LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-JRNL-738793

Security of Additive Manufacturing: Attack Taxonomy and Survey

M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, Y. Elovici

September 21, 2017

Additive Manufacturing

Disclaimer

LLNL-JRNL-738793

Security of Additive Manufacturing: Attack Taxonomy and Survey

Mark Yampolskiy[a,*], Wayne E. King[b], Jacob Gatlin[a], Sofia Belikovetsky[c], Adam Brown[a], Anthony Skjellum[d,e], Yuval Elovici[c,f,g]

[a] *University of South Alabama*
[b] *Lawrence Livermore National Laboratory*
[c] *Ben-Gurion University of the Negev*
[d] *University of Tennessee at Chattanooga*
[e] *Auburn University*
[f] *Cyber Security Research Center*
[g] *Singapore University of Technology and Design*

Abstract

Additive Manufacturing (AM) is a rapidly growing, multibillion dollar industry. AM is increasingly being used to manufacture functional parts, including components of safety critical systems in aerospace, automotive, and other industries. This makes AM an attractive attack target. AM Security is a fairly new field of research that address novel threat.

This paper serves dual purposes: For researchers just entering AM Security, we provide an in-depth introduction to this highly multi-disciplinary research field. And, for active researchers in the field, this paper provides a comprehensive, structured survey of the state of the art, and our proposal for attack taxonomies.

Keywords: `Additive Manufacturing`, 3D Printing, AM Security, Taxonomy, Survey

1. Introduction

Additive Manufacturing (AM), also known as 3D printing, is a process that joins layers of deposited material to make objects based on 3D model data. Compared to traditional manufacturing, AM has numerous socioeconomic, environmental, and technical advantages. It enables shorter design-to-product

*Corresponding author
Email addresses: `yampolskiy@southalabama.edu` (Mark Yampolskiy), `king17@llnl.gov` (Wayne E.King), `jrg1222@jagmail.southalabama.edu` (Jacob Gatlin), `sofia.belikovetsky@gmail.com` (Sofia Belikovetsky), `ajb1425@jagmail.southalabama.edu` (Adam Brown), `Tony-Skjellum@utc.edu` (Anthony Skjellum), `yuval_elovici@sutd.edu.sg` (Yuval Elovici)

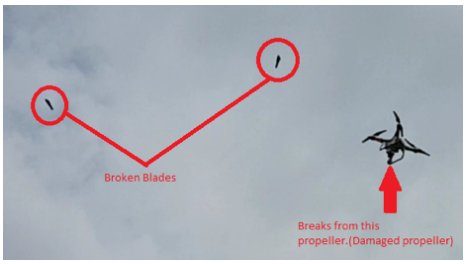

Figure 1: Sabotaged Propeller Breaks During Flight (*dr0wned* Study [6])

time, just-in-time and on-demand production, all in close proximity to assembly lines. AM can produce functional parts with complex internal structures and optimized physical properties, with less material waste than subtractive manufacturing. These properties have made AM a rapidly growing multibillion dollar industry; it is increasingly being used to manufacture functional, safety-critical parts in the aerospace, automotive, and other industries.

Industry 4.0 envisions fully automated manufacturing environments, driven by computerized manufactured equipment—Cyber-Physical Systems (CPS). Additive Manufacturing is a core component in this vision, enabling both manufacturing automation and the creation of parts with properties that could not be achieved with the traditional subtractive manufacturing.

One of the recent examples of AM adoption is GE's fuel nozzle for the next generation LEAP jet engine [1, 2]. Through the use of part consolidation, GE has created a part five times more durable, 25% lighter, and 20% more temperature resistant than would otherwise be possible with typical subtractive manufacturing processes.

According to the Wohlers report [2], in 2016 the AM industry accounted for $6.063 billion of revenue; 33.8% of all AM-produced objects were used as functional parts. A study conducted by Ernst & Young [3] shows rapidly growing adoption of this technology worldwide. In the U.S. alone, 16% of companies surveyed have experience with AM while another 16% are considering adopting this technology in the future. Numerous studies agree that these numbers will continue to rise, potentially leading to the dominance of AM as *the* manufacturing technology of the future [4, 5].

The rapid adoption of AM will likely have geopolitical, socioeconomic, and other ramifications [7, 8, 9]. These can motivate a broad array of cyber- and cyber-physical attacks performed by adversaries from individuals up to and including state actors. The technical feasibility of such attacks has been demonstrated in the research literature; for instance, in the *dr0wned* study conducted by Belikovetsky et al. [6, 10] researchers sabotaged a propeller design. In that study, the 3D-printed, sabotaged propeller broke after a short flight time, causing it to fall and suffer significant damage (see Figure 1).

The need to secure Cyber-Physical Systems (CPS) gives rise to the corresponding need to understand potential attacks, including attacks via manufac-

turing systems. This paper aims to support research on *AM Security*. For researchers just entering AM Security, we provide an in-depth introduction to this highly multi-disciplinary research sub-field. For active researchers in security, this paper provides a structured and comprehensive survey of the state of the art, and presents our proposal for a structured view on the subject matter.

This paper is structured as follows: First, as a basis for the future discussion, we outline the AM workflow in Section 2. We emphasize the complexity and often inter-disciplinary nature of present cyber and physical interactions. Then, in Section 3, we describe how security of such complex systems can be approached methodically. At a first step, we introduce a framework for analysis of attacks *on* or *with* AM. Then, we present the major security threat categories identified for AM. Two of the threat categories, *theft of technical data* and *AM sabotage*, comprise the focus of this paper. Furthermore, we outline benefits and challenges of knowledge systematization in a taxonomical form. It is our view that existing research related to AM vulnerabilities and attacks has garnered sufficient knowledge to justify our current effort to define taxonomies that enumerate aspects of attacks *on* or *with* AM. In our proposal (presented in Sections 4 and 5), we focus exclusively on aspects covered by relevant natural sciences, such as cyber-security or materials science. For both threat categories, we define two top-level taxonomy branches for *attack targets* and *attack methods*. For each taxonomy, we indicate those methods that can achieve given targets. In Section 6, we provide a structured and comprehensive survey of peer-reviewed literature in the area, including conducted attacks, proposed defense measures, and discussed legal aspects. When covering attack-related literature, we indicate which elements of the taxonomies have been addressed by particular publications.

Significantly, our discussion of the surveyed literature in Section 7 shows that many aspects of AM security remain unaddressed. We conclude with a brief summary of our contributions and identified gaps.

2. Additive Manufacturing Workflow

3D printing is not an isolated process; it is embedded in a complex web of automated and manual workflows in which various dependencies—including physical and informational—can be defined. AM workflows might vary drastically based on the AM process employed[1], source materials used[2], and whether manufacturing is performed by the end-users or provided as a service[3]. In this

[1]The American Society for Testing and Materials (ASTM) defines seven different AM process categories [11, 2]; each of these can have several sub-categories, often referred to as AM technology.

[2]Currently, polymers (plastics) and metals/alloys are the most commonly used source materials. AM with other source materials (such as ceramics) is an active area of research and development.

[3]As of September 2017, *3D Printing Businesses* web site (http://3dprintingbusiness.directory/) lists 936 companies offering 3D printing service,

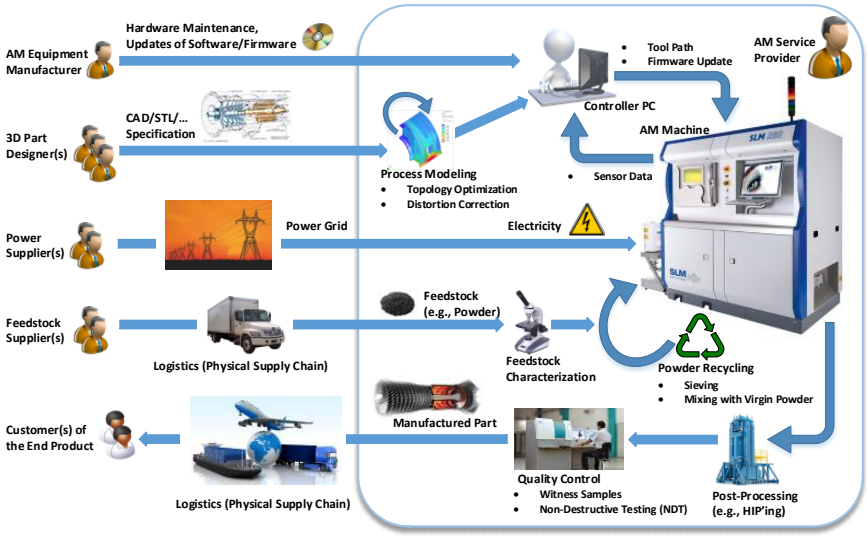

Figure 2: Additive Manufacturing Workflow

section, we outline a workflow that is common in metal AM. Most functional and safety-critical AM parts are produced in metal, and it is generally the most complex type of AM process.

Two AM processes are predominantly employed to work with metals, *power bed fusion* (PBF)[4] and *direct energy deposition* (DED)[5]. PBF enables manufacturing of parts with tight tolerances, but is limited in size to two square feet; DED can produce larger parts, but requires extensive post processing for acceptable surface finishes. We consider a workflow that employs power bed fusion technology.

Figure 2 represents a simplified workflow common in metal AM when manufacturing is provided as a service. This workflow includes multiple actors, a variety of computerized systems, multiple software applications, numerous data transportation methods, and the transportation of physical items (*e.g.,* source materials). Not all of the elements in this workflow are located in the *controlled*

48 of which include metal printing.

[4]A thin layer of powdered source material is used in PDF Processes, most often either metal or polymer in composition, which is distributed in a bed. A heat source is used to fuse each layer (for instance, laser or electron beam); that source melts the surface of the each slice in turn of the 3D part under fabrication. Layer-by-layer, the distribution of the powder source material and subsequent fusion procedure is sequenced until the part is complete.

[5]Directed Energy Deposition (DED) refers to a process in which source material (in a powder or wire form) is deposited on the surface through a nozzle mounted on a multi-axis arm. While depositing, the material is melted by a heat source, usually a laser, electron beam, or plasma arc.

environment of the AM service provider (as indicated with a rectangle on the right side of the figure). Multiple actors, most of which represent enterprises, are involved in AM and provide or consume different services.

AM equipment (not limited to the actual "3D printer") is usually developed and provided by an original equipment manufacturer (OEM)[6]. Along with the machine, the manufacturer provides hardware maintenance along with software and firmware updates. If allowed, some of this is done via remote Internet connection. Some is also accomplished on-site by a representative of the manufacturer with hands-on access to the machine and computers. For maintenance and repair, various mechanical, electrical, and electronic components (motors, filters, etc.) might be required. These are manufactured and sold by the OEM or third-party providers, and shipped via physical carrier.

The part manufacturing process begins with a designer and a Computer-Aided Design (CAD) software package, and possibly a topology optimization application. A model representation of the part (in CAD, STL, or other formats[7]) is transferred to the additive manufacturing service provider, often via network.

At the service provider, the file is delivered to one or more computers. Depending on a part's application area, material employed, and AM technology, the design file might undergo several additional optimization steps. For instance, the designed part might be analyzed and corrected for in-process distortion[8] by process modeling. This step is typically performed at the AM service provider site; the service provider can model the process with the full knowledge of the AM process and equipment specifics.

The conversion of a design file into actual *tool path* commands for a particular AM machine consists of several steps. The solid model is first converted to a format that is accepted by the slicing software, usually STL. This step often requires repair of the STL file to ensure that it is a "water-tight" solid volume [17]. Then, the file is "sliced" into sections that define the thickness of each manufactured layer (this process is done either at the AM machine's computer or elsewhere). The software that slices the STL file usually has an "add-in" from the AM machine provider that ensures the slice file (.sli) contains the required machine-specific commands. At this point, the sliced file is passed

[6] As of March 2017, 97 system manufacturers in 20 countries (37 in Europe, 20 in the U.S., 19 in China, 10 in Japan, four in South Korea, three in Israel, and one each in Australia, Singapore, South Africa, and Taiwan) were actively manufacturing and selling AM systems of industrial-grade. Hundreds of smaller companies evidently offer desktop 3D printers as well [2].

[7] The legacy STereoLithography [12] (STL) remains the most common file format describing an object's geometry for 3D printing. The abbreviation STL is overloaded with several 'backronyms" including but not limited to Standard Tesselation Language, Surface Tesselation Language, etc. Compared to STL, the recently adopted Additive Manufacturing File (AMF) format [13, 14] url2014amfstd and 3D Manufacturing Format (3MF) [15, 16] can specify 3D geometry with a higher precision and also enable additional features such as the incorporation of multiple materials.

[8] Distortions can occur because of overhang structures or high temperature gradients.

to the AM machine where the machine operator lays the part out on the build plate, selects the build orientation, applies support structures, and enters the relevant laser and layer parameters for the build. Vendor-specific software then generates the laser path plan for each slice. The build instructions[9] are sent directly to the machine for execution (without being stored).

Meanwhile, the feedstock (the raw material) must also be prepared for use. Service providers may or may not characterize the feedstock to ensure that it meets specifications. During feedstock characterization, parameters like material chemistry, particle size, shape, and homogeneity are examined; all these can impact the material properties of produced parts [19]. It is, however, a time- and labor-intensive process, and there is still much to learn about what needs to be characterized.

Feedstock is typically purchased from a vendor, which may or may not be the producer of said raw material. The feedstock can be purchased to specification or ordered such that it falls within a range of parameters. A number of additive manufacturing machine makers require that powder be purchased through their supply chain to maintain the machine warranty. The powder needs to be kept dry in an oxygen free environment[10].

During the manufacturing process, AM equipment consumes electricity and a variety of source and auxiliary materials. While source materials are included in the end-product, auxiliary materials provide support or enable production in some way. For instance, support structures enable the printing of complex geometries; inert gas (usually, argon) is often used if lasers are the heat source[11], etc.

Various manufacturing parameters are constantly monitored during the build process. This is mainly done to prevent potentially dangerous situations like excessive pressure or an overabundance of O_2[12] inside the process chamber [20]. Sensor information is increasingly being integrated into open- and closed-loop process control [21, 22], in order to improve final build quality and minimize time-consuming and costly post processing steps. One promising approach for *in-situ* quality assurance is *infrared thermography*. The primary intent of IR thermography is to detect the formation of voids in the manufactured object, referred to as *porosity*[13], or else non-uniformity in build temperature that can lead to *thermal stress*[14].

[9] In the case of desktop 3D Printers employing *fused deposition modeling* (FDM) technology; a legacy language "G-code" [18] is frequently used. For metal AM, G-code is not applicable.

[10] These storage conditions are irrelevant for polymers.

[11] *Electron beam melting* (EBM) systems require a vacuum in the process chamber.

[12] Metal powder can ignite or form an explosive gas in combination with ambient air. To avoid this, oxygen content in the process chamber should be below 1000 *ppm* [20].

[13] 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 [23] or from an insufficient energy density leading to incomplete powder melting [24]. Porosity can decrease a part's mechanical strength, increase fatigue cracks initiation, and increase anisotropic effects.

[14] The resulting microstructural variations in the object can impair the final part quality,

It is common practice for service providers to recycle leftover metal powder. This minimizes manufacturing costs while reducing environmental impact. However, certain powder properties degrade with recycling. Heat exposure during the manufacturing process can cause powder particles to agglomerate in clusters, change geometry, entrap gas, etc. All such factors can impair the final part quality. To counter this, used powder is sieved and often is blended with fresh powder.

After the build, the part is separated from its build plate and sent for post processing (if needed). This includes heat treatments such as *annealing* or *hot isostatic pressing* (HIP) to achieve the required material properties. In addition, *finish machining* is often required to remove the part from the build plate and improve surface finish and fit.

The build can include witness samples at the request of the customer. The witness samples are typically built with the same parameters as the requested part with the assumption that the witness samples will exhibit the same properties.

For functional parts, *non-destructive testing* (NDT) is usually the final step; these can include *fluorescent penetrant inspection* (FPI), *radiographic inspection*, and *computed tomography* (CT). However, according to the Wohlers Report [2], NDT methods that are well-established in traditional subtractive manufacturing are not entirely sufficient to validate the quality of AM-produced parts. As they begin to understand the unique nature of AM parts, many manufacturers of inspection technologies are exploring a variety of techniques tuned for AM. In the production environment, statistical process control tools such as *Cp*, *Cpk*, and *gage R&R* are also being used [2].

3. Attacks on or with AM

The aforementioned AM workflow is both complex and highly inter-disciplinary. To understand and secure such a complex system, a methodical approach is needed. In this section, we present how this task can be approached in the AM Security context. We first outline a framework that supports differentiation between semantically distinct aspects of attacks on or with AM. We then introduce major threat categories identified for AM. Lastly, we discuss the benefits of knowledge systematization in a taxonomical form.

3.1. Framework for Analysis of Attacks on/with AM

In our prior work [27], we proposed a framework for the analysis of attacks on or with AM (see Figure 3). According to this framework, diverse *attack vectors* that compromise one or more elements of the AM workflow are applicable. The *compromised element(s)*, their roles in the workflow, and the degree to which an adversary can exert control these element(s) determine which *manipulations* an adversary can perform. These manipulations, together with the specific

causing effects like strong anisotropy and reduction of tensile strength [25, 26].

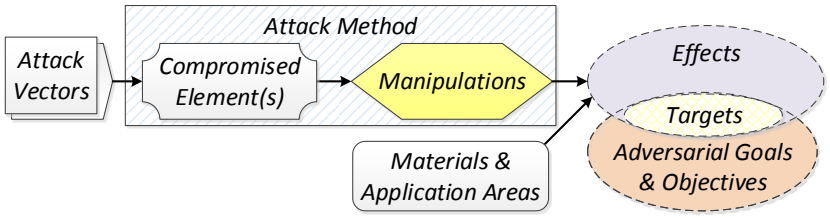

Figure 3: Framework for Analysis of Attack on/with Additive Manufacturing (based on [27])

type of AM equipment, source materials (polymers, metals, etc.), and object application area, determine the achievable *effects*. Typically, only a fraction of the achievable effects intersect with the adversary's goals. The intersection of attack effects and adversarial goals are *attack targets* (or *threats*). The goals and objectives (the latter can be seen as "stepping stones" to achieving adversarial goals) can differ for various adversaries.

We use the dr0wned study [6] to illustrate this framework. This is the first study that shows an entire chain of *sabotage attack* on/with AM[15], from exploiting an attack vector up to achieving the specified attack target. In this study, a phishing e-mail (attack vector) with a malicious attachment was sent to a desktop 3D printer owner. The attachment was crafted to exploit a known cyber vulnerability and to install a reverse shell backdoor on the computer (compromised element). In the study's scenario, the same computer was used to submit jobs to the 3D printer (thus acting as the Controller PC depicted in Figure 2).

The installed backdoor was used to search the PC for stored STL files. During this search, a quadcopter propeller blueprint was found and subsequently downloaded. Researchers then developed a design modification to cause rapid material fatigue in the sabotaged propeller. After the modification was empirically tested, researchers used the same backdoor to replace the benign design. The file exfiltration, design change, and file replacement can be seen as individual *manipulations*. From the AM Security perspective, most crucial is the manipulation performed on the design file.

A replacement propeller was printed based on the tampered design and installed on a small quadcopter drone (*application area*). After a few minutes of flight under normal operational conditions the sabotaged propeller broke apart (*effect*), the drone fell from the sky and suffered significant damage (thus achieving an *adversarial goal* that was stated as the dr0wned study's *target*).

In *dr0wned*, there are elements of the attack similar to those in traditional cyber security, and elements specific to CPS security. Yampolskiy et al. [29]

[15]Several complete attacks have been shown that steal technical data. Particularly, should be noted is the study conducted by Al Faruque et al. [28], who presented the first acoustic side-channel attack on a desktop 3D printer. This attack reconstructs the printed object's 3D geometry.

applied the same framework to compare the security of AM against a "cousin"-technology, CNC-controlled subtractive manufacturing. The authors identified a significant overlap between the two, and also to some extent with classical cyber security. Similarities are especially prominent in exploitable attack vectors, and present but less prominent in compromised elements. However, even comparing these fairly similar technologies, the authors also identified 24 fundamental differences. The majority of differences lie in malicious manipulations that can be performed with AM but not with other manufacturing technologies, which results in a broader variety of achievable effects. To outline just a few differences, attack vectors can include compromise of source or auxiliary material, compromised elements might include a powder recycling system, manipulations can include disruption of communication timing or manipulation of power supply characteristics, and attacks might affect a part's fatigue life. Importantly, defects like internal cavities as well as changes of material properties are manipulations that are specific only for AM. Furthermore, classical cybersecurity solutions are not always applicable, especially in the systems with hard real-time requirements and limited processing capabilities. All this justifies the necessity of addressing *AM Security* as a separate discipline.

Adjustments for Taxonomy Definition: Identical manipulations can be performed by different compromised elements. For instance, the same modification can be introduced in part blueprint files if the computers of involved actors (*e.g.*,, 3D Parts Designers, AM Service Provider) are compromised, or else network communication between them. Further, semantically distinct but functionally identical modifications are possible. For instance, modifications to a 3D object design can be introduced in blueprint files by a compromised Controller PC, in the toolpath by a compromised internal network, or in electrical signals to individual actuators initiated by compromised 3D printer firmware.

To provide a conceptual view in the taxonomy, we introduce ***Attack Methods*** as semantically identical ***Manipulations***. They can be introduced by different Compromised Elements and have different syntactic representations. We also identify ***Attack Targets*** as ***Effects*** that directly correspond to ***Adversarial Goals***.

A singular modification does not necessarily lead to a singular and terminal effect. Instead, it often triggers a complex chain of effect propagation. In AM systems, these effects can occur in and across the cyber and physical domains [30, 31].

3.2. Security Threats in AM

Security threats originate from the intersection of attack effects and adversarial goals because these are both achievable by and of interest to an adversary. So far, two major categories of attack targets have been identified for AM (see Figure 4): *theft of technical data* (or *violation of intellectual property*, IP) and *sabotage of AM*.

IP violation is the act of illegally gaining access to and using IP (*e.g.,* for infringement of the original product). It should be noted that, in the AM context, IP might include the blueprints of 3D objects, the required physical

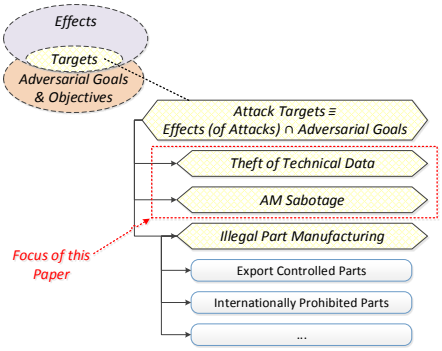

Figure 4: Major security threat categories in AM

properties of an object (especially for functional parts), and the specification of AM process parameters [32]. The latter can be essential to achieving the part's required properties; otherwise, a functional part might break during normal operation, or develop fatigue faster in its expected useful life.

Sabotage of AM targets functional part manufacturing. It aims either to reduce a part's mechanical strength [33, 34, 35], or to reduce its fatigue life [6]. The scope of sabotage attacks can include AM equipment and the surrounding environment [27].

Additionally, several articles [36, 37, 38, 39] have raised the issue of using 3D printers to manufacture *export-controlled* or *nationally/internationally prohibited* items (*e.g.,* firearms, or components of explosive devices). Peer-reviewed scientific publications [40, 41, 42, 43, 44, 45] have only addressed the legal aspect of the issue thus far. Furthermore, there are no security-related technical differences between illegal manufacturing using AM or using traditional CNC machines[16] [29]. Because of a lack of technical differences for attacks, we explicitly exclude the latter threat category from consideration in this paper.

Both threat categories can be represented in the classical cyber-security CIA (confidentiality, integrity, availability) triad [46]. Theft of technical data, including critical national security information and valuable commercial intellectual property, is a confidentiality concern. Sabotage attacks will generally require alteration of data, processes, and products. This is an integrity concern. Sabotage attacks can further impair or deny the process control, thereby damaging or shutting down operations. This is an availability concern.

3.3. Systematization of Knowledge in a Taxonomy

Security confronts the fact that a system's weaknesses are exploited deliberately [47]. Unlike dependability, obscure and unlikely system states are major security concerns, because adversaries are motivated to seek them out. This

[16] For the countermeasures, this might be different.

governs that, in order to protect a system, we first have to understand how it can be attacked and what properties various attacks can have.

One methodology for obtaining this understanding is through a "systematization of knowledge." It is customary to achieve this systematization through careful development of taxonomies in which information is organized into categories of main concepts and then into associated groups [48]. For taxonomies to be useful, they need to be accepted, comprehensible, determined, exhaustive, mutually exclusive, repeatable, unambiguous, useful, and incorporate well-defined terms [49].

The development of such taxonomies is difficult because they can be quite complex. Further, there is currently no standard classification scheme [50]. The situation becomes more complicated for CPS in general and for additive manufacturing in particular as CPS are inherently multidisciplinary in nature. That is, for additive manufacturing the development of a taxonomy requires expertise in cyber and physical security along with materials science, mechanical engineering, and socio-economic and political sciences.

In our proposal (presented in Sections 4 and 5) we focus exclusively on aspects covered by relevant natural science domains. For both threat categories, we define two top-level taxonomy branches, *attack targets* and *attack methods*, and indicate which methods can achieve given targets.

Several taxonomies for AM security have been recently proposed. Even applied to the same problem domain, taxonomies can vary to a great extent. This results from the difference of scope (which aspects are included), detail grade (at what abstraction level elements are included), and especially, organizing principles (semantic rules defining how elements are grouped in a tree-like structure). Compared to our proposal, all these proposals have broader scope, list elements at a higher abstraction layer, and follow different organizing principles.

In our prior work [27] (see *6.4.18 yampolskiy2016using* on p. 45), we have proposed a two-level taxonomy for sabotage attacks on or with 3D printers. At the top level, we distinguished between *attack vectors*, *compromised elements*, *manipulations*, and *effects*; we further proposed five categories to characterize the effects. Overlapping with our current proposal are *compromised elements*, *manipulations*, and *attack target*. Our current proposal has different organizing principles (combining semantically identical *manipulations* exercised by different *compromised elements* to a single *attack method*), includes a taxonomy for *theft of technical data*, and is of significantly greater depth.

Pan et al. [51] (see *6.4.7 pan2017taxonomies* on p. 43) propose a pair of taxonomies: a CPS attack-classification taxonomy against manufacturing systems, and a quality control countermeasures taxonomy. In the attack-classification taxonomy, the authors categorize elements of the chain from attack vectors to impacts, with the most detail given to impacts. This section contains mainly impacts with economic ramifications, and the integrity impacts that directly affect part behavior are considered from an economic standpoint. Overall, the taxonomies are geared towards private-sector manufacturing companies and their means of mitigating attacks.

Wu et al. [52] (see *6.4.13 wu2017taxonomy* on p. 44) propose a three-level

CyberManufacturing System Attacks taxonomy. At the top level, it distinguishes between *Attack Vector*, *Attack Impact*, *Attack Target*, and *Attack Consequence*, each of which is sub-divided in *cyber* and *physical* categories. The authors provide only a brief appraisal of each taxonomic category, as their goal is to establish a shared terminology for researchers and security practitioners dealing with attacks against manufacturing systems.

While mainly contributing a novel counterfeit protection method, Gupta et al. [53] (see *6.1.4 gupta2017obfuscade* on p. 30) also outlines a two-level *Additive Manufacturing Attacks* taxonomy. The taxonomy provides a flat categorization of descriptive elements for AM attacks (when, how, what, why, and where). Taxonomic choices and greater explanation are not provided by the authors; it is used chiefly as a convenient format for briefly overviewing AM security concerns.

4. Taxonomy: Theft of Technical Data

A frequently discussed aspect of AM security is the potential to steal AM-related technical data. Depending on a country's legal framework, such actions might[17] violate Intellectual Property (IP) protection laws. Later in this paper, we will use terms *theft of technical data* and *IP violation* interchangeable.

Figure 5 depicts our taxonomy reflecting both *attack targets* and *attack methods*. In this section, we describe the categories in detail.

4.1. Theft of Technical Data: Attack Target

For the theft of technical data in AM, we propose to distinguish between the following attack targets, described in the following subsections.

4.1.1. Part Specification

Depending on a variety of factors, including the source material and AM technology, *part specification* can refer to different sets of information. The files that are associated with the metal additive manufacturing process currently contain or will contain in the future sufficient information to reproduce the part including the full 3D geometry of the part required to meet performance requirements. The only additional information required would be the manufacturing process specification and the post processing specification. On the other end of the spectrum is the part specification for desktop 3D Printers; files usually specify only the part's geometry and occasionally colors or materials.

Part Geometry: The part's 3D geometry, or blueprint, is commonly specified in a CAD or STL file format[18]. The blueprint specifies external shape and internal cavities. A full part specification might also include acceptable tolerances and required surface finish. All these parameters can have an immediate

[17] This is not always the case [54].

[18] Other formats, including proprietary ones, can be used as well. AMF and 3MF file formats might become widespread in the future.

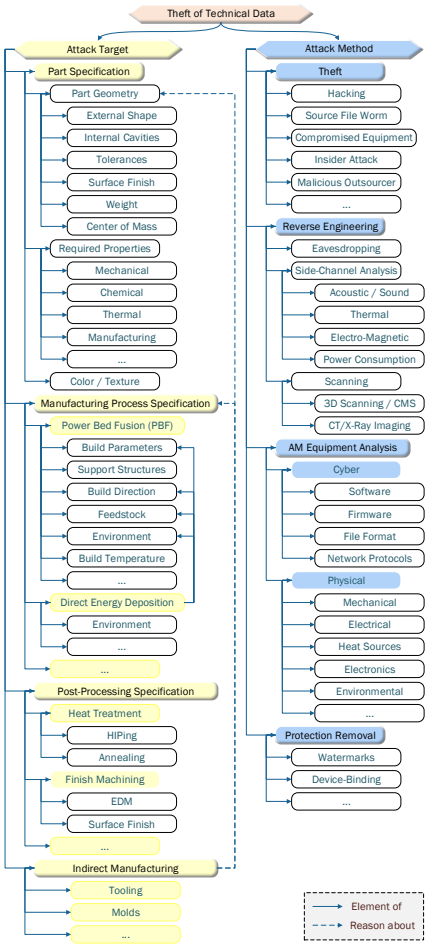

Figure 5: Intellectual Property (IP) Violation

impact on the part's weight and center of mass. Depending on the applicaiton, if mass and center of mass are important, they may also be specified.

Required Properties: Application area-optimized physical properties are an essential aspect of the part's specification. These might include mechanical, chemical, thermal, and other requirements on the manufactured part. Meeting requirements can require choosing specific AM processes or adjusting process parameters.

The files that are associated with the metal additive manufacturing process currently contain or will contain in the future sufficient information to reproduce the part including the full 3D geometry of the part required to meet performance requirements. The only additional information required would be the manufacturing process specification and the post processing specification. Digital blueprints for desktop 3D printers contain no such information.

Color / Texture: While the STL file format is sufficient to describe the geometry of a 3D object, the recently adopted AMF file format also supports specification of its color and texture. This information is irrelevant for metal AM.

4.1.2. Manufacturing Process Specification

The American Society for Testing and Materials (ASTM) International Committee F42 on Additive Manufacturing Technologies has approved seven different AM process categories [2]. Evidently, These processes differ in the source materials that are supported (for instance polymers or metals). Also, they differ by that means that the source material is distributed (for instance, via powder bed or nozzle) and, finally, they differ in terms of the heat sources employed, as exemplified by laser, electron beam, or arc technologies, among others.

As opposed to traditional subtractive manufacturing, where milling and turning machines can define only the object's shape, adjusting AM process parameters can influence the material's micro-structure, thus affecting the part's physical properties. These parameters are numerous[19] and AM process specific. In the *powder bed fusion* (PBF) process, operators can control various build parameters (*e.g.,* laser power and speed, hatch spacing, etc.), environmental properties (in the case of PBF, background gas atmosphere and humidity in the build chamber), build (Z) direction, material and location of support structures, feedstock properties, etc. *Direct energy deposition* (DED) shares some parameters, such as build direction, but also has a set of different parameters, like nozzle distance [56, 57, 34, 58].

As of 2017, the relationship between manufacturing parameters and physical properties remains an active area of research [2, 59, 60]. The exact specification of manufacturing process parameters that ensures a manufactured part's quality can be considered IP.

The files that are associated with the metal additive manufacturing process

[19] Rehme [55] lists 157 parameters, arranged in an *Ishikawa diagram*, a form of *causal diagram* that graphically represents causal relationships between different variables.

currently contain or will contain in the future the optimized process parameters to build a qualified part. The only additional information required would be the post processing specification. On the opposite end of the spectrum, digital blueprints for desktop 3D printers contain no such information.

4.1.3. Post-Processing Specification

Post processing is often required before a part can be put into service. In metal AM, this includes heat treatments such as *annealing*[20] or *hot isostatic pressing*[21] (HIP) to achieve the required material properties. In addition, finish machining is often required to remove the part from the build plate and improve *surface finish*[22] and *fit*. For this, traditional mechanical surface finish or electrical discharge machining (EDM) can be used.

Parameters such as duration, temperature, and pressure cycle can vary, based on factors like a specific material. The exact values of post-processing parameters might greatly impact quality. Because post-processing steps are excluded from patents about AM itself, post-processing may be separately patentable if novel and nonobvious.

4.1.4. Indirect Manufacturing

One of the main uses of metal additive manufacturing today is indirect manufacturing. That is, making parts that help in the fabrication of a finished part. AM can produce tools and molds that are used in traditional manufacturing processes [63].

In indirect manufacturing, part specification (*e.g.,* cast for molding) enables reasoning about both part itself and manufacturing process that is required to manufacture it. For instance, it might be essential to control the temperature of the molding process. Such temperature control has the potential to produce parts with lower residual stresses and to shorten manufacturing cycle time. To accomplish this, molds are created with internal cooling passages. These better control the temperature of the molding cavity throughout the process cycle [64].

4.2. Theft of Technical Data: Attack Method

Related to the targets of an attack are the methods that can be used. Figure 6 presents our assessment of the correlation between target and method. We propose the following categories of methods to steal technical data in the AM context, described in the following subsections.

[20] Annealing is a process of a cooling in a controlled manner. It helps to relief internal stress.

[21] HIP is a process during which a part is exposed to elevated temperature in a high pressure environment; as a pressurizing isostatic gas, argon is commonly used. HIP helps to eliminate residual internal porosity and enhance mechanical strength [61, 56].

[22] Surface finish can significantly improve the part's fatigue life by minimizing sites where fatigue cracks can form [62].

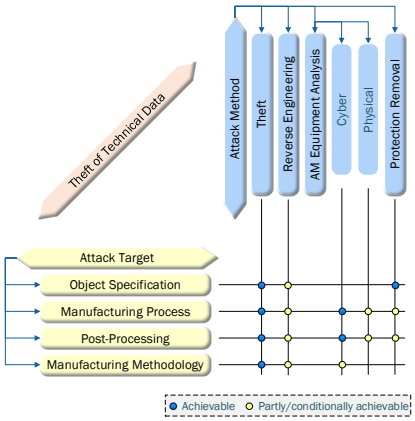

Figure 6: Theft of Technical Data, Correlation between Attack Methods and Attack Targets

4.2.1. Theft

Theft of technical data, particularly electronic representations such as blueprint files, can be performed by various means. Because a printer is typically accessible on an internal network, a common attack vector is through hacking the corporate network. In more specialized cases, adversaries may construct malware, like the ACAD/Medre.A worm targeting CAD files, that propagates across devices and copies digital blueprints files and related documentation to a foreign server [65].

However, the blueprint file is not the only avenue of attack; AM equipment can be compromised as well, especially if the controller PC is connected to the Internet. Physical attacks can also be used to steal technical data. The existence of malicious insiders, whether direct employees or outsourced companies, cannot be excluded either.

4.2.2. Reverse Engineering

IP can also be reconstructed by various means without requiring theft. This can be performed either during the manufacturing process or post-factum, from the manufactured object. We propose to distinguish between theft of technical data and its reconstruction, as they have different technical properties and legal consequences [54].

From the legal perspective, reverse engineering does not necessarily violate IP protection laws [54]. Several authors argue that the propagation of cheap 3D scanners will lead to uncontrollable copying of 3D objects [66, 67, 68]. The absence of legal consequences will likely accelerate this development.

Eavesdropping & Side-Channel Analysis: There are several different methods for reconstructing IP through indirect observation. During manufacturing, eavesdropping network communication (*e.g.,* toolpath commands exchanged between the controller PC and a 3D printer) or conducting side-channel

analysis (*e.g.,* sound of the 3D printer's motors as shown in [28, 69, 70]) can be used to model the 3D object. The former can also provide insight into the manufacturing process specification.

SCANNING: After a 3D object has been manufactured, a variety of tools ranging from a hand-held 3D scanner to a high precision Coordinate Measuring Machine[23] (CMM) can be used to reconstruct the external shape of the object. Radiographic inspection and CT scanning tools, commonly used in quality control for detecting internal cracks, voids, and trapped powder [2], can be used to gain information about internal cavities. These reverse engineering methods introduce deviations from the original IP, due to the precision of the tool or noise in the measurements.

4.2.3. AM Equipment Analysis

An analysis of the AM equipment itself provides another means of IP reconstruction. Both 3D printers and post-processing equipment can be analyzed. Unlike reverse engineering, this only reveals information related to the manufacturing process or post-processing.

CYBER: Analysis of the cyber components can extract the default process specifications, an OEM's proprietary IP. For instance, it can reveal the scanning strategy, or how sensor information is used in quality control. The distribution of this kind of IP across software and firmware can vary for different equipment. The file formats and network communication protocols used can reveal the separation of responsibilities between software and firmware; it can also reveal which adjustments are possible, *e.g.,* because of the precision achievable with the used file formats and protocols.

PHYSICAL: The analysis of physical components mainly reveals to what extent individual manufacturing parameters can be adjusted during part production, *e.g.,* in order to meet requirements for a part's mechanical strength.

4.2.4. Protection Removal

AM is increasingly offered as a service for customers who provide object blueprints. At the same time, with the printing quality of desktop 3D printers increasing and their prices falling, several articles predict a shift to at-home manufacturing of purchased objects [8, 72, 73, 9]. Both tendencies could lead to a situation where an adversary can access IP legally, then attempt to violate the terms that an IP owner has placed on that access.

While forms of digital rights management (DRM) can be used to enforce licensing agreements and usage compliance, their functionality can be disabled by dedicated effort. Even resilient measures that integrate identifiers, as opposed to wrapping the protection around a blueprint, can be bypassed by sophisticated parties.

To deter such endeavors, the Digital Millennium Copyright Act of 1998 criminalizes the removal of technical measures meant to control access and usage.

[23] Contemporary CMM can achieve accuracy of up to $20\mu m$ [71].

However, in the case of managing printing rights, the printed objects, as tangible products, are not directly protected under the Act [54].

Should a blueprint carry identifying properties, such as a watermark, modification to that protected file could remove them. Objects that are printed without identifiers may serve as evidence for copyright infringement. Legal enforcement of this form of IP protection will likely remain indirect until laws are implemented that consider safeguarding digital patents [74, 75].

5. AM Sabotage

AM is an important representative of Computer Aided Manufacturing (CAM) [76], and as such of Cyber-Physical Systems (CPS). Generally, attacks on CPS aim to cause physical damage. This goal can be achieved by manipulations in cyber domain (thus representing a cross-domain *cyber-physical* attack [30]). Some adversarial goals can be also achieved by manipulations in the physical domain (thus representing a *physical* or *physical-to-physical* attack [30]).

Figure 7 presents our approach for the classification of *attack targets* and *attack method* of AM sabotage. In this section, we describe taxonomies for both these dimensions.

5.1. AM Sabotage: Attack Target

We propose to distinguish between three categories of attack targets in AM: the manufactured part, the AM equipment, and the environment. These categories can be structured as follows:

5.1.1. Manufactured Part

Sabotage attacks can target various properties of the manufactured parts.

Fit and Form: Fit involves the ability of a part to physically interface with, connect to, or become an integral part of another part or assembly. Form involves the shape, size, dimensions, mass, and visual parameters that uniquely distinguish a part. This type of attack produces confusion and delay. While all inputs of the process look correct, the part still emerges from the machine with bad fit or form. This would cause remaking of the part and perhaps recalibration of the machine.

Function: Function refers to the action or actions that a part is designed to perform. In the additive manufacturing process, we are creating the material at the same time that we create the part. Thus the impact here is in the quality of the material or in other functions that may have been added in the process. The quality of material includes its physical, chemical, thermal, electrical, magnetic, optical, and mechanical properties. The subset of relevant properties depends on factors like the intended function of the part, its operating conditions, and its interactions with other parts in a device. For instance, parts in high temperature environments need certain thermal properties. In the emerging field of 3D

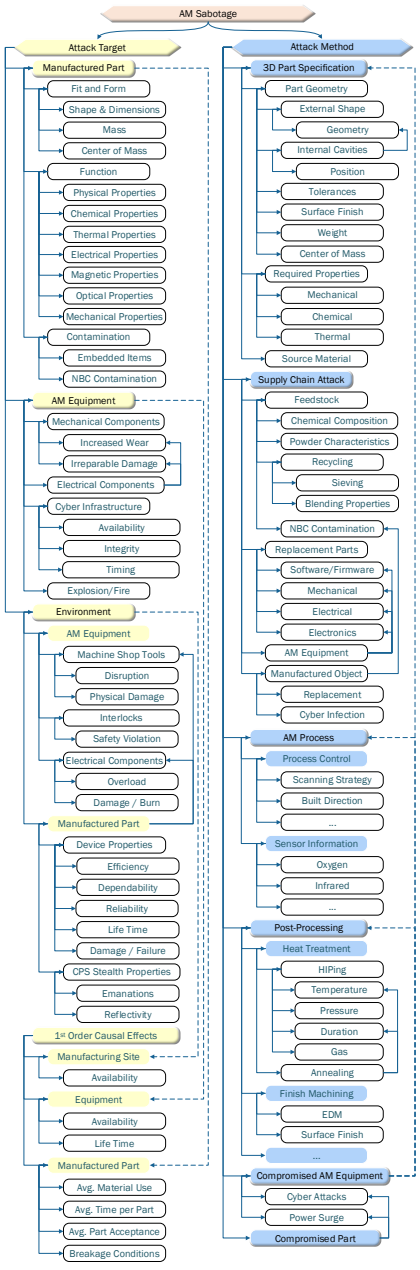

Figure 7: AM Sabotage

printed electronics[24], electrical properties like resistance and dielectric strength are essential for the part's function.

So far, only sabotage attacks that degrade mechanical properties have been shown in the research literature. These can be organized in two sub-categories of quality degradation. First, the mechanical strength of the part can be degraded below tolerance. This might cause the part's destruction under normal operational conditions [33, 34, 35]. Second, an attack can reduce the fatigue life of the part [6]. If the fatigue cracks are detected in time, early replacement of the part will only cause financial damage. If the fatigue goes unnoticed, a functional part can fail prematurely during operation, causing damage to the device and the system employing it.

Contamination: Unexpected materials and foreign objects could be embedded into objects during the AM process. Further, the manufactured part can be used as a "carrier" of NBC (nuclear, biological, chemical) contamination [27]. This can contaminate the environment exposed to the manufactured object.

5.1.2. AM Equipment

The additive manufacturing equipment itself can be a target of attack, including the mechanical and electrical components and the cyber infrastructure.

Mechanical Components: The mechanical components of an AM machine are critical to its function. In metal AM, potential targets would include galvanometer mirrors, powder handling equipment, seals (to maintain the controlled atmosphere of the machine), and re-coater systems. Attacks can cause excess wear, thereby reducing the affected mechanical parts' lifespan, in extreme cases leading to irreparable damage[25].

Electrical Components: Electrical components likewise play a critical role in the function of the additive manufacturing machine including sensors, interlocks, motors, power supplies, and energy sources. Similar to mechanical components, attacks targeting electrical components can increase their wear or cause irreparable damage.

Cyber Infrastructure: The cyber infrastructure includes software, firmware, hardware, and networks. The software involved is diverse and often comes from multiple suppliers and includes the CAD software, process modeling (commercial or in-house) software, slicing software, tool path generation and machine specific instructions, and process monitoring software.

Cyber infrastructure is involved in a complex flow of data transmission and transformation. Similar to cyber-security, sabotage attacks can impair the availability and integrity of the data. Specific to CPS, this data can relate to the commands or sensor information in a control loop [82]. Even with correct data,

[24] At the end of 2015, *Voxel8* announced the world's first 3D electronics printer [77]. There are now several companies offering 3D printers that can lay electrically conductive material. Such 3D printers are already capable of printing devices like antennas [78, 79].

[25] While we are not aware of any evidence of similar attacks on AM, attacks like Stuxnet [80] and the Aurora experiment [81] have demonstrated feasibility of such attacks for other systems.

changes in timing can have a direct impact on CPS functionality [83]. In AM, even data delivered too early or out of order can have this impact [84, 29].

EXPLOSION/FIRE: The use of fine powders opens the potential for inducing a fire or explosion in the equipment [27, 85, 86].

5.1.3. Environment

An attack on an additive manufacturing process could impact the surrounding environment and beyond (when the part is delivered to the customer). We propose to distinguish between the environmental impact generated by AM equipment and that which is generated by the manufactured part.

AM EQUIPMENT: An attack on the additive manufacturing equipment could affect other equipment located nearby, including powder sieving equipment and feedstock storage. Contaminated feedstock might affect the entire supply chain infrastructure and the machine environment, if it is used. Compromised electrical components could damage the machine and have broader implications for the source of electrical power. If the cyber components of a machine are compromised, they can carry out traditional cyberattacks.

MANUFACTURED PART: An attack on the manufactured part could affect the environment when the part is integrated into the final assembly. For example, it is conceivable that a defect could be introduced in a safety-critical part that causes the part to fail in-service. For example, embedding a defect in a rotating part to fail at a predetermined speed has been documented [6]. Embedding of active or passive electronic components or contaminants could affect the customer upon the delivery of the part.

Sabotage attacks against military equipment might target the detectability of a CPS. Malicious modifications can cause a broad variety of emanations, including EM, heat, or vibrations. Further, it can also contribute to the reflectivity factor of a CPS as a whole. While it might not affect the functionality of the part itself, it can reduce the overall stealthiness of the CPS.

5.1.4. 1st Order Causal Effects

Sabotage attacks can have a variety of consequences, which we refer to as 1^{st} *Order Causal Effects*. Among these effects, most noticeable are impacts on manufacturing sites, manufacturing equipment, or the acceptance of a part after quality control. Further out from manufacturing, attacks can damage systems employing sabotaged (or allegedly sabotaged) parts. Apart from physical damage, attacks might effect the manufacturing efficiency and the cost per part; these can be influenced by parameters like material use, average production time per part, and part acceptance rate (this can be either because a part is defective, or because the testing equipment is compromised).

While the effects of sabotage attacks are not the focus of this taxonomy, they inform the motivations of attackers. Economically motivated attacks might focus on cost efficiency and acceptance rate, where military or strategic attacks might target manufacturing availability. A full examination of sabotage attack

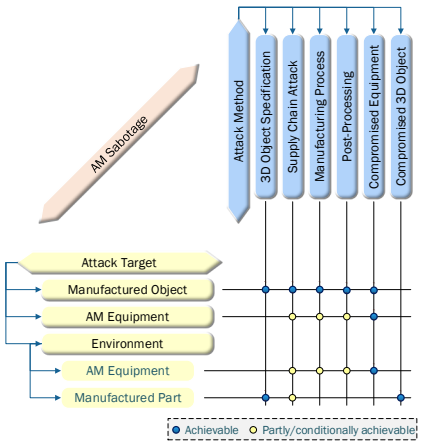

Figure 8: AM Sabotage, correlation between attack methods and attack targets

effects moves beyond AM as a discipline and into more general fields of security, strategy, and risk evaluation.

5.2. AM Sabotage: Attack Method

It is clear that not all methods can be used to achieve any goal. Some attack methods can be used with several attack targets and vice versa (see Figure 8). We propose to distinguish between the following categories of attack methods aiming to sabotage AM:

5.2.1. 3D Part Specification

In the AM workflow, a part's specification can have several representations. The description of the 3D object geometry can be represented by CAD, STL, or other file format, then "sliced" into thin layers, sent from controller PC to 3D printer as tool path commands, and finally become a sequence of proprietary protocol instances and signals for communication between embedded controllers in AM equipment. Any of these representations can be modified by an attack, resulting in changes to the printed part [87].

Part Geometry: Malicious modification of the part geometry can affect the part fit and form. Defects can also be inserted in the internals of the 3D structure. This is an essential difference with subtractive manufacturing where changes in part geometry are discernable via direct measurement. For additive manufacturing, the defects could be small enough that they cannot be detected even by techniques such as CT scan. Furthermore, the size, geometry, and position of internal cavities present in the original design can be changed. This will have an impact on the part's mass, center of mass, and function (i.e., mechanical, thermal, and other properties).

Required Properties: Modifying machine parameters can affect part function by changing the part's properties. An example would be to alter the

build direction, which can affect anisotropic material properties. Defects introduced in the process can alter the failure behavior and useful lifetime of the part.

Source Material: For multi-material AM processes, substituting incorrect materials is a viable manipulation. Differences between the original and contaminant material affect the part's mechanical, thermal, and other properties.

5.2.2. Supply Chain Attack

Similar to cyber-security, AM is subject to supply chain attacks. In addition to the software and firmware supply chain, the supply chain in AM includes transportation of source materials used in manufacturing, replacement parts for AM equipment, manufactured objects, and AM equipment itself. Compromising the supply chain enables arbitrary replacement or modifications of transported objects.

Feedstock: Feedstock presents particular challenges. First, feedstock is usually purchased from a vendor who may or may not be the producer of the feedstock. Second, characterization of feedstock can be expensive and time consuming, involving expensive equipment. Thus, there is a motivation to accept the feedstock without characterization. Third, the performance of the feedstock can be altered by changing its size distribution that could disrupt the process. Fourth, the feedstock is vulnerable during recycling (blending and sieving) operations. Finally, the feedstock is susceptible to the introduction of contaminates including oxygen, moisture, and NBC[26].

Replacement Parts: Software, firmware, mechanical, electrical, and electronic equipment associated with AM are replaced when components fail or need to be upgraded. Subtle changes in machine control software can have profound effects on part properties. This is why today in additive manufacturing production settings, when end-use parts are being produced, no software upgrades are allowed unless the machine is requalified (which can take months). However, malware can employ complex activation triggers to bypass the requalification process.

AM Equipment: AM machines can be delivered in a compromised state. This could include compromised software, firmware, and hardware. This situation is no different that the delivery of any other CPS.

Manufactured Object: Similar to AM equipment, supply chain attacks on manufactured objects can include their replacement (*e.g.,* to impair a part's fit or function), NBC contamination, or cyber infection of embedded electronics.

5.2.3. AM Manufacturing Process

Many parameters are controlled during manufacturing processes, often based on sensor data. Both process control commands and sensor information can be either interrupted or tampered with [82]. Furthermore, CPS in general are

[26]NBC stands for Nuclear, Biological, and Chemical.

susceptible to timing disruptions [83]. This is true for AM processes, where packets that arrive too late, too early, or out of order can disrupt the process [84].

Property	Can be affected by AM?	
Physical		
Density	yes	Control of power, speed, and hatch spacing
Color	no	
Shape and Size	yes	
Chemical		
Chemical Composition	possibly	High vapor pressure elements can evaporate, Rapid cooling can result in metastable phase formation (e.g. quasi crystals)
Corrosion Resistance	yes	Cooling rate can alter local phase composition
Thermal		
Melting Point	no	
Thermal Conductivity	possibly	By changing part cross section
Thermal Expansion	no	Macroscopic part design
Specific Heat	no	
Electrical		
Conductivity	possibly	By changing part cross section, Strongly dependent on scattering centers
Temperature Coefficient of Resistance	no	
Dielectric Strength	no	
Thermoelectricity	no	
Magnetic		
Coercivity	yes	Particle production in the micron-submicron range, anisotropic particle shapes. Various approaches to achieve
Permeability	yes	Very high cooling rate to produce amorphous structures or met glasses. Grain orientation through shear printing, &c
Remanence	yes	Preferential orientation of crystallites and exploitation of shape anisotropy
Magnetostriction	yes	Anisotropic powder production
Optical		
Refractive Index	no	Through local chemical changes
Emissivity	yes	
Absorptivity	yes	
Diffuse Scattering	possibly	Through local chemical changes
Mechanical		
Brittleness	possibly	By controlling the yield strength
Creep	no	
Elasticity	possibly	By changing part cross section
Fatigue	possibly	By controlling defect population
Ductility	yes	
Toughness	yes	By controlling the yield strength
Yield strength	yes	By changing part cross section

Table 1: Properties that can be Affected be AM Process

Process Control: There are more than 130 parameters that govern the metal additive manufacturing process[27] [88, 55]. Although not all parameters are equally important, certain parameters may be more important for particular geometries. For example, laser delay settings may be compromised to create microscopic leaks in a thin-wall vessel.

The laser scanning strategy is one of the most critical aspects of the additive manufacturing process. For each slice, one hundred percent of the volume needs to be melted and solidified without leaving defects behind. Changes in the scanning strategy can induce lack of fusion or keyhole defects [89]. The slightest change in scanning strategy is sufficient to break a company's part qualification

[27] The amount of parameters and parameter itself vary drastically across different AM technologies.

regime. Scanning strategy includes laser path, power, and speed.

Because of the layer-by-layer nature of additive manufacturing, materials can have anisotropic properties. In some cases, engineers may design with this difference in mind. Thus, altering the build direction could alter the expected part properties.

Some properties depend on the part's thermal history. Changing the number of parts on a build plate, or the powder spreading speed, changes the temperature of the part at different times. Alterations to either could alter part properties.

Not all properties are relevant for a part's function. For instance, a part that is supposed to withstand mechanical stress might have visual properties of no relevance. Further, only some of these properties can be influenced by the AM process. Our preliminary assessment is summarized in Table 1.

Sensor Information: According to Cardenas et al. [82], manipulating sensor information can be used in false state estimation attacks on CPS employing control loops. In the context of AM, an indirect sabotage attack via *in situ* IR Thermography has already been shown [90]. False sensor readings caused a control system to adjust various manufacturing parameters, demonstrating indirect control over these parameters. Further, it is possible that false sensor reading of parameters like oxygen content or pressure in the build chamber can lead to violation of safety requirements.

5.2.4. Post-Processing

The post processing parameters for additively manufactured parts can differ from those of conventionally produced materials. Modification can alter the expected properties of the material.

Heat Treatment: Heat treatment is carried out to relax residual stresses and impart desirable mechanical properties. Alterations can adversely affect both.

Finish Machining: Finish machining is usually required to achieve the desired fit and function. This area has the same security issues as subtractive manufacturing.

5.2.5. Compromised AM Equipment

Compromised AM equipment enables several attack methods including 3D Part Specification, AM Manufacturing Process, and Post Processing. Equipment can include not only the manufacturing devices like 3D printers, but also other devices like CT scanners for quality control, device firmware, a variety of software directly or indirectly involved in the tool chain, and computer networks.

Cyber Attacks: Cyber attacks can render systems inoperable and infect other systems. They include potential physical damage that could be caused in the future by implanted malicious code.

Malicious or compromised software can be used to alter (sabotage) the object model, including 3D geometry, dimensions, and acceptable tolerances. There are several ways this can be achieved. A part's blueprint has a variety of representations in the AM tool chain; each of these representations can be altered [87].

This can be done "on the fly" by compromised 3D printer firmware [91, 92] or highjacked network communication. But this can also be done by a variety of compromised software.

The benign blueprint can be directly compromised; this has been shown experimentally through direct remote access [6, 10] and by malware [33, 10]. The same compromise can be performed indirectly, e.g., during finite element analysis (FEA) or during distortion correction. In this case, malicious FEA software could report acceptable performance when a simulated part has a defect. The situation is much the same for the (topology, support structure, distortion, etc.) optimization step.

Quality control (or testing) measures usually verify whether a produced part complies to its blueprint or requirements. Thus, if the blueprint was maliciously altered, a blueprint comparison will not be able to detect the sabotage. If a blueprint is altered "on the fly," e.g., by a malicious 3D firmware [91, 92], quality control should be also compromised to avoid detection. Last but not least, compromised quality control can be used to identify good parts as deficient, lowering the manufacturing plant's efficiency.

Power Surge: In larger-scale production, an entire fleet of AM machines may be used in unison. If they are all compromised, a coordinated power draw could cause a surge that damages the facility power system.

5.2.6. Compromised Part

Similar to Compromised AM Equipment, manufactured parts (embedded items or contamination) can be used for active attacks on their environment.

6. Survey: State of the Art

AM security is a new but rapidly growing research area. Figure 9 outlines papers published on both threats considered in this paper: *theft of technical data* (or *IP violation*) and *AM sabotage*. Both in this figure and later in this section, each research paper[28] is referred to by a mnemonic commonly used in Google Scholar: concatenation of the author's surname, year of the publication, and the title's first word.

A *Venn diagram* is used to represent the thematic grouping of these papers. For both threats—theft of technical data and sabotage—there is a clear distinction between papers focusing on aspects of attacks, papers proposing countermeasures, and papers discussing the legal aspects of security threats in AM.

[28] Entries do not always reflect the exact amount and the year of the publication(s). In the case of extended journal versions, entries consolidate their descriptions with significant overlap to a single entry related to the earliest publication. In the case of pre-prints posted in the year prior to a peer-reviewed publication, entries use the year of its first appearance. Figure 12 in Section 7 reflects the real number of peer-reviewed publications and the years of their appearance.

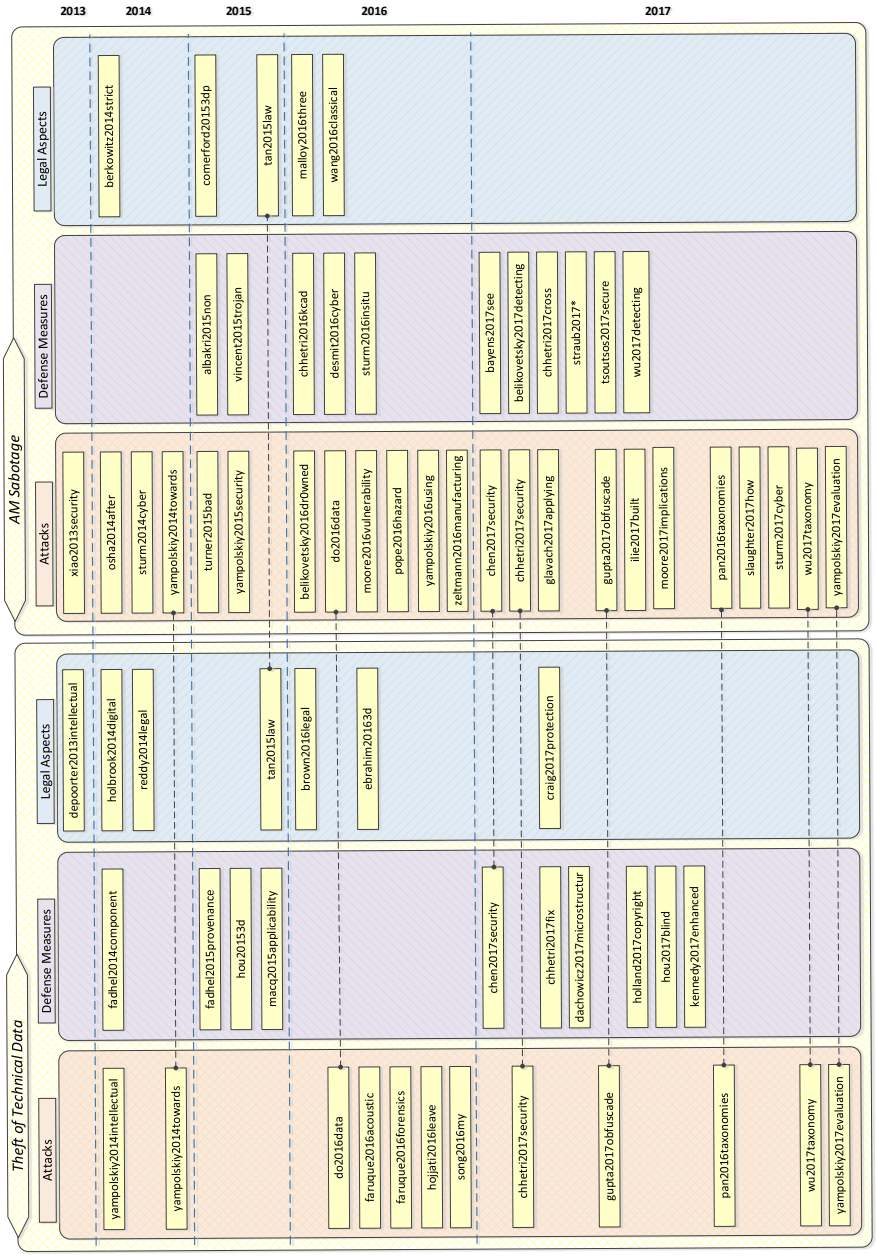

Figure 9: AM Security, State of the Art (State: December 2017, sorted lexicographically within each category/year "silo")

Analysis	
Security Comparison	
Security of Additive vs. Subtractive Manufacturing (Similarities and Differences)	6.4.19 *yampolskiy2017evaluation* [29], p. 46
Theoretical Frameworks	
Attack Analysis Framework	
Confidentiality, Integrity, Availability (CIA) in Product Life-Cycle Phases	6.1 *chhetri2017security* [93, 94], p. 28
Sabotage Attacks on/with AM	6.4.18 *yampolskiy2016using* [27], p. 45
Taxonomies	
AM Security (All Threat Categories)	6.1.4 *gupta2017obfuscade* [53], p. 30 6.4.7 *pan2017taxonomies* [51], p. 43 6.4.13 *wu2017taxonomy* [52], p. 44
Sabotage Attacks on/with AM	6.4.18 *yampolskiy2016using* [27], p. 45

Table 2: Surveyed Publications, Cross-Cutting and Higher Abstraction Level Publications

Several publications (e.g., frameworks for security threat analysis or alternative proposals for a taxonomy) tackle the problem at a higher abstraction level and/or discuss several aspects at the same time. In such cases, these publications are placed in sections to which their major contribution gravitates. These publications are summarized in Table 2.

6.1. IP Violation: Attacks

Table 3 outlines which elements of the attack analysis framework (see Figure 3) have been addressed by the surveyed papers, and outlines the major idea(s) presented within. In addition, Figure 10 summarizes those aspects of the proposed IP violation taxonomy have been addressed by the surveyed papers. Please note that not all identified aspects have been addressed and that some papers cover more than one aspect. All papers are listed in alphabetic order of the mnemonics.

6.1.1. chhetri2017security

Chhetri et al. [93] consider the higher-level perspective of life cycle security in Industry 4.0, of which AM is considered to be an integral part. The authors distinguish between the following six life cycle phases: *design*, *prototyping*, *ordering*, *industrial processing*, *sales*, and *maintenance*. For each of these phases, the authors provide an outline of *confidentiality*, *security*, and *availability* concerns (a.k.a. the CIA security triad). The discussion is supported by examples from the research literature. In its extended version, Chhetri et al. [94] further present a similarly structured outline of works tackling the outlined security threads.

6.1.2. faruque2016acoustic

To our knowledge, Al Faruque et al. [28] presents the first paper describing on an attack on a desktop 3D printer that leverages the sound generated by the 3D printer's motors (that is, an acoustic side-channel). In [28], the authors provide a comprehensive description of how the acoustic emanations can be "tied back" to the actual movements of employed stepper motors. Based on this analysis, the researchers have been able to reconstruct the 3D printed object. Even though the idea of using the acoustic side channel is similar to attacks on

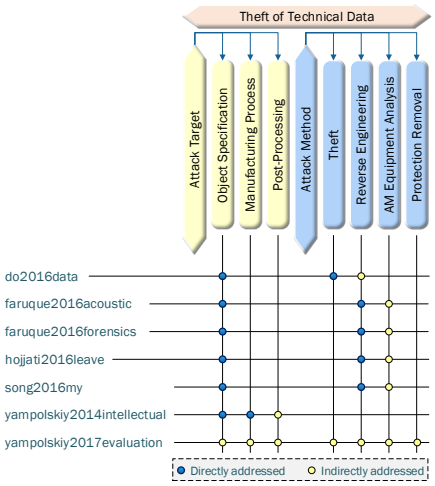

Figure 10: Theft of Technical Data, Aspects addressed in the literature

a dotmatrix printer [95], the physical processes generating and relevant sound in 3D printing are different.

The desktop 3D printer used in the paper employs four stepper motors, three of which are used to move the printer nozzle along the $X/Y/Z$ axes and one to extrude the filament while printing. The authors exploit the fact that parameters like the load and speed of the stepper motor have a distinct impact on the frequency and amplitude of the sound produced by the motor. During the *training phase*, a machine learning approach correlates the recorded sound with the G-code commands influencing the direction, speed, and distance of movement along all axes. During the *attack phase*, this information is used to reconstruct a printed object from the recorded sound[29]. The authors employ experimental evaluation to assess the accuracy of the proposed method to reconstruct a 3D printed object. Based on the experiments performed, they report that their method could achieve on average an 78.35% accuracy of axis prediction; for the length prediction, the proposed method has shown an average error of 17.82% [28].

6.1.3. faruque2016forensics

In [97], an apparent successor of [28], Al Faruque et al. focus on the thermal side channel. The authors utilize an infrared camera to capture thermal images. Based on the image analysis, they attempt to identify individual actions of a 3D printing process, such as nozzle movements. The end goal of the paper is to reconstruct a complete design of a 3D printed object. They de-

[29] Authors require that the sampling frequency of the recording device is higher than 40 kHz.

Attack Vectors	
Cyber-Security	
Flow in Application-Layer Network Protocol	6.4.2 *do2016data* [96], p. 39
Compromised Element	
Cyber-Security	
Computer Network (Wi-Fi)	6.4.2 *do2016data* [96], p. 39
Physical and Cyber-Physical Security	
3D Printer Environment: IR Camera in Physical Proximity	6.1.3 *faruque2016forensics* [97], p. 29
3D Printer Environment: Microphone in Physical Proximity	6.1.2 *faruque2016acoustic* [28], p. 28
3D Printer Environment: Smartphone in Physical Proximity	6.1.5 *hojjati2016leave* [70], p. 31 6.1.6 *song2016my* [69], p. 31
Malicious AM manufacturer	6.1.7 *yampolskiy2014intellectual* [32], p. 31
Attack Method	
Cyber-Security	
Send Valid Protocol Command (Request Last Print Job)	6.4.2 *do2016data* [96], p. 39
Cyber-Physical Security	
Side-Channel Attack: Record Acoustic Emanations	6.1.2 *faruque2016acoustic* [28], p. 28
Side-Channel Attack: Record Acoustic and Magnetic Emanations	6.1.5 *hojjati2016leave* [70], p. 31 6.1.6 *song2016my* [69], p. 31
Side-Channel Attack: Record IR Images	6.1.3 *faruque2016forensics* [97], p. 29
Effect (Theft of Technical Data)	
Cyber Domain	
3D Object's Specification (3D Geometry, Required Properties, etc.)	6.1.7 *yampolskiy2014intellectual* [32], p. 31
3D Print Job (G-code)	6.4.2 *do2016data* [96], p. 39
Printed 3D Object's Geometry	6.1.2 *faruque2016acoustic* [28], p. 28 6.1.3 *faruque2016forensics* [97], p. 29 6.1.5 *hojjati2016leave* [70], p. 31 6.1.6 *song2016my* [69], p. 31

Table 3: Surveyed Publications, Theft of Technical Data

velop a set of algorithms for estimating testbed motions from the video feed, and a mapping algorithm to transform the images into nozzle and base plate activity. The experimental proof of the attack fails to reproduce the movements accurately. The authors assume that this is because of the low quality of the thermal camera (50 Hz, no auto-focus, 640x480 resolution) and the single, fixed viewpoint. Additional and higher quality cameras may improve the accuracy of the algorithm.

6.1.4. gupta2017obfuscade

In an extended version of [98] (see *6.2.2 chen2017security* on p. 32), Gupta et al. [53] propose an anti-counterfeiting system based on pairing defective model features and compensatory manufacturing conditions. The authors demonstrate this system with embedded sphere models and material removal settings. On a printer configured without material removal when slicing, an embedded sphere that is either a surface model or a solid model results in a void, filled with support material. Such voids in functional parts can easily result in fracture under strain. If the printer is configured with material removal, an embedded solid sphere will print with no void, and a surface sphere with support material.

The authors also outline a two-level *Additive Manufacturing Attacks* taxonomy. The taxonomy provides a flat categorization of descriptive elements for AM attacks (when, how, what, why, and where). Taxonomic choices and greater explanation are not provided by the authors; it is used chiefly as a convenient format for briefly overviewing AM security concerns.

6.1.5. hojjati2016leave

Hojjati et al. [70] present a side-channel attack against a wide variety of manufacturing equipment, which reconstructs the form and manufacturing process of an object. The attack uses the acoustic and magnetic side channels, as recorded by a compromised cell phone. A human-led analysis of the recording reconstructs the movements of the manufacturing equipment; the reconstruction is accurate to within one millimeter for line segment length and one degree for turn angles. The authors propose a machine-learning based method for automating the reconstruction. The authors also propose an audio obfuscation method to defend against their attack, in which they play recordings of other, slightly different manufacturing sessions over the current session; early experiments show that the loss of harmonics in the recorded sessions allows the attacker to identify the real session.

The attack implemented here uses methods similar to Al Faruque et al. [28] (see 6.1.2 *faruque2016acoustic* on p. 28), but achieves a substantially greater precision; this may be because of their human-led analysis, the inclusion of magnetic measurements, or better filtering of the data.

6.1.6. song2016my

Song et al. [69] present an attack that is similar to the proposal of Al Faruque et al. [28] (see 6.1.2 *faruque2016acoustic* on p. 28). There are two fundamental distinctions. First, instead of the professional audio equipment used in [28], Song et al. use sensors available in a smartphone. Second, instead of a single side channel, they capture and correlate acoustic and magnetic emanations. This approach enables a significantly more precise reconstruction of the printed object. The authors report a mean tendency error of only 5.87% in reconstructing the printed object.

6.1.7. yampolskiy2014intellectual

Yampolskiy et al. [32] claim that, in the context of AM, IP is not limited to the specification of the 3D object geometry (usually in an STL/ AMF file) alone. It can also include the required properties (corresponding to the operational parameters of a part), and the manufacturing parameters (which ensure that functional parts will satisfy requirements). Further, the authors propose an outsourcing model in which an AM manufacturer offers services to customers, and can rely on the IP of manufacturing parameters provided by a third party.

6.2. IP Violation: Defense Measures

Several solutions have been proposed to either mitigate or detect theft of technical data in AM[30]. Table 4 summarizes the major ideas of the surveyed papers.

[30] We have explicitly excluded from the survey work done on general 3D model watermarking. While such techniques are applicable to AM design files, they will not necessarily consider AM-specific features or the model to printed object transformation. A review of these techniques can be found in Wang et al. [99].

Experimental Works	
Counterfeit Detection	
Physically Unclonable Function (PUF)	6.2.3 *dachowicz2017microstructure* [100], p. 33
Physically Unclonable Function (PUF) with a Blockchain ledger	6.2.10 *kennedy2017enhanced* [101], p. 35
3D Model Watermarks that resistant to 3D Printing and Re-Scanning	6.2.7 *hou20153d* [102], p. 34
3D Model Watermarks that robust to 3D Printing and is blind	6.2.7 *hou2017blind* [103], p. 35
Counterfeit Prevention	
Manufacturing Parameters required for 3D Object Reproduction	6.2.2 *chen2017security* [98, 104], p. 32
Theft Prevention	
Modified Slicer to minimizes Leakage through Acoustic Side-Channel	6.2.3 *chhetri2017fix* [105], p. 33
Theoretical Frameworks	
Counterfeit Detection	
Framework for 3D Printed Objects *Provenance*	6.2.5 *fadhel2014component* [106, 107, 108], p. 34 6.2.6 *fadhel2015provenance* [109], p. 34
3D Object Watermarks	6.2.11 *macq2015applicability* [110], p. 36
Counterfeit Prevention	
Blockchain-based verification of license to print	6.2.9 *holland2017copyright* [111], p. 35
Theft Prevention	
GCode Streaming Model	6.2 *baumann2017model* [112], p. 32

Table 4: Surveyed Publications, Defense against Theft of Technical Data

6.2.1. baumann2017model

Baumann et al. [112] describe a prototype system for securely streaming GCode instructions from an IP owner to a model licensee. With a local adapter on the user's 3D printer, the Streaming Provisioning system transmits GCode from the remote system of the IP owner. This permits the user to print the model without (nominally) possessing redistributable model files. In practice, the authors note there are a number of ways to circumvent the security, including capturing the GCode from the local adapter or scanning the model. Solutions for these are not implemented in the current prototype.

6.2.2. chen2017security

Chen et al. [98] and Gupta et al. [104], in an extended book chapter, consider a scenario where an adversary, despite cyber-security countermeasures, can obtain access to design files. The authors propose to incorporate into the design file features that, if processed and printed with a specific combination of parameters, will result in a high quality part; any other combination of parameters will result in a defective or inferior quality component.

The authors investigate two modifications: (a) a mass- and volume-less split of the original object's body, and (b) incorporating an enclosed spherical object into the part. The authors note that, for the split modification, the difference between the original and tessellated object's geometry depends on the resolution in which the original CAD design is exported into the STL format. Therefore, the authors experiment with a spline (curve-shaped) split. Experiments tested both "x-y" plane and "y-z" plane splits. For a spline in the "x-y" plane, discontinuities appear at a coarse export resolution, but not in fine or custom exports. A spline in the "x-z" plane creates discontinuities under all tested resolutions.

For an enclosed object, the authors first create an empty spherical space and then embed a solid or surface sphere in the cavity. If the embedded sphere is solid, it is printed with the model material; otherwise, it is filled with support

material[31]. All experiments were performed with a Stratasys Dimension Elite 3D printer employing FDM technology. Objects were printed with ABS plastic as a source material and $SR-10^{TM}/P400SR^{TM}$ as soluble support material.

In an invited article [53] (see *6.1.4 gupta2017obfuscade* on p. 30), Gupta et al. extend on this work by proposing a two-level *Additive Manufacturing Attacks* taxonomy.

6.2.3. chhetri2017fix

Chhetri et al. [105] tackle the problem of confidentiality breach resulting from physical-to-cyber domain attacks[32]. For a FDM desktop 3D printer, the authors develop a leakage model that describes the relationship between G-code instructions and information leakage via the acoustic side-channel. The relationships can be quantified in two stages. First, *design-time leakage quantification* can be used to correlate executed G-code commands and information leaked through various side-channels. Second, *run-time leakage information* is necessary to adapt to changes in leakage resulting from equipment wear and change. The authors then integrate the developed model in a slicer and toolpath generation algorithm. This produces design parameters that minimize information leakage through the acoustic side channel. The algorithm iterates through two design variables, *orientation in the x-y plane* and *feedrate*[33]. A benchmark across five objects shows the proposed algorithm reduces acoustic information leakage by 24.76%.

6.2.4. dachowicz2017microstructure

Dachowicz et al. [100] tackle the problem of metal part counterfeiting. Their proposal exploits the fact that, even if the manufacturing process and its control parameters are precisely known, the microstructure still has a high degree of randomness. This makes it impossible to produce a part with exactly the same micrograph, i.e., a specific instance of the random microstructure. Therefore, the micrograph can be used as a fingerprint of a particular part.

The authors propose a physically unclonnable function (PUF) that can be computed over the optically detectable micrograph. The proposed approach first segments the micrograph into several *Regions of Interest* (ROIs) of different length levels. The largest ROI is considered level 0, it is segmented into four ROIs of level 1, and so on. For each of the ROIs, the 3-dimensional mean intercept length of the grains L_3 [113] is calculated. The bit sequence of the PUF is generated by comparing the result for each ROI to the median result across all ROIs; if it is above the median, a bit is set to 1, otherwise to 0.

[31] As shown by Zeltmann et al. [35] (see 6.4.20 *zeltmann2016manufacturing* on p. 46), contamination of the proper material can result in degradation of mechanical properties.

[32] Such attacks are broadly known as *side-channel* attacks.

[33] It should be noted, that these are among manufacturing parameters that can impact a part's function.

The authors argue that the median comparison increases the robustness of this approach against possible damage to a part or slight microstructural changes.

6.2.5. fadhel2014component

Based on the initial results presented in [107, 108], Fadhel et al. [106] propose a framework for providing *provenance* for 3D printed objects. The framework organizes the required data into information security, transmission, and authenticity. The data fields include object ID, timestamps, user authentication, authorizations, etc. In total, the authors refer to this as a 3D Object ID (3DOI). These are to be stored in a secure 3D Data Store and embedded in the object, to allow verification of the object against the 3DOI.

The authors then examine the use of their framework in preventing attacks on 3D printed objects. They consider the cases of a man in the middle attacks producing unlicensed copies, illegal access detection, and counterfeit detection. The authors also examine four proposed systems for implementing their framework: steganography, RFIDs, digital watermarking, and content streaming. Each has incomplete coverage of the framework, with RFIDs covering the most at 5 out of 7 properties.

6.2.6. fadhel2015provenance

In [109], Fadhel et al. propose a signing methodology that aims to transition the metadata associated with the digital 3D object to the physical 3D printed object. They also propose a framework that is intended for securely sharing information about 3D objects using signing methods. The attributes that must transfer to the printed objects are Authentication, Integrity, and Non-Repudiation. They suggest a variety of approaches to maintain provenance, such as steganography[34], digital watermarking, content streaming and RFID hardware. Implanted RFID tags inside the 3D objects also provide tracking capabilities.

6.2.7. hou20153d

Hou et al. [102] present a 3D model watermarking method that can survive the 3D printing and re-scanning process. After aligning a model along its base axis, the method divides the model into layers, corresponding to the layers that will be printed. Each layer of mesh has an exterior with normal vectors in the x-y plane. The watermark is embedded as a modification of these vectors according to a reference pattern, which has been rotated some degree around the object. It can be extracted by a surface scan of the model, which produces a histogram of the features of each layer. However, the method requires that the model be printed along the same axis as the original watermarking. Any statistical feature of the surface can produce a histogram; the authors use normal vector variance in this experiment as it survives several types of attack against 3D watermarks. The authors' method outperforms the earlier method of Cho

[34] Steganography is the art of hiding information in ways that prevent the detection of hidden messages.

et al. [114] in a number of tests, and was successfully extracted in two out of four printed models. In addition, the method performs well against a number of standard attacks against the digital 3D model.

6.2.8. hou2017blind

In a follow-up paper to 6.2.7 *hou20153d* [102], Hou et al. [103] propose a 3D model watermarking system that is both robust to the 3D printing process, and blind, in that no additional information outside the object itself is required to detect the watermark. The system relies on a z-axis invariant watermarking algorithm and a print-axis estimator. By analyzing the layering artifacts characteristic of FDM printing, the estimator realigns a scanned object and allows watermark detection. The authors test their system against a variety of deformations, including noise introduced as a normal part of printing and scanning objects, and common post-processing steps such as painting or sanding. Across three printers and multiple models, the scheme produced varied results. Model characteristics such as size and scaling could reduce detection accuracy, as could higher-resolution printing. Painting or sanding the object likewise made the watermark undetectable. When used with the lower-resolution FDM printers and without post-processing attacks, the scheme produced acceptable false positive rates and print-axis estimates on most models.

6.2.9. holland2017copyright

Holland et al. [111], citing the apparent commoditization of additive manufacturing technologies, urge consideration of methods and tools to aid in the protection of intellectual property. In order to thwart counterfeiting of a copyrighted product or design, the authors discuss the use of product labeling to convey identifying information and to trace a printed object. The authors identify several labeling methods, whether visible, such as with a holographic security tag; invisible, such as with Radio Frequency Identification; and machine-readable only, such as with the incorporation of specialized pigments or foreign particles within or throughout a printed object.

To preserve the rights of the copyright holder, the authors suggest using the labeling method of choice to create an identifier connecting a design document to a copyright license. In particular, blockchain technology can create a chain of trust and prove that a person printing an object did so with a license. In the proposed system, termed Secure Additive Manufacturing Platform (SAMPL), a data base of licenses would be checked by a printer to determine the authenticity of a print request.

6.2.10. kennedy2017enhanced

Kennedy et al. [101] propose a solution for counterfeit detection for fused deposition modeling (FDM) 3D printing with polymers. They combine the generation of a physically unclonable function (PUF) with storing its signature as a blockchain ledger entry. The PUF was generated as a custom feedstock polylactic acid (PLA) enriched with particles of lanthanide-aspartic acid nanoscale

Protected Object
Blueprint
6.3.1 *brown2016legal* [54], p. 36
6.3.4 *ebrahim20163d* [75], p. 38
Design on Object
6.3.1 *brown2016legal* [54], p. 36
6.3.5 *holbrook2014digital* [74], p. 38
Printed Object
6.3.1 *brown2016legal* [54], p. 36
Process
6.3.1 *brown2016legal* [54], p. 36
Protection Method
Copyright
6.3.1 *brown2016legal* [54], p. 36
6.3.2 *craig2017protection* [115], p. 37
Patent
6.3.1 *brown2016legal* [54], p. 36
6.3.4 *ebrahim20163d* [75], p. 38
6.3.5 *holbrook2014digital* [74], p. 38
Trademark
6.3.1 *brown2016legal* [54], p. 36
Liability
Enforcement Challenges
6.3.3 *depoorter2013intellectual* [68], p. 37
Primary and Secondary Products Liability
6.3.5 *reddy2014legal* [116], p. 38

Table 5: Surveyed Publications, Legal Aspects of Intellectual Property (IP) Theft

coordination polymers Ln^{3+}-Asp. While non-altered PLA is used to 3D print the part, the custom material is used to print a unique QR code. The Ln^{3+}-Asp nanoparticles in the QR code generate a chemical signature that can be interrogated nondestructively. The authors propose to store these signatures as Ethereum-based blockchain entries, using QR codes as searchable references.

6.2.11. macq2015applicability

Macq et al. [110] survey watermarking techniques aiming to protect the Intellectual Property Rights (IPR) associated with a 3D object. focusing on 3D digital watermarking techniques. They evaluate the potential of watermarking techniques to withstand shape perturbations, *e.g.,* the intentional alterations or unintentional noise commonly introduced during reverse engineering. This property is necessary to trace the origin of the IP violation. At the same time, the authors argue, watermarks should be small enough to avoid disturbing the visual aspect or surface properties of the object.

6.3. IP Violation: Legal Aspects

Several peer-reviewed publications focus on the legal implications of AM. In this section, we survey publications that consider intellectual property (IP) violation. Table 5 summarizes the central topics of the surveyed papers.

6.3.1. brown2016legal

Brown et al. [54] analyze the ability to protect intellectual property (IP) in AM under current US law. For this, authors investigate which protection

mechanisms are applicable to what items are subject to protection and to what extent. The protection mechanisms considered are *patent*, *copyright*, and *trademark*. The items subject to protection considered are *blueprint*, *process*, *printed object*, and *design of object*. The authors argue that, under current US law, only limited protection of IP in AM can be achieved. While it offers some protection, the existing legal framework evidently has numerous limitations. For instance, a 3D scan of a manufactured object is not considered an original technical drawing (blueprint) [54]. This constitutes a legal technicality/loophole that can be exploited to bypass copyright protection of a blueprint.

6.3.2. craig2017protection

Craig [115] identifies challenges when applying copyright law to additive manufacturing. Agreeing with other authors on the eligibility of copyright, the author proposed that while printed objects are akin to sculpted or architectural works and created blueprint files will likely meet the threshold of originality imposed by the copyright doctrine, there is greater difficulty arguing for copyright status for blueprint files created automatically by scanning an existing tangible object. The lack of originality in the work complicates application of the doctrine and the perceived status of files and printed objects in certain cases.

Citing challenges encountered when protecting the rights to digital media under the Digital Millennium Copyright Act (DMCA) [117], the author expresses concern that the development of technology-based copy-protection methods in additive manufacturing would give rise to circumvention technologies. The ability to recover in the face of a copyright infringement relies on a plaintiff clearing the hurdles of establishing sufficient control over the copyright, possessing the resources necessary to police infringement cases, overcoming an online culture preoccupied with the free availability of electronic resources for efficient use, and interacting with infringers physically located beyond national borders. In response to such challenges, the author proposes the additive manufacturing community collaborate in a manner similar to the Recording Industry Association of America's creation of the Secured Digital Music Initiative to develop a security specification for digital music files. The authors also considers more flexible treatments of copyright and online sales models, which may better serve and survive in the modern media market.

6.3.3. depoorter2013intellectual

Depoorter et al. [68] identifies challenges in creating effective enforcement measures to deter piracy in decentralized manufacturing environments. When infringers cannot be readily identified and the public does not support enforcement, the author predicts challenges in protecting intellectual property for AM. The privacy of home printers, the author claims, gives infringers greater confidence of not being caught.

To compound difficulties in identifying infringers, negative public perception of punitive measures may lead IP owners away from legal action. The author cites lawsuits filed by entities within the music industry, which provoked public

criticism for seeking excessive sums. Enforcement and legal recourse may need to be tempered according to society's opinions, to seem fair and gain support.

6.3.4. ebrahim20163d

In response to the policy recommendations made in Holbrook et al. [74] (see 6.3.5 *holbrook2014digital* on p. 38), Ebrahim [75] challenges the assumptions and issues a rebuttal. Indicating relevant questions left unanswered by the proposed doctrines, the author questions the adequacy of recognizing a digital patent right. Following an analysis of the existing theories supporting patent infringement claims, the author agrees with Holbrook [74] (see 6.3.5 *holbrook2014digital* on p. 38) on the shortcomings of the current doctrine.

To address the practical limitations that prevent effective patent enforcement, the author proposes a shift from punishing end users printing the inventions to targeting the intermediaries distributing the blueprint files. Citing the patent exhaustion doctrine as a potential cause of concern, the author suggests specific reforms that would allow legal disincentives to be created to prevent third-party intermediaries from distributing blueprint files.

6.3.5. holbrook2014digital

Holbrook et al. [74] discuss how patents have limited ability to provide recourse to rights holders of inventions fabricated with 3D printing. Considering the three codified theories on which an infringement claim can be based, the authors state that a claim could be pursued in theory but will likely prove unsuccessful in practice. Noting logistical difficulties in producing supporting evidence, they conclude that patents provide tenuous IP protection for 3D printed inventions.

As an alternative means of recourse, the authors propose an extension of doctrine to recognize digital patent rights. They reason that the unauthorized duplication or transfer of the blueprint scheme is the near-equivalent of printing the patented invention in violation of rights. Similar to protections for digital copyrights, the stronger rights would protect not only the printed inventions but also the digital file used for fabrication. The authors support their recommendation with analogous case law and a series of policy arguments.

6.3.6. reddy2014legal

Reddy [116] discusses both primary and secondary liability while explaining the ramifications of 3D printing for Intellectual Property (IP), contraband production, and at-home regulated items production. Primary liability evolves from the act while secondary liability can result from financial benefit and supervision or knowledge of and contribution to the act. Her note includes steps printer manufacturers and online service providers (OSPs) can take to mitigate illegal acts. OSPs can scan and monitor users and then issue "take down" orders for copyright violations or regulated item designs. Printer manufacturers can include software that will screen and implement restrictions on designs and

materials. Reddy concludes that AM poses a significant threat that requires regulation.

6.3.7. tran2015law

Tran [118] reviews resources discussing the legal implications of 3D printing. Contributing materials include articles printed in journals and law reviews as well as in technical magazines and journals. The author employs a tiered qualitative analysis for each article to discern whether it should be incorporated. To be admitted into the bibliography, a paper must contain at least one section linking 3D printing to law and policy, and that section must be pertinent to the conclusion of the paper as a whole.

6.4. AM Sabotage: Attacks

Tables 6 and 7 outline those elements of the attack analysis framework (see Figure 3) that have been addressed by the surveyed papers[35], and outlines major relevant ideas presented in the paper. In addition, Figure 11 indicates those aspects of the proposed taxonomy that these publications address.

6.4.1. belikovetsky2016dr0wned

While not the first publication raising this issue, to our knowledge Belikovetsky et al. [6, 10] present the first paper with a complete attack chain for sabotage, beginning with the compromise of a benign 3D printing environment, developing and testing a targeted compromise, manipulating the blueprint file, and culminating in the destruction of a $1,000 drone employing a sabotaged propeller. The complete attack is summarized in a YouTube video [124].

Compared to prior work discussing defects in AM [91, 33, 34, 35], one of the authors' most remarkable contributions is that the attack reduces a part's functional life. The defect was crafted to speed the onset of material fatigue, causing the propeller to break after a short time of normal operation. The danger of this attack is that such defects do not necessarily reduce the part's mechanical strength. Therefore, the part could in principle pass non-destructive mechanical tests, and still break much sooner than expected.

6.4.2. do2016data

Do et al. [96] analyze the security of two popular MakerBot 3D printers, the *Replicator* (5*th* gen) and *Replicator Mini*. Both can be connected via Ethernet, Wi-Fi, or USB. Analysis of the communication protocol shows that an adversary on the local network is capable of retrieving current and previously printed 3D models. Further, the authors exploit vulnerabilities in the protocol to obtain credentials (*authentication code* and *client secret*); these credentials could be used to send commands to the 3D printer, such as halting an active printing job or submitting a new one. The network protocol flow also allows retrieving the last submitted print job.

[35] Please note that we have not listed Yampolskiy et al. [29] (see 6.4.19 *yampolskiy2017evaluation* on p. 46) in the table, because of its cross-cutting nature through all elements of the analysis framework.

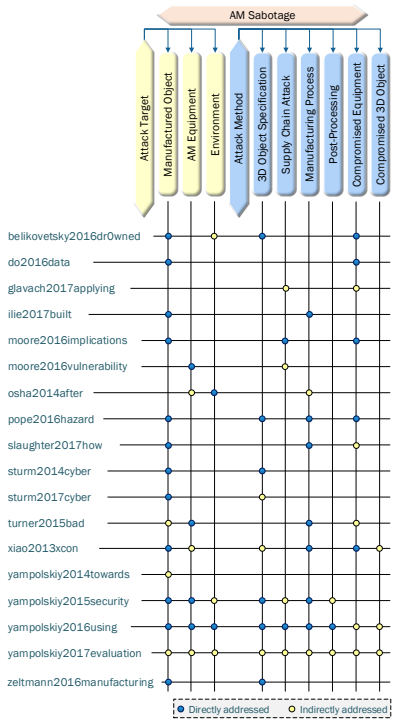

Figure 11: AM Sabotage, Aspects addressed in the literature

Attack Vectors	
Cyber-Security	
Automated Malware (*e.g.*, Computer Worm)	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
	6.4.11 *sturm2014cyber* [33], p. 43
Bugs in 3D Printer Software, Firmware, Network Protocol	6.4.6 *moore2016vulnerability* [119], p. 42
Code injection	6.4.15 *xiao2013security* [91], p. 45
Cyber Supply Chain	6.4.18 *yampolskiy2016using* [27], p. 45
e-Mail Fishing	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
Flow in Application-Layer Network Protocol	6.4.2 *do2016data* [96], p. 39
Internet Connection, Remote Access Enabled	6.4.3 *glavach2017applying* [120], p. 41
Lack of Integrity Checks for Design Files	6.4.13 *turner2015bad* [121], p. 44
Non-Secure Mechanisma for Design Files (*e.g.*, e-Mail, USB)	6.4.13 *turner2015bad* [121], p. 44
Physical Security	
Physical Supply Chain	6.4.18 *yampolskiy2016using* [27], p. 45
Compromised Element	
Cyber-Security	
3D Printer Firmware	6.4.5 *moore2017implications* [92], p. 42
	6.4.15 *xiao2013security* [91], p. 45
Computer Network (Wi-Fi)	6.4.2 *do2016data* [96], p. 39
Controller PC	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
	6.4.11 *sturm2014cyber* [33], p. 43
	6.4.12 *sturm2017cyber* [122], p. 44
	6.4.20 *zeltmann2016manufacturing* [35], p. 46
Physical and Cyber-Physical Security	
Power Grid	6.4.9 *pope2016hazard* [84], p. 43
Powder Recycling System	6.4.18 *yampolskiy2016using* [27], p. 45
Physical Supply Chain (Feedstock, Replacement Parts, etc.)	6.4.17 *yampolskiy2015security* [34], p. 45
Attack Method	
Cyber-Security	
3D Part's External Shape/Size (impacts Part's Fit)	6.4.15 *xiao2013security* [91], p. 45
Insertion of Internal Defects (Voids)	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
	6.4.11 *sturm2014cyber* [33], p. 43
	6.4.12 *sturm2017cyber* [122], p. 44
New Print Job Submission	6.4.2 *do2016data* [96], p. 39
Print Job Cancellation	6.4.2 *do2016data* [96], p. 39
Print Job Substitution	6.4.5 *moore2017implications* [92], p. 42
Physical and Cyber-Physical Security	
AM Process Parameters	6.4.4 *ilie2017built* [123], p. 41
	6.4.17 *yampolskiy2015security* [34], p. 45
	6.4.18 *yampolskiy2016using* [27], p. 45
Built Orientation	6.4.17 *yampolskiy2015security* [34], p. 45
	6.4.20 *zeltmann2016manufacturing* [35], p. 46
Disregard of Safety Regulations	6.4.7 *osha2014after* [85], p. 42
Feedstock (Chemical Composition, Geometry)	6.4.18 *yampolskiy2016using* [27], p. 45
Internal Defect by Replacement of Sourse Material through a Contamenant Material	6.4.20 *zeltmann2016manufacturing* [35], p. 46
Power Supply Interruptions / Manipulations	6.4.9 *pope2016hazard* [84], p. 43
Sensor Readings (Temperature Estimation too High/Low)	6.4.10 *slaughter2017how* [90], p. 43
Temperature of Extruded Filament	6.4.15 *xiao2013security* [91], p. 45
Timing of Commands / Sensor Readings (too late, too early, out of order)	6.4.9 *pope2016hazard* [84], p. 43

Table 6: Surveyed Publications, AM Sabotage (Part 1)

6.4.3. glavach2017applying

Remote access is usually used by OEMs to help setup and calibrate systems, and/or to support maintenance and troubleshooting. However, such connections can lack appropriate security measures. Glavach et al. [120] report an incident where a $750,000 dual-laser 3D printer was connected to the Internet via an open connection normally provided to corporate guests. The OEM could have remote access to the printer, without the owner noticing. The remote access protocol uses the default settings, and was unencrypted [120].

6.4.4. ilie2017built

Although not security-related research *per se*, Ilie et al. [123] cover failure-inducing parameter alterations as proposed by Yampolskiy et al. [34]. For PBF Selective Laser Melting (SLM) [125] and stainless steel alloy 316L, the authors show that by manipulating *laser power* and *exposure time* that it is possible to create layers with increased porosity in the build part. These layers become

Effect (AM Sabotage)	
Manufactured Part	
Different Part (Different Mechanical Properties, and Fit and Form)	6.4.2 *do2016data* [96], p. 39
	6.4.5 *moore2017implications* [92], p. 42
Fit and Form	6.4.15 *xiao2013security* [91], p. 45
Manufactured Object's Microstructure	6.4.10 *slaughter2017how* [90], p. 43
	6.4.17 *yampolskiy2015security* [34], p. 45
Mechanical Properties: Location of Failure Point	6.4.4 *ilie2017built* [123], p. 41
Mechanical Properties: Material Fatigue	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
Mechanical Properties: Tensile Strength, Yield, etc.	6.4.11 *sturm2014cyber* [33], p. 43
	6.4.12 *sturm2017cyber* [122], p. 44
	6.4.18 *yampolskiy2016using* [27], p. 45
	6.4.20 *zeltmann2016manufacturing* [35], p. 46
AM Equipment	
Availability of AM Equipment	6.4.2 *do2016data* [96], p. 39
Explosion of Combustible Dust, and Fire	6.4.7 *osha2014after* [85], p. 42
Increased Wear, Physical Damage	6.4.18 *yampolskiy2016using* [27], p. 45
Environment of 3D-Printed Part	
Physical Damage	6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
	6.4.18 *yampolskiy2016using* [27], p. 45
Contamination	6.4.18 *yampolskiy2016using* [27], p. 45
Environment of AM Equipment	
Physical Damage	6.4.18 *yampolskiy2016using* [27], p. 45
Contamination	6.4.18 *yampolskiy2016using* [27], p. 45

Table 7: Surveyed Publications, AM Sabotage (Part 2)

predictable *failure points* at which the part breaks under mechanical stress. The authors aim for applications where preferential deformation and strategic failure might be desirable. However, exactly the same approach can be used by a sabotage attack.

6.4.5. moore2017implications

Moore et al. [92] present an experimental demonstration of the manipulations that are possible if 3D printer firmware is compromised. The authors modify the popular *Marlin* firmware and load it onto the *Printrbot* desktop 3D printer. This paper shows that it is possible to replace a print job with a completely different object without the controller computer noticing. Further, the authors introduce a novel defect—increasing the amount of extruded filament—and discuss its effect on object geometry.

6.4.6. moore2016vulnerability

Moore et al. [119] analyze open source software broadly used with desktop 3D printers. This includes the *Marlin* firmware and three GUI applications running on a PC and communicating via G-code with the 3D printer: *Cura 3D*, *ReplicatorG*, and *Repetier-Host*. The authors perform a static analysis of the source code and a dynamic analysis of communications between the 3D printer and computer. Numerous exploitable vulnerabilities were present, including the use of fixed size local buffers in combination with potentially unsafe functions like *sscanf* and *memcpy*.

6.4.7. osha2014after

Although it is not a scientific article, the news release [85] describes a serious incident that highlights the sabotage capabilities of AM. On November 5, 2013,

nine serious violations of workplace safety standards at the Woburn, MA 3-D printing company *Powderpart Inc.* resulted in unapproved electrical equipment triggering an explosion of combustible dust[36] and a small fire. As a consequence, one employee suffered third-degree burns.

6.4.8. pan2017taxonomies

Pan et al. [51] (see *6.4.7 pan2017taxonomies* on p. 43) propose a pair of taxonomies: a CPS attack-classification taxonomy against manufacturing systems, and a quality control countermeasures taxonomy. In the attack-classification taxonomy, the authors categorize elements of the chain from attack vectors to impacts, with the most detail given to impacts. This section contains mainly impacts with economic ramifications, and the integrity impacts that directly affect part behavior are considered from an economic standpoint. Overall, the taxonomies are geared towards private-sector manufacturing companies and their means of mitigating attacks.

6.4.9. pope2016hazard

Pope et al. [84] apply the Systems-Theoretic Process Analysis (STPA) framework [126] to hazard analysis in AM. The authors show that this approach can be used to systematically identify manipulations that can be used to sabotage the manufactured part. Timing disruptions in the control loop have potentially hazardous effects; sensor readings and commands that are provided too late, too soon, or out of order are also vulnerabilities. Furthermore, the authors point out that disrupting or manipulating power to the 3D printing process can sabotage the printed object.

6.4.10. slaughter2017how

Slaughter et al. [90] present the first indirect sabotage attack in AM. While prior research on AM sabotage has exercised direct manipulations of either object design or manufacturing process, here the authors exploit the feedback loop existing in *in-situ* quality control. They argue that *in-situ* infrared (IR) thermography can be compromised and provide false sensor readings. Focusing on metal AM with PBF, an analysis shows that this attack can lead to a false state estimation, causing the laser energy to be adjusted either too high or too low. Incorrect laser strength results in microstructural defects like porosity. Such defects can have an immediate impact on a part's mechanical strength or fatigue life. An experimental evaluation on a metal AM machine supports the validity of their analysis.

6.4.11. sturm2014cyber

Sturm et al. [33] discuss that the representation of the object's geometry is transformed by a toolchain used in the AM process. Therefore, the object

[36] According to the Occupational Safety and Health Administration (OSHA) FactSheet [86], dust of fine metal powder particles can be combustible. This also includes titanium and aluminum alloys in powder form that are commonly used in 3D printing [85]

geometry can be corrupted by modifying any of these representations (*e.g.,* additional vertices can be added). This attack can be used to alter the exterior of the object's shape and/or to introduce changes in its internal structure. The authors develop malware that targets STL files, a commonly used file format to represent a 3D object's geometry. This malware automatically inserts voids (internal cavities) in the part's specification described in the STL file. To evaluate the impact of this attack on a part's quality, authors vary properties of the inserted voids, such as its shape, size, location, and whether or not it is located completely inside of the object. A PBF *Sinterstation 2500 Plus* was used with Nylon 12 powder to produce "dogbone" shaped parts, which were run through the ASTM Standard D638-10 tensile test [127]. The experimental evaluation confirms the assumption that the inserted voids will degrade the test object's tensile strength.

6.4.12. sturm2017cyber

Sturm et al. [122] design an attack that automatically places voids in STL files, as they are transferred onto a host PC. The attack algorithm creates a tetrahedral void near high-complexity geometry, ensures that it is fully encapsulated in the object, and scales the void to be as large as possible. An ASTM Standard D638-10 [127] tensile strength test on the infected parts showed an average reduction in yield load of 14%. The authors perform a case study with this attack evaluating a skilled operator's ability to detect sabotage. The subjects, groups of unaware students performing the tensile strength test, failed to attribute the premature fracture of their part to sabotage. Two out of four groups recognized that a void was present and blamed it for the fracture, but believed the void was the result of a machine error. The authors go on to recommend the adoption of software checks and other common file security tools, as well as operator training to detect attacks.

6.4.13. turner2015bad

Turner et al. [121] conduct a study of additive and subtractive manufacturing processes and identify attack surfaces. The manufacturing tool chains contain several attack vectors that can be exploited easily. The authors note that no physical or common cyber-security mechanisms are employed on manufacturing machines. Typically, the design files are transferred via non-secure communication mechanisms like e-mails or USB drives. Further, design files generally incorporate no security mechanisms to verify their integrity. The authors also note that it is impractical to rely on quality control processes to verify a part's integrity because such processes are expensive yet not tailored to detect cyber attacks.

6.4.14. wu2017taxonomy

Wu et al. [52] (see *6.4.13 wu2017taxonomy* on p. 44) propose a three-level *CyberManufacturing System Attacks* taxonomy. At the top level, it distinguishes between *Attack Vector*, *Attack Impact*, *Attack Target*, and *Attack Consequence*,

each of which is sub-divided in *cyber* and *physical* categories. The authors provide only a brief appraisal of each taxonomic category, as their goal is to establish a shared terminology for researchers and security practitioners dealing with attacks against manufacturing systems.

6.4.15. xiao2013security

To the best of our knowledge, the first proof that a desktop 3D printer can be compromised was presented at XCon2013[37] conference by Xiao Zi Hang (Claud Xiao), at that time a senior researcher at *Antiy Labs*[38]. According to his keynote presentation [91], an attack can modify "printing results," including the size of the model, position of components, integrability of components, etc. This could be achieved by modifying software or configuration, object description, or firmware. One of the exploits presented [128], *HalfTemperature*, rewrites the *RepRap* 3D printer's firmware so it sets the target temperature (of extruder and print bed) twice as high as requested by a G-code command and reports back half of the real temperature.

6.4.16. yampolskiy2014towards

Yampolskiy et al. [129] identify the threat of sabotage attacks on AM, particularly degrading print quality and causing damage to equipment. This publication is mainly interesting as one of the earliest on the topic. It was presented as a work-in-progress paper at ACSAC 2014.

6.4.17. yampolskiy2015security

Yampolskiy et al. [34], the authors identify manipulations regarding those manufacturing parameters that can degrade a part's quality. The discussion is based on the related material-science literature for metal AM; it covers AM processes used in manufacturing with metals and alloys, powder bed fusion, direct energy deposition, and sheet lamination. The critical manufacturing parameters identified in this study include build direction, scanning strategy, heat source energy, and degree of vacuum[39]. In a survey by Frazier [56], many of the same parameters are considered from the quality assurance perspective. In [34], the authors also outline manipulations of the manufacturing process that can damage AM equipment; the possibility of inflicting physical damage to the equipment's environment is also discussed.

6.4.18. yampolskiy2016using

Yampolskiy et al. [27] focus on the sabotage of 3D printing. First, the authors propose a framework for analysis of attacks on or with AM (see Figure 3). They begin by classifying the elements of AM workflow that can be compromised. For every class of compromised elements, the authors specify which elements of the

[37] http://xcon.xfocus.org/XCon2013/speakers.html
[38] http://www.antiy.net/
[39] Vacuum is only relevant with AM technologies that employ electron beam (EB) as a heat source.

workflow can be influenced. They then discuss which effects these manipulations can have, focusing on effects commonly attributed to weapons. Three categories are affected by such attacks: *3D objects*, *3D printer*, and *environment*. For every category of affected elements, they propose categories of specific impacts.

The authors also propose to characterize the sabotage of 3D printing based on these criteria: targeting precision, area of impact, collateral damage, stealthiness, and attack repeatability. All identified categories of AM sabotage can subsequently be characterized according to these criteria.

6.4.19. yampolskiy2017evaluation

Yampolskiy et al. [29] evaluate similarities and differences between additive and subtractive manufacturing from the security perspective. To do this, the authors first present workflows for both computer-aided manufacturing technologies and identify common and distinct properties in these workflows. They then apply the framework for attack analysis proposed in [27] (see 6.4.18 *yampolskiy2016using* on p. 45) to investigate the security aspects of three threat categories: theft of technical data (or intellectual property violation), AM sabotage, and manufacturing of illegal items. For the first two threat categories, the analysis identifies 27 similarities and 24 fundamental differences from the security perspective. For the manufacturing of illegal items, the authors could not identify any significant technical differences.

6.4.20. zeltmann2016manufacturing

Zeltmann et al. [35] show that the tensile strength of a test specimen can be degraded by two categories of modifications. First, they test the impact of sub-millimeter scale defects introduced into a 3D printed part. Second, they test the impact of a 3D printed part's orientation during the printing process. A Stratasys Connnex500 printer produced the test parts.

The experimental work of the paper distinguishes it from several earlier works. Compared to Sturm et al. [33] (see 6.4.11 *sturm2014cyber* on p. 43), in which defects have been introduced as voids, the authors use contaminant material to fill cubic defects in three sizes (150 μm, 250 μm, and 500 μm). While changing the build orientation was previously proposed as an attack in Yampolskiy et al. [34] (see 6.4.17 *yampolskiy2015security* on p. 45), the authors show an experimental proof of its effectiveness. Their experiments confirm that this attack can change strength and modulus with respect to the printing direction.

Another significant contribution of this paper is the analysis of defect detectability via non-destructive testing. The authors report that an ultrasonic C-scan has failed to identify the defects; they argue that the surface texture of printed objects causes artifacts that can effectively hide even large defects. For the second defect type, while the authors could clearly distinguish between different printing orientations using an ultrasonic C-scan, they attribute this to the surface roughness introduced in different directions; they assume that surface treatments like polishing and painting would mask these features and prevent detection.

Experimental Works	
3D Geometry	
Acoustic Emanations	6.5.3 *belikovetsky2017detecting* [130], p. 48
	6.5.4 *chhetri2016kcad* [87], p. 49
Impedance-based	6.5.1 *albakri2015non* [131], p. 47
	6.5.8 *sturm2016insitu* [132], p. 50
Visual Imaging and Human-Assitsted Visual Analytics	6.5.7 *straub2017* [133, 134, 135, 136], p. 50
Visual Imaging and Machine Learning	6.5.11 *wu2017detecting* [137, 138], p. 51
Fill Pattern	
Acoustic Emanations and Motion	6.5.2 *bayens2017see* [139], p. 48
Mass Accuracy	
Impedance-based	6.5.1 *albakri2015non* [131], p. 47
	6.5.8 *sturm2016insitu* [132], p. 50
Material	
Raman Spectroscopy	6.5.2 *bayens2017see* [139], p. 48
Overstressed Areas (Visualization)	
Reconstruct of a Close 3D Object Approximation based on G-code & FEA of Properties	6.5.9 *tsoutsos2017secure* [140], p. 51
Theoretical Frameworks	
Cyber-Security	
Vulnerability Assessment	6.5.6 *desmit2016cyber* [141, 142], p. 49
Cyber-Physical Security	
Impedance-based Verification of Dimensional/Positional/Mass Accuracy	6.5.10 *vincent2015trojan* [143], p. 51
Model Relationships between Cyber and Physical Domains	6.5.5 *chhetri2017cross* [144], p. 49

Table 8: Surveyed Publications, Defense against AM Sabotage Attacks

AM security in general and sabotage attacks in particular are relatively new research fields. Sabotaged parts have been identified in the context of non-destructive evaluation (NDE). However, the NDE techniques that are well-suited for subtractive manufacturing have significant limitations when applied to AM. Albakri et al. [131] summarizes the issues as follows: Coordinate Measuring Machines (CMM) [145] and Structured Light (SL) [146] scanning require access to all surfaces of the part; Eddy Current Testing (ECT) [147] and Ultrasonic Testing (UT) [148] for detection of internal porosity require access to all surfaces, offer limited surface penetration, and have been shown to be sensitive to surface roughness. Penetrant Testing and Magnetic Particle Testing [149] are less geometry-sensitive and thus cannot be employed to assess parts with internal structures; Computed Tomography (CT) [150], while capable of detecting deep/embedded defects, is costly, time-consuming, limited by part size, and is unable reliably to detect cracks that are perpendicular to the X-ray beam. Therefore, NIST [151] and NASA [152] see the necessity for new NDE techniques optimized for AM. In this section, we survey new methods developed to detect an ongoing sabotage attack or to identify a sabotaged part.

Table 8 summarizes the major ideas of the papers proposing countermeasures against sabotage attacks in AM.

6.5.1. albakri2015non

Albakri et al. [131] propose to apply impedance-based Structural Health Monitoring (SHM) to detect deviations in a built part, an approach that has shown good results in detecting structural damage (*e.g.,* in a bridge section and a pipe joint [153]). Impedance-based SHM using an attached piezoelectric sensor depends on the mass, stiffness, and damping characteristics of the monitored part. The authors argue that these will be modified by unintentional and intentionally introduced defects.

The authors investigate whether or not the proposed method can be applied to detect the following categories of defects: dimensional inaccuracy, positional inaccuracy, and internal porosity. The test specimens were fabricated in VeroWhitePlus polymer [154] using a Stratasys Connex 350 multi-material jetting AM system [155]. The impedance signature of the produced test specimens was measured for the frequency range 10-20 KHz with a frequency sweep resolution of 10 Hz. The evaluation results show that the first two defect categories can be detected with high confidence. Detecting internal porosity proved to be problematic. The authors argue that it is because this category of defect does not greatly impact the part's mass. They hypothesize that different frequency ranges might provide better results, and that the sensitivity will increase for stiffer materials.

6.5.2. bayens2017see

Bayens et al. [139] consider a threat model in which either the control PC or printer firmware is compromised. When the same object is manufactured multiple times, the authors propose a three-layer framework consisting of acoustic, spectroscopic, and gyroscopic replication verifications. Acoustic verification exploits motor noise to determine whether a print matches a previously known one, similar to the approaches previously proposed by Chhetri et al. and Belikovetsky et al. (see 6.5.4 *chhetri2016kcad* on p. 49 and 6.5.3 *belikovetsky2017detecting* on p. 48, respectively). To address the concerns of material substitutes raised by Yampolskiy et al. (see 6.4.18 *yampolskiy2016using* on p. 45), the material is verified using Raman spectroscopy.

Lastly, spatial verification is used to provide the visualisation of real movements of 3D printer nozzle, not of sent G-code commands as is commonly done by 3D printing software.

The authors verify the proposed approach on a model of a tibial knee implant, using three different models of desktop 3D printers operating on ABS and PLA polymers. They report that changes in fill pattern (*e.g.,* from 60% Rectilinear fill to 20% Honeycomb fill can be reliably detected). A noisy environment or a non-directional microphone reduced detectability significantly. The Renishaw InVia micro-Raman system [156] had a maximum penetration depth of 300 μm; this limits the material verification to exposed surfaces. The authors also report that the gyroscopes have a high degree of error, and therefore should be combined with data acquisition means like cameras.

6.5.3. belikovetsky2017detecting

Belikovetsky et al. [130] exploits the acoustic side-channel to detect sabotage attacks on a FDM desktop 3D printer, similar to works by Chhetri et al. and Bayens et al. (see 6.5.4 *chhetri2016kcad* on p. 49 and 6.5.2 *bayens2017see* on p. 48, respectively). The authors use Principal Component Analysis (PCA) [157] to generate and compare audio signatures of the 3D printing process. Then the validity of the follow-up prints is verified by comparing their signature against the benign signature.

To verify the quality of their approach, the authors define *atomic* (or *minimal*) modifications as insertion, deletion, reordering, or parameter modification of single G-code commands. For these atomic manipulations, they determine thresholds under which they can be reliably detected; all these thresholds are measured in seconds of modified command execution. The proposed approach is capable of reliably identifying all atomic manipulations but changes to filament extrusion. Further, the authors report that the proposed method cannot detect attacks like changes of the source material or of extruded filament temperature.

6.5.4. chhetri2016kcad

In order to detect attacks manipulating object specification (regardless of the stage and representation), Chhetri et al. propose to monitor acoustic side-channel emanations accompanying the 3D printing process, and use this information to reconstruct the model of the printed object. Deviations between the reconstructed model and the original design can indicate an attack.

The work is based on the work of Al Faruque [28] (see 6.1.2 *faruque2016acoustic* on p. 28), who used side-channel analysis for the exfiltration of the 3D object design. To evaluate their approach, the authors consider an attack that changes nozzle speed in the x and y directions while printing. The method is able to detect attacks with 77.45% accuracy.

6.5.5. chhetri2017cross

The proposal of Chhetri et al. [144] can be seen as a generalization of both cross-domain attacks and cross-domain defense approaches shown for AM. The authors introduce the concept of cross-domain security[40]. The proposed model covers relationships between the cyber and physical domain components and their signals. It can be used for various purposes: (i) determining information leakage, (ii) detecting abmormal behavior in physical domain, (iii) predicting system and component failure, and (iv) designing and analyzing cross-domain attacks [144].

6.5.6. desmit2016cyber

Desmit et al. [141] propose an intelligent manufacturing vulnerability assessment approach to comply with the relevant NIST Framework [158]. The approach maps manufacturing processes as a set of entities that intersect with each other, transforming resources through their interactions. Physical resources and equipment, cyber or cyber-physical controls and design tools, and the humans operating the process must all be modeled and assessed. The authors assert that all vulnerabilities occur at the intersections of these entities.

The assessment takes place as a set of self-directed questions for the manufacturer, producing a low, medium, or high vulnerability level along several

[40]The proposal is similar to the approach introduced by Wu et al. [137, 138] in the same year. Similar to the proposal of Wu et al. [137, 138], the visualization of attacks in terms of originating and target domains if based on cross-domain attack introduced by Yampolskiy et al. [30, 31].

criteria at each intersection. Multiple high or medium vulnerability levels indicate a vulnerable node. In a case study published as a follow-up paper [142], the approach correctly identified a vulnerable node used in an independently run attack. The attack, which modified and replaced the CAD file used to manufacture a jet engine bracket, also exposed a flaw in the assessment in bypassing detection in a stage assigned a low risk for detection failures. Because the attack was designed with an awareness of the Coordinate Measuring Machine (CMM) test plan, the testing phase was unable to detect it.

*6.5.7. straub2017**

In a series of papers [133, 134, 135, 136], Straub explores image-based fault detection and security for 3D printing. The initial work [159] uses per-pixel image value comparisons from five different angles to track the completion of a part. Changes to camera position, lighting, or background scenery were found to degrade the quality substantially. Adapting the same technique, the author approaches defect detection [136], mis-positioned prints [135], and the use of incorrect print material [133]. Unlike the programmatic completion analysis in [159], the latter applications rely on human operators to identify issues in the generated comparison images. Further, print material detection is limited to changes in color and reflectivity, and is not tested by printing in different materials. Instead, two identical images are re-processed and compared. Mispositioning is likewise not tested by the standards of the first experiment. The author considers the use of these approaches as part of a combined security system in [134].

6.5.8. sturm2016insitu

Sturm et al. [132] propose a system building upon the prior work of Albakri at el. [131]. The authors assume that a part's material will influence the electrical impedance of a physically coupled piezoelectric sensor. If such sensing is used in-situ during the build process, small defects can be detected as the part is fabricated. Further, because the impedance varies with the whole object's material, changes that might occur in already fabricated layers can be detected. Baseline signatures can be recorded while printing a verifiably benign part[41], at each inspection layer. When the part goes into production, prints can be verified against the baseline signature.

The proposed approach is shown by experiment to be capable of detecting changes in layers. A rectangular prism void defect could be detected at layer 198; the defect volume was 219 mm^3, corresponding to 6.7% of the total part volume. A triangular prism defect could be detected at layer 218; the defect volume was 29 mm^3, corresponding to 0.8% of the total part volume. However, the sensitivity of the method decreases with increases in a part's mass. Sensitivity also falls off with distance between sensor and defect. The authors note that the sensitivity of the proposed approach depends on the stiffness of the part's

[41] Verification can be done post-production using non-destructive and destructive methods.

material and support structure. As polymer is less rigid than metal, they assume that the sensitivity with metal parts will be higher than in the conducted experiments. Furthermore, the authors claim that defects in embedding (*e.g.,* the physical bond between the part and the sensor) can impair the sensitivity.

6.5.9. tsoutsos2017secure

Tsoutsos et al. [140] propose an approach to detect structural integrity defects. The approach has two stages. First, a compiled toolpath (G-code) representation of an object is used to approximate the original 3D object. Second, Finite Element Analysis (FEA) [160] simulates the performance of the object under different stress conditions. The FEA simulation returns a color coded image illustrating any overstressed area. Based on the simulation results and knowledge of the specified stress tolerances, it is possible to determine whether the printed object will meet the requirements.

Among the advantages of this approach is that it only requires the material parameters and force specification. However, as noted by the authors, the granularity of the provided G-code commands (*e.g.,* influenced by slicing parameters like layer height) inevitably leads to information loss; this will limit the detection granularity. This approach also cannot prevent attacks introduced by malicious firmware; such an attack has been already demonstrated by Moore et al. [92] (see 6.4.5 *moore2017implications* on p. 42).

6.5.10. vincent2015trojan

Vincent et al. [143] argue that existing quality control (QC) systems are inadequate for detecting sabotage attacks introduced via a compromised manufacturing system. The authors state that QC measures generally focus on a product's key quality characteristics (KQC), which a sophisticated attacker might avoid altering. Further, they provide a hypothetical scenario where manipulating a design file can cause an additional hole to be punched into a manufactured car's frame rail, reducing its mechanical properties.

The authors propose attaching piezoelectric transducers (PZT) to a manufactured part, to measure its impedance and distinguish between altered and unaltered parts. This solution has shown good results in structural health monitoring (SHM) the context of AM by Albakri et al. [131] and Sturm et al. [132] (see 6.5.1 *albakri2015non* on p. 47 and 6.5.8 *sturm2016insitu* on p. 50, respectively).

6.5.11. wu2017detecting

Building upon the notion and taxonomy of cross-domain attacks introduced by Yampolskiy et al. [30, 31], Wu et al. [137, 138] provide motivation for cross-domain attack detection[42]. With FDM technology in mind, the authors propose to use a combination of feature extraction from gray-scale images and machine

[42] In this regard, this approach is similar to the proposal of Chhetri et al. [144] (see 6.5.5 *chhetri2017cross* on p. 49) published the same year.

Liability
Products Liability
6.5.11 *berkowitz2014strict* [162], p. 52
6.5.11 *comerford20153dp* [163], p. 52
6.6.3 *malloy2016three* [164], p. 53
6.6.3 *wang2016classical* [165], p. 53

Table 9: Surveyed Publications, Legal Aspects related to AM Sabotage

learning. For each section of captured images the following features are extracted: mean of gray-scale, standard deviation of gray-scale, and number of pixels whose gray-scale is larger than 120. To detect an attack, the authors evaluate three machine learning algorithms: k-Nearest Neighbor (kNN), random forest, and anomaly detection. The proposed approach was evaluated on parts with honeycomb infill density[43] varying 8-12%. The simulated attacks contain five categories of defects: seam, irregular polygon, circle, rectangle, and triangle. In all tests, the anomaly detection algorithm showed better results. The authors report 96.1% detection accuracy when the camera was statically mounted. When the camera was mounted on the 3D printer frame and moved during the printing process, the accuracy dropped to 72.5%. The authors explain this by the blur in images caused by the motion.

6.6. AM Sabotage: Legal Aspects

While we are not aware of legal articles directly discussing legal aspects of AM sabotage attacks, there are several articles tackling the related issue of a product liability in the case of injuries. This section surveys these publications, because they might provide a basis for the future explicit discussion of AM sabotage legal aspects. Table 9 indexes the surveyed papers.

6.6.1. berkowitz2014strict

While proposing a micro-seller category between the 'occasional' hobbyist producer and a manufacturing enterprise, Berkowitz [15] analyzes the applicability of negligence and breach of warranty as well as strict liability and the related defenses. She proposes retaining strict liability for 3D printing but creating a new affirmative defense for micro-sellers. Berkowitz argues doing so meets the social policies of balancing protection with fairness.

6.6.2. comerford20153dp

Comerford and Belt [163] discuss strict liability, negligence, and breach of warranty as they examine the exposure of scanning services, providers, and large

[43] In addition to solid fill, slicers often support a number of infill patterns of varying density. This allows one to produce lighter parts while reducing the amount of source material consumed. For example, "honeycomb" is one of the infill patterns supported by *Slic3r* [161], a slicer frequently used by desktop 3D printers.

scale manufacturers. They suggest that with definitive roles and responsibilities the entire AM chain can be characterized by the authorized dealer distribution chain construct, albeit virtual. As such, Comerford and Belt contend that contracts and insurance provide protection and indemnification in case of liability.

6.6.3. malloy2016three

Malloy [164] explores the application of product liability for recovery theories available to a plaintiff injured by a product manufactured by a 3D printer. While the doctrine applies strict liability only to commercial sellers and distributors, negligence is applicable for non-commercial actors. The author's discussion of the topic distinguishes between the original source of a defect and the manifestation of the defect. The source of the defect aids in determining liability for the manufacturer of the printer, the creator of the blueprint, or the person who prints the object; how the defect manifests aids in determining whether the claim pertains to a manufacturing defect, a design defect, or an insufficient warning or instructions.

Because of the nature of additive manufacturing, the applicability of a particular claim is not settled law. Two instances discussed by the author are the determination of the standards to apply for instructions and warnings and the determination of whether an actor is suitably involved commercially for strict liability to apply. While the author tackled the issue pertaining to recovery theories, he did not fully differentiate when a defect in the design of a printed creation would result in liability for the blueprint designer or for the person who had printed the object. Furthermore, the paper did not discuss the applicability of product liability following a duty to inspect a product that had been altered by a third party.

6.6.4. wang2016classical

3D printing services (3DPS) are examined as a liability target in Wang [165]. Major concerns are whether 3DPS provide a product or should be held liable without knowing the CAD file details. His comment also describes design defect determination by risk-utility analysis. The analyses combine risk, utility, and consumer expectations. Utility encompasses reasonable alternatives and risk considers inherent safety and mitigability. Other factors are product desirability and loss distribution. Wang concludes with 'ink' and the impact wrong materials can have on the final product, providing a defense to other actors.

7. Discussion

Figure 12 demonstrates the scientific community's growing attention to the field of AM Security. While the field is still new, there are several lessons that can be learned from the current state of the art presented in Section 6. There are also important aspects that have not been adequately addressed so far. Without seeking to diminish the importance of the extant scientific contributions, in this section we take a critical look at both.

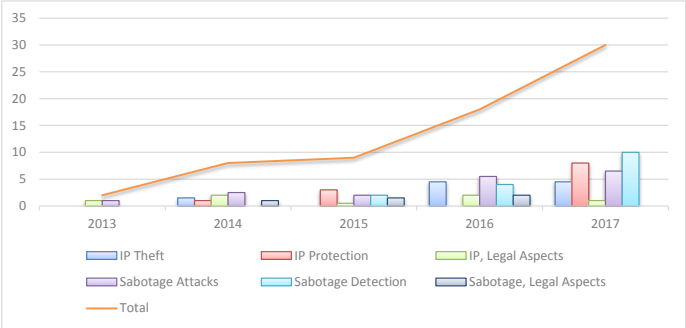

Figure 12: AM Security, Surveyed Publications per Year (State: December 2017)

7.1. AM Processes & Source Materials

We start our discussion with an analysis of AM processes and source materials that have been used in the research thus far. As shown in Table 10, the majority of work in the field has been performed on desktop 3D printers employing *fused deposition modeling* (FDM) [11] AM process. This applies to works on both attacks and defense measures.

FDM is the dominant process for polymers (plastic). However, FDM is not the only AM technology to work with polymers, and—most important—it has no relevance for metal AM. The few publications covering metal AM focus on *powder bed fusion* (PBF). While it is one of the most used processes for metal AM, it is rivaled by *Directed Energy Deposition* (DED). While PBF can produce objects with high degree of precision, it is currently limited by the size of the printed object; DED doesn't have this limitation, but parts produced with DED require extensive post processing for acceptable surface finishes [166].

Another aspect that we would like to highlight is the source materials used. The majority of research has been performed on parts produced with polymers (plastic). Because of material properties, plastic parts are not commonly used in safety-critical systems. Metal and composite material parts are, however, widely used in safety-critical systems, but are of limited relevance to the consumer market, predominantly because of their costs.

Inasmuch as the majority of work has been performed on desktop FDM 3D printers, it is not yet clear whether lessons learned and solutions developed are at all applicable to industrial-grade 3D printers (even those employing the same FDM technology). Moreover, in view of the significant difference between the AM processes employed when working with plastics or metals, it is not likely that many lessons learned with and solutions developed for the FDM process will be applicable either to PBF or DED.

7.2. Thresholds in Attacks and Defense Measures

Numerous studies have provided empirical evidence that both IP violation and AM sabotage attacks are possible. Less commonly explored are questions

Fused Deposition Modeling (FDM), Polymers
IP Violation: Attacks
6.4.2 *do2016data* [96], p. 39
6.1.2 *faruque2016acoustic* [28], p. 28
6.1.3 *faruque2016forensics* [97], p. 29
6.1.5 *hojjati2016leave* [70], p. 31
6.1.6 *song2016my* [69], p. 31
IP Violation: Defense Measures
6.2.2 *chen2017security* [98], p. 32
6.2.3 *chhetri2017fix* [105], p. 33
6.2.7 *hou20153d* [102], p. 34
AM Sabotage: Attacks
6.4.1 *belikovetsky2016dr0wned* [6, 10], p. 39
6.4.2 *do2016data* [96], p. 39
6.4.5 *moore2017implications* [92], p. 42
6.4.6 *moore2016vulnerability* [119], p. 42
6.4.11 *sturm2014cyber* [33], p. 43
6.4.15 *xiao2013security* [91], p. 45
6.4.20 *zeltmann2016manufacturing* [35], p. 46
AM Sabotage: Defense Measures
6.5.1 *albakri2015non* [131], p. 47
6.5.2 *bayens2017see* [139], p. 48
6.5.3 *belikovetsky2017detecting* [130], p. 48
6.5.4 *chhetri2016kcad* [87], p. 49
6.5.7 *straub2017** [133, 134, 135, 136], p. 50
6.5.8 *sturm2016insitu* [132], p. 50
6.5.9 *tsoutsos2017secure* [140], p. 51
Powder Bed Fusion (PBF), Metals
IP Violation: Defense Measures
6.2.3 *dachowicz2017microstructure* [100], p. 33
AM Sabotage: Attacks
6.4.3 *glavach2017applying* [120], p. 41
6.4.4 *ilie2017built* [123], p. 41
6.4.7 *osha2014after* [85], p. 42
6.4.9 *pope2016hazard* [84], p. 43
6.4.10 *slaughter2017how* [90], p. 43
6.4.17 *yampolskiy2015security* [34], p. 45
6.4.18 *yampolskiy2016using* [27], p. 45

Table 10: AM Processes and Materials in the AM Security Literature

regarding how representative these attacks are of real-world attacks, and how they might be prevented and/or detected.

7.2.1. Theft of Technical Data

Several publications show that a 3D object's model can be stolen using side-channel analysis, even based on the information collected by a conventional smartphone. This attack strategy has shown remarkable results like object's 3D geometry reconstruction with above 90% precision. However, current research literature lacks discussion of use cases regarding when and what technical data can be stolen in the AM context, to what degree of precision (or other properties) would an adversary have to achieve in this case, and what methods are available that enable this. For instance, when considering industrial settings, what degree of precision is sufficient in the case of industrial espionage? Or in the case of home manufacturing, what degree of precision can be achieved with other or multiple side channels, so that cyber-security protection measures can be bypassed?

	Current	Needed
3D Printer	Desktop	Industrial-Grade
AM Process	FDM	PBF, DED
Materials	Polymers	Metals, Composites
Attacks	Arbitrary	Optimal / Stealthy
	Attack Categories	Atomic Manipulations
Defense Measures	Proof of Concept for *Chosen Attacks*	Detectability Thresholds

Table 11: Summary of Current & Needed in AM Security

Similarly, several interesting approaches to protect technical data have been proposed. However, the current research literature lacks a thorough discussion of how resistant these measures can be against various classes of attacks. For instance, what is the complexity of identifying and removing an imprinted watermark, or of identifying parameters under which a part will be printed correctly?

7.2.2. AM Sabotage

The sabotage attacks shown thus far impair mechanical properties of a manufactured part, restricting either to tensile strength or fatigue life. For this kind of sabotage, defects such as internal gaps or build orientation have been explored as attack means. No studies thus far of which we are aware have attempted to achieve a target effect while minimizing their attack's detectability, which might more accurately simulate a real attack.

To address this concern, we see the necessity of an *optimal sabotage attack*; such an attack can be defined as the minimal manipulation that, for a particular part and operational conditions, leads to the desired degradation of properties of the given part. When multiple parameters are optimized simultaneously, multiple solutions can exist. Therefore, *constrained optimal* or *prioritized optimal sabotage attacks* can be considered, in which only a subset of parameters should be optimized, the maximum tolerable deviations can be constrained, and the order of the parameter optimization can be prioritized. Sabotage attack detection is in a similar situation. While numerous interesting proposals have been discussed in the literature, the majority of the surveyed papers do not discuss detectability thresholds. Even when the thresholds are given, they are often given in a variety of measures like detection accuracy, volumetric size of the defect, etc. This makes it is virtually impossible to compare the quality of the developed countermeasures. In this context we would like again to mention a proposal by Belikovetsky et al. [130] (see 6.5.3 *belikovetsky2017detecting* on p. 48) to determine thresholds of *atomic* (or *minimal* possible) modifications such as insertion, deletion, reordering, and/or parameter modification of a single G-code command. This would allow threshold definitions based on the minimal possible primitives.

8. Conclusion

Additive Manufacturing (AM), also known as 3D Printing, is an emerging technology for producing 3D objects by joining thin layers of material. Numerous socioeconomic, environmental, and technical advantages have lead to the rapid adoption of this technology. As the pervasiveness and importance of this technology to society and the economy grows, so does the attractiveness of attacks *on* and/or *with* additive manufacturing.

This paper was written to support research on *AM Security*. For researchers just entering AM Security, we provided an in-depth introduction to this highly multi-disciplinary research field in its current state. For active researchers in the field, this paper provided a structured and comprehensive survey that should support identification of the relevant publications.

As a basis for discussion, first we outlined a workflow characteristic for industrial-grade metal AM. Most AM-produced functional parts for safety-critical systems are are made of metals. Then, we explained how attacks on or with AM can be performed, distinguishing between *attack vectors*, *compromised elements*, *manipulations*, and their *effects*. We introduced the notions of (i) an *attack method* as semantically identical modifications introduced by different compromised elements, and (ii) *attack targets* (or *security threats*) as an intersection of achievable effects and adversarial goals (or objectives).

Thus far, two major security threats have been identified and discussed in the research literature: *theft of technical data* and the *sabotage of AM*. We proposed a taxonomy of attacks *on* or *with* AM for each of these threats. Both taxonomies enumerated *attack methods* and *attack targets*, and indicated which methods can achieve given targets. The proposed taxonomies are based on the current state of the art as well as on our estimation of emerging threats. For both threat categories, we presented a comprehensive survey of the relevant AM security research literature, including performed attacks, proposed defense measures, as well as a discussion of legal aspects. For publications discussing attacks, we indicated which elements of the taxonomies have been addressed. Last but not least, we took a critical look at the current state of the art and identified several gaps (see, for example, Table 11). These must be addressed to ensure the security and safety of sectors that increasingly rely on AM products.

Acknowledgment

The authors would like to thank Lynne Graves and further reviewers for very valuable comments that helped to improve this manuscript.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344.

This material is based upon work supported in party by the National Science Foundation under Grants Nos. 1547245, 1642083, and 1642133. Any opinions, findings, and conclusions or recommendations expressed in this material are

those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] T. Kellner, Fit to print: New plant will assemble worlds first passenger jet engine with 3d printed fuel nozzles, next-gen materials (2014).
URL http://www.gereports.com/post/80701924024/fit-to-print

[2] T. Wohlers, Wohlers Report 2017 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report, Wohlers Associates, Inc., Fort Collins, Colorado, USA, 2017, www.wohlersassociates.com.

[3] Ernst & Young, How will 3D printing make your company the strongest link in the value chain?, Tech. rep., Ernst & Young (2016).

[4] NIST, Special publication 1176: Costs and cost effectiveness of additive manufacturing, Tech. rep., NIST (2014).

[5] D. S. Thomas, Special publication 1163: Economics of the u.s. additive manufacturing industry, Tech. rep., NIST (2013).

[6] S. Belikovetsky, M. Yampolskiy, J. Toh, Y. Elovici, dr0wned-cyber-physical attack with additive manufacturing (2016).

[7] T. A. Campbell, O. S. Ivanova, Additive manufacturing as a disruptive technology: Implications of three-dimensional printing, Technology & Innovation 15 (1) (2013) 67–79.

[8] C. Mota, The rise of personal fabrication, in: Proceedings of the 8th ACM conference on Creativity and cognition, ACM, New York, NY, USA, 2011, pp. 279–288.

[9] A. Daly, Regulating revolution: An introduction to 3d printing and the law, in: Socio-Legal Aspects of the 3D Printing Revolution, Springer, London, 2016, pp. 1–17.

[10] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, dr0wned – cyber-physical attack with additive manufacturing, in: 11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, Vancouver, BC, 2017, p. 16.
URL https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky

[11] ASTM International, Standard terminology for additive manufacturing technologies (2012).

[12] J. D. Hiller, H. Lipson, Stl 2.0: a proposal for a universal multi-material additive manufacturing file format, in: Proceedings of the Solid Freeform Fabrication Symposium, no. 1, 2009, pp. 266–278.

[13] H. Lipson, AMF tutorial: The basics (Part 1), 3D Printing and Additive Manufacturing 1 (2) (2014) 85–87.

[14] A. International, Standard Specification for Additive Manufacturing File Format (AMF) Version 1.2, Active standard iso / astm52915-16, ASTM International, West Conshohocken, PA (2016).

[15] 3MF Consortium, 3d manufacturing format specification and reference guide (2015).

[16] America Makes & ANSI Additive Manufacturing Standardization Collaborative (AMSC), Standardization roadmap for additive manufacturing (2017).

[17] Wohlers Associates, Inc., Additive Manufacturing Technology Roadmap for Australia, Wohlers Associates, Inc., Fort Collins, Colorado, Fort Collins, Colorado, USA, 2011.

[18] Electronic Industries Association and others, Interchangeable Variable Block Data Format for Positioning, Contouring, and Contouring/Positioning Numerically Controlled Machines, Electronic Industries Association, 1980.

[19] SAE International, New, revised, reaffirmed, stabilized, and cancelled sae aerospace material specifications (2017).
URL `http://standards.sae.org/recent-ams/`

[20] Y.-C. Hagedorn, Manual for SLM research equipment, Tech. rep., Fraunhofer ILT (2015).

[21] M. Mani, B. Lane, A. Donmez, S. Feng, S. Moylan, R. Fesperman, Measurement science needs for real-time control of additive manufacturing powder bed fusion processes, Nistir 8036, National Institute of Standards and Technology, Gaithersburg, MD (2015).

[22] S. K. Everton, M. Hirsch, P. Stravroulakis, R. K. Leach, A. T. Clare, Review of in-situ process monitoring and in-situ metrology for metal additive manufacturing, Materials & Design 95 (2016) 431–445.

[23] S. Clijsters, T. Craeghs, S. Buls, K. Kempen, J.-P. Kruth, 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.

[24] H. Attar, M. Calin, L. Zhang, S. Scudino, J. Eckert, Manufacture by selective laser melting and mechanical behavior of commercially pure titanium, Materials Science and Engineering: A 593 (2014) 170–177.

[25] Y. Zhai, H. Galarraga, D. A. Lados, 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.

[26] K. Zeng, D. Pal, B. Stucker, A review of thermal analysis methods in laser sintering and selective laser melting, in: Proceedings of Solid Freeform Fabrication Symposium Austin, TX, 2012, pp. 796–814.

[27] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. A. Overfelt, K. R. Sloan, A. Yasinsac, Using 3D Printers as Weapons, International Journal of Critical Infrastructure Protection 14 (2016) 58–71.

[28] M. A. Al Faruque, S. R. Chhetri, A. Canedo, J. Wan, Acoustic side-channel attacks on additive manufacturing systems, in: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), IEEE, 2016, pp. 1–10.

[29] M. Yampolskiy, W. E. King, G. Pope, S. Belikovetsky, Y. Elovici, Evaluation of additive and subtractive manufacturing from the security perspective, presented at IFIP WG 11.10 International Conference on Critical Infrastructure Protection (in print) (2017).

[30] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, J. Sztipanovits, Taxonomy for description of cross-domain attacks on CPS, in: Proceedings of the 2nd ACM international conference on High confidence networked systems, ACM, New York, NY, USA, 2013, pp. 135–142.

[31] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, J. Sztipanovits, A language for describing attacks on cyber-physical systems, International Journal of Critical Infrastructure Protection 8 (2015) 40–52.

[32] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, A. Yasinsac, Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing, in: Proceedings of the 4th Program Protection and Reverse Engineering Workshop, ACM, New York, NY, USA, 2014, p. 7.

[33] L. Sturm, C. Williams, J. Camelio, J. White, R. Parker, Cyber-physical vunerabilities in additive manufacturing systems, Context 7 (2014) 8.

[34] M. Yampolskiy, L. Schutzle, U. Vaidya, A. Yasinsac, Security challenges of additive manufacturing with metals and alloys, in: Critical Infrastructure Protection IX, Springer, 2015, pp. 169–183.

[35] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, R. Karri, Manufacturing and security challenges in 3d printing, Jom 68 (7) (2016) 1872–1881.

[36] N. Bilton, The Rise of 3-D Printed Guns, http://www.nytimes.com/2014/08/14/fashion/the-rise-of-3-d-printed-guns.html?_r=0, [Online; accessed 30-Mai-2016] (2014).

[37] A. Greenberg, Feds Tighten Restrictions on 3-D Printed Gun Files Online, https://www.wired.com/2015/06/feds-restrict-3d-printed-gun-files/, [Online; accessed 30-Mai-2016] (2015).

[38] A. Sternstein, THE FBI IS GETTING ITS OWN, PERSONAL 3D PRINTER FOR STUDYING BOMBS, http://www.nextgov.com/defense/2014/06/fbi-getting-its-own-personal-3d-printer-studying-bombs/86476/, [Online; accessed 30-Mai-2016] (2015).

[39] D. Cooper, 3D printing files for guns are illegal in an Australian state, http://www.engadget.com/2015/11/23/3d-printing-guns-new-south-wales/, [Online; accessed 30-Mai-2016] (2015).

[40] M. A. Lemley, Ip in a world without scarcity, NYUL Rev. 90 (2015) 460.

[41] J. Jacobs, A. Haberman, 3d printed firearms, do-it-yourself guns & the second amendment, Law and Contemporary Problems, Forthcoming 80 (129) (2016) 16–27.

[42] J. Blackman, The 1st amendment, 2nd amendment, and 3d printed guns, Tenn. L. Rev. 81 (2014) 479–538.

[43] K. F. McMullen, Worlds collide when 3d printers reach the public: Modeling a digital gun control law after the digital millenium copyright act, Mich. St. L. Rev. 187 (2014) 187–225.

[44] J. J. Johnson, Print, lock, and load: 3-d printers, creation of guns, and the potential threat to fourth amendment rights, Journal of Law, Technology and Policy 2013 (2) (2013) 337–361.

[45] A. Catalán Flores, et al., Click, print, fire: 3d weapons and the arms trade treaty (2016).

[46] NDIA, Cybersecurity for Advanced Manufacturing (2014).

[47] D. M. Nicol, W. H. Sanders, K. S. Trivedi, Model-based evaluation: from dependability to security, IEEE Transactions on dependable and secure computing 1 (1) (2004) 48–65.

[48] G. P. Malafsky, B. Newman, Organizing knowledge with ontologies and taxonomies, Fairfax: TechI LLC. Available at.

[49] S. Hansman, R. Hunt, A taxonomy of network and computer attacks, Computers & Security 24 (1) (2005) 31–43.

[50] N. Abrek, Attack taxonomies and ontologies, Network 1 (2015) 10.

[51] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, C. Williams, Taxonomies for reasoning about cyber-physical attacks in iot-based manufacturing systems, International Journal of Interactive Multimedia and Artificial Inteligence 4 (Special Issue on Advances and Applications in the Internet of Things and Cloud Computing).

[52] M. Wu, Y. B. Moon, Taxonomy of cross-domain attacks on cybermanufacturing system, Procedia Computer Science 114 (2017) 367–374.

[53] N. Gupta, F. Chen, N. G. Tsoutsos, M. Maniatakos, Obfuscade: Obfuscating additive manufacturing cad models against counterfeiting, in: Design Automation Conference (DAC), 2017 54th ACM/EDAC/IEEE, IEEE, 2017, pp. 1–6.

[54] A. Brown, M. Yampolskiy, J. Gatlin, T. Andel, Legal aspects of protecting intellectual property in additive manufacturing, in: Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers 10, Springer, 2016, pp. 63–79.

[55] O. Rehme, C. Emmelmann, Cellular design for laser freeform fabrication, Cuvillier Göttingen Verlag, Göttingen, Germany, 2010.

[56] W. E. Frazier, Metal additive manufacturing: a review, Journal of Materials Engineering and Performance 23 (6) (2014) 1917–1928.

[57] T. Krol, M. Zäh, C. Seidel, Optimization of supports in metal-based additive manufacturing by means of finite element models, in: 23rd Annual International Solid Freeform Fabrication Symposium - An Additive Manufacturing Conference, SFF 2012, 2012, pp. 707–718.

[58] G. Ameta, P. Witherell, S. Moylan, R. Lipman, Tolerance specification and related issues for additively manufactured products, in: ASME 2015 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, American Society of Mechanical Engineers, 2015, pp. V01AT02A027–V01AT02A027.

[59] A. Tarantola, DARPA to develop best practices for 3D printing, http://www.engadget.com/2015/05/31/darpa-to-develop-best-practices-for-3d-printing/ (2015).

[60] M. Maher, Open manufacturing, http://www.darpa.mil/program/open-manufacturing (2015).

[61] H. Atkinson, S. Davies, Fundamental aspects of hot isostatic pressing: an overview, Metallurgical and Materials Transactions A 31 (12) (2000) 2981–3000.

[62] K. S. Chan, M. Koike, R. L. Mason, T. Okabe, Fatigue life of titanium alloys fabricated by additive layer manufacturing techniques for dental implants, Metallurgical and Materials Transactions A 44 (2) (2013) 1010–1022.

[63] A. Gebhardt, Understanding additive manufacturing: rapid prototyping-rapid tooling-rapid manufacturing, Carl Hanser Verlag GmbH Co KG, Munich, Germany, 2012.

[64] E. Sachs, E. Wylonis, S. Allen, M. Cima, H. Guo, Production of injection molding tooling with conformal cooling channels using the three dimensional printing process, Polymer Engineering & Science 40 (5) (2000) 1232–1247.

[65] ESET, ACAD/Medre.A – 10000's of AutoCAD Designs Leaked in Suspected Industrial Espionage, white paper (2012).
URL `https://www.welivesecurity.com/media_files/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf`

[66] M. Weinberg, It will be awesome if they don't screw it up (2010).

[67] T. Campbell, C. Williams, O. Ivanova, B. Garrett, Could 3d printing change the world (2011).

[68] B. Depoorter, Intellectual property infringements & 3d printing: Decentralized piracy, Hastings LJ 65 (2013) 1483.

[69] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, W. Xu, My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3d printers, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York, NY, USA, 2016, pp. 895–907.

[70] A. Hojjati, A. Adhikari, K. Struckmann, E. Chou, T. N. Tho Nguyen, K. Madan, M. S. Winslett, C. A. Gunter, W. P. King, Leave your phone at the door: Side channels that reveal factory floor secrets, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York, NY, USA, 2016, pp. 883–894.

[71] Creaform, Portable Coordinate Measuring Machine (CMM): Handyprobe, http://www.creaform3d.com/en/metrology-solutions/coordinate-measuring-machines-handyprobe?gclid=CJWL6s65oMUCFZTLtAodVTsAGw, [Online; accessed 21-April-2017] (2016).

[72] T. Rayna, L. Striukova, From rapid prototyping to home fabrication: How 3d printing is changing business model innovation, Technological Forecasting and Social Change 102 (2016) 214–224.

[73] BIG THINK Editors, Will 3D Printing Spark a Home Manufacturing Revolution?, http://bigthink.com/articles/will-3d-printing-spark-a-home-manufacturing-revolution, [Online; accessed 30-Mai-2016] (2015).

[74] T. R. Holbrook, L. Osborn, Digital patent infringement in an era of 3d printing, UC Davis Law Review 48 (2015) 1319–1385.

[75] T. Y. Ebrahim, 3d printing: Digital infringement & digital regulation, Nw. J. Tech. & Intell. Prop. 14 (2016) 37.

[76] I. Gibson, D. W. Rosen, B. Stucker, et al., Additive manufacturing technologies, Vol. 238, Springer, New York City, 2010.

[77] The world's first 3D electronics printer, http://www.voxel8.co/ (2015). URL http://www.voxel8.co/

[78] A. Rida, L. Yang, R. Vyas, M. M. Tentzeris, Conductive inkjet-printed antennas on flexible low-cost paper-based substrates for rfid and wsn applications, IEEE Antennas and Propagation Magazine 51 (3).

[79] P. Nayeri, M. Liang, R. A. Sabory-Garcı, M. Tuo, F. Yang, M. Gehm, H. Xin, A. Z. Elsherbeni, et al., 3d printed dielectric reflectarrays: low-cost high-gain antennas at sub-millimeter waves, IEEE Transactions on Antennas and Propagation 62 (4) (2014) 2000–2008.

[80] N. Falliere, L. O. Murchu, E. Chien, W32. stuxnet dossier, White paper, Symantec Corp., Security Response 5 (2011) 6.

[81] M. Swearingen, S. Brunasso, J. Weiss, D. Huber, What you need to know (and don't) about the aurora vulnerability, http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/ (2013).

[82] A. A. Cardenas, S. Amin, S. Sastry, Secure control: Towards survivable cyber-physical systems, System 1 (a2) (2008) a3.

[83] E. A. Lee, Cyber physical systems: Design challenges, in: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), IEEE, 2008, pp. 363–369.

[84] G. Pope, M. Yampolskiy, A Hazard Analysis Technique for Additive Manufacturing, in: Better Software East Conference, 2016, p. 17. URL http://arxiv.org/abs/1706.00497

[85] OSHA Regional News Release, After explosion, US Department of Labor's OSHA cites 3-D printing firm for exposing workers to combustible metal powder, electrical hazards Powderpart Inc. faces $64,400 in penalties (May 2014).

[86] OSHA, OSHA FactSheet (2014).

[87] S. R. Chhetri, A. Canedo, M. A. Al Faruque, Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems, in: Computer-Aided Design (ICCAD), 2016 IEEE/ACM International Conference on, IEEE, 2016, pp. 1–8.

[88] I. Yadroitsau, Selective laser melting: Direct manufacturing of 3D-objects by selective laser melting of metal powders, Lambert Academic Publishing, Saarbrücken, Germany, 2009.

[89] W. E. King, H. D. Barth, V. M. Castillo, G. F. Gallegos, J. W. Gibbs, D. E. Hahn, C. Kamath, A. M. Rubenchik, Observation of keyhole-mode laser melting in laser powder-bed fusion additive manufacturing, Journal of Materials Processing Technology 214 (12) (2014) 2915–2925.

[90] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, Y. Elovici, 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, ACM, New York, NY, USA, 2017, pp. 78:1–78:10.

[91] Xiao Zi Hang (Claud Xiao), Security attack to 3d printing, keynote at XCon2013 (2013).
URL `http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf`

[92] S. B. Moore, W. B. Glisson, M. Yampolskiy, Implications of malicious 3d printer firmware, in: Proceedings of the 50th Hawaii International Conference on System Sciences, IEEE, 2017, pp. 6089–6098.

[93] S. R. Chhetri, N. Rashid, S. Faezi, M. A. Al Faruque, Security trends and advances in manufacturing systems in the era of industry 4.0, in: IEEE/ACM international conference on computer aided design, 2017.

[94] S. R. Chhetri, S. Faezi, N. Rashid, M. A. Al Faruque, Manufacturing supply chain and product lifecycle security in the era of industry 4.0, Journal of Hardware and Systems Security (2017) 1–18.

[95] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, C. Sporleder, Acoustic side-channel attacks on printers., in: USENIX Security Symposium, USENIX Association, 2010, pp. 307–322.

[96] Q. Do, B. Martini, K.-K. R. Choo, A data exfiltration and remote exploitation attack on consumer 3d printers, IEEE Transactions on Information Forensics and Security 11 (10) (2016) 2174–2186.

[97] M. A. Al Faruque, S. R. Chhetri, A. Canedo, J. Wan, Forensics of thermal side-channel in additive manufacturing systems, Tech. rep., Tech. Rep., 2016.[Online]. Available: http://cecs. uci. edu/files/2016/01/CECS-TR-01-16. pdf (2016).

[98] F. Chen, G. Mac, N. Gupta, Security features embedded in computer aided design (cad) solid models for additive manufacturing, Materials & Design 128 (2017) 182–194.

[99] K. Wang, G. Lavoué, F. Denis, A. Baskurt, A comprehensive survey on three-dimensional mesh watermarking, IEEE Transactions on Multimedia 10 (8) (2008) 1513–1527.

[100] A. Dachowicz, S. C. Chaduvula, M. Atallah, J. H. Panchal, Microstructure-based counterfeit detection in metal part manufacturing, JOM 69 (11) (2017) 2390–2396.

[101] Z. C. Kennedy, D. E. Stephenson, J. Christ, T. R. Pope, B. Arey, C. A. Barrett, M. G. Warner, Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology, Journal of Materials Chemistry C 5 (2017) 9570–9578.

[102] J.-U. Hou, D.-G. Kim, S. Choi, H.-K. Lee, 3d print-scan resilient watermarking using a histogram-based circular shift coding structure, in: Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, ACM, New York, NY, USA, 2015, pp. 115–121.

[103] J.-U. Hou, D.-G. Kim, H.-K. Lee, Blind 3d mesh watermarking for 3d printed model by analyzing layering artifact, IEEE Transactions on Information Forensics and Security.

[104] N. Gupta, F. Chen, K. Shahin, Design features to address security challenges in additive manufacturing, in: Advances in Manufacturing Techniques for Materials: Engineering and Engineered, Taylor and Francis, 2017.

[105] S. R. Chhetri, S. Faezi, M. A. Al Faruque, Fix the leak! an information leakage aware secured cyber-physical manufacturing system, in: 2017 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2017, pp. 1408–1413.

[106] N. F. Fadhel, R. M. Crowder, F. Akeel, G. B. Wills, Component for 3d printing provenance framework: Security properties components for provenance framework, in: Internet Security (WorldCIS), 2014 World Congress on, IEEE, 2014, pp. 91–96.

[107] N. F. Fadhel, R. M. Crowder, G. B. Wills, Maintaining provenance throughout the additive manufacturing process, International Journal for Information Security Research (IJISR) 3 (3) (2013) 466–475.

[108] N. F. Fadhel, R. M. Crowder, G. B. Wills, Approaches to maintaining provenance throughout the additive manufacturing process, in: Internet Security (WorldCIS), 2013 World Congress on, IEEE, 2013, pp. 82–87.

[109] N. F. Fadhel, R. M. Crowder, G. B. Wills, Provenance in the additive manufacturing process, IFAC-PapersOnLine 48 (3) (2015) 2345–2350.

[110] B. Macq, P. R. Alface, M. Montanola, Applicability of watermarking for intellectual property rights protection in a 3d printing scenario, in: Proceedings of the 20th International Conference on 3D Web Technology, ACM, New York, NY, USA, 2015, pp. 89–95.

[111] M. Holland, C. Nigischer, J. Stjepandić, Copyright protection in additive manufacturing with blockchain approach, Transdisciplinary Engineering: A Paradigm Shift 5 (2017) 914–921.

[112] F. Baumann, T. Ludwig, N. Abele, S. Hoffmann, D. Roller, Model-data streaming for additive manufacturing securing intellectual property, Smart Sustain. Manuf. Syst 1 (2017) 142–152.

[113] S. Ghosh, D. M. Dimiduk, Computational methods for microstructure-property relationships, Springer, 2011.

[114] J.-W. Cho, R. Prost, H.-Y. Jung, An oblivious watermarking for 3-d polygonal meshes using distribution of vertex norms, IEEE Transactions on Signal Processing 55 (1) (2007) 142–155.

[115] S. Craig, Protection for printing: An analysis of copyright protection for 3d printing, U. Ill. L. Rev. (2017) 307.

[116] P. Reddy, The legal dimension of 3d printing: Analyzing secondary liability in additive layer manufacture, Colum. Sci. & Tech. L. Rev. 16 (2014) 222.

[117] U. Congress, Digital millennium copyright act, Public Law 105 (304) (1998) 112.

[118] J. L. Tran, The law and 3d printing, J. Marshall J. Computer & Info. L. 31 (2015) 505–657.

[119] S. Moore, P. Armstrong, T. McDonald, M. Yampolskiy, Vulnerability analysis of desktop 3d printer software, in: Resilience Week (RWS), 2016, IEEE, 2016, pp. 46–51.

[120] D. Glavach, J. LaSalle-DeSantis, S. Zimmerman, Applying and assessing cybersecurity controls for direct digital manufacturing (ddm) systems, in: Cybersecurity for Industry 4.0, Springer, 2017, pp. 173–194.

[121] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, R. Parker, Bad parts: Are our manufacturing systems at risk of silent cyberattacks?, IEEE Security & Privacy 13 (3) (2015) 40–47.

[122] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, R. Parker, 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.

[123] A. Ilie, H. Ali, K. Mumtaz, In-built customised mechanical failure of 316l components fabricated using selective laser melting, Technologies 5 (1) (2017) 9.

[124] S. Belikovetsky, M. Yampolskiy, J. Toh, Y. Elovici, Youtube video: dr0wned - am cyber attack (2016).
URL www.youtube.com/watch?v=zUnSpT6jSys

[125] C. Yap, C. Chua, Z. Dong, Z. Liu, D. Zhang, L. Loh, S. Sing, Review of selective laser melting: Materials and applications, Applied physics reviews 2 (4) (2015) 041101.

[126] N. Leveson, J. Thomas, An STPA primer, MIT Press, 2013.
URL http://psas.scripts.mit.edu/home/wp-content/uploads/2015/06/STPA-Primer-v1.pdf

[127] ASTM International, Standard Test Method for Tensile Properties of Plastics, Active standard astm d638-10, ASTM International, West Conshohocken, PA (2010).

[128] Xiao Zi Hang (Claud Xiao), Three demos of attacking arduino and reprap 3d printers, code to Keynote at XCon2013 (2013).
URL https://github.com/secmobi/attack-arduino-and-reprap

[129] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, A. Yasinsac, Towards security of additive layer manufacturing (2014).
URL https://arxiv.org/ftp/arxiv/papers/1602/1602.07536.pdf

[130] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, Y. Elovici, Detecting cyber-physical attacks in additive manufacturing using digital audio signing (2017).

[131] M. Albakri, L. Sturm, C. B. Williams, P. Tarazaga, Non-destructive evaluation of additively manufactured parts via impedance-based monitoring, in: Proceedings of the 25th Annual International Solid Freeform Fabrication Symposium An Additive Manufacturing Conference, 2015, pp. 1475–1490.

[132] L. Sturm, M. Albakri, C. B. Williams, P. Tarazaga, In-situ detection of build defects in additive manufacturing via impedance-based monitoring, in: Proceedings of the 26th Annual International Solid Freeform Fabrication Symposium An Additive Manufacturing Conference, 2016, pp. 1458–1478.

[133] J. Straub, Physical security and cyber security issues and human error prevention for 3d printed objects: detecting the use of an incorrect printing material, in: SPIE Commercial+ Scientific Sensing and Imaging, International Society for Optics and Photonics, 2017, pp. 102200K–102200K.

[134] J. Straub, A combined system for 3d printing cybersecurity, in: SPIE Commercial+ Scientific Sensing and Imaging, International Society for Optics and Photonics, 2017, pp. 102200N–102200N.

[135] J. Straub, Identifying positioning-based attacks against 3d printed objects and the 3d printing process, in: SPIE Defense+ Security, International Society for Optics and Photonics, 2017, pp. 1020304–1020304.

[136] J. Straub, An approach to detecting deliberately introduced defects and micro-defects in 3d printed objects, in: SPIE Defense+ Security, International Society for Optics and Photonics, 2017, pp. 102030L–102030L.

[137] M. Wu, Z. Song, Y. B. Moon, Detecting cyber-physical attacks in cybermanufacturing systems with machine learning methods, Journal of Intelligent Manufacturing (2017) 1–13.

[138] M. Wu, H. Zhou, L. L. Lin, B. Silva, Z. Song, J. Cheung, Y. Moon, Detecting attacks in cybermanufacturing systems: additive manufacturing example, in: MATEC Web of Conferences, Vol. 108, EDP Sciences, 2017, p. 06005.

[139] C. Bayens, T. Le, L. Garcia, R. Beyah, M. Javanmard, S. Zonouz, See no evil, hear no evil, feel no evil, print no evil? malicious fill patterns detection in additive manufacturing, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC, 2017, pp. 1181–1198.
URL `https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/bayens`

[140] N. G. Tsoutsos, H. Gamil, M. Maniatakos, Secure 3d printing: Reconstructing and validating solid geometries using toolpath reverse engineering, in: Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, ACM, New York, NY, USA, 2017, pp. 15–20.

[141] Z. DeSmit, A. E. Elhabashy, L. J. Wells, J. A. Camelio, Cyber-physical vulnerability assessment in manufacturing systems, Procedia Manufacturing 5 (2016) 1060–1074.

[142] Z. DeSmit, A. E. Elhabashy, L. J. Wells, J. A. Camelio, An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems, Journal of Manufacturing Systems 43 (2017) 339–351.

[143] H. Vincent, L. Wells, P. Tarazaga, J. Camelio, Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems, Procedia Manufacturing 1 (2015) 77–85.

[144] S. R. Chhetri, J. Wan, M. A. Al Faruque, Cross-domain security of cyber-physical systems, in: Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific, IEEE, 2017, pp. 200–205.

[145] R. J. Hocken, P. H. Pereira, Coordinate measuring machines and systems, CRC Press, 2016.

[146] R. J. Valkenburg, A. M. McIvor, Accurate 3d measurement using a structured light system, Image and Vision Computing 16 (2) (1998) 99–110.

[147] B. Auld, J. Moulder, Review of advances in quantitative eddy current nondestructive evaluation, Journal of Nondestructive evaluation 18 (1) (1999) 3–36.

[148] J. Krautkrämer, H. Krautkrämer, Ultrasonic testing of materials, Springer Science & Business Media, 2013.

[149] C. Hellier, Handbook of nondestructive evaluation, McGraw-Hill, 2001.

[150] R. Hanke, T. Fuchs, N. Uhlmann, X-ray based methods for non-destructive testing and material characterization, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment 591 (1) (2008) 14–18.

[151] National Institute of Standards and Technology (NIST), Measurement science roadmap for metal-based additive manufacturing, Tech. rep., NIST (2013).

[152] J. M. Waller, B. H. Parker, K. L. Hodges, E. R. Burke, J. L. Walker, Non-destructive evaluation of additive manufacturing state-of-the-discipline report, Nasa/tm2014218560, NASA, Hampton, VA (2014).
URL https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140016447.pdf

[153] G. Park, H. H. Cudney, D. J. Inman, Impedance-based health monitoring of civil structural components, Journal of infrastructure systems 6 (4) (2000) 153–160.

[154] StrataSys, Verowhiteplus polyjet technology material specifications (2015).
URL https://www.stratasysdirect.com/wp-content/themes/stratasysdirect/files/material-datasheets/polyjet/PolyJet_VeroWhitePlus_Material_Specifications.pdf

[155] StrataSys, Objet350 and objet500 connex3 (2016).
URL http://global72.stratasys.com/~/media/Main/Files/Machine_Spec_Sheets/PSS_PJ_Connex3.ashx

[156] Renishaw, inVia confocal Raman microscope, http://www.renishaw.com/en/invia-confocal-raman-microscope–6260 (2017).

[157] S. Wold, K. Esbensen, P. Geladi, Principal component analysis, Chemometrics and intelligent laboratory systems 2 (1-3) (1987) 37–52.

[158] National Institute of Standards and Technology (NIST), Framework for improving critical infrastructure cybersecurity, Tech. rep., NIST (2014). URL https://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf

[159] J. Straub, Initial work on the characterization of additive manufacturing (3d printing) using software image analysis, Machines 3 (2) (2015) 55–71.

[160] B. A. Szabo, I. BabuÂška, Finite element analysis, John Wiley & Sons, Hoboken, NJ, 1991.

[161] G. Hodgson, A. Ranellucci, J. Moe, Slic3r manual (2015). URL http://manual.slic3r.org/expert-mode/infill

[162] N. D. Berkowitz, Strict liability for individuals-the impact of 3-d printing on products liability law, Wash. UL Rev. 92 (2014) 1019.

[163] P. J. Comerford, E. P. Belt, 3dp, am, 3ds and product liability, Santa Clara L. Rev. 55 (2015) 821.

[164] E. M. Malloy, Three-dimensional printing and a laissez-faire attitude toward the evolution of the products liability doctrine, Fla. L. Rev. 68 (2016) 1199.

[165] S. Wang, When classical doctrines of products liability encounter 3d printing: New challenges in the new landscape, Hous. Bus. & Tax LJ 16 (2016) 104.

[166] T. DebRoy, H. Wei, J. Zuback, T. Mukherjee, J. Elmer, J. Milewski, A. Beese, A. Wilson-Heid, A. De, W. Zhang, Additive manufacturing of metallic components–process, structure and properties, Progress in Materials Sciencedoi:https://doi.org/10.1016/j.pmatsci.2017.10.001.