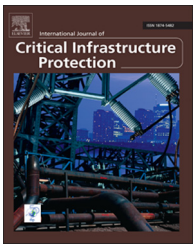
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Using 3D printers as weapons

Mark Yampolskiy[a,*], *Anthony Skjellum*[b], *Michael Kretzschmar*[d], *Ruel A. Overfelt*[d], *Kenneth R. Sloan*[e], *Alec Yasinsac*[a]

[a]*School of Computing, University of South Alabama, Shelby Hall 1113, 150 Jaguar Drive, Mobile, Alabama 36688, USA*
[b]*Department of Computer Science and Software Engineering, Auburn University, Shelby 3101, 345 W. Magnolia, Auburn, Alabama 36849, USA*
[c]*Information Assurance and Cyber Defence Office, BICES Group Executive, NATO HQ Building Z, Boulevard Leopold III, 1110 Brussels, Belgium*
[d]*Department of Mechanical Engineering, Auburn University, 282 Wilmore Hall on Wilmore Drive, Auburn, Alabama 36849, USA*
[e]*Department of Computer and Information Sciences, University of Alabama at Birmingham, 1720 2nd Avenue South, Birmingham, Alabama 35294, USA*

ARTICLE INFO

Article history:
Received 6 October 2015
Received in revised form
6 June 2016
Accepted 7 June 2016
Available online 23 June 2016

Keywords:
Additive Manufacturing
3D Printing
Weaponization
Security Taxonomy

ABSTRACT

Additive manufacturing, also known as 3D printing, is a transformative manufacturing technology that will play a significant role in the critical manufacturing sector. Industrial-grade 3D printers are increasingly used to produce functional parts for important systems. However, due to their reliance on computerization, 3D printers are susceptible to a broad range of attacks. More importantly, compromising a 3D printer is not a goal, but rather a staging point for launching subsequent attacks with the printer. For example, an adversary can compromise a 3D printer in order to manipulate the mechanical properties of manufactured parts. If the manufactured parts are used in jet engines or in other safety-critical systems, they could endanger human life, disrupt critical infrastructure assets and produce significant economic and societal impacts.

This paper analyzes the ability of an adversary to "weaponize" compromised additive manufacturing equipment in order to cause kinetic, nuclear/biological/chemical or cyber damage. In particular, the paper presents categories (taxonomies) of the elements in an additive manufacturing workflow that can be compromised by successful attacks, the manipulations that the compromised elements can exercise and the weapon-like effects resulting from these manipulations. The relationships between these taxon[illegible] are discussed. Finally, the weaponization capabilities of 3D printers are characteriz[illegible]

1. Introduction

Additive manufacturing (AM), also known as additive layer manufacturing or 3D printing, creates objects incrementally by adding thin layers to build up the objects from two dimensions to their desired three-dimensional forms [80]. Additive manufacturing has several technical and economic advantages compared with traditional manufacturing. This

*Corresponding author.
E-mail address: yampolskiy@southalabama.edu (M. Yampolskiy).

http://dx.doi.org/10.1016/j.ijcip.2015.12.004
1874-5482/

includes just-in-time and on-demand production, manufacturing parts closer to assembly lines, shortening design-to-product times and producing functional parts with complex internal geometries and mechanical properties optimized for a variety of application areas.

The market penetration of additive manufacturing technology has tremendous potential. Wohlers Associates [80] reported in 2014 that the additive manufacturing industry had $4.1 billion in revenue, with 29% of all manufactured objects being used as functional parts. According to NIST [72,73], additive manufacturing technology will reach 50% of its market potential between 2031 and 2038, accounting for about $50 billion in revenue between 2029 and 2031.

As additive manufacturing emerges as a transformative technology [10], numerous agencies and companies are investigating applications of the technology. SpaceX has used additive manufacturing to produce engine chambers for its newest Dragon spacecraft [27]. General Electric has built complex brackets that weigh 80% less than conventional structural parts [29]. NASA has created a rocket injector designed for high loads and temperature gradients [60]. A Dutch company, DUS Architects, plans to use additive manufacturing to print a entire three-story home [19].

The tremendous market potential coupled with economic, geopolitical and other implications of additive manufacturing technology [6,9,35] will inevitably draw the attention of adversaries ranging from individuals to state actors. Because of their reliance on computerization, 3D printers are susceptible to a broad range of attacks. This is supported by a number of attacks on cyber-physical systems detected "in the wild" as well as attacks hypothesized in the research literature. These include attacks on industrial control systems [8,25,41,66], state-of-the-art automobiles [14,39] and unmanned and manned aeronautic systems [26,81,84]. All these examples lead to the conclusion that attacks on additive manufacturing systems and the misuse of additive manufacturing technology are just over the horizon.

This paper examines how a 3D printer can be misused as a weapon. It does not discuss specific cyber or physical attacks that can enable an adversary to take control of the manufacturing process. Instead, it begins by identifying the elements that can be compromised by successful attacks. Following this, the paper discusses the manipulations that the compromised elements could exercise. Finally, the paper highlights the effects of these manipulations and demonstrates that they are comparable with those produced by several categories of weapons.

2. Related work

This section discusses additive manufacturing security and outlines some security-related (attack) taxonomies.

2.1. *Additive manufacturing security*

At this time, the literature on additive manufacturing security is exceedingly sparse. However, recent articles (see, e.g., [67,77]) demonstrate the growing awareness of the threat of intellectual property violations and damage to additive manufacturing systems and infrastructures.

Aspects of intellectual property protection discussed in the literature include open challenges [18,53], intellectual property law applied to additive manufacturing [7], embedding malware in source files to steal intellectual property (e.g., the ACAD/Medre.A worm [23]), technical challenges of intellectual property protection in outsourcing scenarios [82] and the application of watermarking techniques to detect counterfeit parts [46].

The ability of an attack on an additive manufacturing infrastructure to inflict physical damage is a major concern [83]. Several recent publications share this assessment (see, e.g., [52,67,68,87]). Sternstein [67] discusses the possibility of a 3D printer exploding because of mismanagement; such an incident actually occurred in November 2013 [56].

Yampolskiy et al. [87] have conducted an extensive survey of the material science and mechanical engineering literature and provide a qualitative analysis of an adversary's ability to influence the physical characteristics of manufactured objects. They also list the manufacturing parameters of metal printers that can be potentially manipulated, along with their impacts on the microstructures of manufactured parts and, consequently, on their physical properties. Similar conclusions are presented by Frazier [28] in a survey of the additive-manufacturing-related material science literature that focuses on the factors that influence the quality of manufactured parts.

Consider, for example, the popular powder bed fusion process [17,28,87]. In this process, a layer of source material (metal or polymer) in powder form is distributed in a chamber. The layer is fused by a heat source (laser or electron beam) that melts the profile of the next slice of the 3D object. This powder distribution and fusion sequence is repeated layer by layer. A number of factors influence a powder bed fusion process. These include powder properties (material, shape, regularity and size) [24,44,64], heat source and its properties (electron beam or laser, diameter, intensity/distance between material and heat source) [48], vacuum or inert gas used [3,30], accuracy of the mechanisms in the machine (control of chamber, heat source position and heat source orientation) [87], support structure [80], melting pattern [5] and the number of transitions between liquid and solid states [37,38,76]. The quantification of the causal relationships between additive manufacturing parameters and the physical characteristics of the manufactured parts is an active field of research. For example, DARPA [70] recently announced its Open Manufacturing Program that seeks to develop models for predicting part properties based on the manufacturing parameters.

Experimental proof that an attacker can manipulate source stereolithography (STL) files and insert voids (i.e., cavities) that reduce the tensile strengths of the manufactured objects is provided in [68]. Similarly, manipulations of the object descriptions can be used to change the dimensions of manufactured parts [79,87]. Manipulations of source files, however, can only change object geometry.

2.2. Attack taxonomies

At this time, no attack taxonomies have been developed for additive manufacturing security. However, numerous cyber security taxonomies have been published and some of them are useful for developing taxonomies for the additive manufacturing domain.

Yampolskiy et al. [85] state that "taxonomy" is an overloaded term. The term can refer to a single-category classification, multi-dimensional characterization or multi-dimensional description. This paper develops single-category taxonomies, which are typically represented as tree-like structures. Examples include taxonomies that categorize wireless security threats [78], network infrastructure attacks [11] and distributed denial-of-service attacks [50]. Venn diagrams have also been used to express single-category taxonomies; an example is the characterization of attacks on embedded systems [61]. Interested readers are referred to [31] for descriptions of some prominent taxonomies and a discussion of their limitations.

Some researchers have categorized the concepts of dependability and security according to their attributes, threats and means [4,42]. Avizienis et al. [4], in particular, have introduced several techniques that are relevant to this paper. The possible combinations of fault classes can be viewed as a cross-product of the elements of a taxonomy; Avizienis and colleagues represent this as a matrix and as a tree structure. Error propagation is also a good example of a causal chain of effect propagation in a system with complex interdependencies.

Key taxonomies related to cyber-physical systems include interdependencies in industrial critical infrastructures [32,62] and attacks on SCADA systems [20,36,88].

3. Background

This section describes the additive manufacturing workflow. Also, it highlights the most representative materials and application areas of additive manufacturing, including electronics, human tissue and food and drug printing.

3.1. Additive manufacturing workflow

Fig. 1 shows the interactions between the actors involved in additive manufacturing. Additive manufacturing systems – also referred to as 3D printers in what follows – are usually constructed and supplied by original equipment manufacturers (OEMs) and third-party vendors. In 2014, 49 system manufacturers in thirteen countries produced and sold industrial-grade additive manufacturing equipment and it is estimated that hundreds of small companies offer desktop 3D printers [80]. The user community often develops and releases firmware updates for embedded controllers in 3D printers and software updates for "controller computers" used to submit and control manufacturing jobs. These personal computers are also used to apply firmware updates to additive manufacturing equipment.

The 3D object to be printed is typically specified using the stereolithography (STL) format [34] or additive manufacturing file (AMF) format [16,43], which represent a "sliced" version of a computer-aided design (CAD) model of a 3D object. Based on the 3D object description stored in an STL or AMF file, the controller computer sends commands to a 3D printer that produces the specified object. These commands, which position the building platform and nozzle, adjust the platform temperature, etc., are usually encoded as G-code [21], a language often used in computer-aided manufacturing (CAM).

An additive manufacturing process requires source materials. The American Society for Testing and Materials (ASTM) International Committee F42 on Additive Manufacturing Technologies has approved seven additive manufacturing process categories [80]. The processes differ in the supported source materials (e.g., polymers or metals), means of source material distribution (e.g., powder bed or nozzle), heat sources (e.g., laser, electron beam or arc), etc.

In the powder bed fusion (PBF) process, a thin layer of the source material (usually metal or polymer) in powder form is distributed in a powder bed. The layer is fused by a heat source (laser or electron beam) that melts the profile of a slice of the 3D object; this powder distribution and fusion sequence is repeated layer by layer. In this process, only a fraction of the powder distributed in the bed is melted to create the produced object. The unused powder can be

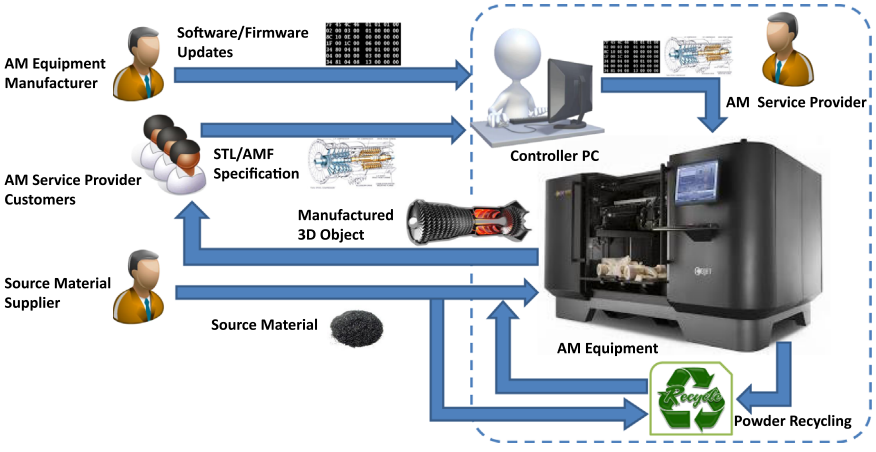


Fig. 1 – Additive manufacturing workflow.

recycled to reduce waste and, consequently, reduce production costs. However, because the residual powder would have been exposed to high temperatures, its properties could change – for example, the metal particles may agglomerate into large clusters. Since this can affect the mechanical properties of the manufactured 3D objects, reused powder is commonly sieved and mixed with "virgin" powder in a proportion that reduces the negative impact to an acceptable level.

Depending on the additive manufacturing process, source material and part geometry, the production workflow can include several steps that are not shown in Fig. 1. Two important aspects are support structures and post-processing, both of which can have a significant impact on the quality of the printed parts.

Support structures are necessary to print parts with complex geometries – the structures primarily serve to prevent the sagging of overhangs. When printing with metals and alloys, the support structure material can have a significant impact on part quality because of its role in heat distribution [40]. After a part is printed, the support structure is normally removed and discarded.

Post-processing is frequently required during the production of metal parts. Specifically, hot isostatic pressing (HIP) is often required to eliminate the residual internal porosity and to enhance the mechanical properties of printed objects [28]. In the case of the Ti-6Al-4 V alloy, post-processing involves a hot isostatic pressing cycle of 100 MPa and 926 °C for two to four hours, followed by furnace cooling below 427°C [28]. The surface finish can also have a significant impact on properties such as fatigue life by providing sites for cracks to initiate [12].

4. Materials and application areas

The application areas of the manufactured parts are highly dependent on the properties achievable with different source materials. Indeed, the variety of supported source materials and application areas are continually expanding. According to the Wohlers Report (an important annual survey of worldwide progress in the additive manufacturing industry) [80], the two major categories of additive manufacturing materials are plastics and metals.

Plastics (or polymers) are the largest group of additive manufacturing source materials that offer a broad variety of properties, including color, transparency, tensile strength, rigidity and biocompatibility. The materials range from extremely hard plastics to rubber-like elastomers. Because of the broad range of achievable properties, the application areas of 3D-printed plastic objects range from models to functional parts in the automotive and aerospace industries.

The list of metals and alloys supported by additive manufacturing equipment includes stainless steel, titanium and aluminum alloys, gold and silver. The application areas vary based on the material and the properties achievable with the material. Metal is used to produce functional parts ranging from watch housings to entire jet engines [65].

Bio-compatible materials (both plastics and metal) can be used to produce customized medical implants (e.g., for the hip and knee). Along with plastics and metals, ceramics, ceramic-metal hybrids and a variety of composites are among the well-established and broadly-used source materials.

Additive manufacturing is now used in several emerging fields, some of which require novel materials. Three important areas with significant implications with regard to additive manufacturing security are electronics, biological tissue and ingestibles (food and drugs).

Although the concept dates back to 2004 [47,58], the 3D printing of electrical and electronic circuits continues to be an active field of research. At this time, however, the use of additive manufacturing technology to produce functional electronics such as high-speed computing units, sensors and wireless communications components is in its infancy [80]. In 2015, Voxel8 [74] released the first commercial 3D printer that supports the printing of electronic circuits. The 3D printer incorporates a dual-material system that extrudes plastics and conductive silver ink, enabling circuit printing and electronics component integration. The printer can be stopped to install electronic components produced via conventional means. This eliminates many of the limitations that have beset direct circuit printing.

The printing of living tissue has the potential to become a transformative technology. Although the printing of body parts and entire internal organs is anticipated to become a reality [80], much work remains to be done. It is important to note that, in biological tissue, different types of cells are frequently organized in unique hierarchical structures and substructures (also referred as architectures). The cells and their spatial organization are critical to the biological function of the tissue. Nevertheless, this area is advancing rapidly and several application areas have emerged.

Cosmetics companies such as L'Oreal have used human epidermics (i.e., pieces of skin) for several years to test new products [15]. Human epidermics are currently grown *in vitro* in-house or by external entities such as Episkin [22], but the process could soon be replaced by 3D bio-printing. Another company, TeVido Biodevices [71,80], has announced plans to print skin and fat grafts for breast cancer reconstruction using the recipients' own cells. Meanwhile, Organovo [57] offers custom 3D-printed-tissue for drug discovery, enabling drug toxicity and efficacy to be investigated in pre-clinical trials. Indeed, Organovo offers "fully human, architecturally correct, functional 3D tissues" that can be constructed for "nearly any tissue type, for nearly any disease." One of its products is living liver tissue.

Another emerging additive manufacturing area is food and drug printing. At this time, food printing is rather basic – it is limited to a few ingredients that can be mixed and "cooked" as desired. Current food printers use containers prefilled with ingredients or have refillable containers are replenished with fresh ingredients by the owner of the 3D printer [54]. One of the advantages of food printing is the production of healthy meals [45]. NASA [51] believes that food printing in space will satisfy the nutrition needs of astronauts while offering a larger variety of foods, especially during extended space missions.

In August 2015, Aprecia Pharmaceuticals announced that the U.S. Food and Drug Administration (FDA) had approved the first 3D-printed drug product [33]. The printing of drugs is

expected to enable cost-effective personalized medicine. 3D printing in proximity to patients would enable the customized production (pharmaceutical compounds, dosages and buffering agents geared for specific individuals) and the delivery of fresh medication [75]. For this type of production to reach the mainstream, 3D printers will have to be adapted to operate on a variety of pharmaceutical compounds.

5. Taxonomies

This section describes the dimensions of the semantic aspects of attacks on or with additive manufacturing equipment. Next, classifications of the following dimensions are presented: (i) compromised elements in the additive manufacturing workflow; (ii) manipulations of these elements; (iii) subset of the effects of these manipulations that overlap with the adversarial goal of using 3D printers as weapons.

5.1. *Attacks on/with 3D printers*

Fig. 2 outlines how attacks on or with 3D printers can be performed. A variety of attack vectors can be used to compromise elements of the additive manufacturing workflow described in Section 3.1. The compromised components, their roles in the workflow and the degree to which an adversary can control the components determine the manipulations that an adversary can perform. In conjunction with the types of additive manufacturing equipment, source materials and applications of the manufactured parts, the manipulations determine the achievable effects.

According to Yampolskiy et al. [85,86], every manipulation can be specified as one or more tuples of Influenced Element (i.e., manipulated object) and Influence (i.e., exercised change). Similarly, effects can be specified as tuples of Affected Element and Impact. Yampolskiy et al. [85,86] consider a manipulation to be a Cause (of one or more effects). This naming enables the seamless description of effect propagation causal chains. This paper emphasizes initial manipulations.

Only a fraction of the effects that can be produced intersect with the adversarial goals. Moreover, only a small subset of the intersection causes damage that is commonly associated with a weapon. The effects in the small subset are what an adversary seeks when attempting to misuse a 3D printer as a weapon (3D-PaaW).

The weaponization of a 3D printer means that it can be used to inflict damage that is associated with a weapon. Conventional weapons inflict kinetic damage, causing physical destruction, injuries and death. Nuclear, biological and chemical (NBC) weapons are commonly considered to be non-conventional weapons; these weapons contaminate the environment and cause health problems and death. The most recent addition to the arsenal are cyber weapons. As the Stuxnet attack [25] and the Aurora experiment [69] have demonstrated, cyber weapons can cause physical destruction to infrastructures and, possibly, injuries and deaths.

This paper considers situations where additive manufacturing equipment or the manufactured objects can cause one of the types of damage mentioned above. An electronic warfare system is not deemed to be a weapon in this paper; therefore, electronic warfare is not discussed. However, the possibility of misusing a 3D printer to produce electronic warfare effects cannot be discounted.

This paper does not discuss attack vectors in detail. This is because the attack vectors are essentially the same as the attack vectors for other classes of cyber-physical systems; these are covered extensively in the research literature. The materials used in additive manufacturing for creating parts in various application areas are well known and are outlined in Section 4.

The remainder of this section focuses on the aspects that are central to the security of additive manufacturing: (i) elements in the additive manufacturing workflow that can be compromised; (ii) manipulations that can be performed by these elements; and (iii) potential to weaponize a 3D printer. The taxonomies for all these aspects (or dimensions) of an attack on/with 3D printers are presented below.

5.2. *Compromised elements*

The following taxonomy is proposed for the elements in the additive manufacturing workflow that can be compromised:

- **Actors:** It is fair to assume that any actor in the workflow could be malicious and that any other actor could be the victim. Therefore, any outgoing edge from an actor could be malicious and any incoming edge to an actor could generate a negative impact. This means that any software updates, replacement components (e.g., hardware or mechanical parts), STL/AMF files or source materials could be specially crafted by a malicious actor.
  Additionally, an external adversary could attempt to impersonate a legitimate actor with similar effects on the workflow. Furthermore, because every actor in the additive manufacturing workflow represents an organization (company or agency), a malicious employee could circumvent the actor's internal processes in a manner that makes it appear to be malicious.
- **Software, Hardware and Firmware:** Cyber security compromises over the decades reveal that software, hardware and firmware in a computing system workflow – and by

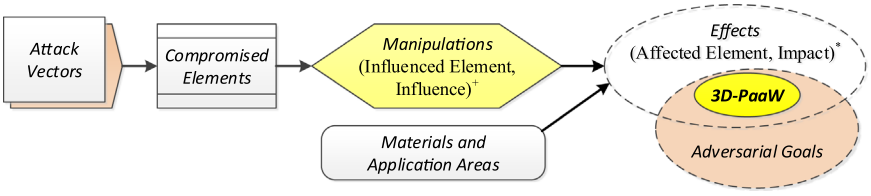


Fig. 2 – Attacks on/with 3D printers.

extension in the additive manufacturing workflow – can be successfully targeted by adversaries. Social engineering has proven to be an effective attack vector to persuade legitimate users to install malicious software or firmware. Buffer overflow attacks and their variants, "return to libc" and return-oriented programming [13,63], are still the most effective attack vectors, enabling code injection into software and firmware via carefully-crafted inputs. Stuxnet [25] has demonstrated that malicious software running on a control computer can install malicious firmware on a system and vice versa. Furthermore, hardware Trojans can be embedded in devices; these Trojans could have complex activation triggers [59] to evade premature detection during functional testing. Side-channel methods as described in [1] are limited in their ability to detect Trojans.

- **Network Communications:** Network communications channels can be compromised in numerous ways, as detailed in the cyber security literature. For example, malware running on the controller computer (see Fig. 1) could install a network filter and gain access to all incoming and outgoing packets. This approach is broadly used by firewalls and network monitoring tools, but it is often misused by malware.
- **Physical Supply Chain:** The additive manufacturing workflow involves the delivery of various physical components. These include replacement components (electronic and mechanical), all kinds of materials used in production and post-production (source materials and support structure materials) and the manufactured 3D parts. The physical supply chain, which explicitly covers the transportation and storage of physical components, offers myriad opportunities for compromise. In addition to the obvious methods, even environmental parameters pose hazards – especially temperature and humidity during storage and transportation, and vibration during transportation.

5.3. *Manipulations*

Compromised elements of the additive manufacturing workflow can be used to perpetrate attacks. The ability to exercise manipulations depends on the category of the compromised element, its role (or location) in the additive manufacturing workflow and the degree of control that an adversary has over the compromised element. For the sake of simplicity, it is assumed that an adversary can exercise full control over a compromised element.

Fig. 3 presents the correlation between classes of compromised elements (independent of their locations in the additive manufacturing workflow) and the manipulations that the elements are capable of exercising. A manipulation is represented as one or more tuples of (Influenced Element, Influence). Therefore, a two-level classification is presented. The top-level classification specifies the categories of influenced elements. The classification of relevant influences is expressed as a sub-classification of the influenced elements.

The following taxonomy is proposed for manipulations:

- **Source Materials:** The ability to manipulate source materials is a signature aspect that distinguishes the security of additive manufacturing systems from the security of other cyber-physical systems. Source materials refers not only to the materials used to create 3D objects, but all the other materials used in the production process, including those used for support structures and inert gas (argon) when a laser is used as the heat source (a vacuum is required when an electron beam is used as the heat source). The source materials can be manipulated by a malicious actor who produces and/or supplies the material, or by an external adversary who has compromised the supply chain. Whereas a malicious producer or supplier can manipulate only their own source materials, an adversary who has successfully targeted the physical supply chain can compromise any and all source materials. In both instances, the following source material properties can be manipulated:
  - *Materials*: The modification or replacement of materials is a key manipulation. For example, a metal or alloy with different mechanical properties can be mixed with or can replace the source powder, or a material with different thermal conductivity can replace the support material. Apart from the direct manipulation of materials, indirect manipulations are also a possibility. If properties such as temperature or humidity are manipulated during the storage or transportation, the source material properties could be modified. This is especially true for source materials used in human tissue and food and drug printing.
  - *Geometry*: In the case of source materials in the form of wire, the manipulations of geometry are limited to the wire diameter. In the case of a powder, the particle size, form factor and regularity can be modified without changing the chemical composition of the source material.

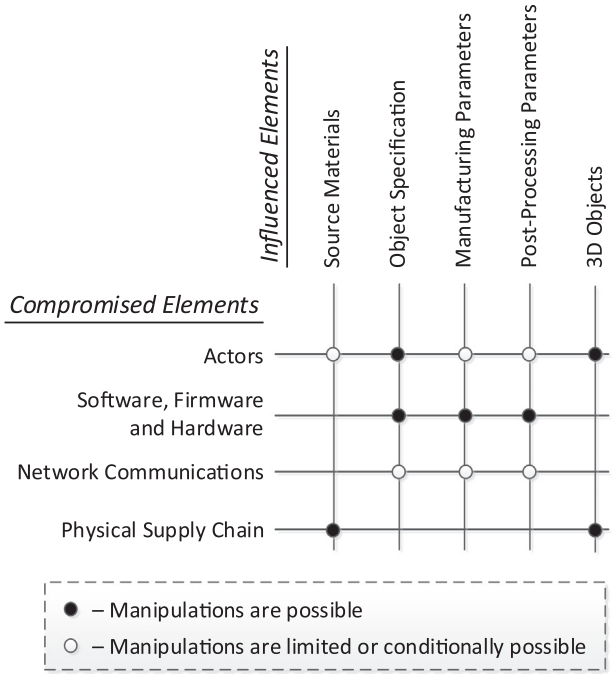


Fig. 3 – Compromised elements × manipulations.

- *Nuclear/Biological/Chemical Contamination*: A special category of source material manipulation is its contamination with hazardous nuclear, biological or chemical materials.
- *Explosives*: Another special category of source material manipulation is its mixture with flammable or explosive materials.

Note that the focus is not on the physical supply of altered components of additive manufacturing equipment such as circuit boards, motors and mechanical parts. This is an attack vector that can be used to compromise numerous elements of additive manufacturing equipment.

- **Object Specification:** Object specification usually involves the description of the object's 3D geometry. As mentioned above, the 3D geometry is commonly specified using the STL or AMF formats. But the object specification could also include mechanical properties, especially when the parts are used in a safety-critical system. Because STL and AMF files do not support the description of such information, it is usually provided in complementary documents (e.g., in the form of PDF files). The manipulation of object specification has various origins and motivations:
  - *Exploit*: A malicious actor can craft the object specification in order to compromise equipment at the 3D printer manufacturer's site. A network compromise can be used for this kind of manipulation. It is well-known that specially-crafted PDF files can exploit Adobe Acrobat and Adobe Reader vulnerabilities [49]; these files can be used to compromise the personal computer used for control. STL and AMF files have not yet been crafted to enable code injection into software or firmware, but such compromises are a distinct possibility.
  - *Nonconformity*: Deviations or nonconformities of a 3D object from the original specification include 3D geometry, size and object orientation during printing. The orientation is important because of the anisotropy of objects produced by additive manufacturing [2]. An adversary who has compromised network communications can manipulate STL or AMF files during their transmission. Malicious software running on the controller computer can send incorrect or modified control commands to the 3D printer. Malicious firmware or hardware in the 3D printer can change legitimate commands before their execution, or simply ignore them and execute commands based on the specification provided by the adversary.

The degree to which manipulation is possible depends on the malicious or compromised element of the additive manufacturing workflow. Malicious software, firmware and hardware can perform arbitrary modifications. Network communications, however, are often protected by encryption for privacy and/or message authentication codes for integrity. Therefore, manipulations of object specifications via compromised network communications may be feasible only when they are not protected or when the protection mechanisms have flaws that can be exploited.

- **Manufacturing Parameters:** The seven additive manufacturing processes defined by ASTM differ in how source materials are deposited and fused. This inevitably determines the manufacturing parameters that can be manipulated. A complete discussion of the topic is beyond the scope of this paper. However, some of the key manufacturing parameters in powder bed fusion include the thickness of the powder layer, energy of the heat source and melting pattern. Security-relevant manufacturing parameters that can be manipulated in additive manufacturing processes involving metals and alloys are discussed in [87]. Regardless of the manufacturing parameters, the following two categories of manipulations are based solely on their extent:
  - *Nonconformity*: The precision of the geometry of a 3D object and its mechanical properties depend on numerous manufacturing parameters [28,87]. A combination of manufacturing parameters is classified as nonconforming if at least one parameter is outside the range needed to produce a 3D object with the desired properties.
  - *Out of Operational Range*: Every system is designed to support parameter modification within specific operational ranges. The same applies to a 3D printer. A combination of manufacturing parameters is classified as being out of operational range if at least one parameter is outside the range for which the 3D printer was designed.

In general, nonconformity is independent of the operational ranges supported by additive manufacturing equipment. Several manufacturing parameters can be manipulated by compromised software, firmware, hardware or network communications. However, whereas nonconformity can be easily achieved by all these compromised elements, the second category of manipulations by compromised network communications or by software running on a controller computer are only conditionally achievable. The reason is that uncompromised firmware or hardware are likely to implement safety checks to prevent operations outside the supported parameter ranges. Similarly, malicious actors can be limited by firmware or hardware checks as well as by their own skill sets. Furthermore, in the case of the insider threat, physical and cyber access control can restrict the manipulations that an insider can perform accidentally or intentionally.

- **Post-Processing Parameters:** Similar considerations apply to post-processing. In the case of the hot isostatic pressing of metal parts, manipulations can involve the temperature and time of processing as well as the furnace temperature. Once again, the same two categories of manipulations exist:
  - *Nonconformity*: At least one post-processing parameter is outside the range needed to achieve the required part quality; however, none of the parameters are outside the operational range supported by the equipment.
  - *Out of Operational Range*: At least one post-processing parameter is outside the range for which the post-processing equipment was designed.

In this situation, compromised firmware or hardware can have unrestricted manipulation capabilities. Manipulations by compromised software or network communications can be limited by safety and security mechanisms integrated in

the firmware or hardware. The same mechanisms would also limit the manipulations performed by malicious actors. Physical and cyber access control measures would further restrict the manipulations performed by an insider either accidentally or maliciously.

- **3D Objects:** Numerous manipulations of a 3D object are possible between its production and final delivery. These manipulations are somewhat similar to those performed on source materials. The manipulations are only possible if the corresponding segments of the supply chain are compromised. The following categories of manipulations are possible:
  - *Physical Damage*: The manufactured object is damaged physically. Additionally, as in the case of the manipulations of source materials, indirect damage by manipulating environmental controls (e.g., temperature during transportation) can be very effective in the case of tissue and food and drug printing.
  - *Nuclear/Biological/Chemical Contamination*: The contamination of manufactured products with hazardous nuclear, biological or chemical materials is possible.

5.4. 3D printer as a weapon

The effects of manipulations and adversarial goals are both manifold, and the same is true for the intersection of these two sets. This section focuses on a subset of this intersection – the ability to misuse a 3D printer as a weapon (3D-PaaW). As mentioned in Section 5.1, this means that either physical damage occurs, or health and lives are endangered by a physical (kinetic) attack, nuclear, biological or chemical contamination, or a cyber attack.

This category of attacks is especially attractive to nation state adversaries and terrorist groups. However, the category is also attractive to criminal organizations, hacktivist groups, competitors and disgruntled individuals.

A two-level categorization is proposed for 3D printer as a weapon attacks. The top-level category specifies the target that is immediately affected by the attack. The sub-category describes the kind of impact on this target.

The following taxonomy is proposed:

- **3D Objects:** The properties of a manufactured object are altered in a manner that enables it to inflict damage. The damage varies based on how the object has been altered and on its application. Based on the source material used, category of manipulation and application area of the 3D object, the following sub-categories are identified:
  - *Physical Properties*: The physical properties (e.g., mechanical or biological) of the manufactured object can be altered. Any of the discussed manipulations can have an impact on the physical properties. The manner in which the physical properties are altered depends on numerous factors, including the application area, source material and additive manufacturing process. For example, changing the melting pattern in a powder bed fusion process can affect the mechanical properties of the metal part and changing the 3D-placement of cells can affect the biological properties of the printed tissue.
  - *Nuclear/Biological/Chemical Contamination*: An object could be contaminated during or after its production. The contamination of the source material may not always be effective. For example, volatile chemicals or biological materials are unlikely to survive the high temperatures in the powder bed fusion process.
  - *Electronic Circuits*: The ability to print or imprint electronics in a manufactured object opens the possibility of altering the 3D-printed electronic circuits. In particular, altering the object specification opens a broad variety of attacks that leverage the compromised electronics in a manufactured object. This includes the incorporation of hardware Trojans and side channels for information leakage. Note that the alteration of the object specification can be performed in advance by altering STL or AMF files or "on the fly" by malicious software, firmware or hardware Trojans (see the associated discussion in Section 5.3). Manipulations of the source materials and manufacturing parameters would have somewhat limited effects on electronics such as negatively impacting performance and increasing side-channel leakage. Moreover, unlike the manipulation of an object specification, a manipulation of source materials or the manufacturing process would not enable full control of the impact on the 3D-printed electronics component.
- **3D Printer:** In the context of the critical infrastructure, a major concern is the ability to inflict physical damage to an infrastructure by manipulating control parameters from the cyber domain. Stuxnet [25] and the Aurora experiment [69] illustrate the legitimacy of this concern. Clearly, additive manufacturing equipment that creates parts for infrastructure assets would itself be an attractive target. These attacks would produce the following categories of impacts:
  - *Reduced Lifetime*: Modifications to manufacturing parameters can increase the wear on additive manufacturing equipment components, reducing the lifetime of the equipment. The affected equipment components include motors as well as the mechanical parts moved by the motors. The manipulation of post-processing parameters can lead to similar effects. For example, manipulations of the pressure and temperature during the hot isostatic pressing process can reduce the lifetime of the high pressure vessel used by the process. Manipulations of the source materials (e.g., mixing source materials with solvents or flammable materials) can also increase equipment wear.
  - *Irreparable Damage*: In the reduced lifetime category, some components of the additive manufacturing equipment are damaged. However, in many instances, the costs involved in identifying and replacing the damaged components may render equipment repair economically infeasible. This situation also occurs when there are repeated and/or multiple component failures.
    Additionally, manipulations during the manufacturing process or post-processing can render additive manufacturing equipment irreparably damaged. In the case of 3D printers that work with metals, manipulation of the laser or electron beam targeting system can lead to uncontrollable flow of the source material and damage

to the containment chamber, leading to irreparable equipment damage. Similar effects can be achieved by manipulations of source materials. In the case of powder bed fusion, if the source material is replaced by material with a lower melting point, the resulting uncontrollable flow can irreparably damage the equipment. Manipulations of the object specification may also have a similar effect. However, the extent of the damage would depend on the safety mechanisms implemented in the equipment and its firmware to prevent printing outside the designated boundaries.

- *Explosion/Implosion*: Mixing highly flammable or explosive materials in the source materials can lead to an explosion during the manufacturing process. Similar effects can be achieved by manipulating the manufacturing and post-processing parameters. A high vacuum is needed when an electron beam is used as a heat source [3]; otherwise the beam of electrons is deflected and does not focus on the part. If the manufacturing parameters are adjusted to focus the beam on some other location such as the containment chamber, the damage to the chamber could lead to an implosion.
  A laser can operate effectively in a normal atmospheric environment. However, an inert gas (usually argon) is introduced in the containment chamber because metal powders (e.g., titanium and aluminum alloys) are often combustible. If the containment chamber is damaged and metal powder is exposed to the atmosphere, a fire or dust explosion could occur [55,56].

- **Environment:** Finally, the additive manufacturing environment (e.g., building) could be the target of a 3D printer as a weapon attack. The following categories of impacts are possible:
  - *Explosion/Implosion*: An explosion or implosion could damage additive manufacturing equipment as well as its surrounding environment, which includes the building that houses the equipment. In the case of the powder bed fusion process, an explosion or implosion could release combustible powder to the environment. A secondary explosion can be much more destructive than a primary explosion due to the increased quantity and concentration of dispersed combustible dust [55]. This can result in injuries, deaths and the destruction of the manufacturing facility [55].
  - *Fire*: A fire is a common secondary effect of an explosion or implosion. The extent of the fire depends on the presence of flammable materials in proximity to the explosion or implosion. Manipulations of source materials or manufacturing parameters can cause a fire without an explosion or implosion. For instance, the replacement of the plastic filaments used for printing with a flammable material could lead to a fire.
  - *Nuclear/Biological/Chemical Contamination*: Clearly, if the source materials or the manufactured 3D objects are contaminated, their immediate environments are also contaminated and the people in these environments are exposed to the hazardous materials. The manipulation of an additive manufacturing process could also release fine powder into the environment. Depending on the chemical content and particle size, the released powder could be classified as a hazardous material.

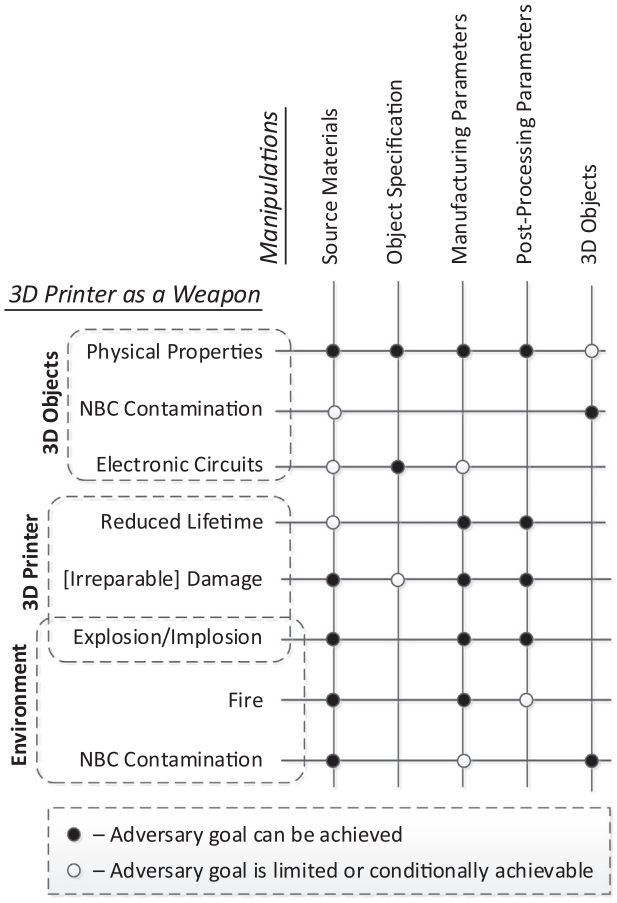


Fig. 4 – Manipulations × 3D printer as a weapon attacks.

Note that cyber attacks on additive manufacturing equipment and its environment are not mentioned in the 3D printer as a weapon categorization. While these attacks are possible, indeed likely, they are considered to be vectors (see Fig. 2) for compromising various elements of the additive manufacturing workflow.

Additionally, only individual uncoordinated attacks on/with additive manufacturing equipment are considered. It is conceivable that coordinated attacks could cause additional effects that would fall in the 3D printer as a weapon category. For example, a coordinated attack by multiple 3D printers could produce power surges that may result in an electric power outage.

Fig. 4 summarizes the 3D printer as a weapon attacks discussed above. Clearly, the attacks would lead to safety violations and generate numerous secondary effects, including possible effects in the physical, environmental, socio-economic and geopolitical domains.

6. 3D printer as a weapon characteristics

Different weapon types are characterized by different properties. For automatic weapons, the properties include precision and firing rate; for guided bombs, the properties include

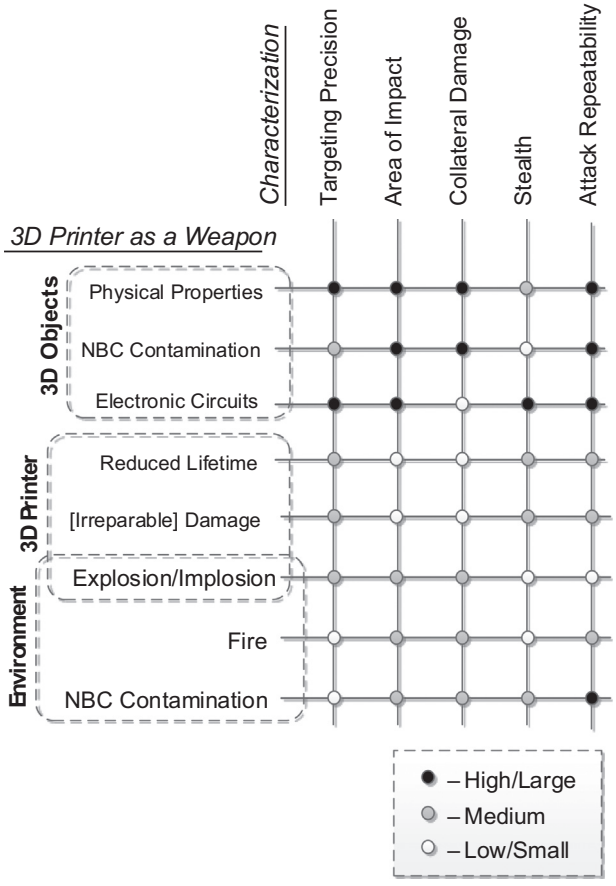


Fig. 5 – 3D printer as a weapon characteristics.

precision, penetration depth and explosion radius. Similar characteristics are needed for the weaponization of 3D printers.

The following taxonomy, which is summarized in Fig. 5, is proposed for 3D printers as weapons:

- **Targeting Precision:** Precision is an important characteristic of a weapon. It specifies the deviation from the desired target.
  - *3D Objects*: It is possible to achieve high targeting precision when manipulating 3D objects. When manipulations are made by malicious software, firmware or hardware, it is possible to identify the unique blueprint for the targeted 3D object and use it as a trigger for an attack. In the case of nuclear, biological or chemical contamination, however, the targeting precision depends on whether the source material or the manufactured object has been contaminated. In the former case, the precision is rather low and is limited to the source material manufacturer or a supply chain compromise actor. In the later case, the precision is very high, because it is possible to target a single manufactured part created for a specific customer.
  - *3D Printer*: When additive manufacturing equipment is targeted, the achievable precision is medium. Focus on the manufacturer's site can be achieved, but it would be barely possible to distinguish between identical additive manufacturing systems that are headed to different customers.
  - *Environment*: The ability to precisely target an additive manufacturing environment is rather low. This is because the adversary cannot control the environment, including its changes over time and the presence of personnel at a particular location at a particular time.
- **Area of Impact:** Another important characteristic is the ability of an attack to impact a broad area.
  - *3D Objects*: When manufactured functional parts are manipulated, the area of impact is very large. This is because the parts would be used as functional components in numerous, potentially, safety-critical systems and devices across the critical infrastructure.
  - *3D Printer*: When additive manufacturing equipment is targeted, the area of impact is small because it is localized to a single piece of equipment. The only exception is in the case of an explosion or implosion, which could also impact the immediate environment.
  - *Environment*: An attack on the environment would have a medium area of impact. The impact would be confined to the manufacturing site and, at most, its immediate neighborhood.
- **Collateral Damage:** Collateral damage is an important property of a weapon. It is a measure of the magnitude to which the weapon impacts unintended targets (systems, humans and environment).
  - *3D Objects*: The collateral damage produced by the manipulation of a manufactured 3D object depends on the type of the manipulation. When electronic circuits are manipulated, it is possible to control the conditions under which an attack is performed (e.g., by introducing a complex trigger). When physical (e.g., mechanical) properties are manipulated or a 3D object is contaminated, the collateral damage can extend to any system or person that uses the manufactured object as well as the environment in which the object is used.
  - *3D Printer*: When additive manufacturing equipment is targeted, the collateral damage is rather low because the damage is contained to the affected equipment. However, in the case of an explosion or implosion, the immediate environment may also be affected.
  - *Environment*: Fire and contamination generate a medium amount of collateral damage. The damage would be confined to the manufacturing site and, at most, its immediate neighborhood.
- **Stealth:** A weapon is stealthy if it is not detected immediately or if its effects are not necessarily attributed to the weapon.
  - *3D Objects*: The manipulation of the physical properties of a manufactured object can go undetected for an extended period of time. However, in the case of an airplane crash, it is a common practice to ground the particular type of airplane and to perform a thorough investigation of the incident and its cause. Such an investigation would likely discover that the physical properties of the object were modified. Therefore, the level of stealth of the manipulation would be medium. The stealth level of nuclear, biological or chemical contamination would be even lower because they would

be easier to detect. The modification of electronics, however, could go undiscovered for an extended period of time, until the device is triggered and the incident is investigated.

- *3D Printer*: As Stuxnet has shown, the reduction in equipment lifetime and damage can go undetected or be attributed to other reasons for an extended period of time. However, after recurring problems are noticed, a thorough investigation would eventually discover the attack. An explosion or implosion would immediately trigger a comprehensive investigation.
- *Environment*: A fire, like an explosion or implosion, would be detected almost immediately. Thus, the level of stealth of an attack would be low. Detection of environmental contamination, however, would depend on the sensors installed at the manufacturing site. If sensors for certain types of contamination are not installed, then the attack could go undiscovered until health problems or some other anomalies trigger an investigation.

- **Attack Repeatability:** A weapon is also characterized by its potential to be used multiple times.
  - *3D Objects*: Clearly, an attack on a 3D object could be replicated for numerous produced parts.
  - *3D Printer*: Assuming that the compromised element is not damaged by the attack itself, an attack that reduces equipment lifetime or causes equipment damage can be repeated over and over again. However, the attacks are limited to the period when the equipment is in use. An attack that causes an explosion or implosion or some other irreparable damage to additive manufacturing equipment would be a one-time attack.
  - *Environment*: Unless a fire irreparably damages the additive manufacturing equipment or the attack that caused the fire is discovered, the attack would be repeatable. The same holds true for an attack that contaminates the environment.

Note that only individual uncoordinated attacks on/with additive manufacturing equipment have been considered. In the case of coordinated attacks, the 3D printer as a weapon attack categories and their characteristics would require extensions to account for the multiple attacks and the coordination involved in conducting the attacks.

7. Conclusions

Additive manufacturing or 3D printing is a transformative technology that will play a significant role in the critical manufacturing sector. However, the tremendous market potential, along with the economic, geopolitical and other implications of additive manufacturing, will inevitably draw the attention of a number of adversaries, from individuals to nation state actors.

This paper has mapped the landscape of attacks on or with 3D printers that could produce physical impacts. Because these attacks could inflict physical damage as well as injuries and deaths, they are referred to as attacks that use a 3D printer as a weapon. Taxonomies have been specified for the elements of the additive manufacturing workflow that can be compromised, for the manipulations that the compromised elements can exercise and for the 3D printer as a weapon subset of attacks that reside in the intersection of adversarial goals and effects achievable by the manipulations. Additionally, numerous possible examples of 3D printer as a weapon attacks have been detailed.

The attacks presented in this paper are primarily hypothetical and their validity requires experimental confirmation or reports from the real world. Regardless, given the great potential for harm, hypothetical and real 3D printer as a weapon attacks must be cataloged and analyzed to better understand their nature and scope.

It is hoped that the taxonomies presented in this paper will stimulate serious research on the security aspects of additive manufacturing. Additive manufacturing is a promising – but extremely dangerous – technology. It is imperative that the research and vendor communities focus more intensely on the development of defensive strategies and mechanisms as well as approaches for mitigating the potentially serious effects that could occur when 3D printers are used as weapons.

Note that the opinions and conclusions expressed in this paper are those of the authors. They do not necessarily represent the opinions or positions of the BICES Group Executive or its members.

Acknowledgements

The authors wish to thank Angela Jordan for helping edit the original manuscript.

REFERENCES

[1] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, Trojan detection using IC fingerprinting, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 296–310, 2007.

[2] S. Ahn, M. Montero, D. Odell, S. Roundy and P. Wright, Anisotropic material properties of fused deposition modeling ABS, *Rapid Prototyping Journal*, vol. 8(4), pp. 248–257, 2002.

[3] Arcam, Electron Beam Melting – in the Forefront of Additive Manufacturing, Molndal, Sweden (arcam.com/technology/electron-beam-melting), 2014.

[4] A. Avizienis, J. Laprie, B. Randell and C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing*, vol. 1(1), pp. 11–33, 2004.

[5] A. Bagsik, V. Schoppner and E. Klemp, FDM part quality manufactured with Ultem*9085, *Proceedings of the Fourteenth International Scientific Conference on Polymeric Materials*, 2010.

[6] B. Berman, 3-D printing: The new industrial revolution, *Business Horizons*, vol. 55(2), pp. 155–162, 2012.

[7] S. Bradshaw, A. Bowyer and P. Haufe, The intellectual property implications of low-cost 3D printing, *ScriptEd*, vol. 7(1), pp. 5–31, 2010.

[8] E. Byres and J. Lowe, The myths and facts behind cyber security risks for industrial control systems, *Proceedings of the VDE Kongress*, 2004.

[9] T. Campbell and O. Ivanova, Additive manufacturing as a disruptive technology: Implications of three-dimensional printing, *Technology and Innovation*, vol. 15, pp. 67–79, 2013.

[10] T. Campbell, C. Williams, O. Ivanova and B. Garrett, Could 3D Printing Change the World? Technologies, Potential and Implications of Additive Manufacturing, Atlantic Council, Washington, DC, 2011.
[11] A. Chakrabarti and G. Manimaran, Internet infrastructure security: A taxonomy, *IEEE Network*, vol. 16(6), pp. 13–21, 2002.
[12] 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.
[13] S. Checkoway, L. Davi, A. Dmitrienko, A. Sadeghi, H. Shacham and M. Winandy, Return-oriented programming without returns, *Proceedings of the Seventeenth ACM Conference on Computer and Communications Security*, pp. 559–572, 2010.
[14] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, Comprehensive experimental analyses of automotive attack surfaces, *Proceedings of the Twentieth USENIX Conference on Security*, 2011.
[15] K. Collins, L'Oreal is 3D printing its own human skin to test cosmetics, *Wired*, May 19, 2015.
[16] Cornell Creative Machines Lab, Standard Specification for Additive Manufacturing File Format (Draft F XXXX-10), Cornell University, Ithaca, New York (creativemachines.cornell.edu/sites/default/files/AMF_V0.47.pdf), 2014.
[17] S. Dadbakhsh and L. Hao, Effect of layer thickness in selective laser melting on microstructure of Al/5 wt.%Fe_2O_3 powder consolidated parts, *Scientific World Journal*, vol. 2014, article id. 106129, 2014.
[18] K. Dempsey and C. Paulsen, Risk Management for Replication Devices, NISTIR 8023, National Institute of Standards and Technology, Gaithersburg, Maryland, 2015.
[19] DUS Architects, 3D PRINT Architecture, Amsterdam, The Netherlands (www.dusarchitects.com), 2014.
[20] S. East, J. Butts, M. Papa and S. Shenoi, A taxonomy of attacks on the DNP3 protocol, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 67–81, 2009.
[21] Electronic Industries Association, Interchangeable Variable Block Data Format for Positioning, Contouring and Contouring/Positioning Numerically Controlled Machines, EIA Standard RS-274-D, Washington, DC, 1980.
[22] Episkin, RHE SkinEthic, Lyon, France (www.episkin.com/RHE.asp), 2015.
[23] ESET, ACAD/Medre.A, 10000's of AutoCAD Designs Leaked in Suspected Industrial Espionage, San Diego, California (www.welivesecurity.com/media_files/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf), 2015.
[24] European Powder Metallurgy Association, Additive Manufacturing Technology, Shrewsbury, United Kingdom (epma.com/additive-manufacturing-technology), 2014.
[25] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.
[26] L. Forbes, H. Vu, B. Udrea, H. Hagar, X. Koutsoukos and M. Yampolskiy, SecureCPS: Defending a nanosatellite cyber-physical system, *Proceedings of the SPIE*, vol. 9085, 2014.
[27] J. Foust, SpaceX unveils its "21st century spaceship," *NewSpace Journal* (www.newspacejournal.com/2014/05/30/spacex-unveils-its-21st-century-spaceship), May 30, 2014.
[28] W. Frazier, Metal additive manufacturing: A review, *Journal of Materials Engineering and Performance*, vol. 23(6), pp. 1917–1928, 2014.
[29] General Electric, Hardware meets software in advanced manufacturing, Fairfield, Connecticut (www.ge.com/stories/hardware-meets-software-advancedmanufacturing), 2015.
[30] I. Gibson, D. Rosen and B. Stucker, *Additive Manufacturing Technologies: Rapid Prototyping to Direct Digital Manufacturing*, Springer, New York, 2010.
[31] S. Hansman and R. Hunt, A taxonomy of network and computer attacks, *Computers and Security*, vol. 24(1), pp. 31–43, 2005.
[32] D. Helbing, Globally networked risks and how to respond, *Nature*, vol. 497(7447), pp. 51–59, 2013.
[33] J. Hicks, FDA approved 3D printed drug available in the US, *Forbes*, March 22, 2016.
[34] 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.
[35] S. Huang, P. Liu, A. Mokasdar and L. Hou, Additive manufacturing and its societal impact: A literature review, *International Journal of Advanced Manufacturing Technology*, vol. 67 (5–8), pp. 1191–1203, 2013.
[36] P. Huitsing, R. Chandia, M. Papa and S. Shenoi, Attack taxonomies for the Modbus protocols, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.
[37] S. Kelly and S. Kampe, Microstructural evolution in laser-deposited multilayer Ti-6Al-4V builds: Part I; Microstructural characterization, *Metallurgical and Materials Transactions A*, vol. 35(6), pp. 1861–1867, 2004.
[38] S. Kelly and S. Kampe, Microstructural evolution in laser-deposited multilayer Ti-6Al-4 V builds: Part II; Thermal modeling, *Metallurgical and Materials Transactions A*, vol. 35(6), pp. 1869–1879, 2004.
[39] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, Experimental security analysis of a modern automobile, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.
[40] T. Krol, M. Zah and C. Seidel, Optimization of supports in metal-based additive manufacturing by means of finite element models, *Proceedings of the International Solid Freeform Fabrication Symposium*, 2012.
[41] 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.
[42] J. Laprie, Dependable computing and fault-tolerance: Concepts and terminology, *Proceedings of the Fifteenth International Symposium on Fault Tolerant Computing*, pp. 2–11, 1985.
[43] H. Lipson, AMF tutorial: The basics (Part 1), 3D Printing and Additive Manufacturing, vol. 1(2), pp. 85–87, 2014.
[44] B. Liu, R. Wildman, C. Tuck, I. Ashcroft and R. Hague, Investigation of the effect of particle size distribution on processing parameters optimization in the selective laser melting process, *Proceedings of the International Solid Freeform Fabrication Symposium*, pp. 227–238, 2011.
[45] J. Luimstra, Star Trek inspires Nestle to work on personalized nutrition project, 3DPrinting.com (3dprinting.com/news/star-trek-inspires-nestle-workpersonalized-nutrition-project), June 25, 2014.
[46] 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.
[47] E. Malone and H. Lipson, Freeform fabrication of electroactive polymer actuators and electromechanical devices, *Proceedings of the Fifteenth Solid Freeform Fabrication Symposium*, pp. 697–708, 2004.
[48] D. Manfredi, F. Calignano, M. Krishnan, R. Canali, E. Ambrosio and E. Atzeni, From powders to dense metal parts: Characterization of a commercial AlSiMg alloy processed

through direct metal laser sintering, *Materials*, vol. 6(3), pp. 856–869, 2013.
[49] Microsoft, Microsoft Security Intelligence Report, Volume 18, July through Deecember 2014, Redmond, Washington, 2015.
[50] J. Mirkovic and P. Reiher, A taxonomy of DDoS attacks and DDoS defense mechanisms, *ACM SIGCOMM Computer Communication Review*, vol. 34(2), pp. 39–53, 2004.
[51] National Aeronautics and Space Administration, 3D Printing: Food in Space, Washington, DC (www.nasa.gov/directorates/spacetech/home/feature_3d_food.html#.V1IdJpErKhd), 2013.
[52] National Defense Industrial Association, Cybersecurity for Advanced Manufacturing, White Paper, Arlington, Virginia, 2014.
[53] National Institute of Standards and Technology, Measurement Science Roadmap for Metal-Based Additive Manufacturing, Workshop Summary Report, Gaithersburg, Maryland, 2013.
[54] Natural Machines, Foodini – A 3D food printer, Barcelona, Spain (www.naturalmachines.com), 2015.
[55] Occupational Safety and Health Administration, Hazard Alert: Combustible Dust Explosions, OSHA Fact Sheet, DSG 12/2014, Washington, DC (www.osha.gov/OshDoc/data_General_Facts/OSHAcombustibledust.pdf), 2014.
[56] Office of Public Affairs, After explosion, U.S. 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, OSHA Regional News Release, Department of Labor, Washington, DC, May 20, 2014.
[57] Organovo, Structurally and functionally accurate bioprinted human tissue models, San Diego, California (www.organovo.com), 2015.
[58] D. Periard, E. Malone and H. Lipson, Printing embedded circuits, *Proceedings of the Eighteenth Solid Freeform Fabrication Symposium*, pp. 503–512, 2007.
[59] R. Rad, X. Wang, M. Tehranipoor and J. Plusquellic, Power supply signal calibration techniques for improving detection resolution of hardware Trojans, *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, pp. 632–639, 2008.
[60] G. Ram, Y. Yang and B. Stucker, Effect of process parameters on bond formation during ultrasonic consolidation of aluminum alloy 3003, *Journal of Manufacturing Systems*, vol. 25(3), pp. 221–238, 2006.
[61] S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady, Security in embedded systems: Design challenges, *ACM Transactions on Embedded Computing Systems*, vol. 3(3), pp. 461–491, 2004.
[62] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.
[63] R. Roemer, E. Buchanan, H. Shacham and S. Savage, Return-oriented programming: Systems, languages and applications, *ACM Transactions on Information and System Security*, vol. 15(1), article no. 2, 2012.
[64] C. Schade, T. Murphy and C. Walton, Development of Atomized Powders for Additive Manufacturing, Hoeganaes Corporation, Cinnaminson, New Jersey (www.gkn.com/hoeganaes/media/Tech%20Library/Schadeade-Atomized%20Powders%20for%20Additive%20Manufacturing%20(1).pdf), 2014.
[65] Science in Public, The world's first printed jet engine, Melbourne, Australia (www.scienceinpublic.com.au/mediareleases/monash-avalonairshow-2015), February 26, 2015.
[66] J. Slay and M. Miller, Lessons learned from the Maroochy water breach, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 73–82, 2007.
[67] A. Sternstein, Things can go kaboom when a defense contractor's 3-D printer gets hacked, *Nextgov*, September 11, 2014.
[68] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vunerabilities in additive manufacturing systems, *Proceedings of the Twenty-Fifth International Solid Freeform Fabrication Symposium*, 2014.
[69] 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.
[70] A. Tarantola, DARPA to develop best practices for 3D printing, *Engadget* (www.engadget.com/2015/05/31/darpa-to-develop-best-practicesfor-3d-printing), May 31, 2015.
[71] TeVido BioDevices, About Us, Austin, Texas (tevidobiodevices.com/about-us), 2015.
[72] D. Thomas, Economics of the U.S. Additive Manufacturing Industry, NIST Special Publication 1163, National Institute of Standards and Technology, Gaithersburg, Maryland, 2013.
[73] D. Thomas and S. Gilbert, Costs and Cost Effectiveness of Additive Manufacturing, NIST Special Publication 1176, National Institute of Standards and Technology, Gaithersburg, Maryland, 2014.
[74] Voxel8, The world's first 3D electronics printer, Somerville, Massachusetts (www.voxel8.co), 2015.
[75] J. Wakefield, First 3D-printed pill approved by U.S. authorities, *BBC News*, August 4, 2015.
[76] F. Wang, S. Williams, P. Colegrove and A. Antonysamy, Microstructure and mechanical properties of wire and arc additive manufactured Ti-6Al-4V, *Metallurgical and Materials Transactions A*, vol. 44(2), pp. 968–977, 2013.
[77] M. Weinberg, It will be awesome if they don't screw it up: 3D printing, intellectual property and the fight over the next great disruptive technology, Public Knowledge, Washington, DC (www.publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf), 2010.
[78] D. Welch and S. Lathrop, Wireless security threat taxonomy, *Proceedings of the IEEE SMC Information Assurance Workshop*, pp. 76–83, 2003.
[79] L. Wells, J. Camelio, C. Williams and J. White, Cyber-physical security challenges in manufacturing systems, *Manufacturing Letters*, vol. 2(2), pp. 74–77, 2014.
[80] Wohlers Associates, Wohlers Report 2015, Fort Collins, Colorado, 2015.
[81] M. Wolf, M. Minzlaff and M. Moser, Information technology security threats to modern e-enabled aircraft: A cautionary note, *Journal of Aerospace Information Systems*, vol. 11(7), pp. 447–457, 2014.
[82] 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 no. 7, 2014.
[83] 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.
[84] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, Systematic analysis of cyber-attacks on the CPS-evaluating applicability of the DFD-based approach, *Proceedings of the Fifth International Symposium on Resilient Control Systems*, pp. 55–62, 2012.
[85] 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.
[86] 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.

[87] 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.

[88] B. Zhu, A. Joseph and S. Sastry, A taxonomy of cyber attacks on SCADA systems, *Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing*, pp. 380–388, 2011.