International Journal of Multidisciplinary Research and Growth Evaluation

International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 05-05-2021; Accepted: 25-05-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 3; May-June 2021; Page No. 492-495

General issues in 3D printing security domain

Giao N Pham
Department of Computing Fundamentals, FPT University, Hanoi, Vietnam

Corresponding Author: **Giao N Pham**

Abstract
With the development of 3D printing technology, 3D printing has recently been applied to many areas of life including education, healthcare, aerospace, automotive, industrial design and so on. Due to the fact that the benefit of 3D printing is great, 3D printing models are often copied, shared and used several times without charging any copyright fee from the original providers. Besides, user can download 3D weapon models from the Internet and easily print them out without any restriction from the production managers or share them unlimitedly. Moreover, 3D printing models are also attacked by hackers and distributed without agreement from the original providers. Furthermore, certain special models and anti-3D weapon models in 3D printing must be protected against unauthorized users. Therefore, the original providers desire a watermarking algorithm to protect the copyright of 3D printing. In addition, an anti-3D weapon model detection algorithm for safe 3D printing is also necessary to restrict the printing of dangerous 3D weapon in 3D printing industry. Finally, in order to prevent attacks, illegal copying and to ensure that all access is authorized, 3D printing models should be encrypted before being transmitted and stored. In this paper, I would like to present general issues in 3D printing security domain.

Keywords: 3D printing, 3D printing security, 3D model watermarking, Data encryption, and 3D weapon

1. Introduction

The three-dimensional (3D) printing is a process of making 3D solid objects directly by adding material layer by layer in a variety of ways. It is also known as rapid prototyping or additive manufacturing that is a mechanized method whereby 3D objects are quickly made on a reasonably sized machine connected to a computer containing blueprints for the object [1, 2]. So, 3D printing allows users to turn any digital file into a 3D physical product (see Fig. 1). The technology for printing physical 3D objects from digital data was first developed by Charles Hull in 1984 [3, 4]. He named the technique as Stereo lithography and obtained a patent for the technique in 1986. While Stereo lithography systems had become popular by the end of 1980s, other similar technologies such as Fused Deposition Modeling (FDM) and Selective Laser Sintering (SLS) were introduced. In 1993, Massachusetts Institute of Technology patented another technology, named "Three Dimensional Printing Techniques", which is similar to the inkjet technology used in 2D Printers. In 1996, three major products, "Genisys" from Stratasys, "Actua 2100" from 3D Systems and "Z402" from Z Corporation, were introduced. In 2005, Z Corporation launched a breakthrough product, named Spectrum Z510, which was the first high definition color 3D Printer in the market. Nowadays, there are different technologies that were developed to build 3D structures and objects such as Stereo Lithography (SLA), Digital Light Processing (DLP), Fused Deposition Modeling (FDM), Selective Laser Sintering (SLS), Selective Laser Melting (SLM), Electronic Beam Melting (EBM) and Laminated Object Manufacturing (LOM).

In order to print out physical 3D objects from 3D printing models, user have to cut 3D printing model into a set of 2D slices, called a set of layers and 3D Printer will print 3D object from these 2D slices. 3D Printers are machines that produce physical 3D objects from digital data as shown in Fig. 1. It is used in a variety of industries including jewelry, footwear, industrial design, architecture, engineering and construction, automotive, aerospace, medical and healthcare industries, education and consumer products [5, 6]. For example: in healthcare domain, the applications of 3D printing in the context of health have the potential of increasing the life expectancy of humans [7]. 3D printing can improve the quality of life of individuals whose organs have failed. In aerospace domain, the airline industry is a driving force in the evolution of this technology for both manufacturing end-use parts and prototyping such as air ducts, wall panels, seat frameworks and engine components.

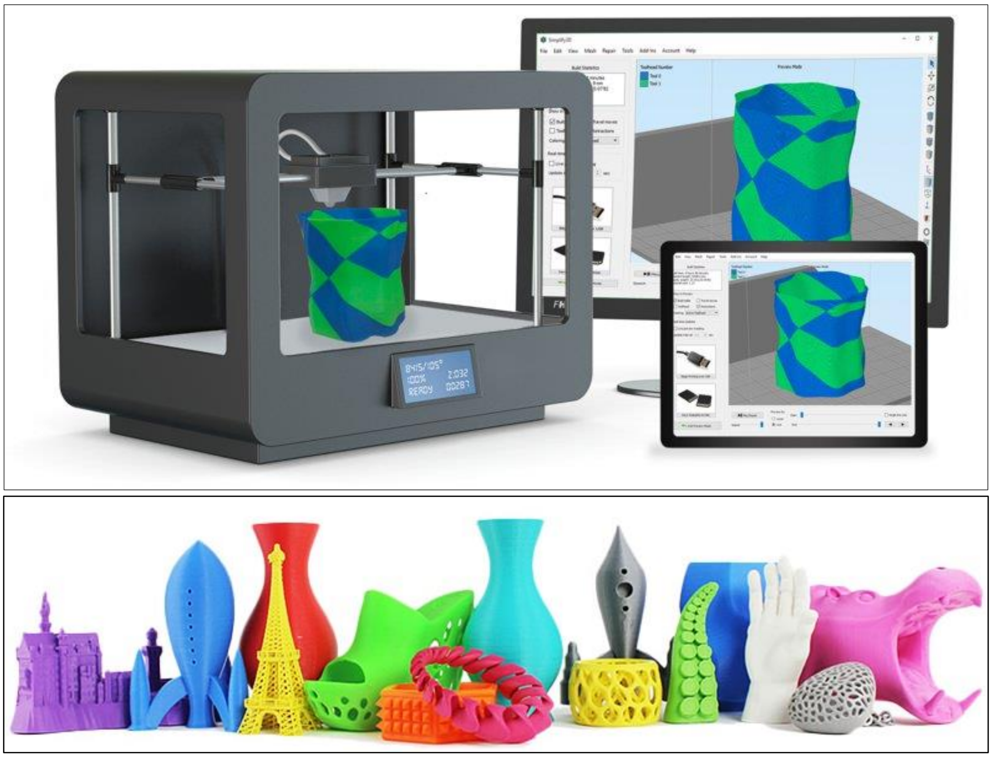

Fig 1: Making of physical 3D objects from digital data by 3D Printer.

2. General Issues in 3D Printing

With the development of 3D printing technology, the applications of 3D printing and the price of a 3D printer is not expensive, individual users can buy a 3D printer and download 3D printing models on the Internet to print physical 3D objects. This leads to security concerns in 3D printing industry. The first aspect of 3D printing security is the ownership identification and copyright protection [8]. Because user can copy or download 3D printing models from the Internet without charging and then distribute them unlimitedly as shown in Fig. 2. It makes a great damage to the manufacturers and the original providers. Therefore, manufacturers need a solution to protect copyright, and providers need a solution to identify their products in commercial transactions.

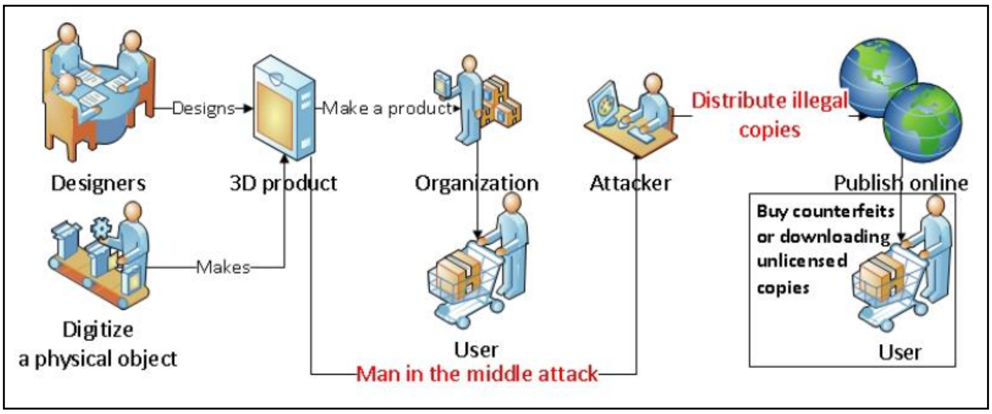

Fig 2: Copyright issue for 3D printing.

With the development of 3D printing technology, people can search 3D weapon models as firearm, gun, and knife to print physical 3D objects with home 3D printers as shown in Fig. 3 or share them unlimitedly. Specially, with new materials user can print dangerous weapons and can use them to do damage. This leads to the concerns for 3D printing security because anyone can print dangerous weapons [9]. Until now, the danger of 3D printed weapons is proved but worries about the danger of 3D printed weapons have just come to the hints, considerations and policies. Researchers have not been interested in issue “how to restrict the printing of 3D weapon models” yet, and there is no solution to stop the printing of 3D weapon models in 3D printing industry. So, the second aspect of 3D printing security is safe 3D printing and the current target of safe 3D printing is anti-3D weapon model detection.

Fig 3: 3D printed weapon by 3D Printer.

In addition, in order to produce 3D printing models and maintain the database of 3D printing models, producers consume a lot of money and human resources while 3D printing models are easily copied in the storage process by un-authorized users or attacked in the transmitting process by attackers (see Fig. 4). Furthermore, some special 3D printing models or dangerous 3D weapon models must be protected and secured from un-authorized user. Thus, 3D printing models should be encrypted before being stored and transmitted to prevent illegal copying and to ensure access control. So, an encryption method is suitable for this purpose. Summary, from the aspects of 3D printing security are above mentioned, we have to solve three issues for 3D printing security: copyright protection and ownership identification, anti-3D weapon model detection for safe 3D printing, and 3D printing model encryption as described in Fig. 5.

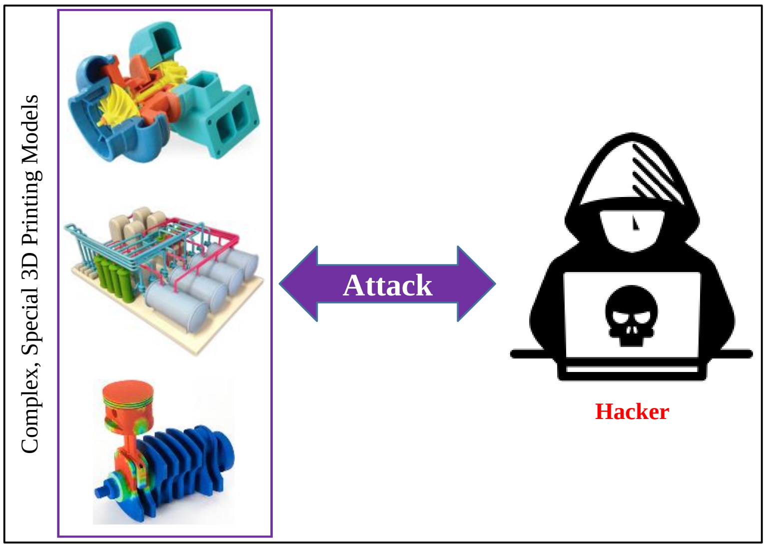

Fig 4: Hacker attacks 3D printing models.

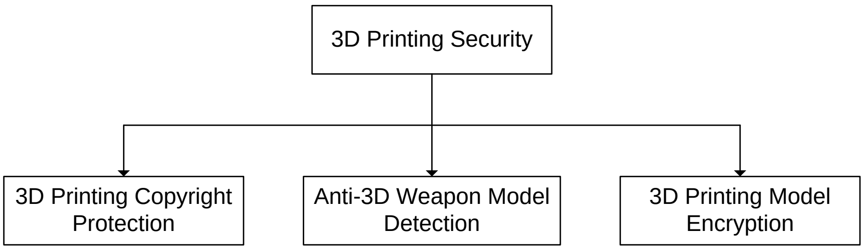

Fig 5: Aspects of 3D printing security.

3. Strategies for 3D Printing Security

To protect copyright and identify ownership for 3D printing, a watermarking method is necessary. Previously, there are many watermarking methods for 3D contents, 3D mesh and 3D animals. But these methods are only useful for the copyright protection and ownership identification of 3D contents. They could not be applied to the copyright protection and ownership identification of 3D printing. Because the output of 3D printing is a physical 3D printed object. So, the aim of a watermarking method for 3D printing is how to extract the embedded watermark data from the scanned 3D printing model of a physical 3D printed object.

For anti-3D weapon model detection, manufacturers desire to prevent the printing of anti-3D weapon models. Therefore, they need an algorithm to filter anti-3D weapon models when these models are used as the input of 3D printers. Up to the present time, there is no solution to stop the printing of 3D weapon models in 3D printing industry. The handgun detection techniques based on image processing methods applied to the surveillance systems or the checking security systems in special places as airport or building. They could not be applied to safe 3D printing. Because the input of 3D printing is a 3D printing model, it is not an image. Besides, 3D model matching techniques could not also apply to safe 3D printing in order to prevent the printing of 3D weapon models. Because, 3D model matching techniques have to access to the database of 3D models to give the decision. If the sample models of a model type are not stored in the database of 3D models, an input model will be not matched to any model when it is queried by 3D model matching techniques. So, an anti-3D weapon model detection solution for safe 3D printing is necessary and suitable to prevent the printing of 3D weapon models for safe 3D printing industry.

The purpose of attackers or un-authorized users is to steal valuable 3D printing models without charging. So, an encryption method for 3D printing model can prevent the actions of attackers and un-authorized users. Therefore, the target of 3D printing model encryption is how to change the content of 3D printing models or how to distort the shape of 3D printing models before they are stored and transmitted to prevent attacks, illegal copying and to ensure access control in the storage and transmission process. The encrypting techniques for 3D printing model must be effective to the entire content of 3D printing model and ensured the conversation between the databases of 3D printing models. Furthermore, these techniques must be responsive to the various formats of 3D printing models.

4. Conclusion

In this paper, I presented general issues in 3D printing security. It includes three aspects: 3D printing watermarking; 3D printing encryption; and 3D weapon model recognition. I hope that this paper is useful for researchers, who are researching and intending to study about 3D printing technology.

5. Acknowledgments

This work is supported by FPT University, Hanoi, Vietnam

6. Disclosure of conflict of interest

On behalf of all authors, corresponding author declares that there is no conflict of interest to publish this research.

7. References

1. How 3D Printing Works: The Vision, Innovation and Technologies Behind Inkjet 3D Printing. 3D Systems: Rock Hill, CA, USA, 2012. Available online: http://www.officeproductnews.net/sites/default/files/3dWP_0.pdf (accessed in 2021).
2. Lidia HA, Paul AJ, Jose RJ, Will H, Vincent CA, White Paper: 3D printing, Atos: Irving, TX, USA, 2014. Available online: https://atos.net/wp - content/uploads/2016/06/01052014 - AscentWhitePaper - 3dPrinting - 1.pdf (accessed in 2021).
3. 3D Printing Technology. Available online: http://up.nic.in/knowdesk/3D-Printing-Technology.pdf (accessed in 2021).
4. Types of 3D printers or 3D printing technologies overview. Available online: http://3dprintingfromscratch.com/common/types-of-3d-printers-or-3d-printing-technologies-overview/ (accessed in 2021).
5. Chandra TA, Patel M, Singh PK. Study of 3D Printing and its Application, International Journal for Research in Advanced Computer Science & Engineering. 2016; 2(3):9-12.
6. Learn how 3D Printing is useful everywhere. Available online: https://www.sculpteo.com/en/applications/ (accessed in 2021).
7. Helena D. Applications of 3D printing in healthcare," Kardiochirurgiai Torakochirurgia Polska. 2016; 13(3):283-293.
8. Deven D. Master's Thesis: 3D Printing and the Implications on Intellectual Property from a Belgian-European Perspective, Faculty of Law, Ghent University, 2016.
9. Gerald Walther. Printing Insecurity? The Security Implications of 3D-Printing of Weapons, Sci. Eng., Ethics. 2015; 21(6):1435-1445.