TALLINN UNIVERSITY OF TECHNOLOGY
SCHOOL OF ENGINEERING
Tartu college

ANALYSIS OF POSSIBLE 3D PRINTER CYBERSECURITY VULNERABILITIES AND THEIR MITIGATION SOLUTIONS

ANALÜÜS 3D PRINTERITE VÕIMALIKEST KÜBERTURBE OHTUDEST JA NEID LEEVANDAVATEST MEETMETEST

PROFESSIONAL HIGHER EDUCATION THESIS

Student: Fanny Lamp

Student code: 193027EDTR

Supervisors: Rinaldo Rüütli, Engineer
Karin Muoni, Lecturer

Tartu 2023

AUTHOR'S DECLARATION

Hereby I declare, that I have written this thesis independently.

No academic degree has been applied for based on this material. All works, major viewpoints and data of the other authors used in this thesis have been referenced.

04.01.2023.

Author: Fanny Lamp

/signature /

Thesis is in accordance with terms and requirements

04.01.2023.

Supervisor: Rinaldo Rüütli

/signature/

Accepted for defence

04.01.2023.

Chairman of theses defence commission: Aime Ruus

/signature/

Non-exclusive Licence for Publication and Reproduction of Graduation thesis[1]

I, Fanny Lamp (date of birth: 29.01.1999) hereby

1. grant Tallinn University of Technology (TalTech) a non-exclusive license for my thesis Analysis of Possible 3D Printer Cybersecurity Vulnerabilities and Their Mitigation Solutions.

supervised by Rinaldo Rüütli and Karin Muoni.

1.1 reproduced for the purposes of preservation and electronic publication, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright;

1.2 published via the web of TalTech, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright.

1.3 I am aware that the author also retains the rights specified in clause 1 of this license.

2. I confirm that granting the non-exclusive license does not infringe third persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[1] *Non-exclusive Licence for Publication and Reproduction of Graduation Thesis is not valid during the validity period of restriction on access, except the university`s right to reproduce the thesis only for preservation purposes.*

_____ (*signature*)

04.01.2023.

TalTech School of Engineering

THESIS TASK

Student: Fanny Lamp, 193027EDTR
Study programme, EDTR17, Telematics and Smart Systems,
main speciality: Cyber Physical Systems
Supervisor(s): Rinaldo Rüütli, Engineer, 6204808; Karin Muoni, Lecturer, 6204814

Thesis topic:

Analysis of Possible 3D Printer Cybersecurity Vulnerabilities and Their Mitigation Solutions,

(in Estonian) Analüüs 3D printerite võimalikest küberturbe ohtudest ja neid leevendavatest meetmetest

Thesis main objectives:

1. Find cybersecurity vulnerabilities associated with 3D printers
2. Provide measures to mitigate the vulnerabilities associated with 3D printers
3. Conduct risk analysis on the found vulnerabilities

Thesis tasks and time schedule:

No	Task description	Deadline
1.	Choosing initial thesis topic	05.04.2022
2.	Finalising thesis topic and writing literature overview	25.09.2022
3.	Writing cybersecurity overview chapter	30.10.2022
4.	Writing security measures chapter	20.11.2022
5.	Conducting risk assessment	30.11.2022
6.	Writing introduction and summary	31.12.2022

Language: English **Deadline for submission of thesis:** 04.01.2023.

Student: Fanny Lamp

"...".....2023 /signature/

Supervisor: Rinaldo Rüütli

".....".....2023 /signature/

Supervisor: Karin Muoni

".....".....2023 /signature/

Head of study programme: Aime Ruus

"...".....2023 /signature/

1. INTRODUCTION **7**

2. CONCEPT OF 3D PRINTING **9**
2.1. What is 3D printing? 9
2.2. Applications of 3D printing 10
2.3. Methods of 3D printing 11

3. CYBERSECURITY IN 3D PRINTING. VULNERABILITIES **14**

OF 3D PRINTERS **14**
3.1. What is cybersecurity? 14
3.2. Application vulnerabilities in 3D printers 16
3.3. Network vulnerabilities in 3D printers 18
3.4. Cloud vulnerabilities in 3D printers 19
3.5. Endpoint vulnerabilities in 3D printers 22

4. MEASURES TO MITIGATE CYBERSECURITY VULNERABILITIES IN 3D PRINTERS 24
4.1. Application security measures 25
4.1.1 Improper user validation mitigation 25
4.1.2 Consequences of improper user validation 25
4.1.3 Access privileges exploitation mitigation 26
4.1.4 Consequences of access privileges exploitation 26
4.2. Network security measures 27
4.2.1 DoS attack mitigation 27
4.2.2 Consequences of DoS attack 28
4.2.3 Data non-encryption mitigation 28
4.2.4 Consequences of data non-encryption 29
4.2.5 Lack of authentication methods mitigation 29
4.2.6 Consequences of lack of authentication methods 30
4.2.7 Outdated patches mitigation 30
4.2.8 Consequences of outdated patches 30
4.3. Cloud security measures 31
4.3.1 Misconfiguration of cloud environment mitigation 32
4.3.2 Consequences of misconfiguration of cloud environment 32
4.3.3 Insufficient credential and access management mitigation 33
4.3.4 Consequences of insufficient credential and access management 34
4.3.5 Cloud environment disclosure to the public Internet mitigation 34
4.3.6 Consequences of cloud environment disclosure to the public Internet 35
4.3.7 System vulnerabilities mitigation 35
4.3.8 Consequences of system vulnerabilities 36
4.4. Endpoint security measures 36
4.4.1 Malware in 3D printers mitigation 37
4.4.2 Consequences of malware in 3D printers 37
4.4.3 Missing port authentication mitigation 37

4.4.4 Consequences of missing port authentication 38

5. 3D PRINTERS VULNERABILITIES RISK ASSESSMENT 39

6. CONCLUSION 48

7. KOKKUVÕTE 50

8. REFERENCES 52

1. INTRODUCTION

3D printers are mostly Internet connected devices. Internet connection makes them vulnerable to different kinds of threats spreading online called cybersecurity vulnerabilities. In recent years cybersecurity has become increasingly important due to the growing reliance on technology and the Internet, therefore it is crucial to establish proper security measures to protect devices and systems connected with the Internet.

As the cybersecurity field particularly in 3D printers is rather not a thoroughly researched topic, it was decided to conduct analysis on the possible cybersecurity vulnerabilities that 3D printers could face and propose mitigation solutions to the found vulnerabilities. While conducting research on the cybersecurity part regarding 3D printers, not a single research was found that could cover all the important cybersecurity aspects. A huge amount of articles have been written highlighting the importance of the cybersecurity of the 3D printers but only very few pieces covered the actual aspects to keep in mind when working with the printers. The majority of the researches briefly covered network security without going into any details and pointing to direct mitigation solutions. Therefore two conclusions were made. Firstly, due to the fact that the cybersecurity field in 3D printers is relatively new there has not been enough time to produce materials to cover the field. Secondly, since there is a lack of information on this topic, there is an actual need for a compound research to be put together which could cover all the important cybersecurity aspects together with their mitigation solutions. Pointing out only the cybersecurity vulnerabilities is not enough since it will leave the topic partly hanging. The real threats occur when there are no or only partially implemented security controls implemented.

Therefore, based on the above, this thesis has three main objectives. First, find possible cybersecurity vulnerabilities that 3D printers might have. Secondly, provide security measures to mitigate these vulnerabilities and thirdly evaluate the impact and risk of vulnerabilities on 3D printers.

This thesis has the following research questions:

- Why are network vulnerabilities considered to be the main threat category?
- Is applying firewalls enough for networked 3D printers to protect them from possible vulnerabilities?

- Why is it important to install 3D printer management software?
- What are the benefits of proper access management for 3D printers?

In the second chapter there is a general description of the concept of 3D printing. Statistics about 3D printers' is provided together with different applications and descriptions of the most common printing methods. This is an introductory chapter to give background of the 3D printer field.

The third chapter gives a description of cybersecurity vulnerabilities in 3D printers. This chapter is divided into four sub-categories, application, network, cloud and endpoint vulnerabilities, based on the types of cybersecurity this thesis focuses on. For each of the category vulnerabilities associated with 3D printers are provided.

In the fourth chapter security measures are proposed for the vulnerabilities described in the second chapter together with possible consequences on 3D printers. Security measures and consequences are highlighted for all four cybersecurity types.

The fifth chapter describes risk assessment conducted on the vulnerabilities found in chapter two. This chapter provides an impact and likelihood risk analysis matrix and provides the risk scores together with analysis for all provided vulnerabilities.

A qualitative research method has been used to reach the objectives and research questions of this thesis. All used resources are online publications and the majority of them are published within the past year. The proposed security measures are the author's own sole ideas and knowledge based on personal experience while using similar devices and the acquired knowledge from research papers.

2. CONCEPT OF 3D PRINTING

The following chapter provides an overview of the concept of 3D printing to get a better understanding of the field. This chapter provides descriptions about the 3D printing process, its applications and different methods in use.

2.1. What is 3D printing?

3D printing is a way of producing objects through an automated additive process where a product is created by building it up layer by layer using 3D printing methods (Carlo, 2021). In other words 3D printing is a manufacturing method to produce solid three dimensional materials from a digital Standard Triangle Language (STL) file format which is given as an input to a 3D printer (Almaliki, 2015). 3D printing is in its concept a method which uses Additive Manufacturing (AM) techniques to make 3D objects based on preceding designing process in specific software (Almaliki, 2015). A majority of 3D object designs are created by Computer Aided Design (CAD) software where an object is put together one layer after another once it makes up a consistent piece (Almaliki, 2015). After the design process, a file containing the layout of the object is uploaded to the 3D printer where the creation process is commenced (Yang et al, 2017).

3D printing is becoming an integral part of worldwide manufacturing (Errera, 2022). The global 3D printing market is predicted to triple in size by 2026 and reach the value of more than $44 billion (Perez, 2022). The industry is expected to grow at a compound annual growth rate of some 17 percent between 2020 and 2023, as shown in Figure 1 (Statista Research Department, 2022). Moreover, 55% of companies believe that 3D printing can simplify their logistics, transport and inventories by digitalising actual products instead of shipping them (Errera, 2022). 69% of the users think that the main benefit of 3D printers is the possibility to produce complex geometries, 52% think that the top benefit is fast iteration and 41% of the users think that customizability is the main advantage of the 3D printer (Kauppila, 2022). People are mainly using 3D printing for prototyping, producing end-user detailed parts or for personal interests and hobbies (Kauppila, 2022).

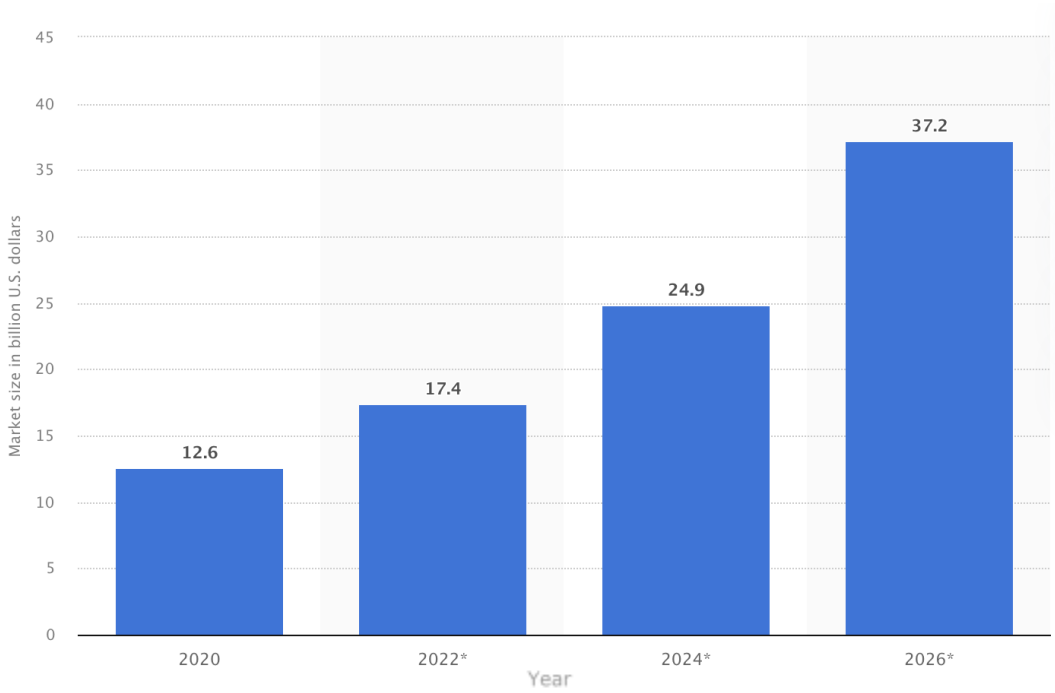

Figure 1. Global 3D printing market size from 2020 to 2026 (Statista Research Department, 2022).

2.2. Applications of 3D printing

3D printers came to widespread use in the beginning of 2000s making 3D printing accessible for everybody and created the possibility to produce an infinite number of applications across a vast range of industries. Before wider use these were mainly used by bigger corporations and major research universities due to the high cost. (Moore, 2022)

Nowadays the biggest industries using 3D printing are aerospace, medical devices and automotive where precision is in high demand (Thakar et al, 2022). 3D printing is considered to be the most flexible manufacturing solution on the market because of the ways the end result can be customised and personalised, the variety of materials that can be used, the texture that can be formed and the composition of the parts that can be created (TWI, 2022). With the help of 3D printing we can reduce the amount of manufacturing waste produced by creating cost efficient printer models and designing smart 3D objects (TWI, 2022).

2.3. Methods of 3D printing

There is a huge variety of 3D printing methods developed each serving different functionalities. Each method has its own application depending on the needs of the user. This thesis focuses on the following three major 3D printing methods: Stereolithography (SLA), Fused Deposition Modelling (FDM) and Selective Laser Sintering (SLS) (Alsop, 2021).

Firstly, Stereolithography (SLA) was the first 3D printing method ever created and it is still in use nowadays (Haines, 2022). SLA is widely in use in prototyping due to being relatively cheap in terms of production costs and consumes less time than other methods (3D Printing from scratch, 2015). The 3D object printing process starts with creating a 3D model in a Computer Aided Design (CAD) program where the object is built up layer by layer. The design file in .STL format is imported to the printer to start the printing process (All3DP, 2021). SLA printers involve an ultraviolet laser, scanning mirror, moving platform, liquid photopolymer, and bath container as shown in Figure 2. The light from the laser, which is usually ultraviolet (UV) light, connects molecular chains of the material and forms polymers which form a three-dimensional solid entity, is reflected from the scanning mirror directly to the built object according to the layer design (Thakar et al, 2022). The liquid polymer is solidified at its surface by exposure to UV light (Ambrosi and Pumera, 2016). The successive layers are created one after another by lowering the moving platform allowing fresh liquid resin to be exposed and excess resin to be drained and washed off (Ambrosi and Pumera, 2016).

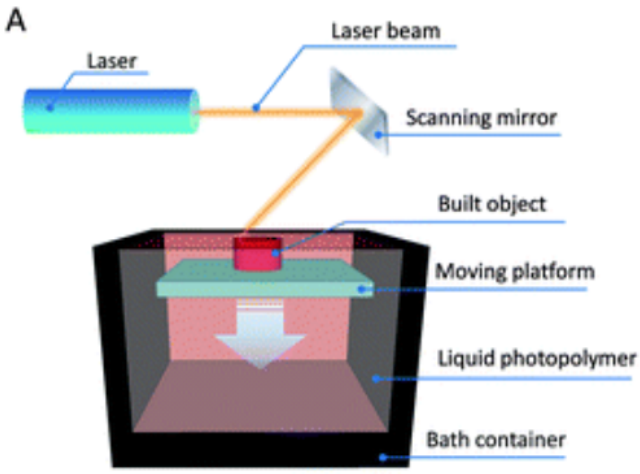

Figure 2. Illustration of SLA process (Ambrosi and Pumera, 2016).

The moving platform moves downwards until the desired 3D object is printed (Ambrosi and Pumera, 2016). In terms of printer software, the majority of the SLA printers operate in Windows operating system, have Ethernet and TCP/IP, USP port as their main network type and protocol (Ambrosi and Pumera, 2016).

Secondly, Selective Laser Sintering (SLS) is the second most used 3D printing technology (Alsop, 2021). By concept it is similar to the stereolithography technique, instead the liquid photopolymer as in the bath container of the SLA technique is replaced with powder (Ambrosi and Pumera, 2016). Therefore for the SLS technique only powdered materials can be used (Ambrosi and Pumera, 2016). SLS technology is used for powder-based materials to develop 3D objects in a matter of hours by applying a laser to fuse powder particles together (Godoi et al, 2016). A typical SLS printer consists of the following parts, as shown in Figure 3: a laser, scanning mirror, levelling roller, powder supply, powder bed, and build platform. Laser and hot-air beam as a heat source are directed onto the powder bed and fuse the powder particles together on specific areas of the powder bed according to the premade CAD model design using cross-section motion (Godoi et al, 2016). Once the layer is created, the levelling roller distributes another material layer on top of the previous layer onto the building platform and the previously described process starts again (Ambrosi and Pumera, 2016). The build platform is lowered until the desired object is created following the layer-after-layer structure (Ambrosi and Pumera, 2016). SLS printed objects do not require specific post-processing apart from removing excess powder from the powder bed therefore it is considered to be one of the fastest 3D printing technologies (Varvara et al, 2021). SLS printers mostly operate on Windows operating system and have Ethernet, Wi-fi and USB connectivity (Top3dshop, 2022).

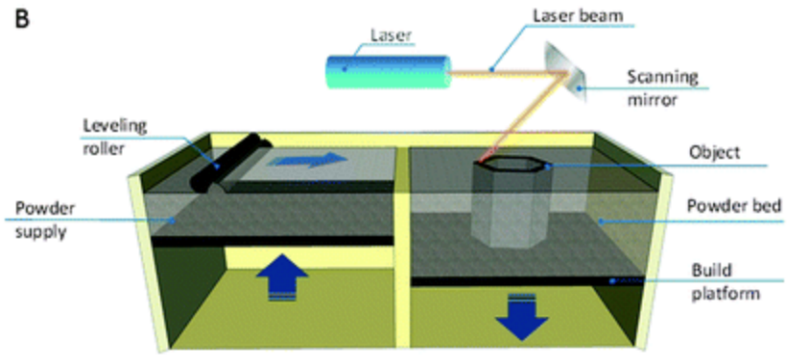

Figure 3. Illustration of the SLS process where the object is created layer by layer onto the downward moving build platform (Ambrosi and Pumera, 2016).

Thirdly, Fused Deposition Modelling (FDM) is the most common and affordable 3D printing technology available on the market due to its simplicity and low operational costs (Ambrosi and Pumera, 2016). FDM is a technology to create 3D objects by depositing semi-molten materials layer-by-layer on top of each other (Ambrosi and Pumera, 2016). FDM is used to create 3D objects by depositing semi-liquid or viscous material through a moving nozzle with constant pressure using an automated piston to create desired layers (Pitayachaval et al, 2018). The nozzle head and movement controlled by a computer-aided manufacturing (CAM) software package and stepper motors move the extrusion head (Kun, 2016). Once printed layers are fused on top of each other one layer at a time from the bottom up on the support platform and material has solidified the object is ready, as shown in Figure 4 (Pereira et al, 2021). The way to solidify the material is either to increase or decrease the temperature of the substance that is being dosed on the support platform for the material to harden or cool down. (Wilms et al, 2021). The deposited material solidifies on top of the previous layer according to the layered model design which has been previously created by the CAD programme (Ambrosi and Pumera, 2016). One of the biggest advantages of FDM printers is having the cloud server feature (Pal, 2021). It is possible to give printing commands to printers thanks to the availability of printers being connected to the network (Pal, 2021). The majority of FDM printers operate on Windows operating system, and have both wired (TCP/IP and wireless-ready (IEEE 802.11 or WPA2-PSK) network connectivity possibilities (Stratasys, 2022).

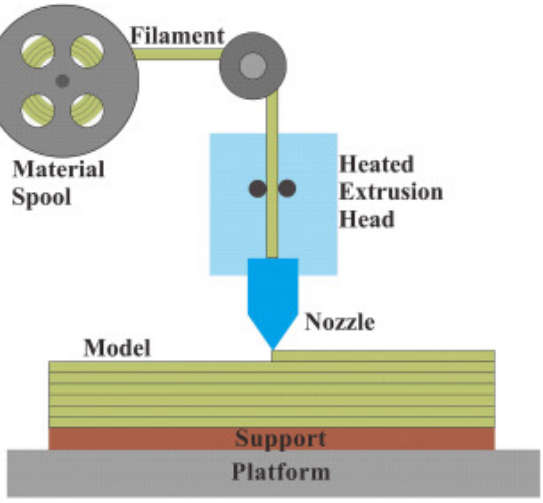

Figure 4. Illustration of the FDM process where the model is built on top of the support platform layer by layer (Zou et al, 2016).

3. CYBERSECURITY IN 3D PRINTING. VULNERABILITIES OF 3D PRINTERS

Each 3D printer has its own printing method and printing processes established according to the needs and requirements. In order to keep the printer healthy and ensure that the machine performs its job sustainably for a maximum amount of time, the user must think about the vulnerabilities and risks that may occur throughout the time and within the printing process. As stated in the previous chapter, 3D printers are mainly networked devices with Internet connection. Therefore they are susceptible to different kinds of vulnerabilities spreading online, which can have an impact on the performance of the 3D printing process and many other fields. The following chapter focuses on cybersecurity aspects of 3D printers and describes possible vulnerabilities related to 3D printers.

3.1. What is cybersecurity?

Cybersecurity is the practice to protect systems, networks and programs from digital attacks following the defence strategies that go along with the confidentiality, integrity and availability (CIA) triad, as illustrated in Figure 5 (Cisco, 2022). ”Confidentiality” in the CIA triad represents the idea of information being protected from not authorised access and uses (Chai, 2022). “Integrity” in the triad represents the idea of information not being modified or altered in any ways and the source of information is known and reliable (Chai, 2022). “Availability” stands for the idea of information being consistently available for all relevant parties (Chai, 2022). It is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, trainings, best practices, and technologies that can be used to protect the cyber environment (Craigen et al, 2014). The term “cyber” refers to everything associated with information technology (IT), more precisely with electronic communication networks and virtual reality (Craigen et al, 2014).

The term "security" refers to the concept of being free from danger of threat (Craigen et al, 2014). The aim of cyber attacks is to access, change, and destroy sensitive information that is stored on not publicly available locations or interrupt normal business hours (Craigen et al, 2014).

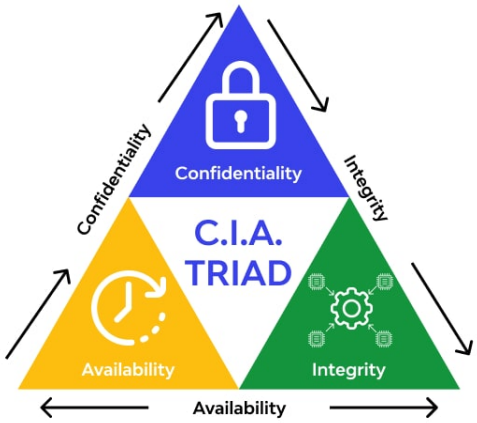

Figure 5. Illustration of the CIA triad components. Confidentiality in the CIA triad represents the protection of information from being accessed by unauthorised parties. Integrity represents the authenticity of the information, meaning that information should not be altered and the source of information is genuine. Availability represents the availableness of information to authorised parties at all times (Zuziak, 2020).

Cybersecurity has various different categorisations but this thesis focuses on the four primary types. These types are: application security, network security, cloud security, and endpoint security (Shea, 2022). Application security refers to addressing vulnerabilities from the software development process (IT Governance, 2022). Network security includes addressing network architecture which involves servers and hosts, firewalls, wireless access points, and network protocols protected with proper access management systems (IT Governance, 2022). Cloud security includes protective mechanisms for securing data, applications, and infrastructure in the cloud such as encryption of data assets, proper cloud access controls and strong compliance implementation (Checkpoint, 2022). Endpoint security refers to the end-user physical devices with data and network security controls (Checkpoint, 2022). The most common cybersecurity threats are malware, ransomware, phishing attacks, and social engineering (Fichtner, 2022). Additionally to having comprehensive plans in place for the above-mentioned four types, there should also be proper postures for people, processes, and technology as well in order to have a strong cybersecurity base determined (Fichtner, 2022).

Cybersecurity can be often confused with information security but in scope these are completely different. As described above, cybersecurity focuses on protecting systems,

networks, and programs from unauthorised accesses or being damaged in any other ways whereas information security focuses on protecting all information assets in general no matter if it is in a hard or digital copy (IT Governance, 2022). Therefore, the scope of information security is much broader.

3.2. Application vulnerabilities in 3D printers

Application regarding 3D printers is the software used inside the printer and the design software which is used to create the models. The majority of cyber attacks today still occur as a result of exploiting software vulnerabilities caused by software bugs and design flaws (Jang-Jaccard and Nepal, 2014). A bug in the software causes the system to behave unintendedly and in ways different from expected (Jang-Jaccard and Nepal, 2014). The following chapter describes the most common application vulnerabilities for 3D printers.

This thesis deals with two types of software, the design software and the software inside the printer. The design software used for model creation is typically CAD software, for example AutoCAD, Google SketchUp, and Blender (Hoffman, 2020) downloaded from the Internet. The software, which is used to control the printer and translate the models into understandable instructions for printers, usually is either supplied on disk or available for download online as a package (Hoffman, 2020) such as Simplify3D (Simplify3D, 2022).

Poor coding practices can be considered the result of many software vulnerabilities (Moore et al, 2016). Application vulnerabilities can be classified into the following different categories: user input validation exploitation and access privileges exploitation (Hoffman, 2020), as shown in Figure 6.

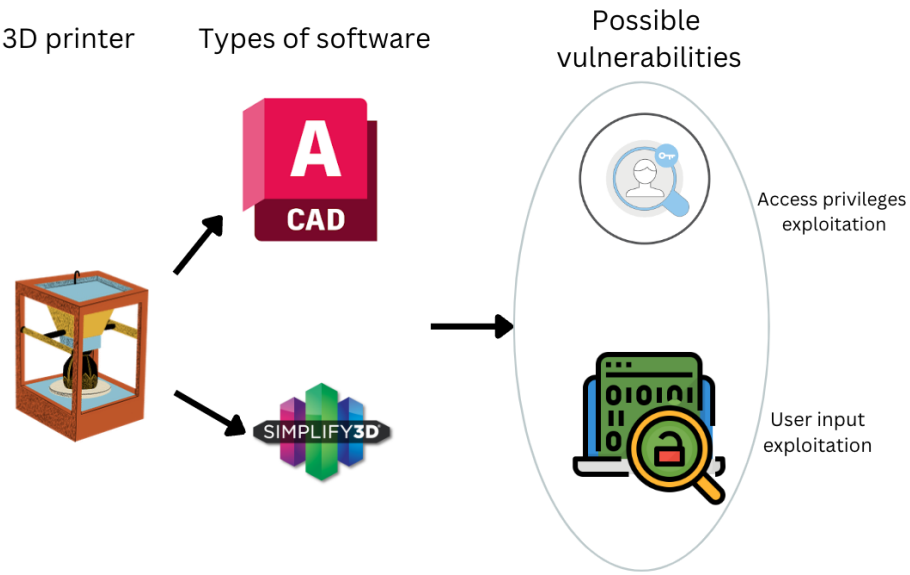

Figure 6. Summary of the application vulnerabilities applying to both the model creating software like CAD and the software that is used to control the 3D printer like Simplify3D.

Firstly, in case of user input validation the attacker is manually trying to enter harmful inputs to the normal user input field with the intention to decrease the system's performance (Fitzgibbons, 2019). One of the most common input validation attacks is cross-site scripting (XSS) where a suspicious website link is placed alongside a valid link without the user being unable to detect or distinguish between the legitimate and malicious link (GeeksforGeeks, 2022). For XSS attack attackers inject scripts with malicious code embedded into them to trusted websites with an aim to hijack user sessions, deface websites or redirect users to malicious sites (Kaur and Kaur, 2014).

Secondly, in case of access privileges exploitation in software the user gets elevated access to the resources that normally are protected from the user. As a result of the privileged access, the user has the ability to perform unauthorised actions inside the application such as modifying the source code and changing the configurations. (Hoffman, 2020)

3.3. Network vulnerabilities in 3D printers

Network in this thesis is considered to be the wireless connectivity of 3D printers. Networked 3D printers are an emerging trend in manufacturing (Perez, 2022) but unfortunately many such printers lack proper security controls leaving the door open for attackers to cause cybersecurity incidents and perform destructive actions on the printer in general (Alley, 2022). Denial of service attacks, the transcription of unencrypted data, wrong authentication configurations and outdated patches - in general these are the types of network security vulnerabilities that 3D printers are nowadays facing, as shown in Figure 7 (McCormack et al, 2020). The following chapter focuses on network vulnerabilities 3D printers face.

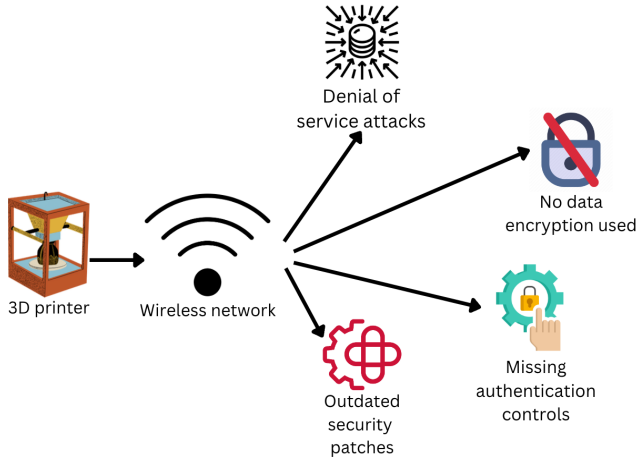

Figure 7. Summary of 3D printer network vulnerabilities. These kinds of vulnerabilities affect 3D printers due to the Internet connection the machines have.

First of all, 3D printers are susceptible to simple and low-rate denial of service (DoS) attacks due to the fact that most networked 3D printers have a small number of concurrent clients. This state helps the attacker create temporary DoS conditions with minimal effort. (McCormack et al, 2020)

Secondly, most 3D printers do not use data encryption when in transit (Ahmed, 2022). This means that data that is sent to and out of the printer is unencrypted and potentially available for the attacker to view (Ahmed, 2022).

Thirdly, there is no proper control implemented on how 3D printers can authenticate themselves to users. Printers will usually provide their hostname and Internet Protocol (IP) address to the user / personal computer (PC) for authentication but since the PC can only utilise the first reply it receives it will be possible for the attacker to impersonate the printer. This can be done when listening to the TCP socket to spoof the 3D printer and the printer command will be sent to the attacker instead. (McCormack et al, 2020)

Fourthly, 3D printers can have unused or not up to date network services in use vulnerable to known exploits, social engineering attacks and malware. This is a result of not having the latest Operating System (OS) patch installed, broadcast protocols are used without authentication and so on. (McCormack et al, 2020)

Lastly, 3D printers can be easily accessible on the public network when configured wrongly. This vulnerability comes purely down to the awareness of the person behind the printing machine as they will be the ones operating the machine. (McCormack et al, 2020).

3.4. Cloud vulnerabilities in 3D printers

Cloud in 3D printers refers to the cloud environment in which the project files are stored. There is always a possibility to store necessary files locally in a computer as well but the trend is towards moving the physical storage to the cloud environment (Wasabi, 2023). Therefore this thesis focuses on cloud file storing possibilities. It is up to the project owner to decide whether they want to store the files in public, private, community or hybrid cloud. (Mushtaq et al, 2017)

The following chapter focuses on the vulnerabilities like misconfiguration of cloud environment, insufficient credential and access management, cloud environment disclosure to the public Internet and system vulnerabilities as shown in Figure 8, of each cloud type.

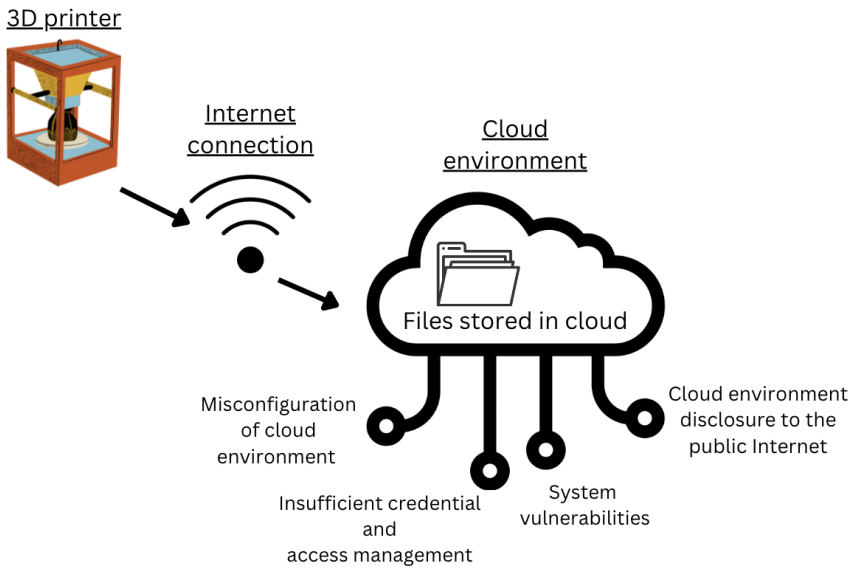

Figure 8. Summary of 3d printer cloud vulnerabilities. As the majority of 3D printers have the Internet connection, it is possible to upload the files to the cloud environment. Cloud vulnerabilities affect the files stored in the cloud environment.

Cloud is a set of hosted servers along with the applications that run on it and which are accessible over the Internet (Kumar, 2020). Inside the cloud there are four different cloud deployment models: public cloud, private cloud, community cloud and hybrid cloud, as shown in Figure 9 (Pandey, 2019). The description of each cloud deployment model follows after the visualisation.

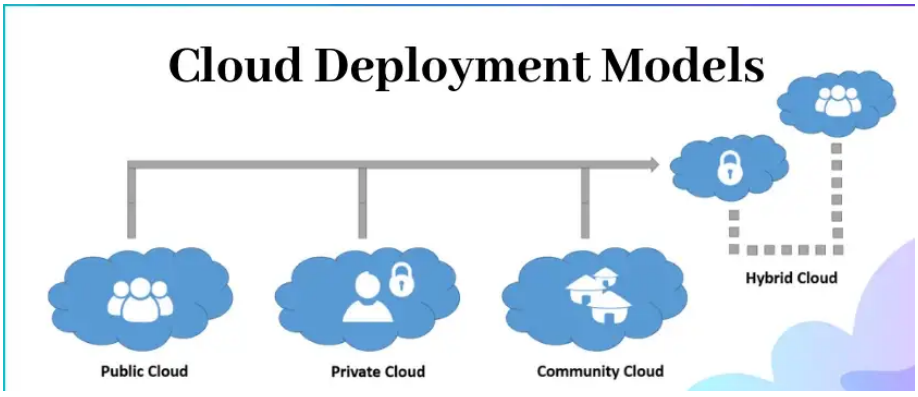

Figure 9. Visualisation of different cloud deployment models which are public, private, community and hybrid cloud. (Manrai, 2020).

Public cloud is a third party hosted service that may have several servers and data centres (Kumar, 2020). All resources stored in the public cloud are publicly available therefore hard to protect from cyber attacks (Mushtaq et al, 2017). Private cloud is managed and maintained by a single user who can set up the infrastructure on their own (Mushtaq et al, 2017). Community cloud is a shared cloud between users having similar interests or concerns like policy, security requirements, mission or compliance requirements (Neenan and Bigelow, 2021). This type of cloud is rather meant for a specialised group of users with very common interests that work together towards the same goal (Mushtaq et al, 2017). Hybrid cloud is a combination of private and public clouds meaning that it creates the flexibility to operate both on-premises and in public cloud resources giving the user better cost management and compliance options (Neenan and Bigelow, 2021).

Cloud services are offered to users by third party Cloud Service Providers (CSP) (Eliacik, 2022). The most popular CSPs are Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) (Zhang, 2022). Therefore, it is the shared responsibility between the user and the CSP to assure that there are no vulnerabilities in the cloud environment (Eliacik, 2022).

Firstly, the vulnerability that potentially has the biggest consequences is misconfiguration of the cloud environment. If there is a lack of access restrictions, an attacker can access data stored in the cloud and download sensitive project files, make adjustments to the files or completely destroy them. Moreover, faulty misconfiguration can lead to extensive data breach, regulatory fines and other penalties. (Eliacik, 2022)

Secondly, insufficient credential and access management is considered to be the next crucial vulnerability in cloud environments (Mello Jr., 2022). Therefore it is simpler for attackers to gain unauthorised access to the cloud based environment when there are proper authorisation controls lacking (Eliacik, 2022).

Thirdly, cloud environments are usually disclosed to the public Internet which means that everyone who wishes can access the environment easier than when it is in controlled on-premise infrastructure (Eliacik, 2022).

Fourthly, due to the fast pace and need to adapt with the business needs it is often forgotten how important it is to pay attention to the cloud technical implementation and

security considerations. The lack of architecture design can result in system failures or data breaches such as ransomware attack or data breach. (Eliacik, 2022)

Lastly, system vulnerabilities in cloud environments are the flaws that can compromise the CIA of data stored in the cloud. These vulnerabilities are zero days, missing or not up to date patches, servers run on outdated software, default settings and credentials which all are easily obtainable and crackable for the attackers. (Mello Jr., 2022)

3.5. Endpoint vulnerabilities in 3D printers

Endpoint regarding 3D printers refer to physical printers themselves. Based on the published materials there is little or partially no information available about the physical printer cybersecurity vulnerabilities. The possible reason could be that the majority of the vulnerabilities are technology based and most likely protected with trade secrets. Malware and missing proper port authentication methods are the main vulnerabilities in the endpoint category, as shown in Figure 10.

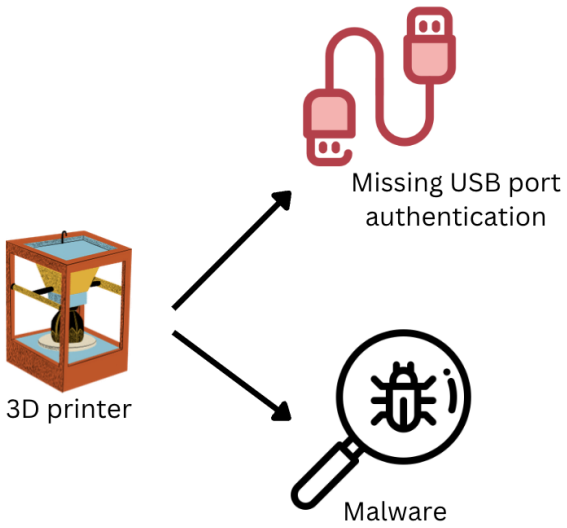

Figure 10. Summary of 3d printer endpoint vulnerabilities. These vulnerabilities have a direct impact on the device.

3D printers are cyber devices which means they are subject to the same vulnerabilities that imperil other networked devices (Liotine, 2018). These vulnerabilities can be intrusions, virus infections, trojans, denial of service attacks, malware and other cyber threats, as

shown in Figure 10, which are usually a result of out-of-date antivirus software or operating system. (Liotine, 2018). Many endpoints usually lack security agents as well which will monitor network traffic, control patch updates and make sure endpoints are healthy (Cook, 2007).

In addition, 3D printers have USB port connection possibility and this means that everyone can connect any kind of medium or drive or device into the printer and compromise the machine (Cook, 2007).

4. MEASURES TO MITIGATE CYBERSECURITY VULNERABILITIES IN 3D PRINTERS

Based on the literature overview it can be concluded that there are four major types of vulnerabilities that pose a threat to 3D printers. As seen in Figure 11 the vulnerabilities are application, network, cloud, and endpoint vulnerabilities. The aim of this chapter is to give possible mitigation solutions to the above-mentioned security vulnerability domains.

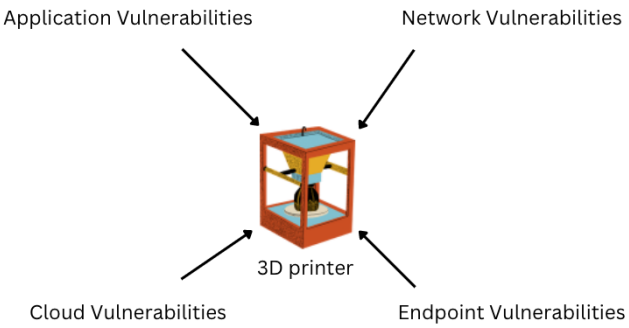

Figure 11. Illustration of the posing threats to 3D printers which are categorised into four main types: application, network, cloud and endpoint vulnerabilities.

The proposed mitigation solutions address the vulnerabilities covered in paragraphs 3.2-3.5 keeping in mind the cybersecurity basics covered in paragraph 3.1 and the 3D printing methods covered in paragraph 2.3. In addition, this chapter outlines the consequences regarding 3D printers and its printing methods that may come along when the vulnerabilities are not properly mitigated. Based on the cause of the vulnerability, all vulnerabilities are divided into three different categories: targeted attack by the hacker, untargeted attack or attack that happened as a result of the printer user lacking enough skills or knowledge. Moreover, risk analysis on the vulnerabilities, their mitigations and consequences stated in paragraphs 3.2-4.4 is performed. Separate analysis can be found in chapter 5 which helps to evaluate the impact and risks associated with each vulnerability.

4.1. Application security measures

Application, as stated in chapter 3.2, refers to both the software used locally inside the 3D printers and the design software that can be downloaded from the Internet. Both software in this thesis are seen as software which is installed from the Internet to a local machine. In majority of the researches the term "application" refers to the software part of the whole system therefore the two above-mentioned software were included in the following chapter.

As mentioned above, both the printer management software and the design software can be downloaded from the internet (to be noted that some printer software still come on disk drive) they still serve different purposes in the whole printing process. Therefore, in this chapter, separate mitigation solutions for both software based on the vulnerabilities described in chapter 3.2 are provided. These vulnerabilities are categorised into two: improper user validation and access privileges exploitation.

4.1.1 Improper user validation mitigation

The first vulnerability category is improper user validation. In order to get the printer and design software locally installed to devices the user must download these from a website first. These websites are the places where improper user validation attacks usually take place. To mitigate falling victim to XSS attacks the user should check that the website hyperlink begins with HTTPS not HTTP. Websites which addresses begin with HTTP usually have less protection as the data is not encrypted. Whereas HTTPS provides an extra layer of security between the browser and the website offering encryption for data in-transit. In addition, the user should ensure that the webpage is legitimate by checking possible grammar mistakes, validating website domain and scanning the website with a scan engine such as Virustotal.

4.1.2 Consequences of improper user validation

As a consequence of improper user validation the user might be directed to a completely different website which looks similar to the initial one but actually has malicious content. This is dangerous particularly in this case when the user wants to download printer or design software and hopes to install it from a reliable source. Instead the user is directed to

another webpage mimicking the original page but which actually contains infected files instead of the verified CAD and printer software files. The infected files can contain malware which infects and corrupts either the 3D printer or device used for designing purposes. Therefore, the 3D printer and the computer for design software might suffer from malfunctioning or refuse to work at all, depending on the planted malware inside the file. This kind of vulnerability goes against the availability component of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge or it is a targeted attack by the hacker.

4.1.3 Access privileges exploitation mitigation

The second vulnerability category is access privileges exploitation. To mitigate access privileges exploitation in the printer management and design software several mitigation solutions can be taken into use. Both above-mentioned software should be stored in an environment with strong access controls. These controls should follow the least privilege and need-to-know principles which state that only relevant people with relevant needs get access to the source. This also prevents the situation of users having privileged accesses without certain reason. Privileged access means that the user has more rights and authority to perform security related functions and change configurations. The fewer there are people who can possibly cause changes to the software the lower is the likelihood of unauthorised actions happening inside the application. In addition, the users who are given privileged access should be audited periodically. This ensures the necessity of elevated access and decreases the threat vector.

4.1.4 Consequences of access privileges exploitation

If the user starts exploiting the given accesses and gets privileged access to printer software, then the biggest consequences can result in erroneous printer behaviour. The user can make modifications to the printer software source code which makes the 3D printer behave differently from the expected. For example, in case of stereolithography or selective laser sintering methods, the source code can be modified so that the laser beam width is not sufficient to fuse the material particles together on the build platform which means that the printed object fails in structure and does not form a compound object. In case of access privileges exploitation in the design software this could result in failures using the software. Such failures can be lack of functionalities, improper design environment setup or decreased

performance or the software in general. This kind of vulnerability goes against the integrity component of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.2. Network security measures

Almost all 3D printers nowadays are connected to the Internet making the printers vulnerable to all sorts of different threats online. As cybersecurity mainly focuses on the non physical and virtual part of the reality, network security issues can be considered as one of the main vulnerability types in this thesis. The actuality and importance of this topic is also reflected in the amount of materials published. Out of all the other vulnerability types covered in this thesis, the network vulnerability field has received remarkably more attention than the other three types such as application, cloud and endpoint vulnerabilities, if any.

Network vulnerabilities can be divided into four main categories: DoS attacks, data not being encrypted in transit, missing authentication and outdated patches. In this section possible mitigation solutions to these vulnerability categories are provided.

4.2.1 DoS attack mitigation

The first vulnerability category is DoS attacks. As a first step to avoid such attacks is to understand what the threat vectors are and what the possible weaknesses of the configured network setup be. It is important to know what kind of assets in the network might have public appearance, for example a server or a router that the printer is connected to, what are the public Internet Protocol (IP) addresses which could be used as an attack against the network. The more publicly available information there can be found online about the network, the more susceptible the printers are to falling under an attack connected to the network. That is why it is important to invest some money in buying a proper router which has the option to adjust the bandwidth when needed. In addition, it is crucial to invest time in configuring the router and setting up a firewall. It will only let through the traffic which has been established by the firewall rules beforehand leaving the door closed for the attackers to exploit the systems and the printers connected to the network. Additionally, the

less public IP addresses for printers there are available the less attractive printers look for the attackers. Apart from the manual work and configurations that can be done, the network administrators can also set up an alerting system which could inform the users about possible attacks. Depending on the available resources it is also possible to buy a separate intrusion detection system (IDS) which will help to detect unusual network traffic. An example of an IDS is Snort (Snort, 2022).

4.2.2 Consequences of DoS attack

DoS attack is considered to be one of the major threats according to the research published by Carnegie Mellon University (McCormack et al, 2020). Once the network of the 3D printer gets attacked, the printer is most likely not able to perform any kind of activity since the system is compromised. Imagine that the printer operator wants to create an object using the FDM method which requires semi-liquid or viscous material to be deposited through the nozzle. If the printer is not working properly, the material that is fused onto the support platform will not be solidified and as a result the desired object is not properly printed. Now if we add a time constraint to this process as well and imagine that we have agreed on a Service Level Agreement (SLA) our printer should operate within, the effect of a DoS attack on the general process flow is quite extensive. The DoS attack also goes against one of the CIA triad components which is availability. The cause of such vulnerability most likely is a result of a targeted attack by an attacker.

4.2.3 Data non-encryption mitigation

The second vulnerability category is the transcription of unencrypted data. By this is meant that the majority of the information which is either sent out or to the 3D printers is not encrypted and can be possibly available for the attacker. This information can be for example printing files and printer configuration logs. This also means that the attacker has gained access to the network where the printer is connected to but following the proposals described in the DoS mitigation paragraph the chances should be minimised. The most common practice for this kind of deficit in data protection is to implement encryption both for data in transit and at rest. It means that the information sent to the printer while being in the movement is fully encrypted using a strong encryption method, for example

Advanced Encryption Standard (AES). Together with selecting the encryption method comes the need to have a proper key management system in place as well. The same applies for the information stored at rest in the printer. Encryption decreases the likelihood for the attackers to get access to the context stored inside the documents because it takes more time and effort for them to crack the encryption algorithm than to plainly view the information stored there.

4.2.4 Consequences of data non-encryption

If the data is not encrypted, imagine it is a design file shared between the 3D printer and the laptop and used to print the desired 3D object, the attacker could easily make adjustments, for example redesign the object or what is even worse, delete the design completely. The attacker could also steal the design file while being sent to the printer meaning the desired object never gets printed. Once the attacker has gained access to the information shared in transit, he could share this kind of information to a wider audience as well which can result in intellectual property theft. This is a violation of confidentiality and integrity components of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.2.5 Lack of authentication methods mitigation

The third vulnerability category is missing authentication configuration. In order to improve the authentication between the printer and the user computer, additional measures besides the currently existing hostname and IP address sent to the PC from the printer should be implemented. Without proper authentication the user could communicate with any other printer connected to the same network without having control what kind of files have been shared with the printer, what is the status of the printing process and so on. In addition, without proper authentication controls it is possible for the attacker to impersonate the printer and relevant information will be sent to the attacker instead. As a solution it would be possible to implement only private and fixed IP ranges where the 3D printers could operate. These fixed IPs or IP whitelist should be used together with VPN accompanied with Two-Factor Authentication (2FA) as it will be easy for the attackers to guess the range. VPN

helps to redirect and hide the fixed IPs so that the user can conveniently continue using the static IPs.

4.2.6 Consequences of lack of authentication methods

Lack of authentication methods can lead to unauthorised users accessing and performing actions with 3D printers connected to the same network. The attackers could act as impersonators of the real printers while at the same time stealing information related to printing process, commands, design files and used materials. The divulgement of this kind of information could result in intellectual property theft of the original owner. In case such vulnerability is not mitigated this is a violation of the CIA triad confidentiality component. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.2.7 Outdated patches mitigation

The fourth vulnerability category is outdated patches in 3D printers. This mainly applies to locally installed printer software. With each new patch or update the software receives improvements to the security and technical aspects. Missing a software update means increasing the likelihood of being vulnerable to different kinds of attacks, malware and exploits which spread through the network. The above-mentioned issues could be solved using some sort of central management system that could automatically check and enforce updates to the software. Another option is to have periodic audits on the software. Throughout the audit the user manually reviews necessary versions of the software and applies patches when a new version of the software is available from the software managing company.

4.2.8 Consequences of outdated patches

According to the research published by the Web Security team, 80% of the breaches could have been prevented if the software used in devices had been up to date (Digicert, 2021). Outdated patches could leave the door open for the attackers to exploit the printer from the

network side. The not patched software would cause the printer to be exploitable for different malware, such as worms or viruses, or have an affect on the performance of the 3D printer in general. Each new update contains an upgrade from the previous version which in majority of the cases includes fixes in bugs related to printer performance such as possible lags in printing process or some parts of the printer not moving as they supposed to. In case outdated patches are not mitigated this is a violation of the availability component of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.3. Cloud security measures

Cloud environment plays a crucial role in the 3D printing process. There needs to be a place where the 3D printed design files are managed and stored. Taking into consideration the emerging trend to move the storage of the physical drivers to the cloud environment, it was decided to include the cloud storage option into this thesis as well (Kim, 2021). Therefore the existence of a cloud environment can be considered as an essential part of the whole process. Without such an environment, the user may have the physical printer which performs the work but it does not have the necessary input to base its work on.

There are four different cloud environment vulnerabilities this chapter tries to propose solutions for. The vulnerabilities are: misconfiguration of cloud environment, insufficient credential and access management, cloud environment disclosure to public, Internet and system vulnerabilities in general. The chapter focuses on providing possible mitigation solutions for all four cloud types stated in chapter 3.4.

As the cloud services are mostly offered to users by third party CSPs, it is the mutual responsibility between the user and service providers to tend the configuration and security aspects. As the cloud environment users cannot have control over the CSP because they are the ones buying services from the providers, this thesis focuses on the possible mitigation solutions from the 3D printer user’s side.

4.3.1 Misconfiguration of cloud environment mitigation

First vulnerability category is misconfiguration of the cloud environment. It should be the user's responsibility to conduct periodic risk assessments and have a proper disaster management plan together with disaster recovery plan (DRP) in place in case the cloud service is malfunctioning or refuses to work at all. First of all, risk assessment helps to map the possible shortcomings and risks that may come along when using the cloud service as file storage. The disaster management plan puts in place the processes in case the risk actually occurs and helps to behave accordingly to the risks pointed out in the risk assessment. The DRP includes the instructions and action items to be taken after the accident or attack has been realised on the cloud environment. Developing these three components for cloud environments help to get an understanding of posing risks to the storage environment and prepare appropriate action items in case disaster occurs. Having an understanding of the possible vulnerabilities that can pose a threat to the cloud environment helps to better understand the threat vector as well. The risk assessment and both disaster management and recovery plans should be tested on a regular basis to ensure its suitability and relevance in terms of proper storage management. The abovementioned applies to all four cloud deployment models, no matter whether it is a public, private, hybrid, or community cloud therefore there is no point to make separate distinctions for each type.

4.3.2 Consequences of misconfiguration of cloud environment

Misconfiguration of cloud environment can have widespread consequences mostly affecting the printer files stored in the cloud. The files stored in the cloud can be either modified, copied, replaced, or deleted. In case the files are modified the attacker could for example change the layer-by-layer design so that the final object results in having no inner structure and does not stick together at all. What is even worse, if the file contains a design about some sort of medical product, for example prosthetic or dental product, then even a small change in the overall design means failures in usage when the object is put into use in the human body. In case of copying the design file, this can result in intellectual property theft if the user of the copied files has not referred to the initial source. For such a scenario the design files owner must understand that he cannot claim the ownership of these files solely to himself and cannot call the designs a unique creation anymore. In case the file is

replaced, the usual design format is .STL but the attacker can displace it with a completely different format unrecognisable for the 3D printer. In case of file deletion the design files are erased from the cloud environment leaving no materials to be sent to the printer and the user has to start creating the files from scratch. In case of no backup created of these files either the user either spends loads of work hours to recreate the files or in worst case close down the business. In case such misconfiguration is not mitigated, this is a violation of the confidentiality and integrity of the CIA triad components. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.3.3 Insufficient credential and access management mitigation

Second vulnerability category is insufficient credential and access management. Lack of proper credential and access management controls can be considered as the next crucial threat to the cloud environment. If anyone were able to access the environment without any kind of restrictions in place the content inside the cloud environment would be left unmanaged. This leaves the doors open for people with bad intentions to perform violations on everything that is stored in the cloud. Having in place strict access controls such as Single sign-on (SSO) which enable the users to authenticate themselves using just one set of credentials to access several websites or 2FA for multi layer authentication, will decrease the likelihood of unauthorised people getting access to the cloud environment without proper authentication. In case of 2FA the user is usually required to enter the username and password combination which is accompanied with an extra layer of security, which in most cases is a security token or some other kind of biometric scan to ensure the person's authenticity. When logging in to the cloud environment console either the SSO or 2FA sign-on methods are recommended for authentication. As to keeping the sign-on credentials, the best practice is to use a credential management system or password manager which stores sensitive login credentials securely in encrypted format inside the application or browser extension. Examples of password managers are LastPass and Dashlane (Kurko, 2022). The abovementioned applies to all four cloud deployment models because in order to access each of the cloud types the user must pass the authentication successfully.

4.3.4 Consequences of insufficient credential and access management

Insufficient credential and access management has similar consequences to the misconfiguration of the cloud environment. Lack of credential and access management can be considered as a part of the misconfiguration which results in unauthorised access to the environment console. This could mean either making changes, copying or deleting the design files stored in the cloud or the attacker could change the current login credential in a way that the real users of the files are not able to access the environment at all. This means that the cloud environment has been fully exploited by third party attackers making it unavailable for the actual authorised users. In case proper credential and access management controls are not put in place, this is a violation of all the components of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.3.5 Cloud environment disclosure to the public Internet mitigation

Third vulnerability category is cloud environment disclosure to the public Internet. The fact that cloud environments are disclosed to the public Internet can happen as a result of the user misconfiguration of the cloud environment or the actual intention of the user. As described in chapter 3.4 the public cloud format makes the resources stored in such an environment accessible for everyone but the access and authentication still relies on the cloud environment owner itself. Security measures this chapter proposes are meant in case the environment has been left intentionally disclosed to the public.

First of all, it is important to define what kind of files users want to store in the cloud, whether these files are general design files that could be used by other people as well or rather meant for a small group of people in private. In case of sensitive files, instead of choosing a public cloud for file storage, the user should either think about private or community cloud. In a private cloud the user can fully define the environment himself, control the accesses and configure the security aspects. In a community cloud the user can collaborate with users having similar interests which makes file sharing much easier and more manageable between groups. In both ways the environment is not publicly available, if

no misconfiguration has been made in the setup, and the users do not have to be worried about the content of the cloud environment being available to the rest of the world.

In case there is a need to use the public cloud, mainly for cost saving and scalability reasons as the cloud is a shared environment, the user should consider accessing the cloud via Virtual Private Network connection (VPN). VPN establishes a secure connection between the user's host and the server the user is connecting to by rerouting the network traffic and leaving no trace behind to track the user. This makes it harder for the attacker to track down the user's path to the cloud environment and access the cloud himself.

4.3.6 Consequences of cloud environment disclosure to the public Internet

Cloud environment disclosure to the public Internet can have several consequences. Firstly, if the cloud environment is intended to be private but it accidentally is configured to be public, then this could have a huge impact on the confidentiality of the stored files. If files, for example containing sensitive information about specific material type or characteristics particular to each layer of the object, are disclosed to the public unintendedly this could be considered a breach of delicate information. Secondly, when the environment is disclosed to the public, it is an easy target for the attackers to exploit. Examples of such exploits can be DoS attack, unauthorised authentication to the environment, and XSS attacks. The exploits described can result in making the files stored in the cloud temporarily or depending on the attack surface permanently unavailable for the printer user. In case a cloud environment is unintentionally disclosed to the public, this is a violation of the confidentiality and integrity of the CIA triad whereas when the environment is intentionally kept as public the violation of all the CIA triad components can possibly be considered. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.3.7 System vulnerabilities mitigation

Fourth vulnerability category is system vulnerabilities. System vulnerabilities are mainly related to the software of the CSP servers which provide the cloud environment service. It is

the responsibility of CSP to keep the servers up to date with latest patches, ensure servers run on updated software, default settings and credentials are changed and no zero-day vulnerabilities are left unpatched. As there are several cloud service providers it is up to the user to choose the most reliable option. The more accredited and specialised the CSP is the more likely the company puts emphasis on the security aspects covered above. If it is a reliable CSP the company usually publishes materials related to patching frequency, software updates and credential management publicly available online or these can be reviewed upon request. Based on the user's knowledge base and adequacy to assess the available information, a suitable provider should be chosen. The abovementioned applies to all four cloud deployment types.

4.3.8 Consequences of system vulnerabilities

System vulnerabilities can cause several consequences for the cloud services users. Such consequences can be for example the users not being able to access the cloud environment or unknown file operations due to outdated patches and software making the servers vulnerable to distributed malware such as worms, trojans, and viruses. This can result in the modification or deletion of files or the user is not able to access the files at all. This poses a great threat to the sustainability of the storage location and the documents stored there. In case system vulnerabilities might occur, depending on the scope, these can violate all the components of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.4. Endpoint security measures

Endpoint security measures refer to the controls taken regarding physical 3D printers and to secure its working operations. On one side of the 3D printer there are the physical parts or the hardware of the printer such as laser, nozzle and build platform but on the other side there is the printer system software which manages both the hardware and software associated with printers. In other words it is the Windows OS as described in chapter 2.2. This chapter focuses primarily on the operating system software security measures inside the printer which can be taken to avoid the vulnerabilities described in chapter 3.5.

4.4.1 Malware in 3D printers mitigation

First vulnerability category is malware. In order to prevent malware infecting the 3D printers several precautions can be taken. As the printers are networked objects they could be connected to one central device management system which makes it easier for the user to monitor the health of the printers and manage the updates. The proposed solution should be something similar to the Avalanche Printer Management service offered by Ivanti which gives the user the ability to manage all deployed printers across the network and different locations (Ivanti, 2020). This service is mainly focused on printer troubleshooting and configuration, therefore it is possible to get insight into printer system software versions. The more outdated the software is, the more likely the printer is vulnerable to different kinds of malware. The tool offers users the ability to centrally force upgrades and therefore keep the printers in the system continuously up to date. While being physically near the 3D printer, it is also important to ensure that only authorised users could get access to the device. Therefore a privileged access management (PAM) system should be in place which ensures that only the required number of people would get access to the 3D printer system. Enforcing PAM on 3D printers would decrease the likelihood of unauthenticated users getting access to the printer and distributing malware across the system.

4.4.2 Consequences of malware in 3D printers

Malware in the 3D printers can have an effect on the printer performance and therefore on the printed object. 3D printer performance may decrease meaning that the printing process might get slower, some steps from the printing process may be omitted, some printer parts may not be moving properly or stop moving at all, material may stop coming out from the nozzle or is pushed through the nozzle with wrong texture and other errors may occur. The exact consequence depends on the scope and type of a vulnerability therefore it is possible that these vulnerabilities can violate all the components of the CIA triad. The cause of such vulnerability most likely relies on the printer user and his lack of skills or knowledge.

4.4.3 Missing port authentication mitigation

Second vulnerability category is missing port authentication. Since it is hard to close or block the USB ports built into the 3D printer the mitigation can rely on the software. All files that are sent to the printer are beforehand scanned in the user’s laptop to detect malware.

3D printer users should use antivirus software such as Bitdefender Antivirus which scans all data such as print jobs and scans for potential malware and virus (Ctrl-print, 2022). The user can never be fully aware of the content stored in the USB drive connected to the 3D printer therefore if the software could initiate a scan for malicious files the printer would most likely not be affected by the malware or virus that was stored in the drive.

4.4.4 Consequences of missing port authentication

Missing port authentication can harm the 3D printer system with malware or virus by compromising the device. As a result the machine is most likely not able to perform any jobs or might malfunction in general. In case ports miss authentication this can be considered as violation of the availability component of the CIA triad. The cause of such vulnerability to occur is either targeted attack by the hacker or untargeted attack if the USB drive contains an unknown malicious file.

5. 3D PRINTERS VULNERABILITIES RISK ASSESSMENT

In order to get a better understanding of the impact the above-mentioned vulnerabilities may have on 3D printers and what could be the possible consequences, a risk assessment is conducted. Knowing all the vulnerabilities and their possible consequences makes it easier for the 3D printer user to mitigate or reduce the possible damage that may occur or it may help to prevent accidents from happening at all.

In this thesis a simple impact and likelihood risk assessment matrix is used which categorises all vulnerabilities into three different risk categories, "Low'', ''Medium" or ''High" based on the impact and likelihood scores given. As seen in Table 12 both Impact and Likelihood attributes are evaluated on scale one to five, where one having the lowest and five the highest impact or likelihood value. Impact and likelihood values are multiplied in a column named Risk score, according to Table 12. The higher the Risk score of the vulnerability the greater the risk for the 3D printer. According to the evaluated Risk score, Risk category is determined as follows: Risk category equals "Low" when Risk score is equal or lower than four, Risk category equals "Medium" when Risk score is equal or lower than 10 and bigger than five and Risk category equals "High" when Risk score is bigger than 10. For each of the vulnerabilities, mitigation solutions to decrease the risk as described in the last column of Table 12 are provided.

Table 12. Risk analysis matrix of 3D printer vulnerabilities.

Sequence	**Vulnerability type**	**Vulnerability**	**Impact of the vulnerability**	**Cause of the vulnerability**	**Impact** (1-5)	**Likelihood** (1-5)	**Risk score** (Impact * Likelihood)	**Risk category**	**Mitigation solutions to decrease the risk**
1	Application	Improper input validation	Corrupted 3D printer or device used for designing purposes decreases the possible amount of workload that can be done therefore having an impact on the availability of the 3D printer	Targeted attack by the hacker and printer user lacking enough skills or knowledge	5	2	10	Medium	Website hyperlink encryption (HTTPS), legitimacy of the website to be ensured, website scanning using scan engine
2		Access privileges exploitation	Behavioural problems with 3D printer and design software performance issues decrease the efficiency and	Printer user lacking enough skills or knowledge	2	2	4	Low	Enforced least privilege and need-to-know principles, periodic auditing of access rights

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
			have an impact on the integrity matters.						
3	Network	DoS attacks	Compromised 3D printer system makes it impossible to put the device into use therefore having an impact on the availability of the 3D printer.	Targeted attack by the hacker	5	5	25	High	Threat vector mapping, proper network setup which includes configuration of router and establishing firewall rules, alerting system set in place, IDS for unusual network traffic
4		Lack of data encryption	Accessing and modifying design files has an impact on confidentiality and integrity	Printer user lacking enough skills or knowledge	4	2	8	Medium	Enforced encryption for both data in rest and in transit, proper key management

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
			matters and can result in intellectual property theft.						system in place
5		Lack of printer authentication methods	Impersonation of 3D printers makes it possible to steal printer related information which has an impact on confidentiality matters.	Printer user lacking enough skills or knowledge	3	2	6	Medium	Implementation of only private and fixed IP ranges, IP whitelists, enforced VPN usage accompanied with 2FA
6		Outdated patches	Malware has an impact on the printer performance in general by making it behave differently from the	Printer user lacking enough skills or knowledge	4	3	12	High	Central management system for checking and managing updates to be enforced, conduct periodic audits

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
			expected. This will have an impact on the availability of the 3D printer.						on software
7	Cloud	Misconfiguration of cloud environment	Problems with design files confidentiality and integrity occur. Files can be modified, copied, replaced or deleted.	Printer user lacking enough skills or knowledge	4	2	8	Medium	Periodic risk assessments, proper disaster management plan and disaster recovery plan in place
8		Insufficient credential and access management	Problems with design files confidentiality and integrity occur. Files can be modified, copied, replaced or deleted. In addition, the	Printer user lacking enough skills or knowledge	4	2	8	Medium	Strict access controls in place such as SSO or 2FA, enforce credential management system/password manager for secure

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
			user might be unable to access stored files.						credential storing
9		Cloud environment disclosure to public Internet	Depending on the intention, such a vulnerability can have an impact on the confidentiality and integrity of the stored data but can also have an impact on the availability of the whole store information in the cloud as being an easy target for the attackers.	Printer user lacking enough skills or knowledge	2	1	2	Low	Cloud type to be changed to private or community cloud if there is a need to store sensitive files in the cloud environment. Accessing public cloud should be via VPN to reroute the network traffic.

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
10		System vulnerabilities	Unknown file operations or restricted cloud access refers to the impact of confidentiality, integrity and availability of the environment.	Printer user lacking enough skills or knowledge	4	1	4	Low	Main mitigation solutions to be handled by CSP. From the user side, proper research to be done to ensure the reliability of the CSP.
11	Endpoint	Malware in 3D printers	Behavioural problems with 3D printer impact the end result and the object that is desired to be created. Depending on the scope of the malware the impact can include confidentiality, integrity and	Printer user lacking enough skills or knowledge	4	3	12	High	Enforce central device management system, PAM to be implemented

Sequence	Vulnerability type	Vulnerability	Impact of the vulnerability	Cause of the vulnerability	Impact (1-5)	Likelihood (1-5)	Risk score (Impact * Likelihood)	Risk category	Mitigation solutions to decrease the risk
			availability of the endpoint.						
12		Missing port authentication	Compromised 3D printer system makes it impossible to put the device into use therefore having an impact on the availability of the 3D printer.	Targeted attack by the hacker or untargeted attack	2	1	2	Low	Suitable antivirus software to be chosen

In total it is found that there are four "Low" risk, five "Medium" risk and three "High" risk vulnerabilities, as shown in Figure 13, posing potential threat to 3D printers. The highest risk score belongs to DoS attacks vulnerability, which has the biggest possible risk score that could be calculated using this matrix and formula. The second and third highest scores refer to vulnerabilities "Outdated patches" and "Malware in 3D printers." All mentioned vulnerabilities fall under network or endpoint vulnerability type making these the most vulnerable categories for the attackers to harm the device. The least concerning, but still important to mitigate vulnerabilities are "Cloud environment disclosure to the public Internet" and "Missing port authentication" under cloud and endpoint vulnerability type accordingly. In addition, nine out of twelve vulnerabilities have been marked as the cause of vulnerability "Printer user lacking enough skills or knowledge."

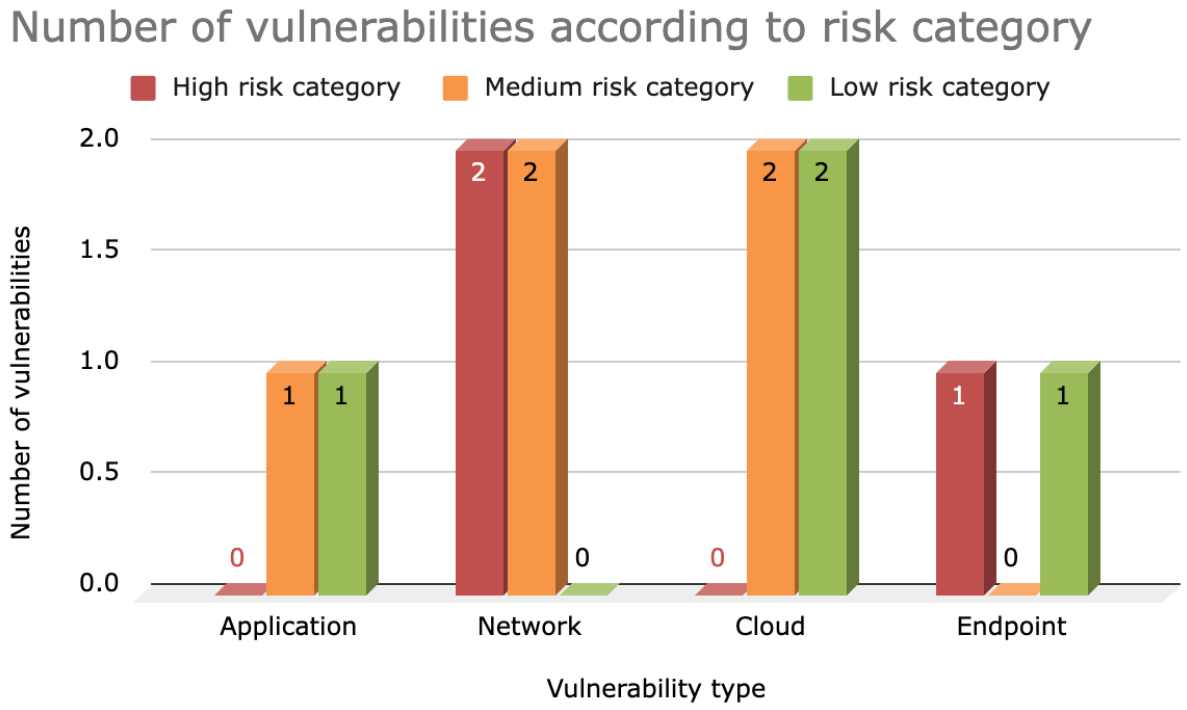

Figure 13. Number of 3D printer vulnerabilities based on risk categories.

It can be concluded that network vulnerabilities, especially DoS attacks pose the greatest threat to 3D printers since there are only "Medium" and "High" risk vulnerabilities and no "Low" risk vulnerabilities at all. The main cause for the vulnerabilities to occur is the 3D printer users lacking enough skills to protect the device.

6. CONCLUSION

In this thesis it was found that there are 12 possible cybersecurity vulnerabilities that could have an impact on 3D printers. These vulnerabilities were categorised into four, application, network, cloud and endpoint vulnerabilities. User input validation exploitation and access privileges exploitation were the main application vulnerabilities. Denial of service attacks, the transcription of unencrypted data, wrong authentication configurations and outdated patches were the main network vulnerabilities. Misconfiguration of cloud environment, insufficient credential and access management, cloud environment disclosure to the public Internet and system vulnerabilities in general were the main cloud vulnerabilities. Malware and missing port authentication were the main endpoint vulnerabilities. All vulnerabilities were also categorised based on the cause of the vulnerability.

To the above listed vulnerabilities possible mitigation solutions and security measures have been proposed to minimise the potential harmful impact on the 3D printer in case the vulnerability occurs. Improper input validation could be mitigated using website hyperlink encryption, the legitimacy of the website is ensured and the website is scanned by an engine. Access privileges exploitation could be mitigated by enforcing least privilege and need-to-know principles to 3D printer users and conducting periodic auditing on access rights. The above mentioned are security measures proposed for application vulnerabilities. Denial of service attacks could be mitigated by conducting threat vector mapping, having a proper network setup and alerting system set in place. Lack of data encryption could be mitigated by enforcing encryption for both data in rest and in transit and having a proper key management system in place. Lack of printer authentication methods could be mitigated by implementing only private and fixed IP ranges, creating IP whitelists and enforcing VPN usage accompanied with 2FA. Outdated patches could be mitigated using a central 3D printer management system for checking and managing updates and conducting periodic audits on software. The above mentioned are security measures proposed for network vulnerabilities. Misconfiguration of cloud environments could be mitigated by conducting periodic risk assessments and having a proper disaster management plan and disaster recovery plan in place. Insufficient credential and access management could be mitigated by having strict access controls in place such as Single Sign-On or Two-Factor Authentication and enforcing credential management system. Cloud environment disclosure to the public Internet could be mitigated by changing cloud type to private or community cloud and accessing public via VPN only. System vulnerabilities in the cloud environment

could be mitigated by conducting proper research to ensure the reliability of the service provider. The above mentioned are security measures proposed for cloud vulnerabilities. Malware in 3D printers could be mitigated by enforcing a central device management system and implementing privileged access management. Missing port authentication could be mitigated by choosing suitable antivirus software. The above mentioned are security measures proposed for endpoint vulnerabilities.

Based on the conducted risk assessment it can be concluded that there were three possible high risk vulnerabilities threatening 3D printers. Out of all the vulnerability types, network vulnerabilities posed the greatest risk on 3D printers. The main cause for the vulnerabilities to occur is printer users lacking enough skills or knowledge to secure the machine.

The objectives set for this thesis were all met. An overview of possible cybersecurity vulnerabilities that 3D printers might have was given. In addition, a list of security measures to minimise the likelihood of such vulnerabilities to happen were provided. Lastly, risk assessment was conducted on the vulnerabilities to better understand the impact on 3D printer. Thesis also provided answers to all posed research questions.

7. KOKKUVÕTE

Käesolevas lõputöös analüüsiti võimalikke 3D printeritega seotud küberturbe ohtusid. Ohud kategoriseeriti nelja erinevasse küberturbe ohu kategooriasse, milleks olid rakenduse ohud, võrguturbe ohud, pilvekeskkonna ohud ning lõppseadme ohud. Iga välja toodud ohu kohta pakkus autor välja võimalikud ohtu minimeerivad lahendused või meetmed, mille rakendamisel väheneks erinevate küberturbealaste ohtude realiseerumine 3D printeritele.

Töös leiti kokku 12 erinevat võimalikku ohtu. Kasutaja sisendi ja ligipääsude pahatahtlik ekspluateerimine on peamised rakenduse ohud. Teenusetõkestusrünne, mitte krüpteeritud andmete saatmine, ebapiisavad kasutaja autentimise seadistused ja iganenud turvapaikade kasutamine on peamised võrguturbe ohud. Pilvekeskkonna valed seadistused, ebapiisav ligipääsuhaldus, pilvekeskkonna avalik ligipääsetavus ning üldised süsteemi vead on peamised pilvekeskkonna ohud. Pahavara ja puudulik pordi autentsuse kontrollimine on peamised lõppseadme ohud. Kõik ohud on lisaks kategoriseeritud põhjuse või põhjustaja järgi.

Leitud ohtudele pakkus autor välja ka võimalikke ohte minimeerivaid lahendusi ning rakendatavaid turvameetmeid. Kasutaja sisendi pahatahtlikku ekspluateerimist on võimalik minimeerida krüpteerides veebisaidi hüperlinki, veendudes veebisaidi autentsuses ja veebilehte skanneerides. Ligipääsude pahatahtlikku ekspluateerimist on võimalik minimeerida võttes kasutusele teadmisvajaduse põhimõtte ning läbi viies perioodilisi ligipääsuõiguste kontrolli auditeid. Kõik eelpool nimetatud meetmed on rakenduse ohtude minimeerimiseks. Teenusetõkestusrünnet on võimalik minimeerida kui kaardistada võimalikud ohuvektorid, korrektselt seadistada internetivõrk ja püsti panna asjakohane hoiatussüsteem ebatavalise võrguliikluse kohta. Mitte krüpteeritud andmete saatmist on võimalik minimeerida kui krüpteerida kõik andmed, mida hoitakse nii lokaalselt kui ka nende liigutamisel ja korraldada turvaline krüpteerimise võtme haldus. Ebapiisavad kasutaja autentimise seadistused on võimalik minimeerida kui võtta kasutusele privaatsed või fikseeritud IP aadressid või nende vahemikud, luua eraldi IP aadresside *whitelist*'id ning kasutada virtuaalset privaatvõrku koos mitmekäigulise autentimisega. Iganenud turvapaikade kasutamist on võimalik minimeerida kui võtta kasutusele keskne 3D printerit haldav süsteem ja teostada perioodilisi versioonihalduse kontrolli auditeid. Kõik eelpool nimetatud meetmed on võrguturbe ohtude minimeerimiseks. Pilvekeskkonna valesid seadistusi on võimalik minimeerida teostades perioodilisi riskianalüüse ning pannes paika

kohased kriisihaldus- ja talitluspidevusplaanid. Ebapiisavat ligipääsuhaldust on võimalik minimeerida kui kasutada turvalist sisselogimisandmete lahendust. Pilvekeskkonna avaliku ligipääsetavust on võimalik minimeerida kui võtta kasutusele õige pilvekeskkonna tüüp ning kasutada sellele ligipääsuks virtuaalset privaatvõrku. Kõik eelpool nimetatud meetmed on pilvekeskkonna ohtude minimeerimiseks. Pahavara on võimalik minimeerida kui kasutada keskset 3D printerit haldavat tarkvara ja rakendada priviligeeritud kasutajahalduse põhimõtet. Puudulikku pordi autentsuse kontrollimist on võimalik minimeerida kui valida sobiv antiviiruse tarkvara.

Lisaks koostati leitud ohtudele riskianalüüs, millest järeldub, et 3D printeritel on kolm kõrge riskiskooriga võimalikku ohtu. Võrguturbe ohud on kõikidest teistest ohtudest kõige suurema riskiga. Peamine ohtude realiseerumise põhjus seisneb 3D printerite kasutajate ebapiisavates oskustes ja teadmistes seadet turvata ning õigeid meetmeid rakendada.

Kõik tööle püstitatud eesmärgid ning uurimisküsimused said töö käigus lahendatud. Töös toodi välja võimalikud 3D printerite küberturbe ohud, pakuti välja erinevaid turvameetmeid ja ohte minimeerivaid lahendusi ning koostati riskianalüüs paremaks ohtude mõju hindamiseks 3D printeritele.

8. REFERENCES

Ahmed, J. (2022). *Combating Cyber Security Risks in 3D Printing.* Source: https://www.selfcad.com/blog/how-to-combat-cybersecurity-risks-in-the-3d-printing-industry. (Last accessed 15.11.2022).

Alley, A. (2022). *Cybersecurity Implications in 3D Printing*. Source: https://www.automationalley.com/articles/cybersecurity-implications-in-3d-printing#:~:text=As%20additive%20manufacturing%2C%20or%203D,critical%20manufacturing%20hardware%20and%20software. (Last accessed 15.11.2022).

All3DP. (2021). *What Is an STL File? – The STL Format Simply Explained.* Source: https://all3dp.com/1/stl-file-format-3d-printing/. (Last accessed 28.12.2022).

Ambrosi, A., Pumera, M. (2016). *3D-printing technologies for electrochemical applications.* Source: https://pubs.rsc.org/en/content/articlehtml/2016/cs/c5cs00714c. (Last accessed 19.10.2022).

Carolo, L. (2021). *3D Printed Food: All You Need to Know in 2022.* Source: https://all3dp.com/2/3d-printed-food-3d-printing-food/. (Last accessed 19.10.2022).

Chai, W. (2022). *Confidentiality, integrity and availability (CIA triad).* Source: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. (Last accessed 10.11.2022).

Checkpoint. (2022). *What is Cloud Security?* Source: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/. (Last accessed 22.10.2022).

Cisco. (2022). *What is Cybersecurity?* Source: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works. (Last accessed 22.10.2022).

Cook, R. (2007). *Securing the Endpoints: The 10 Most Common Internal Security Threats.* Source:

https://www.cio.com/article/274958/infrastructure-securing-the-endpoints-the-10-most-common-internal-security-threats.html. (Last accessed 28.10.2022).

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). *Defining Cybersecurity.* Source: https://www.timreview.ca/article/835. (Last accessed 22.10.2022).

Ctrl-print. (2022). *Printer Malware & How You Can Protect Your Printer From It.* Source: https://ctrl-print.co.uk/printers/printer-malware-protect/. (Last accessed 22.11.2022).

GeeksforGeeks. (2022). *What is Input Validation Attack?.* Source: https://www.geeksforgeeks.org/what-is-input-validation-attack/. (Last accessed 25.11.2022).

Eliaçık, E. (2022). *16 dangerous cloud computing vulnerabilities in 2022.* Source: https://dataconomy.com/2022/05/cloud-computing-vulnerabilities/. (Last accessed 28.10.2022).

Errera, R. (2022). *3D Printing Statistics (2022 Additive Manufacturing Data).* Source: https://www.tonerbuzz.com/blog/3d-printing-statistics/#:~:text=Various%20analysts%20predict%20that%20the,materials%20market%20was%20%241.7%20billion. (Last accessed 29.12.2022).

Fichtner, E. (2022). What are the common types of cyber security attacks?. Source: https://www.datto.com/blog/common-types-of-cyber-security-attacks. (Last accessed 21.12.2022).

Fitzgibbons, L. (2019). *input validation attack.* Source: https://www.techtarget.com/whatis/definition/input-validation-attack. (Last accessed 27.10.2022).

Haines, J. (2022). *History of 3D Printing: When Was 3D Printing Invented?.* Source: https://all3dp.com/2/history-of-3d-printing-when-was-3d-printing-invented/. Last accessed 19.10.2022.

Hoffman, T. (2020). *3D Printing: What You Need to Know.* Source: https://www.pcmag.com/news/3d-printing-what-you-need-to-know. (Last accessed 27.10.2022).

IT Governance. (2022). *What is Cyber Security? Definition and Best Practices.* Source: https://www.itgovernance.co.uk/what-is-cybersecurity. (Last accessed 22.10.2022).

Ivanti. (2020). *Avalanche Printer Management.* Source: https://www.ivanti.com/resources/v/doc/datasheets/ivi-2438-avalanche-printer-mgmt-ds-en. (Last accessed 22.11.2022).

Jang-Jaccard, J., Nepal, S. (2014). *A survey of emerging threats in cybersecurity.* Source: https://www.sciencedirect.com/science/article/pii/S0022000014000178#br1040. (Last accessed 27.10.2022).

Jani, M. (2020). *Never Forget Your Roots: A Brief History of RepRap.* Source: https://e3d-online.com/blogs/news/history-of-reprap. (Last accessed 19.10.2022).

Jones, D. J. B. (2022). *AM Basics. An Introduction to Additive Manufacturing (Also known as 3D printing)*. Source: https://additivemanufacturing.com/basics/. (Last accessed 08.10.2022).

Kauppila, I. (2022). *Every 3D Printing Statistics in One Place!*. Source: https://www.solidprint3d.co.uk/every-3d-printing-statistic-in-one-place/. (Last accessed 29.12.2022).

Kaur, N., Kaur, P. (2014). *Input Validation Vulnerabilities in Web Applications.* Source: https://scialert.net/abstract/?doi=jse.2014.116.126. (Last accessed 27.10.2022).

Kim, J. (2021). *How the World Is Moving to the Cloud and Why We Should Follow*. Source: https://www.linkedin.com/pulse/how-world-moving-cloud-why-we-should-follow-jack-kim/. (Last accessed 15.11.2022).

Kumar, A. (2020). Cloud computing environment 101. Source: https://www.ecloudcontrol.com/cloud-computing-environment-101/#:~:text=Cloud%20ref

ers%20to%20a%20set,%2C%20platforms%20and%2For%20software. (Last accessed 27.10.2022).

Kun, K. (2016). *Reconstruction and Development of a 3D Printer Using FDM Technology.* Source: https://www.sciencedirect.com/science/article/pii/S1877705816311651. (Last accessed 15.10.2022).

Kurko, M. (2022). *Best Password Managers*. Source: https://www.investopedia.com/best-password-managers-5080381. (Last accessed 15.11.2022).

Liotine, M. (2018). *Securing 3D Printing*. Source: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/securing-3d-printing. (Last accessed 28.10.2022).

Manrai, T. (2020). *Cloud Computing Deployment Models: Technical know how.* Source: https://manrai-tarun.medium.com/cloud-computing-deployment-models-technical-know-how-33a3ad30cb66. (Last accessed 29.12.2022).

Mello Jr, J. P. (2022). *11 top cloud security threats.* Source: https://www.csoonline.com/article/3043030/top-cloud-security-threats.html. (Last accessed 28.10.2022).

Mohit, A. (2021). *Best 3D printing management software solutions.* Source: https://layers.app/blog/best-3d-printing-management-software-solutions/. (Last accessed 22.11.2022).

Moore, S. (2022). *The Global 3D Printing Market - Growth, Trends, and Applications.* Source: https://www.azom.com/article.aspx?ArticleID=22152#:~:text=The%20global%203D%20printing%20market%20was%20valued%20at%20%2413.84%20billion,21.5%20million%20units%20by%202030. (Last accessed 28.12.2022).

Moore, S., Armstrong, P., McDonald, T., Yampolskiy, M. (2016). Vulnerability analysis of desktop 3D printer software. *IEEE Xplore.* Source:

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7573305. (Last accessed 27.10.2022).

Neenan, S., Bigelow, S. J. (2021). *What is hybrid cloud? Everything you need to know.* Source: https://www.techtarget.com/searchcloudcomputing/definition/hybrid-cloud. (Last accessed 28.10.2022).

Pal, B. (2021). *FDM Printing Advantages & Disadvantages | Detailed.* Source: https://themechninja.com/07/fdm-printing-advantages-disadvantages-detailed/. (Last accessed 15.10.2022).

Pereira, T., Barroso, S., Gil, M. M. (2021). *Food Texture Design by 3D Printing: A Review*. Source: https://www.mdpi.com/2304-8158/10/2/320. (Last accessed 15.10.2022).

Perez, D. (2022). *3D Printing Market to Triple by 2026, Reveals Latest Hubs Report.* Source: https://www.engineering.com/story/3d-printing-market-to-triple-by-2026-reveals-latest-hubs-report. (Last accessed 15.11.2022).

Petch, M. (2022). *2022 trends in 3D printing, forecasts from additive manufacturing experts and leaders.* Source: https://3dprintingindustry.com/news/2022-trends-in-3d-printing-forecasts-from-additive-manufacturing-experts-and-leaders-202426/. (Last accessed 29.12.2022).

Pitayachaval, P., Sanklong, N., Thongrak, A. (2018). A Review of 3D Food Printing Technology.*MATEC Web of Conferences,* 213, 01012. https://doi.org/10.1051/matecconf/201821301012

Saptarshi, S. M., Zhou, C. (2018). Chapter 2 - Basics of 3D printing: Engineering aspects. *3D Printing in Orthopaedic Surgery, (17-30).* Source: https://www.sciencedirect.com/science/article/pii/B9780323581189000026#. (Last accessed 08.10.2022).

Savini, A., Savini, G. G. (2015). A short history of 3D printing, a technological revolution just started. *IEEE Xplore.* Source: https://ieeexplore.ieee.org/abstract/document/7307314. (Last accessed 19.10.2022).

Shea, S. (2022). *IoT security (internet of things security).* Source: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security. (Last accessed 22.10.2022).

Shea, S., Gillis, A. S., Clark, C. (2022). *What is cybersecurity?*. Source: https://www.techtarget.com/searchsecurity/definition/cybersecurity. (Last accessed 21.12.2022).

Simplify3D. (2022). *Our product.* Source: https://www.simplify3d.com/. (Last accessed 27.10.2022).

Snort. (2022). *Documents.* Source: https://www.snort.org/. (Last accessed 9.11.2022).

Statista Research Department. (2022). *Global 3D printing products and services market size from 2020 to 2026.* Source: https://www.statista.com/statistics/315386/global-market-for-3d-printers/ (Figure 2.1.1., 29.12)

Stratasys. (2022). *F123 Composite-Ready 3D Printers.* Source: https://www.stratasys.com/en/3d-printers/printer-catalog/fdm-printers/F123-composite-ready/. (Last accessed 15.10.2022).

Thakar, C. M., Parkhe, S. S., Jain, A., Phasinam, K., Murugesan, G., Ventayen, R. J. M. (2022). 3d Printing: Basic principles and applications. *ScienceDirect.* Source: https://www.sciencedirect.com/science/article/pii/S2214785321046575. (Last accessed 19.10.2022).

Top3dshop. (2022). *The Evolution of SLS 3D Printers: from Industrial to Desktop Models.* Source: https://top3dshop.com/blog/the-evolution-of-sls-3d-printers-from-industrial-to-desktop-models. (Last accessed 15.10.2022).

TWI. (2022). What are the advantages and disadvantages of 3D printing? Source: https://www.twi-global.com/technical-knowledge/faqs/what-is-3d-printing/pros-and-cons. (Last accessed 28.12.2022).

Wallarm. (2022). *CIA Triad Definition. Examples Of Confidentiality, Integrity, And Availability.* Source: https://www.wallarm.com/what/cia-triad-definition. (Last accessed 10.11.2022).

Wasabi. (2023). *Migrate from on-premise storage to the cloud.* Source: https://wasabi.com/migrate-premise-storage-cloud/. (Last accessed: 03.01.2023).

Wilms, P., Daffner, K., Kern, C., Gras, S. L., Schutyser, M.A.I., Kohlus, R. (2021). Formulation engineering of food systems for 3D-printing applications – A review. *ScienceDirect.* Source: https://www.sciencedirect.com/science/article/pii/S0963996921004841. (Last accessed 15.10.2022).

Yang, F., Zhang, M., Bhandari, B. (2017). *Recent development in 3D food printing.* Source: https://www.tandfonline.com/doi/full/10.1080/10408398.2015.1094732?scroll=top&needAccess=true. (Last accessed 19.10.2022).

3D Printing from scratch. (2015). *Types of 3D printers or 3D printing technologies overview.* Source: http://3dprintingfromscratch.com/common/types-of-3d-printers-or-3d-printing-technologies-overview/. (Last accessed 19.10.2022).

3D systems. (2022). *Stereolithography Printers*. Source: https://www.3dsystems.com/sites/default/files/2022-07/3d-systems-sla-brochure-usen-2022-06-30-web.pdf. (Last accessed 15.10.2022).