 2016*. IEEE, 46–51.
- [25] Samuel Bennett Moore, William Bradley Glisson, and Mark Yampolskiy. 2017. Implications of Malicious 3D Printer Firmware. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- [26] Shawn Moylan, Eric Whitenon, Brandon Lane, John Slotwinski, Dale E Chimenti, Leonard J Bond, and Donald O Thompson. 2014. Infrared thermography for laser-based powder bed fusion additive manufacturing processes. In *AIP Conference Proceedings*, Vol. 1581. AIP, 1191–1196.
- [27] Gregory Pope and Mark Yampolskiy. 2016. A Hazard Analysis Technique for Additive Manufacturing, In Better Software East Conference. *arXiv preprint arXiv:1706.00497*.
- [28] Tuomas Purtonen, Anne Kalliosaari, and Antti Salminen. 2014. Monitoring and adaptive control of laser processes. *Physics Procedia* 56 (2014), 1218–1231.
- [29] Reza M Rad, Xiaoxiao Wang, Mohammad Tehranipoor, and Jim Plusquellic. 2008. Power supply signal calibration techniques for improving detection resolution to hardware Trojans. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 632–639.
- [30] HK Rafi, NV Karthik, Haijun Gong, Thomas L Starr, and Brent E Stucker. 2013. Microstructures and mechanical properties of Ti6Al4V parts fabricated by selective laser melting and electron beam melting. *Journal of Materials Engineering and Performance* 22, 12 (2013), 3872–3883.
- [31] GE Reports. 2014. *Fit To Print: New Plant Will Assemble World's First Passenger Jet Engine With 3D Printed Fuel Nozzles, Next-Gen Materials*. Technical Report. <http://www.gereports.com/post/80701924024/fit-to-print>
- [32] Emmanuel Rodriguez, Jorge Mireles, Cesar A Terrazas, David Espalin, Mireya A Perez, and Ryan B Wicker. 2015. Approximation of absolute surface temperature measurements of powder bed fusion additive manufacturing technology using in situ infrared thermography. *Additive Manufacturing* 5 (2015), 31–39.
- [33] Jan Schwerdtfeger, Robert F Singer, and Carolin Körner. 2012. In situ flaw detection by IR-imaging during electron beam melting. *Rapid Prototyping Journal* 18, 4 (2012), 259–263.
- [34] Kei Shibata, Wataru Ishigaki, Takuma Koike, Tomoki Umetsu, Takeshi Yamaguchi, and Kazuo Hokkirigawa. 2016. Friction and wear behavior of stainless steel fabricated by powder bed fusion process under oil lubrication. *Tribology International* 104 (2016), 183–190.
- [35] L Sturm, CB Williams, JA Camello, J White, and R Parker. 2014. Cyber-physical vulnerabilities in additive manufacturing systems. *Context* 7 (2014), 8.
- [36] Gustavo Tapia and Alaa Elwany. 2014. A review on process monitoring and control in metal-based additive manufacturing. *Journal of Manufacturing Science and Engineering* 136, 6 (2014), 060801.
- [37] Di Wang, Yongqiang Yang, Ziheng Yi, and Xubin Su. 2013. Research on the fabricating quality optimization of the overhanging surface in SLM process. *The International Journal of Advanced Manufacturing Technology* 65, 9-12 (2013), 1471–1484.
- [38] Terry Wohlers. 2017. *Wohlers Report 2017 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report*. Wohlers Associates, Inc., Fort Collins, Colorado, USA. www.wohlersassociates.com.
- [39] Eric Wycisk, Andreas Solbach, Shafaqat Siddique, Dirk Herzog, Frank Walther, and Claus Emmelmann. 2014. Effects of defects in laser additive manufactured Ti-6Al-4V on fatigue properties. *Physics Procedia* 56 (2014), 371–378.
- [40] Xiao Zi Hang (Claud Xiao). 2013. Security Attack to 3D Printing. (2013). <http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf> Keynote at XCon2013.
- [41] Mark Yampolskiy, Wayne E. King, Gregory Pope, Sofia Belikovetsky, and Yuval Elovici. 2017. Subtractive vs. Additive Manufacturing: Similarities and Differences from the Security Perspective. In *Critical Infrastructure Protection XI*. Springer.
- [42] Mark Yampolskiy, Lena Schutzle, Uday Vaidya, and Alec Yasinsac. 2015. Security Challenges of Additive Manufacturing with Metals and Alloys. In *Critical Infrastructure Protection IX*. Springer, 169–183.
- [43] Mark Yampolskiy, Anthony Skjellum, Michael Kretschmar, 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.
- [44] Steven Eric Zeltmann, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. 2016. Manufacturing and Security Challenges in 3D Printing. *JOM* (2016), 1–10.
- [45] Kai Zeng, Deepankar Pal, and Brent Stucker. 2012. A review of thermal analysis methods in Laser Sintering and Selective Laser Melting. In *Proceedings of Solid Freeform Fabrication Symposium Austin, TX*.
- [46] Yuwei Zhai, Haize Galarraga, and Diana A Lados. 2015. Microstructure evolution, tensile properties, and fatigue damage mechanisms in Ti-6Al-4V alloys fabricated by two additive manufacturing techniques. *Procedia Engineering* 114 (2015), 658–666.