Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing

Mark Yampolskiy, Todd R. Andel, J. Todd McDonald, William B. Glisson, Alec Yasinsac
University of South Alabama
Mobile, AL
{yampolskiy, tandel, jtmcdonald, bglisson, yasinsac}@southalabama.edu

ABSTRACT

Additive Layer Manufacturing (ALM) is a new technology to produce 3D objects adding layer by layer. Agencies and companies like NASA, ESA, and SpaceX are exploring a broad range of application areas of ALM, which includes printing of device components, replacement parts, houses, and even food. They expect that this technology will greatly reduce production costs, manufacturing time, and necessary storage space. The broad variety of application areas and the high grade of computerization of this manufacturing process will inevitably make ALM an attractive target of various attacks.

This research examines the problem of Intellectual Property (IP) protection in the case of outsourcing the ALM manufacturing process. We discuss the existing process and introduce a new model for the outsourcing of ALM-based production. For the proposed outsourcing model, focusing on IP protection, we present a risk assessment, specify requirements addressing mitigation of the identified risks, and outline approaches to implement the specified requirements. The fulfillment of the specified requirements will enable secure outsourcing of ALM production.

Keywords

Additive Manufacturing, Additive Layer Manufacturing, 3D Printing, Outsourcing, Intellectual Property Protection

1. INTRODUCTION

Cyber Physical Systems (CPS) are under constant and increasing attack as core components of critical infrastructure [19, 49, 13, 30, 14, 60, 21, 27, 53, 9, 41, 25, 51, 36, 40, 16, 47, 7]. Additive Layer Manufacturing (ALM), also known as Additive Manufacturing, solid freeform fabrication, and maybe most commonly as 3D printing, is a fairly new class of CPS for producing 3D objects. As opposed to the conventional manufacturing process, in which a mold is poured or a solid block of a material is reduced with milling and turning to a desired form, in ALM, 3D objects are created by adding thin layers, one layer at a time to build up the object from two dimensions to three in the desired form.

Agencies and companies like NASA, ESA, GE, and SpaceX are exploring a broad range of application areas of ALM. SpaceX has used additive manufacturing to produce engine chambers for the newest Dragon spacecraft [22]; GE builds complex brackets that weigh 80% less than conventional structural parts [23]; NASA has already tested a rocket injector that is exposed to high loads and temperature gradients [26]; a Dutch company, DUS Architects, plans to print a complete three story house [3]; BAE Systems in its futuristic vision plans to print on demand an entire UAV designed for specific operational requirements [56].

ALM technology will greatly reduce production costs, manufacturing time, and required storage space. The broad variety of application areas and benefits are likely to make ALM one of the widely used manufacturing technologies in the near future. However, whereas 3D Printers for low quality prototyping with plastics became affordable (starting at few thousand dollar [2]), ALM equipment capable of producing high quality and precision components out of metals, alloys, and composites remains extremely expensive (over $20,000 for high quality plastics [15] and often well over $100,000 for high quality metal alloys [5, 6]). Furthermore, depending on the supposed application, manufactured objects should satisfy a broad range of physical requirements, e.g., resistance to mechanical or thermal stress. For this, tuning of various manufacturing parameters (e.g., orientation during manufacturing, pattern of heat source, etc. [48, 59, 64]) is necessary, which requires expert knowledge of the ALM equipment and deep understanding of how various parameters influence physical properties of the manufactured object. Because of both high costs of AML equipment and dependence on knowhow for tuning of manufacturing parameters, outsourcing the production to third parties specializing in the ALM process and possessing essential knowledge becomes a necessity.

The broad variety of application areas and the dependency on computerization of this manufacturing process inevitably makes ALM an attractive attack target. The outsourcing creates an additional attack surface that can be exploited. In conjunction with outsourcing and of special concern are attacks violating Intellectual Property (IP) of either of the parties involved in the process. This includes the proprietary 3D shape and required physical parameters owned by the 3D object designer, but also the tuning of the manufacturing parameters usually owned by the ALM manufacturer. Further kinds of attack include those aiming to manipulate proper-

PPREW-4, December 09 2014, New Orleans, LA, USA

http://dx.doi.org/10.1145/2689702.2689709

ties of manufactured objects, damage ALM equipment, or even endanger the safety of the manufacturing process [59, 64, 63, 52, 46]. After attacks have occurred, the ability to investigate these attacks is paramount.

It is our belief that IP protection will be of significance to the realm of 3D printing and ALM techniques. However, whereas several articles have raised concerns regarding IP protection in context of 3D Printing [57, 8, 11, 44, 11, 10, 37], we are not aware of any prior scientific research introducing technical solutions for this issue. We see a major necessity to develop technical means for the enforcement of IP protection in ALM. The present paper is only the first step towards understanding the problem and identifying areas for technical research.

In this paper, we focus on the issue of Intellectual Property protection. We first discuss the outsourcing model current used in ALM manufacturing. Then, in Section 3, we propose an alternative outsourcing model, which can provide greater flexibility for a customer of the ALM manufacturer. In Section 4 we present risk assessment of the proposed model and formulate requirements, the fulfillment of which would enable secure outsourcing. In Section 5 we outline several approaches which can be used to fulfill specified requirements. Section 6 discusses the investigation of these attacks. Section 7 presents the conclusions along with a short overview of our future research plans.

2. STATE OF THE ART

As of now, 3D models are first designed in Computer-Aided Design (CAD) software. Then the CAD model is "sliced" into thin layers described either in Surface Tessellation Language (STL) or in the recently defined Additive Manufacturing File Format (AMF) [32]. Neither STL nor AMF have any security features integrated. Both STL and AMF describe the 3D shape of the object, which is the input for the ALM equipment. If the 3D object is a part of a complex device, e.g., a jet engine blade, this object should satisfy various requirements. For instance, it should be able to withstand specified mechanical or thermal stress. Such requirements are specified additionally to the STL or AMF description of 3D shape.

The 3D shape of the object and, if specified, the requirements of its properties are the IP of the 3D Object Designer. Both are essential for being able to manufacture objects according to the requirements. Therefore, this information is passed to the ALM manufacturer (see Figure 1).

There are three different approaches to fusing metals and alloys using ALM techniques: powder bed fusion, direct metal deposition, and metal sheet lamination [20, 58, 26, 48, 24, 33]. Each of these methods are strongly dependent on automation and computer control. Depending on the ALM technology used, various manufacturing parameters influence the microstructure of the manufactured object [64, 48] and, as a consequence, also its physical properties. For instance, if powder bed technology is used, among influential parameters are size and form factor of powder grain, orientation of manufactured object, pattern of heat source, etc. [18, 54, 31]. Therefore, if customer requirements exceed properties natively supported by a particularly used (usually cost-optimized) manufacturing process, tuning of the manufacturing parameters might be needed. Currently, such tuning is performed by a company specializing in the ALM production. The specific combination of manufacturing process parameters is considered as IP of this company. Commonly, none of this information is shared with the customers ordered manufacturing of a 3D objects.

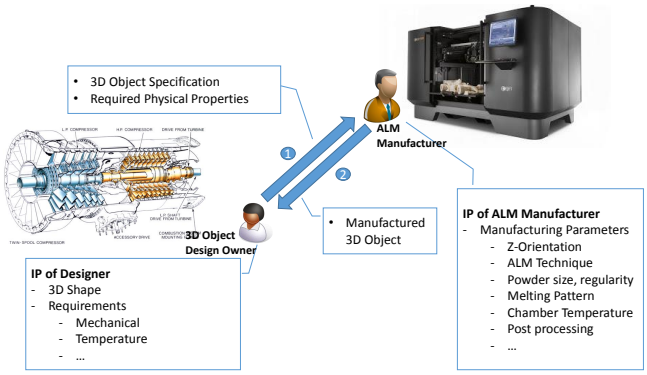

Figure 1: Current Outsourcing Model

In concluison, the currently existing outsourcing model considers two roles: *3D Object Designer* and *ALM Manufacturer* (see Figure 1). Both actors are IP owners. However, whereas the 3D Object Designer (either an enterprise or an individual) shares its IP, i.e., 3D shape and required physical properties, with the ALM Manufacturer, the latter (usually an enterprise) does not share its IP for the manufacturing parameters at all. In this outsourcing model, the exposed IP of the 3D Object Designer is protected by contractual agreements and the necessity for the ALM manufacturer of maintaining its reputation. However, as multiple recent examples show, contractual relationships and reputation are not necessarily sufficient to prevent the IP violation [4, 45, 50].

The IP of the ALM Manufacturer is protected by keeping it secret from the customer (i.e., 3D Object Designer). This, however, creates several negative consequences to the customer. First of all, it binds the customer to the particular ALM Manufacturer capable of tuning the manufacturing parameters according to the requirements. As it has been noticed in other industries, such binding generally has a negative impact on competition and thus results in higher manufacturing prices for the customer. Furthermore, in the case of bottlenecks at the ALM Manufacturer side or a burst of demand at the 3D Object Designer side, outsourcing with the already proven manufacturing parameters to an alternative ALM Manufacturer becomes close to impossible. All these drawbacks make the development of an alternative, more flexible outsourcing model necessary.

3. OUTSOURCING MODEL

We propose an alternative outsourcing model that mitigates outlined drawbacks of the existing model. This is a basic outsourcing model because it does not consider hierarchical outsourcing (or customer-provider relationships). However, it contains the building blocks necessary to compose hierarchical outsourcing models.

In the proposed model, we distinguish between three roles (see Figure 2): (i) *3D Object Designer*, an enterprise or an individual, (ii) *Manufacturing Process Tuning Experts*, an enterprise or an individual, and (iii) *ALM Manufacturer*, an enterprise. Compared to the outsourcing model currently existing in ALM, the proposed model "splits" the capabili-

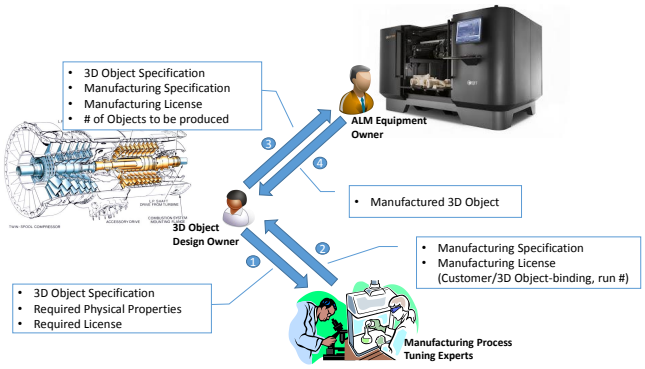

Figure 2: Basic Secure Outsourcing Model

ties currently associated with the ALM Manufacturer into two independent roles, which can, but should not be, exercised by distinct enterprises or individuals. Since numerous discovery mechanisms exist that can be used to find actors capable of providing particular services like manufacturing, the discovery of actors has been avoided in this discussion.

In the proposed model, we distinguish between the following four communication interactions between involved actors:

- In the first communication step, the 3D Object Designer contacts the Tuning Expert and requests specifications of manufacturing parameters. This request might contain the 3D object specification, i.e., its shape, and, if necessary, the specification of required physical properties, as well as the desired license for the usage of the manufacturing parameters. Such license should incorporate the amount of "production runs" for which the particular manufacturing process may be legally used. This reflects common practice by licensed production [1]. Furthermore, we assume that it might be desirable to "bind" the license to the particular 3D object and/or to the customer (i.e., 3D Object Designer). We assume that further preferences (i.e., optimization parameters) can be specified as well, e.g., particular ALM technology, manufacturing time, production costs, etc.

- In the second communication step, the Tuning Experts provide the specification of the manufacturing parameters as well as the license to the 3D Object Designer. If necessary, modifications of the 3D object, e.g., its rotation in order to adjust object orientation during the manufacturing process, should be provided as a part of the tuning specification.

- After the 3D Object Designer has the manufacturing specifications, the third step involves the designer contacting the ALM Manufacturer with the request to produce the object. In this step, specification of the 3D object, manufacturing parameters, the license, and the amount of objects to be produced are passed to the ALM manufacturer. It is reasonable to expect that often the amount of production runs requested will be less than the amount of licensed runs. For instance, it is common that parts and complex machines are manufactured on demand, in order to reduce costs.

- In the last step, the manufactured 3D object(s) are delivered to the 3D Object Designer.

The proposed outsourcing model has several, mainly economical, advantages compared to the currently established one. From the 3D Object Designer perspective, first of all, it negates the ALM Manufacturer-binding and thus introduces more flexibility at the customer side. In addition to the expected benefits like reduced manufacturing costs, it also provides a way of verifying the quality of the manufacturing parameters specification, e.g., by ordering small quantity production at different ALM Manufacturers and performing various tests. The license cost usually depends on the amount of users (in this case, "production runs") it is specified. This also introduces the possibility of ordering small-run licenses from various tuning experts, thus selecting the manufacturing parameters most suitable for the particular customer. Furthermore, ordering additional runs (or new licenses with additional runs) for a particular already-specified manufacturing parameter tuning becomes possible.

The proposed outsourcing model also has potential advantages for the ALM Manufacturer. This is because the proposed model has building blocks enabling establishing hierarchical outsourcing relationships. Whereas the contractual and communication relationships between the 3D Object Designer and the ALM Manufacturer can remain as they are right now (see Figure 1 in Section 2), the ALM Manufacturer does not necessarily have to maintain its own team of tuning experts. Instead, the outsourcing of this task to third party tuning experts becomes possible. In this case, the communication flows 1 and 2 (see Figure 2) will be between ALM Manufacturer and Manufacturing Process Tuning Experts. The above-described advantages and considerations associated with the licenses and production runs limitations also apply here.

Last but not least, the proposed model also has economic advantages for Manufacturing Process Tuning Experts. Instead of being employed and having contractual relationships with a single ALM Manufacturer, the proposed model enables creation of dynamic, multiple relationships with numerous customers, including both 3D Object Designers and ALM Manufacturers. This, in turn, will increase the economic resilience and sustainability of individuals and companies assuming this role.

4. IP PROTECTION REQUIREMENTS

Whereas the proposed outsourcing model introduced a number of (predominantly economical) advantages, it makes the task of Intellectual Property (IP) protection more difficult. The reason is the increased number of actors as well as communication flows for the information exchange. This increases the probability for malicious actors to be involved or the communication flow being eavesdropped by an adversary. Furthermore, as multiple actors share the same information, identification of IP violators becomes nontrivial. This erodes the power of contractual as well as reputation-based enforcement of IP protection. Therefore, there is a major necessity to develop technical means for the enforcement of IP protection in ALM.

In this section, we first present a qualitative risk assessment of the proposed outsourcing model. We consider risks related to the IP violation only. Then we specify requirements for the technical measures, fulfilment of which will

allow mitigation of the risks and thus transforming the proposed outsourcing model to a secure one.

4.1 Risk Assessment

Similar to [60], we perform risk assessment based on the model describing all actors and information flows (see Figure 2). However, instead of considering all risks associated with the outsourcing of ALM production (i.e., considering each possible threat to confidentiality, integrity, or availability through interception, fabrication, modification, or interruption of each part of the process), we focus on aspects relevant to IP violation only.

In the proposed model, actors playing any of the three specified roles can be malicious. Additionally, we consider an External Adversary who is not immediately involved in the outsourcing process. We assume that any adversary actor intends to violate IP, i.e., either make an illegal copy of IP or remove/modify restrictions associated with it. The possibilities for the malicious actors to violate IP of other actors are as follows:

Manufacturing Process Tuning Experts: Outsourcing participants acting as Tuning Experts receive the whole IP of the 3D Object Designer, including both the 3D shape as well as the required physical properties. This gives the tuning experts the opportunity to make illegal copies of this IP or parts of it, e.g., in order to sell it. Customers for such information can be any competitor of the 3D Object Designer.

3D Object Designer: A license for the ALM manufacturing tuning specifies several restrictions, e.g., the amount of objects which can be legally produced using this specification, or even who might use this license and for the production of which objects. A malicious 3D Object Designer might be interested in removing and/or to modifing these restrictions. Doing this, the malicious 3D Object Designer could illegally reduce the costs of production or even create revenues by reselling the manufacturing specification.

ALM Manufacturer: The ALM Manufacturer receives access to the IP of both 3D Object Designer and Tuning Experts. As such it has the opportunity to make illegal copies of the 3D object and the manufacturing parameters specifications. A malicious ALM Manufacturer could offer, to other customers, the service of the ALM production with particular physical properties, thus illegally using the tuning modifications specified in the IP of the Tuning Experts. Similarly, the malicious ALM Manufacturer might be interested in violation of restrictions on the amount of production runs in particular licenses (both tuning modifications and 3D object). This can be done, e.g., in order to manufacture and sell illegal copies of the 3D object.

External Adversary: Additionally, we have to consider an external adversary who might be interested in getting access to the IP of 3D Object Designer and/or of Tuning Experts. The most obvious way is eavesdropping or a man-in-the-middle attack on the communication channel between actors exercising specified roles. Furthermore, the External Adversary can modify the equipment (software and hardware) used by any other actor. In this case, however, its capability to violate the IP cannot exceed those of the corresponding actors. Therefore, this fact is of lesser importance for the vulnerability analysis, but should be reflected in the requirements. Last but not least, the External Adversary can get physical access to the manufactured 3D object in order to reverse engineer the IP used in its production.

	Malicious Intents (IP-related only)
3D Object Designer	▪ Remove and/or Modify restrictions on usage of manufacturing parameters specification
Tuning Experts	▪ Copy [parts of] specification of 3D object shape and required physical properties
ALM Manufacturer	▪ Copy [parts of] specification of 3D object shape and required physical properties ▪ Copy and reuse manufacturing parameters specification; remove or modify restrictions associated with the specification
External Adversary	▪ Copy [parts of] specification of 3D object shape and required physical properties ▪ Copy manufacturing properties specification

Table 1: IP Violation Goals of Malicious Actors

Table 1 summarizes the IP violation goals malicious actors can pursue in the proposed outsourcing model.

4.2 Requirements for Secure Outsourcing

Whereas the adversary actors have (predominantly economic) incentives to violate IP, the IP owners have incentives to protect their IP. Making the IP violation less lucrative to an adversary is a very challenging task, which is commonly considered as a cost-benefit analysis. Costs of an adversary can be associated either with the technical means needed to (and difficulty of) violate IP or with the capability to identify the violator, thus enabling legal persecution or impacting the reputation of the malicious actor.

In cyber-security, it is common to develop measures for prevention and detection of malicious behavior violating security goals. We apply this approach to all potentially malicious actors present in the model. However, there is a slight difference between the way these objectives are used in cyber-security and how we define them. In particular, under prevention we consider measures aiming to prevent IP violation, increase the difficulty of performing it, or decrease the valuable outcome thereof. Under detection we understand, in the first place, the identification of IP used for the manufacturing of an object and its attribution to the actors having access to it.

A summary of the IP protection goals is given in Table 2. We define the IP protection goals as follows (the bold text on the left specifies the top-level objectives and sub-objectives as outlined in the table):

	Prevention	Detection
3D Object Designer	▪ Copying ▪ Modification of Restrictions	▪ Identification of used IP ▪ Liability
Tuning Experts	▪ Copying	▪ Identification of used IP ▪ Liability
ALM Manufacturer	▪ Copying ▪ Modification of Restrictions ▪ Side-Channel Analysis ▪ Reverse Engineering	▪ Identification of used IP ▪ Liability
External Adversary	▪ Interception of Communication ▪ Reverse Engineering	▪ Distinction between internal/ external adversaries

Table 2: IP Protection Goals

Prevention / Copying: It should be impossible or very difficult to extract information about the 3D Object Designer's IP. This includes the possibility of extracting information related to the 3D shape and to the physical properties of the manufactured object. An unrestricted access to the IP should be either eliminated or limited to the extent absolutely necessary for the accomplishment of needed tasks, including (i) formulation of the specification of the required manufacturing parameters adjustments and (ii) process of the object manufacturing.

Prevention / Manipulation of Restrictions: It should be impossible or very hard to remove or modify the restrictions associated with the licenses provided by the IP owners, including (i) 3D Object Designer and (ii) Tuning Experts. The prevention measures should work even in the case of the 3D Object Designer ordering small production runs from several independent ALM manufacturers, which could be located in different countries. An important aspect is that the protective measures should be capable of accommodating cases of failures during the manufacturing process, e.g., due to ALM equipment failure, issues with the source material, etc.

Prevention / Side-Channel Analysis: During the manufacturing process, the ALM Manufacturer can observe and measure various aspects of the process, e.g., slices of the 3D shape, patterns of the heat source movement etc. Even if files containing IP of other actors are protected, e.g., encrypted, such side-channel analysis can potentially provide deep insights in the IP. Of especial concern are various side-channel attacks on embedded systems within ALM equipment, which can be used to break the protection mechanisms [43, 42, 28, 29, 12]. Therefore, measures are needed to prevent or significantly limit the possibility and value of such analysis.

Prevention / Reverse Engineering: The manufactured 3D objects can be physically analyzed by examining their 3D shape and microstructure. Such an analysis can give insights in the IP of 3D Object Designer and Tuning Experts. The ALM manufacturer is in the best position to perform such an attack. However, this is the least probable one because the ALM Manufacturer has the opportunity to perform a broad variety of attacks which are more promising and less complex than this one. For an External Adversary (including a malicious end-customer of the 3D object or a machine the manufactured object is a part of) it might be the only possible attack. Therefore, measures should be taken in order to reduce the amount of useful information that can be extracted with Reverse Engineering.

Prevention / Interception of Communication: All communication channels are commonly considered as objects for eavesdropping, Information exchange in the steps 1, 2, and 3 in the Figure 2 contain electronic representations of the intellectual property of involved actors. Therefore, communication protocols should ensure the secrecy of these IP. Furthermore, manipulations of the information in these steps should be prevented as well, in order to avoid undesired changes of the manufactured object or attacks on ALM equipment (for an elaborate discussion about these topics see [64]). Communication protocols can be protected through the implementation of the state of the art applied cryptography techniques. We specify this requirement mainly for the sake of completeness.

Detection / Identification of used IP: If a third party reuses unlawfully copied IP of the 3D Object Designer or Tuning Experts, it should be possible to detect the IP violation. In order to do this, it should be possible to identify the IP used for manufacturing of an object and its attribution to the IP owner. Furthermore, it is desirable that the detection and validation of the IP violation is possible. This is applicable and, potentially, more prevalent in cases where only part of the IP (e.g., parts of 3D shape, specific pattern of heat source, etc.) has been unlawfully reused.

Detection / Liability: Tightly related to the identification of the used IP is the requirement to identify the third party which had an access to this IP, e.g., which 3D Object Designer and ALM Manufacturer had access to the particular IP of the Tuning Experts. In other words, in case the IP was violated, it should be possible to identify the actor(s) which has/have violated it. This requirement also addresses the situation when the 3D Object Designer orders specifications for tuning of the manufacturing parameters by more than one actor acting as the ALM manufacturing Tuning Expert. The non-repudiable identification is essential for the criminal investigation and legal prosecution.

Detection / Distinction between Adversaries: It should be possible to distinguish between IP violation performed by an actor involved in the outsourcing process and one performed by an external adversary who

has compromised equipment of the legitimate actor. This is especially important to avoid false accusations and legal persecutions of genuine actors involved in the ALM outsourcing process. Note that we don't require identification of the External Adversary who committed the IP violation.

Analysis / Forensics: In the case that IP was violated, it should be possible to reconstruct the process leading to this. This requirement especially focuses on understanding of technical means used for the IP violation. The fulfillment of this requirement will provide additional insights necessary for the prevention of the particular IP violation path in the future. Additionally, a possibility of identifying the actor, department, or even persons involved in the IP violation is a beneficial outcome of the forensics analysis. This information potentially influences the outcome of legal cases. It also provides insight into possible organizational improvements that would prevent or mitigate the impact of future violations.

5. TOWARDS SECURE OUTSOURCING

We see several ways to approach solutions for some of the specified requirements. In our future work, we plan to evaluate the following approaches:

- In order to protect a 3D Object Designer's IP from malicious Tuning Experts, the following research questions should be answered: What level of details of the 3D Object Designer's IP is necessary in order to develop the manufacturing parameter adjustments sufficient to satisfy all requirements on this object? What aspects influence this level of detail and to what extent? Are these aspects different for different ALM technologies? If it is possible to define a one-way transformation of the 3D Object Designer's IP to a state where it is useless for the ALM manufacturing but still sufficient for the tuning of the manufacturing parameters, this IP will be effectively protected. This can even increase the IP protection in the existing outsourcing model.

- In order to protect the IP of the 3D Object Designer and of the Tuning Experts from a malicious ALM Manufacturer, the following model can be considered. The automated parameters of both IPs can be encrypted. However, all parameters, which should be known to the ALM Manufacturer before the process starts (e.g., material, form factor, and size of the metal alloy powder), should be made accessible to the ALM Manufacturer. If ALM equipment has both Internet access and a Trusted Platform Module (TPM) integrated, the following scenario is possible: ALM equipment can automatically request a decryption key for the production run from a trusted third party, which has no access to IP but manages decryption keys for various IP owners. The TPM module decrypts the encrypted STL/AMF file as well as encrypted manufacturing specification and uses this information to produce the required 3D object. This approach is similar to the state of the art applied cryptography solutions. However, several challenges should be solved. First of all, we assume an untrusted end party (i.e., ALM Manufacturer), who has an unrestricted access to the ALM equipment. This requires thorough design of the placement and role of the TPM module, which security otherwise could be bridged. At the same time, it should not interfere with time-critical processes during the manufacturing. Otherwise, the production impact of the security implementation will render it infeasible to produce 3D objects with required properties. Furthermore, a legitimate concern of the ALM Manufacturer is the possibility that the provided (in encrypted form) manufacturing parameters specification could damage ALM equipment. Last but not least, Internet access to the ALM equipment creates additional vectors that ALM Manufacturers would like to avoid.

- In order to detect and trace back the IP violation, various possibilities of "watermarking" should be investigated. In particular, the following research questions should be addressed. Is it possible to introduce watermarking changes in the specification of the 3D object so that: (i) these "watermarks" do not affect the required properties of the 3D object, (ii) are hard to impossible to remove from the object specification, and (iii) can be used to uniquely identify all actors assuming different roles in the proposed outsourcing process. In particular, we plan to investigate two distinct watermarking types: (i) watermarking of the 3D object and (ii) of the manufacturing process.

- In order to develop an understanding of motives and technical means of ALM-related IP violation, a catalogue of known attacks should be developed. This requires the capability to describe attacks in the way that (a) both multi-stage attacks and the resulting effect propagations across multiple domains can be described and (b) the description provides structure for comparison and identification of quantitative attack properties. For this purpose we plan to use and, if necessary, extend Cyber-Physical Attack Description Language [62, 61], a language capable of describing attacks on CPS exceeding cyber domain.

- Evidently, so far the security research has not been able to produce a cost-effective solution capable of preventing attacks. This means that forensics in general or residual data analysis in particular should play an important role in the suite of measures ensuring IP protection. When IP violation occurs, investigations need to take place to scrutinize potential impacts on intellectual property. Hence, this research should ensure reconstruction of successful attacks through the examination of residual data and digital forensic analysis, as discussed in greater detail in section six.

6. RESIDUAL DATA ANALYSIS

One approach to preventing attacks is to understand and successfully demonstrate how security can be breached from a malicious software perspective. This includes the investigation of native operating systems along with the development of stand-alone code to see how they can be modified and/or utilized through the initialization of common libraries to induce, sustain or propagate malicious software. Once these opportunities have been identified, successful strategies will be developed to mitigate identified security

deficiencies. Another approach is to implement hardware and software obfuscation techniques that would mitigate reverse engineering efforts and alert investigators to non-standard hardware and software calls.

An initial target will be to develop code that will modify inputs slightly and variably to weaken the integrity of the products without being visually detectable. As this technology becomes more prevalent, company surveys will be developed and implemented to acquire improved market comprehension of the security threats introduced by this technology, the countermeasures that industry is currently implementing, and the types of attacks that they have experienced. Experienced attacks will be reconstructed to confirm existing security breaches and identify new ones.

Counter solution research aimed at detecting modifications will include the development and implementation of water marks that are imprinted on the product at various stages of the production process to provide a visual indicator that something in the input has been modified, either intentionally or accidently. The visual verification can be automated once the development and implementation of the water marks have been refined. The automation of water mark verification provides faster verification with increased accuracy and consistency.

Printers and associated hardware will be forensically examined using existing tools to identify their applicability and appropriateness for use in ALM. Experiments will be developed to compare the effectiveness and appropriateness of traditional forensic tools like FTK and Encase in ALM environments. The results of these types of experiments will contribute to the development of forensic methodologies and solutions that are tailored to ALM implementations. These experiments will explore opportunities for the implementation of tailored black-box solutions along with traditional IP tracking, network tools and general logging information.

Ultimately, this research will investigate the development of intelligent forensic tools to identify potentially harmful changes in production ALM environments and forensic analysis environments. If an ALM forensic analysis environment is compromised it has potential ripple effects due to data integrity requirements in intellectual property investigations. Current investigations could be negatively impacted due to compromised data and/or investigation procedures. Past investigations could be re-opened if future techniques prove that the data recovered during the course of the investigation has been tainted due to malicious software installed on the ALM device. A potential solution could be a virtualized implementation and comparison of the existing code against a pristine copy of the code. The development of intelligent digital forensic tools is arguably a functionality evolution of traditional forensic solutions currently accepted in the market.

7. CONCLUSION

Additive Layer Manufacturing (ALM) is a fairly new class of CPS for producing 3D objects. The broad variety of application areas and a high degree of computerization of this manufacturing process will inevitably make ALM an attractive target of various attacks.

It is our belief that Intellectual Property (IP) protection will be of significance to the realm of 3D printing and ALM techniques. Due to the growing importance of ALM, which is expected to become interwoven in numerous production chains, we would compare the incentives of IP violation in ALM to those in processors. Many instances in current processors already fall prey to IP theft. These include instances such as counterfeit chips through repackaging techniques [55], reverse engineering of hardware circuits as seen in the attacks against the European MiFare card [38], and the current work in digital device fingerprinting to combat chip designs from working on non-authorized implementations [35, 34, 39, 17]. We see a major necessity to develop technical means for the enforcement of IP protection in ALM. The present paper is only the first step towards understanding the problem and identifying areas for technical research.

In this paper, we have first outlined an existing outsourcing model and discussed a variety of drawbacks. We then proposed a novel outsourcing model for ALM. In this model, a designer of a 3D object can outsource both tuning of the manufacturing parameters as well as the manufacturing itself to different parties. The proposed model supports restrictions on the IP usage of various participants, e.g., the number of objects which may be manufactured.

The proposed outsourcing model has numerous potential benefits which include, but are not limited to, the creation of new jobs and business models, support of more dynamic collaborations between participants with different expertise, and lower prices for the customers ordering ALM production of various 3D objects.

However, the proposed outsourcing model introduces several additional attack surfaces. The introduction of these attack surfaces creates environments where investigations need to be conducted to scrutinize impacts on intellectual property. Hence, this research examines strategies aimed at preventing, detecting and investigating residual data in ALM environments.

The effort to improve security also formulated technical requirements, based on the risk assessment, which should be developed and integrated in the ALM production chain in order to enforce the IP Protection in the proposed model. Last but not least, we have outlined several approaches to address some of these requirements. The next major effort will be to expand on and implement both the security and digital forensics ideas presented in this paper.

8. REFERENCES

[1] Licensed production. http://www.caat.org.uk/resources/publications/economics/licensed-production-0801.pdf.

[2] Comparison chart of all 3d printer choices for approximately $20,000 or less. http://www.additive3d.com/3dpr_cht.htm, 2014.

[3] DUS Architects. http://www.dusarchitects.com/, 2014.

[4] Intellectual property theft: Get real facts and figures. http://www.ncpc.org/topics/intellectual-property-theft/facts-and-figures-1, 2014.

[5] The rapid prototyping industry, major us-based vendors. http://www.additive3d.com/ind_211.htm, 2014.

[6] The rapid prototyping industry, vendors outside the us. http://www.additive3d.com/ind_22.htm, 2014.

[7] D. Albright, P. Brannan, C. Walrond, I. for Science, and I. Security. Did Stuxnet Take Out 1,000

Centrifuges at the Natanz Enrichment Plant? Technical report, 2010.

[8] M. Barnett. The next big fight: 3d printing and intellectual property. January 2014.

[9] BBC. Energy firms hacked by 'cyber-espionage group Dragonfly'. *BBC*, July 2014.

[10] B. Berman. 3-d printing: The new industrial revolution. *Business horizons*, 55(2):155–162, 2012.

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

[12] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems-CHES 2004*, pages 16–29. Springer, 2004.

[13] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, volume 116, 2004.

[14] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of USENIX Security*, 2011.

[15] I. C. Computer Aided Technology. Stratasys objet24 - desktop 3d printer. 2014.

[16] L. Constantin. Hackers targeting industrial control systems. *Computerworld*, August 2013.

[17] J. W. Crouch, H. J. Patel, Y. C. Kim, J. T. McDonald, and T. C. Kim. Creating digital fingerprints on commercial field programmable gate arrays. In *ICECE Technology, 2008. FPT 2008. International Conference on*, pages 345–348. IEEE, 2008.

[18] S. Dadbakhsh and L. Hao. Effect of Layer Thickness in Selective Laser Melting on Microstructure of Al/5 wt.% Fe 2 O 3 Powder Consolidated Parts. *The Scientific World Journal*, 2014, 2014.

[19] N. Falliere, L. Murchu, and E. Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 2011.

[20] P. Fastermann. *3D-Drucken*. Springer-Verlag, 2014.

[21] L. Forbes, H. Vu, B. Udrea, H. Hagar, X. D. Koutsoukos, and M. Yampolskiy. SecureCPS: Defending a Nanosatellite Cyber-Physical System. In *SPIE Defense+ Security*, pages 90850I–90850I. International Society for Optics and Photonics, 2014.

[22] J. Foust. (spacex unveils its "21st century spaceship, 2014.

[23] GE. Hardware Meets Software in Advanced Manufacturing. http://www.ge.com/stories/hardware-meets-software-advanced-manufacturing, 2014.

[24] I. Gibson, D. W. Rosen, and B. Stucker. *Additive manufacturing technologies*. Springer, 2010.

[25] D. Goodin. Attackers poison legitimate apps to infect sensitive industrial control systems. *Ars Technica*, June 2014.

[26] G. Janaki Ram, Y. Yang, and B. Stucker. Effect of process parameters on bond formation during ultrasonic consolidation of aluminum alloy 3003. *Journal of Manufacturing Systems*, 25(3):221–238, 2006.

[27] A. Judge. Hacker proves passenger airplanes are open to cyber-attack. *ITProPortal*, August 2014.

[28] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in Cryptology-CRYPTO'99*, pages 388–397. Springer, 1999.

[29] P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in Cryptology-CRYPTO'96*, pages 104–113. Springer, 1996.

[30] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Proc. IEEE Symp. Security and Privacy (SP)*, pages 447–462, 2010.

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

[32] C. C. M. Lab. Standard Specification for Additive Manufacturing File Format (AMF). http://creativemachines.cornell.edu/.

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

[34] J. T. McDonald, Y. Kim, and D. Koranek. Deterministic circuit variation for anti-tamper applications. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, page 68. ACM, 2011.

[35] J. T. McDonald and Y. C. Kim. Examining tradeoffs for hardware-based intellectual property protection. In *Proceedings of the 7th International Conference on Information Warfare and Security*, page 192. Academic Conferences Limited, 2012.

[36] J. R. Michael Riley. UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat. *Bloomberg Buisnessweek*, June 2014.

[37] M. Mimler. 3d printing, the internet and patent law–a history repeating? *La Rivista di Diritto Industriale (2013) Vol*, 62:352–370, 2013.

[38] K. Nohl, D. Evans, S. Starbug, and H. Plötz. Reverse-engineering a cryptographic rfid tag. In *USENIX Security Symposium*, volume 28, 2008.

[39] H. Patel, Y. Kim, J. T. McDonald, and L. Starman. Increasing stability and distinguishability of the digital fingerprint in fpgas through input word analysis. In *Field Programmable Logic and Applications, 2009. FPL 2009. International Conference on*, pages 391–396. IEEE, 2009.

[40] T. Peter. US utility's control systems hit by advanced cyber attack - DHS. *RT*, May.

[41] S. Peters. As Stuxnet Anniversary Approaches, New SCADA Attack Is Discovered. *DARKReading*, June 2014.

[42] W. Rankl. Overview about attacks on smart cards. *Information Security Technical Report*, 8(1):67–84, 2003.

[43] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady. Security in embedded systems: Design

challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3):461–491, 2004.

[44] M. Rüberg. Germany: 3d printers and intellectual property rights. August 2014.

[45] J. Reed. Cyber attacks and intellectual property theft. 2011.

[46] O. R. N. Release. After explosion, US Department of Labor's OSHA cites 3-D printing firm for exposing workers to combustible metal powder, electrical hazards Powderpart Inc. faces $64,400 in penalties. *OSHA Regional News Release*, May 2014.

[47] M. Rockwell. ICS-CERT sounds alarm on critical infrastructure attacks. *FCW*, July 2014.

[48] L. Schutzle. Research on the impact of Additive Layer Manufacturing for future space missions. Internship report CDF-STA-009, ESA, 2014.

[49] J. Slay and M. Miller. Lessons learned from the maroochy water breach. *Critical Infrastructure Protection*, pages 73–82, 2007.

[50] C. D. Smith. Counterfeiting and piracy: How pervasive is it? 2008.

[51] A. Sternstein. Flaw Lets Hackers Control Electronic Highway Billboards. *Nextgov*, June 2014.

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

[53] A. Thomson and C. Rahn. Russian Hackers Threaten Power Companies, Researchers Say. *Bloomberg*, July 2014.

[54] TWI. Selective Laser Melting. http://www.twi-global.com/technologies/welding-surface-engineering-and-material-processing/additive-manufacturing/selective-laser-melting/, 2014.

[55] J. Villasenor and M. Tehranipoor. Chop-shop electronics. *IEEE SPECTRUM*, 50(10):41–45, 2013.

[56] K. Watcham. On-board 3D printing. 2014.

[57] M. Weinberg. It will be awesome if they don't screw it up: 3d printing, intellectual property, and the fight over the next great disruptive technology (white paper). *Public Knowledge*, November 2010.

[58] T. Wohlers. *Wohlers report 2012*. Wohlers Associates, Inc, 2012.

[59] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac. Towards Security of Additive Layer Manufacturing. 2014. In Proceedings of the 30st Annual Computer Security Applications Conference (ACSAC) 2014.

[60] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pages 55–62. IEEE, 2012.

[61] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 135–142. ACM, 2013.

[62] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 2014.

[63] M. Yampolskiy, J. Ivanidze, A. Skjellum, R. Overfelt, and A. Yasinsac. 3D Printer as a Weapon. Submitted to IFIP Working Group 11.10 Conference on Critical Infrastructure Protection (CIP), 2015.

[64] M. Yampolskiy, L. Schuetzle, U. Vaidya, and A. Yasinsac. Additive Layer Manufacturing with Metallic Alloys: Security Challenges. Submitted to the ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2015.