Chapter 8

# LOW-MAGNITUDE INFILL STRUCTURE MANIPULATION ATTACKS ON FUSED FILAMENT FABRICATION 3D PRINTERS

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

**Abstract** As 3D printing applications in industry verticals increase, researchers have been developing new attacks on additive manufacturing processes and appropriate defense techniques. A major attack category on additive manufacturing processes is printed object sabotage. If an attack causes obvious deformations, the part will be rejected before it is used. However, the inherent layer-by-layer printing process enables malicious actors to induce hidden defects in the internal layers of finished parts. The stealthiness of an attack increases its chances of evading detection and the printed part being used in an operational environment where it can cause harm. Several detection schemes have been proposed for identifying attacks on external and internal features of printed objects, but all these schemes have detection thresholds that are well above printer accuracy. Reducing the attack magnitude to the order of printer accuracy can evade detection.

This chapter describes two infill structure manipulation attacks that are easy to launch at the cyber-physical boundary and evade conventional cyber security tools by employing subtle printed part variations below the detection horizon. Specifically, the magnitudes of the variations fall within the printer resolution and trueness values, rendering it challenging for detection schemes to differentiate printed part modifications from benign printing errors. Destructive testing demonstrates that the infill structure manipulation attacks consistently reduce the strength of printed parts. This chapter also highlights the need to incorporate the physical characteristics of printed parts in attack detection.

**Keywords:** 3D printing, fused filament fabrication, localized infill structure attacks

Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XVI, IFIP AICT 666, pp. 205–232, 2022.
https://doi.org/10.1007/978-3-031-20137-0_8

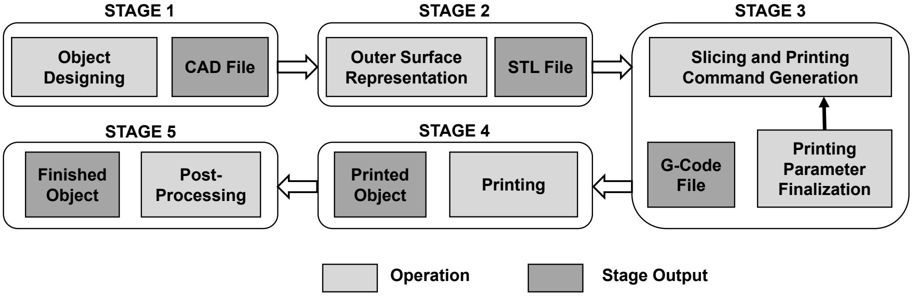


*Figure 1.* Additive manufacturing process chain.

## 1. Introduction

Additive manufacturing (AM) or 3D printing encompasses manufacturing techniques that create objects by stacking thin layers of material. Additive manufacturing is inherently different from conventional subtractive manufacturing in which a block of material is cut from various sides to create the desired part. Rapid prototyping, customized design, reduced wastage and complex object printing capabilities are some of the distinctive features offered by additive manufacturing. The increased range of printing materials and reduced capital expenditures for printing have significantly expanded the additive manufacturing footprint. In fact, additive manufacturing is forecasted to grow at a sustained compound annual growth rate of 22.5% over the next five years [12]. Additive manufacturing is an essential component of Industry 4.0, which advocates mass customization in the manufacturing industry [6].

Figure 1 shows the five-stage additive manufacturing process chain. During the first stage, a design file is created using computer-aided design (CAD) software. Next, the 3D design is converted to an outer geometry representation, commonly a stereolithography (STL) file. An STL file represents the outer surfaces of an object as a collection of contiguous triangles. The STL file and a set of printing design parameters are then sent to slicer software, which generates the corresponding series of printing commands such as G-code. The commands are executed sequentially by the printer firmware to create the object layer by layer. The printed object finally undergoes post-processing, which involves operations such as curing and surface polishing.

3D printers are increasingly used to print functional components of critical systems [8], rendering them attractive targets for malicious actors. Appreciating the need for cyber security, researchers have examined the attack opportunities in the additive manufacturing process chain. The most obvious attacks are intellectual property (object design) theft, denial of printing service, illegal printing and printed part sabotage.

Additive manufacturing is a cyber-physical process with the first three stages belonging to the cyber domain and the last two stages belonging to the physical domain. Conventional cyber attacks and mitigation schemes are applicable to the cyber portion of the additive manufacturing process chain. The uniqueness of additive manufacturing security primarily lies beyond the cyber domain of the process chain. To mitigate cyber-physical attacks, researchers have proposed approaches that independently examine the printing process in the physical domain using various side channels. Although the attack detection thresholds are improving, they are still well above printer tolerances. The main reason for the current gap is the inability of detection schemes to reliably capture the physical process at high resolution.

If a malicious actor keeps the attack magnitudes within the tolerances of a printing process, the attacks would likely circumvent most detection approaches. To ascertain the exploitation potential of tiny deviations, this research focuses on two low-magnitude attacks that are within the order of magnitude of printing tolerances and well below attack detection thresholds. The new attacks are computed and launched within 150 ms using multiple attack vectors, including a man-in-the-middle (MitM) attack after Stage 3 of the additive manufacturing process chain (Figure 1) or by compromising the printer firmware in Stage 4. The attack vectors have been demonstrated to be feasible for cyber-physical systems [2, 17, 18]

This research has targeted infill connecting segments by modifying the G-code commands at the point of attack. The attacks were executed on ASTM D638 Type IV tensile bars created by a fused filament fabrication (FFF) printer using polylactic acid (PLA) material. Fused filament fabrication is the most common additive manufacturing technique in use today [24] and most additive manufacturing attack detection techniques in the research literature are demonstrated using fused filament fabrication printers. Infill structure manipulation attacks ensure that no visual deformations are observed on the finished objects. Object dimensions, toolpath profiles, printing timing profiles and filament consumption profiles show imperceptible deviations, but destructive tensile strength tests confirm that the attacks significantly reduce the mechanical strength of the printed objects. Micro-computed tomography (Micro-CT) scans also confirm the structural abnormalities in the internal layers of attacked objects.

## 2. Related Work

This section discusses research related to sabotage attacks on the fused filament fabrication process and techniques for detecting attacks that bypass pure cyber-domain security mechanisms.

Researchers intending to create hidden defects in printed objects have targeted CAD and STL files during the design stage of the additive manufacturing process chain. Zeltmann et al. [29] introduced tiny defects in the internal layers of printed objects through design file modifications to degrade their strength. Sturm et al. [25] manipulated STL files to create internal voids in printed objects. Belikovetsky et al. [4] demonstrated an attack on the propeller joint of a drone that induced hidden structural weakness, causing it to fail during flight. However, a key limitation of these design file modification attacks is their enlarged footprints during the printing stage.

Rais et al. [22] demonstrated how subtle variations in design file attacks are translated to large, easy-to-detect footprints during the printing stage. They also presented G-code attacks that create internal cavities and filament density and thermodynamic variations that have minimal impacts on the kinetic and thermodynamic profiles of printing operations. Moore et al. [14] identified and exploited a firmware validation vulnerability to install malicious code and demonstrated its harmful effects. Xiao [28] attacked open-source fused filament fabrication printers using an Android device and a computer connected to the USB printer port. Pearce et al. [16] created a bootloader-level Trojan for Marlin-compatible 3D printers. They demonstrated two attacks, implemented via simple code inserted in constrained bootloader space, that manipulated printing operations.

Defensive research has leveraged various side channels to detect sabotage attacks. Chhetri et al. [5] utilized audio signals emitted from 3D printer stepper motors to identify the printing profiles of objects. Belikovetsky et al. [3] employed audio sensors to detect one-second deviations in printing time per layer; attacks were detected by matching the actual printing profiles to a master profile generated in a secure, non-compromised environment. Gao et al. [7] used inertial measurement unit sensors and a camera to detect kinetic attacks on a printing process. Wu et al. [27] utilized static and moving cameras to detect infill pattern attacks; good results were obtained for deviations of 10% or higher. Rais et al. [23] employed optical encoders and thermal sensors to estimate the printing state. They transformed the G-code file and sensor inputs into a compatible format to accurately identify most of the attacks reported in the literature with high accuracy.

A common problem with all these detection methods is that they do not engage printing process knowledge. The low-magnitude infill structure attacks developed in this research exploit knowledge about the fused filament fabrication process to target the mechanical strength of printed objects.

# 3. Low-Magnitude Infill Structure Attacks

The low-magnitude infill structure attacks degrade the mechanical properties of printed objects in a manner that evades most detection and assurance checks. The degraded objects would fail prematurely during operation.

## 3.1 Attack Success Criteria

The following criteria are used to assess attack success:

- **Criterion 1:** Feasible to launch the attack after Stage 3 (after the control computer shown in Figure 1).
- **Criterion 2:** No deviations in printhead kinetics above the printing tolerance specifications.
- **Criterion 3:** Detection schemes described in the literature are bypassed.
- **Criterion 4:** Imperceptible visual deformations to the dimensions and shape of the printed object.
- **Criterion 5:** Reduction in the mechanical strength of the printed object.

## 3.2 Printing Accuracy

Kim et al. [10] evaluated the precision and trueness of 3D printers by printing dental models using four additive manufacturing technologies. The precision and trueness values for fused filament fabrication printers were reported to be $99 \pm 14\,\mu$m and $188 \pm 14\,\mu$m, respectively. In another study, Msallem et al. [15] reported precision and trueness values of $50 \pm 5\,\mu$m and $160 \pm 9\,\mu$m, respectively, for an Ultimaker 3 Ext fused filament fabrication printer. Stratasys [9], a renowned 3D printer manufacturer, reported that Fortus 360mc/400mc printers produce two-sigma (95%) parts within a $130\,\mu$m tolerance of the true value.

These precision and trueness values offer malicious actors windows of opportunity. Without increasing the false positive rate, a detection scheme that relies on the printer toolpath and applies thresholding to

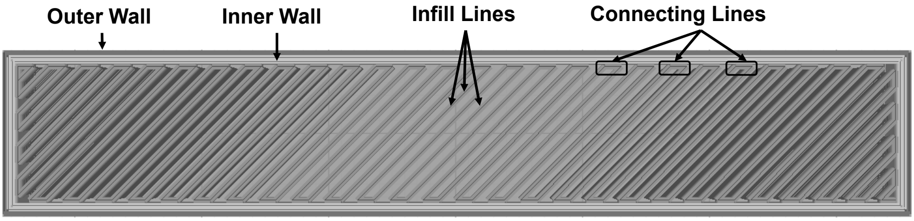


*Figure 2.* Lines-type infill structure showing infill and connecting lines.

identify anomalies may not work for attacks that produce deviations of the order of 0.1 mm. The low-magnitude infill structure attacks described here exploit the windows of opportunity to maintain stealth, an important success criterion.

## 3.3 Attacking Infill Structures

Infill refers to the internal printing structure of a printed object. The outer walls and bottom and top layers of a printed object completely hide its infill structure. The infill pattern in each print layer is encapsulated by the inner and outer walls.

Figure 2 shows a cross-section of an intermediate layer of a rectangular bar with a lines-type infill pattern. For 100%-filled parts, slicer software, such as Ultimaker Cura, replaces any selected infill pattern with a lines-type pattern. The strength of a printed object depends on the infill pattern and density of the infill structure.

Figure 3 shows six examples of infill patterns commonly provided by slicer software. If the slicer software is compromised, the infill patterns of printed objects can be modified very easily. However, even a simple design modification triggers much larger modifications to the printer toolpath (nozzle kinetics) and filament kinetics. Almost all the independent-monitoring-based detection schemes discussed in the literature would be able to detect such attacks.

The kinetic process in fused filament fabrication printing constitutes nozzle kinetics, filament kinetics and printbed kinetics. Printing the infill structure of a single layer involves nozzle kinetics and filament kinetics. Most attack detection schemes monitor nozzle kinetics. Previous research has exploited the less-monitored filament kinetics to create cavities and density variations in the internal layers of printed objects [22]. The attacks developed in this research evade these detection schemes by maintaining nozzle kinetics and filament kinetics by employing highly-localized, compensating patterns to minimize the attack footprints. In

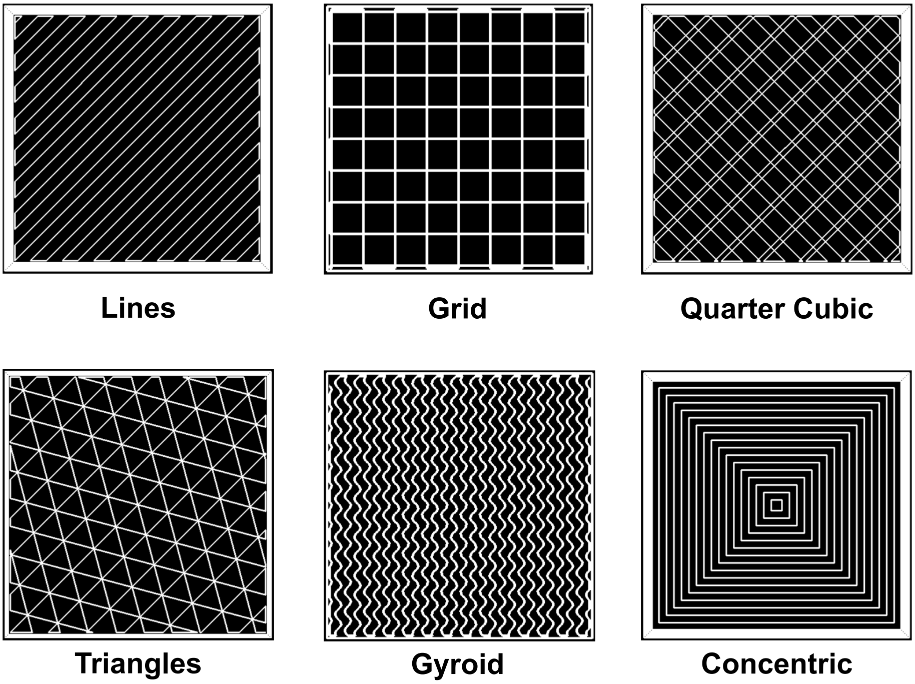


*Figure 3.* Common infill patterns.

the lines-type infill structure shown in Figure 2, consecutive infill lines are connected by a small line segment called the connecting segment. The attacks manipulate the connecting segments to create a localized asymmetric distribution of material at the target location that results in a weaker structure.

The length of a connecting segment is inversely proportional to the gap between two consecutive infill lines, and is also inversely proportional to the infill density. As the infill percentage is increased, the connecting segment length is reduced and the infill lines get closer. The connecting segments are attractive targets for stealthy attacks due to their small lengths. A fractional change in length of a connecting segment results in a very low absolute deviation, increasing the complexity of attack detection. Moreover, even a small deviation in an infill pattern can induce structural weakness in the printed object.

**Infill Lines Spacing Attack.** An infill lines spacing attack moves two consecutive infill lines at the target location by a fraction of the length of the connecting segment. This modification is repeated over

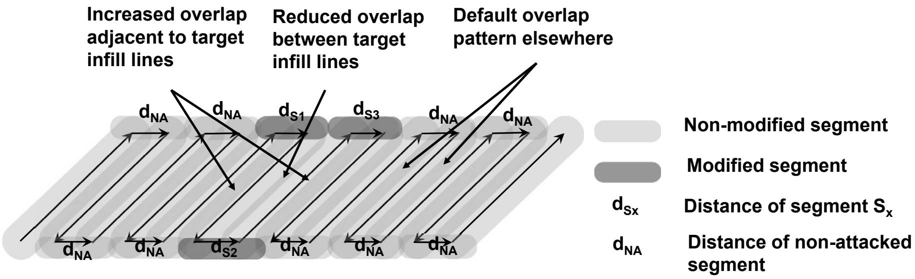

Increased overlap adjacent to target infill lines
Reduced overlap between target infill lines
Default overlap pattern elsewhere
d_NA
d_NA
d_S1
d_S3
d_NA
d_NA
d_NA
d_NA
d_S2
d_NA
d_NA
d_NA
Non-modified segment
Modified segment
d_Sx Distance of segment S_x
d_NA Distance of non-attacked segment

*Figure 4.* Infill lines spacing attack.

multiple internal layers. The attack is computed and launched within 150 ms from a man-in-the-middle position. It is assumed that a malicious actor leverages knowledge about the targeted object to select the specific locations and layers to be attacked. The malicious actor identifies the infill structure zone in each layer of the G-code file. After identifying the connecting segment linked to the infill lines bordering the targeted location, the malicious actor increases its length in the G-code by a small fraction.

Figure 4 shows an exaggerated view of the attacked and compensatory segments resulting from an infill lines spacing attack. For an object with 100% infill density, the rule of thumb is to maintain the attack magnitude under 50% of the segment length to avoid creating an obvious cavity at the point of attack. Figure 4 shows the attack scheme. The targeted zone is selected in the infill section of the G-code and the following condition is evaluated:

$$0 \ < \ \Delta d_{S_1} = \Delta d_{S_3} \ < \ \Delta d_{S_2}$$

where $\Delta d_{S_2}$ is the deviation in the length of the connecting segment between the targeted infill lines, $\Delta d_{S_1}$ and $\Delta d_{S_3}$ are the deviations in the lengths of the adjacent segments. An appropriate $\Delta d_{S_2}$ value is selected to compensate for the increase in the length of segment $S_2$ by distributing $\Delta d_{S_2}$ equally between the adjacent segments $S_1$ and $S_3$ as shown in Figure 4.

**Infill Vertices Spacing Attack.** An infill vertices spacing attack creates an inverse-wedge-shaped cavity at the targeted location. Figure 5 shows the attack scheme. Instead of moving two consecutive infill lines at both ends, the consecutive lines are only parted at one end. The lengths $d_{S_1}$ and $d_{S_3}$ of the connecting segments $\mathrm{S}_1$ and $\mathrm{S}_3$ are reduced whereas there is no change to $d_{S_2}$. After confirming that the targeted location is part of the infill structure, the attack magnitude is finalized

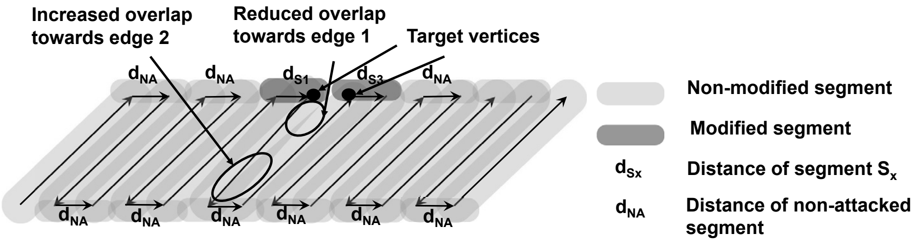

Increased overlap towards edge 2
Reduced overlap towards edge 1
Target vertices
d_NA
d_NA
d_S1
d_S3
d_NA
d_NA
d_NA
d_NA
d_NA
d_NA
d_NA
Non-modified segment
Modified segment
d_Sx Distance of segment S_x
d_NA Distance of non-attacked segment

*Figure 5.* Infill vertices spacing attack.

to ensure that the deviation remains within the printing tolerance and does not create an obvious inverse-wedge-shaped cavity.

The infill vertices spacing attack modifies the lengths and (raster) angles of the infill lines slightly. The modified infill line length $d_{IF_{atk}}$ and angle $\theta_{IF_{atk}}$ are given by:

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

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

where $d_{IF_{dft}}$ is the original infill line length, $\Delta d_S$ is the change in the connecting segment length and $\theta_{dft}$ is the infill line angle configured during the slicing stage. For example, given a 10 mm infill line configured at an angle of $45^o$, a 0.1 mm decrease in the connecting segment length changes the infill line length $\Delta d_{IF}$ by around 0.07 mm. This magnitude is well within the printing tolerance and far from the detection thresholds reported in the literature. Similarly, the change in infill line angle is approximately $0.4^o$ for an infill angle of $45^o$. Because the attack modifies two consecutive infill lines, the polarities of the changes are opposite for the pairs of infill line lengths and angles. If infill line 1 $IF_1$ is larger than $d_{IF_{dft}}$, then infill line 2 $IF_2$ is smaller than $d_{IF_{dft}}$, and vice versa. This compensation within each instance deceives detection schemes that monitor the accumulated values of performance parameters such as the total nozzle travel and toolpath.

Algorithm 1 specifies the infill lines spacing and infill vertices spacing attacks.

## 4. Attack Implementation

The performance of the infill lines spacing and infill vertices spacing attacks at various attack magnitudes was evaluated on objects produced by an Ultimaker-3 fused filament fabrication printer. The printed objects were ASTM D638 Type IV standard tensile bars printed using polylactic

**Algorithm 1**: Infill lines spacing and infill vertices spacing attacks.

```
Input: G-code$_{Original}$
Input: Layers$_{Attacked}$
Input: Loc$_{Attacked}$
Input: Magnitude ($A_m$)
Output: G-code$_{Attacked}$
while $Location_{Attacked} \notin$ Infill-structure do
    Shift_location
end
Compute $A_{m_{max}}$ based on segment length, filament consumption and
        maximum attack magnitude
if $A_m > A_{m_{max}}$ then
    $A_m \leftarrow A_{m_{max}}$
end
for $\forall i \in Layers_{Attacked}$ do
    Seg$_1$ ← Nearest connecting segment to Loc$_{Attacked}$
    Attack 1: Displace two consecutive infill lines
            Compute new x and y coordinates such that there are
            no changes to the slopes of all the infills and segments
    $|d_{S_1}| \leftarrow |d_{S_1}| - |A_m|$
    $|d_{S_2}| \leftarrow |d_{S_2}| + |A_m|$
    $|d_{S_3}| \leftarrow |d_{S_3}| - |A_m|$
    No changes to $|Infill_1|$ and $|Infill_2|$
    for $\forall i \in$ Attacked commands do
        modified_G-code ← compute_new_G-code(i)
    end
    Attack 2: Displace two consecutive infill vertices
            Compute new x and y coordinates such that there are
            no changes to the slopes of the old and new segments
            (Infill line slopes change slightly)
    $|d_{S_1}| \leftarrow |d_{S_1}| - |A_m|$
    No change to $|d_{S_2}|$
    $|d_{S_3}| \leftarrow |d_{S_3}| - |A_m|$
    (Infill lines magnitude changes slightly)
    for $\forall i \in$ Attacked commands do
        modified_G-code ← compute_new_G-code(i)
    end
end
G-code$_{Attacked}$ ← update_G-code(G-code$_{Original}$, modified_G-code)
return G-code$_{Attacked}$
```

acid polymer. The printer was controlled by Ultimaker Cura software version 4.10, which also served as the slicer software. Table 1 specifies the printing parameters.

Five attacked specimens were printed for each variant of the two types of attacks along with two sets of five reference (non-attacked) specimens. Specimens corresponding to each attack type were printed using a differ-

*Table 1.* Printing parameters.

| **Printing Parameter** | **Value** |
|---|---|
| Layer Thickness | 0.2 mm |
| Nozzle Diameter | 0.4 mm |
| Build Plate Temperature | $60^o$C |
| Nozzle Temperature – Layer 1 | $210^o$C |
| Nozzle Temperature – Layer 2 Onwards | $205^o$C |
| Infill Pattern | Lines at $45^o$ |
| Infill Percentage | 100% |
| Number of Layers | 20 |
| Printing Speed – Layer 1 | 20 mm/s |
| Printing Speed – Layer 2 Onwards | 45 mm/s |
| Top and Bottom Layers | 0 |
| Number of Walls | 2 |

ent polymer spool with a different color primarily to address availability issues. The reference specimens were printed using each spool and their test results were used to gauge the attack impacts. This arrangement did not affect the study results.

Non-destructive tests included measurements, optical microscopy and micro-computed tomography (micro-CT) imaging. Destructive tensile tests performed using MTS Insight 30 equipment enabled the evaluation of the impacts of the attacks on the mechanical strength of the printed parts.

## 4.1 Attack Overview

The malicious actor is assumed to be an insider with local area network access, but is not authorized to access the printer control computer. Since the printer and control computer employ an unencrypted communications channel, the malicious actor chooses to obtain a man-in-the-middle position using ARP poisoning. Figure 6 shows an attack scenario in which the legitimate communications channel between a client and the printer is interrupted and routed through the malicious actor's machine. When the authorized client sends a print request to the printer, the malicious actor's code receives the original G-code file, computes the attacks, modifies the G-code and sends the modified G-code file to the printer. The sub-second delay introduced by the attack is imperceptible to the authorized client in a practical additive manufacturing environment.

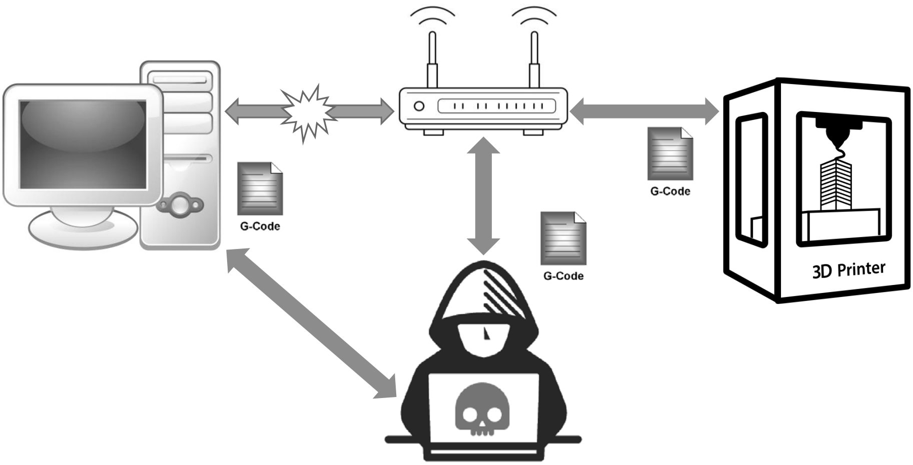


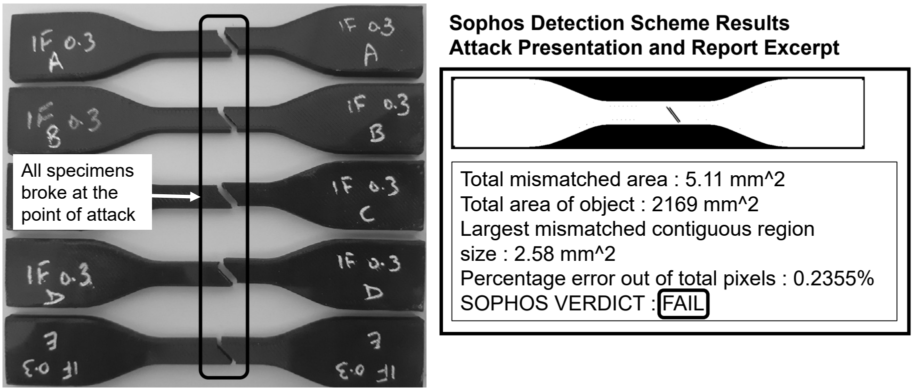
*Figure 6.* Attack scenario using a MitM position to sabotage a G-code file.

## 4.2 Attack Plan

The infill attacks were targeted at the central portions of the internal layers of the tensile bar specimens. The unmodified lengths of the infill lines $d_{IF_{dft}}$ and connecting segments $d_{S_{dft}}$ were 6.54 mm and 0.594 mm, respectively. The attacks involved two phases:

- **Phase 1:** The first phase established the maximum attack magnitude that enables an attack to evade detection. Since it was infeasible to implement all the attack detection techniques mentioned in the literature, the Sophos tool that identifies sub-millimeter variations was employed [23]. Infill lines spacing attacks starting with an initial maximum attack magnitude $A_{m_{max}}$ of 0.3 mm infill lines (IFLs) spacing were conducted. The attack magnitude was reduced over several iterations until Sophos was unable to reliably detect the deviations. The stealthiness and impacts of the attacks were evaluated by performing measurements, visual inspections, micro-CT scans and tensile strength tests.

  No measurement changes or visual deformations were observed on the attacked printed parts. The tensile tests showed consistent and significant reductions in part strength and all the attacked specimens broke at the point of attack. However, Sophos successfully detected the infill lines spacing attack with a 0.3 mm magnitude at every attacked layer. Figure 7 shows the attacked specimens and the Sophos verdict about a specimen.



**Sophos Detection Scheme Results**
**Attack Presentation and Report Excerpt**

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

*Figure 7.* Phase 1 attacked specimens and detection results.

*Table 2.* Phase 1 measurements and tensile test results for the attacked specimens.

| | **Average of Five Specimens** | **Standard Deviation** | **Difference from Normal 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% |
| Young's Modulus (MPa) | 1,246.074 | 136.373 | –418.399 | –33.58% |

Table 2 presents the measurements and tensile test results for the attacked specimens, including a greater than 50% reduction in tensile strength. The micro-CT scan identified an anomaly (slit) in the affected layers. Because the 0.3 mm attack magnitude could not evade detection by Sophos, the attack does not satisfy the third success criterion and is, therefore, considered unsuccessful. However, reducing the attack magnitude to 0.2 mm enabled the attack to evade detection by Sophos. Therefore, the maximum attack magnitude $A_{m_{max}}$ was set to 0.2 mm in the experiments.

- **Phase 2:** The second phase executed attacks with magnitudes ranging from 0.2 mm to 0.015 mm in five steps. Although all the attacks evaded detection, the stealthiness of the attacks increased as their magnitudes reduced. Six types of specimens were printed for each of the two infill spacing attacks, making a total of 60 specimens. Dimensional verification and visual inspection were

*Table 3.* Phase 2 infill structure manipulation attack details.

| **Attack Magnitude** | **Infill Lines Specimens** | **Spacing Attacks Attack Location** | **Infill Vertices Specimens** | **Spacing Attacks Attack Location** |
|---|---|---|---|---|
| No Attack | 5 | NA | 5 | NA |
| 0.015 mm | 5 | 6 IFLs from center | 5 | Center |
| 0.025 mm | 5 | 6 IFLs from center | 5 | Center |
| 0.050 mm | 5 | Center | 5 | 4 IFLs from center |
| 0.100 mm | 5 | Center | 5 | 4 IFLs from center |
| 0.200 mm | 5 | 4 IFLs from center | 5 | 4 IFLs from center |

performed on all the specimens, but micro-CT scans were performed only for certain specimens. Table 3 presents the attack details.

## 5. Evaluation Results

This section analyzes the experimental data in accordance with the five attack success criteria. All the attacks were launched after Stage 3 of the additive manufacturing process chain and none of the attacks created perceptible deformations to the final printed objects. Thus, the first and fourth attack success criteria were met by all the attacks. The footprints produced by the attacks in Phase 2 were small enough to bypass detection schemes, although the micro-CT scans revealed the presence of structural anomalies. As the attack magnitude was reduced, the impact on the mechanical strength was also reduced, providing a minimum effective deviation threshold value for successful attacks. The experimental data was examined in terms of stealthiness and effectiveness (mechanical strength impacts).

### 5.1 Stealthiness Performance

Attacks on the additive manufacturing process chain can be detected by a broad spectrum of methods, including visual inspection, dimension measurement, microscopic surface analysis, computer tomography, toolpath verification and others. Bulk parameters, such as the total printing time, total filament consumption and outer part dimensions, provide cumulative insights into the additive manufacturing process. Localized parameters, such as toolpath deviations, G-code command execution time and printing speed profile, offer instantaneous estimates of an additive manufacturing process.

**Bulk Parameters.** Table 4 presents the stealthiness performance of the attacks assessed using bulk parameters. The bulk parameters include the printing time per attacked layer, printed part dimensions and visual deformations. The maximum printing time variation for the attacks was within 14 ms of the mean value of the non-attacked specimens. The dimensions of the printed parts did not change – the maximum mean difference along each dimension of the attacked specimens was less than 0.036 mm, well within the printer accuracy tolerance. The dimension measurements of the attacked specimens fell on both sides of the mean values of the non-attacked specimens and were all within one standard deviation. No deformations were observed on the objects during naked eye inspections and optical microscope examinations.

**Localized Parameters.** Since some of the attack detection schemes monitor additive manufacturing processes continuously in the time and space domains to identify anomalies, it was important to assess the attack footprints with respect to localized or instantaneous process deviations.

Table 5 shows the performance with respect to the localized parameters. The parameters include the attack launch time delay, toolpath distance and direction (angle) deviations, and execution time and filament consumption per G-code command. The attack launch time delay is a key stealthiness performance parameter because a large delay in receiving an acknowledgement to a printing request could raise an attack alert. Detailed manual analyses of micro-CT scans were also conducted to identify the attacked areas in the printed parts.

The results reveal that the attack launch time delays were under 150 ms for all the attacks. The largest toolpath deviation per G-code command was just 0.2 mm for the infill lines spacing attacks. For the infill vertices spacing attacks, the largest toolpath deviation was 0.2 mm for the connecting segment and 0.143 mm for the corresponding infill line. The angular deviation was zero for the infill lines spacing attacks and a maximum of $1.21^o$ for the infill vertices spacing attacks. The maximum G-code execution time deviation was less than 5 ms. For the selected sampling rate of 200 samples/s, the time deviation resolution of the measurements was 5 ms. Although the attacks had different time variations within the 5 ms interval, the values were below existing attack detection thresholds. None of the attacks produced deviations in the filament consumption per command values.

The microstructures of the 3D printed specimens were evaluated using x-ray micro-computed tomography. A Skyscan 1173 machine was employed to recreate the 3D models. Micro-CT analysis was performed

*Table 4.* Stealthiness performance (bulk parameters).

| Attack | Printing Time per | | Printed Part Dimensions | | | | Visual |
|---|---|---|---|---|---|---|---|
| Magnitude | Attacked Layer (s) | | (Complete Printed Parts) | | | | Deformations |
| | Ave. | Std. Dev. | Width (mm) | | Thickness (mm) | | |
| | | | Ave. | Std. Dev. | Ave. | Std. Dev. | |
| *Infill Lines Spacing Attacks* | | | | | | | |
| No Attack | 61.513 | 0.000 | 6.582 | 0 | 4.088 | 0 | None |
| 0.015 mm | 61.518 | 0.005 | 6.580 | 0.002 | 4.080 | 0.008 | None |
| 0.025 mm | 61.520 | 0.008 | 6.568 | 0.014 | 4.090 | –0.002 | None |
| 0.050 mm | 61.523 | 0.010 | 6.568 | 0.014 | 4.083 | 0.005 | None |
| 0.100 mm | 61.521 | 0.009 | 6.570 | 0.012 | 4.090 | –0.002 | None |
| 0.200 mm | 61.526 | 0.014 | 6.563 | 0.019 | 4.085 | 0.003 | None |
| *Infill Vertices Spacing Attacks* | | | | | | | |
| No Attack | 61.513 | 0.000 | 6.582 | 0 | 4.088 | 0 | None |
| 0.015 mm | 61.525 | 0.012 | 6.562 | 0.020 | 4.086 | 0.002 | None |
| 0.025 mm | 61.525 | 0.012 | 6.592 | –0.010 | 4.084 | 0.004 | None |
| 0.050 mm | 61.521 | 0.009 | 6.546 | 0.036 | 4.064 | 0.024 | None |
| 0.100 mm | 61.523 | 0.010 | 6.580 | 0.002 | 4.078 | 0.010 | None |
| 0.200 mm | 61.520 | 0.008 | 6.584 | –0.002 | 4.086 | 0.002 | None |

*Table 5.* Stealthiness performance (localized parameters).

| Attack | Launch | Toolpath Deviation | | Max Time | Filament | Micro-CT Scan |
|---|---|---|---|---|---|---|
| Magnitude | Time | per IF Line Cmd | Max | Deviation | Deviation | Manual |
| | Delay | Distance | Angle | per Command | per Command | Detection |
| | (s) | (mm) | (deg) | (ms) | (mm) | |
| *Infill Lines Spacing Attacks* | | | | | | |
| 0.015 mm | 0.15 | 0.015 | 0 | < 5 | None | Negative |
| 0.025 mm | 0.15 | 0.025 | 0 | < 5 | None | Negative |
| 0.050 mm | 0.15 | 0.050 | 0 | < 5 | None | Positive |
| 0.100 mm | 0.15 | 0.100 | 0 | < 5 | None | Positive |
| 0.200 mm | 0.15 | 0.200 | 0 | < 5 | None | Positive |
| *Infill Vertices Spacing Attacks* | | | | | | |
| 0.015 mm | 0.15 | 0.011 | 0.093 | < 5 | None | Negative |
| 0.025 mm | 0.15 | 0.018 | 0.154 | < 5 | None | Negative |
| 0.050 mm | 0.15 | 0.035 | 0.308 | < 5 | None | Negative |
| 0.100 mm | 0.15 | 0.071 | 0.612 | < 5 | None | Probable |
| 0.200 mm | 0.15 | 0.143 | 1.211 | < 5 | None | Positive |

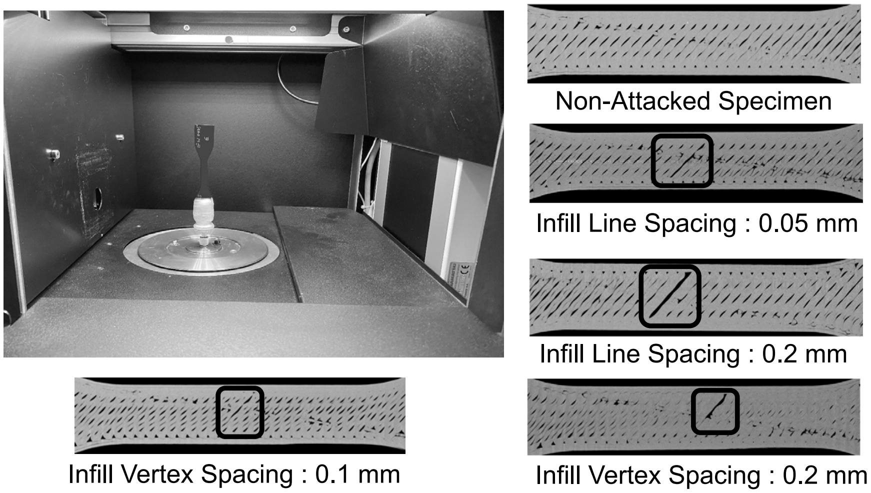

Non-Attacked Specimen
Infill Line Spacing : 0.05 mm
Infill Line Spacing : 0.2 mm
Infill Vertex Spacing : 0.1 mm
Infill Vertex Spacing : 0.2 mm

*Figure 8.* Micro-CT scan results for selected attack specimens.

at 40 kV, 200 $\mu$A, 1,800 ms exposure, 0.5 rotational step and 20 $\mu$m pixel size. The scanned raw data was reconstructed using N-Recon software version 1.7.4.4. Volumes of interest were defined in the 3D reconstructed coronal image views and the images were subsequently analyzed using data viewing software.

Micro-CT analysis detected infill lines spacing attacks with magnitudes of 0.05 mm and higher. However, it did not reveal any signs of infill vertices attacks at a magnitude of 0.05 mm and only a hint of a probable attack at a magnitude of 0.1 mm. At the 0.2 mm magnitude, the infill vertices spacing attack was clearly visible in the micro-CT scan. As the attack magnitude increased, micro-CT analysis identified the attacked area with higher confidence. Figure 8 shows the micro-CT equipment employed along with selected attack specimens.

## 5.2 Mechanical Strength Impacts

Tensile tests were employed to evaluate the impacts of attacks on the mechanical strength of printed specimens. The tests were conducted using an MTS-Insight 30 tensile testing machine. Not all the attacks were consistently effective at reducing the tensile strength or load-extension profiles. All the attacked specimens broke at the point of attack for attack magnitudes above 0.05 mm. Figure 9 shows sample attacked specimens after the tensile tests.

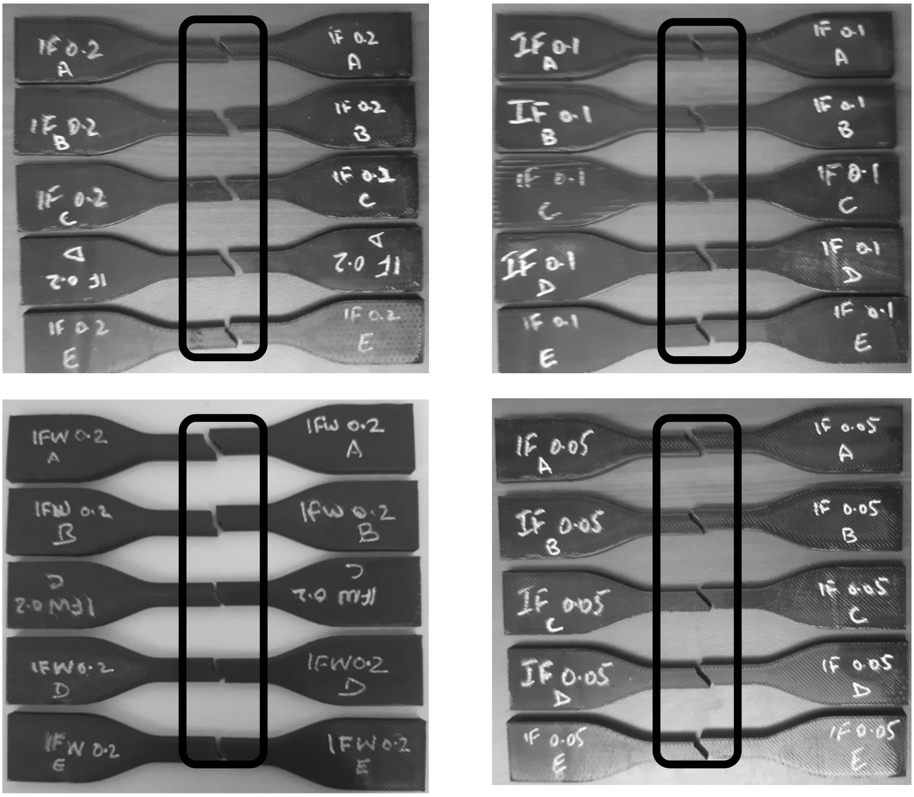


*Figure 9.* Broken tensile test specimens at attack magnitudes above 0.05 mm.

Tables 6 and 7 show the tensile test results for non-attacked specimens and specimens exposed to infill lines spacing and infill vertices spacing attacks, respectively. The maximum reductions in the peak loads of the attacked specimens were 33.55% for infill lines spacing attacks and 11.57% for infill vertices spacing attacks.

Figures 10 and 11 show the stress-strain curves for infill lines spacing and infill vertices spacing attack specimens, respectively. Most of the infill lines spacing and infill vertices spacing attack specimens broke earlier in the load versus time (stress-strain) curves compared with the non-attacked specimens. The Young's modulus decreased for the infill lines spacing attack specimens. However, the variations were not as consistent and pronounced for the infill vertices spacing attacks.

*Table 6.* Tensile test results for infill lines spacing attacks.

| **Attack** | **Peak Load (N)** | | | **Peak Stress (MPa)** | | | **Young's Modulus (MPa)** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Magnitude** | **Ave.** | **Std. Dev.** | **Diff.** | **Ave.** | **Std. Dev.** | **Diff.** | **Ave.** | **Std. Dev.** | **Diff.** |
| No Attack | 936.94 | 98.78 | 0.00% | 35.45 | 3.45 | 0.00% | 1,730.22 | 167.85 | 0.00% |
| 0.015 mm | 938.09 | 40.86 | 0.12% | 35.49 | 1.65 | 0.12% | 1,708.45 | 75.17 | –1.26% |
| 0.025 mm | 919.89 | 35.68 | –1.82% | 34.37 | 1.55 | –3.06% | 1,756.83 | 42.87 | 1.54% |
| 0.050 mm | 694.75 | 18.01 | –25.85% | 25.93 | 0.68 | –26.87% | 1,267.56 | 106.84 | –26.74% |
| 0.100 mm | 622.57 | 34.66 | –33.55% | 23.17 | 1.39 | –34.65% | 1,498.47 | 147.25 | –13.39% |
| 0.200 mm | 624.32 | 32.57 | –33.37% | 23.28 | 1.29 | –34.34% | 1,323.59 | 107.12 | –23.50% |

*Table 7.* Tensile test results for infill vertices spacing attacks.

| **Attack** | **Peak Load (N)** | | | **Peak Stress (MPa)** | | | **Young's Modulus (MPa)** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Magnitude** | **Ave.** | **Std. Dev.** | **Diff.** | **Ave.** | **Std. Dev.** | **Diff.** | **Ave.** | **Std. Dev.** | **Diff.** |
| No Attack | 1,036.11 | 42.45 | 0.00% | 38.60 | 1.54 | 0.00% | 1,771.42 | 129.52 | 0.00% |
| 0.015 mm | 1,054.48 | 30.37 | 1.77% | 39.33 | 1.35 | 1.88% | 1,850.70 | 168.24 | 4.48% |
| 0.025 mm | 1,041.91 | 59.80 | 0.56% | 38.70 | 2.41 | 0.26% | 2,052.87 | 116.97 | 15.89% |
| 0.050 mm | 1,008.68 | 39.05 | –2.65% | 37.92 | 1.28 | –1.76% | 1,901.28 | 44.97 | 7.33% |
| 0.100 mm | 953.37 | 44.39 | –7.99% | 35.52 | 1.76 | –7.98% | 1,726.44 | 163.31 | –2.54% |
| 0.200 mm | 916.28 | 36.46 | –11.57% | 34.06 | 1.19 | –11.76% | 1,796.00 | 261.93 | 1.39% |

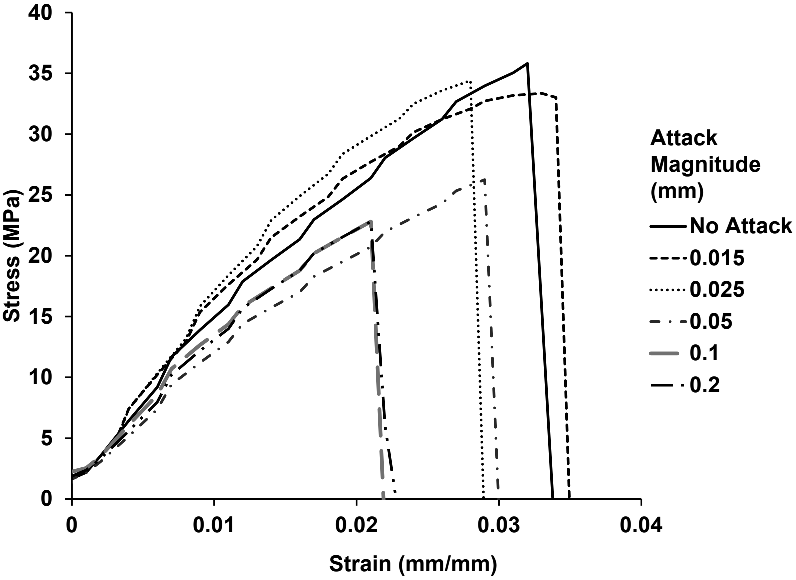


*Figure 10.* Stress-strain curves for infill lines spacing attack specimens.

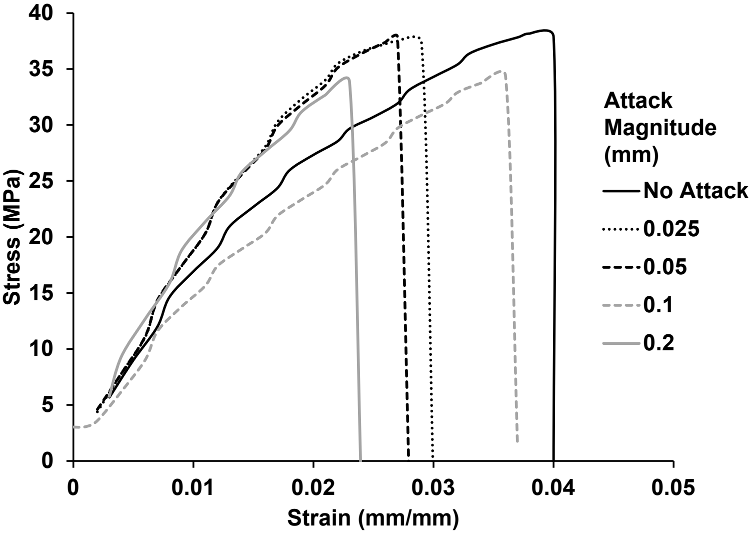


*Figure 11.* Stress-strain curves for infill vertices spacing attack specimens.

## 6. Analysis and Discussion

Conducting an attack on a design file is a pure cyber-domain modification that can be detected by conventional cyber security methods such

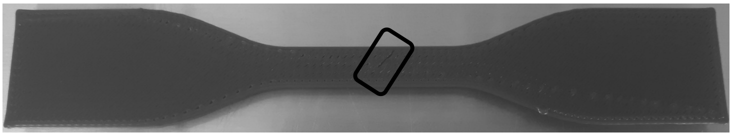


*Figure 12.* Detection of a 0.2 mm magnitude infill vertices spacing attack.

as file hashing and operating system audit logs. However, the infill modification attacks launched between the control computer (excluded) and printer (included) bypassed cyber-domain operating systems and standard security tools. A recent study by McCormack et al. [13] revealed that 12 out of 13 surveyed printing environments did not use encrypted communications between the control computers and printers, exposing them to man-in-the-middle attacks.

The low-magnitude infill modification attacks created footprints smaller than the reported resolutions of attack detection schemes that monitor printing processes. The attack magnitudes were also within the order of fused filament fabrication printer accuracy, which would pose challenges to threshold-based detection methodologies. Although, all the infill modification attacks were concealed in the final printed objects, the effects of higher magnitude attacks were somewhat visible during printing. As shown in Figure 12, a continuous imaging technique can detect the anomalies induced by attacks. Specifically, the image taken after pausing the process when printing an attacked layer revealed the inverse-wedge-shaped cavity. Very low magnitude attacks – up to 0.025 mm for infill lines spacing attacks and up to 0.05 mm for infill vertices spacing attacks – had limited impacts on the physical strength of attacked parts.

For identical attack magnitudes, infill lines spacing attacks were more damaging than infill vertices spacing attacks. Figures 13 and 14 show the strength vs. attack magnitude plots for infill lines spacing and infill vertices spacing attacks, respectively. The two types of attacks exhibit different strength-reduction profiles based on the attack magnitudes. Infill lines spacing attacks have a peak impact zone between attack magnitudes of 0.35 mm and 0.1 mm. In contrast, the peak impact zone for infill vertices spacing attacks is between 0.05 mm to about 0.1 mm and has a gradual reduction thereafter. In an infill lines spacing attack, the separation of two adjacent infill lines is increased from end to end. In an infill vertices spacing attack, the separation between two adjacent infill lines is increased only at one end, resulting in increased bonding and overlap between the two lines as they progress from the point of attack

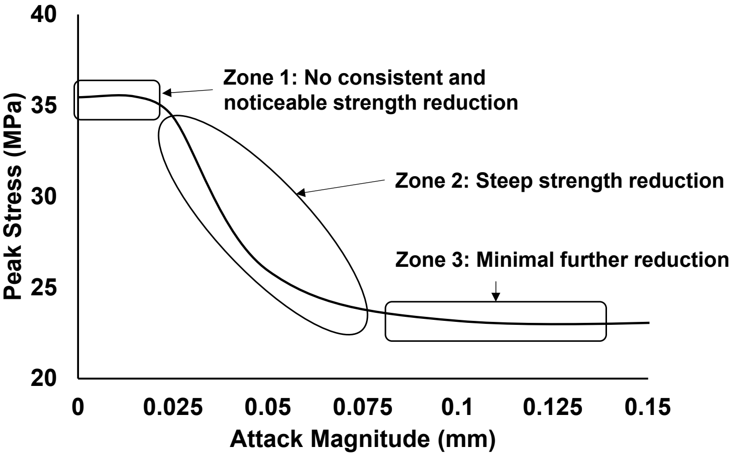


*Figure 13.* Strength vs. attack magnitude plot for infill lines spacing attacks.

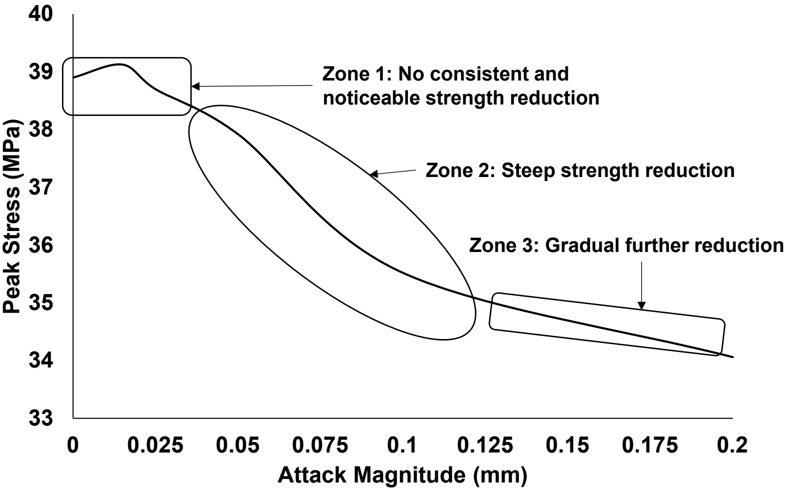


*Figure 14.* Strength vs. attack magnitude plot for infill vertices spacing attacks.

towards the other vertex. This explains the lower strength reduction and shifted impact zone in the case of infill vertices spacing attacks.

The micro-CT analysis revealed that non-attacked printed objects with 100% infill density also contained tiny gaps between the infill structure and surrounding walls, and within the infill structure. Optimizing the printing parameters could remove these gaps and also increase the overlaps of infill lines. In such cases, the attacks would be more interesting and more pronounced. Although the optimization of printing parameters is not considered in this work, it is important to note that this finding impacts the choices made by a malicious actor. Interestingly, when micro-CT analysis confirmed the presence and location of an attack, destructive tests also showed reductions in part strength. For a 20-layer object with around 200 cross-sectional images, a micro-CT scan can capture the structural weakness due to a single attacked layer, making it an important tool for detecting microstructural attacks.

A limitation of the infill lines spacing and infill vertices spacing attacks is that they effectively target only solid-filled objects. In a variation of these attacks, the infill connecting segments may be made to drift slightly in order to weaken the bonds between the infill and walls. These weaknesses would reduce the compression strength and shear strength of a part with a minimal attack footprint.

In a low-magnitude sabotage attack, a malicious actor would target one or more physical properties of the printed object. Since most detection techniques compare actual process behavior against true or expected behavior, a low-magnitude attack can evade detection. Instead of mapping the space, thermal and timing profiles of a printer to the expected state, a different detection approach is to estimate the potential targeted physical properties. For example, a small variation at one location may be safely ignored, but it could induce high residual stress at another location. A detection scheme that considers this phenomenon can be more effective at distinguishing between damaging low-magnitude attacks and benign printing errors.

## 7. Attack Countermeasures

This section discusses two categories of countermeasures for the low-magnitude infill spacing attacks described in this chapter.

The first category of countermeasures focuses on attack avoidance. Controlling physical access to a printing facility reduces the probability that malicious code would make its way through physical printer ports. Implementing authenticated and encrypted communications between the control computer and printer would significantly hinder man-in-the-middle attacks. Techniques such as DHCP snooping and ARP inspection would help prevent ARP table manipulation. Researchers have proposed several techniques for countering network layer attacks in cyber-physical environments [1, 11]. Reverse engineering application layer transactions in network traffic is also helpful in detecting anomalies [19]. To avoid attacks from compromised printer firmware, the firmware should be verified periodically. Instead of inline firmware acquisition, researchers have proposed out-of-band methods for securely acquiring memory content for embedded systems [20] and extracting running firmware [21, 26].

The second category of countermeasures focuses on attack detection. If a malicious actor succeeds in launching an attack, micro-CT scans can identify a potent structural abnormality caused by the attack. However, the time and manual effort required to perform micro-CT scans and analyze them do not render this a scalable solution. Although some implementation challenges exist, in-printing scanning with an automated anomaly detection function is more feasible in a busy printing facility. While micro-CT scans are far more detailed, high-speed in-printing optical imaging may still be useful for detecting structural non-conformity.

## 8. Conclusions

This research has developed two low-magnitude infill structure manipulation attacks on objects created by fused filament fabrication printers. An infill lines spacing attack reduces the overlap between two consecutive infill lines at the target location whereas an infill vertices spacing attack creates an inverse-wedge-shaped low-density zone at the target location. The magnitudes of the infill structure manipulation attacks are maintained below the horizon of existing detection methods as well as within the resolution and trueness tolerances of fused filament fabrication printers. The attacks were executed on solid-filled ASTM D638 type-IV tensile bars by manipulating G-code commands corresponding to attack locations in selected internal layers. Tensile tests conducted on the attacked specimens demonstrate that attacks with magnitudes of just 0.05 mm can reduce the mechanical strength of printed parts. Such attack magnitudes are within the confusion zones of detection schemes that only monitor printer actions against printing commands. However, if an attack detection scheme can obtain adequate physical property estimates for current process states, attacked specimens can be distinguished from random printing errors. Another scheme for detecting low-magnitude attacks is to incorporate automated real-time analysis of micro-CT scans to identify structural abnormalities in attacked parts.

## Acknowledgement

This research was partially supported by the Virginia Commonwealth Cyber Initiative.

## References

[1] H. Adjei, T. Shunhua, G. Agordzo, Y. Li, G. Peprah and E. Gyarteng, SSL stripping technique (DHCP snooping and ARP spoofing inspection), *Proceedings of the Twenty-Third International Conference on Advanced Communication Technology*, pp. 187–193, 2021.

[2] A. Ayub, H. Yoo and I. Ahmed, Empirical study of PLC authentication protocols in industrial control systems, *Proceedings of the IEEE Security and Privacy Workshops*, pp. 383–397, 2021.

[3] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh and Y. Elovici, Digital audio signature for 3D printing integrity, *IEEE Transactions on Information Forensics and Security*, vol. 14(5), pp. 1127–1141, 2018.

[4] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin and Y. Elovici, dr0wned – Cyber-physical attack with additive manufacturing, presented at the *Eleventh USENIX Workshop on Offensive Technologies*, 2017.

[5] S. Chhetri, A. Canedo and M. Al Faruque, KCAD: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems, *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, 2016.

[6] U. Dilberoglu, B. Gharehpapagh, U. Yaman and M. Dolen, The role of additive manufacturing in the era of Industry 4.0, *Procedia Manufacturing*, vol. 11, pp. 545–554, 2017.

[7] Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou and Z. Jin, Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2(3), article no. 108, 2018.

[8] G. Goh, S. Sing and W. Yeong, A review of machine learning in 3D printing: Applications, potential and challenges, *Artificial Intelligence Review*, vol. 54(1), pp. 63–94, 2021.

[9] J. Hanssen, Fortus 360mc/400mc Accuracy Study, Stratasys, Eden Prairie, Minnesota (`nanopdf.com/download/fortus-360mc-400mc-accuracy-study_pdf`), 2013.

[10] S. Kim, Y. Shin, H. Jung, C. Hwang, H. Baik and J. Cha, Precision and trueness of dental models manufactured with different 3-dimensional printing techniques, *American Journal of Orthodontics and Dentofacial Orthopedics*, vol. 153(1), pp. 144–153, 2018.

[11] Y. Li, L. Zhu, H. Wang, F. Yu and S. Liu, A cross-layer defense scheme for edge-intelligence-enabled CBTC systems against MitM attacks, *IEEE Transactions on Intelligent Transportation Systems*, vol. 22(4), pp. 2286–2298, 2021.

[12] Markets and Markets, 3D Printing Market by Offering (Printer, Material, Software, Service), Process (Binder Jetting, Direct Energy Deposition, Material Extrusion, Material Jetting, Powder Bed Fusion), Application, Vertical, Technology and Geography (2021–2026), Market Research Report SE 2936, Northbrook, Illinois (`www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html`), 2021.

[13] M. McCormack, S. Chandrasekaran, G. Liu, T. Yu, S. DeVincent Wolf and V. Sekar, Security analysis of networked 3D printers, *Proceedings of the IEEE Security and Privacy Workshops*, pp. 118–125, 2020.

[14] S. Moore, W. Glisson and M. Yampolskiy, Implications of malicious 3D printer firmware, *Proceedings of the Fiftieth Hawaii International Conference on System Sciences*, 2017.

[15] B. Msallem, N. Sharma, S. Cao, F. Halbeisen, H. Zeilhofer and F. Thieringer, Evaluation of the dimensional accuracy of 3D-printed anatomical mandibular models using FFF, SLA, SLS, MJ and BJ printing technology, *Journal of Clinical Medicine*, vol. 9(3), article no. 817, 2020.

[16] H. Pearce, K. Yanamandra, N. Gupta and R. Karri, FLAW3D: A Trojan-Based Cyber Attack on the Physical Outcomes of Additive Manufacturing, arXiv: 2104.09562 (`arxiv.org/abs/2104.09562`), 2021.

[17] S. Qasim, A. Ayub, J. Johnson and I. Ahmed, Attacking the IEC-61131 logic engine in programmable logic controllers, in *Critical Infrastrucure Protection XV*, J. Staggs and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 73–95, 2022.

[18] S. Qasim, J. Lopez and I. Ahmed, Automated reconstruction of control logic for programmable logic controller forensics, in *Information Security*, Z. Lin, C. Papamanthou and M. Polychronakis (Eds.), Springer, Cham, Switzerland, pp. 402–422, 2019.

[19] S. Qasim, J. Smith and I. Ahmed, Control logic forensics framework using a built-in decompiler of engineering software in industrial control systems, *Forensic Science International: Digital Investigation*, vol. 33(S), article no. 301013, 2020.

[20] M. Rais, R. Awad, J. Lopez and I. Ahmed, JTAG-based PLC memory acquisition framework for industrial control systems, *Forensic Science International: Digital Investigation*, vol. 37(S), article no. 301196, 2021.

[21] M. Rais, R. Awad, J. Lopez and I. Ahmed, Memory forensic analysis of a programmable logic controller in industrial control systems, *Forensic Science International: Digital Investigation*, vol. 40(S), article no. 301339, 2022.

[22] M. Rais, Y. Li and I. Ahmed, Dynamic thermal and localized filament kinetic attacks on a fused-filament-fabrication-based 3D printing process, *Additive Manufacturing*, vol. 46, article no. 102200, 2021.

[23] M. Rais, Y. Li and I. Ahmed, Spatiotemporal G-code modeling for secure FDM-based 3D printing, *Proceedings of the Twelfth ACM/IEEE International Conference on Cyber-Physical Systems*, pp. 177–186, 2021.

[24] D. Roach, C. Roberts, J. Wong, X. Kuang, J. Kovitz, Q. Zhang, T. Spence and H. Qi, Surface modification of fused filament fabrication (FFF) 3D printed substrates by inkjet printing polyimide for printed electronics, *Additive Manufacturing*, vol. 36, article no. 101544, 2020.

[25] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems, *Proceedings of the International Solid Freeform Fabrication Symposium*, pp. 951–963, 2014.

[26] S. Vasile, D. Oswald and T. Chothia, Breaking all the things – A systematic survey of firmware extraction techniques for IoT devices, in *Smart Card Research and Advanced Applications*, B. Bilgin and J. Fischer (Eds.), Springer, Cham, Switzerland, pp. 171–185, 2019.

[27] M. Wu, H. Zhou, L. Lin, B. Silva, Z. Song, J. Cheung and Y. Moon, Detecting attacks in cyber manufacturing systems: Additive manufacturing example, *Proceedings of the International Conference on Mechanical, Aeronautical and Automotive Engineering*, 2017.

[28] C. Xiao, Security attack on 3D printing, presented at the *xFocus Security Conference* (`www.claudxiao.net/Attack3DPrinting-Claud-en.pdf`), 2013.

[29] S. Zeltmann, N. Gupta, N. Tsoutsos, M. Maniatakos, J. Rajendran and R. Karri, Manufacturing and security challenges in 3D printing, *Journal of the Minerals, Metals and Manufacturing Society*, vol. 68(7), pp. 1872–1881, 2016.