Intellectual Property Protection and Security in Additive Manufacturing

Abraham GEORGE[a], Anthony NEWELL[a], and Nikolaos PAPAKOSTAS[a,1]
[a]Laboratory for Advanced Manufacturing Simulation and Robotics, School of Mechanical and Materials Engineering, University College Dublin, Dublin 4, Ireland

Abstract. Product data management along a product lifecycle is complicated due to a wide range of resources, stakeholders and technologies being involved. During the product development phase, complex information is exchanged among several engineering teams and legal entities. Product lifecycle management (PLM) systems streamline and control the product data shared with other engineering and manufacturing parties. In additive manufacturing (AM), however, as opposed to the conventional manufacturing (CM) data supply chain, the ease with which intellectual property (IP) can be compromised by theft or malicious attacks, creates a significant challenge. These attacks can lead to loss of revenue due to illegal counterfeiting, or even failure of mission-critical parts where design could be modified to a functionally impaired configuration. This paper outlines and reviews the current strategies and new approaches possible to secure IP in AM systems, comparing the advantages and disadvantages of these technologies.

Keywords. Manufacturing workflow, blockchain technologies, design for additive manufacturing, agent-based systems.

1. Introduction

AM is defined as “the process of joining materials to make objects from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies, such as traditional machining” [1]. AM provides many advantages and opportunities that could potentially lead to novel manufacturing strategies, including increased design freedom, improved spare parts management policies, decentralised manufacturing, highly customised one-of-a-kind products and enhanced supply chain management. Moreover, organizations can achieve faster product development cycles and lower development costs using AM [2]. AM’s digital workflow enables automated, cyber-physical manufacturing systems and faster data flow between systems and stakeholders. However, this same digital workflow makes it much easier for malicious agents to steal or modify IP. In order to remain competitive in today’s globalised market, it is of paramount importance for companies and original equipment manufacturers (OEMs) to securely manage product IP [3]. The following sections of this paper will consider IP security and vulnerabilities along the AM workflow and product lifecycle together with attack methods and their implications. A review of technologies developed for securing companies’ IP follows in the next sections of this paper.

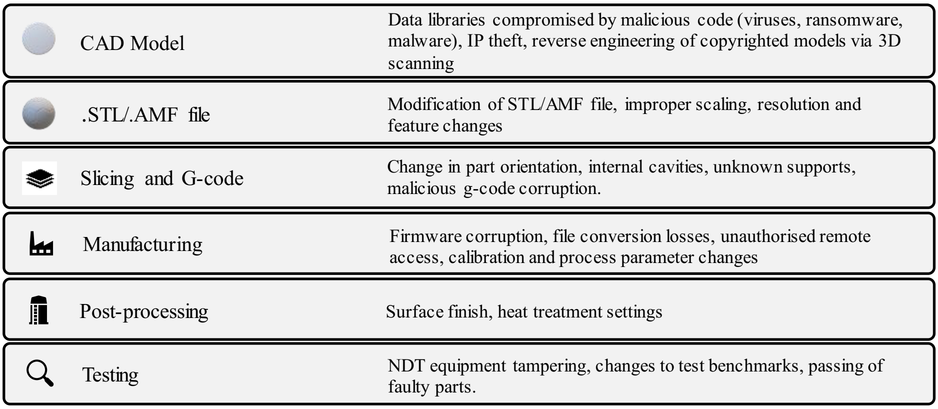
[1] Corresponding Author. nikolaos.papakostas@ucd.ie

2. AM IP security vulnerabilities and attack points

PLM systems enable the efficient management and exchange of data among diverse stakeholders and across different phases of the product lifecycle [4]. Sensitive product data can typically be exchanged using PLM or Product Data Management (PDM) systems, including IP related to AM product data [5]. PLM systems typically provide their own trusted domains, allowing for the integration of trusted third parties (TTP), enforcing, in theory, secure information sharing and management policies. However, outside of this domain, visibility, control and the tracking of data are almost impossible [6]. There is also a substantial risk involved in using TTPs such that if they are compromised, so is all the sensitive IP.

AM product IP and especially digital information pertaining to the design, manufacture, and maintenance of parts is constantly exchanged between different PLM and data management platforms, stakeholders and computer systems. A challenge for companies is preventing the theft or the malicious modification of IP during transfer and use [7]. Vulnerabilities do exist across the AM product lifecycle, which can be exploited by malicious agents, resulting in lost revenue due to counterfeit products or sabotage of part designs by alteration of 3D models and process parameters. For example, an unintentional or intentional change in the design data, such as the introduction of defects, removal or alteration of features, may compromise the structural integrity of a manufactured part leading to its failure when in use. Similar possibilities exist in the aerospace and medical devices industry, where sabotage of sensitive IP related to mission-critical part designs and implants for patients could lead to injury or death.

Specifically, possible attack points for the AM workflow can lead to the theft or corruption of IP, which in turn can undermine the design data, machine code, toolpath, process parameters, post-processing steps, and test methods [3]. Some of the possible attack points across the product lifecycle for AM are outlined in Figure 1. At the beginning of the workflow, an attack can occur by the theft or modification of the CAD model. A CAD 3D part model alone is not sufficient for generating the machine code for manufacturing an AM part. A Computer Aided Manufacturing (CAM) tool is required for this task.



CAD Model	Data libraries compromised by malicious code (viruses, ransomware, malware), IP theft, reverse engineering of copyrighted models via 3D scanning
.STL/.AMF file	Modification of STL/AMF file, improper scaling, resolution and feature changes
Slicing and G-code	Change in part orientation, internal cavities, unknown supports, malicious g-code corruption.
Manufacturing	Firmware corruption, file conversion losses, unauthorised remote access, calibration and process parameter changes
Post-processing	Surface finish, heat treatment settings
Testing	NDT equipment tampering, changes to test benchmarks, passing of faulty parts.

Figure 1. Attack points in the AM process flow [3].

In particular, it is typically first converted to a format readable by specific CAM software, which is normally used with specific AM machines, to generate the toolpath instructions (G-code). The STL file format is the most common standard. STL files are commonly shared rather than CAD models, as they are not directly editable in CAD software which can protect the IP. They are, however, unencrypted and can in certain cases be converted to solid models by methods available in proprietary CAD software.

The modification of an STL file leading to the part failure was demonstrated in a study, whereby a deliberate modification was made to a propeller STL file for a drone, through a hacked computer system. The introduction of the functional defect into the propeller model led to the accelerated fatigue and failure of this critical AM part during operation and resulted in substantial damage [8].

At the manufacturing stage, AM processes produce acoustic, thermal and electrical emissions during their operation. Side channel attacks are a kind of reverse engineering method, which exploits the recording of these emissions for the theft of IP by its reconstruction. The frequency and amplitude of the sound generated by the stepper motors movement along each axis and the filament extrusion can be uniquely correlated with the toolpath, thus allowing attackers to generate the 3D model [9]. Experimental demonstration of this method was evaluated and shown an average accuracy for axis prediction at a level of 78.35% and an average prediction error of 17.82% when regression models and machine learning algorithms were employed [9]. Even smartphone sensors can be effectively used for side channel attacks [10]. Shortcomings of this method include the required proximity of recording source, difficulties correlating features involving short and rapid motions as well as acquiring features with multi-axis movements [10].

At the use stage, 3D scanning of AM parts can be used to reverse engineer proprietary designs leading to counterfeiting of parts and lost revenue. Further to this, poor quality and untested models generated from 3D scans can lead to defective products. Photogrammetry may be used for this purpose whereby a series of 2D photographs of a part are combined to generate a 3D model. Design feature-measurement algorithms can also be used to recreate proprietary models with higher fidelity using CAD software tools.

3. AM IP security protection solutions

3.1. Security through obscurity

IP related to AM CAD models may be protected by modifying the models through embedding or introducing design features. ObfusCADe is an experimental deployment of this technique with promising results [11]. The obscure features in a component modify the model in such a way that the embedded features can be printed as defects and therefore, reduce the life and performance of the component. The examples tested included an embedded solid sphere surface or solid model, which would print a void within the part depending on the printer material removal configuration. These design features restrict the development of AM products to a unique set of the process parameters in order to ensure the quality and integrity of the finished product. Any deviation from the unique set of parameters can result in premature failure under typical conditions of stress and temperature.

3.2. Protection against AM part counterfeiting using optical and chemical agents

Embedding security features in AM parts, such as optical refractive nanoparticles (NPs), has been used to protect IP by safeguarding it against counterfeiting [12]. These particles are called Physical Unclonable Functions (PUFs). One of the advantages of this method is that the number and location of NPs embedded within the part are randomly assigned such that every configuration of these NPs is unique to each part. The NP could be in the form of a Quantum Dot (QD) particle that is able to absorb ultraviolet (UV) light and emit in the visible light spectrum. This feature is used for providing verification of the product by checking the NP cluster through a secure computer algorithm. In a similar manner, it is possible to dope the product with chemicals during AM and then analyse the chemical signature during non-destructive testing in the finished product [13]. Both methods make counterfeiting of parts containing these features almost impossible.

3.3. Blockchain technologies for IP protection

Blockchain is a ledger-based system consisting of a chain of blocks connected using cryptographic methods [14]. Blockchains maintain a permanent decentralized record of transactions, which is visible to anyone on the network. The ease of verification means that data stored within blockchains are not easily corrupted. There are public and private blockchain networks. To address privacy concerns a private blockchain network could be used for managing IP. Private blockchains do not require the highly demanding proof-of-work methods that are used for verifying blocks in public blockchains but instead take advantage of trusted verifiers on the network to add blocks.

The ‘Secure Additive Manufacturing Platform’ (SAMPL) is a blockchain-based AM data management platform, which is used for IP protection by managing the product data digital licenses [15]. SAMPL can manage the exchange of licenses across a series of product development phases, starting with the sharing of the product by the IP holder and ending with the fabrication of the part by the AM service provider. The combination of blockchain technologies with physical security features, such as radio frequency identification (RFID) tags for AM products, creates a secure platform, which the researchers referred to as “Chains of Trust” [15]. The public blockchain Ethereum was utilised for the transfer of licenses within this platform.

A conceptual framework employing a multi-agent system for managing AM product development data utilising blockchain technology principles was proposed [16]. This system could provide a more lightweight and affordable product data management option for small to medium enterprises (SMEs).

3.4. Protection from side channel attacks

Protection of IP from side-channel attacks can be achieved by modification of the CAM software used to generate the toolpath or by configuration of the AM process parameters and hardware. For protection against acoustic side-channel attacks, one of the methods is to create a dynamic toolpath, in which different print speeds and environment settings can be selected from the acceptable ranges for the material, such that the quality is not compromised [10]. This aims at disrupting the toolpath prediction models used to gauge the printer speed and axis of movement of the nozzle head. Another method is to create dummy tasks by displacing nozzle head in random directions with no actual extrusion, to trick the malicious sensors. The downside to this method is the increase in print time.

As far as the possible modification of the hardware is concerned, it is possible to provide shielding of acoustic and electromagnetic emissions from the printer. The shielding can be in the form of ferromagnets for disrupting electromagnetic signals and fabric padding or gaskets to isolate the acoustic signals. The disadvantage of this method is that it adds further cost and may affect the usability of the printer [10].

3.5. Patenting

Patenting protects IP by giving its owner the right to exclude other partners from making, using, selling, and importing an invention for a limited period of time [17]. Patenting can be realised in the form of a design patent, which patents the design concepts of a product with features of the design but might not extend to the functionality of the product [18]. On the other hand, a utility patent is a more extensive patenting process that includes the materials, AM machines, features of the product, functionality, manufacturing and assembly detail. The downsides to patenting are that the time and cost of successfully filing a patent are both quite significant and it requires a lot of expertise to go through the entire process. The average time for a successful filing may well be around 20 months and as far as costs are concerned, there are legal, filing, and maintenance fees to be taken into consideration. This is a significant hurdle as it can increase time and cost associated with product development [19]. Further to this, the effective legal enforcement of patents is complicated by the ease with which AM parts can be replicated through the democratisation of manufacturing and the difficulty associated with identifying patent rights infringement [19].

4. Conclusion

The security of AM product IP is an important consideration for manufacturing companies. IP theft can lead to lost revenue by illegal counterfeiting. Furthermore, product development data may be maliciously modified leading to functionally impaired products. This paper presents an overview of AM IP security vulnerabilities and attack points along the AM product lifecycle given its predominantly digital workflow. The security shortcomings across the product lifecycle were discussed together with how sophisticated attacks can circumvent IP protection methods, such as side-channel attacks in AM systems. As a CAD file is typically all that is required for the replication of a part using AM technologies, it is important to develop and use systems, which can effectively secure IP. Technologies including modified CAD models, embedding NPs, blockchain for license transfer, shielding from side-channel attacks, and obtaining patent licenses have the potential to combat the rising threats to AM IP security and are still being tested and developed for widespread adoption. These technologies were reviewed in the pursuit to identify effective methods. Blockchain-based technologies have shown promise for enabling better IP protection. Due to the low technology readiness levels of some of the proposed solutions, further research is necessary to understand the financial and technological implications of their deployment in the AM workflow. CAD file encryption and advanced product authentication methods, such as monitoring RFID tags and embedded NPs could deter counterfeiting and may provide further solutions for AM IP security in the future.

Acknowledgements

This publication has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) under Grant Number 16/RC/3872 and is co-funded under the European Regional Development Fund and I-Form industry partners.

References

[1] ASTM International, ISO/ASTM 52900:2015(E) Standard terminology for additive manufacturing technologies - general principles - terminology, (2015).

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

[3] A. Brown, M. Yampolskiy, Y. Elovici, S. Belikovetsky, A. Skjellum, W.E. King, and J. Gatlin, Security of additive manufacturing: Attack taxonomy and survey, Additive Manufacturing 21 (2018), 431–457.

[4] J. Li, F. Tao, Y. Cheng, and L. Zhao, Big Data in product lifecycle management, International Journal of Advanced Manufacturing Technology 81 (1–4) (2015), 667–684.

[5] M. David and F. Rowe, What does PLMS (product lifecycle management systems) manage: Data or documents? Complementarity and contingency for SMEs, Computers in Industry 75 (2016), 140–150.

[6] R. Ranchal and B. Bhargava, Protecting PLM Data Throughout Their Lifecycle, QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 115 (2013), 633–642.

[7] C. Holligan, V. Hargaden, and N. Papakostas, Product lifecycle management and digital manufacturing technologies in the era of cloud computing, in 2017 Int. Conf. Eng. Technol. Innov. Eng. Technol. Innov. Manag. Beyond 2020 New Challenges, New Approaches, ICE/ITMC 2017 - Proc., (2018): pp. 909–918.

[8] S. Belikovetsky, M. Yampolskiy, J. Toh, and Y. Elovici, dr0wned - Cyber-Physical Attack with Additive Manufacturing, in 11th USENIX Work. Offensive Technol., (2016): pp. 1–16.

[9] 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 Int. Conf. Cyber-Physical Syst. ICCPS 2016 - Proc., (2016).

[10] 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 Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16, (2016): pp. 895–907.

[11] N. Gupta, F. Chen, N.G. Tsoutsos, and M. Maniatakos, ObfusCADe, in Proc. 54th Annu. Des. Autom. Conf. 2017, (2017): pp. 1–6.

[12] O. Ivanova, A. Elliott, T. Campbell, and C.B. Williams, Unclonable security features for additive manufacturing, Additive Manufacturing 1 (2014) (2014), 24–31.

[13] T.R. Pope, J.F. Christ, Z.C. Kennedy, D.E. Stephenson, M.G. Warner, C.A. Barrett, and B.W. Arey, Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology, Journal of Materials Chemistry C 5 (37) (2017) , 9570–9578.

[14] S. Trouton, M. Vitale, and J. Killmeyer, 3D opportunity for blockchain, Deloitte University Press (2016).

[15] M. Holland, J. Stjepandic, and C. Nigischer, Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology, in 2018 IEEE Int. Conf. Eng. Technol. Innov. ICE/ITMC 2018 - Proc., (2018).

[16] N. Papakostas, A. Newell, and V. Hargaden, A novel paradigm for managing the product development process utilising blockchain technology principles, CIRP Annals - Manufacturing Technology (2019), In Press.

[17] A. Brown, M. Yampolskiy, J. Gatlin, and T. Andel, Legal aspects of protecting intellectual property in additive manufacturing, in IFIP Adv. Inf. Commun. Technol., (2016): pp. 63–79.

[18] T. Kurfess and W.J. Cass, Rethinking Additive Manufacturing and Intellectual Property Protection, Research-Technology Management 57 (5) (2014), 35–42.

[19] J. Hornick, 3D Printing and IP Rights: The Elephant in the Room, Santa Clara L. Rev. 55 (2015) , 801.