Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad

Mark Yampolskiy
Auburn University
USA

Jacob Gatlin
Auburn University
USA

Moti Yung
Google LLC
Columbia University
USA

ABSTRACT

It is natural, as the demand for Additive Manufacturing (AM) Security grows, to adopt established approaches from other security research areas. However, such “imports,” if not done carefully, can be misleading, and sometimes even counterproductive, and thus may negatively affect actual security of AM. We argue that this is the case for the CIA triad (Confidentiality, Integrity, Availability), a fundamental model of data security. To this end, we present arguments showing that the CIA triad cannot substitute concrete threat categories already established in AM. AM is an area which is not “pure data,” but rather an area involving software, data files, and transforming data into physical artifacts, where established threats in this ecosystem include: Technical Data Theft, Sabotage, and Illegal Part Manufacturing.

CCS CONCEPTS

• **Applied computing** → **Computer-aided manufacturing**; • **Computer systems organization** → *Embedded and cyber-physical systems*; • **Security and privacy** → **Formal security models**.

KEYWORDS

Additive Manufacturing, 3D Printing, Security, CIA Triad.

ACM Reference Format:

Mark Yampolskiy, Jacob Gatlin, and Moti Yung. 2021. Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. In *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security (AMSec '21)*, November 19, 2021, Virtual Event, Republic of Korea. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3462223.3485618>

1 INTRODUCTION

“Nothing is more dangerous for a new truth than an old misconception.” – Johann Wolfgang von Goethe [33]

Multiple researchers have attempted to apply the CIA Triad to AM Security in the literature [7, 9, 12, 40], often conflating it with security threat categories in AM. To guard against the danger identified by Goethe, we, in fact, present an argument against the adoption of the *CIA Triad for Additive Manufacturing Security* (AM Security). We note that in security research the above danger is real,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

AMSec '21, November 19, 2021, Virtual Event, Republic of Korea.

© 2021 Association for Computing Machinery.

ACM ISBN 978-1-4503-8480-3/21/11...\$15.00

<https://doi.org/10.1145/3462223.3485618>

(a) CIA Triad in Network Security

(b) Threat Categories identified for AM (based on [17, 37])

Figure 1: Models to Reconcile... or Not

since the wrong old model may be used to claim “security,” which is actually insufficient.

The CIA Triad is a broadly used cyber-security concept, identifying the Confidentiality, Integrity, and Availability of data as key elements to secure. Applied to network security, as in the classical example of two trustworthy communicating parties, the CIA triad maps directly onto the types of attacks that a Man in the Middle can conduct (See Figure 1a). When sensitive information is communicated, outside access to that information is a Confidentiality breach. When information is altered, that is an Integrity breach. When the delivery of information is prevented, that is an Availability breach. It should be noted that even within network security there have been proposals that extend the CIA model for wider coverage, such as the Parkerian hexad [25].

Additive Manufacturing (AM), also known as 3D printing, is a family of manufacturing techniques that produce parts incrementally, often layer by layer, based on a digital design file. There are seven AM processes recognized by the ASTM [18], each differing in the way materials are deposited and fused. These are capable of producing parts in polymers, composites, metal alloys, and a variety of more exotic materials. The AM sector is undergoing explosive growth, with the average annual revenue growth rate over past four years (2017-2020) of 20.8% [34]. The market has found a wide range of applications, from rapid prototypes to functional components of safety-critical systems. This wide adoption, rapid growth, and the fundamentally computerized nature of the technology have made security a key concern in the area.

Three major concrete threat categories have been identified for AM Security: Theft of Technical Data, Sabotage, and Illegal Part Manufacturing [37] (See Figure 1b). Theft of Technical Data covers attempts to steal, capture, or reverse engineer the necessary data to produce a printed object. This includes part geometry, but also the required physical properties of the part, the operational parameters of the printer, etc. Sabotage is the intentional degradation of a printed object's characteristics, such as geometry or mechanical properties. It could also refer to damaging AM equipment or contaminating the surrounding environment. Illegal Part Manufacturing typically corresponds to the misuse of AM, as specified by local legal authorities, for the production of restricted goods such as weaponry or nuclear equipment. It is occasionally also used to mean the violation of legal agreements on production, such as overproduction or counterfeiting.

In this note, we address the questions: are these two models reconcilable, and is the CIA triad an apt fit for modeling AM concrete security threat? We assert that the answer is no on both counts, and provide our analysis and argumentation in Section 2. In fact, we argue that though there are areas of overlap between AM security and the CIA triad, there are, however, many factors present in AM Security threats which make them irreconcilable with the CIA triad, and this is the main point of this work, and the focal point of our analysis. As our analysis makes frequent reference to the literature, we omit a dedicated Related Works section. Section 3 summarizes our concluding thoughts on the relation of the models.

2 ANALYSIS

In this section, we present arguments that each element of the CIA triad is not directly analogous to the security threats identified for AM, and that one of the three major threats is not covered by the

Figure 2: Reconstruction of a 3D-Printed Object based on Acoustic Side-Channel Emanations [1]

triad at all. Instead, the base terms of Confidentiality, Integrity, and Availability correspond to elements of AM Security in complex and incomplete ways. Our arguments will consist of examples drawn from the research literature and the real world to demonstrate where the two models correspond naturally, where they can be adjusted to fit, and where they are completely irreconcilable.

2.1 Confidentiality

Confidentiality is typically applied to data in its digital representations, such as the contents of files on a hard drive, data in memory, or packets being transmitted over a network. There are some cases in AM Security where Technical Data exists in these forms, and Confidentiality concerns map directly onto Technical Data Theft.

Digital Design Files: The design files used in printing processes are classical examples of digital data. There are numerous attacks in the literature that compromise these files, including a spear phishing attack for remote access to files [5], hijacking a network session to retrieve models from a 3D printer [12], and forensic examination of the SD card internal memory of a 3D printer [21]. In each of these cases, a compromise of the files' Confidentiality directly corresponds to Technical Data Theft.

Toolpath Commands: During the printing process, the digital model is transformed into a set of toolpath commands, such as the G-code commonly used in consumer 3D printers. These commands, which instruct the printer on operating the actuators involved in printing, are also a digital representation of the design. Commercial and freeware tools such as Wireshark can capture these commands in transit; the commands have been used in the literature to reconstruct the original model [30], achieving Technical Data Theft. Further, access to toolpath commands allow a trivial record-replay attack against printers of the same make and model.

With Technical Data Theft, as opposed to Confidentiality, one must consider adversarial goals. Stealing only the design files may not fulfill the goal of recreating a print, which could require technical data that does not necessarily have an accessible digital representation. A variety of technical data, such as feedstock specifications and requirements on mechanical properties, falls into this category. These forms of technical data are not natively digital and Confidential, but could be covered by an expanded or relaxed definition of the term.

Part Specification: In addition to geometry, which is specified by its design file, functional parts will also have an accompanying set of required mechanical properties. These are commonly provided by supplementary documentation in PDF or other formats, simulated by a separate Finite Element Analysis system, and verified in the Quality Assurance stage. The necessity of this information as part of an object's technical data is frequently referenced in the AM Security literature [38]. This makes it a valid target for Technical Data Theft, but one whose Confidentiality is more difficult to specify and defend owing to the variety and diffuse nature of data sources.

Manufacturer's Institutional Knowledge: Off-the-shelf manufacturing parameters are often insufficient to produce a part to specification. Components of the AM equipment must be manually calibrated, manufacturing parameters like laser scanning strategies must be selected, and feedstock satisfying certain characteristics must be used. These activities and information constitute the institutional knowledge of the manufacturer, and are a key aspect of their technical data. The vast majority of these have no concrete digital realization, and while it is sensitive information it is typically not legally protected. Thus, these types of data are also valid targets for Technical Data Theft but not Confidential by the CIA triad definition.

Technical Data Theft can target data not considered Confidential or not defensible by any known cyber-security means. In these cases, it is difficult or impossible to reconcile the two.

Physical Part: Most Additively Manufactured items are produced for sale, rather than internal use. In these cases, the physical object itself cannot be kept confidential, and might be subjected to analysis and reverse engineering. This can allow the production of a 3D model to produce counterfeit versions of the part, or to inform the development of a competing product. More strikingly, this reverse engineering of the 3D printed object is not necessarily illegal under current US law [6]. Here, the Confidentiality of the printed object is impossible to protect.

Side Channel Data: One can break Confidentiality for key print data without breaking Confidentiality in cyber-space through the use of side-channels. Such attacks, which reason about the printed object by recording physical emanations from the printer, are well established in AM Security [8, 14, 15]. While the results of this reconstruction have a degree of error, they are still useful for many applications from counterfeiting to intelligence gathering. Such side channel emanations have no legal protections at all, and technical protections are notoriously difficult. Especially for printing equipment out of the direct control of the manufacturer, as in the case of outsourced manufacturing [15], maintaining Confidentiality is quite impossible.

Confidentiality is not expansive enough to cover the category of technical data theft. It is often either difficult to define for technical data that is inherently public-facing or messily analog, or impossible to secure for resources that lack technical protections. Since these forms of technical data must be studied and secured regardless, a

Figure 3: *dr0wned*: Sabotaged Propeller Breaks during Flight, Leading to Crash and Destruction of a Quadcopter UAV [4]

different definition and modeling approach than Confidentiality is required.

2.2 Integrity

There are several clear examples where a violation of Integrity, by its classical definition, leads to the Sabotage of an additively manufactured part.

Design File Integrity: The majority of sabotage attacks demonstrated in the research literature are conducted by design file manipulations, which violate the file's Integrity. This includes changes in geometry affecting part form and fit [31, 37], or those affecting part functions such as fatigue life [4] and tensile strength [29, 41]. Practical implementations can be either targeted, via APT-like methods [4], or indiscriminate, via automated malware [29]. Although they are not widely integrated today, classical cyber-security countermeasures such as cryptographic file hashing would serve to mitigate this Integrity threat.

Software and Firmware Integrity: Throughout the printing process, there are many pieces of software and firmware that operate on digital representations of the design. These include the CAD software used to model the original design, tools like Finite Element Analysis software that simulate its physical properties, the slicer that translates a model into an executable toolpath, and the printer firmware itself which interprets and executes toolpath commands. Vulnerabilities have been enumerated for open-source slicers and printer firmware [22]. Some of these vulnerabilities have even been used to execute full sabotage attacks [23, 35]. Here as well, classical Integrity-based approaches model the problems well and can be applied to prevent Sabotage.

Outside of the classical cyber-focused strategies, Sabotage in AM has also been conducted in gray areas where digital and analog representations begin to overlap. In these areas, Integrity can only be applied with some adaptation. Further, there are clear cases where Integrity violations do not indicate Sabotage.

Benign Process Fluctuations: Additive Manufacturing, despite operating based on digital inputs, is an analog process and exhibits stochastic behavior. Each parameter of

the print, from the filament extrusion rate of FDM printers to the laser power of PBF, varies over time from the input level requested by the controller. Therefore, all of the physical properties of the print are natively violating an exact definition of Integrity. Because such fluctuations, and their expected range, are well known and accounted for during the design phase, this form of violation does not constitute Sabotage. Integrity can theoretically be adapted by defining the same allowable range of fluctuation before a violation occurs.

Sensor Data Integrity: To account for fluctuations and improve the quality of the final product, some printing processes compensate for stochastic behavior through a feedback loop. Currently, a common trend is to incorporate infrared in-situ monitoring of the melt pool in PBF machines to adjust laser power parameters. This system enables indirect attacks that have already been demonstrated in the literature [28], causing incorrect adjustments through false sensor readings. These readings were not only spoofed, which can be accounted for by Integrity violations, but caused to have systematic error through miscalibration. Sensor calibration is more difficult to define Integrity for, as it relies on a manual testing methodology comparing readings to real-world conditions.

In some cases, the physical properties of the printing process make Integrity impossible to define. Stretching the definition can in fact be misleading, giving a false sense of security while leaving a process vulnerable to Sabotage.

Compound Manipulations: Although thresholds can be established for individual print parameters, they are only reliable if you assume random error. In security, we cannot rely on such a cheerful scenario; against a human adversary, who can intentionally search for and create multiple errors simultaneously, no such assumption can be made. Compound attacks have been proposed [16] that, while only requiring minimal variations in individual parameters, produce a final effect amounting to Sabotage. Considering the number of process parameters (over 150 reported for PBF [27]) and their variation from printer to printer, fully quantifying and accounting for compound effects like this is an intractable problem for defining the Integrity of a physical part.

Closed Control Loops: In-situ monitoring and closed control loops have been implemented for several subsystems of AM machines, including laser power, oxygen level, and build chamber temperature. The incorporation of a control loop continuously adjusts the control signal based on the difference between the measured level and a set value. While these are necessary to achieve consistent quality and stable process parameters, they fundamentally prevent definitions of Integrity for the control signals of those subsystems. The “correct” control signal varies continuously over time, based on unknowable and uncontrollable conditions of the printing process.

Feedstock Sabotage: There is a great deal of variation in AM feedstock, even within narrow categories such as metal powder. Feedstock sabotage, carried out via powder contamination or

other means, has been proposed in the security literature [38]. Vock et al. [32] presented an overview of key characteristics such as morphology, impurities, moisture, and density, as well as how these characteristics interact with the AM process to determine final part properties. The specification of these properties is an active area of research, relying on complex and time consuming characterization of powder samples. Applying an Integrity measure to feedstock sabotage therefore has a fundamental problem with sampling. The cyber-security definition of Integrity is deterministic where all of the values available for feedstock characterization are stochastic; there is no absolute certainty whether contaminated powder will be in the analyzed sample, or how much. Even defining Integrity on the digital records of such a test has limited use, as the exact measurements of that sample will likely never be replicated.

There are multiple further examples where Sabotage and Integrity cannot be reconciled, either where parts can be sabotaged without any violation of data integrity (timing attacks [36], power supply attacks [36], environmental manipulations[37], etc.), or where Integrity cannot be meaningfully defined. Some of these, in particular timing attacks, can instead be interpreted as temporary Availability compromises, as we discuss in Section 2.3.

2.3 Availability

Attacks against Availability can be considered at two levels of abstraction. An attack can deny access to a resource, such as a single email being transmitted, or to a service, such as an organization’s email server. Some Availability attacks in both these categories overlap with the goals and methods of Sabotage, though they do so inconsistently and in complex ways.

Denial of Service (DoS) Attacks: A DoS attack is an attack against the availability of a resource, leading to the disruption of a service essential for organizational function. In addition to traditional targets at the level of network infrastructure, they can be executed against component-level systems such as in-situ monitoring controllers. Sabotage Attacks targeting AM equipment itself have been hypothesized in AM Security [39] and have equivalents in real-world attacks against industry [13]. Such attacks would clearly disrupt the manufacturing service of an organization, constituting a DoS attack. However, they can also be conducted using means such as ransomware, or classical cyber-approaches like message flooding, which would not qualify as Sabotage. In this case, we still consider traditional DoS attacks as a point in favor of Availability, as a type of attack not well modeled in AM Security.

In the classical cyber-security context, Availability is often considered as a binary; a resource is either available or unavailable. While binary Availability might be workable in cyber-security, it does not suffice for many AM systems. Availability can be stretched to non-binary definitions, which allows it to be applied to further aspects of AM Security.

Figure 4: The Liberator Handgun: Confidential, Full Integrity, and Available Now. Photo Courtesy of AP Photo/Eric Gay [2]

Timing Attacks: AM equipment constitutes a Cyber-Physical System (CPS), which are known to have hard real-time requirements; disrupting the timing of actions can disrupt the correct functioning of the CPS [20]. If we redefine Availability to mean Availability within a designated time window, as is critical for real-time systems, several methods of AM Sabotage apply. It has been discussed in the AM Security literature that packets arriving too late or even too early can disrupt the manufacturing process and degrade part quality [36]. This would apply in particular to interconnected subsystems, such as in-situ monitoring systems passing data to a laser controller [10].

Out of Order Attacks: A special case of timing attacks are those that cause packets to arrive in an unintended order. These have also been speculated on in the AM Security literature [36], and would have particular significance when used against systems being controlled by commands passed over a network. Out-of-order attacks conducted between the host PC and a 3D printer, for example, could misorder toolpath commands and cause a part to print incorrectly.

Even applied in these ways, Availability does not encompass all Sabotage concerns.

Sabotage without Availability Violations: The majority of Sabotage attacks have been introduced via Integrity manipulations, or by methods not covered by the CIA triad (see Section 2.2). This means that Availability and Sabotage can never be completely equated.

We've presented that Availability can be both the means of, and the result of, a Sabotage attack. The relationship is complex, with some elements of Availability clearly not being Sabotage and vice versa. This complex mapping indicates that Availability can be a concern in AM Security, as with DoS attacks, but doesn't itself reflect the fundamental threats in AM described by the existing categories.

2.4 The Missing Threat: Illegal Part Manufacturing

Even in its field of origin, the CIA triad was identified as not covering all the necessary aspects of data security. The Parkerian hexad, for example, extended the triad with Possession, Authenticity, and Utility [25]. There is a similar problem of missing coverage when applying the CIA triad to AM Security.

In AM Security, Illegal Part Manufacturing has been identified as a critical area of concern, with multiple real-world incidents of crackdowns on illegal 3D-printed objects [2, 3]. It encompasses a number of distinct threats, including infringement and overproduction, the unauthorized production of export-controlled goods, or the production of locally or internationally prohibited items. Many of these threats have nothing to do with data security, placing them completely outside the CIA triad.

Not Confidentiality: The design files necessary to produce an illegal part can be developed independently and may be available freely online. The export control and prohibitions that make a part illegal are not necessarily on the data or design of an object, though designs can be export-controlled too. They are often instead based on their intended uses or capabilities. For example, the Bureau of Industry and Commerce, which regulates export controls in the US, restricts the sale of firearms based on their capabilities specifically (fully automatic, above a certain caliber, etc.) [24]. They make no mention of manufacturing method or designs; any firearm produced with AM having the same capabilities would be equally restricted.

Not Integrity: The concern with Illegal Part Manufacturing is not the correctness of data or object printability, but rather the object being printed and its real-world use. In most cases, the person or group producing the illegal part will be concerned with maintaining the Integrity of their own process and manufactured parts. Here, preventing Integrity breaches actually works in support of an Illegal Part Manufacturing threat.

Not Availability: The same logic of Integrity applies to Availability and Illegal Part Manufacturing. A manufacturing system and design being kept available means that a group can use it to manufacture illegal parts. Many of the papers in this area are actually concerned with making printers unavailable for certain types of manufacturing, such as counterfeiting or the production of known firearm designs [11, 19, 26].

This concludes our analysis.

3 CONCLUSION

This paper has analyzed if and where the CIA triad can be reconciled with security threats in Additive Manufacturing. We have shown that, while some specific threats can be mapped onto Confidentiality, Integrity, and Availability, in each case there are numerous examples of real threats in AM that cannot be reconciled. Further, the well-established threat category of Illegal Part Manufacturing is not covered by any aspect of the triad. Table 1 summarizes our conclusions.

Confidentiality maps partially onto the concerns of Theft of Technical Data, as some elements of Technical Data are traditional

Table 1: Analysis results: There is no equivalency between elements of the CIA Triad (Confidentiality, Integrity, Availability) and the “corresponding” AM Security Threats.

AM SECURITY THREATS	CIA TRIAD		
	<u>C</u>	<u>I</u>	<u>A</u>
<i>Theft of Technical Data</i>	(✓)	✗	✗
<i>Sabotage</i>	✗	(✓)	(✓)
<i>Illegal Part Manufacturing</i>	✗	✗	✗
✓ – Direct correlation, always (✓) – Correlation in certain cases only ✗ – No correlation at all			

digital files. However, we also presented a variety of technical data that, while necessary for the manufacturing process, cannot be easily defined as Confidential. In addition to the technical considerations, there are significant limitations in the legal protections for technical data.

The violation of Integrity maps partially onto Sabotage, as changes to design files can be used to conduct such attacks. However, equating the two categories is both incomplete and misleading. Many published attacks were carried out without any violation of Integrity; at the same time, many violations of Integrity will not result in Sabotage. The true distinction that should be made in AM is instead Safety, as AM Security is typically considered for functional and safety-critical parts.

Availability does not map onto Illegal Part Manufacturing, as the structures of the models might suggest. Instead, it also maps partially onto Sabotage, as compromises to the Availability of certain data or equipment can be used to conduct such attacks. It does not map completely, as the majority of published Sabotage attacks do not disrupt Availability. Interestingly, there are several obvious Availability attacks (such as Denial of Service against manufacturing equipment) that would not result in the Sabotage of a part or of equipment, but are clearly viable attacks. This indicates that further work is necessary on the AM threat model.

We have shown that the CIA triad is poorly-fit for AM Security. Instead of relying on decades-old data security models respected in another field, fundamental security modeling tailored for the cyber-physical world of AM must be used, such as the one in Figure 1b. Indeed, the same may apply to any digital manufacturing technology.

ACKNOWLEDGMENTS

This work was funded in part by the U.S. Department of Commerce, National Institute of Standards and Technology under Grant NIST-70NANB20H193.

REFERENCES

- [1] Mohammad Abdullah Al Faruque, Sujit Rokka Chhetri, Arquimedes Canedo, and Jiang Wan. Acoustic side-channel attacks on additive manufacturing systems. In *2016 ACM/IEEE 7th international conference on Cyber-Physical Systems (ICCPs)*, pages 1–10. IEEE, 2016.
- [2] Michael Balsamo and Chris for AP News Grygiel. Coalition of states sue over rules governing 3d-printed guns, 2020.
- [3] BBC. Japan man held over ‘3d-printed guns’, 2020.
- [4] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, and Yuval Elovici. dr0wned – cyber-physical attack with additive manufacturing, 2016.
- [5] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. dr0wned – cyber-physical attack with additive manufacturing. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, page 16, Vancouver, BC, 2017. USENIX Association.
- [6] Adam Brown, Mark Yampolskiy, Jacob Gatlin, and Todd Andel. Legal aspects of protecting intellectual property in additive manufacturing. In *International Conference on Critical Infrastructure Protection*, pages 63–79. Springer, 2016.
- [7] Siva Chaitanya Chaduvula, Adam Dachowicz, Mikhail J Atallah, and Jitesh H Panchal. Security in cyber-enabled design and manufacturing: A survey. *Journal of Computing and Information Science in Engineering*, 18(4), 2018.
- [8] Sujit Rokka Chhetri, Arquimedes Canedo, and Mohammad Abdullah Al Faruque. Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. In *Proceedings of the 35th International Conference on Computer-Aided Design*, page 74. ACM, 2016.
- [9] Sujit Rokka Chhetri, Sina Faezi, and Mohammad Abdullah Al Faruque. Information leakage-aware computer-aided cyber-physical manufacturing. *IEEE Transactions on Information Forensics and Security*, 13(9):2333–2344, 2018.
- [10] Stijn Clijsters, Tom Craeghs, Sam Buls, Karolien Kempen, and J-P Kruth. In situ quality control of the selective laser melting process using a high-speed, real-time melt pool monitoring system. *The International Journal of Advanced Manufacturing Technology*, 75(5-8):1089–1101, 2014.
- [11] Adam Dachowicz, Siva Chaitanya Chaduvula, Mikhail Atallah, and Jitesh H Panchal. Microstructure-based counterfeit detection in metal part manufacturing. *JOM*, 69(11):2390–2396, 2017.
- [12] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. A data exfiltration and remote exploitation attack on consumer 3d printers. *IEEE Transactions on Information Forensics and Security*, 11(10):2174–2186, 2016.
- [13] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29, 2011.
- [14] Yang Gao, Borui Li, Wei Wang, Wenyao Xu, Chi Zhou, and Zhanpeng Jin. Watching and safeguarding your 3d printer: Online process monitoring against cyber-physical attacks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–27, 2018.
- [15] Jacob Gatlin, Sofia Belikovetsky, Yuval Elovici, Anthony Skjellum, Joshua Lubell, Paul W. Witherell, and Mark Yampolskiy. Encryption is futile: Reconstructing 3d-printed models using the power side channel. In *The 24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2021)*. ACM, 2021.
- [16] LMG Graves, W King, P Carrión, S Shao, N Shamsaei, and M Yampolskiy. Sabotaging metal additive manufacturing: Powder delivery system manipulation and material-dependent effects. *Additive Manufacturing*, page 102029, 2021.
- [17] Lynne MG Graves, Joshua Lubell, Wayne King, and Mark Yampolskiy. Characteristic aspects of additive manufacturing security from security awareness perspectives. *IEEE Access*, 7:103833–103853, 2019.
- [18] ASTM International. F2792-12a-standard terminology for additive manufacturing technologies. *Rapid Manufacturing Association*, 12:10–12, 2013.
- [19] Zachary C Kennedy, David E Stephenson, Josef Christ, Timothy R Pope, Bruce Arey, Christopher A Barrett, and Marvin G Warner. Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. *Journal of Materials Chemistry C*, 5:9570–9578, 2017.
- [20] Edward A Lee. Cyber physical systems: Design challenges. In *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*, pages 363–369. IEEE, 2008.
- [21] Daniel Bradford Miller, William Bradley Glisson, Mark Yampolskiy, and Kim-Kwang Raymond Choo. Identifying 3d printer residual data via open source documentation. *Computers & Security*, 2018.
- [22] Samuel Moore, Phillip Armstrong, Todd McDonald, and Mark Yampolskiy. Vulnerability analysis of desktop 3d printer software. In *Resilience Week (RWS), 2016*, pages 46–51. IEEE, 2016.
- [23] Samuel Bennett Moore, William Bradley Glisson, and Mark Yampolskiy. Implications of malicious 3d printer firmware. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.
- [24] Bureau of Industry and US Department of Commerce Security. Us commerce control list, 2021.
- [25] Donn Parker. Our excessively simplistic information security model and how to fix it. *ISSA Journal*, 8(7):12–21, 2010.
- [26] Giao N Pham, Suk-Hwan Lee, Oh-Heum Kwon, and Ki-Ryong Kwon. Anti-3d weapon model detection for safe 3d printing based on convolutional neural networks and d2 shape distribution. *Symmetry*, 10(4):90, 2018.
- [27] Olaf Rehme. *Cellular design for laser freeform fabrication*, volume 4. Cuvillier Verlag, 2010.
- [28] Andrew Slaughter, Mark Yampolskiy, Manyalibo Matthews, Wayne E King, Gabe Guss, and Yuval Elovici. How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, page 78. ACM, 2017.
- [29] L Sturm, CB Williams, JA Camelio, J White, and R Parker. Cyber-physical vulnerabilities in additive manufacturing systems. *Context*, 7:8, 2014.

- [30] Nektarios Georgios Tsoutsos, Homer Gamil, and Michail Maniatakos. Secure 3d printing: Reconstructing and validating solid geometries using toolpath reverse engineering. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, pages 15–20. ACM, 2017.
- [31] Hamilton Turner, Jules White, Jaime A Camelio, Christopher Williams, Brandon Amos, and Robert Parker. Bad parts: Are our manufacturing systems at risk of silent cyberattacks? *IEEE Security & Privacy*, 13(3):40–47, 2015.
- [32] Silvia Vock, Burghardt Klöden, Alexander Kirchner, Thomas Weißgärber, and Bernd Kieback. Powders for powder bed fusion: a review. *Progress in Additive Manufacturing*, pages 1–15, 2019.
- [33] Johann Wolfgang Von Goethe. *Maximen und reflexionen*. Jazzybee Verlag, 2012.
- [34] Terry Wohlers. *Wohlers Report 2017 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report*. Wohlers Associates, Inc., Fort Collins, Colorado, USA, 2021. www.wohlersassociates.com.
- [35] Xiao Zi Hang (Claud Xiao). Security attack to 3d printing, 2013. Keynote at XCon2013.
- [36] Mark Yampolskiy, Wayne King, Gregory Pope, Sofia Belikovetsky, and Yuval Elovici. Evaluation of additive and subtractive manufacturing from the security perspective. In *International Conference on Critical Infrastructure Protection*, pages 23–44. Springer, 2017.
- [37] Mark Yampolskiy, Wayne E King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, and Yuval Elovici. Security of Additive Manufacturing: Attack Taxonomy and Survey. *Additive Manufacturing*, 2018.
- [38] Mark Yampolskiy, Lena Schutzle, Uday Vaidya, and Alec Yasinsac. Security challenges of additive manufacturing with metals and alloys. In *Critical Infrastructure Protection IX*, pages 169–183. Springer, 2015.
- [39] Mark Yampolskiy, Anthony Skjellum, Michael Kretzschmar, Ruel A Overfelt, Kenneth R Sloan, and Alec Yasinsac. Using 3D Printers as Weapons. *International Journal of Critical Infrastructure Protection*, 14:58–71, 2016.
- [40] Alireza Zarreh, HungDa Wan, Yooneun Lee, Can Saygin, and Rafid Al Janahi. Risk assessment for cyber security of manufacturing systems: A game theory approach. *Procedia Manufacturing*, 38:605–612, 2019.
- [41] Steven Eric Zeltmann, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. Manufacturing and security challenges in 3d printing. *JOM*, pages 1–10, 2016.