This is a preprint of an article published in *Progress in Additive Manufacturing 2021*, ed. N. Shamsaei, N. Hrabe, and M. Seifi (West Conshohocken, PA: ASTM International, 2022), 177–191. http://doi.org/10.1520/STP164420210125

Protecting Additive Manufacturing Information when Encryption is Insufficient

Joshua Lubell*

ABSTRACT

Recent research shows that a side-channel attack on a 3D printing process can bypass encryption-based defenses to obtain proprietary design information. This result has critical implications for outsourced additive manufacturing (AM). Three complementary cyber-risk management guidance specifications can help point the way for customers of AM services in protecting against such attacks – when the usual defenses are inadequate. This paper provides an overview of the three specifications, discussing what each provides. It then shows how the technology-agnostic specifications can be used in conjunction with attack taxonomies and threat classifications from the AM security research literature, and knowledge of AM technology, to determine which safeguards to implement to mitigate the risk of a side-channel attack scenario. The takeaway from this investigation is that there is more to AM security than encryption. A risk-based process, supplemented with AM specific knowledge of the manufacturing process and

* Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, 20899, USA; https://orcid.org/0000-0002-5776-1850

its security risks, is also needed to help find appropriate alternatives when technical controls are not an option.

Keywords

Additive Manufacturing, Cybersecurity, Risk Management, Security Controls, Side-Channel Attack, Technical Data Theft, Outsourced Additive Manufacturing.

Note

The author wishes to thank the internal NIST reviewers and ASTM peer reviewers for their insightful comments. He acknowledges the inclusion of many of their ideas. The opinions, recommendations, findings, and conclusions are the author's and do not necessarily reflect the views or policies of NIST or the United States Government.

Introduction

Additive manufacturing (AM) today is being used to create end products in industries ranging from aerospace and automotive to healthcare[1]. Freedom in design complexity plus improvements in AM technology have fueled this growth of adoption. Outsourced AM, a new business opportunity made possible by AM's success, enables AM customers and service providers to connect with one another through an online marketplace. This marriage of AM with e-commerce enables the customers to have their parts manufactured simply by uploading the part's digital 3D model specification to a website. But outsourced AM is vulnerable to a variety of maliciously-motivated cyber-threats[2].

AM security researchers have proposed AM attack classifications to better understand the risks and possible mitigations for outsourced AM and other scenarios. One such classification, developed by Yampolskiy et al.[3], defines three broad groups of an attacker's potential goals: theft

of technical data (the illegal gain of access to the customer's intellectual property (IP)), AM sabotage, and illegal part manufacturing (counterfeiting). Each of these groups forms the root of a twin taxonomy of goal sub-groups and applicable attack methods, with links between goals and methods feasible for achieving them. Gupta et al.[4] propose an alternative classification that defines physical supply chain models for AM printer hardware and for raw materials for manufacturing parts, along with a virtual supply chain model for design information representing part geometry and printing instructions. Attack methods are then classified according to how they interact with components in the supply chain targeted. As will be shown in the "Results and Discussion" section, Yampolskiy's attack-focused and Gupta's supply chain-focused classifications are complementary and are both useful for managing the risk of theft of technical AM data.

One attack method for stealing AM technical data is through side-channels, which are leakages of non-digital information such as timing measurements, acoustic measurements, power usage, or electromagnetic radiation[5]. Side-channels are an active area of security research. Side-channel analysis applied to AM enables an attacker to reverse-engineer a part during printing using non-digital information from the 3D printer's motors. Side-channel attacks bypass encryption, a commonly used cybersecurity measure, and thus require alternative defenses. Yampolskiy's taxonomy characterizes side-channel attacks as a type of reverse engineering where an attacker can steal the specification of a part's 3D geometry, required properties, or manufacturing process. Gupta's supply chain-centric approach views a side-channel attack as an attack on the printer hardware, which may be physically located either at an original equipment manufacturer (OEM) performing AM in-house or at a supplier providing AM services to an OEM under contract.

This paper's motivation is an outsourced AM attack scenario studied and implemented by

Gatlin et al.[6] and shown in figure 1. An AM customer contracts with an AM service provider to print a part specified as a digital 3D model file that the customer sends to the service provider. The AM service provider uses a material extrusion polymer 3D printing process. End-to-end encryption provides secure communication between the customer and service provider. Digital Rights Management protection is implemented on the service provider's host computer. Toolpath commands between the host computer and 3D printer are encrypted as well. Additionally, the 3D printer has a Trusted Platform Module to limit the presence of plaintext on the printer. The scenario assumes that access to the digital 3D model file is limited to the software application on the AM service provider's host computer that generates printing instructions from the data in the file uploaded by the AM customer.

To evade these security measures, a malicious actor at the service provider uses traces from multiple oscilloscopes, with probes attached to the printer's stepper motors, to reconstruct the part model data from a power side-channel analysis of the motor signals. The reconstruction algorithm, described in detail in Gatlin et al.[6], produces a point cloud representation of the printed part from the traces. None of the currently available defensive side-channel countermeasures are feasible for detecting or preventing this attack, and the power draw from the probes is too low to be noticeable.

This scenario requires an attacker who is sufficiently knowledgeable of 3D printing technology and electronics. The attacker must also be motivated enough to go to the trouble of instrumenting the printer and applying the reconstruction algorithm on the oscilloscope output. On the other hand, the instrumentation hardware is low-cost, and instrumentation can be accomplished such that the setup is compact enough to hide inside the enclosure of a typical desktop 3D printer[6]. Thus, the attack is achievable by anyone possessing the necessary skills and motivation. Also, it

is feasible even if the attacker is an insider acting alone without the AM service provider's knowledge.

The manufacturing process is shown in figure 2. Slicing software[7] residing on the AM service provider's host computer converts the 3D part model received from the AM customer into a sequence of 2D "slices". If support structures[8] are required to keep the part from collapsing during the manufacturing process, it is assumed that the AM customer has incorporated these into the part model prior to its upload to the AM service provider. The slicing software generates a set toolpath commands for printing each slice. Any slicing software configuration settings required to manufacture the part are included as metadata in the uploaded part model file. Metadata may include settings such as printing speed, build orientation, printing temperature, and infill pattern and density.

The explored research scenario has three key limitations. The first is that the experiment was limited to a single printing technology – polymer extrusion – and may not be reproducible for other additive manufacturing processes. The second, which relates to the first limitation, is the disconnect between toolpath motions and the true part shape, a result of the slicer's compensation for physical characteristics of the extruded material and extrusion process. These compensation techniques, some of which are user-configurable, are outside the scope of the side-channel analysis. Thus, a mesh generated from the reconstructed point cloud will vary from the original. The third limitation is that the algorithm does not distinguish between the part body and its support structures. Despite these limitations, in this scenario, the evaluation of part reconstruction was shown to be 99 % accurate[6].

This AM side-channel attack scenario raises the following question: how can the AM

customer reduce the risk of such an attack when encryption is insufficient, and the attack target (the service provider's 3D printer) is an externally managed entity? This paper looks to risk-based guidance from the National Institute of Standards and Technology (NIST) for answers. The next section provides an overview of principles underpinning the NIST approach, with a focus on three sources of guidance: SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)[9], the Cybersecurity Framework[10], and Special Publication (SP) 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)[11]. Although the NIST guidance is technology-agnostic, it is designed in such a way as to lead the user to technology-specific and threat-specific solutions. However, this does not obviate the importance of understanding AM technology and its vulnerability to an attacker using power side-channel analysis to steal technical data. Subsequent sections of the paper show how the NIST guidance – supplemented with AM specific knowledge of the manufacturing process and its security risks – can be applied to the attack scenario shown in figure 1 and which security controls other than encryption might be able to mitigate the AM customer's risk of technical data theft.

Risk-based Cybersecurity

The foundation of the NIST approach to cyber-risk management[12] is the CIA triad, where "CIA" stands for Confidentiality, Integrity, and Availability of information that a system produces, consumes, or transmits. Confidentiality is the prevention of unauthorized access and disclosure. Integrity is the guarding against improper modification and destruction such that the information's authenticity is guaranteed. Availability ensures timely and reliable information access and use.

> A system's impact may be either "low" (limited), "moderate" (serious), or "high"

(catastrophic). Federal Information Processing Standards Publication (FIPS) 200[13] provides a method for determining system impact based on the system's high water mark with respect to a loss of CIA. As an example, consider the AM service provider shown in figure 1 to be a "system" that is external to the AM customer's organization. This system processes multiple varieties of information that may be subject to a loss of CIA, the most consequential of which is a loss of confidentiality of the model data received from the AM customer or toolpath commands flowing between the host computer and the 3D printer. Hence, the system impact depends primarily on the consequences to the customer of the malicious actor stealing this data. Suppose the confidentiality of the data is critical to the AM customer's competitive advantage, financial health, or reputation. Then the AM service provider would be a high-impact system. On the other hand, if confidentiality of the data is not a major concern, the AM service provider would be a low-impact system. If a loss of design or toolpath data confidentiality were serious but not dire to the AM customer (e.g., the information is proprietary and commercially valuable but is not central to the business), the AM service provider might be considered a moderate-impact system.

SP 800-53[9] defines a collection of hundreds of security controls (safeguards), each of which protects the CIA of the system and the information it processes or transmits. This catalog of controls is highly detailed and comprehensive, yet implementation-agnostic. Controls are grouped into families, where each family relates to a specific topic, for example, access control or risk assessment. Most of these topics correspond to security requirements specified in FIPS 200.

The size and complexity of the SP 800-53 catalog can make it daunting and overwhelming to users. A companion specification, SP 800-53B[14], helps tame this complexity by providing baselines for low, moderate, and high impact information systems as starting points for security

control selection. For example, an organization selecting security controls for a low impact system might begin with the controls in the baseline for the low impact level (or more succinctly, the low baseline) and modify them as appropriate. Examples of modification include identification of common controls (controls that can be inherited to reduce duplication and save costs), assigning values to organization-defined control parameters (e.g., frequency of updates to a risk assessment), adding additional controls or enhancements, and providing additional guidance (e.g., implementation guidance).

Although the SP 800-53B baselines may require only minimal modification for common types of information system (e.g., enterprise desktop computers and file servers), they are likely to require far more modification for cyber-physical systems such as a 3D printer or complex systems, such as an AM service provider, that are composed of a mix of information technology, operational technology, and people. Therefore, the analysis discussed in the next section does not make direct use of SP 800-53B and instead relies on consideration of system characteristics, risks, and threats specific to the AM service provider technical data theft scenario.

The Cybersecurity Framework[10] is a hierarchically-organized taxonomy of security requirements intended to facilitate communication among stakeholders of an organization's current or target security posture. The Cybersecurity Framework's top-down model makes it easy to navigate and understand. The top level has five high-level risk management functions (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER). Each function is subdivided by a set of security outcome categories from the middle level. Each category is further divided by a set of outcome subcategories from the bottom level, which contains more than 100 distinct outcomes.

SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and

Organizations)[11] offers a middle ground between the high-level simplicity of the Cybersecurity Framework and the low-level complexity of SP 800-53. Unlike SP 800-53 and the Cybersecurity Framework, SP 800-171 is targeted to a specific user community: nonfederal organizations that receive United States government funding (although the guidance is also applicable to organizations that are not government-funded). SP 800-171's scope is limited to controlled unclassified information (CUI). CUI includes personally identifiable information (PII) as well as proprietary and other sensitive (but not classified) information. SP 800-171 has gotten increased attention recently resulting from greater awareness of the need to protect information pertaining to critical infrastructure coupled with a recent uptick in critical infrastructure cyber-attacks[15]. SP 800-171 contains a set of 110 security requirements for protecting CUI, each of which maps to one or more SP 800-53 controls. The SP 800-171 security requirements are organized into families nearly identical to the SP 800-53 control families. A *basic* requirement corresponds to the family's FIPS 200 requirement. A *derived* requirement supports its family's basic requirement(s).

These three documents not only complement one another, but also enable the development of a security plan or implementation that is traceable to requirements. Traceability is enabled by unique identifiers assigned to Cybersecurity Framework outcomes, SP 800-171 requirements, and SP 800-53 controls. NIST-provided mappings referencing the identifiers, discussed in the next section, further enable traceability and encourage it as a best practice. An organization can use these identifiers and mappings to help document that a deployed or proposed security solution implements a security control, which in turn supports an SP 800-171 requirement, which in turn is linked to a Cybersecurity Framework outcome. The security solution could be technological (public-key cryptography), physical (analog lock and key), or people-oriented (human guards).

Traceability helps ensure that security solutions meet requirements and are updated when requirements change.

Applying Guidance to the Side-Channel Scenario

This section illustrates how one might use the three guidance documents discussed in the previous section to develop a set of countermeasures to mitigate the risk of technical data theft to the AM customer in the scenario discussed in the Introduction section. A key challenge is that, because the AM service provider is an external system, the AM customer lacks direct control over the AM service provider's security practices. The approach, shown in figure 3, is to use the high-level guidance in the Cybersecurity Framework to lead to more detailed SP 800-171 requirements, which in turn point to yet more specific SP 800-53 security controls. The NIST Online Informative Reference Catalog's[16] mapping between Cybersecurity Framework version 1.1 subcategories and SP 800-171 security requirements provides the linkage between the Framework and SP 800-171. The mapping tables in Appendix D of SP 800-171 provide the linkage between SP 800-171 and SP 800-53.

This approach is not the only possible approach to using NIST guidance documents for this specific scenario. However, the approach has several characteristics making it an appealing choice:

- The progression from the Cybersecurity Framework to SP 800-171 to SP 800-53 follows the well-established principle of stepwise refinement[17], making use of hierarchies and information hiding to manage the inherent complexity of cyber-risk management.
- The AM customer's model data file and the toolpath commands are both CUI, making protection of their confidentiality within the scope of SP 800-171.

- Assuming that the AM service provider is at least a moderate-impact system (or possibly a high-impact system), SP 800-171 guidance applies. SP 800-171 assumes a confidentiality impact value of no less than moderate for CUI.

We begin applying the guidance by narrowing our focus to the Cybersecurity Framework's IDENTIFY function, whose definition is "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities." Unlike IDENTIFY, the four other Framework functions are implementation-focused (i.e., their definitions begin with "Develop and implement…"). Because AM is outsourced, the customer cannot implement any security controls without cooperation from the AM service provider or, as a last resort, deciding not to do business with the AM service provider. Identifying and understanding security risks is a logical first step to taking appropriate actions to mitigate those risks. This is not to say that other Framework functions such as PROTECT cannot be part of a strategy for ensuring that the AM customer's technical data is not stolen. For example, a legally binding contract between the AM customer and service provider might offer an acceptable amount of risk reduction of technical data theft.

Two IDENTIFY function categories relevant to the attack scenario are shown in figure 4. Asset Management (ID.AM), the first category, is relevant because you cannot secure what you do not know you have. Of particular interest within ID.AM is outcome ID.AM-4 (External systems are catalogued). Another category of the IDENTIFY function, Risk Assessment (ID.RA), pertains to understanding the risks that theft of the AM customer's technical data from the AM service provider pose to the AM customer's operations, profits, reputation, and stakeholders. Outcome ID.RA-3, which requires identifying and documenting all threats, including those that are external,

would include the possibility of a malicious AM service provider or a lone malicious insider using side-channel analysis to steal the customer's data from the printer.

ID.AM-4 and ID.RA-3 translate to SP 800-171 requirements, as shown in figure 5, using the mapping from the Online Informative References Catalog[16]. ID.RA-3 maps to SP 800-171 Basic Requirement 3.11.1, which corresponds to the FIPS 200 Risk Assessment requirement and directs organizations to periodically assess risk to business processes, assets and individuals resulting from processing, storing, or transmitting CUI. Basic Requirement 3.11.1 contains guidance emphasizing two points: (1) effective risk assessments require well-defined system boundaries, and (2) risk from external parties such as service providers must be considered. Both points reinforce the importance of considering the AM service provider as an external system and categorizing the information assets the service provider could gain from the AM customer via a side-channel attack.

ID.AM-4 maps to SP 800-171 Derived Requirement 3.1.20, which supports the Access Control family's Basic Requirements 3.1.1 and 3.1.2. These Basic Requirements collectively limit who can use a system and, for authorized users, what types of access are permitted. Derived Requirement 3.1.20 pertains specifically to external systems. Its guidance defines an external system as one where the organization has no direct supervision or authority to apply or assess security controls. The guidance also provides examples of external systems, including "platform as a service" which characterizes the AM service provider. The guidance goes on to recommend that organizations "establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures." If the organization (AM customer) and external system owner (AM service provider company) cannot agree on terms and conditions, the

organization (AM customer) may restrict its use of the external system (AM services).

The mapping tables in SP 800-171 Appendix D link basic requirement 3.11.1 and derived requirement 3.1.20 to SP 800-53 security controls RA-3 (Risk Assessment) and AC-20 (Use of External Systems), respectively, as shown in figure 6. Security control RA-3's control statement (from the SP 800-53 document) adds these additional pertinent details to basic requirement 3.11.1:

- A list of what a risk assessment should include, such as identification of threats and vulnerabilities and determination of the likelihood and magnitude of harm from threats.
- Parameters an organization can instantiate to specify how assessment results should be documented, how often they should be reviewed, who they should be shared with, and how often they should be updated.

Security control AC-20's control statement from the SP 800-53 document expands upon derived requirement 3.1.20 by adding:

- Parameters for an organization to specify terms and conditions governing the use of external systems or controls required to be implemented on external systems (consistent with the trust relationship between the originating and system-owning organizations).
- A parameter for specifying the types of external systems for which use is prohibited. For example, the AM customer could use this parameter to forbid use of the AM service provider if terms and conditions cannot be agreed upon or are not met.
- Supplemental guidance regarding trust relationships between the organization

owning the external system (e.g., a company providing on-demand AM services) and the originating organization (e.g., the AM customer).

Results and Discussion

Analysis using the guidance documents and mappings discussed in the previous section points to two SP 800-53 security controls that are highly relevant to the AM customer: RA-3 and AC-20. This section looks more closely at these two controls and shows how leveraging the Yampolskiy[3] and Gupta[4] taxonomies and knowledge of the AM process workflow (fig. 1) can enhance the SP 800-53 guidance to make it more applicable to the outsourced AM scenario discussed in the "Introduction" section.

RA-3 specifies in imperative language what constitutes a risk assessment. In the context of our scenario, the assessment is of the risk to the AM customer of relying on the AM service provider for AM services. According to RA-3, a risk assessment includes identification of:

- **The threat.** The threat in this scenario is theft of the AM customer's technical data resulting from a side-channel attack, circumventing protection afforded by encrypting the technical data in transit and at rest.
- **Vulnerabilities to the threat.** Gupta's supply chain-focused classification informs us that the printer's power supply mechanism (part of the printer hardware supply chain) is vulnerable to a side-channel attack and that the printer may be physically located either at the AM customer or at a contract-based print shop (the AM service provider).
- **Likelihood of the threat occurring and being successfully executed.** The likelihood of successful theft of technical data occurring depends on multiple

factors, including:

- Complexity and novelty of the technical data. If the part model file is for a critical part whose design is sophisticated and innovative with complex geometry and detailed slicing instructions, then a bad actor would be more motivated to steal the data using side-channel analysis. Conversely, if the 3D model were simplistic and buildable using the slicing software's default configuration settings, the bad actor would probably be less motivated to execute a side-channel attack.
- Printing technology. Yampolskiy's taxonomy tells us that side-channel analysis may *conditionally* achieve success in reverse-engineering a part specification or its manufacturing process information. Therefore, although Gatlin et al.[6] was able to achieve a high level of accuracy reconstructing parts using toolpath data obtained via a polymer extrusion-based printer's power side-channel, the likelihood of success may be less certain for other printing technologies. More research is needed to determine the viability of power and other types of side-channel analysis for directed energy deposition (DED) and powder bed fusion (PBF), two printing technologies for metal AM. Investigations of AM side-channel attacks in the research literature to date have focused primarily on polymer extrusion printing processes[3].

- **Consequences of a successful attack.** This depends on how valuable the data is to the AM customer. Would technical data theft result in reduced market share?

Would the production of inferior-quality counterfeits result in reputational damage or lawsuits? Could customer safety be jeopardized? Each of these possibilities would increase a successful attack's damage to the AM customer and its stakeholders.

AC-20 provides extensive but scenario-agnostic guidance on establishing terms and conditions for use of external systems. For the AM customer, this translates into terms and conditions required to do business with the AM service provider. These include:

- The safeguards the AM service provider must implement to protect against a malicious insider using a side-channel attack to steal the customer's data, assuming the malicious insider is acting alone and that the service provider is non-malicious. Since encryption is insufficient, the service provider could deploy alternative, non-technical controls such as allowing only authorized personnel physical access to the facility where the printer is located, video surveillance, and training employees to be aware of and responsive to insider threats. Again, this assumes an honest service provider.
- Verification that the AM service provider has implemented the necessary controls. Verification methods are highly dependent on how much the AM customer trusts the AM service provider's honesty and diligence to provide adequate security.

The terms, conditions, and verification methods are informed by the likelihood and impact of a successful attack as determined in the risk assessment specified in RA-3. If a successful attack is highly unlikely or its impact is low, then the AM customer might decide the risk of a less-than-trustworthy AM service provider is acceptable. For example, if the part to be manufactured is of

low value with minimal quality requirements, the AM customer may be willing to go with a less expensive but less trustworthy service provider. At the opposite extreme, the AM customer may decide its technical data is so valuable and so critical to mission and business goals that in-house manufacturing is the only acceptable alternative.

Yet another possibility is that the AM customer cares about the quality of the manufactured part but not so much about the confidentiality of the design IP. For example[4], suppose the AM customer is an antique car owner looking for a replacement part that is no longer available but for which a publicly available 3D part model exists. The customer contracts with the AM service provider to print the part. A supply chain model of this sub-scenario of our outsourced AM scenario is shown in figure 7. Since the confidentiality of the design data is not a concern, the AM customer can establish terms and conditions with the AM service provider without worry of a side-channel attack on the service provider's printer.

To implement security controls RA-3 and AC-20, the AM customer must first instantiate the parameters mentioned in the previous section. But how does the AM customer decide upon the best parameter values? Doing so is nontrivial and entails a requirements engineering process. Glinz's aspect-orientation approach[18] points to a helpful way to start. Glinz observed a common pattern with requirements. There is usually a dominant concern, typically a functional requirement that is composed of aspects. The aspects may be either functional or non-functional requirements. The outsourced AM attack scenario fits this pattern. The dominant functional requirement is that the printed part conforms to its digital design specification (as expressed in the 3D part model) and build instructions (as expressed in the slicer configuration settings). Security, a non-functional aspect of this functional requirement, is a condition resulting from the deployment of controls that

enable the AM customer to satisfy this dominant functional requirement despite risks posed by threats to its use of the AM service provider. The threat to the AM customer is theft, via a side-channel attack on the service provider's 3D printer, of IP uploaded to the service provider.

Thus, the AM customer's SP 800-53 parameter value choices should be strongly influenced by characteristics of the uploaded data such as its level of sophistication, novelty, and how much of it constitutes the customer's IP (versus publicly available information such as the antique car part data in the example discussed earlier). Reputation should also be considered. For example, if the uploaded IP was determined to be central to the AM customer's "brand", that would merit frequent risk re-assessments and imposing (and enforcing) stringent terms and conditions on the AM service provider. Conversely, if the IP constituted model data needed to print low-cost promotional items to be given away at trade shows, then the parameter settings could be more permissive.

Conclusion

The Cybersecurity Framework, SP 800-171, and SP 800-53 together provide helpful guidance in assessing and mitigating cyber-risks. Using an outsourced AM side-channel attack scenario as an example, this paper illustrated how the guidance can help an AM customer reduce the risk of theft of technical data when encryption alone is insufficient. Even though the guidance documents are neither technology-specific nor business-specific, this research showed how – when supplemented with attack taxonomies and threat classifications from the AM security research literature – they can lead to potential solutions that are informed by business considerations, trust between the parties involved, and some understanding of AM technology.

An important lesson learned from this investigation is that risk can be managed but never

eliminated. Encryption is an excellent cybersecurity measure that has proven indispensable for protecting cyber-assets, yet it is neither practical nor effective against some threats. Sometimes non-technical alternatives are the only options. Rigorous application of NIST's risk management guidance can enable development for AM security solutions that are effective and are traceable to business objectives, operating environment, AM process characteristics, and security threats. Traceability is essential for assuring stakeholders that due diligence was done, especially when the best security solution is the least bad among a set of bad choices.

The best way to avoid being left with a set of undesirable security options is to view security not with a compliance mindset but instead as a key aspect supporting an organization's mission. Security should have parity with other "ilities" such as reliability, usability, maintainability, and adaptability. This means applying risk management guidance early on when designing a system or business activity and not as an afterthought. A proactive aspect-oriented approach to risk management can be particularly helpful when deciding whether to adopt a new technology such as outsourced additive manufacturing where technology-specific security advice is scarce.

References

1. M. Srivastava and S. Rathee, "Additive manufacturing: recent trends, applications and future outlooks," *Progress in Additive Manufacturing* (2021). https://doi.org/10.1007/s40964-021-00229-8
2. C. Adkins, S. Thomas and D. Moore, "Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing Platforms," in *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security* (ACM, 2021): 61–65.

https://doi.org/10.1145/3462223.3485622

3. M. Yampolskiy *et al.*, "Security of additive manufacturing: Attack taxonomy and survey," *Additive Manufacturing,* 21 (2018): 431–457. https://doi.org/10.1016/j.addma.2018.03.015
4. N. Gupta, A. Tiwari, S. T. S. Bukkapatnam, and R. Karri, "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks," *IEEE Access* 8 (2020): 47322 – 47333. https://doi.org/10.1109/ACCESS.2020.2978815
5. F.-X. Standaert, "Introduction to Side-Channel Attacks," in *Secure Integrated Circuits and Systems*, ed. Verbauwhede, I. M. R. (Springer US, 2010), 27–42. https://doi.org/10.1007/978-0-387-71829-3_2
6. J. Gatlin *et al.*, "Encryption is Futile: Reconstructing 3D-Printed Models Using the Power Side-Channel," in *24th International Symposium on Research in Attacks, Intrusions and Defenses* (ACM, 2021): 135–147. https://doi.org/10.1145/3471621.3471850
7. F. Baumann, H. Bugdayci, J. Grunert, F. Keller and D. Roller, "Influence of slicing tools on quality of 3D printed parts," *Computer-Aided Design and Applications* 13 (2016): 14–31. https://doi.org/10.1080/16864360.2015.1059184 /
8. J. Jiang, X. Xu and J. Stringer, "Support Structures for Additive Manufacturing: A Review," *JMMP* 2 (2018): 64. https://doi.org/10.3390/jmmp2040064
9. Joint Task Force Interagency Working Group, "*Security and Privacy Controls for Information Systems and Organizations*" (2020). https://doi.org/10.6028/NIST.SP.800-53r5
10. National Institute of Standards and Technology, "*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*" (2018). https://doi.org/10.6028/NIST.CSWP.02122014

11. R. Ross, V. Pillitteri, K. Dempsey, M. Riddle and G. Guissanie, "*Protecting controlled unclassified information in nonfederal systems and organizations*" (2020). https://doi.org/10.6028/NIST.SP.800-171r2
12. Joint Task Force Transformation Initiative, "*Risk management framework for information systems and organizations: a system life cycle approach for security and privacy*" (2018). https://doi.org/10.6028/NIST.SP.800-37r2
13. National Institute of Standards and Technology, "*Minimum security requirements for federal information and information systems*" (2006). https://doi.org/10.6028/NIST.FIPS.200
14. Joint Task Force, "*Control Baselines for Information Systems and Organizations*" (2020). https://doi.org/10.6028/NIST.SP.800-53B
15. K. Slonka, "Managing Cyber Security Compliance Across Business Sectors," *IIS* 21 (2020). https://doi.org/10.48009/1_iis_2020_22-29
16. N. Keller, S. Quinn, K. Scarfone, M. C. Smith and V. Johnson, "*National Online Informative References (OLIR) Program: Program Overview and OLIR Uses*" (2020). https://doi.org/10.6028/NIST.IR.8278
17. H. D. Mills, "Stepwise refinement and verification in box-structured systems," *Computer* 21 (1988): 23–36. https://doi.org/10.1109/2.948
18. M. Glinz, "On Non-Functional Requirements," in *15th IEEE International Requirements Engineering Conference (RE 2007)* (IEEE, 2007): 21–26. https://doi.org/10.1109/RE.2007.45

FIGURE 1. A malicious actor with an oscilloscope steals the design of a printed part even though data is encrypted in transit and at rest.

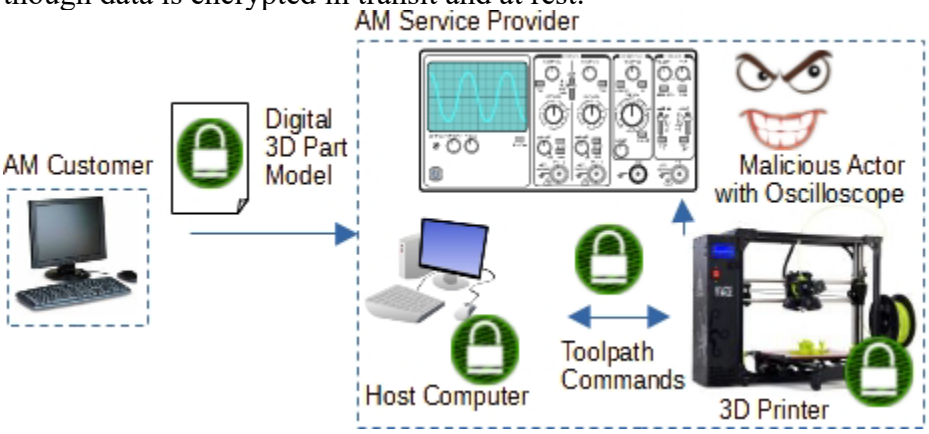

FIGURE 2. AM process workflow.

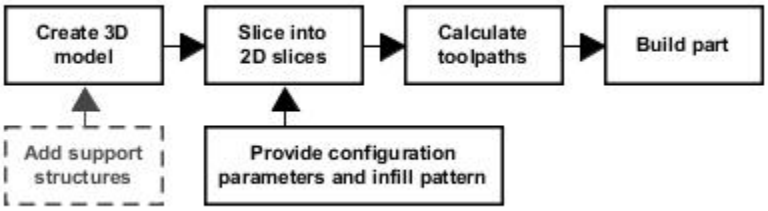

FIGURE 3. Applying the guidance.

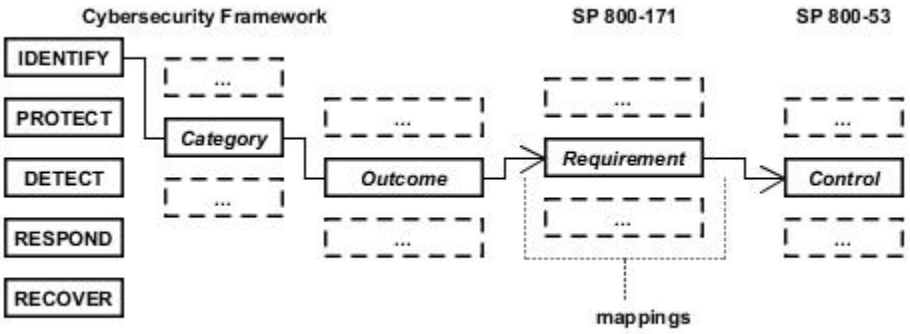

FIGURE 4. Some relevant Cybersecurity Framework outcomes.

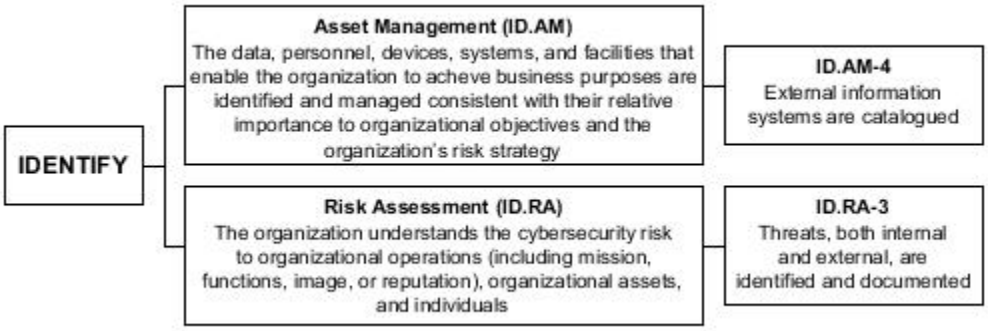

FIGURE 5. Mappings from ID.AM-4 and ID.RA-3 to SP 800-171 requirements from the Risk Assessment and Access Control families.

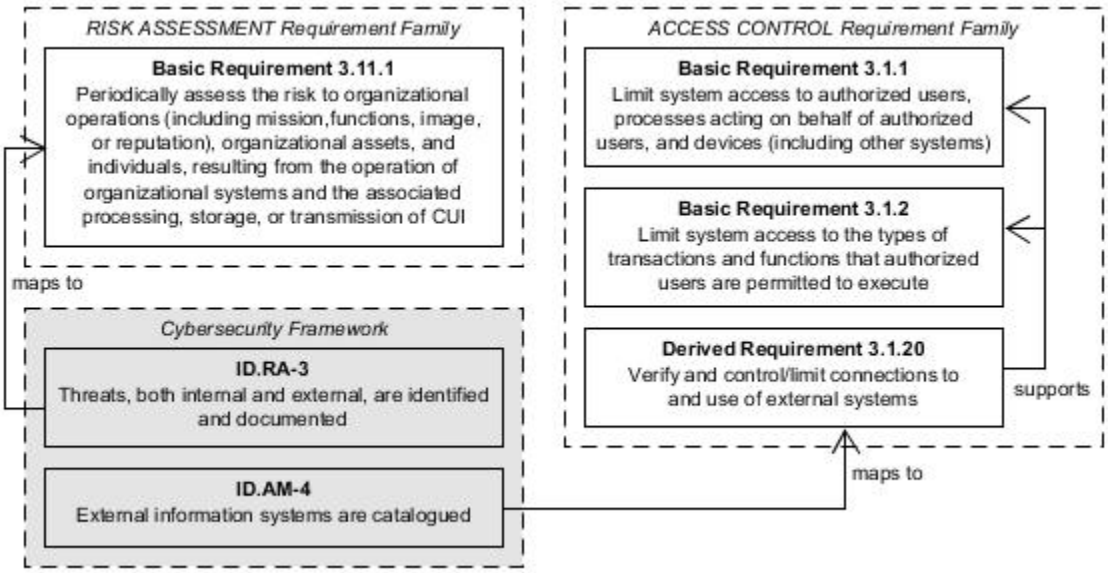

FIGURE 6. Mappings from SP 800-171 requirements to SP 800-53 controls.

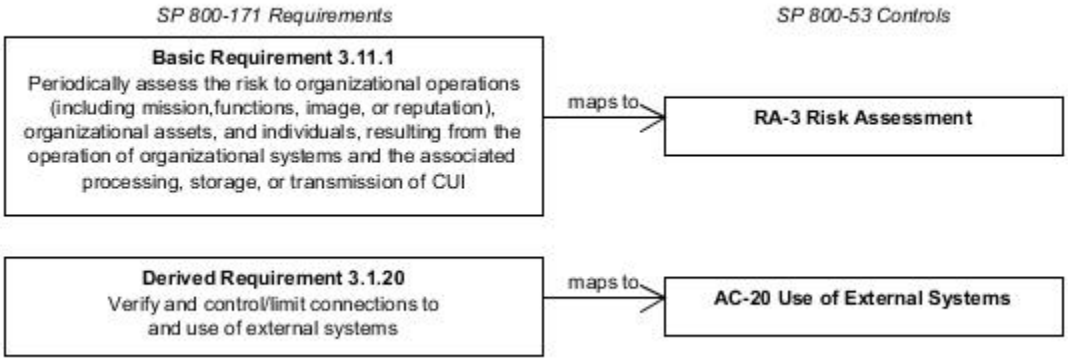

FIGURE 7. Supply chain model of antique car part AM scenario (adapted from Gupta et al.[4]).