Chapter 1

LOW-MAGNITUDE INFILL STRUCTURE MANIPULATION ATTACKS ON FFF-BASED 3D PRINTERS

Muhammad Haris Rais, Muhammad Ahsan, Vaibhav Sharma, Radhika Barua, Rob Prins and Irfan Ahmed

Abstract With the increasing importance of 3D printing in various industry verticals, researchers are exploring new attacks on Additive Manufacturing (AM) processes and the defense techniques. A major attack category on AM processes aims to sabotage the printed object. If an attack causes obvious deformations, the part will be rejected before being employed. The inherent layer-by-layer processing nature of 3D printing allows attackers to induce defects in the internal layers that are hidden in the finished part. Attack's stealthiness raises its probability of going unnoticed by the user, and getting employed in the operational setup causing more damage. Researchers have proposed various detection schemes to identify attacks on external and internal features of the object. However, all schemes have detection thresholds well above the printer's accuracy. If the attacker reduces the attack magnitude to the order of the printer's accuracy, they can bypass the detection solutions. In this study, we are proposing two new infill manipulation attacks that are easy to launch at the cyber-physical boundary avoiding conventional cybersecurity tools, and create planned subtle variations beneath the existing independent monitoring based detection horizon. The magnitude of variations remain within the printer's trueness and resolution values, making it challenging for the detection schemes to differentiate such attacks from benign printing errors. Through destructive testing, we demonstrate that the attacks still create consistent reduction in the material strength. The paper also highlights the need of studying the defensive techniques from a united perspective by incorporating physical characteristics of the printed part in the attack detection process.

Keywords: Critical Infrastructure, Additive Manufacturing, Fused Filament Fabrication, Cyberattacks, Localized Infill Attacks, Cyber-physical Systems security

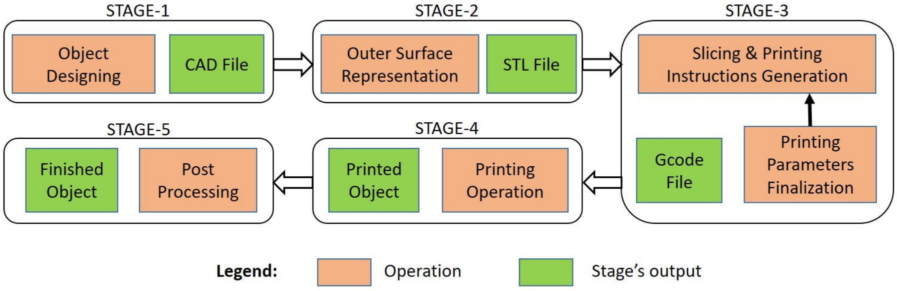


Figure 1: A typical Additive Manufacturing process chain

1. Introduction

Additive Manufacturing (AM) or 3D printing is a collection of manufacturing techniques that create objects from ground zero by stacking thin layers of material. The mechanism is inherently different from the predecessor subtracting manufacturing technology where a block of material is cut from all sides to create a desired part. Rapid prototyping, customized design, low wastage and complex objects printing capability are few distinguished features offered by AM. With the increased choices of printing materials in recent years and reduced capital expenditure of printing setup, AM market is expanding and forecasted to grow at a sustained CAGR of 22.5% over the next five years [1]. Additive Manufacturing is considered as an essential component of Industry 4.0 that advocates mass customization in the manufacturing industry [2].

Figure 1 presents a typical AM process chain comprising five stages. At the stage 1, a designer creates a design file using a Computer Aided Design (CAD) software. The solid 3D drawing is then converted into an outer geometry representation, commonly through a STL (Stereolithography) file. A STL file represents the outer surfaces of an object as a collection of contiguous triangles. STL file along with a set of printing design parameters is sent to a slicer software that generates a corresponding series of printing instructions (such as G-codes). The instructions are sequentially executed by the printer firmware to manufacture the object layer after layer. The printed object passes through a post processing phase that may include curing, surface polishing, etc.

3D printed parts are being used for printing functional components of critical systems [3] raising incentives for the attackers. Appreciating the need for its cybersecurity, researchers have examined the potential attack opportunities in AM process chain from the designing stage to the printer's firmware. The most obvious aims of attacks on AM process are stealing the intellectual property (object's design), denial of printing service, illegal printing, and sabotaging the printed object. AM is a cyber-physical process with the first 3 stages belonging to the cyber-domain and the next 2 stages belonging to the physical domain. Conventional cyber-domain attacks and mitigation schemes are applicable to the cyber part of the AM process chain. The uniqueness of AM process cybersecurity primarily lies beyond the cyber-domain of the process chain. To mitigate the cyber-physical attacks, researchers have proposed approaches that independently examine the printing process in the physical domain through various side-channels. Although the attack detection thresholds are getting better, they are still far above the printer's tolerance specifications. Main reason for this gap (as of today) is the detection scheme's lack of capability to reliably capture the physical process at a higher resolution.

If an attacker keeps the attack magnitudes within the printer's tolerances, it will sneak through most of the existing detection approaches. However, would such a tiny attack be able to negatively and consistently impact the mechanical properties of the object? To find answer to this question, we have proposed two low-magnitude attacks within the order of magnitude of the printing tolerances, and well below the existing attack detection thresholds. The proposed attacks are quick to launch through multiple attack vectors, including man-in-the-middle (MiTM) attack after stage 3 of the process (refer to Figure 1), or by compromising the printer's firmware at the stage 4. Both the attack vectors are feasible for cyber-physical systems and already demonstrated by the researchers [4].

In this study, we have attacked the infill connecting segments by modifying the corresponding G-code instructions at the point of attack. The proposed attacks are conducted on ASTM D638 Type IV tensile bars printed through PLA material using fused filament fabrication (FFF) based printer. FFF is the most common AM technique used today, and most AM attack detection techniques in research literature are demonstrated over FFF printers. Infill structure manipulation ensures that no visual deformation is observed in the finished object. Object dimensions, toolpath profile, printing timing profile, and filament consumption profile shows unnoticeable deviations, where as the destructive tensile strength tests confirms that the attacks reduce the mechanical strength of the printed objects. Micro-CT scans also confirm the structural abnormalities in the internal layers of the object, caused by the attacks.

The rest of the paper is organized as follows. Related work is outlined in the section 2. Section 3 presents the proposed attacks followed by the experiment's details in section 4. The results and discussion is detailed in section 5 and 6, followed by countermeasures in section 7, and the conclusion.

2. Related Work

In this section, we cover the existing work related to the proposed sabotage attacks on the FFF process, and the attack detection techniques capable to detect attacks that successfully bypass pure cyber-domain security mechanisms.

In the past, researchers intending to create hidden defects in the object target the design stage of the process chain, either CAD or STL files. Sturm *et. al* [5] manipulate STL files for creating an internal void in the printed object. Belikovetsky *et. al* [6] demonstrate an attack on the propeller joint of a drone to induce hidden structural weakness, causing it to fail during the flight. This attack is also conducted on the design file. Zeltmann *et. al* [7] introduce tiny defects in the internal layers through design file modification to degrade the strength of the printed object. An important limitation with the design file modification based attacks is the enlarged footprint at the printing stage.

Rais *et. al* [8] demonstrate how design file level attacks create larger attack footprint for tiny looking modifications, and presents G-code level attacks that create tiny cavities, and filament-density and thermodynamic variations with minimal impact on the kinetic and thermodynamic profile of the printing operation. Moore *et. al* [9] present the potential effects of malicious firmware installed on a printer. They also highlight a vulnerability in firmware validation and exploit it to install the malicious code. Claud Xiao [10] demonstrates the feasibility of attacking the open-source FFF 3D printers using an Android device or a PC connected to the PC via a USB cable. Pearce *et. al* [11] presents a bootloader level trojan for Marlin compatible 3D printers. Authors demonstrate two attacks through simple and small code that would fit in the constrained bootloader space, and can manipulate the printing operation.

On the defense side, researchers have utilized different side-channels to detect sabotage attacks. Chhetri *at. el* [12] utilize audio signals emitted from the 3D printer stepper motors to identify the printing object's profile. Later, Belikovetsky *et. al* [13] utilize the audio sensors input with a different algorithm and report improved results with successful detection of 1 second deviation in printing time per layer. To detect an attack, they match the actual printing profile to a master profile generated in a secure and non-compromised environment. Gao *et. al* [14] utilize Inertial Measurement Unit (IMU) sensors and camera to detect kinetic attacks on the printing process. Wu *et. al* [15] use static and moving camera to detect infill pattern attacks. The results show that the approach works well for 10% or higher deviation. Rais *et. al* [16] utilize optical encoder and thermal sensors to estimate the printing state. They transform the G-code file and the sensors input into compatible format to accurately identify most of the attack in the literature with high accuracy.

One common problem with these detection methods is the lack of accommodation of FFF process specific knowledge. The low magnitude infill structure attacks presented in the study exploit this weakness to attack the printed object's mechanical strength.

3. Proposed Attacks

The aim of our proposed attacks is to degrade the mechanical properties of the printed object in a manner that it passes most of the detection and assurance checks, and prematurely failing during operations. The damage caused in operations can be significantly higher than rejecting the part during or after printing.

3.1 Attack Success Criteria

To examine the effectiveness of the attacks, we outline the following success criteria before designing the attacks.

1 Should not cause any visual deformations (in dimensions or shape)

2 Should be feasible to launch after stage 3 (after the control PC as shown in the figure 1

3 Should be able to bypass the detection schemes available in the existing literature, and discussed in section 2

4 Should reduce the mechanical strength of the printed object

5 Should not create deviations in the printhead kinetics more than the order of the printing tolerance specifications

3.2 Printing Accuracy in FFF printers

Kim *et al.* [17] evaluate the precision and trueness of various 3D printers by printing a dental structure using 4 different technology printers. The precision and trueness values for FFF printer are reported to be $99 \pm 14\mu m$ and $188 \pm 14\mu m$ respectively. In another study, Msallem *et al.* [18] report $160 \pm 9\mu m$ and $50 \pm 5\mu mm$ as the trueness and precision

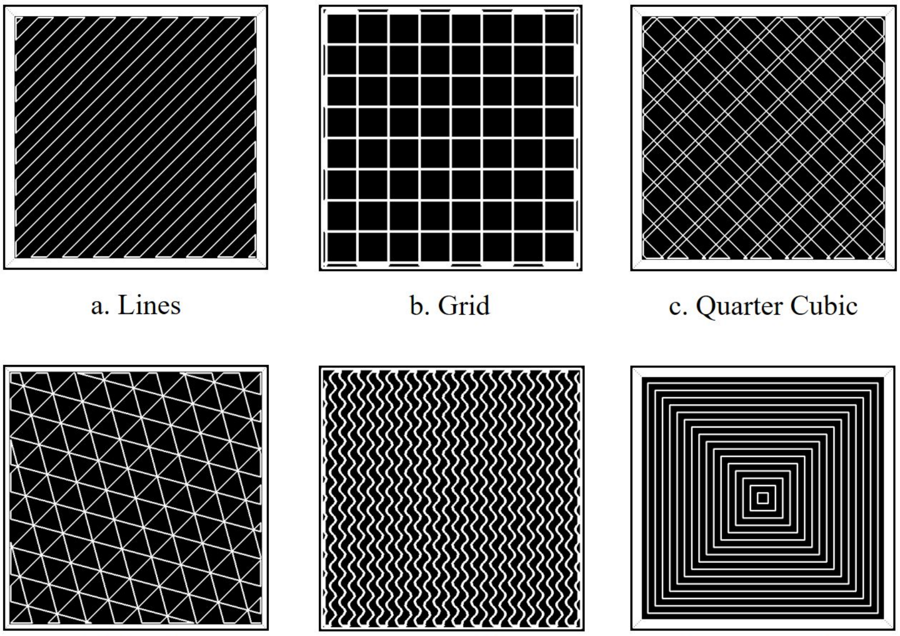


Figure 2: Few common infill patterns in use

values for Ultimaker 3 Ext FFF-based printer, respectively. Stratasys, a renowned brand in 3D printing, publishes a white paper [19] mentioning that Fortus 360mc/400mc printers produce two-sigma (95%) parts within 130 μm tolerance of the true value.

The above discussed trueness and precision values offers an opportunity window to the attackers. Without increasing false-positives, an attack detection scheme relying on capturing the toolpath and applying thresholding to declare an anomaly may not work for attacks in the order of 0.1 mm deviations. Our proposed attacks are based on exploiting this opportunity window to maintain stealthiness - an important success criterion.

3.3 Attacking the Infill Structure

In accordance with the criteria enumerated above, we propose two infill manipulation attacks. The term 'Infill' refers to the internal printing structure of the printed object. The outer walls, the bottom and the top layers completely hide the infill structure in the final print. Each layer's infill pattern is encapsulated by a set of walls (inner and outer

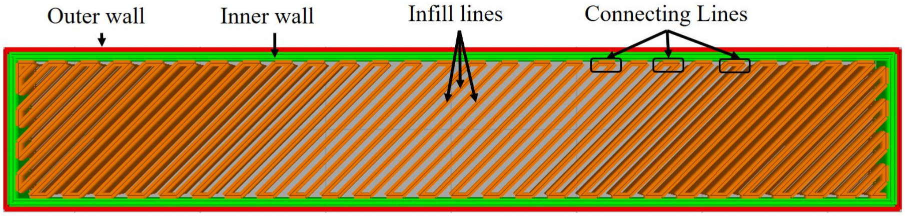


Figure 3: An example of 'Lines' type of Infill structure showing infill and connecting lines

walls). Figure 3 shows a labeled cross-section of an intermediate layer of a rectangular bar with 'Line' type infill pattern. The strength of the object highly depends upon the pattern and the density of infill structure. Figure 2 shows few examples of infill patterns commonly available in the slicing software. If the slicing software is hacked, the complete infill pattern of an object can be easily modified. However, this simple modification in the design triggers much bigger modification in the object toolpath (nozzle-kinetics) and the filament-kinetics. Almost all independent monitoring based detection schemes discussed in the section 2 can detect such attacks.

The kinetic process in FFF-based 3D-printing constitutes nozzle-kinetics, filament-kinetics and printing-bed kinetics. Printing the infill structure of a single layer involves nozzle-kinetics and filament-kinetics. Monitoring the nozzle-kinetics had been the prime focus of the attack detection schemes. In a previous work [8], we exploited the less monitored filament-kinetics to create tiny cavities and density variations in a printed object internal layers. In this work, we challenge the detection solutions by modifying the filament and the nozzle kinetics both in a strictly localized and compensating pattern to ensure minimal footprint. In the *Line* type infill structure, as presented in the figure 3, the consecutive infill lines are connected through a small line segment, named as 'connecting segment'. The proposed attacks manipulate the small connecting segments to create localized asymmetric distribution of material at the target location resulting in a weaker structure.

As evident in the figure 4, the length of the connecting segments is inversely proportional to the gap between 2 consecutive infill lines, and thus to the infill density. As the infill percentage is increased, the connecting segment length reduces and the infill lines get closer. An advantage of selecting infill connecting lines for the proposed attacks is their small length. A fractional change in length of the connecting segment results in a very low absolute deviation, increasing the complexity

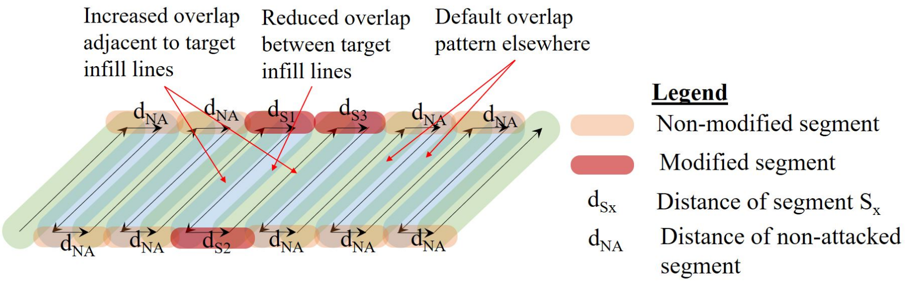

Increased overlap adjacent to target infill lines
Reduced overlap between target infill lines
Default overlap pattern elsewhere
d_{NA}
d_{S1}
d_{S3}
d_{S2}
Legend
Non-modified segment
Modified segment
d_{Sx} Distance of segment S_x
d_{NA} Distance of non-attacked segment

Figure 4: Infill-line spacing attack: Exaggerated view showing the attacked and compensatory segments

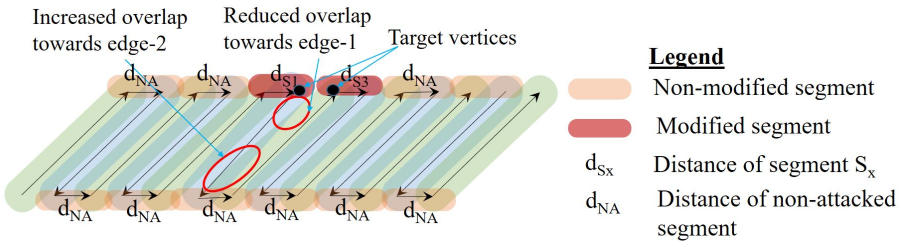

Increased overlap towards edge-2
Reduced overlap towards edge-1
Target vertices
d_{NA}
d_{S1}
d_{S3}
Legend
Non-modified segment
Modified segment
d_{Sx} Distance of segment S_x
d_{NA} Distance of non-attacked segment

Figure 5: Infill-vertex spacing attack: Exaggerated view showing the attacked segments

for the security solutions to reliably detect it. On the other hand, this small deviation in the infill pattern can be sufficient enough to introduce structural weaknesses in the printed object.

3.3.1 Infill Lines Spacing Attack. First proposed attack is the Infill lines spacing attack. In this attack, two consecutive infill lines at a critical location are distanced by a fraction of the connecting segment's length. The modification is repeated over multiple internal layers. The attack is quick to calculate and can be easily launched through MiTM attack without raising any alert. It is assumed that the attacker has some knowledge of the attacked object, and has selected the target location and the layers to be attacked. Within each layer, the attacker identifies the infill structure zone in the G-code file. If the target location is not within the infill structure, the attack location is modified to be within the infill structure. After identifying the corresponding connecting segment linked to the infill lines bordering the target location, the attacker increases its length by a small fraction.

For the object with 100% infill density, we use a thumb rule to not exceed the attack magnitude over 50% of the segment length to avoid obvious cavity at the point of attack. An exaggerated view of the attack scheme is presented in the figure 4. The attacker selects the target zone of attack within the infill section of the G-code instructions, and evaluates the following conditions:

$$0 \; > \; \Delta d_{S_1} = \Delta d_{S_3} \; > \; \Delta d_{S_2} \tag{1}$$

where Δd_{S_2} is the deviation in length of the connecting segment between the target infill lines, Δd_{S_1} and Δd_{S_3} are the deviations in length in the adjacent segments. The attacker chooses a smart Δd_{S_2} value, and compensates for the increase in the segment S_2 by equally distributing Δd_{S_2} between the adjacent segments S_1 and S_3, as evident in the figure 4.

3.3.2 Infill Vertices Spacing Attack . In the second proposed attack, the attacker creates a tiny inverse wedge shaped cavity at the target location. Instead of distancing the pair of infill lines at both ends, they are only parted at one end. The length d_{S_1} and d_{S_3} of the connecting segments S$_1$ and S$_3$ are reduced, whereas there is no change in d_{S_2}. Figure 5 presents an attack scenario showing the target vertices, concerned infill lines and connecting segments. After confirming that the attack location is part of the infill structure, the attacker finalizes the attack magnitude to ensure that the deviation remains within the printer's tolerances mentioned in the subsection 3.2, and does not result in obvious inverse-wedge shaped cavity.

In this attack, the direction and length of the infill lines do not remain unaltered, but the change is minimal. Equation 2 represents the change in length of the infill lines, and equation 3 represents the change in infill angle (also called raster angle).

$$d_{IF_{atk}} \;=\; \sqrt{d^2_{IF_{dft}} + \; 2 * \Delta d_S * sin(\theta_{dft}) * d_{IF_{dft}} + \Delta d^2_S} \tag{2}$$

$$\Theta_{IF_{atk}} = tan^{-1}\{(d_{IF_{dft}} * sin(\theta_{dft}) + \Delta d_S)/d_{IF_{dft}} * cos(\theta_{dft})\} \tag{3}$$

where $d_{IF_{dft}}$ represents the non-attacked infill line length, $d_{IF_{atk}}$ is the modified infill length, Δd_S is the change in the connecting segment length, and Θ is the infill line angle configured at the slicing stage. For instance, a 10 mm infill line configured at an angle of 45^o, 0.1 mm decrease in the connecting segment length will result in Δd_{IF} (change in infill line length) of around 0.07 mm. This magnitude is well within

S/No	Printing Parameter	Selected Value
1	Layer Thickness	0.2 mm
2	Nozzle Diameter	0.4 mm
3	Build Plate Temperature	60^{o}C
4	Nozzle Temperature - Layer 1	210^{o}C
5	Nozzle Temperature -Layer 2 onwards	205^{o}C
6	Infill Pattern	LINE at 45^o
7	Infill percentage	100%
8	Number of layers	20
9	Printing Speed - Layer 1	20 mm/sec
10	Printing Speed - Layer 2 onwards	45 mm/sec
11	Top and Bottom layers	Nil
12	Number of walls	02

Table 1: Printing parameters selected for the experiment

the printing tolerances and far from the detection thresholds claimed in the existing literature. Similarly, the change in infill line angle is approximately 0.4^o for an infill angle of 45^o. As the attack modifies two consecutive infill lines, the polarity of change is opposite for both infill lines length and direction. If IF_1 (infill line 1) is bigger than $d_{IF_{dft}}$, then IF_2 will be smaller than $d_{IF_{dft}}$ and vice versa. As the attack is repeated over a few layers, this compensation within each attack instance helps in deceiving the detection schemes tracking the accumulative value of performance parameters - such as the total nozzle travel (or toolpath). Algorithm 1 outlines the attack process for both the attacks.

4. Implementation of the Attacks

To evaluate the performance of the proposed attacks at different magnitudes on real objects, we conduct a case study over American Standard of Testing Materials (ASTM) D638 Type IV standard tensile bars printed using Polylactic Acid (PLA) polymer. Ultimaker-3 is employed as the FFF printer for the case study. The printer is controlled through Ultimaker Cura software version 4.10, which also serves as the slicer software. The printing parameters used for the study are outlined in the table 1. Five specimen are printed for each variant of both types of attacks, along with two sets of five specimens for non-attacked tensile bars. Each type of attack specimens are printed using different PLA spools with different colors, primarily to address the availability issues. As we printed the reference specimens through each spool and used their test results to gauge the corresponding impact of any attack, the study aim is not effected by this arrangement. We conduct non-destructive

Algorithm 1 Proposed Infill Attacks Algorithm

```
Output: G-code$_{Attacked}$
Input: G-code$_{Original}$, Layers$_{Attacked}$, Loc$_{Attacked}$, Magnitude ($A_m$)
while Location$_{Attacked}$ $\notin$ Infill-Structure:
    Shift_location
Calculate $A_{m_{max}}$ based on segment length, filament consumption,
maximum attack magnitude
if $A_m >$ $A_{m_{max}}$: $A_m \leftarrow A_{m_{max}}$
$\forall$ i $\in$ Layers$_{Attacked}$ :
    Seg$_1$ $\leftarrow$ Identify nearest connecting segment to Loc$_{Attacked}$
    Attack 1: Displacing 2 consecutive Infill lines
    Calculate new x and y coords, such that
        No change in the slope for any infill or segment
        $|d_{s_1}| \leftarrow |d_{s_1}|$ - $|A_m|$
        $|d_{s_2}| \leftarrow |d_{s_2}|$ + $|A_m|$
        $|d_{s_3}| \leftarrow |d_{s_3}|$ - $|A_m|$
        No change in $|Infill_1|$ & $|Infill_2|$
    $\forall$ i $\in$ Attacked commands :
        modified_G-code $\leftarrow$ compute_new_G-code(i)
    Attack 2: Displacing 2 consecutive Infill remote vertices
    Calculate new x and y coords, such that
        No change in the slope of old and new segments
        (Infill lines slope will slightly change)
        $|d_{s_1}| \leftarrow |d_{s_1}|$ - $|A_m|$
        $|d_{s_2}|$ not modified
        $|d_{s_3}| \leftarrow |d_{s_3}|$ - $|A_m|$
        (Infill lines magnitude will slightly change)
    $\forall$ i $\in$ Attacked commands :
        modified_G-code $\leftarrow$ compute_new_G-code(i)
G-code$_{Attacked}$ $\leftarrow$ update_G-code (G-code$_{Original}$ , modified_G-code)
Return: G-code$_{Attacked}$
```

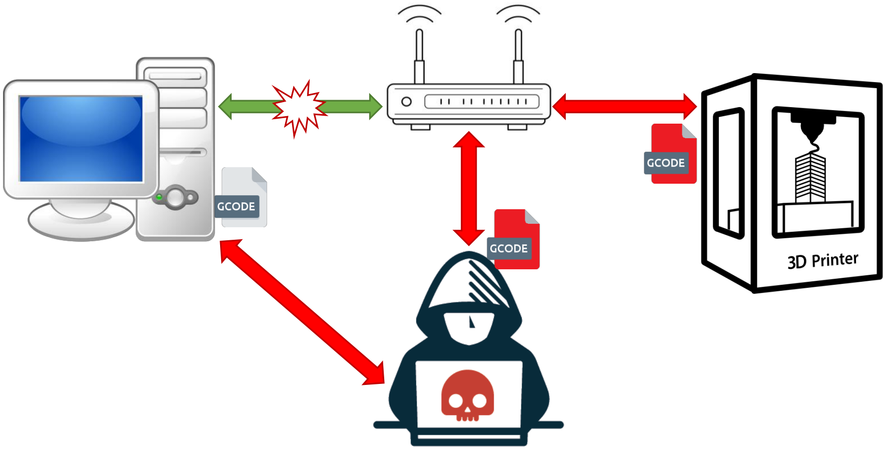


Figure 6: Attack Scenario using MITM technique to sabotage G-code file

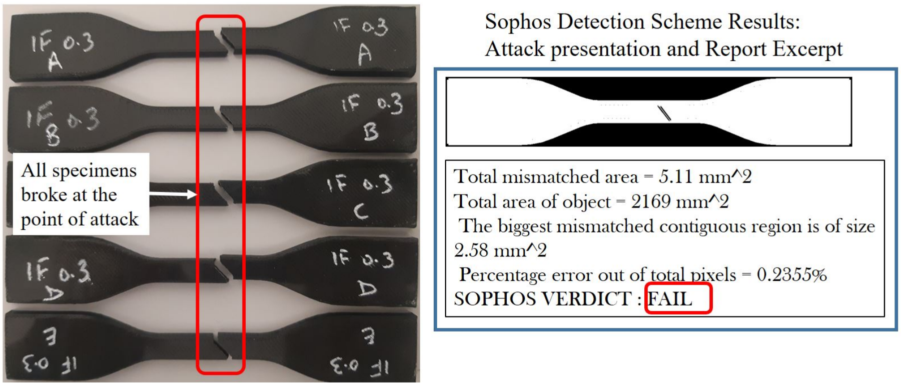
tests including measurement analysis, optical microscopy and micro-CT scans. Ultimately, through tensile tests performed through MTS Insight 30 equipment, we evaluate the attack's impact on the mechanical strength.

4.1 Attack Vector

The attacker is assumed to be an insider with the access to the printer's local area network. As the printer and the control PC utilize unencrypted communication channel, we opt for man-in-the-middle (MiTM) through ARP poisoning as our attack vector to launch the proposed attacks. The process is shown in figure 6 wherein a client's legitimate communication channel with the printer is interrupted and routed through the attacker's machine. Once the user sends a printing request to the printer, the attacker's code receives the original G-code file, calculate the attacks, and sends the modified file to the printer. The sub-second delay introduced by the attacker is not noticeable by a user in a practical printing setup.

4.2 Attack Plan

The attacks are targeted at the central portion of the internal layers of the tensile bar. The unmodified length of the infill lines $d_{IF_{dft}}$ and the connecting segments $d_{S_{dft}}$ are 6.54 mm and 0.594 mm, respectively. The attacks are planned in two phases.


1F 0.3 A
1F 0.3 A
1F 0.3 B
1F 0.3 B
All specimens broke at the point of attack
1F 0.3 C
1F 0.3 D
1F 0.3 D
1F 0.3 E
1F 0.3 E
Sophos Detection Scheme Results:
Attack presentation and Report Excerpt

Total mismatched area = 5.11 mm^2
Total area of object = 2169 mm^2
The biggest mismatched contiguous region is of size 2.58 mm^2
Percentage error out of total pixels = 0.2355%
SOPHOS VERDICT : FAIL

Figure 7: Attack phase-1 specimens and Sophos detection results excerpt

Phase-1. In phase-1 of the experiment, we establish the maximum magnitude that an attacker can afford without being detected by the attack detection schemes. As it is not practically feasible to implement all detection techniques mentioned in the related work, we use **Sophos** [16] that claims to identify sub-millimeter variations. We conduct Infill-line spacing attack starting with an attack magnitude of $A_{m_{max}}$ (0.3 mm in our case). In the next iterations, we reduce the magnitude till Sophos is unable to reliably detect the deviations. To further gauge the stealthiness and impact of attack, we conducted measurement tests, visual inspection, micro-CT scan and tensile strength test for the specimens.

No visual deformation or measurement changes are observed in the attack. The tensile tests show a consistent and significant reduction in the strength, and all samples broke at the point of attack. However, Sophos successfully detects the attack for each attacked layer. Figure 7 presents the attack samples, and the Sophos verdict about the printed part. Table 2 presents the measurements and tensile tests performance for the attacked samples, showing over 50% reduction in tensile strength. The micro-CT scan also identifies some anomaly (a slit) within the affected layers. As the attack could not bypass a detection solution, it does not satisfy condition 3 of the success criteria mentioned in the section 3.1, and hence considered unsuccessful. On reducing the attack magnitude to 0.2 mm, we successfully evaded Sophos, marking the maximum attack magnitude for our experiment.

Phase-2. For phase-2, the main phase of attack experiment, we implement attacks with magnitude ranging from 0.2 mm to 0.015 mm in five steps. Although, all the attacks get concealed in the final printed

	Average of 5 Specimen	Std. Deviation	Difference with Non Attacked Specimen	Percentage Difference
Width (mm)	6.576	0.013	0.022	0.33%
Thickness (mm)	4.090	0.025	0.026	0.64%
Peak Load (N)	606.540	42.371	-311.180	-51.30%
Peak Stress (MPa)	22.540	1.705	-12.140	-53.86%
Strain At Break (mm/mm)	0.027	0.007	-0.002	-5.88%
Modulus (MPa)	1246.074	136.373	-418.399	-33.58%

Table 2: Attack Phase-1: 0.3 mm magnitude Infill-line spacing attack results showing significant reduction in the strength

	Attack Type			
	Infill Line Spacing Attack		**Infill Vertex Spacing Attack**	
Attack Category	**Specimen Count**	**Attack Location**	**Specimen Count**	**Attack Location**
Non-Attacked (NA)	5	Nil	5	Nil
0.015 mm	5	6 IFLs from center	5	Center
0.025 mm	5	6 IFLs from center	5	Center
0.05 mm	5	Center	5	4 IFLs from center
0.1 mm	5	Center	5	4 IFLs from center
0.2 mm	5	4 IFLs from center	5	4 IFLs from center

Table 3: Attack Plan Phase-2: Attack categories defined as per attack magnitude for both the proposed attacks

object, the stealthiness increases as the magnitude reduces. A total of six categories of specimen printed for each of the two proposed attacks making a total of 60 specimens. Dimensional verification and visual inspection are carried out for all the specimen, but micro-CT scans are conducted for selected samples. Table 3 outlines the attack plan details for the main phase.

5. Evaluation Results

We analyse the results in accordance with the success criteria mentioned in the section 3.1. None of the attacks created any visual deformation in the final printed object, and all attacks are launched after stage-3 of the process chain. Thus, success criteria 1 and 2 are met by all the attacks. The footprints produced by the attacks in the main phase are small enough to bypass the detection schemes. However, the micro-CT scan does reveal the presence of structural anomaly in the potentially damaging attacks. As the attack magnitude is reduced, the impact on

Attack Type & Magnitude (mm)		**Printing Time per Attacked Layer**		**Printed Part Dimensions (Complete Printed Parts)**				**Visual Deformation in Printed Object**
		Average (sec)	**Deviation (sec)**	**Width (mm)**		**Thickness (mm)**		
				Avg	**Deviation**	**Avg**	**Deviation**	
No Attack		61.513	0.000	6.582	0	4.088	0	None
Infill Line Spacing Attack	0.015	61.518	0.005	6.58	0.002	4.08	0.008	None
	0.025	61.520	0.008	6.568	0.014	4.09	-0.002	None
	0.05	61.523	0.010	6.568	0.014	4.083	0.005	None
	0.1	61.521	0.009	6.57	0.012	4.09	-0.002	None
	0.2	61.526	0.014	6.563	0.019	4.085	0.003	None
Infill Vertex Spacing Attack	0.015	61.525	0.012	6.562	0.02	4.086	0.002	None
	0.025 mm	61.525	0.012	6.592	-0.01	4.084	0.004	None
	0.05 mm	61.521	0.009	6.546	0.036	4.064	0.024	None
	0.1 mm	61.523	0.010	6.58	0.002	4.078	0.01	None
	0.2 mm	61.520	0.008	6.584	-0.002	4.086	0.002	None

Table 4: Stealthiness Performance - Cumulative Parameters

the mechanical strength also reduces marking a minimum effective deviation threshold value for a successful attack. The results of the study are examined from the stealthiness and the effectiveness standpoint, both.

5.1 Stealthiness Performance of the Attacks

An attack in the printed process chain at or post cyber-physical boundary can be detected through a broad spectrum of activities, including visual inspection, dimensions measurement, microscopic analysis of the surface, computer tomography, toolpath verification and others. Some of the parameters offer a cumulative insight into the process, such as the total printing time, or total filament consumption, or part's outer dimensions. Other type of parameters offer instantaneous or localized estimates of the process, such as deviation in the toolpath, time to execute a G-code command, and printing speed profile.

5.1.1 Cumulative Parameters Stealthiness Performance.

Table 4 presents the stealthiness performance of the attacks for the cumulative parameters. The cumulative parameters tested for stealthiness are the printing time per layer, visual deformation, and printed part dimensions. No deformation is observed in the object through naked eye or optical microscope. The maximum printing time variation for the attacks is within 14 ms from the non-attacked samples' mean value. The printed parts' dimensions are also not changed. The maximum mean difference for any dimension for the attack sets is less than 0.036 mm - well within the printer's accuracy tolerance. The dimensions measurements

Attack Type & Magnitude (mm)		**Launch Time Delay (sec)**	**Toolpath Deviation per IF line cmd - max**		**Max Time Deviation per cmd (ms)**	**Filament Deviation per cmd-max (mm)**	**Micro-CT Scan - Manual Detection**
			Distance (mm)	**Angular (Degree)**			
No Attack		-		-	-	-	-
Infill Line Spacing Attack	0.015	0.15	0.015	0	< 5	None	Negative
	0.025	0.15	0.025	0	< 5	None	Negative
	0.05	0.15	0.05	0	< 5	None	Positive
	0.1	0.15	0.1	0	< 5	None	Positive
	0.2	0.15	0.2	0	< 5	None	Positive
Infill Vertex Spacing Attack	0.015	0.15	0.011	0.093	< 5	None	Negative
	0.025	0.15	0.018	0.154	< 5	None	Negative
	0.05	0.15	0.035	0.308	< 5	None	Negative
	0.1	0.15	0.071	0.612	< 5	None	Probable
	0.2	0.15	0.143	1.211	< 5	None	Positive

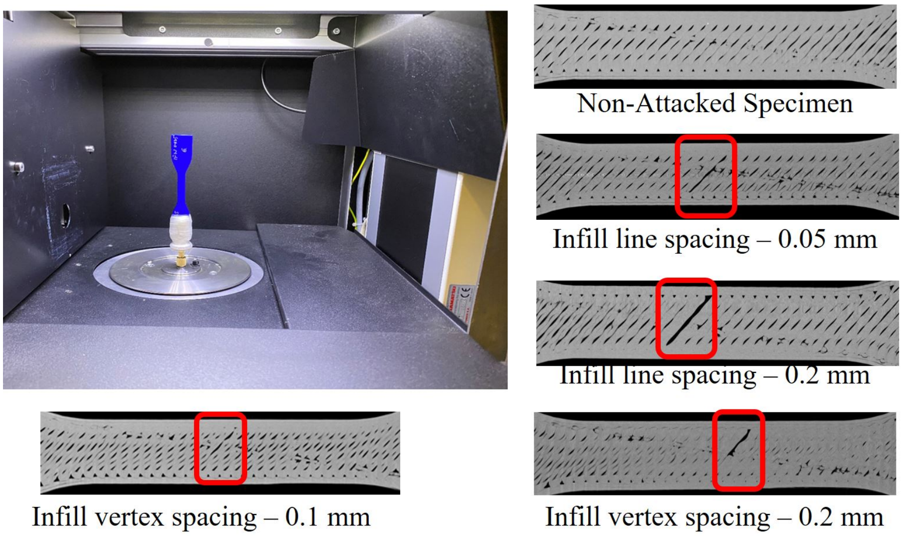
Table 5: Stealthiness Performance - Localized Parameters

for attacked samples go on both sides of the non-attacked samples' mean value within the standard deviation distance.

5.1.2 Localized Parameters Stealthiness Performance.

As some of the attack detection schemes monitor the process continuously in time and space domain to predict any anomaly, it is important to assess the attacks' footprint with respect to instantaneous deviations in the process. Table 5 shows the performance against the instant-based parameters. We measure the deviation in the toolpath (in terms of distance and direction), execution time and filament consumption per G-code instruction. As a high delay in printer's acknowledgement to the printing request may raise an alert, we measure the attack launch time as a stealthiness performance parameter. Finally, we include a detailed manual analysis of micro-CT scanned images to identify the attacked areas in the printed parts.

The attack launch time is under 150 ms for all types of attacks. Highest toolpath deviation per G-code command is 0.2 mm for infill-line spacing attacks. For infill-vertex spacing attack, highest toolpath deviation is 0.2 mm for the connecting segment, and 0.143 mm for the corresponding infill line. The angular deviation is none for infill-line spacing attack, and 1.211^o for infill-vertex spacing attack. Maximum G-code execution time deviation is less than 5 ms. Due to the selected sampling rate of 200 samples / second, the time deviation resolution of our measurement is 5 ms. Although the attacks may be causing different time variations within 5 ms, the value is well within the existing attack detection thresholds. There is no filament deviation per command for any of the proposed attacks.



Non-Attacked Specimen

Infill line spacing – 0.05 mm

Infill line spacing – 0.2 mm

Infill vertex spacing – 0.1 mm

Infill vertex spacing – 0.2 mm

Figure 8: Specimens from phase-2 attack: All specimen above 0.05 mm attack magnitude broke at the point of attack

Micro-CT Scan. The microstructure of the 3D printed specimens are observed using X-ray micro-computed tomography. Skyscan 1173 machine is employed to recreate a 3D model. Micro-CT analysis is performed at 40 kV voltage, 200 μA current, 1800 ms exposure, 0.50 rotational step, and pixel size of 20 μm. The scanned raw data is reconstructed through N-Recon software version 1.7.4.4. Subsequently, the reconstructed images are centered for COR VOI, and analyzed using data viewer software.

Micro-CT analysis shows the attacks at a magnitude of 0.05 mm and above for infill-line spacing attacks. For the infill-vertex spacing attacks, micro-CT analysis does not show any sign of attack at 0.05 mm, and a hint of probable attack at 0.1 mm magnitude. 0.2 mm mgantidue infill-vertex spacing attack is clearly visible in the micro-CT scan. As the magnitude increases, the micro-CT analysis identifies the attacked area with higher confidence. Micro-CT equipment and selected images are presented in the figure 8.

5.2 Attack Impact on the Mechanical Strength

As the attack is conducted on the tensile bars, we evaluate the effectiveness through tensile strength tests. The tests are conducted through MTS-Insight 30 tensile testing machine. Not all attacks are found to be consistently effective in reducing the tensile strength or the load-

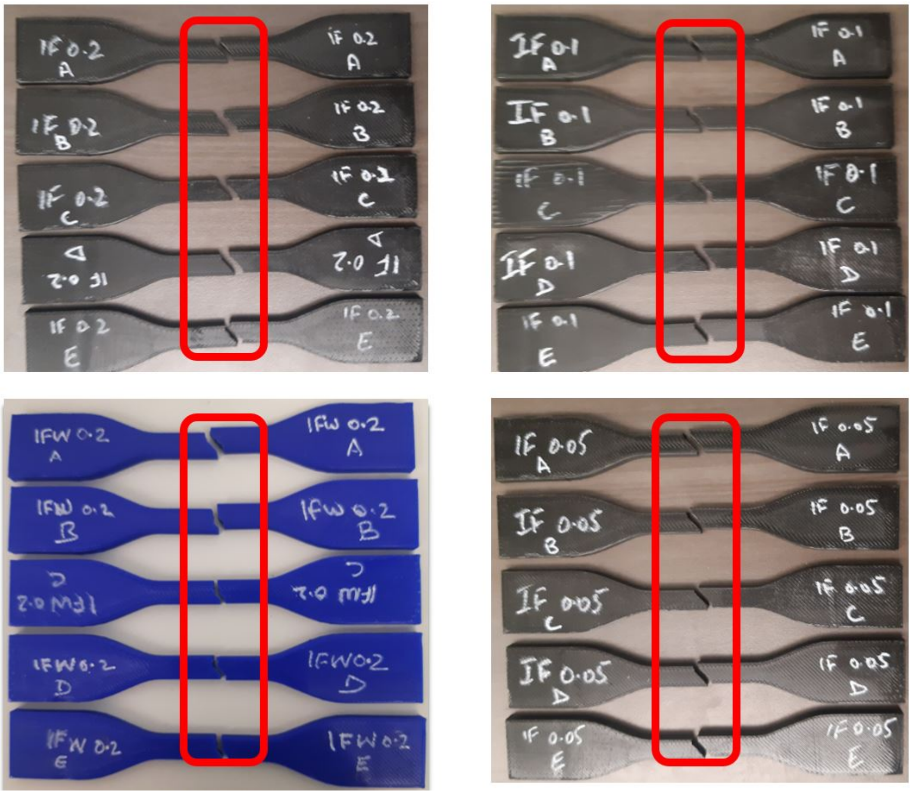


Figure 9: Specimens from phase-2 attack: All specimen above 0.05 mm attack magnitude broke at the point of attack

extension profiles. All attacked specimen with magnitude above 0.05 mm broke at the point of attack. Few specimen are presented in the figure 9.

Table 6 summarizes the results for the first type of attacks related to infill-line spacing, and table 7 presents the results for the infill-vertex spacing attacks. Figure 10 and figure 11 presents the representative stress vs strain curves for both the attacks. Most attacked samples for all types of attacks broke at a shorter extension as compared to the non-attacked samples (or broke earlier considering the load vs time curves). The young modulus value decreases in infill-line spacing attacks, but the variations are not consistent and pronounced in infill vertex spacing attacks. Maximum reduction in the 'Peak Load' for the main phase attacks is observed to be 33.55% in infill-line spacing attack, and 11.57% in infill-vertex spacing attack.

Infill Line Spacing Attack									
Attack Magnitude (mm)	**Peak Load (N)**			**Peak Stress (MPa)**			**Moduls (MPa)**		
	Average	**Std Dev**	**%age Diff**	**Average**	**Std Dev**	**%age Diff**	**Average**	**Std Dev**	**%age Diff**
No Attack	936.94	98.78	0.00	35.45	3.45	0.00	1730.22	167.85	0.00
0.015	938.09	40.86	0.12	35.49	1.65	0.12	1708.45	75.17	-1.26
0.025	919.89	35.68	-1.82	34.37	1.55	-3.06	1756.83	42.87	1.54
0.05	694.75	18.01	-25.85	25.93	0.68	-26.87	1267.56	106.84	-26.74
0.1	622.57	34.66	-33.55	23.17	1.39	-34.65	1498.47	147.25	-13.39
0.2	624.32	32.57	-33.37	23.28	1.29	-34.34	1323.59	107.12	-23.50

Table 6: Tensile test results for Infill-line spacing attacks

Infill Vertex Spacing Attack									
Attack Magnitude (mm)	**Peak Load (N)**			**Peak Stress (MPa)**			**Moduls (MPa)**		
	Average	**Std Dev**	**%age Diff**	**Average**	**Std Dev**	**%age Diff**	**Average**	**Std Dev**	**%age Diff**
No Attack	1036.11	42.45	0.00	38.60	1.54	0.00	1771.42	129.52	0.00
0.015	1054.48	30.37	1.77	39.33	1.35	1.88	1850.70	168.24	4.48
0.025	1041.91	59.80	0.56	38.70	2.41	0.26	2052.87	116.97	15.89
0.05	1008.68	39.05	-2.65	37.92	1.28	-1.76	1901.28	44.97	7.33
0.1	953.37	44.39	-7.99	35.52	1.76	-7.98	1726.44	163.31	-2.54
0.2	916.28	36.46	-11.57	34.06	1.19	-11.76	1796.00	261.93	1.39

Table 7: Tensile test results for Infill-vertex spacing attacks

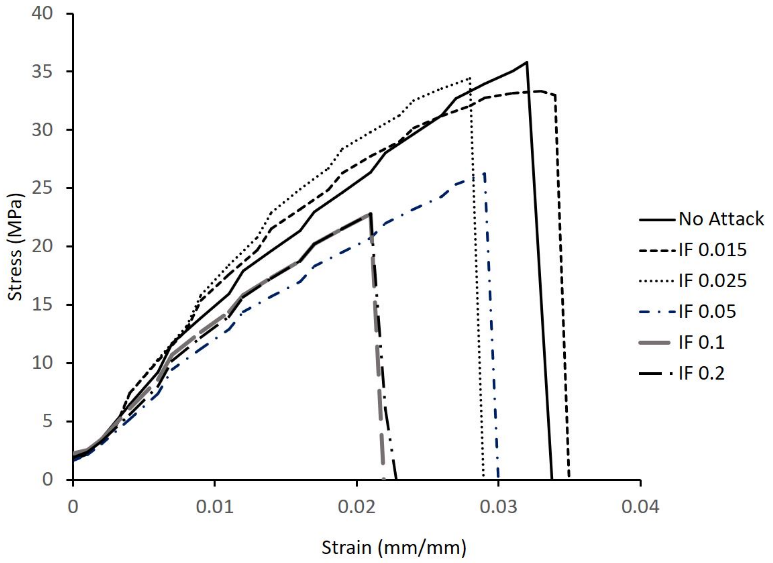


Figure 10: Infill-line spacing attack - Stress vs Strain curves

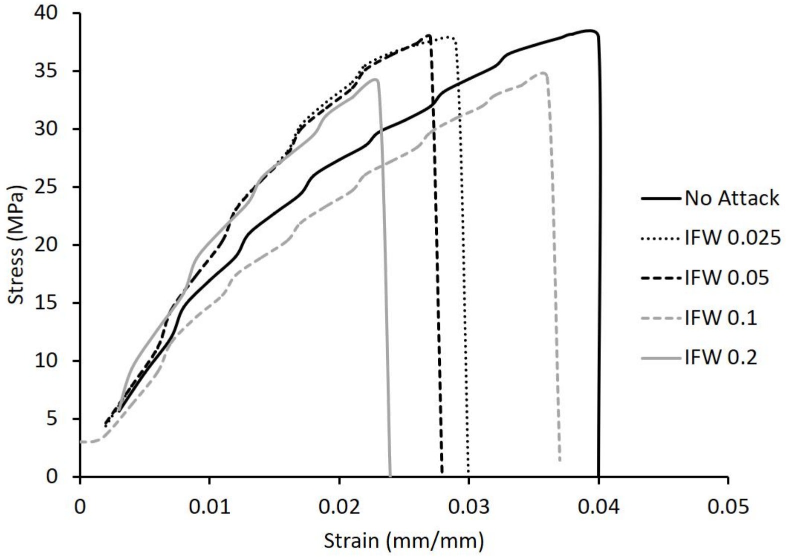


Figure 11: Infill-vertex spacing attack - Stress vs Strain curves

6. Analysis and Discussion on the Attacks

Conducting an attack on the design file is a pure cyber domain modification that can be detected through conventional cybersecurity tools such as file hashes and operating system audit logs. However, the proposed attacks launched between the control PC (excluded) and the printer (included) do not encounter cyber-domain operating systems and their standard security tools. As per a study, 12 out of 13 surveyed printers do not use encrypted communication between control PC and the printer [20], making them susceptible to simple MiTM attacks.

The proposed low-profile attacks create a footprint that is smaller than the reported resolution of the attack detection schemes based on printing process monitoring. The attack magnitudes are within the order of the reported tolerance of the FFF-based printers accuracy, posing further challenge for the thresholding based detection methodologies. Although, all the attacks get concealed in the final printed object, the effect is somewhat visible during printing (as shown in the figure 12), and techniques based on continuous imaging may detect the anomaly.

For identical attack magnitudes, infill-line spacing attacks are more damaging than infill-vertex spacing attacks. As presented in the figure 13 and 14, both the attacks also exhibit different strength-reduction profiles with reference to the attack magnitudes. Infill-line spacing attacks have

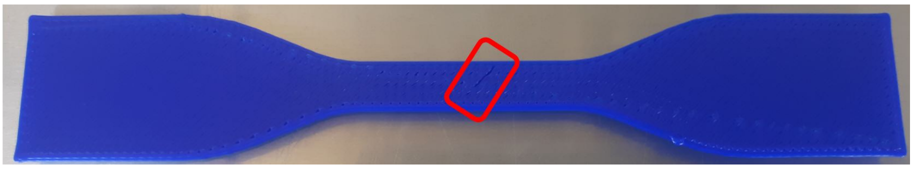


Figure 12: Infill-vertex spacing attack with 0.2 mm magnitude: Image taken after pausing the printing process during one of the attacked layers shows the inverse wedge cavity

the peak impacting zone between 0.35 mm and 0.1 mm magnitude. The peak impacting zone for infill-vertex spacing attack is between 0.05 mm to 0.1 mm approximately, but still follows a gradual reduction. In infill-line spacing attack, two adjacent infill lines are distanced from end-to-end. In infill-vertex spacing attacks, infill lines only part at one end, resulting in increased bonding and overlap between the two lines as they progress from the point of attack towards the other vertex. This explains the lesser strength reduction and the shifted impact zone for infill-vertex spacing attacks.

The micro-CT image analysis revealed that the non-attacked printed object with 100% infill density also contains tiny gaps between the infill structure and the surrounding walls, and within the infill structure. Optimizing the printing parameters may remove these gaps and also increase the infill lines overlap. In such cases, these attacks will be more interesting and pronounced. Although the study is not focused on the printing parameters optimization, this finding impacts the attacker's choices as well. Interestingly, when micro-CT analysis confirms the presence and location of an attack, the destructive tests also show a reduction in strength. For a 20 layer object with around 200 cross-sectional images, CT can capture structural weaknesses resulting within a part of a single attacked layer, making it an important tool for detecting micro-structure related attacks in Additive Manufacturing.

One limitation of these attacks is that they can only effectively target solid filled objects. In a variation of the attacks, the infill connecting segments may be drifted slightly from the inner and outer walls structure to introduce weakness in their bond. Such weaknesses may negatively effect the compression and sheer strength of the object with minimal attack footprint.

Estimating physical properties. In low-magnitude sabotage attacks, the attacker targets one or more physical properties of the object. As most of the detection techniques focus on mapping the actual pro-

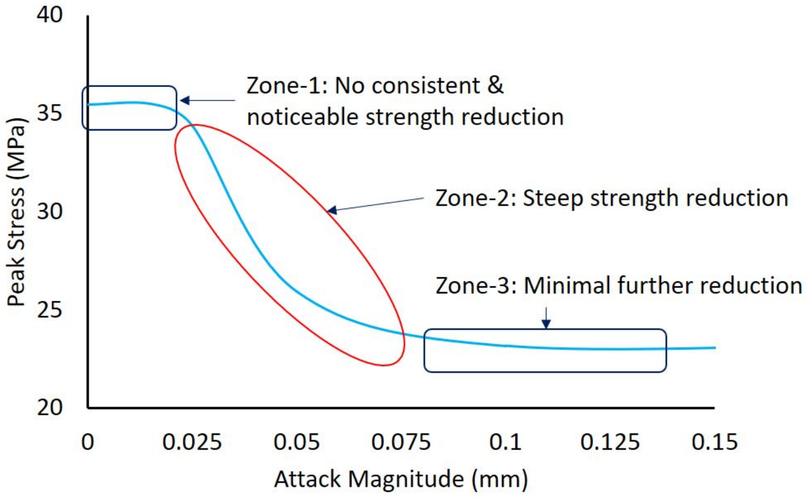


Figure 13: Infill-line spacing attack - - Strength vs Attack Magnitude

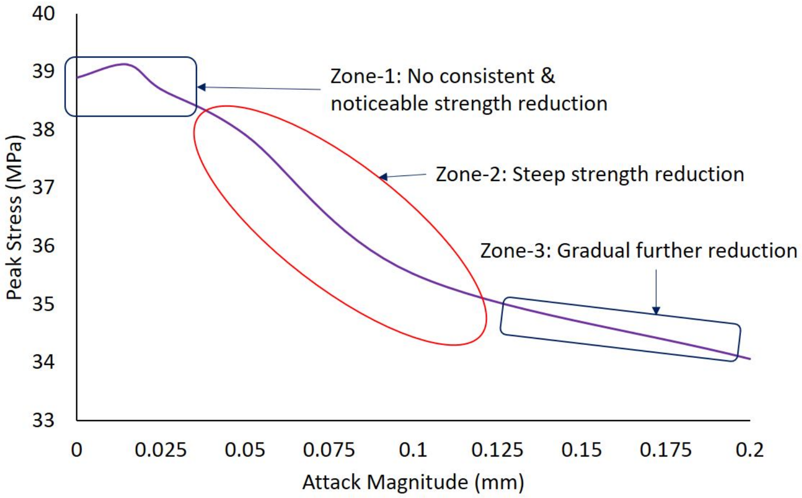


Figure 14: Infill-vertex spacing attack - Strength vs Attack Magnitude

cess behavior to the true and expected behavior, these low-magnitude attacks can evade these techniques. Instead of focusing on mapping the printer's space, thermal and timing profile to the expected state, a different approach is to estimate the potential targeted physical properties. For instance, a small variation at one location may be safely ignored, but can induce high residual stresses at another location. If a detection scheme understands this phenomenon, it can be more effective in distinguishing between damaging low-magnitude attacks and benign printing errors.

7. Attacks' Countermeasures

Two categories of countermeasures are presented here. First category discusses the measures to avoid the attack occurrence. Physical access to the critical printing facility should be controlled and monitored to deny any malicious code making its way through printer's physical ports. Avoiding unencrypted and unauthenticated communication between the control-PC and the printer minimizes the success chances of MiTM attacks. Features such as DHCP Snooping and ARP inspection can help avoid ARP table manipulation by the attacker. Researchers have proposed multiple techniques to counter network layer attacks in a cyber-physical environment [21, 22]. To avoid attacks through a compromised firmware, the printer's running firmware should be periodically verified. Instead of inline firmware acquisition, out of band methods [23] offer an authentic copy of the running firmware.

If the attacker succeeds in launching the attack, micro-CT scans can identify a potent structural abnormality caused by an attack. The time and manual effort required in conducting the CT scans and the post-analysis do not offer a scalable solution. Although there are implementation challenges, an in-printing scanning with automated anomaly detection function is operationally more feasible approach for a busy and critical printing facility. While CT scan is far more detailed, high speed in-printing optical imaging based methods may also be useful in detecting structural non-conformity.

8. Conclusion

In this paper, we present two low-magnitude infill-structure manipulation attacks on a FFF-based 3D printed object. Infill line-spacing attack reduces the overlap between two consecutive infill lines at the target location, and the infill vertex spacing attack creates an inverse wedge shaped low density zone at the target location. The attack magnitudes are kept below the existing detection horizon in the available literature, and also within the reported tolerance in trueness and resolution of the FFF-based printers. The attacks are implemented on solid-filled ASTM D638 type-IV tensile bars by manipulating the G-code instructions at the attack location in the selected internal layers. The tensile tests conducted on the attacked specimens demonstrate that the attacks magnitude of 0.05 mm can still reduce the mechanical strength of the printed parts. Such attack magnitudes will remain within the confusion zone of the detection schemes that only monitor the printer's actions against the printing commands. If an attack detection scheme can attain the physical properties estimates against the current process state, the attacked instance can be magnified and distinguished from the random printing errors. Another approach to detect such attacks is to incorporate automated analysis of real-time micro-CT scans to identify the structural abnormalities.

Acknowledgement

This work was supported, in part, by the Virginia Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information, visit `www.cyberinitiative.org`.

References

[1] https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html

[2] Ugur M. Dilberoglu and Bahar Gharehpapagh and Ulas Yaman and Melik Dolen, The Role of Additive Manufacturing in the Era of Industry 4.0, Procedia Manufacturing,volume 11,https://doi.org/10.1016/j.promfg.2017.07.148,

[3] Goh G. D., Sing S. L., Yeong W. Y., 2021, A review on machine learning in 3D printing: applications, potential, and challenges, Artificial Intelligence Review, https://doi.org/10.1007/s10462-020-09876-9

[4] Qasim S.A., Ayub A., Johnson J., Ahmed I. (2022) Attacking the IEC 61131 Logic Engine in Programmable Logic Controllers. In: Staggs J., Shenoi S. (eds) Critical Infrastructure Protection XV. ICCIP 2021. IFIP Advances in Information and Communication Technology, vol 636. Springer, Cham. https://doi.org/10.1007/978-3-030-93511-5_4

[5] Sturm L., C. Williams, J. Camelio, J. White, and R. Parker, "Cyber-Physical Vunerabilities in Additive Manufacturing Systems", Con-

text, 7(2014, pp. 8)

[6] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, dr0wned–cyber-physical attack with additive manufacturing, in: Proceedings of the Eleventh USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, Vancouver, BC, 2017.

[7] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and Security Challenges in 3D Printing," JOM, vol. 68, no. 7, pp. 1872–1881, Jul. 2016.

[8] Muhammad Haris Rais, Ye Li, Irfan Ahmed, Dynamic-thermal and localized filament-kinetic attacks on fused filament fabrication based 3D printing process, Additive Manufacturing, Volume 46, 2021, 102200, ISSN 2214-8604, https://doi.org/10.1016/j.addma.2021.102200.

[9] Moore, Samuel & Glisson, William & Yampolskiy, Mark. (2017). Implications of Malicious 3D Printer Firmware. 10.24251/HICSS.2017.735.

[10] Xiao Zi Hang (Claud Xiao), Security Attack to 3D Printing, 2013. Keynote at XCon2013.

[11] Hammond Pearce, Kaushik Yanamandra, Nikhil Gupta, Ramesh Karri: FLAW3D: A Trojan-based Cyber Attack on the Physical Outcomes of Additive Manufacturing. CoRR abs/2104.09562 (2021), https://arxiv.org/abs/2104.09562

[12] S.R., Chhetri, A., Canedo, M.A., Al Faruque, Kcad: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems, in: Proceedings of the 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 1–8

[13] S. Belikovetsky, Y. A. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici. Digital audio signature for 3d printing integrity. IEEE Transactions on Information Forensics and Security, 14(5):1127–1141, 2019

[14] Y., Gao, B., Li, W., Wang, W., Xu, C., Zhou, Z., Jin, Watching and safeguarding your 3d printer: Online process monitoring against cyber-physical attacks, in: Proceedings of the ACM Interact. Mob. Wearable Ubiquitous Technol, 2, 2018. https://doi.org/10.1145/3264918

[15] Mingtao Wu, Heguang Zhou, Longwang Lin, Bruno Silva, Zhengyi Song, Jackie Cheung, and Young Moon. Detecting attacks in cyber-manufacturing systems: Additive manufacturing example. MATEC Web of Conferences, 108:06005, 01 2017. doi: 10.1051/matec-conf/201710806005.

[16] Muhammad Haris Rais, Ye Li, and Irfan Ahmed. 2021. Spatiotemporal G-code modeling for secure FDM-based 3D printing. Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems. Association for Computing Machinery, New York, NY, USA, 177–186. DOI:https://doi.org/10.1145/3450267.3450545

[17] Kim SY, Shin YS, Jung HD, Hwang CJ, Baik HS, Cha JY. Precision and trueness of dental models manufactured with different 3-dimensional printing techniques. Am J Orthod Dentofacial Orthop. 2018 Jan;153(1):144-153. doi: 10.1016/j.ajodo.2017.05.025. PMID: 29287640.

[18] Msallem B, Sharma N, Cao S, Halbeisen FS, Zeilhofer H-F, Thieringer FM. Evaluation of the Dimensional Accuracy of 3D-Printed Anatomical Mandibular Models Using FFF, SLA, SLS, MJ, and BJ Printing Technology. Journal of Clinical Medicine. 2020; 9(3):817. https://doi.org/10.3390/jcm9030817

[19] https://www.stratasys.co.kr/-/media/files/white-papers-new/wp_fdm_fortus360mc400mcaccuracystudy_en_1213b_web.pdf

[20] M. McCormack, S. Chandrasekaran, G. Liu, T. Yu, S. DeVincent Wolf and V. Sekar, "Security Analysis of Networked 3D Printers," 2020 IEEE Security and Privacy Workshops (SPW), 2020, pp. 118-125, doi: 10.1109/SPW50608.2020.00035.

[21] Y. Li, L. Zhu, H. Wang, F. R. Yu and S. Liu, "A Cross-Layer Defense Scheme for Edge Intelligence-Enabled CBTC Systems Against MitM Attacks," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2286-2298, April 2021, doi: 10.1109/TITS.2020.3030496.

[22] H. Adjei, T. Shunhua, G. Agordzo, Y. Li, SSL Stripping Technique "(DHCP Snooping and ARP Spoofing Inspection)", *Twenty Third International Conference on Advanced Communication Technology (ICACT)*, pp. 187–193, 2021.

[23] M. Rais, R. Asmar, J. Jr, I. Ahmed, JTAG-based PLC Memory Acquisition Framework for Industrial Control Systems, *Twentieth Annual Digital Forensics Research Conference*, 2021.