Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing Platforms

Chris Adkins
Identify3D, Inc.
Lexington, KY USA
chris@identify3d.com

Stephan Thomas
Identify3D, Inc.
San Francisco, CA USA
stephan@identify3d.com

Daniel Moore
Identify3D, Inc.
Lexington, KY USA
daniel@identify3d.com

ABSTRACT

Additive Manufacturing (AM) Platform is a new technology and commercial business model which enables production of additively made parts through an on-line market of AM designs, services, and manufacturing. Customers who are designing parts to be manufactured with additive technologies can upload their designs to the AM Platform and find a manufacturing partner based on technical capabilities, geographic location, and cost. By providing an easy to use online platform, companies can expect to optimize their cost, quality, and lead-time through a competitive bid process.

This research investigates the cybersecurity issues inherent to an online marketplace and platform which shares data containing Intellectual Property (IP) between multiple companies. Based on currently implemented business models in the AM Platform industry, the most common use cases will be examined to determine any vulnerabilities associated with data and IP sharing between the platform, its customers, and vendors. Finally, based on the vulnerabilities discovered, a set of cybersecurity solutions will be proposed in order to protect the confidentiality and integrity of the data and ultimately the customers IP through the AM Platform.

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

ACM ISBN 978-1-4503-8480-3/21/11□$15.00
https://doi.org/10.1145/3462223.3485622

CCS CONCEPTS

• Security and privacy ~ Security services ~ Digital rights management

KEYWORDS

AM Printing, AM Platform, Cybersecurity, Digital Rights Management, IP Protection, Data Integrity, Data Security

ACM Reference format:

Chris Adkins, Stephan Thomas and Daniel Moore. 2021. Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing Platforms. In *Proceedings of AMSec 2021: International Workshop on Additive Manufacturing (3D Printing) Security. November 19, 2021. Virtual Event.*, 5 pages. https://doi.org/10.1145/3462223.3485622

1 Background of AM Platform

The technological advances in Additive Manufacturing (AM) have enabled the emergence of not only new companies in hardware, software, and material but also completely new business models such as Additive Manufacturing Platforms. The main concept of an AM Platform is to provide the opportunity for a customer to upload or select from a catalogue, a digital part, obtain a quote for its manufacturing, and select one or many manufacturers to additively produce the part.[1]

The ultimate benefit of these platforms is to provide true decentralized manufacturing by allowing a part to be produced at the time and place of need (hence reducing inventory, obsolescence and transportation costs). It also provides scalability for companies using additive manufacturing internally by enabling a rapid ramp up of production when resources are at capacity. Finally, through the quote/bidding process, these platforms are in a position to potentially reduce AM production costs.

Some of the major players in the platform space are established industrial players such as Siemens (Siemens Additive Network), and Wilhelmsen/Thyssenkrupp (a platform focused on maritime parts). Startups such as Xometry (which recently went public through an IPO), 3Dhubs (acquired by Prodways), Replique (incubated by BASF), Jellypipe, and Abilista have also entered their own competing products into the marketplace.

2 Use Cases

Before security can be considered, customer use cases for an AM Platform must be outlined and discussed. As the AM Platform industry is nascent, and the technology is quickly evolving, predicting the long-term usage scenarios is difficult. Therefore, the focus will be on identifying the most common use cases that represent the most diverse data flow and contribute to security vulnerabilities.

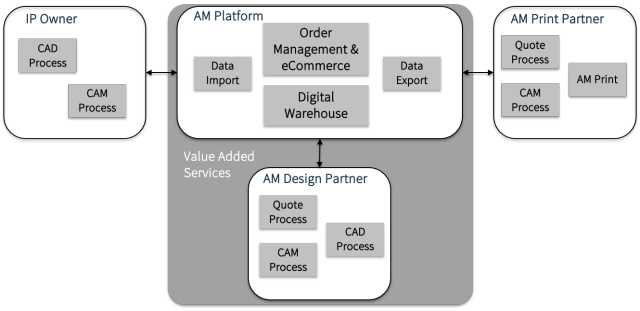

Figure 1: AM Platform Processes and Interactions

The primary customer of the AM Platform is the owner of the design data/IP. Whether the IP owner is interested in producing parts, licensing their IP, or selling parts directly, they need to retain as much control over their IP as possible. To be successful, the AM Platform must protect their customers IP from theft, counterfeit, non-intentional or malicious modification, and unauthorized production.

Within a digital AM workflow, there are several data transformations that occur from initial part concept to production on an additive machine. In most cases, the IP owner will use a CAD process to produce a 3D part file as a digital representation of the physical part to be produced by the AM printer. Although the CAD process itself is complex and may require multiple CAD tools, generally the IP owner performs and controls this entire process. Once the 3D part file is designed, the AM manufacturing process must be defined using CAM tools. In general, a CAD tool will convert the 3D part file into an STL representation for processing by CAM tools. To optimize the final part, the CAM process needs the STL generated by the CAD tools. An AM expert will take the quality, mechanical, and material requirements for the physical part then orient the part on the build plate, generate appropriate support structures, and set the printer specific parameters based on these requirements. Once these steps are complete, the CAM tool will generate a build file, specific for each targeted machine. The build file will be consumed by the AM printer in order to manufacture the part.

With the IP owner as the customer, there are two primary use case classes to consider. The first is the case in which the IP owner has provided build files that are ready for production. In this case, the AM Platform will send the build file to an AM Print Partner to produce a defined number of physical parts. In the second case, the part data files require CAM processing, and in some cases additional CAD processing, in order to generate a build file that is ready for AM production. At that point, the IP owner could download the build files to be manufactured in their own facility or continue with the first use case and produce AM parts through an AM Print Partner.

The beginning of the AM lifecycle at the AM Platform starts with the IP owner uploading data to the platform. Depending on the preference of the IP owner, this data could be an STL with no CAM processing or a build file ready for consumption by an AM printer, along with associated production requirements. Once the data is uploaded, the AM Platform will store the 3D data files in the platform's digital warehouse. Additionally, the AM Platform will initiate the order management process for the uploaded part data.

Whether the IP owner needs CAM processing or just part manufacturing, the AM Platform must find appropriate partners to provide these services. Currently, AM Platforms use multiple approaches to establish these partnership services. Often the AM Platform will have existing partnerships with multiple vendors and will choose the vendor based on availability to perform the needed services and on geographic location for manufacturing. Some platforms are using Artificial Intelligence (AI) to find an optimal match. In other cases, the AM Platform will facilitate a competitive Request for Quote (RFQ), in which vendors can bid on the services, and the IP owner choses the vendor based on the quote results. If high-value and specialized services are required, then the AM Platform may have a complex algorithm it uses to determine the unique requirements of the AM part and find a vendor with the capabilities to deliver the required service. Additionally, some CAD/CAM services may be offered as value added services by the AM Platform itself, as show in Figure 1.

Regardless of the system used to match the customer with a service provider, the AM Platform must utilize some type of RFQ process. To provide an accurate quote, the vendor must have a complete understanding of the requirements for the CAM process and part manufacturing as well as an appropriate level of detail about the part itself.

Once the RFQ is complete and a service provider is chosen, the AM Platform must provide the STL, or build file, to the vendor along with quality, mechanical, and material requirements for the physical part. Additionally, the contractual obligations for the service provided by the vendor must be agreed upon and clearly conveyed to the vendor.

When CAM services are provided, the AM Platform must allow the CAM service vendor to upload the completed build file back to the AM Platform and once again store the file(s) in the digital warehouse. In some cases, the completed CAM files will be downloaded by the IP owner to either complete the service request, or to approve the CAM process is satisfactory. However, there are cases in which the completed CAM process files contain valuable IP from the AM CAM Partner and the AM Platform must provide

appropriate protection of those files based upon the commercial agreement with the AM CAM Partner.

When the AM Platform provides AM printing services, the STL or build file(s) must be downloaded from the AM Platform by the AM Print Partner. If an STL file is downloaded, then the AM Print Partner must provide CAM services to orient and place the part on the build plate, create appropriate support structures, and then generate the build file. If the IP owner provides the build file, then they must be careful to provide enough parts on the build plate to maximize the build area. Otherwise, the cost could be unnecessarily high, or the AM Print Partner will require the ability to generate a new build file to add parts from other orders in order to maximize the build area.

Once the AM part printing is complete, the AM Print Partner must follow the post-process steps set by the IP owner, test for quality, and ship the physical parts to its final destination. To complete the process, the AM Print Partner must provide a report back to the AM Platform, and the IP owner must accept that the parts meet their requirements. The more detailed the report provided by the AM Print Partner, the more trust the AM Platform and IP owner will have in the production of the physical parts.

Certainly, there are many other use cases actively practiced in the AM Platform industry than those described above. However, the cases presented here provide a good overview of the technology and will enable careful examination of the security vulnerabilities currently existing in the industry.

3 Security Vulnerabilities

For commercial success, the AM Platform must facilitate sharing of digital AM data between several commercial entities. There are multitudes of well-known attacks on AM design data [2]. The Inspector General recently published an audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems concluding that the five agencies audited did not consistently secure or manage their AM systems to prevent unauthorized changes and ensure the integrity of the design data [3]. Generally, these attacks fall into two classes: data modification and data theft. Data modification may be used for malicious purposes [4] or used by the service provider to simplify their work. Both the intellectual property of the original design by the IP owner as well as the IP generated by the CAM process is a valuable target for theft, providing advancements in technology of an adversary or enabling an opportunity to counterfeit parts.

Although the DoD did not consider availability of AM data, as an important AM security requirement, this is likely due to AM technology being early in its adoption. As AM matures and manufacturers (both government and private) depend on AM as core components of their business the need for availability of the AM data and processes will become more relevant.

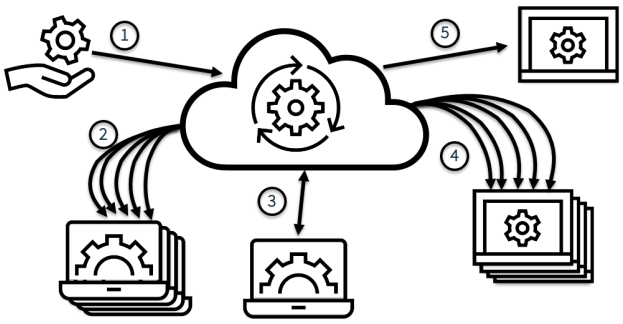

Figure 2: Data Flow When IP Owner Requires CAM and Print Service

Each occasion the AM Platform shares data between entities there is an opportunity for an attack on the data. As an example shown in Figure 2, a scenario will be examined with the most extensive data sharing. In this scenario an IP owner needs CAM service and AM printing. The IP owner will 1) upload data to the platform, and the AM Platform will then 2) share the data with CAM vendors for an RFQ. Once the CAM vendor is selected, the platform will enable the AM CAM Partner to 3) download the STL file and will then upload the modified build file back to the platform when the CAM service is complete. Next, another RFQ process will be 4) executed to find the AM Printer Partner to produce the physical parts, which requires sending the build file to multiple AM manufacturers. Once the AM Print Partner is chosen, then the build file will be 5) downloaded, and the parts will be manufactured based on the order.

This extensive data flow is shown in Figure 2. Clearly, the majority of data sharing is to support the RFQ process. Although, it may be possible for a vendor to accurately provide a commercial quote for a CAM or AM Printing service without the STL, providing the full STL is the most straightforward approach from the perspective of the AM Platform. The classic tradeoff between convenience and security is at the forefront of the RFQ process. AM Platforms that invest and innovate to secure the RFQ process, will have an advantage in the industry over the long-term.

From the perspective of the platform, the Data Import and Data Export processes are potential points of vulnerability when sharing AM data files. Even if cryptography is used to encrypt data during the exchange between commercial entities, managing the cryptographic keys is very challenging especially when establishing a trusted key between semi-trusted entities [5]. Additionally, weak authentication of either internal or external users leaves significant vulnerabilities to unauthorized access of the platform. The initial establishment of login credentials is a critical process, especially if email is used to communicate the credentials, thereby allowing for phishing attacks [6].

A commercially successful AM Platform will contain a significant amount of AM design and production data in its Digital Warehouse. This treasure trove of data is an enormous target for prospective attacks through data breaches or ransomware attacks. Any vulnerabilities in the data authorization system, either automated or manual, will eventually be exploited with such a large target. If a data breach does occur, then without a strong audit system in place, the AM Platform liability will grow as there is no evidence to prove what data remained protected.

When AM data is downloaded by an AM Design Partner, if there is no strong authorization protection for data access, the data will be available to virtually all engineers and designers in the CAM group. In addition to the same potential vulnerabilities at the AM platform, the AM Design Partner will require human interaction with the data to achieve the desired CAM processing. Additionally, the data may require processing by multiple CAM designers using different computing systems. Once again, the availability of the IP owners AM data to a wide range of users will create vulnerabilities through unauthorized modifications and data theft.

Finally, when the AM data is sent to the AM Printer Partner, the same vulnerabilities from the AM Platform and AM Design Partner will apply here as well. Additionally, the AM printing process will bring a whole class of potential vulnerabilities. These security issues have been widely studied in the literature [7]. Of particular interest, is the motivation of the AM Printer Partner to minimize their operational cost. If the AM Printer Partner can speed up the printing process or lower the material cost, then their profit will increase. Modification of the STL or build file, can lead to faster printing and different material requirements; therefore this issue should be considered a vulnerability that must be addressed by the AM Platform.

4 Proposed Solutions

Securing the AM Platform ecosystem is extremely complex with modern cybersecurity technologies and processes available to the enterprise. Protecting the confidentiality and integrity of data when shared with multiple companies while controlling how that data is used is outside the scope of most standard solutions. Therefore, there are opportunities for innovation in the AM Platform ecosystem to provide a fully secure end-to-end solution that protects data, controls usage, and enables audits.

The AM Platform security solution must begin with the AM Platform ingestion of STL and build files from the IP owner. Ideally, the data protection should begin at the IP owner's system and provide protection through the AM Platform Digital Warehouse and Data Export. In most cases, the AM Platform will not need direct access to the AM files, therefore, the platform can decrease their liability by assuring that their systems and employees never have the authorization to decrypt AM files. In order to protect both confidentiality and integrity, all data files must be encrypted and cryptographically signed. Therefore, the platform must have a system for sharing cryptographic keys with customers and vendors and must implement a method to authorize only the users who need to have access to the files to be able to decrypt the data. Additionally, each time the data is accessed, the cryptographic signatures must be verified in order to ensure that data has not been modified.

In addition to sharing AM data between customers and vendors, the AM Platform also needs to authorize CAM processing and AM Printing of the part files. From a security perspective, these are the most difficult problems to solve. For CAM processing, normally the data files are imported into the CAM applications from the file system, then once the CAM processing is complete, the updated STL or build file is again stored back to the file system. Ideally a digital rights management system would be integrated into the CAM software so that the AM Platform can control what the AM Design Partner is allowed to do with the CAM software. At a minimum, the CAM software should be able to ingest an encrypted file, decrypt the data, verify the cryptographic signature, allow CAM processes, then only allow data to be exported in encrypted format. In this way, the data will be protected from theft and the data will only be modified by the appropriate CAM process. There are few if any DRM solutions integrated into AM CAM software today.

Similarly on the AM printer, the device must be able to ingest an encrypted file, decrypt the AM build file, cryptographically verify the file, then allow printing based on the printing process defined by the AM Platform. Ideally, the AM Platform will be able to specify the settings, controls, and material used by the AM printer such that the part defined by the ingested build file will only be printed if the process requirements are set and controlled by the AM printer.

In the future, as Artificial Intelligence (AI) and Machine Learning (ML) algorithms are used to predict the quality of the printed part from data generated by sensors embedded in the printer, sensor data will need to be sent back to the AM Platform and IP owner as a measure of part quality. These data sets will need to be secured in the same way the STL and build files were protected.

To properly implement data protection through encryption and cryptographic signatures, the AM Platform must have a method in place to authorize who should have access to perform the CAM and printing operations. As part of the authorization, the people and systems must be authenticated strongly to ensure only trusted users and systems have data access rights. For authenticating the system, a proven solution such as OAuth 2.0 must be implemented to authenticate the digital systems and provide authorized data access. To authenticate users, modern secure authentication techniques must be utilized with an emphasis on Multi-Factor Authentication (MFA) for the most trusted implementation.

Once end-to-end data protection is in place, the AM Platform must provide a method to collect and secure transaction reports defining

each time the data is accessed, modified, or ingested by an AM printer, so that a complete audit report is available for each data set and part manufactured through the AM Platform.

Although securing the AM Platform is complex and will require innovation, the platforms that are successful in protecting their customer's IP will have an advantage in the marketplace.

5 Benefits of Securing AM Platform

There are 2 main benefits to properly securing AP Platform:
- From the IP owner perspective, it is critical to trust and have confidence that the data (therefore the IP) are protected. OEM's will not provide the data if they don't trust their IP is under control, and the platform success will be dependent on that trust to successfully process and share the data with AM Print Partners and/or carry a sizeable inventory of digital parts. If there are not enough OEM participants in the platform, it will not generate enough transactions and therefore will not generate enough revenue.
- From the customer perspective (i.e. the users of the physical part), they need to also trust the integrity of the digital supply chain. They need to have the confidence that the data used to 3D print the part is coming from the original IP owner and has not been, intentionally or not, modified before or during the manufacturing process.

Finally, with the increased cybersecurity attacks on the manufacturing sector and the new Department of Defense cybersecurity requirements on its Defense base, AM Platforms and its AM Printer Partners will have to demonstrate their adherence to standards such as NIST 800-171 [8] and obtain the Cybersecurity Maturity Model Certification [9] to participate in the U.S. Defense Industrial Base (DIB). Although the details of these requirements are outside the scope of this paper, fundamental cybersecurity requirements that must be addressed to comply with these standards include: use of FIPS certified components, Multi-Factor Authentication (MFA) of all users, encryption of all data, full audit retention of all transactions, separation of duties and authentication of devices.

6 Conclusion

There are a lot of factors to take into account to make the AM Platform business model a success. From the quality of the network of partners to the platform workflow and ease of use, end users of additively produced parts will need to see substantial benefits in quality, cost and lead-time performance. None of these benefits can be achieved if the platform ecosystem is not a trusted environment: OEM's will not participate for fear of losing control of their IP, and customers won't come due to the limited availability of parts. This trust starts, among other things, with a fully secured end-to-end workflow that protects the data from ingestion to consumption.

REFERENCES

[1] Wohlers, Terry T., Campbell, Ian, Diegel, Olaf, Kowen, Joseph, Mostow, Noah Wohlers Report 2021, 375-page publication, Wohlers Associates, Inc., March 2021

[2] Mark Yampolskiy, Wayne E King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, Yuval Elovici, Security of Additive Manufacturing: Attack Taxonomy and Survey, Additive Manufacturing, vol. 21, pp. 431-457, 2018.

[3] https://media.defense.gov/2021/Jul/07/2002757308/-1/-1/1/DODIG-2021-098.PDF

[4] L. Sturm, C. Williams, J. Camelio, J. White, R. Parker, Cyber-physical vunerabilities in additive manufacturing systems, Context 7 (2014) 8.

[5] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, Incorporated, 2020

[6] Kenneth D Nguyen, Heather Rosoff, Richard S John, Valuing information security from a phishing attack, Journal of Cybersecurity, Volume 3, Issue 3, November 2017, Pages 159–171, https://doi.org/10.1093/cybsec/tyx006

[7] Elhabashy, A., Wells, L., & Camelio, J. (2019). Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review. Procedia Manufacturing, 34, 921-931.

[8] National Institute of Standards and Technology Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Department of Commerce, Washington, D.C.), SP 800-171 Rev. 2, Change Notice February, 2020. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

[9] https://www.acq.osd.mil/cmmc/index.html