Evaluation of additive and subtractive manufacturing from the security perspective

Mark Yampolskiy, Wayne King, Gregory Pope, Sofia Belikovetsky, Yuval Elovici

Chapter 2

EVALUATION OF ADDITIVE AND SUBTRACTIVE MANUFACTURING FROM THE SECURITY PERSPECTIVE

Mark Yampolskiy, Wayne King, Gregory Pope, Sofia Belikovetsky and Yuval Elovici

Abstract Additive manufacturing involves a new class of cyber-physical systems that manufacture 3D objects incrementally by depositing and fusing together thin layers of source material. In 2015, the global additive manufacturing industry had $5.165 billion in revenue, with 32.5% of all manufactured objects used as functional parts. Because of their reliance on computerization, additive manufacturing devices (or 3D printers) are susceptible to a broad range of attacks. The rapid adoption of additive manufacturing in aerospace, automotive and other industries makes it an attractive attack target and a critical asset to be protected.

This chapter compares emerging additive manufacturing and traditional subtractive manufacturing from the security perspective. While the discussion compares the two manufacturing technologies, the emphasis is on additive manufacturing due to its expected dominance as the manufacturing technology of the future. The chapter outlines the additive and subtractive manufacturing workflows, proposes a framework for analyzing attacks on or using additive manufacturing systems and presents the major threat categories. In order to compare the two manufacturing paradigms from the security perspective, the differences between the two workflows are identified and the attack analysis framework is applied to demonstrate how the differences translate into threats. The analysis reveals that, while there is significant overlap with regard to security, fundamental differences in the two manufacturing paradigms require a separate investigation of additive manufacturing security.

Keywords: Additive manufacturing, subtractive manufacturing, attack framework

1. Introduction

The U.S. Department of Homeland Security has designated manufacturing as one of the sixteen critical infrastructure sectors [40]. The critical infrastructure sectors are not isolated, but are entangled in a complex web of dependencies and interdependencies [32]. A large-scale critical infrastructure disruption poses technical as well as economic, geopolitical, environmental and societal risks [17]. As a result, maintaining the security of manufacturing systems is of paramount importance.

Since the introduction of computer numeric control (CNC) machines in the 1940s, manufacturing processes have become increasingly computerized. Computer numeric control machines enable software control of cutting tools – they reduce a solid block of source material to a desired shape in a process commonly referred to as subtractive manufacturing (SM). In the 1980s, additive manufacturing (AM) was introduced – it is an alternative process in which thin layers of source material are deposited and fused together to form a 3D object. Additive manufacturing machines are often referred to as 3D printers. Subtractive and additive manufacturing machines, which are examples of cyber-physical systems (CPSs), are employed in computer-aided manufacturing (CAM), a process in which manufacturing as well as source material loading and physical transportation are computerized.

Subtractive manufacturing has dominated the manufacturing industry for decades and, until recently, additive manufacturing was predominantly used to produce low-quality plastic parts. However, additive manufacturing technologies have now matured to produce high-quality plastic and metal 3D-printed objects that are usable as functional parts, even in safety-critical systems such as jet engines. Additive manufacturing with other source materials, including ceramics, glass and composites, is rapidly approaching the maturity needed for industrial applications.

According to the 2015 Wohlers Report [41], the additive manufacturing industry had \$5.165 billion in revenue with 32.5% of all manufactured objects used as functional parts. An Ernst & Young study [30] reports that additive manufacturing technologies are being rapidly adopted around the world. In the United States, 16% of the surveyed companies had experience with additive manufacturing and another 16% were considering adopting the technology. The current world leader in additive manufacturing adoption is Germany with 37% of the surveyed companies already employing additive manufacturing and another 12% considering the technology. Numerous studies indicate that the adoption of additive manufacturing will continue to rise, potentially leading to its dominance as the manufacturing technology of the future.

The growing importance of additive manufacturing and its reliance on computerization have led several researchers to voice security concerns [2, 9, 39, 44, 45, 48–50]. However, it is not clear whether and how additive manufacturing security differs from the security of other cyber-physical systems, especially as traditional subtractive manufacturing serves the same purpose and employs similar processes and computerized components. This chapter attempts to an-

swer these questions and identify the similarities and differences between additive and subtractive manufacturing technologies from the security perspective, but the emphasis remains on additive manufacturing.

2. Related Work

Additive and subtractive manufacturing systems are both cyber-physical systems. Therefore, the fundamental aspects of cyber-physical system attacks are applicable to both types of systems. Industrial control systems are also computer-controlled systems, but their mission and implementation differ significantly from additive and subtractive manufacturing systems.

No information is available about attacks that have specifically targeted subtractive manufacturing systems. However, there is a growing body of literature on potential attacks on or using additive manufacturing systems. Therefore, this topic is discussed in this section.

2.1 Cyber-Physical System Security

Cyber-physical systems generally employ closed or open control loops. A closed-loop system directly uses feedback information from sensors for decision making while an open-loop system makes decisions based on a model of a controlled physical process or the input of a human operator who makes decisions based on sensor readings. In a control system, information from sensors is fed to a computing unit that chooses the necessary actions; the signals from the computing unit are sent to actuators. As discussed in [10], a cyber-physical system can be attacked by interrupting one of these communications links or by injecting incorrect sensor information or control commands. Of course, cyber-physical systems may also be attacked by compromising their computing units.

Many cyber-physical systems operate under tight real-time constraints [24]. This is especially the case with safety-critical systems such as automobiles and airplanes. In these systems, disrupting the timing can significantly impact system behavior, even when all the commands and sensor information are correct.

Manipulations performed on cyber-physical systems and the effects of the manipulations are not necessarily in the same domain [46, 47]. While most cyber-physical system attacks focus on manipulations in the cyber domain that lead to effects in the physical domain, this does not have to be the case. Manipulations in the physical domain can cause effects in the physical and/or cyber domains.

Stuxnet is the most famous example of attacks on a production cyber-physical system [15]. The attacks were performed by malware installed on programmable logic controllers that managed centrifuges at a uranium enrichment facility in Natanz, Iran. When activated, the malware caused the centrifuges to rotate at speeds much higher and much lower than the normal operational speed. The attacks reportedly damaged more than 1,000 centrifuges at the uranium enrichment facility.

2.2 Additive Manufacturing Security

Several researchers have analyzed 3D printers and 3D printing processes for vulnerabilities. Networking and communications systems have been found to lack integrity checks when receiving design files [39]. Furthermore, communications protocols employed by desktop 3D printers can be exploited, enabling the retrieval of current and previously-printed 3D models, the termination of active printing jobs and the submission of unauthorized (new) jobs [13]. Software and firmware commonly used in desktop 3D printers contain numerous vulnerabilities [28]. A phishing attack can be used to install a backdoor that enables arbitrary, targeted manipulations of design files by a remote adversary [6]. Malicious software installed on a computer can be used to automate manipulations of design files [35]. Firmware installed on a 3D printer can be malicious [29] or compromised [42], enabling a range of manipulations of the manufacturing process. A range of physical attacks are also possible; manipulations of source materials can have far-reaching impacts on manufactured objects as well as on 3D printers and their manufacturing environments [48].

One of the broadly discussed topics in additive manufacturing security is the impact on intellectual property. Numerous problems have been identified by researchers who have analyzed the legal aspects of intellectual property protection in additive manufacturing environments [9, 20, 38] . For example, a 3D scan of a manufactured object is not considered to be an original technical drawing (blueprint) and, therefore, does not have the same legal protections [9]; thus, it can be used to circumvent copyright protection.

On the technical side, several attack schemes have been discussed and partially evaluated. In a scenario where additive manufacturing is outsourced, a malicious actor can assume the role of a manufacturing service provider and gain unrestricted access to design files and related specifications [44]. Side-channel emanations can be recorded and analyzed in order to steal designs, even when a 3D printer is air-gapped. Analyses of the acoustic emanations of desktop 3D printers have enabled the reconstruction of the geometries of printed objects [2, 33]. Researchers have also demonstrated that similar attacks are possible using infrared imaging [3] and magnetic side channel analysis [19].

It is important to note that, in the context of additive manufacturing, intellectual property is not limited to the specifications of the 3D object geometry – it can also include the specifications of the properties of the manufactured object and the manufacturing process parameters that ensure the fulfillment of the physical requirements [44]. Physical watermarking techniques have been discussed as a means to protect intellectual property in additive manufacturing environments [26].

Another broadly discussed threat category is the ability to inflict physical damage, especially when the quality of a manufactured part is sabotaged. Part quality can be degraded by introducing defects such as voids (internal cavities) [35] or printing portions of objects with the wrong or contaminated materials [50]. The sizes of the defects and their geometries and locations define the extent of manufactured part degradation [6].

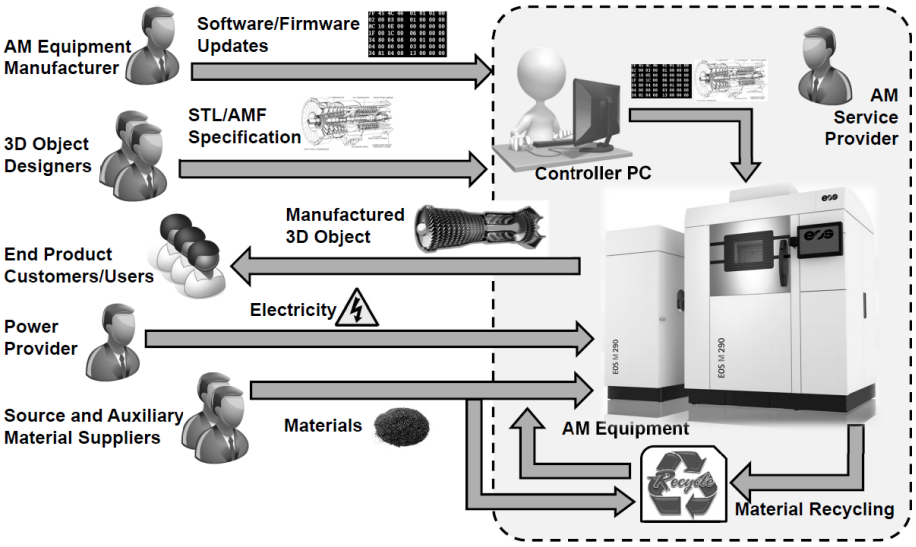

Figure 1. Additive manufacturing workflow.

Other manipulations involve changing the orientation of a printed part [48, 50], introducing additional skew along one of the built axes [12], changing the thickness of layers [29] and varying manufacturing parameters such as the energy of the heat source and scanning strategy in the case of the powder bed fusion process [48]. Manipulations of network command timing [31], energy supply [31] and source material composition [48] have also been identified as potential means of sabotaging parts. Indeed, in the case of additive manufacturing of metal parts, manipulations of manufacturing parameters can damage the additive manufacturing machinery itself and even contaminate the manufacturing environment [48, 49]. Researchers have proposed game theory [43] and side-channel emanation monitoring [12] as approaches for combating sabotage in additive manufacturing environments.

3. Manufacturing Workflows

This section describes the additive and subtractive manufacturing workflows.

3.1 Additive Manufacturing Workflow

Figure 1 presents an additive manufacturing workflow. This workflow is increasingly common when additive manufacturing is offered as a service. As of January 2017, the 3D Printing Businesses Directory lists 892 companies as offering 3D printing services (`3dprintingbusiness.directory`).

Additive manufacturing equipment (which includes but is not limited to 3D printers) is usually developed and provided by an original equipment manufacturer (OEM). In 2015, 62 system manufacturers in 20 countries produced and

sold industrial-grade additive manufacturing equipment and hundreds of small companies offered desktop 3D printers [41]. Firmware and software updates for additive manufacturing equipment and controller workstations that extend functionality and fix bugs are provided by third-party companies. Open-source software is also commonly used by desktop 3D printers. Various mechanical, electrical and electronic components (motors, filters, etc.) are required for replacement purposes; these are sold by original equipment manufacturers or third-party companies and shipped directly to customers.

3D object blueprints are provided in the stereolithography [18] (STL) format, additive manufacturing file (AMF) format [4, 25] or 3D manufacturing format (3MF) [1], each of which specifies the computer-aided design (CAD) model of the 3D object to be manufactured. Object blueprints specified in STL/AMF/3MF files are often provided by external 3D object designers directly to additive manufacturing service providers. Another scenario involves a design being provided by the end-product customer who created the design (common for enterprise customers) or purchased it from a designer (common for individual customers).

At the additive manufacturing service provider's facility, an STL/AMF/3MF file can be directly transferred to a 3D printer (via a computer network or USB stick) or interpreted by the controller workstation. In the latter case, the workstation sends the 3D printer individual control commands (often in G-code [14], a language commonly used in computer-aided manufacturing) or as a tool path file containing a sequence of (often proprietary, 3D printer-specific) commands [35].

Additive manufacturing requires electricity and a variety of source and auxiliary materials. While source materials are included in the end-product, auxiliary materials support or enable production in some way. For example, support material structures enable the printing of complex geometries and inert gas (e.g., argon) is often employed when a laser is the heat source. Source materials for plastic printers are usually supplied by original equipment manufacturers; the source material market for metal printers is more open [41].

Depending on the additive manufacturing process, source material and part geometry, the production workflow can include several post-processing steps (not shown in Figure 1). The removal of support structures is a common step in the case of plastic objects; metal parts require hot isostatic pressing, finish machining and surface finishing. For functional parts, non-destructive testing is usually the final step. The Wohlers Report [41] lists several non-destructive testing methods commonly used in traditional subtractive manufacturing that are inadequate to validate the quality of additively-manufactured parts; these include fluorescent penetrant inspection (FPI), radiographic inspection and computed tomography (CT). Also, the inability to detect small defects in additively-manufactured parts using an ultrasonic c-scan has been reported [50]. After all the required production and post-production steps are completed, the manufactured objects are delivered to customers via physical carriers.

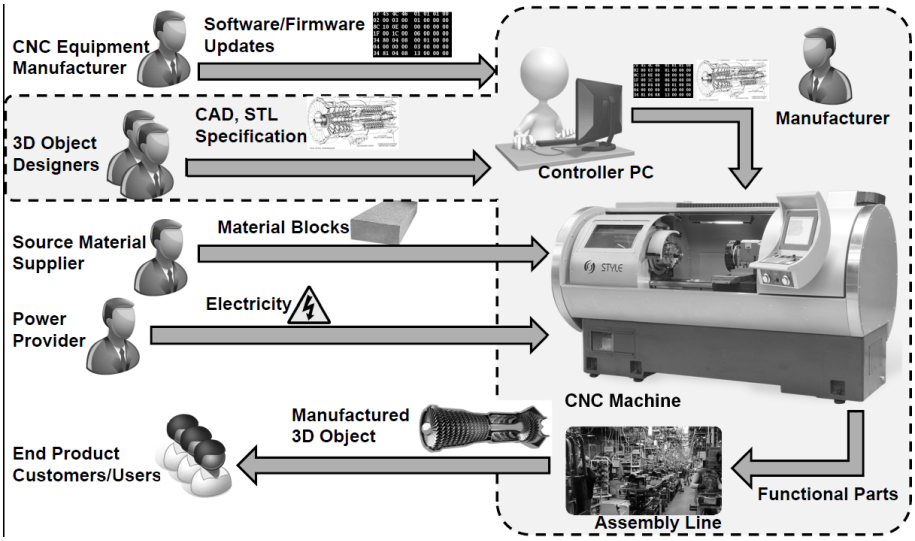

Figure 2. Subtractive manufacturing workflow.

In order to reduce the environmental impact and manufacturing costs, some of the source materials that remain after an additive manufacturing process may be recycled. This is especially true for power bed fusion in which thin layers of powdered source material (usually metal or polymer) are distributed in a bed and fused by a heat source (laser or electron beam). The exposure of unused powder to high temperatures causes the properties of particles to change (in the case of plastic) and/or the particles to agglomerate into large clusters. Both these changes can have negative impacts on the final product quality. Therefore, the remaining powder is often sieved and mixed with "virgin" powder in proportions that minimize the negative impact on part quality.

Table 1 summarizes the main aspects of additive and subtractive manufacturing and compares their workflows.

3.2 Subtractive Manufacturing Workflow

The subtractive manufacturing workflow presented in Figure 2 is broadly similar to the additive manufacturing workflow, but some notable differences exist. While a subtractive manufacturing facility may provide manufacturing services to external customers, it is significantly less common than in the case of additive manufacturing. Instead, a subtractive manufacturing provider typically supplies complete products as a commodity and the part designers are usually located "in house."

As with additive manufacturing, software and firmware updates and manufacturing jobs are initiated from a workstation. However, unlike additive manufacturing, software and firmware updates are usually provided by origi-

Table 1. Comparison of additive and subtractive manufacturing.

	Additive Manufacturing	**Subtractive Manufacturing**
Actors		
Software Provider	• OEMs and commercial software developers	
	• Open-source/community	• –
3D Object Designer	• Increasingly individuals • External to enterprise	• Predominantly enterprises • Internal to enterprise
Customer Relationship	• Increasingly short term • Low volume	• Long term • High volume
Actors/Roles	• High	• Low
Materials		
Source	• Often wire or powder	• Solid blocks
Auxiliary	• Extensively used • Influence product quality	• Barely used/relevant • –
Manufacturing Process		
G-Code Command Defines	• Deposited/fused material • Exterior/interior geometry • Object physical properties	• Material to be removed • Exterior geometry • –
Power Outage	• Impacts manufacturing speed	
	• Impacts part quality	• –
Timing	• Impacts manufacturing speed	
	• Impacts part quality	• –
Maturity Level		
Workflows	• Mature and well-established (manual and CAM)	
Software and Firmware	• New and immature with many bugs	• Very mature with few bugs
Quality Control	• SM tools/approaches conditionally applicable • Immature tools/approaches	• Tools/approaches well-established and understood • Mature tools/approaches
Availability/Accessibility		
Equipment	• Enterprises/employees	
	• Private individuals	• –
Blueprints	• Restricted access (enterprise-guarded intellectual property)	
	• Third-party commercial and non-commercial websites	• –

nal equipment manufacturers or commercial software developers; community involvement in open-source efforts are negligible. Furthermore, control com-

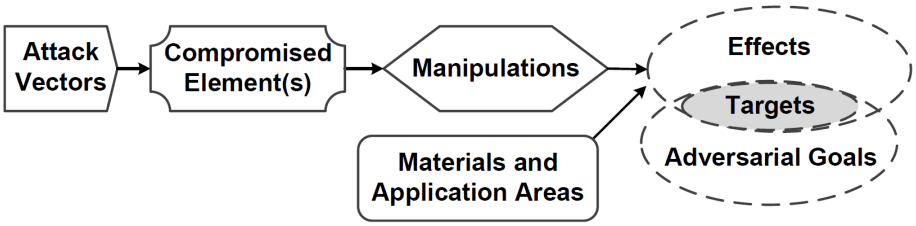

Figure 3. Attacks on or using computer-aided manufacturing (based on [49]).

mands (in G-code) sent from a controller workstation to a computer numeric control machine define the movements of tools that remove the extraneous material to create an object.

The source material used in subtractive manufacturing also differs. In additive manufacturing, the source material is usually in wire or powder form; in the case of subtractive manufacturing, solid blocks of material are used. Auxiliary material is less important in subtractive manufacturing; for example, a stream of water can be used to remove shavings or cool a manufactured part. While a computer numeric control machine also uses electrical power, its importance to the process is different (this is discussed in more detail below).

Probably the most obvious difference between the additive and subtractive manufacturing workflows is that subtractive manufacturing has no material recycling. Instead, subtractive manufacturing requires assembly; this is because subtractive manufacturing is limited to defining the external shape of an object – if internal structure is needed, the object is produced by assembling multiple components, each of which is manufactured separately.

Finally, the two workflows have different numbers of actors and different actor relationships. Subtractive manufacturing usually has long-term, high-volume customer-provider relationships; in additive manufacturing, these relationships are short-term with small production runs. Additionally, the number of additive manufacturing service providers is growing rapidly. This is because the same additive manufacturing equipment can be used to produce a variety of 3D objects. In contrast, subtractive manufacturing often requires highly specialized equipment.

4. Attack Analysis Framework

This section presents a framework for analyzing attacks on or using computer-aided manufacturing. The security threat categories for additive manufacturing are also presented. The threats are also relevant to subtractive manufacturing.

4.1 Attacks

Figure 3 presents key attacks on or using computer-aided manufacturing [49]. Several attack vectors can be used to compromise one or more elements of the manufacturing workflows shown in Figures 1 and 2 (for additive manufacturing

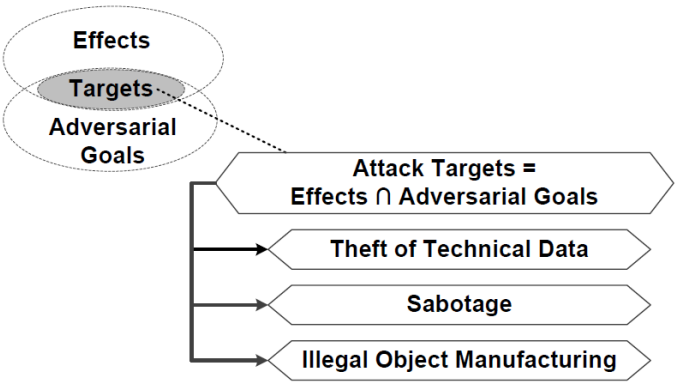

Figure 4. Major threat categories.

and subtractive manufacturing, respectively). For example, social engineering can be used to trick users into installing malicious software or firmware updates. The compromised element(s), their roles in a workflow and the degree to which an adversary can control the element(s) determine the specific manipulations that the adversary can perform. In conjunction with the manufacturing equipment, source materials and application area of the manufactured parts, the manipulations determine the achievable effects. In the case of a functional part of a device (e.g., jet engine blade), slight changes to the size or shape can render the entire device less efficient. Other changes may degrade the mechanical properties of a part so that it breaks during use [35, 48, 50] or may cause material fatigue to develop much faster than expected [6].

4.2 Security Threat Categories

Only a fraction of the effects that can be produced by attacks intersects with the goals of an adversary. For example, not all changes to the internal geometry of an object (e.g., positions and sizes of internal cavities) would compromise the mechanical properties of the object. Furthermore, the goals and objectives (i.e., "stepping stones" for achieving the adversary's goals) differ across adversaries. For instance, a hostile nation state may be interested in compromising safety whereas a malicious competitor may be interested in increasing manufacturing costs. The intersection of the attack effects and adversarial goals are referred to as attack targets or threats because they are both achievable by an adversary and are of interest to the adversary.

Figure 4 presents the three major security threat categories (or attack targets) that have been identified for additive manufacturing. Two of the categories, theft of technical data and sabotage of additive manufacturing, are discussed in the research literature (see Section 2). A theft of technical data attack seeks to illegally replicate 3D objects or the manufacturing process itself. Sabotage attacks seek to inflict physical damage, e.g., by compromising the

quality of manufactured parts or physically damaging additive manufacturing equipment.

Several articles discuss the misuse of 3D printers for manufacturing illegal items such as firearms and components of explosive devices [7, 34, 37]. With the exception of discussing the legal aspects [8, 22, 27, 38], the research literature has largely ignored this last category.

5. Security Analysis

This section compares the additive and subtractive manufacturing paradigms from the security perspective. The analysis focuses on the similarities and differences in the manufacturing workflows discussed in Section 3. The analysis is structured according to the semantically-distinct elements of attacks on or using cyber manufacturing. The results are summarized in Tables 2 and 3.

5.1 Attack Vectors

Additive and subtractive manufacturing equipment are cyber-physical systems. Both types of manufacturing have similar workflows with almost identical categories of actors and information, software and material flows. Cyber and physical attack vectors can be exploited to compromise various elements of the manufacturing systems. Therefore, the attack vectors that can be used to compromise the two types of systems are almost identical.

Many attack vectors considered in cyber security studies also apply to both workflows, enabling the compromise of cyber components. These include spear phishing, hacking, source file worms, etc. Because of the novelty and relative immaturity of additive manufacturing, additive manufacturing software and firmware are significantly more vulnerable to cyber attacks than their subtractive manufacturing counterparts.

Malicious insiders are a classical attack vector that can target both manufacturing workflows and compromise cyber and physical supply chains. Also, social engineering is applicable to both workflows.

However, certain differences between the attack vectors for the two workflows arise from the differences existing between the workflows themselves (Table 1). The following are the most notable differences that enable the attack vectors unique to additive manufacturing:

- Supplier-consumer relationships in additive manufacturing are significantly more dynamic and flexible than in subtractive manufacturing.

- The number of potential suppliers in additive manufacturing is much larger than in subtractive manufacturing; this also includes third-party software and firmware providers.

- The number of additive manufacturing service providers is much higher than in subtractive manufacturing. More importantly, they often provide manufacturing services instead of specific products.

Table 2. Comparison of additive and subtractive manufacturing security.

	Additive Manufacturing	**Subtractive Manufacturing**
Attack Vectors		
External Adversary Compromises Benign Workflow	• Hacking • Source file worms • Physical attack on physical supply chain • Social engineering • Et cetera	
	• Specially-crafted blueprint files	• –
	• Malicious software and/or firmware	• –
Malicious Actors Assume Existing Roles	• 3D object designer	• –
	• Service provider	• –
	• Software developer	• –
	• Source/auxiliary materials provider	• –
Compromised Elements		
Source Material	• Often wire or powder	• Solid blocks
General Categories	• Roles/actors • Software, firmware and hardware • Network communications • Physical supply chain • Power supply	
Workflow-Specific	• Post-processing	• Assembly line
	• Material recycling	• –

- Object designers in additive manufacturing are primarily external actors while designers in subtractive manufacturing are internal actors (e.g., a division in an enterprise).

These differences induce attack vectors in additive manufacturing environments; the attack vectors are either new or have lower probability and limited impact in subtractive manufacturing environments. First, in an additive manufacturing environment, an adversary can assume one of two roles: (i) 3D object designer; or (ii) additive manufacturing service provider. These two roles are potentially malicious and do not require hacking, social engineering or some other means to compromise the actor. A malicious 3D object designer can create special files (e.g., with embedded worms) while a malicious additive manufacturing service provider could obtain access to and compromise STL/AMF/3MF 3D object blueprint files. Additionally, the involvement of third parties in software and firmware development provides opportunities for

Table 3. Comparison of additive and subtractive manufacturing security.

	Additive Manufacturing	**Subtractive Manufacturing**
Manipulations		

General Categories	• Compromise another workflow element
	• Information exfiltration
	• Control loop attacks
	  • False sensor reading is provided
	  • False control action is provided
	  • Sensor reading is not provided or is not followed
	  • Control action is not provided or is not followed
	  • Control action is provided too late or is out of sequence
	  • Control action is stopped too soon or is applied too long
	  • Sensor reading is provided too late or is out of sequence
	  • Sensor reading is stopped too soon or is applied too long
	• Power supply spikes
	• Source material chemical composition	

Workflow-Specific	• Source material properties • Auxiliary materials • Power supply interruption • Power supply properties • Operation duration/speed	• Source block quality • – • – • – • –
Effects/Attack Targets		
Theft of Technical Data	• 3D object geometry	
	• Required properties • Manufacturing process specifications	• – • –
Sabotage	• Integration ability • Equipment damage • Environmental contamination	
	• Physical properties of degraded part • Weight • Weight distribution • Implosion/explosion • Environmental damage	• – • – • – • – • –
Illegal Part Manufacturing	• Access to illegal or illegally-manufactured items	
	• Required equipment is increasingly accessible • Blueprints are increasingly available on the Internet	• – • –

adversaries to develop and distribute malicious software and firmware, compromising equipment at additive manufacturing service provider sites.

5.2 Compromised Elements

According to Yampolskiy et al. [49], elements that can be compromised in the additive manufacturing workflow belong to four general categories: (i) actors or workflow roles assumed by the actors; (ii) software, firmware and/or hardware; (iii) network communications; and (iv) physical supply chain. An additional fifth category is power supply, whose impact on additive manufacturing is discussed in [31].

All five categories of elements can be compromised in additive and subtractive manufacturing environments. There are, however, noticeable differences at a fine level – based on where the elements belonging to the five categories are employed in a workflow and their purpose in the workflow. A major difference arises from the multiplicity and diversity of the auxiliary materials, and their significance on the quality of a manufactured part compared with traditional subtractive manufacturing. Another is that additive manufacturing employs several post-processing steps to improve part quality, some of which have limited or no importance in subtractive manufacturing (e.g., hot isostatic pressing). Furthermore, in some additive manufacturing processes, unused source material can be recycled and reused whereas in subtractive manufacturing, removed material is not directly reusable. Indeed, the recycling process in additive manufacturing itself can impact part quality because it affects the overall quality of the source material used. Additionally, the subtractive manufacturing workflow usually incorporates a step that is largely irrelevant in additive manufacturing – the assembly phase during which individually-manufactured pieces are assembled to create a functional part. Last, but not least, non-destructive testing equipment is commonly employed to verify the quality of manufactured functional parts; this equipment is largely computerized and, therefore, can be compromised by cyber attacks. Note that this is independent of reports that various non-destructive testing approaches used in subtractive manufacturing fail to detect defects in additively-manufactured parts [41, 50].

5.3 Manipulations

Every compromised element of an additive or subtractive manufacturing workflow can be used as a staging point to compromise other workflow elements. The role of the compromised element(s) in a manufacturing workflow and degree to which an adversary exercises control over it/them determine the manipulations that are possible.

If the controller workstation or other computing equipment is compromised and connected to the Internet, classical cyber attacks that exfiltrate information or enable remote access via backdoors are possible. The attacks can be used to gain access to technical data, manipulate STL/AMF/3MF 3D object design files and modify key manufacturing process parameters. Illegal access to technical data or its use by an adversary who impersonates an additive manufacturing service provider are plausible attack vectors. An adversary who has direct access to equipment can also create restricted objects such as firearms; of

course, this applies to both additive and subtractive manufacturing equipment that can produce the restricted objects or their components. Principal differences between additive and subtractive manufacturing technologies with regard to malicious manipulations are the broad availability of additive manufacturing equipment and access to object blueprints on the Internet.

A number of manipulations are possible if the controller workstation, additive manufacturing equipment or network communications between the controller and equipment are compromised. Since these three components comprise a cyber-physical system, most cyber-physical attacks are applicable to additive manufacturing systems. At the fundamental level, communications between a sensor and controller or between a controller and actuator can be interrupted or corrupted [10]. Furthermore, in the case of real-time processes – characterized by cyber-physical systems in general and additive/subtractive manufacturing systems in particular – the correctness of operations and their timing are of paramount importance [24]. Therefore, manipulations of sensor readings and control commands involve disruptions of their timing and order [31]. The physical process that is controlled by the particular control loop ultimately determines the effects of any manipulations; this applies to additive and subtractive manufacturing alike. Furthermore, the timing of manipulations in the manufacturing cycle influences the effects and their extent [23].

Additive and subtractive manufacturing equipment require power. Power spikes can affect both types of equipment in a similar manner (e.g., damage electric motors). However, power supply interruptions have different impacts on the manufactured objects. In the case of subtractive manufacturing, power interruptions only affect the speed of production. However, interruptions can have severe impacts on additively-manufactured part quality (this is discussed this in more detail below); therefore, these manipulations are categorized as additive-manufacturing-specific. Similarly, manipulations (e.g., control loop attacks) that affect the durations of particular operations impact additive and subtractive manufacturing differently – manufacturing speed for both technologies and part quality, in addition, for additive manufacturing.

Manipulations of source materials are possible in additive and subtractive manufacturing, but the available manipulations can be quite different. In both cases, the chemical compositions of source materials can be changed. In subtractive manufacturing, the quality of the source material blocks can be manipulated (e.g., they can have different microstructures). In the case of additive manufacturing, properties such as the form factor can be manipulated (e.g., size and shape of the powder particles or diameter of the wire). Additionally, the chemical compositions of the auxiliary materials used in additive manufacturing can be manipulated. In general, the attack vectors that enable source and auxiliary material manipulations in additive manufacturing are manifold and are much easier to exploit than in the case of subtractive manufacturing.

5.4 Effects

This section discusses the effects of attacks on additive and subtractive manufacturing. The discussion of effects is structured in terms of the three security threat categories (Figure 4).

Theft of Technical Data. Two scenarios in which intellectual property violations are possible in additive and subtractive manufacturing are: (i) compromise of the cyber infrastructure of a benign manufacturer (e.g., when a controller workstation is connected to the Internet); and (ii) manufacturer is a malicious actor. In both cases, the adversary is interested in gaining access to the victim's intellectual property and eventually commits an infringement.

The differences between the two manufacturing technologies arise from what is considered to be intellectual property. Clearly, 3D object geometry corresponds to intellectual property in both manufacturing paradigms. However, in the case of subtractive manufacturing, the material properties of the manufactured part depend directly on the properties of the source material block. In contract, in additive manufacturing, the part material is created (and, thus, its properties are defined) during the manufacturing process itself. Therefore, in additive manufacturing, the required properties of the manufactured 3D object as well as the manufacturing process specifications correspond to intellectual property [44].

Sabotage. The following scenarios enable the quality of a manufactured part and/or manufacturing equipment to be sabotaged:

- Manipulation of the object specifications regardless of its representation, which could be a STL/AMF/3MF file, individual G-code commands, toolpath file, etc.
- Compromise of the cyber infrastructure of the manufacturing process.
- Compromise of the physical supply chain of source and auxiliary materials.
- Manipulation of the power supply.

As discussed in [42] and demonstrated experimentally in [35], manufactured parts can be sabotaged by modifying their exterior shapes and dimensions, thereby affecting their integration; this is clearly applicable to both manufacturing paradigms. In particular, this is achieved by modifying object specification files or compromising the cyber infrastructure of the manufacturing process. For example, compromised firmware could manipulate the thickness of the printed layers in additive manufacturing [29].

However, several sabotage attacks are specific to additive manufacturing and are not possible in subtractive manufacturing. Introducing voids in a manufactured object [35] or replacing portions of a manufactured object with a different material [50] can degrade the physical properties of the object; this

can also change the weight and weight distribution of the object [49]. Furthermore, various additive manufacturing parameters can be manipulated to affect the microstructure of the manufactured object and, thus, its physical properties; the parameters include build direction, heat source energy and scanning strategy [48]. The ability to sabotage the quality of a 3D-printed part by manipulating some of these parameters has been proven experimentally [29, 42, 50].

As Stuxnet [15] and the Aurora experiment [36] have demonstrated, a cyber-physical attack that forces equipment to operate outside its designated operational ranges can induce physical damage. Such cyber-physical attacks, which exploit the fact that cyber components control physical processes, are applicable to both manufacturing paradigms. An attack that damages a process chamber used in additive manufacturing could release hazardous materials to the environment. This is a manufacturing-process-specific case of sabotage. An example is the release of the metal powder used in selective laser melting, which is hazardous because of the fine particle size (0.1 to 5 μm) [21].

Last, but not least, in the case of additive manufacturing with metals, damage to the process chamber can lead to an explosion or implosion with subsequent damage to the manufacturing equipment environment and a likely fire [48, 49]. For example, when the heat source is a laser, the production chamber is commonly filled with inert gas to prevent an exothermic reaction; increasing the oxygen pressure can cause the combustible fine metal powder to explode. A vacuum environment is maintained to minimize the deflection of electrons when an electron beam is used as the heat source. Therefore, a slow leak is a more likely outcome of process chamber damage, but an implosion caused by a specially-crafted attack cannot be ruled out [49]. While safety mechanisms are implemented to shut down the heat sources used in additive manufacturing during safety-critical events, these mechanisms can be disabled by malicious or compromised 3D printer firmware.

Illegal Object Manufacturing. Two possible scenarios for this threat category are: (i) an adversary owns the blueprint of a potentially illegal object and the requisite manufacturing equipment; and (ii) an adversary has access to the blueprint and the manufacturing equipment.

In these scenarios, there are no technical differences in using additive or subtractive manufacturing to produce illegal items. The only practical differences arise from two factors. First, high quality additive manufacturing equipment is increasingly accessible to private owners, unlike industrial-grade subtractive manufacturing equipment that is predominantly owned by enterprises. Second, STL/AMF/3MF blueprint files for 3D printing are widely available on the Internet (e.g., from makers' forums); in contrast, blueprints used in subtractive manufacturing are generally well protected because of their intellectual property value to subtractive manufacturing enterprises.

6. Conclusions

The rapid proliferation of additive manufacturing has raised concerns about its security. In this context, it is important to understand the extent to which additive manufacturing differs from traditional subtractive manufacturing. This chapter has evaluated the additive and subtractive manufacturing workflows, and has presented a framework for analyzing attacks on or using computer-aided manufacturing systems along with the major threat categories that target additive manufacturing. In particular, the framework was applied to identify how the differences in the workflows translate to the security domain.

The analysis concludes that, while there are overlaps in the security of additive and subtractive manufacturing, significant differences exist. This is true for all the components in the analysis framework – attack vectors, compromised elements, manipulations and attack targets. Two of the three major threat categories for additive manufacturing – theft of technical data and sabotage – differ considerably from subtractive manufacturing. However, in the case of the third category – illegal object manufacturing – no notable differences exist between additive and subtractive manufacturing. The results of this investigation coupled with the increasing importance of additive manufacturing in all the critical infrastructure sectors emphasize the need to address the security aspects in a comprehensive and timely manner.

References

[1] 3MF Consortium, 3D Manufacturing Format, Core Specification and Reference Guide, Version 1.1, Wakefield, Massachusetts (`3mf.io/wp-content/uploads/2016/03/3MFcoreSpec_1.1.pdf`), 2015.

[2] M. Al Faruque, S. Chhetri, A. Canedo and J. Wan, Acoustic side-channel attacks on additive manufacturing systems, *Proceedings of the Seventh International Conference on Cyber-Physical Systems*, article 19, 2016.

[3] M. Al Faruque, S. Chhetri, S. Faezi and A. Canedo, Forensics of Thermal Side-Channels in Additive Manufacturing Systems, CECS Technical Report #16–01, Center for Embedded and Cyber-Physical Systems, University of California, Irvine, Irvine, California, 2016.

[4] American Society for Testing and Materials, ISO/ASTM52915-16: Standard Specification for Additive Manufacturing File Format (AMF), Version 1.2, West Conshohocken, Pennsylvania, 2016.

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

[6] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin and Y. Elovici, dr0wned – Cyber-physical attack with additive manufacturing, *Proceedings of the Eleventh USENIX Workshop on Offensive Technologies*, 2017.

[7] N. Bilton, The rise of 3-D printed guns, *The New York Times*, August 13, 2014.

[8] J. Blackman, The 1st Amendment, 2nd Amendment and 3D printed guns, *Tennessee Law Review*, vol. 81(3), pp. 479–538, 2014.

[9] A. Brown, M. Yampolskiy, J. Gatlin and T. Andel, Legal aspects of protecting intellectual property in additive manufacturing, in *Critical Infrastructure Protection X*, M. Rice and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 63–79, 2016.

[10] A. Cardenas, S. Amin and S. Sastry, Secure control: Towards survivable cyber-physical systems, *Proceedings of the Twenty–Eighth International Conference on Distributed Computing Systems Workshops*, pp. 495–500, 2008.

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

[12] S. Chhetri, A. Canedo and M. Al Faruque, KCAD: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems, *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, 2016.

[13] Q. Do, B. Martini and K. Choo, A data exfiltration and remote exploitation attack on consumer 3D printers, *IEEE Transactions on Information Forensics and Security*, vol. 11(10), pp. 2174–2186, 2016.

[14] Electronic Industries Association, ANSI/EIA RS-274-D-1980: Interchangeable Variable Block Data Format for Positioning, Contouring and Contouring/Positioning Numerically Controlled Machines, Washington, DC, 1980.

[15] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.

[16] W. Frazier, Metal additive manufacturing: A review, *Journal of Materials Engineering and Performance*, vol. 23(6), pp. 1917–1928, 2014.

[17] D. Helbing, Globally networked risks and how to respond, *Nature*, vol. 497(7447), pp. 51–59, 2013.

[18] J. Hiller and H. Lipson, STL 2.0: A proposal for a universal multi-material additive manufacturing file format, *Proceedings of the Solid Freeform Fabrication Symposium*, pp. 266–278, 2009.

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

[20] T. Holbrook and L. Osborn, Digital patent infringement in an era of 3D printing, *University of California Davis Law Review*, vol. 48(4), pp. 1319–1385, 2015.

[21] Inside Metal Additive Manufacturing, The Role of (Super) Powders in SLM (www.insidemetaladditivemanufacturing.com/blog/the-role-of-super-powders-in-slm), April 10, 2014.

[22] 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*, vol. 2013(2), pp. 337–361, 2013.

[23] M. Krotofil, A. Cardenas, J. Larsen and D. Gollmann, Vulnerabilities of cyber-physical systems to stale data – Determining the optimal time to launch attacks, *International Journal of Critical Infrastructure Protection*, vol. 7(4), pp. 213–232, 2014.

[24] E. Lee, Cyber physical systems: Design challenges, *Proceedings of the Eleventh IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, pp. 363–369, 2008.

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

[26] B. Macq, P. Alface and M. Montanola, Applicability of watermarking for intellectual property rights protection in a 3D printing scenario, *Proceedings of the Twentieth International Conference on 3D Web Technology*, pp. 89–95, 2015.

[27] K. McMullen, Worlds collide when 3D printers reach the public: Modeling a digital gun control law after the Digital Millennium Copyright Act, *Michigan State Law Review*, vol. 2044(1), pp. 187–225, 2014.

[28] S. Moore, P. Armstrong, T. McDonald and M. Yampolskiy, Vulnerability analysis of desktop 3D printer software, *Proceedings of the 2016 Resilience Week*, pp. 46–51, 2016.

[29] S. Moore, W. Glisson and M. Yampolskiy, Implications of malicious 3D printer firmware, *Proceedings of the Fiftieth Hawaii International Conference on System Sciences*, pp. 6089–6098, 2017.

[30] A. Muller and S. Karevska, How Will 3D Printing Make Your Company the Strongest Link in the Value Chain? EY's Global 3D Printing Report 2016, Ernst & Young, Mannheim, Germany, 2016.

[31] G. Pope, STPA for additive manufacturing, presented at the *Systems Theoretic Accident Model and Processes Workshop*, 2016.

[32] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

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

[34] A. Sternstein, Things can go kaboom when a defense contractor's 3-D printer gets hacked, *Nextgov*, September 11, 2014.

[35] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems, *Proceedings of the Twenty-Fifth International Solid Freeform Fabrication Symposium*, pp. 951–963, 2014.

[36] M. Swearingen, S. Brunasso, J. Weiss and D. Huber, What you need to know (and don't) about the Aurora vulnerability, *POWER Magazine*, September 1, 2013.

[37] D. Tirone and J. Gilley, 3D printing: A new threat to gun control and security policy? *The Conversation* (`theconversation.com/3d-printing-a-new-threat-to-gun-control-and-security-policy-61416`), July 19, 2016.

[38] J. Tran, The law and 3D printing, *John Marshall Journal of Information Technology and Privacy Law*, vol. 31(4), pp. 505–520, 2015.

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

[40] U.S. Department of Homeland Security, Critical Infrastructure Sectors, Washington, DC (`www.dhs.gov/critical-infrastructure-sectors`), 2017.

[41] Wohlers Associates, Wohlers Report 2016, Fort Collins, Colorado, 2016.

[42] C. Xiao, Security attack on 3D printing, presented at the *xFocus Information Security Conference*, 2013.

[43] Z. Xu and Q. Zhu, Cross-layer secure cyber-physical control system design for networked 3D printers, *Proceedings of the American Control Conference*, pp. 1191–1196, 2016.

[44] M. Yampolskiy, T. Andel, J. McDonald, W. Glisson and A. Yasinsac, Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing, *Proceedings of the Fourth Program Protection and Reverse Engineering Workshop*, article 7, 2014.

[45] M. Yampolskiy, T. Andel, J. McDonald, W. Glisson and A. Yasinsac, Towards security of additive layer manufacturing, presented at the *Thirtieth Annual Computer Security Applications Conference*, 2014.

[46] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, Taxonomy for descriptions of cross-domain attacks on CPSs, *Proceedings of the Second ACM International Conference on High Confidence Networked Systems*, pp. 135–142, 2013.

[47] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, A language for describing attacks on cyber-physical systems, *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 40–52, 2015.

[48] M. Yampolskiy, L. Schutzle, U. Vaidya and A. Yasinsac, Security challenges of additive manufacturing with metals and alloys, in *Critical Infrastructure Protection IX*, M. Rice and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 169–183, 2015.

[49] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. Overfelt, K. Sloan and A. Yasinsac, Using 3D printers as weapons, *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 58–71, 2016.

[50] S. Zeltmann, N. Gupta, N. Tsoutsos, M. Maniatakos, J. Rajendran and R. Karri, Manufacturing and security challenges in 3D printing, *Journal of the Minerals, Metals and Materials Society*, vol. 68(7), pp. 1872–1881, 2016.