Security Challenges of Additive Manufacturing with Metals and Alloys

Mark Yampolskiy, Lena Schutzle, Uday Vaidya, Alec Yasinsac

Chapter 11

SECURITY CHALLENGES OF ADDITIVE MANUFACTURING WITH METALS AND ALLOYS

Mark Yampolskiy, Lena Schutzle, Uday Vaidya and Alec Yasinsac

Abstract Cyber-physical systems are under constant and increasing attacks as components of the critical infrastructure. Additive manufacturing systems are a new class of cyber-physical systems that produce three-dimensional objects layer by layer. Agencies and companies such as NASA, the European Space Agency, General Electric and SpaceX have explored a broad range of application areas for additive manufacturing, including creating functional parts of safety-critical systems such as jet engines. The range of application areas and dependence on computerization makes additive manufacturing an attractive target for attackers.

This chapter focuses on attacks that seek to change the physical properties of additive-manufactured components. Such attacks can weaken, damage or destroy manufactured components and, in scenarios where weak or damaged components are used in safety-critical systems, potentially endanger human lives. Attacks intended to damage additive manufacturing equipment and additive manufacturing environments are also discussed.

Keywords: Additive manufacturing, 3D printing, threats, risks

1. Introduction

Cyber-physical systems are under constant and increasing attack. Examples encountered "in the wild" as well as those considered in the research literature include attacks on industrial control systems [5, 14, 25, 44], automobiles [7, 23] and unmanned vehicles [16, 53].

Additive manufacturing, also known as additive layer manufacturing, solid freeform fabrication and, perhaps most commonly, 3D printing, employs an important class of cyber-physical systems that produce 3D objects. Unlike a traditional subtractive manufacturing process, in which a mold is poured or a solid block of a material is reduced via milling and turning to a desired form,

additive manufacturing creates 3D objects by adding thin layers one at a time to gradually build up an object from two dimensions to three dimensions and, ultimately, to the desired form [50].

The market penetration of additive manufacturing as a manufacturing technology has tremendous potential. The reasons include technical and economic advantages such as just-in-time and on-demand production, the ability to manufacture components closer to assembly lines, shorter design-to-product time and, especially, the ability to produce functional parts with complex internal structures and with complex (task-specific) physical properties. In 2014, Wohlers Associates [50] reported that the additive manufacturing industry had a total revenue of $4.1 billion, with 29% of all manufactured objects used as functional parts. According to NIST reports [46, 47], additive manufacturing revenue will rise to about $50 billion between 2029 and 2031.

However, the economical, geopolitical and other implications of additive manufacturing technology [6] will inevitably draw the attention of adversaries ranging from malicious individuals to state actors. As research in the area of critical infrastructure protection has revealed, attacks will often seek to achieve physical impacts via cyber means [14, 20, 40, 44, 55]. In the case of additive manufacturing, the attacks would likely translate to physical impacts on the manufactured 3D objects, especially in cases where the objects are used as functional parts of safety-critical systems such as jet engines.

This chapter presents a qualitative analysis of attacks that can be executed on additive manufacturing equipment that works with metals and alloys. Special attention is directed at attacks that change the physical properties of additive-manufactured components. Such attacks can contribute to weak and unreliable components and, in scenarios where these components are used in safety-critical systems, endanger human lives. Attacks intended to damage additive manufacturing equipment and additive manufacturing environments are also discussed.

2. Related Work

Very little research has focused on the security aspects of additive manufacturing. However, a growing body of research discusses the impact of 3D printing, including its socioeconomic [6, 22, 38, 39], geopolitical [6, 33] and environmental [10, 34] aspects. These impacts can motivate a variety of adversaries ranging from malicious individuals to state-sponsored actors and nation states.

Two security threat categories are associated with additive manufacturing [52]: (i) intellectual property theft; and (ii) physical (i.e., kinetic) damage. Recent articles have shown that there is a growing awareness of intellectual property violations in the context of additive manufacturing [4, 49, 51]. However, literature research reveals that the second threat category has not been considered adequately. The only notable exception is the possibility of a 3D printer exploding due to mismanagement [45], which actually occurred in November 2013 at Powderpart Inc. [36]. There is, however, a significant body of

literature in materials science and mechanical engineering that provides a basis for analyzing attacks that can inflict physical damage by altering the physical properties of manufactured 3D objects.

The American Society for Testing and Materials (ASTM) International Committee F42 on Additive Manufacturing Technologies has approved a list of seven additive manufacturing process categories [50]. Three of the seven processes are suitable for fusing metals and alloys, materials that are commonly used in safety-critical applications: powder bed fusion, directed energy deposition and sheet lamination [15, 27, 37, 50]. All these processes are strongly dependent on computer control and automation. Depending on the chosen additive manufacturing technique, various manufacturing process parameters can influence the quality of manufactured parts. This section outlines the basic principles of the three additive manufacturing processes. The next section discusses the manufacturing parameters that affect the quality of the produced 3D objects.

In the powder bed fusion process, a layer of material (usually metal or polymer) in powder form is distributed in a chamber. A heat source, typically a laser or electron beam, is then used to selectively melt and fuse regions of the powder bed, thus producing a slice of the 3D object [50]. This process involving powder distribution and melting is repeated layer by layer.

In the directed energy deposition process, wire or powder is distributed via a nozzle [19, 26, 32]. Focused thermal energy, typically produced by a laser, melts and fuses the source material during its deposition [50].

In the sheet lamination process, thin sheets of metal or fiber-reinforced composites are bonded by compressive force and ultrasonic energy supplied by a rolling sonotrobe [18, 50]. A complex 3D part is then created by cutting the fused sheets of metal or composite lamina according to the desired shapes of the layers.

3. Additive Manufacturing Threat Surface

This section discuss two aspects of attacks involving 3D printers: (i) attack vectors (i.e., how attacks can be launched); and (ii) changes to additive manufacturing process parameters that impact the physical properties of manufactured objects or even damage the additive manufacturing equipment itself. Although the additive manufacturing attack vectors have a significant overlap with traditional cyber attack vectors, several new attack vectors are unique to the additive manufacturing domain. Note that the types of adversaries and their motivation and business models are outside the scope of this research, although they are very important to understand.

3.1 Attack Vectors

Attack vectors should be analyzed in the context of the additive manufacturing workflow. Any actor in the workflow can be malicious and may compromise or circumvent communications channels.

Additive manufacturing equipment is usually obtained from dedicated manufacturers. In 2014, 49 manufacturers in thirteen countries produced and sold industrial-grade additive manufacturing equipment and hundreds of small companies sold desktop 3D printers [50]. The manufacturers, third-party companies and the user community develop and provide software and firmware that execute in the embedded controllers of additive manufacturing equipment as well as in the personal computers (control computers) that are used to submit manufacturing jobs. The control computers are also used to apply firmware updates to additive manufacturing equipment. The specification of a 3D object is provided using the Surface Tessellation Language (STL) [21] or the Additive Manufacturing File (AMF) format [1, 8, 28, 29], both of which specify "sliced" versions of a computer-aided design (CAD) model of the 3D object to be manufactured. Based on the 3D object description stored in an STL or AMF file, the control computer sends commands to the 3D printer that creates the specified object (e.g., positioning the build platform and nozzle, and adjusting the platform temperature). These commands are usually encoded in G-code [11], a language commonly used in computer-aided manufacturing (CAM).

- **Supply Chain Attacks:** Protecting against supply chain attacks is extremely challenging and expensive. Since software and hardware and the tools used for their design and development are commonly provided by third parties, it is impossible to guarantee that they are free from malicious content [48]. In the context of additive manufacturing, supply chain attacks can alter the hardware, firmware and software used in 3D printers and control computers. For example, hardware Trojans, backdoors and other malware can be embedded in 3D printers and control computers, enabling adversaries to alter manufacturing process parameters. Also, modifications of the tools used in additive manufacturing (e.g., to generate STL files) are categorized as supply chain attacks.

  Two types of supply chain attacks on additive manufacturing systems are not encountered in the cyber domain. One category of attacks involves the manipulation of physical components (e.g., mechanical parts used to distribute powder, motors used to move mechanical parts and heat sources); obviously, such attacks can have tremendous effects on the manufactured 3D objects. The second category includes attacks that target the production and distribution of source materials; these attacks result in different properties (e.g., composition, size, form factor and/or consistency) of the materials used in additive manufacturing. These two types of supply chain attacks cause physical manipulations that generally have more serious ramifications than typical cyber attacks.

- **Software and Firmware Updates:** Attacks on software and firmware updates are supply chain attacks that deserve special consideration and treatment. The updates, which are commonly used to fix bugs and vulnerabilities as well as to incorporate new features, can themselves introduce new bugs and vulnerabilities, and may even contain malware. Malicious

updates can enable adversaries to manipulate a range of additive manufacturing parameters, affecting the manufacturing processes and, consequently, the physical properties of the manufactured objects. Because of their embedded nature, firmware updates are most commonly updated via device-to-device connections. Vendors distribute updates on media that are directly connected to the equipment by a trusted party in the additive manufacturing environment. Malicious updates can be passed by a malicious supplier that delivers malware as a component of a legitimate update, by a malicious entity that delivers an update that masquerades as a legitimate update, or by a malicious insider with physical access to the device who uses the update facility to install unauthorized firmware.

- **Code Injection:** It has been demonstrated over and over again that program bugs in third-party software can be exploited, as in the case of PDF files and viewers. Although the STL/AMF (and ASCII and binary) file formats are very simple, there is no guarantee that additive manufacturing devices have bugs that cannot be exploited by specially-crafted STL/AMF or other files. These bugs can enable the injection and execution of arbitrary code in additive manufacturing equipment. In fact, code injection attacks on additive manufacturing equipment would be expected to be very common because of the exposure of the equipment to STL and other files submitted by customers.

- **Modification of 3D Models:** Whereas the previously-described attack vectors compromise additive manufacturing equipment and, thus, affect selected or all manufacturing jobs, more targeted attacks are also possible. An important category of attacks are those that modify 3D models. An STL file specifies the geometric properties of an object that is to be manufactured. It also defines how the object should be manufactured, layer by layer; as such, it specifies the orientations involved during manufacturing. Modifications of the internal form (e.g., by creating internal cavities that are larger or smaller than designed, and changing the manufacturing orientation) can be hard to detect, but can have a significant impact on the physical (mechanical) properties of the manufactured object. Like a supply chain attack, the modifications can be performed by a malicious entity in the chain between the customer who designs the 3D object model and the additive manufacturing service provider that creates the object. Such attacks are commonly referred to as man-in-the-middle attacks.

- **Manufacturing Process Specification:** A scenario in which the specifications of manufacturing processes come from third parties is certainly futuristic. However, as discussed in [51], this would create new business opportunities and specialization models for different companies. At the same time, this would create an additional attack vector. Just like the modification of an object model, the modification of a manufactur-

ing process specification would have direct implications on the physical properties of the manufactured objects.

It is clear that the attack vectors determine which attacks are possible. It is also obvious that different attack vectors can be used to launch the same type of attack. For example, multiple attack vectors can affect additive manufacturing parameters in the same way, resulting in the same impact on the manufactured objects.

3.2 Impact of Manufacturing Parameters

Successful attacks can exercise various influences on a manufacturing process. The attack vector determines the possible influences and their impacts on a manufactured 3D object as well on the additive manufacturing equipment. The exact relationship between the influence on the manufacturing process and the impact on the 3D object is extremely complex and depends on multiple parameters. The following qualitative causal relationships involving manufacturing parameters have been derived by analyzing the materials science and mechanical engineering literature related to additive manufacturing.

- **3D Shape:** Probably the most straightforward influence on an additive manufacturing process is a change in the specification of an object, especially its 3D shape. A particular customer or manufacturer could be targeted via a man-in-the-middle attack that intercepts and changes an STL or AMF file as it is transmitted from the customer to the manufacturer. On a broader scale, if the software, firmware or hardware of a 3D printer or control computer have been compromised, then changes to the 3D object description can be performed "on the fly." Modifications to 3D modeling and/or STL/AMF file generation tools have similar impacts.

  Modifications to the shape of an object can have various consequences. The most profound, albeit easy to detect, is a change to the external shape or size of a 3D object. If the manufactured object is a functional part of a complex device (e.g., jet engine), a change to its external shape or size can prevent its integration. One of the biggest advantages of additive manufacturing is its ability to produce objects with complex internal shapes (e.g., with custom shaped cavities) that reduce weight and save source material while ensuring the required structural properties. An attack that changes the shapes and/or sizes of the internal cavities can affect the weight of a 3D object and even its physical properties, affecting the reliability of the device. Furthermore, the exact size, location and form of a cavity can have an immediate impact on various physical properties, including resistance to mechanical and thermal exposure. These properties can greatly affect the lifetime of the functional part as well as that of the entire device.

- **Manufacturing Orientation:** Tensile tests reveal that the material used to manufacture 3D objects exhibits anisotropy – this means that

the mechanical properties of a 3D object depend on its orientation when it was printed. An attack that rotates the description of a 3D object (e.g., 90 degrees around an axis) can significantly impact its mechanical properties. Compared with the more obvious changes to the shape or size of an object, a change in the object orientation is much harder to discern. Such an attack can impact the lifetime of the object (e.g., jet engine) and, by extension, the reliability of the larger system in which the object is used (e.g., airplane).

- **Powder Deposition:** When a powder bed fusion process is used, an attack can influence the thickness of the powder layer by manipulating the height of the build platform. To some extent, the thickness of the powder layer is also affected by the height of the powder dispenser platform. Furthermore, a manipulation of the distribution mechanism that levels the powder layer can create irregularities in powder layer thickness. Powder layer thickness has a strong impact on the microstructure. If the thickness of each layer is increased by a constant amount, the exterior dimensions and proportions of the manufactured object are affected. As in the case of a modification to the 3D object specification in an STL or AMF file, this attack can affect the ability to integrate the part in a complex device. Fortunately, the modifications are easily detected by taking measurements of the 3D object. In a more complex attack scenario, the thicknesses of the layers can be varied so that the exterior measurements do not exceed a threshold, which means that the changes would remain undetected even by a sophisticated tool such as a coordinate measuring machine. The varying thicknesses would almost certainly change the object microstructure, affecting the physical properties of the object and the larger device of which it is a component.

- **Wire Feed Speed:** The speed of the heat source in a powder bed process and both the speed of the wire feed and the heat source in a directed energy deposition process affect the quality and the degree of bonding of adjacent layers of material. If the wire feed system (nozzle) runs too fast, the material does not fuse or does not fuse properly due to the lower temperature. On the other hand, the quality of an object may be affected negatively if the heat source moves too slowly. In this case, some portions of an object would be exposed to higher temperature gradients than other portions, which would lead to an uneven microstructure and possibly high pore density. Moreover, the speed of the wire feed system influences the amount of the deposited material. This, in turn, influences the manufactured precision of the 3D object and may render the object non-compliant with the customer's specification.

- **Targeting and Positioning System:** In the directed energy deposition and powder bed fusion processes, a laser or an electron beam target the spot where the source material is supposed to melt (with the help of a scanning mirror in the case of the laser). In the directed energy

deposition process, the nozzle and the build platform must be positioned properly in order to add a new droplet at the correct location. In some cases, the build platform moves relative to the nozzle (four- or five-axis-movements). Regardless of which nozzle deposition technology is used, the manipulation of the targeting or positioning systems would have an immediate impact on the shape and precision of the manufactured object. Furthermore, if a particular area is targeted by the heat source for an extended period of time, the resulting melting and uncontrollable material flow could significantly impact the precision as well as the microstructure of the manufactured object.

In an extreme case, selective heat source targeting can damage the additive manufacturing equipment. Furthermore, using a laser or an electron beam as a heat source requires the chamber to contain an inert gas or a high vacuum, respectively [2]; therefore, damage to the chamber can eventually lead to an explosion or implosion, respectively. If combustible metal powders such as titanium or aluminum alloys are used, damage to the containment chamber can lead to a fire or dust explosion [35], like the November 2013 incident at Powderpart Inc. [36]. Last, but not least, secondary explosions can be far more destructive than a primary explosion due to the increased quantity and concentration of dispersed combustible dust [35]. These can potentially cause deaths and injuries, and even the destruction of a manufacturing facility [35].

- **Fusing Material Patterns:** Another factor that greatly influences the temperature gradient is the pattern of the heat source [3]. The manipulation or replacement of this pattern changes the temperature gradient and negatively influences the microstructure and, consequently, the mechanical properties of the manufactured object. In the worst case, an adversary can selectively create weak points in a manufactured object, arbitrarily reducing its lifetime or causing a specific type of damage.

- **Timing:** In additive manufacturing, new layers should be applied over already-solidified underlying layers. Several timing attacks are possible. If the time intervals between the depositions of layers are insufficient, the consequences can be melting and uncontrollable material flow, which negatively impact the shape and physical properties of the manufactured object. If the time periods are too long, the object microstructure can be affected quite severely because of the weak bonding of adjacent layers. In composite parts, weak interfaces can lead to debonding and delamination, leading to premature failure of the manufactured objects. These patterns are often seen when the additive manufacturing process has been interrupted and continued shortly thereafter.

  A timing attack can also influence the positioning mechanism. If the speed of the heat source or the depositing nozzle are manipulated, the material is exposed to less heat so that it does not optimally bond to the previous layer. The timing attack can be performed by manipulating

the control software or the clock used by the additive manufacturing equipment.

- **Support Material:** If a support structure is necessary during additive manufacturing, then changing the amount of the support material or its physical properties can have an impact on the manufactured object. An attack that reduces the amount of support material can cause portions of the manufactured object to sag, leading to an unacceptable overall 3D shape [24]. Furthermore, the quality of the support material is also important because it enhances heat distribution and increases stiffness. Heat is distributed at the contact points of the support material and part, and is affected by the geometry and properties of the support material. Therefore, manipulations of the support material and its distribution can negatively affect the quality of the manufactured object.

- **Source Material:** Regardless of whether the powder is distributed in a powder bed or via a nozzle, the quality of the manufactured part depends on the powder particle size, shape (spherical/random) and the degree of recycling [43]. Unevenly-distributed particle sizes may lead to a part with higher density whereas evenly-distributed particle sizes may result in greater strength [30, 42]. The powder particle is usually less than 150 μm [12, 43]; the minimum sizes are dependent on the material. The particle size could be reduced further, but for cost and efficiency reasons, 60-150 μm particles are generally used. Some studies indicate that powders with spherical particles have good flow properties and high packing density [41, 42]. Therefore, a supply chain attack that replaces the expected powder with one with different properties can influence the physical properties of the manufactured objects.

- **Powder Recycling:** Powder is recycled to reduce waste. A manipulation of the system that mixes used and new material can have an immediate impact on the manufactured objects. A greater percentage of used powder has a greater negative impact on the microstructure and, consequently, the physical properties of the manufactured objects.

- **Ultrasonic Properties:** In the sheet lamination process (also known as ultrasonic additive manufacturing), thin metal sheets are fused by ultrasonic welding. The ultrasonic horn frequency and amplitude are adjusted by hardware or via a digital card housed in the control computer. An attack can cause the sonotrobe to produce ultrasound with different properties (i.e., frequency or amplitude). For example, high frequency ultrasound provides maximum spatial resolution and is, therefore, effective for bonding thin parts. Varying the frequency negatively impacts the bond strength [12, 18], affecting the mechanical properties of the manufactured objects, with all the possible consequences described above.

- **Temperature Control:** Each additive manufacturing process requires specific temperature conditions. Therefore, an attack that targets the

cooling and/or pre-heating system can change the physical properties of the manufactured objects. Of great concern is the microstructure, which depends significantly on the cooling temperature and gradient. In order to reduce the temperature gradient between layers and to reduce the residual stress in the material, a constant temperature below the melting point is often maintained in the chambers of some additive manufacturing devices. Therefore, manipulations of the temperature in the chamber can affect the physical and interfacial properties of the manufactured objects with all the associated consequences.

An attack that manipulates the heating system can reduce the chamber temperature or increase the temperature of the material above its melting point. In the first case, the lower temperature adversely influences the microstructure and, thus, the physical properties of the 3D objects. In the second case, the higher temperature could lead to uncontrollable material flow, affecting the shape, size and microstructure of the manufactured object as well as requiring expensive cleaning of the chamber.

A cooling process is initiated after object printing and/or during post-processing. A high cooling rate may be used to achieve certain microstructure characteristics during post-processing. Manipulating the cooling process can affect the manufactured objects as well as contribute to increased wear of the additive manufacturing equipment and even damage key components.

- **Heat Sources:** Lasers and electron beams serve as heat sources in additive manufacturing processes. An attack that compromises a heat source can affect the temperature profile of the material. Temperature profiles that are higher or lower than normal can affect the microstructure of a manufactured object and negatively affect its physical properties. In addition to the intensity of the laser or electron beam, parameters such as the distance from the material and the speed at which the heat source rides over the powder influence the temperature gradient and, thus, affect the microstructure. The impact of this attack can be increased by combining it with other attacks such as the manipulation of the cooling system.

- **Chamber Atmosphere:** If a laser or electron beam is used as a heat source, the chamber should have an inert gas or a high vacuum, respectively [2]. In the case of a laser heat source, an attack that manipulates the inert gas pressure can impact the temperature profile and, thus, the object microstructure and physical properties [19]. If the vacuum is manipulated, the electron beam intensity decreases because electrons are deflected; the resulting change in the temperature profile affects the object microstructure and its physical properties.

- **Post-Processing:** Post-processing is intended to increase the quality of the end product. High isostatic pressure processing is commonly used

– it involves heating the manufactured object for several hours at high temperature and pressure [43]. An attack on the post-processing system can negatively impact the quality of the manufactured object; moreover, exceedingly high pressures and/or temperatures can damage the post-processing chamber itself. When composites are processed, it is customary to conduct post-cure cycles ranging from a few hours to a few days to relieve residual stresses in the manufactured objects. Malicious variations of key parameters during this phase can cause warping, shrinkage, stresses and possible damage.

4. Conclusions

Additive manufacturing is an emerging technology that builds 3D objects layer by layer. The range of applications and dependence on computerization make additive manufacturing an attractive target for attackers.

This chapter has focused on attacks that seek to change the physical properties of additive-manufactured components. The attacks can lead to weaker and possibly damaged manufactured components, and, in instances where the compromised components are used in safety-critical systems, the attacks can endanger human lives. In particular, this chapter has identified the attack vectors and the key additive manufacturing parameters that can be targeted to alter the physical properties of manufactured parts, damage additive manufacturing equipment and even a manufacturing facility itself. While some of the attack vectors emanate from the cyber domain, the majority of the attacks and influences target the materials science and mechanical engineering aspects of additive manufacturing processes and equipment.

Deep understanding of additive manufacturing and the potential threats is vital to developing protection and mitigation techniques and tools. Future research will attempt to quantify the effort needed to manipulate additive manufacturing processes and assess the severity of the consequences of successful attacks. The analysis of the commonalities of and differences between attacks will be facilitated by describing the attacks and the related effect propagation chains using CP-ADL, a powerful cyber-physical attack description language [54, 55].

References

[1] American Society for Testing and Materials, ISO/ASTM52915-13, Standard Specification for Additive Manufacturing File Format (AMF), Version 1.1, West Conshohocken, Pennsylvania, 2013.

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

[3] 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.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] A. Drizo and J. Pegna, Environmental impacts of rapid prototyping: An overview of research to date, *Rapid Prototyping Journal*, vol. 12(2), pp. 64–71, 2006.

[11] 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.

[12] European Powder Metallurgy Association, Additive Manufacturing Technology, Shrewsbury, United Kingdom (`epma.com/additive-manufacturing-technology`), 2014.

[13] Fabrisonic, Sound 3D Printing, Columbus, Ohio (`fabrisonic.com`), 2014.

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

[15] P. Fastermann, *3D-Drucken: Wie die Generative Fertigungstechnik Funktioniert*, Springer-Verlag, Berlin Heidelberg, Germany, 2014.

[16] 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.

[17] H. Fujii, M. Sriraman and S. Babu, Quantitative evaluation of bulk and interface microstructures in Al-3003 alloy builds made by very high power ultrasonic additive manufacturing, *Metallurgical and Materials Transactions A*, vol. 42(13), pp. 4045–4055, 2011.

[18] A. Gebhardt, *Understanding Additive Manufacturing: Rapid Prototyping, Rapid Tooling, Rapid Manufacturing*, Hanser Publishers, Munich, Germany, 2012.

[19] I. Gibson, D. Rosen and B. Stucker, *Additive Manufacturing Technologies: Rapid Prototyping to Direct Digital Manufacturing*, Springer, New York, 2010.

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

[21] J. Hiller and H. Lipson, STL 2.0: A Proposal for a Universal Multi-Material Additive Manufacturing File Format, Department of Mechanical and Aerospace Engineering, Cornell University, Ithaca, New York (`creativemachines.cornell.edu/sites/default/files/SFF09_Hiller1.pdf`), 2009.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] J. Kruth, M. Leu and T. Nakagawa, Progress in additive manufacturing and rapid prototyping, *CIRP Annals – Manufacturing Technology*, vol. 47(2), pp. 525–540, 1998.

[27] G. Lewis and E. Schlienger, Practical considerations and capabilities for laser assisted direct metal deposition, *Materials and Design*, vol. 21(4), pp. 417–423, 2000.

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

[29] H. Lipson, AMF tutorial: Colors and textures (Part 2), *3D Printing and Additive Manufacturing*, vol. 1(4), pp. 181–184, 2014.

[30] 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.

[31] 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.

[32] J. Mazumder, D. Dutta, N. Kikuchi and A. Ghosh, Closed loop direct metal deposition: Art to part, *Optics and Lasers in Engineering*, vol. 34(4-6), pp. 397–414, 2000.

[33] C. McNulty, N. Arnas and T. Campbell, Toward the printed world: Additive manufacturing and implications for national security, *Defense Horizons*, no. 73, pp. 1–16, 2012.

[34] A. Munoz and P. Sheng, An analytical approach for determining the environmental impact of machining processes, *Journal of Materials Processing Technology*, vol. 53(3), pp. 736–758, 1995.

[35] Occupational Safety and Health Administration, Hazard Alert: Combustible Dust Explosions, OSHA Fact Sheet, Washington, DC, 2014.

[36] 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.

[37] 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.

[38] M. Ratto and R. Ree, Materializing information: 3D printing and social change, *First Monday*, vol. 17(7), 2012.

[39] P. Reeves, How the socioeconomic benefits of rapid manufacturing can offset technological limitations, *Proceedings of the RAPID Conference and Exposition*, 2008.

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

[41] Sandvik Materials Technology, Metal Powder for Additive Manufacturing, Sandviken, Sweden (`smt.sandvik.com/en/products/metal-powder/additive-manufacturing`), 2015.

[42] 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/Schade ade-Atomized%20Powders%20for%20Additive%20Manufacturing%20(1).pdf`), 2014.

[43] L. Schutzle, Research on the Impact of Additive Layer Manufacturing for Future Space Missions, Internship Report CDF-STA-009, European Space Agency, Paris, France, 2014.

[44] 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.

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

[46] D. Thomas, Economics of the U.S. Additive Manufacturing Industry, NIST Special Publication 1163, National Institute of Standards and Technology, Gaithersburg, Maryland, 2013.

[47] 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.

[48] K. Thompson, Reflections on trusting trust, *Communications of the ACM*, vol. 27(8), pp. 761–763, 1984.

[49] 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.

[50] Wohlers Associates, Wohlers Report 2015, Fort Collins, Colorado, 2015.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.