College of Professional Studies

Northeastern University San Jose

MPS Analytics

Course: ALY6080

Assignment:

Module 3 Project - Annotated Bibliography (Article 2)

Submitted on:

May 2, 2023

Submitted to:

Prof: VENKATA DUVVURI

Submitted by:

ARCHIT BARUA

HEEJAE ROH

NIKSHITA RANGANATHAN

SHYAMALA VENKATAKRISHNAN

Cybersecurity for 3D Printed Medical Devices

The application of 3D printing technology in healthcare has brought about significant changes in the creation and utilization of medical devices. This technology has enabled the production of customized medical devices, including prosthetics and surgical instruments, which are more effective and less expensive than traditional ones. However, 3D printing technology also comes with cybersecurity challenges that must be addressed to protect patient data and the security of medical devices.

Cybersecurity should be considered as the number one priority when designing the medical devices and products in the healthcare 3D printing ecosystem. Hackers can breach the security of these devices and manipulate them to harm patients or access sensitive patient data. Many technological experts are anticipating cyberattacks, medical device malfunctions, cybersecurity breach in the healthcare system and 3D printing space. The key points and takeaways from the presentation provided by Vidya Murthy, VP of Operations for MedCrypt is discussed in this article, providing a general overview on why medical device manufacturers need to pay attention to their cybersecurity strategies.

There is a pressing need for the medical device makers to start to implement cybersecurity strategies more proactively before shipping their products. Stephan Thomas, the Co-founder and Chief Strategy Officer of Identify3d, has discussed two key risk areas that device manufacturers must secure in order to avoid cyberattacks particularly in digital manufacturing space (additive manufacturing). In the past, ensuring the quality of a part was a simpler process due to higher barriers to gray-market or counterfeit operators, before the digitization of manufacturing. However, with the emergence of additive manufacturing, it has become easier for anyone with access to the right 3D printer, materials, and digital design files to create an exact copy of a 'legitimate' part. The risk of unauthorized manufacturing becomes even greater with distributed manufacturing, making it more challenging to manage quality risk once manufacturing data is shared with legitimate third parties or, worse, stolen for unauthorized production. This unauthorized manufacturing can lead to the production of sub-standard quality parts, which can result in costly recalls or system disruptions.

Encryption is one effective method that can be employed to ensure the cybersecurity of 3D printed medical devices. Encryption involves converting sensitive data into code, rendering it incomprehensible to unauthorized users. Furthermore, encryption keys can be used to prevent unauthorized access to medical devices.Another critical cybersecurity measure is the use of secure networks. Medical devices can be connected to networks for remote monitoring and management, but these networks must be secured to prevent unauthorized access. Secure networks require the use of strong passwords and other authentication mechanisms to prevent unauthorized access to medical devices and the data they contain.

With the increasing adoption of digital manufacturing methods, medical device manufacturers are turning to advanced technologies that can protect and validate manufacturing data, manage data flow through licensing, and maintain decentralized and unalterable records of these movements. Additive manufacturing in the medical device industry requires cybersecurity technology that can encrypt, distribute, and track the digital flow of parts to prevent the production of counterfeit and substandard parts. It is necessary to ensure that maliciously modified or uncertified parts are not used in medical devices, as they can pose a significant risk to patients' safety and health. Therefore, medical device manufacturers must implement cybersecurity measures that can guarantee the authenticity and quality of digitally manufactured components.

References

- https://medium.com. *Cybersecurity for 3D Printed Medical Devices*. Retrieved from Medium: https://medium.com/healthcare-3d-printing-stories/cybersecurity-for-3d-printed-medical-devices-560c8a944 ,. (2021, March 3).

- https://3dheals.com/ – *Five Reasons Cybersecurity Will Play a Critical Role in 3D Printing in Healthcare – Part 3*: https://3dheals.com/five-reasons-cybersecurity-will-play-a-critical-role-in-3d-printing-in-healthcare-part-3/?utm_content=buffer39da1&utm_medium=social&utm_source=bufferapp.com&utm_campaign=buffer ., (2019, May 25).