Offensive and Defensive Perspectives in Additive Manufacturing Security

Rohith Yanambaka Venkata, Nathaniel Brown, Daniel Ting and Krishna Kavi

Center for Agile & Adaptive Additive Manufacturing (CAAAM)
and Dept. of Computer Science and Engineering
University of North Texas
Denton, Texas
USA
Email: {ry0080, nathanielbrown, danielting}@my.unt.edu and krishna.kavi@unt.edu

***Abstract*—Additive Manufacturing (AM) is transforming the manufacturing industry by reducing prototyping time and easing the production of complex parts. Notably, use of AM has gained traction in the medical and aerospace fields, and is rapidly increasing in usage in traditional industry. However, AM's cyber-physical nature opens systems up to vulnerabilities that can result in both cyber and physical damage. In this paper, we document and categorize the state of the art in Additive Manufacturing security research in three ways - by using Microsoft's Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE) threat model, by the intent of the attacker, and by the overall purpose of the published works. We also provide a list of security recommendations for AM that could aid in the design of secure AM systems. We hope our approach will enable an understanding of AM security from both the attacker's and defender's perspective, and serve as a survey of relevant research in the field, and stimulate more research into securing AM systems.**

Keywords–additive manufacturing; cybersecurity; threat modeling.

I. INTRODUCTION

Advanced manufacturing is a key component in what is called Industry 4.0 - manufacturing relying on sophisticated technologies including networked sensors and actuators, cyber technologies and machine learning to make processes flexible, agile and cost-effective. However, the reliance on these interconnected yet emerging technologies make these processes prone to cybersecurity attacks. In this paper, we will provide a high-level, concise but comprehensive survey of the currently known vulnerabilities with manufacturing, focusing on AM in particular, and suggested best practices for mitigating cyber attacks. First, we will briefly describe AM processes.

AM can produce a component in a layer-wise fashion rather than starting with a block of material and removing material using milling, cutting, or lathing processes (referred here as Subtractive Manufacturing, or SM). In this way, additive processes are not constrained in the same way as subtractive processes, meaning that the manufacturing envelope is opened very wide to produce technically or financially infeasible components due to such challenges as shape complexities, cost, new material combinations, etc. Relevant examples of AM include surgical joint replacement components (such as titanium hip or knee replacements), components whose traditional manufacturing methods would be cost or time prohibitive [1], or components for which the original tooling (such as the dies for forging) no longer exists (such as various components replaced on aging aircraft systems expected to continue serving for many years into the future [2]). Using this manufacturing method allows mass customization while simultaneously decentralizing the manufacturing and distribution process. Underlining mass customization, three-dimensional (3-D) printing is being developed to fabricate highly dose-specific medication. In 2015, the U.S. Food and Drug Administration (FDA) approved the first 3-D printed drug available in the United States — Levetiracetam (Spirtam - Aprecia), which is used to treat partial onset, myoclonic, and primary generalized tonic-clonic seizures in patients with epilepsy [3]. There have even been efforts to design and print medical equipment from simple face masks to complex ventilators [4] following the shortage during the COVID-19 pandemic.

Presently, there are many types of AM that vary based on cost, material system, manufacturing method, user capabilities, and characteristics of the desired final component. The most common forms of AM/3-D printing are - Vat Photopolymerization, Material Extrusion, Material Jetting and Powder Bed Fusion [1].

The AM process is a complex interaction of automated and manual workflows with numerous dependencies - both informational and physical. Additionally, AM my be provided as a service which would include several actors, software applications, sensors, actuation mechanisms and logistical activities. Not all of these entities may reside within a service provider's controlled environment. This cyber-physical nature of Additive Manufacturing processes leaves systems vulnerable to a certain array of unique attacks, including:

- Side-channel attacks that steal valuable intellectual property by listening to an AM system's sounds during product synthesis and running the data through a machine-learning model [5].
- Attacks that target the design stage to create fatal deficiencies (like voids) in key parts of synthesized products [6].
- Attacks that alter printing orientation to decrease end products' tensile strength [7].
- Attacks that target insecure methods of transferring stereolithographic (STL) files, such as via USB sticks [8].
- Attacks that exploit vulnerabilities in the code and programming languages that control AM systems; [9].
- Attacks that target AM quality-assurance techniques to ensure low product quality [10].

Our goal in this paper is to provide a high-level, concise but comprehensive survey of the current state of the art in security for AM; first from the attacker's point of view, then

from the defender's, using Microsoft's STRIDE security model to reason about security.

The structure of the remainder of the article is as follows. Section II describes related work and how we sourced the material for our research. Section III describes Microsoft's STRIDE threat model and its unique advantages when analyzing AM security. Section IV describes the intents of attackers seeking to exploit vulnerabilities in AM systems. Section V lists security recommendations for AM systems taken from recommendations for similar systems by the National Institute of Standards and Technology (NIST). Finally, Section VI provides conclusions about this work and future extensions.

II. Related Work

There have been a number of practical attacks specific to 3D printing executed in a lab setting. Works that we will touch upon include Sturm et al. [11], Zeltmann et al. [7], and Moore et al. [12]. These papers demonstrate one specific or narrow range of attacks.

Other papers introduce frameworks to reason about threats in this newly emerging domain of cybersecurity. Zhang & Padmanabhan [13] proposed five categories of risk and applied them to six separate stages in the manufacturing pipeline. Yampolskiy et al. [14] discussed multiple taxonomies over the different elements that can be attacked, how they can be attacked, and consequences of an attack. Glavach et al. [8] describe protocols and security recommendations for proper AM system operation.

Table I groups papers into three categories - papers that present or analyze a specific attack, those that propose a security design framework and those that propose/perform risk assessment on cyber attack(s).

In this paper, we organize vulnerabilities that affect Additive Manufacturing systems using the STRIDE threat model, consolidate and catalog research articles to provide an insight into the perspective of an adversary, and identify potential mitigation techniques.

These articles come from a mix of independent research, conferences, and journals focusing on AM or general manufacturing security, and were sourced from searching online databases for research on AM security, as well as from references from other papers. Since AM security is a relatively new field, most of the research we have compiled is recent.

To reiterate, we aim not to propose a new offensive or defensive strategy, but to unify these works under a common theme, the STRIDE model.

III. STRIDE Model

Most software systems today face a variety of cyber threats. The threat landscape is constantly evolving with the advances in technology. Malware that exploits software vulnerabilities grew 151% in the second quarter of 2018 [15]. Threats can originate from within or outside an organization and lead to devastating consequences. To prevent threats from wreaking havoc, system administrators/designers use threat modeling to profile the security posture of a system.

Threat modeling must be performed early in the development cycle to successfully identify and remedy vulnerabilities. Incorporating threat modeling into the design process of a system will lead to proactive architectural decisions that reduce threats from the start. Cyber physical systems in general, and Additive Manufacturing systems in particular, conflate software technology with physical infrastructure, which introduces a unique challenge of multiple stakeholders being involved in the system design process. Performing threat modeling on a cyber physical system from the perspective of multiple stakeholders is essential in identifying and eliminating threats across a wide spectrum of threat types.

Some of the popular threat models are:

- **PASTA :** The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat model developed in 2012 [16]. PASTA brings business objectives and technical requirements together. It utilizes several design and elicitation tools at various stages of design and approaches threat-modeling from a strategic level by involving key decision makers and requiring input from operations, governance, architecture and development. PASTA employs an attacker-centric perspective to produce an asset-centric output in the form of threat enumeration and scoring [16].
- **LINDDUN :** The Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance (LINDDUN) framework focuses primarily on privacy concerns and is used for data security [16]. The frameworks involves constantly iterating over data elements and analyzing them from the perspective of threat categories. The design involves identifying a threat's applicability to the system and building threat trees [16].
- **Attack Trees :** Using trees to model attacks on a system is an old and widely used technique. The trees are diagrams where the root represents the goal of an adversary and the leaves represent ways to achieve that goal. Each goal is represented by a separate tree. For complex systems, the number of attack trees may be too large to provide valuable and actionable insights into the security posture of the system.

The STRIDE threat model was invented in 1999 and adopted by Microsoft in 2002 [16]. This model identifies six main types of threats:

- **Spoofing :** Claiming a false identify in order to gain unauthorized access to resources. This type of threat violates the authenticity requirement of a system. Examples of this threat include spoofing the identity of a user by brute-forcing user credentials and phishing.
- **Tampering :** Malicious modification of data or processes. This modification may occur on data in transit, data at rest or on processes. This type of threat violates the integrity requirement of a system. Examples include SQL injection attacks and code-injection attacks.
- **Repudiation :** Falsely denying the occurrence of an action or event. Typical repudiation attacks involve a user denying performing a destructive action such as deleting records from a database and attackers truncating log files to remove all traces of a system breach.
- **Information disclosure :** Refers to data leaks or breaches. Perhaps, the most common type of threat today, information disclosure violates the confidentiality

requirement of a system. Eavesdropping, data sniffing, unauthorized access to a database are all examples of information disclosure attacks.

- **Denial of Service :** Disruption of a service or network resource. This prevents legitimate users from accessing the desired network service. This type of attack violates the availability requirement of a system. Typical examples include inundating a network service with multiple requests, using up available space on a shared hard drive, etc.
- **Elevation of Privilege :** Unauthorized access to system resources by violating the authorization requirement of a system. A typical example would be a user gaining root privileges on a system using buffer overflow.

We chose STRIDE model for this article because it is the most mature threat model [16]. It provides a balance between risk-assessment, security and privacy, which is vital when modeling complex cyber physical systems. While the other threat models discussed above have useful characteristics in cyber-only systems, we feel that STRIDE is the most well understood and widely used for cyber physical systems. Table II classifies research articles into the constituent attack types of the STRIDE model based on the type and nature of threats described in the articles.

IV. Intent of the Attacker

There are a number of articles focusing on the intent of a possible attacker. Graves et al. [21] propose a framework for the analysis of attacks on or with AM systems. The authors describe the attack targets as the intersection of the effects the attacks would have with the adversarial goals and objectives. The three major threat categories they identified are technical data theft, AM sabotage, and illegal part manufacturing. Table III summarizes research articles into three categories based on the intent or objective of an attacker.

A. Technical Data Theft

Technical data theft is the unauthorized use of Intellectual Property (IP). To an attacker, IP can be the most lucrative target because it forms the basis of an organization's competitive advantage. Stealing IP from an AM system is not so different from other manufacturing systems. However, security in AM systems may be less developed than that in traditional manufacturing, giving an attacker the edge.

AM is very new compared to traditional manufacturing methods that have been extensively tested in the field. An attacker can exploit zero-day flaws in AM systems that would likely have been patched long ago in a SM system. Do, Martini, and Choo [23] demonstrated several severe security oversights in MakerBot consumer 3D printers: print jobs are transmitted and stored unencrypted, allowing anyone on the same network to steal the model. Even worse, although the printer authenticates a computer over Hypertext Transfer Protocol Secure (HTTPS), it does not properly check the legitimacy of the certificate used, allowing them to do an Address Resolution Protocol (ARP) poisoning attack and perform privileged actions on the printer.

Furthermore, AM exhibits unique properties that enable all kinds of attacks. One such property that an attacker could choose to exploit is the fact that 3D printers use a small set of primitive operations that make consistent acoustic and magnetic emissions. Song et al. [24] were able to conduct a side-channel attack using an ordinary smartphone's sensors. By training a support vector machine to convert sensor data into G-code, they could accurately reconstruct the shape of a design being printed by the widely-used Ultimaker 2 Go.

B. AM Sabotage

AM sabotage most commonly exhibits itself in the manipulation of an AM system to degrade the quality of the manufactured part, though it may also refer to damage done to the AM system itself or its surroundings. The bulk of research done about security challenges in AM fall under this category, as the unique properties of AM open up even more possibilities. One attack unique to AM is the insertion of voids in the middle of a product. Sturm et al. [11] discuss such an attack and show that doing so causes a noticeable degradation in strength while slipping undetected by human operators.

Belikovetsky et al. [6] applied this attack to a real-life scenario from start to finish. Exploiting a patched WinRAR vulnerability on an out-of-date test machine, they inserted gaps inside drone propellers that broke apart in flight. The test machine was intentionally left unpatched, but the main takeaway is that once an attacker gains access to an AM system, they have a wider range of opportunities to sabotage manufactured parts. For example, the previous attack required infiltrating the STL file. But if the attacker gains access to the printer's controls, they can choose to alter the orientation that the part is printed in, which also somewhat unintuitively turns out to impact strength as well, as Zeltmann et al. [7] demonstrate.

C. Illegal Part Manufacturing

Illegal part manufacturing is the creation of products prohibited by law. Unlike the other two intentions mentioned above, which consider an attack by an external actor on the end user, illegal part manufacturing is not an attack in the traditional sense. However, it is still an important consideration, more for the printer manufacturer than the end user. As with all technologies with potential for danger, the thin balance between liberty and safety ought to be explored. There are currently little published works that describe scenarios where such attacks were conducted.

V. Security Recommendations

Although currently there are no specific recommendations for AM systems, guidance is available from NIST for industrial control systems (ICS) and general manufacturing processes. We believe ICS recommendations found in [27] contain many valuable recommendations due to the shared security concerns of AM and ICS systems. Additionally, [28], which is primarily distributed for Federal Information Systems, contains many recommendations relevant to the security of Additive Manufacturing systems due to information systems' reliance on a consistent flow information and the relevance of many of the paper's recommendations to general manufacturing security. Where applicable, recommendation names and descriptions have been paraphrased to contain specific terms that fit the context of AM.

This section is a compilation from three major papers and technical articles from the National Institute of Standards and

TABLE I. CATEGORIZATION OF PAPERS BY PURPOSE

Analyzing a specific attack: Papers with the primary purpose of presenting and analyzing a specific AM attack.	Belikovetsky et al. [6] demonstrate an attack in which a largely undetectable void is added to an AM drone part, causing a disastrous loss of structural integrity. Moore et al. [12] demonstrate an attack on AM quality via malicious printer firmware. Sturm et al. [11] examine potential attack vectors along the AM process chain, and present security recommendations for preventing and detecting attacks. Al Faruque et al. [5] demonstrate an attack that derives the intellectual property of an AM-constructed object by listening on the sounds produced by the construction process and running them through a machine-learning model.
Proposing a security framework: Papers with the primary purpose of presenting a new or modified security framework for the benefit of AM cybersecurity.	Hutchins et al. [17] establish a framework that identifies specific vulnerabilities within a manufacturing supply chain. Padmanabhan and Zhang [13] review cybersecurity risk and mitigation strategies in AM, and propose a framework to "detect threats and assess vulnerabilities in the AM process." They also suggest a new encryption technique to help secure the AM process. Yampolskiy et al. [18] propose a new model for outsourcing Additive Layer Manufacturing (ALM) based manufacturing. Vincent et al. [19] propose an approach to detect attacks in cyber-physical manufacturing systems through the use of structural health monitoring techniques.
Risk Assessment/Analyzing Multiple Attacks: Papers that analyze a variety of attacks on AM or the potential attack vectors of Additive Manufacturing systems.	Prinsloo et al. [20] explore cybersecurity risks associated with the transition to Industry 4.0 and address relevant countermeasures. Yampolskiy et al. [14] analyze attacks that can cause AM machines to exhibit weaponized effects. Zeltmann et al. [7] provide a brief overview of AM security risks and evaluate risks posed by two classes of modifications to the AM process that "are representative of the challenges that are unique to AM." Glavach et al. [8] "address cybersecurity threats to the Direct Digital Manufacturing (DDM) community." Graves et al. [21] assess AM from three security awareness perspectives: "exposure to an attack, evaluation of the system, and potential liability for a successful attack." Slaughter et al. [10] identify techniques used to ensure bad quality in metal AM through malicious manipulating an infrared thermography quality assurance device. Straub [22] discusses attacks on the 3D printing process that involve changes in printing orientation, and proposes an imaging-based solution to combat the problem.

TABLE II. A STRIDE ASSESSMENT OF ADDITIVE MANUFACTURING

Threat type	**Papers**
Spoofing	An attacker may spoof a printer or computer's identity to intercept 3D models [23] or as part of a larger attack to take control of and sabotage an AM system [6].
Tampering	Assuming access was gained through another attack, an adversary may choose a number of ways to sabotage the system, including, but not limited to, inserting invisible voids [11], altering print settings [7], and/or installing malicious firmware [12].
Repudiation	Repudiation is a generally overlooked threat in AM security articles. Considering secure logging is not a built-in standard in 3D printers, an attacker would simply need to target the tracing capabilities of the surrounding infrastructure.
Information Disclosure	Traditional malware could be deployed to steal the 3D model, which can exist in many forms and place [11]. There also exists side-channel attacks that listen to the predictable acoustic and magnetic emissions of a printer to reconstruct IP with a machine learning model [5] [24].
Denial of Service	One who has gained control of a poorly designed 3D printer may hypothetically manipulate its operating parameters e.g. the electron/laser beam or source material to inflict irreversible damage upon itself.
Elevation of Privilege	Privilege escalation is used as a stepping stone to launch further attacks [6]. However, it is not even needed for some AM systems that perform incorrect authentication or none at all [23].

TABLE III. CATEGORIZATION OF ATTACKS BY INTENT

Adversary's intent	**Papers**
Technical data theft	Al Faruque et al. [5] describe a novel side-channel attack in which a machine learning model is used to derive an object's geometry by analyzing the noise created by a Fused Deposition Modeling (FDM) 3D printer. Yampolskiy et al. [18] emphasize how there are many places along the AM supply chain in which IP can be stolen, and offer a unique outsourcing model to help secure the process. Campbell and Ivanova [25] describe the potential for AM to increase the ease of violating patents and producing patented products.
AM sabotage	Sturm et al. [11] describe the ease of creating voids in products fabricated by AM to sabotage their mechanical strength. Zeltmann et al. [7] describe how embedded defects and altered printing orientation can negatively affect a printed object's integrity as well. Belikovetsky et al. [6] and Vincent et al. [19] demonstrate the consequences of these attacks by testing sabotaged parts on real-life equipment. Moore et al. [12] takes another route and sabotages the printer firmware, replacing it with a malicious version that can corrupt the print jobs as they are received.
Illegal part manufacturing	Kietzmann et al. [26] describe the potential for AM to catalyze the creation of fake medical products and drugs. Campbell and Ivanova [25] describe the potential of bad actors to manufacture illegal gun parts through AM.

Technology (NIST) regarding security practices to counteract malicious attacks in the cyber and cyber-physical domains. The recommendations come from NIST's Guide to Industrial Control Systems (ICS) Security [27], Security and Privacy Controls for Federal Information Systems and Organizations [28], and Framework for Improving Critical Infrastructure Cybersecurity [29]. We organized these recommendations along STRIDE threat model, describing how to mitigate the different threat types.

A. Spoofing and Repudiation

- **Identity Management, Authentication and Access Control:** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- **Security Monitoring:** The system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. This includes monitoring for unauthorized personnel, connections, devices and software.
- **Access Enforcement:** The system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- **Remote Access:** The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed, and authorizes remote access to the system prior to allowing such connections.
- **Least Functionality:** The organization configures the system to provide only essential capabilities; and

prohibits or restricts the use of prohibited or restricted functions, ports, protocols, and/or services.

- **Device Authentication:** The system uniquely identifies and authenticates devices before establishing a connection.
- **Adaptive Identification and Authentication** The organization requires that individuals accessing the system employ supplemental authentication techniques or mechanisms under circumstances or situations determined to need the extra security.
- **Physical Access Authorizations:** The organization develops, approves, and maintains a list of individuals with authorized access to the location of the system and issues authorization credentials for such access.
- **Developer Security Architecture and Design:** The organization requires the developer of the system, system component, or system service to produce a design specification and security architecture that:
    - Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
    - Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
    - Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
- **Boundary Protection:** The system connects to external networks or other systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
- **Network Disconnect:** The system terminates the network connection associated with a communications session at the end of the session or after an organization-determined time period of inactivity.
- **Session Authenticity:** The system protects the authenticity of the communications sessions.
- **Information System Monitoring:** The organization
    - Monitors the system to detect:
        - Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and
        - Unauthorized local, network, and remote connections.
    - Identifies unauthorized use of the system through relevant techniques and methods;
    - Deploys monitoring devices:
        - Strategically within the system to collect essential information; and
        - At ad hoc locations within the system to track specific types of transactions of interest to the organization; and
    - Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- **Firewalls:** The organization deploys appropriate firewall policies at pertinent locations to avoid unauthorized access to systems and resources.
- **Repudiation:** The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation, which may include creating information, sending and receiving messages, or approving information.

B. Tampering, Denial of Service and Elevation of Privilege

- **Risk Assessment:** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- **Anomalies and Events:** Anomalous activity is detected and the potential impact of events is understood.
    - Detected events are analyzed to understand attack targets and methods;
    - Event data are collected and correlated from multiple sources and sensors; and
    - The impact of events is determined.
- **Security Continuous Monitoring:** The system and its assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
    - The network is monitored to detect potential cybersecurity events;
    - The physical environment is monitored to detect potential cybersecurity events;
    - Personnel activity is monitored to detect potential cybersecurity events;
    - Malicious code is detected;
    - Unauthorized mobile code is detected;
    - External service provider activity is monitored to detect cybersecurity events; and
    - Vulnerability scans are performed.
- **Detection Processes:** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
- **Continuous Monitoring:** The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
    - Establishment of metrics to be monitored.
    - Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.
- **Software Usage Restrictions:** The organization uses software and associated documentation in accordance with contract agreements and copyright laws, and tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution.
- **User-Installed Software:** The organization establishes policies governing the installation of software by users and enforces software installation policies through organization-defined methods.

- **Incident Monitoring:** The organization tracks and documents security incidents impacting the system.
- **Risk Assessment:** The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits.
- **Vulnerability Scanning:** The organization:
    - Scans for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
    - Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
        - Enumerating platforms, software flaws, and improper configurations;
        - Formatting checklists and test procedures; and
        - Measuring vulnerability impact.
    - Analyzes vulnerability scan reports and results from security control assessments; and
    - Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk.
- **Supply Chain Protection:** The organization protects against supply chain threats to the system, system component, or system service by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.
- **Criticality Analysis:** The organization identifies critical system components and functions by performing a criticality analysis.
- **Tamper Resistance and Detection:** The organization implements a tamper protection program for the system, system component, or system service.
- **Customized Development of Critical Components:** The organization re-implements or custom develops system components deemed critical enough by the organization to take such measures.
- **Application Partitioning:** The system separates user functionality (including user interface services) from system management functionality.
- **Security Function Isolation:** The system isolates security functions from nonsecurity functions.
- **Trusted Path:** The system establishes a trusted communications path between the user and organization-defined security functions to include at a minimum, system authentication and re-authentication.
- **Protection of Information at Rest:** The system protects the confidentiality and/or integrity of organization-defined information at rest.
- **Malicious Code Protection:** The organization:
    - Employs malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
    - Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
    - Configures malicious code protection mechanisms to:
        - Perform periodic scans of the system at a defined frequency and real-time scans of files from external sources at specified endpoints and/or entry and exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
    - Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
- **Software, Firmware, and Information Integrity:** The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.
- **Information Input Validation:** The system checks the validity of organization-defined information inputs.
- **Error Handling:** The system
    - Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
    - Reveals error messages only to trusted personnel or roles.
- **Memory Protection:** The system implements organization-defined security safeguards to protect its memory from unauthorized code execution.
- **Denial of Service Protection:** The system protects against or limits the effects of denial of service attacks by employing aforementioned organization-defined security safeguards.

C. Information Disclosure

- **Governance:** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- **Data Security:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- **Information Protection Processes and Procedures:** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of systems and assets.
- **Component Authenticity:** The organization develops and implements anti-counterfeit policy and procedures that include the means to detect and prevents counterfeit components from entering the system.

- **Information in Shared Resources:** The system prevents unauthorized and unintended information transfer via shared system resources.
- **Transmission Confidentiality and Integrity:** The system protects the confidentiality and/or integrity of transmitted information.
- **Wireless Link Protection:** The system protects external and internal wireless links from designated types of signal parameter attacks or references to sources for such attacks.
- **Boundary Protection:** Boundary protection devices are implemented to control the flow of information between interconnected security domains to protect the system against malicious cyber adversaries and non-malicious errors and incidents...Boundary protection devices determine whether data transfer is permitted, often by examining the data or associated metadata.

VI. Conclusion and Future Work

Additive Manufacturing is a technology with enormous potential. However, this makes it easy to rush things to market without taking due consideration of security implications. And because AM is still a developing area of research, it is a challenge to properly secure systems against the expanded variety of things that could go wrong. In this paper, we considered the mind of the opposition by analyzing the intent of the attacker and discussing many possible ways for an attacker to achieve their goal. Furthermore, we categorized these attacks into the STRIDE model and compiled a number of steps that one could take to secure each category. Since AM is a developing area of research, there are still a number of questions that should be further explored:

A. Exactly how much work have manufacturers of consumer and industrial AM devices put into securing their systems?

Do, Martini, and Choo [23] have shown an instance where a 3D printer manufacturer neglected fundamental security practices. However, this is just a single case in a consumer printer. Although we believe this may be an expected symptom of the emerging nature of AM, we do not have enough data to conclude if this is an isolated incident or a widespread concern, and how much worse, if at all, it is than in traditional manufacturing.

B. Are there any additional properties unique to AM that an attacker could exploit?

A key benefit of AM is that it gives manufacturers more flexibility, but at the same time gives malicious actors more opportunities to attack. We covered several such attacks that are only possible or simplified on AM, such as those given by [11] and [7]. We anticipate that a motivated adversary will find even more ways to cleverly exploit AM's advantages. More work can be done to explore other attacks and raise awareness among AM users.

C. What steps, if any, should be taken to prevent the use of 3D printers for potential harm, such as illegal part manufacturing?

We have so far exclusively focused on securing 3D printers so that the user is protected from any malicious actions by outside actors. Graves et al. [21] make the case for considering securing 3D printers so that the outside community environment is protected from destructive uses of this technology.

Regardless, we hope this paper provides a useful, understandable overview of AM security from all sides and concrete ideas for what next steps can be taken.

Acknowledgment

The authors would like to acknowledge the infrastructure and support of Center for Agile & Adaptive and Additive Manufacturing funded through State of Texas Appropriation (#190405-105-805008-220).

References

[1] D. Thomas, "Costs, benefits, and adoption of additive manufacturing: a supply chain perspective," The International Journal of Advanced Manufacturing Technology, vol. 85, no. 5, 2016, pp. 1857–1876. [Online]. Available: https://doi.org/10.1007/s00170-015-7973-6

[2] P. O, "3-d printing is changing the way air force fixes its aging planes," URL: https://www.military.com/defensetech/2017/05/02/3-d-printing-is-changing-way-air-force-fixes-its-aging-planes [accessed : 2020-05-21].

[3] J. Kite-Powell, "Fda approved 3d printed drug available in the us," URL: https://www.forbes.com/sites/jenniferhicks/2016/03/22/fda-approved-3d-printed-drug-available-in-the-us [accessed: 2020-06-02].

[4] R. Tino, R. Moore, S. Antoline, P. Ravi, N. Wake, C. Ionita, J. Morris, S. Decker, A. Sheikh, F. Rybicki, and L. Chepelev, "Covid-19 and the role of 3d printing in medicine," 3D Printing in Medicine, vol. 6, 12 2020.

[5] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). IEEE, Apr 2016. [Online]. Available: http://dx.doi.org/10.1109/ICCPS.2016.7479068

[6] S. Belikovetsky, M. Yampolskiy, J. Toh, and Y. Elovici, "dr0wned - cyber-physical attack with additive manufacturing," CoRR, vol. abs/1609.00133, 2016. [Online]. Available: http://arxiv.org/abs/1609.00133

[7] S. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3d printing," JOM, vol. 68, 2016, pp. 1872–1881.

[8] D. Glavach, J. LaSalle-DeSantis, and S. Zimmerman, Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems. Springer International Publishing, 2017, p. 173–194. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-50660-9_7

[9] S. Moore, P. Armstrong, T. McDonald, and M. Yampolskiy, "Vulnerability analysis of desktop 3d printer software," in 2016 Resilience Week (RWS). IEEE, Aug 2016. [Online]. Available: http://dx.doi.org/10.1109/RWEEK.2016.7573305

[10] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, and Y. Elovici, "How to ensure bad quality in metal additive manufacturing," in Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17. ACM Press, 2017. [Online]. Available: http://dx.doi.org/10.1145/3098954.3107011

[11] L. Sturm, C. Williams, J. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .stl file with human subjects," Journal of Manufacturing Systems, vol. 44, Jul 2017, p. 154–164. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612517300961

[12] S. Moore, W. Glisson, and M. Yampolskiy, "Implications of malicious 3d printer firmware." Proceedings of the 50th Hawaii International Conference on System Sciences, 01 2017, pp. 6089–6098.

[13] A. Padmanabhan and J. Zhang, "Cybersecurity risks and mitigation strategies in additive manufacturing," Progress in Additive Manufacturing, vol. 3, no. 1-2, 2018, pp. 87–93.

[14] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. A. Overfelt, K. R. Sloan, and A. Yasinsac, "Using 3d printers as weapons," International Journal of Critical Infrastructure Protection, vol. 14, 2016, pp. 58 – 71. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548215300330

[15] W. Ashford, "WannaCry and NotPetya inspiring new attacks," URL: https://www.computerweekly.com/news/252449265/WannaCry-and-NotPetya-inspiring-new-attacks [accessed: 2020-05-21].

[16] N. Shevchenko, "Threat Modeling: 12 Available Methods," URL: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html [accessed: 2020-05-24].

[17] M. J. Hutchins, R. Bhinge, M. K. Micali, S. L. Robinson, J. W. Sutherland, and D. Dornfeld, "Framework for identifying cybersecurity risks in manufacturing," Procedia Manufacturing, vol. 1, 2015, pp. 47 – 63, 43rd North American Manufacturing Research Conference, NAMRC 43, 8-12 June 2015, UNC Charlotte, North Carolina, United States. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978915010604

[18] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac, "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in Proceedings of the 4th Program Protection and Reverse Engineering Workshop, ser. PPREW-4. New York, NY, USA: Association for Computing Machinery, 2014. [Online]. Available: https://doi.org/10.1145/2689702.2689709

[19] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," Procedia Manufacturing, vol. 1, 2015, p. 77–85. [Online]. Available: http://dx.doi.org/10.1016/j.promfg.2015.09.065

[20] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," Applied Sciences, vol. 9, no. 23, Nov 2019, p. 5105. [Online]. Available: http://dx.doi.org/10.3390/app9235105

[21] L. M. G. Graves, J. Lubell, W. King, and M. Yampolskiy, "Characteristic aspects of additive manufacturing security from security awareness perspectives," IEEE Access, vol. 7, 2019, pp. 103 833–103 853.

[22] J. Straub, "Identifying positioning-based attacks against 3D printed objects and the 3D printing process," in Pattern Recognition and Tracking XXVIII, M. S. Alam, Ed., vol. 10203, International Society for Optics and Photonics. SPIE, 2017, pp. 22 – 34. [Online]. Available: https://doi.org/10.1117/12.2264671

[23] Q. Do, B. Martini, and K.-K. R. Choo, "A data exfiltration and remote exploitation attack on consumer 3d printers," IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, 2016, pp. 2174–2186.

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

[25] T. A. Campbell and O. S. Ivanova, "Additive manufacturing as a disruptive technology: Implications of three-dimensional printing," Technology & Innovation, vol. 15, no. 1, Jan. 2013, pp. 67–79. [Online]. Available: https://doi.org/10.3727/194982413x13608676060655

[26] J. Kietzmann, L. Pitt, and P. Berthon, "Disruptions, decisions, and destinations: Enter the age of 3-d printing and additive manufacturing," Business Horizons, vol. 58, no. 2, 2015, pp. 209 – 215, eMERGING ISSUES IN CRISIS MANAGEMENT. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0007681314001608

[27] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security," Tech. Rep., Jun. 2015. [Online]. Available: https://doi.org/10.6028/nist.sp.800-82r2

[28] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations," Tech. Rep. 53, Apr. 2013. [Online]. Available: https://doi.org/10.6028/nist.sp.800-53r4

[29] Critical Infrastructure Cybersecurity, "Framework for improving critical infrastructure cybersecurity," URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [accessed: 2020-06-18].