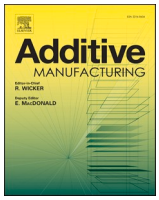
Additive Manufacturing 46 (2021) 102200

Contents lists available at ScienceDirect

Additive Manufacturing

journal homepage: www.elsevier.com/locate/addma



Research Paper

Dynamic-thermal and localized filament-kinetic attacks on fused filament fabrication based 3D printing process

Muhammad Haris Rais [a,*], Ye Li [b], Irfan Ahmed [a]

[a] Virginia Commonwealth University, USA
[b] Bradley University, USA

ARTICLE INFO

Keywords:
Additive manufacturing
Filament-kinetic attack
Thermodynamic attack
FDM
Cyber manufacturing
Cyberattack

ABSTRACT

3D printing materializes physical objects through sequentially depositing thin layers. The layer-by-layer stacking involves controlling 3D printing parameters (e.g., fan speed, nozzle temperature, printing bed temperature, and filament extrusion rate) to ensure conformity to a CAD (Computer-aided Design) model. Attackers target the parameters during a printing process to sabotage the printing object. This paper presents four new sabotage attacks on the fused filament fabrication (FFF)-based 3D printing process: (1) cavity through filament-kinetics, (2) density variation through filament state, (3) density variation through filament speed, and (4) dynamic-thermal manipulation. These attacks produce an insignificant attack footprint on a finished printed object by targeting localized regions or using small changes in temperature profile, making them hard to detect. Specifically, the first three attacks manipulate filament-kinetics to change the print density or create a cavity in a small localized region, while the fourth attack makes slight changes to the nozzle temperature to manipulate thermal stress in a printing object without creating any visual deformation. Mechanical (tensile and three-point bending) tests carried out on the objects under attack demonstrate that these attacks with insignificant attack footprints can still change the physical properties (e.g., stress and strain) of the printed objects.

1. Introduction

3D printing collectively refers to a group of manufacturing processes that materialize physical objects through sequentially depositing thin layers [1]. Although each process applies different physical/chemical interactions on the building materials, each layer is constructed using a predefined building direction and stacked sequentially based on a CAD (Computer-aided Design) model. The layer-by-layer stacking in a 3D printing process exposes it to a different set of vulnerabilities than other manufacturing processes, such as machining. Generally, attackers target a 3D printing process with one of the two objectives: (1) intellectual property theft, and (2) sabotage attack [2]. The seminal work of Farouque et al. [3] demonstrates intellectual property theft using side-channel acoustic signals by printer motors. On the other hand, sabotage attacks weaken, damage or destroy a 3D printed object by causing geometrical nonconformity and workpiece deformation [4]. This paper demonstrates and measures the effectiveness of new filament-kinetics and thermal stress-based sabotage attacks on the fused filament fabrication (FFF) based 3D printing process.

A FFF printer consists of a heated printing bed and a printhead that hosts one or more nozzles. The printhead moves in 2 dimensions (x and y axes) and simultaneously extrudes the filament to print a thin layer. Once a layer is completed, the bed moves down (z-axis) to create space for another layer to be printed on top of the previous layer. The movement path of the nozzle during the printing process is also referred to as "toolpath". Solid filament is fed to the nozzle where it is converted to molten state, and extruded out from the tip in synchronization with the nozzle movement. Usually, 4 different stepper motors are used to achieve the movement in x,y,z and filament axes.

Researchers have demonstrated that the object properties can be altered by manipulating the manufacturing parameters of a printing process such as object orientation [5], fan speed [6], nozzle temperature [7], printing bed temperature [8], and fusing material patterns [9]. Changing the printing parameters affect one or more of the three processes involved in FFF-based 3D printing i.e., nozzle-kinetics, filament-kinetics and thermodynamics. Up till now, the focus of attack detection research in additive manufacturing remains on the nozzle-kinetics [6,10–13]. Although, the adverse and conspicuous effects of manipulating filament-kinetic and thermodynamic profiles have been demonstrated over the entire object earlier (discussed ahead in

* Corresponding author.
E-mail addresses: raismh@vcu.edu (M.H. Rais), yli@bradley.edu (Y. Li), iahmed3@vcu.edu (I. Ahmed).

https://doi.org/10.1016/j.addma.2021.102200
Received 18 January 2021; Received in revised form 7 June 2021; Accepted 19 July 2021
Available online 27 July 2021

Section 2.2), the practicality of achieving inconspicuous and localized attacks that degrade the mechanical properties of the printed object is not yet explored.

This paper presents four new attacks in this direction on the FFF-based 3D printing process. The attacks are (1) cavity through filament-kinetics, (2) density variation through filament state, (3) density variation through filament speed and (4) dynamic-thermal manipulation. They are designed to produce an insignificant attack footprint (discussed in Section 5.1) on a finished printed object, making them hard to detect. Precisely, the first three attacks manipulate filament-kinetics to change the print density or create a cavity in a small localized region. The fourth attack makes small changes to the nozzle temperature to alter thermal stress profile of the printing object without creating any visual deformation.

We implement the attacks over PLA (Polylactic Acid) printed rectangular-bars and perform the tensile and three-point bending tests to evaluate both attacked and benign specimens. The evaluation results find that the attacked bars show a noticeable deviation in physical properties such as peak load, flexure stress, and strain. Note that the attacks are generally applicable to all common FFF-based 3D printers that share same set of printing process parameters.

The contribution of the paper is three fold:- .

- We demonstrate new *localized filament-kinetic* attacks for cavity creation and density variation without changing the printing path sequence. Moore et al.'s work [14] is closest to our filament-kinetic attacks in that they modify the feed-rate parameter for the entire printing of an object. However, our localized filament-kinetic attacks target specific object region, with minimal to no change in object weight, center of gravity, dimensions, and nozzle kinetic process to achieve concealed internal cavities or density variations.
- We demonstrate new *dynamic-thermal* attacks that do not create any visual deformation. Claud et al.'s work [15] is closest to our dynamic-thermal attacks in that they increase the nozzle temperature for the entire printing process. However, our dynamic-thermal attacks use planned, localized, and minor modifications in the thermodynamic profile and further ensure invisible deformation.
- A subsequent question arises about the effectiveness of such inconspicuous and minute changes targeted at specific sub-processes. In our work, we show that such attacks are effective in modifying the mechanical properties of the object. Specifically, we perform mechanical (tensile and three-point bending) tests on 3D printing objects under attack to validate the impact of localized filament-kinetic and dynamic-thermal attacks on the physical properties (e.g., stress and strain) of the object.

2. Background and related work

2.1. 3D printing process chain

3D printing is a layer-by-layer manufacturing process that is substantially different from the traditional subtractive manufacturing technique. As described in the Fig. 1, the 3D printing process starts with creating a 3D model of the desired object in a computer-aided design (CAD) software. The model is converted to a geometry file in stereolithography (STL) format, which contains the outer surface information of the 3D object as a collection of small contiguous triangles. The STL file is passed to slicing software with the printing design parameters, such as the infill pattern, layer thickness, and temperature profile. The slicer software converts the STL file and the design parameters into a sequence of instructions, called G-codes. The G-code file is passed to the printer through a USB interface, SD-card, or network using a printer control software. The printer firmware interprets the G-code commands in the file and prints the object.

2.2. 3D printing sabotage attacks

Most of the existing attacks sabotage a 3D object by modifying the design files, i.e. the first stage of the process chain as shown in the Fig. 1. The changes in CAD file simultaneously modify the filament-kinetics and nozzle kinetics, resulting in bigger attack footprint easier to detect by existing techniques. The changes at the advanced level in the process chain, such as the G-code or firmware can manipulate only a specific sub-process resulting in smaller attack footprint. However, the existing work is only limited to manipulating nozzle kinetics during a printing

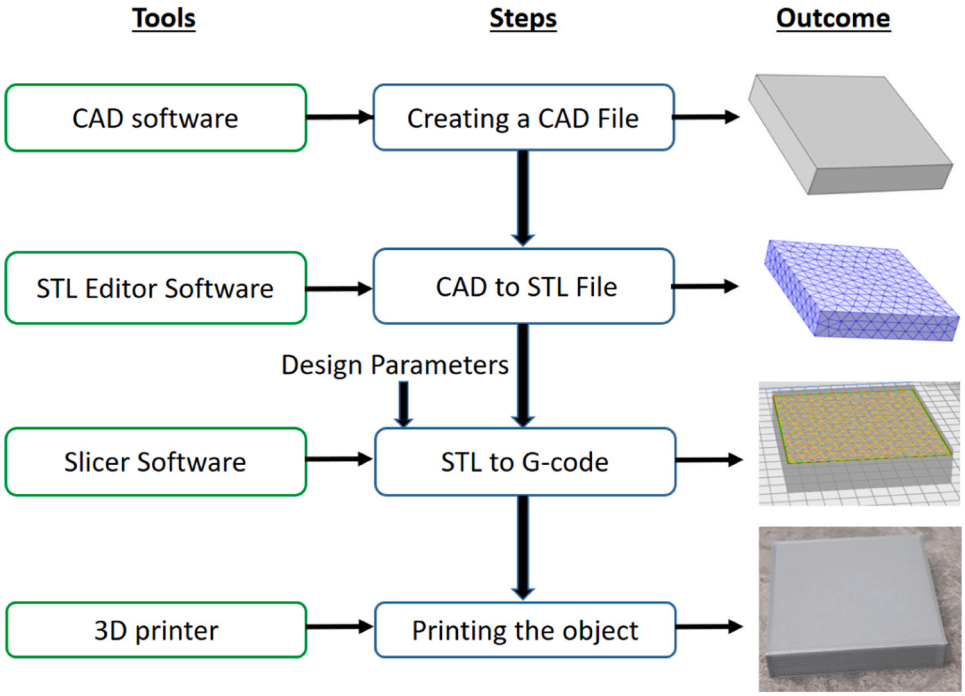


Fig. 1. 3D printing process chain.

process.

2.2.1. Design file modifications

Sturm et al. [16] manipulate the STL files to create denial of service, indents, scaling and void attacks without modifying printing parameters during a printing process. They present a case study of void attack by using heuristic rules to find a high impacting location in the object, and then creating an enclosed void.

Belikovetsky et al. [4] demonstrate an attack on a 3D-printed quadcopter propeller by reducing its fatigue life, which causes it to fail prematurely during mid-flight. Specifically, they target the joint connecting the blades to the cap of the propeller and introduce gaps between them. Apparently, the gaps weaken the mechanical strength below operational conditions and thus, cause the propeller to break within seconds of normal operation.

2.2.2. Nozzle kinetics

Zeltmann et al. [5] demonstrate a print orientation attack resulting in degradation of the mechanical properties of the printed object. Moore et al. [14] hijack the printer firmware and changes internal feed-rate variable by 10–40%, resulting in deformed printed object. The attack impact is visible, distributed over the entire object, and also changes the object's weight proportional to the modification percentage. Similarly, Claud et al. [15] hijack the printer firmware and increase the temperature variable value, while reporting the actual temperature.

3. Proposed sabotage attacks on FFF-based 3D printing

We present new *localized filament-kinetic* and *dynamic-thermal* attacks with an insignificant attack footprint (refer to Table 2) on a finished printed object. The attacks can modify the physical properties (e.g., peak load, flexure stress, and strain) of a target object.

3.1. Localized filament-kinetic attacks

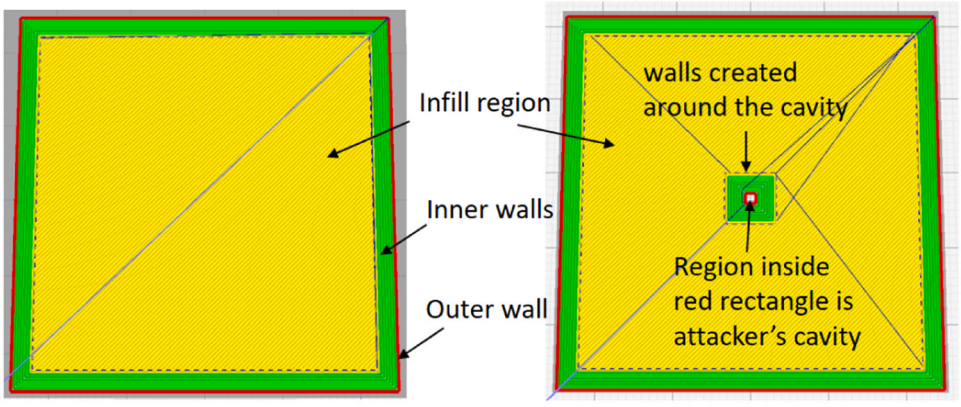
In FFF based 3D printer, a stepper motor (called filament motor) pushes the filament through the nozzle to extrude the material from the nozzle tip. The filament motor works synchronously with the printhead motors (x and y axes motors) to ensure a homogeneous print density across the entire object. We propose three attacks that manipulate this relation by briefly tweaking filament motor kinetics to target a small localized region of a 3D printing object. The attacks target the intermediate layers and are concealed by the unmodified top and bottom layers.

3.1.1. Cavity attack through filament-kinetics

This attack prevents the extrusion of the filament over the target area of an object to create cavity. It can be performed at any stage of the process chain. However, if the attack modifies the design file at CAD or STL stages, it will have a much bigger attack footprint than a cavity size. To illustrate further, consider the Fig. 2, where a cavity attack using a design file produces a refined cavity visible as a small square enclosed within red and green concentric squares.

When a slicer software finds a tiny cavity in an object's design, it creates inner and outer walls around it, similar to the object borders. In this attempt, the toolpath sequence is significantly disturbed and can be detected. For instance, the move instruction count in this example is increased from 164 to 218 per attacked layer, and the time to print is raised over 2 s for higher-speed upper layers and over 4 s for lower-speed starting layers. From the attacker's perspective, the effectiveness of a cavity protected by multiple protecting walls, is also questionable in reducing the object's physical properties.

Our proposed cavity attack is performed through filament-kinetics only, with minimal change in the move instructions (zero in most cases), no change in toolpath sequence, and minimal printing-time



(a) Actual Deign 5cm x 5cm x 1cm cube – single layer shown

(b) 1mm x 1mm cavity introduced in design

Impact on Printing-Per Layer Stats	(a) No Cavity	(b) Cavity via Design File
No of mov commands	164	218
Time taken (sec)	57	59
Sequence	Infill > object inner-walls > object outer-wall	Infill > cavity inner-walls > cavity outer-wall > object inner-walls > object outer-wall

Fig. 2. Cavity attack through STL or CAD file modification. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

difference from the original design. Due to the abrupt removal of material, the cavity through filament-kinetics does not create a well-designed structure, arguably increasing the chances of higher reduction in mechanical properties. Fig. 3 illustrates the modified G-code instructions as a sample for our cavity attack. There is no move instruction inclusion against the printing sequence. Three lines are added in the G-code for attacking a single move instruction (0.3–0.5 mm thickness). Modifying the G-code file is one way of launching this attack. If the attacker controls the firmware, the attack can be performed by controlling the motor directly.

3.1.2. Density variation through filament state attack

This attack manipulates the filament motor state (i.e. ON or OFF) to reduce the material density in an object's target region without disturbing nozzle kinetics and toolpath. To launch the attack, the filament motor state is changed to OFF. We observed that the switching OFF event gradually affects the target object due to residual filament available at the nozzle's tip that continues to extend the filament string. However, with the filament supply cut-off, the material density in that zone is less than the actual desired value. The situation is analogous to the last sentence written from the ink pen whose cartridge is detached. As the maximum impact occurs with a delay, the attack is initiated slightly earlier than the target area. To find the exact starting point, we consider two possible cases. In case I, the attack duration is much smaller than the time to completely dry out the residual filament as shown in Eq. (1).

$$\Delta t_{attack} = |t_{ON} - t_{OFF}| < (d_{res} / v_{nozzle}) \quad (1)$$

where Δt_{attack} is the attack duration, $t_{ON} and t_{OFF}$ are the filament motor's switching OFF and switching ON time, d_{res} is the distance to completely consume the residual filament and v_{nozzle} is the nozzle speed at that instance. In case II, the attack duration is comparable or greater than the time to consume the residual filament, as shown in Eq. (2).

$$\Delta t_{attack} = |t_{ON} - t_{OFF}| \geq (d_{res} / v_{nozzle}) \quad (2)$$

To calculate the maximum impact point of the attack, we investigate the value of d_{res}, which is a function of nozzle speed, nozzle temperature, material properties, max acceleration and jerk settings in the G-code, as shown in Eq. (3). For case I, the weakest density point corresponds to the nozzle position when the filament motor is switched back ON. The material density remains higher in the neighboring regions. In case II, where attack duration is prolonged enough to dry out the residual filament completely, we attain a zero material density zone with gradual downward density slope to precede it in response to the switching OFF event, and a steeper upward slope to follow the switching ON event.

$$d_{res} = f(G_{nozzle}, V_{nozzle}, T_{nozzle}, max(v, a, j), h) \quad (3)$$

where G_{nozzle}, V_{nozzle} and T_{nozzle} are the nozzle's geometry, speed and temperature, max(v, a, j) are the maximum speed, acceleration and jerk settings in the printing profile, "h" is the printing material viscosity property. Although these functions can be calculated through fluid dynamics knowledge, our experiments show that the d_{res} value remains around 25–30 mm for the settings used in our experiment. The attack is designed by choosing the highest impact region of an object, calculating the t_{OFF} time as per the desired intensity of the attack, and then, modifying the G-code commands to mute the filament in the region of interest. We identify two variants of the attack depending upon the object design and G-code commands.

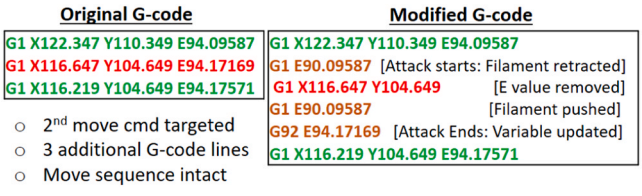


Fig. 3. G-code snippet of filament-kinetic cavity attack.

Variant I: The attack may require removing filament field "e" value in a single or multiple G-code instructions, and then updating the current filament length variable through "G92" command.

Variant II: The attack split a single command that may cause a very minimal time variation. The reason is the max acceleration and higher order peak value settings that have to be adhered when the command is split. However, the effect is very minimal (less than 20 ms as observed under most common conditions). The attacker can still avoid it by increasing the zone of attack to the complete instruction. To be effective, this attack usually continues for more than one commands, thus rounding off to next complete command is not a big change. In attacks where command splitting is not required, nozzle kinetics is not affected at all.

3.1.3. Density variation through filament speed attack

This attack modifies the filament motor speed to manipulate the relation between filament and nozzle kinetics without changing the nozzle speed. In FFF printers, a printing move command may trigger movement of 3 motors (x, y and filament e). The axis undergoing the biggest move inherits the max-speed value. The printer proportionally adjusts the speed of the remaining axes to ensure that all motors start and stop at the same time, and the filament deposition is symmetric throughout the path.

In this attack, the attacker reduces the filament speed in the target zone and compensates for the slowness by increasing the filament speed over the non-critical areas, thus ensuring that the target area receives lesser filament, while the object's net weight still remains the same. Although the weight difference in other 2 attacks is also minimal, it is zero in this attack. There is also no impact on the toolpath sequence or the printing time.

3.2. Dynamic-thermal attacks

Thermodynamics of a FFF printer is a complex process, and is critical for the printed object's health. Asymmetric heating and cooling profiles at different regions in an object may create residual thermal stresses [17]. If the thermodynamic profile is tweaked too far than the optimal setting, it results in noticeable deformation or warping. On the other side, tiny changes do not consistently change the material properties. The critical question in designing this attack is to find small magnitude deviation patterns that do not create any visible deformation but still change the object properties.

There are two heating elements in a FFF printer, i.e., printing nozzle and heated bed. This attack mainly targets the nozzle's temperature and does not alter any nozzle- and filament-kinetics. There are two ways to set the nozzle temperature. First, the "M109" command pauses the printing, the printer attains the desired temperature, and resumes the printing. Creating a steep temperature variation will result in higher thermal stress. Thus, it is desirable from the attacker's standpoint; however, pausing the printing for a few seconds creates enough deviation in nozzle kinetics to generate an alert. Second, the "M104" command continues to print while simultaneously working to achieve the desired temperature. The temperature fluctuation is gradual.

This attack utilizes the "M104" command to instruct the temperature change before the nozzle passes over the target area. A small change in a single layer has a negligible impact on the object. To increase the attack impact, multiple internal layers are printed with the same modified profile. Different temperature profiles incur consistently different outcomes in physical properties. Thus, the attacker can use a temperature profile that can give the desired impact on material properties. Note that when the temperature is reduced, under-extrusion will also occur. However, in this attack, we ensure that the temperature fluctuations are within the printer's extrusion capabilities.

4. Attack implementation

4.1. Adversary model

4.1.1. Assumptions

Our threat model assumes that the CAD and STL files are intact; they are protected by other security measures such as file integrity checker. However, the attacker compromises the printer firmware and G-code (e.g., Harvey [18]) and installs a rootkit that can manipulate the printing process, including printer (internal) sensors and actuator movements. This model is commonly used by the existing security research on 3D printers [13–15,18].

4.1.2. Attacker's goal

The user is printing a batch of critical rectangular bars exposed to tensile and bending stresses during operation. The attacker aims to carry out inconspicuous attacks on the target object to achieve degradation in mechanical properties while evading the visual inspection and necessary quality checks (such as weight and the center of gravity).

4.1.3. Attack method

To achieve the goal, the attacker utilizes our proposed filament-kinetic and dynamic-thermal attacks. In control of the printer's firmware and G-code, the attacker generates the G-code files, each containing one type of attack sequence and utilize it in the target 3D printer to attack the printing object.

4.2. Experimental settings

We implement the attacks on rectangular bars with dimensions (60 mm length × 6 mm depth × 4 mm height). The bars are printed with PLA material through the Ultimaker-3 printer hosting a 0.4 mm nozzle. On a control PC connected over the IP network, Ultimaker Cura 4.0.0 is used as the slicer and controlling software. The default object settings include 0.2 mm layer thickness (making 20 layers in the object), 100% infill density, and "Line" infill-pattern at 45° angle. The default temperature for layer-1 is 210° C, while 205 °C for the remaining layers. The printing speed is set at 50 mm/sec.

4.3. Localized filament-kinetic attacks

4.3.1. Cavity attack through filament-kinetics

Three layers from the top and bottom are not modified to attain a cavity within the internal layers. The attacker calculates the bar's central point and modifies the G-code move instructions near the center. To keep the cavity fully encapsulated from all sides, the attacker splits each line into three parts and produces a cavity only in the middle part of the line. The effective cavity dimensions per layer are around 2 mm × 0.6 mm. The filament values are adjusted using the methods described in Section 3. The attack starts after the 1^{st} part of the attacked command is completed. The filament is retracted by 4 mm. This value is measured empirically, starting from 1 mm upwards to ensure minimum retraction distance that results in zero residual filament, resulting in a clean cavity at the target spot. After retraction, the nozzle follows the toolpath for the 2^{nd} part, but without filament extrusion. When the nozzle reaches the end of the cavity, the filament is pushed back 4 mm; the filament length variable is updated to avoid 'e' value modification in the subsequent commands. The 3^{rd} part is then printed normally. The phenomenon is explained in the Fig. 4.

4.3.2. Density variation through filament state attack

In this attack, the attacker mutes the three adjacent infill lines near the center of the object. Two small connecting lines (0.5 mm) that connects two infill lines are also muted as a consequence. The attack is made by removing the "e" field in the required move instructions and updating the software's filament length variable. Although no visual impact is expected in this attack as the nozzle stays well within the case-1 discussed in Section 3.1.2, the attacker keeps the top three and bottom three layers unmodified for re-assuring no visual anomaly in the finished object. The purpose of extending this attack over more layers is to increase the attack impact on the object properties.

4.3.3. Density variation through filament speed attack

In this attack, the attacker selects three lines in the center of the object and reduces their material density by 30% by reducing the value of Δe (which is the difference in the filament length value for the i^{th} and $(i\text{-}1)^{th}$ command). To compensate for the anticipated reduction in weight, the attacker selects three lines in the middle of the right half and three lines in the middle of the left half and distributes the lost material equally among them. As per the attacker's knowledge, these locations are less critical from the object's operational perspective. The top and bottom three layers are not attacked in this case as well. Although the deviation magnitude in this attack is smaller than the previous two attacks, a larger area of the layer is disturbed in this case.

4.4. Dynamic-thermal attacks

The variation of temperature at different locations in an object induces thermal stresses that impact the printed object's mechanical properties. Exploiting this fact, the attacker manipulates the nozzle temperature by a small magnitude (±12 °C), causing residual thermal stress with no visible deformation or warping. The magnitude was

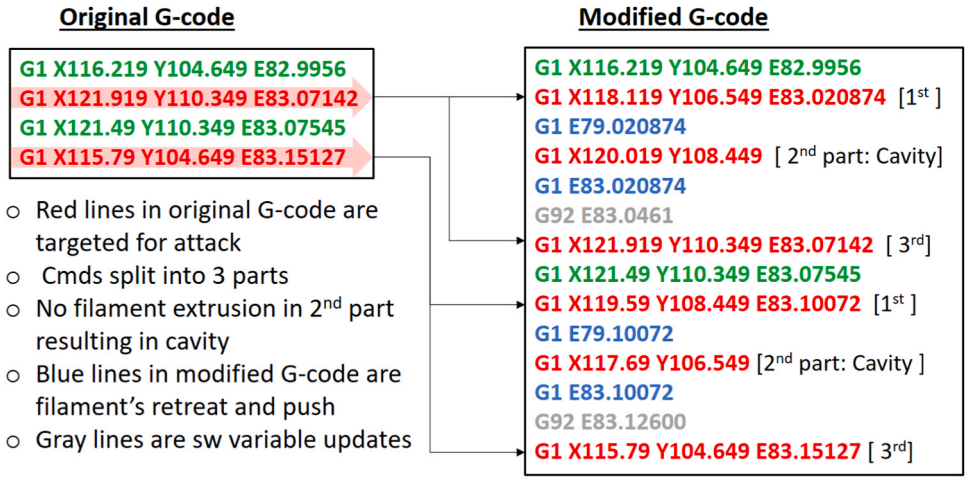


Fig. 4. G-code comparison of single instance of cavity attack.

selected after no particular trend was observed with a deviation of (±5 °C) and (± 7°C) for the chosen attack types. The printing of each layer starts at one end (bottom right as per the user's settings) and finishes at the other end (top left), as shown in Fig. 5.

When the attacked layer printing starts, the temperature begins to change due to the influence of the M104 command inserted by the attacker. The printer proceeds towards the center in line by line fashion. As the nozzle reaches the center, another M104 command is issued to revert the temperature to the default value. Before the nozzle reaches the other end of the object, it attains the default temperature. Sufficient time is required to ensure that the required change in temperature can be achieved as the printer reaches the center. In addition to the warping over higher temperature changes, this factor also creates an upper bound on the attack magnitude.

Fig. 5 shows sufficient time-gap between printing of the central portion and the sides of the bar to attain the temperature difference. If the infill pattern angle is changed to 0^o, launching the dynamic-thermal attack in this manner would not be possible. However, the infill angle (or raster angle) value is an important design decision with significant impact on the material properties [19], and it's modification is not a trivial operational change.

Two different attack patterns are used in our experiment. In the first attack, the central part is printed at 12 °C higher temperature than the default value, while in the second attack, the central part is printed at 12 °C lower temperature. We observed minor variation (around ±2 °C) in the peak temperature difference induced in different samples.

5. Evaluation results

5.1. Stealthiness standpoint

The stealthiness of the attack is part of the success criteria. We observed no change in the object dimensions for the attacked samples. Table 1 shows the results of the object dimensions measured for 5 samples of each type of attacked and benign specimens. The stealthiness also includes changes in the printing time, weight differences, or modification of the toolpath. Table 2 summarizes the attacks performance from detection or stealthiness standpoint. We did not observe any visual indication in the attacked objects throughout the printing process. One exception is the clean-cavity attack, where a cavity can be visible to an observer during the internal layers' printing. Ultimately, the cavity is covered by the non-attacked top layers in due course. In case of dynamic-thermal attacks, when temperature reduction was attempted over 15 °C, occasionally warping was observed in the workpiece. We restricted our attacks to 12 °C where no deformation was observed for any specimen above the available 3D-scanner resolution (0.5 mm). All other attack samples were printed smoothly.

5.2. Confirmation of parameter changes

To examine if our attacks change the desired parameters, we carried out few exercises. For the cavity attack, we know that the cavity (if created) will be visible during the printing of the attacked layers. As shown in the Fig. 6a, the cavity is created at the correct spot as intended. The image is captured during a test print by pausing the printing during one of the attacked layers. Since there is no visual indication for the other two filament-kinetic attacks, we printed a rectangular prism with

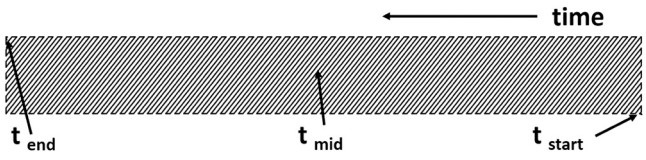


Fig. 5. Infill printing sequence.

Table 1
Statistics of attacked and benign samples outer dimensions.

Attack type	Length (mm)		Width (mm)		Height (mm)	
	Mean	Std dev	Mean	Std dev	Mean	Std dev
No Attack	60.52	0.10	6.57	0.03	4.14	0.02
Clean Cavity Attack	60.53	0.05	6.55	0.03	4.14	0.01
Filament State Attack	60.54	0.07	6.59	0.02	4.14	0.01
Filament Speed Attack	60.54	0.04	6.61	0.03	4.14	0.01
High Temperature	60.53	0.05	6.61	0.04	4.15	0.01
Low Temperature	60.58	0.07	6.56	0.03	4.16	0.02

less infill density and higher attack magnitude (by muting the filament motor for more time) to confirm visual deformation. Thinning of infill lines can be visually observed in the target area, as seen in the Fig. 6b. For dynamic-thermal attacks, we installed a thermocouple near the tip of the nozzle to examine the actual temperature during the printing. Fig. 7a shows the traces of the high temperature profile attack. The middle part is printed at the highest temperature, and both sides are printed at default temperature. Fig. 7b shows that the nozzle temperature is reduced when the central part of the object is being printed. The traces confirm that the temperature is modified for the attacked prints. Fig. 7 does not represent a thermal image taken at one instance; rather, it provides the temperature value of each pixel when it was printed.

6. Mechanical testing for attack impact measurement

After confirming that the attacks met the criteria of inconspicuousness and parameter modification, we carried out the mechanical tests of the original prints and the attacked prints. We performed two important destructive tests: tensile strength test using *MTS Insight 30* and three-point bending test using *Instron 5948* test equipment. Filament-kinetic attacks and dynamic-thermal attacks were carried out in two separate circumstances. Therefore, a separate set of default prints is used for each of them.

6.1. Mechanical testing of filament-kinetic attacks

6.1.1. Tensile test

The results of tensile tests for the filament-kinetic attacks are summarized in Table 3.

All the attacks show a decrease in the peak load, peak stress and the modulus value. Clean cavity attack shows the biggest reduction in the peak load and stress values, followed by the filament state attack. However, the Young's modulus reduction for the cavity attack was minimal compared to the filament state and filament speed attacks. Another interesting finding is the reduction in yield value for all types of attacks, as visible in the Fig. 8b.

All the attack samples broke earlier than the non-attacked samples. Another important observation is that the samples broke exactly at the point of attack, while the non-attacked samples break at random locations as visible in the Fig. 9b. In the case of cavity attack, the cavity got exposed after the failure, as shown in the Fig. 9a. During the failure investigation, this evidence can point to the presence of an attack. As shown in the Fig. 9c and d, there was no obvious indication leading to the presence of attack in other two cases.

6.1.2. Three-point bending test

The three-point bending tests also show a minor reduction in the peak stress value for the attack samples. Clean cavity attack samples are the fastest to break, followed by filament state attack samples. Filament speed attack samples did not break till the maximum extension limit of the test. It is also evident from the heaviest tailed curve of filament-speed attack in the Fig. 10. It indicates that the density reduction across multiple layers in the central region negatively affects the layers

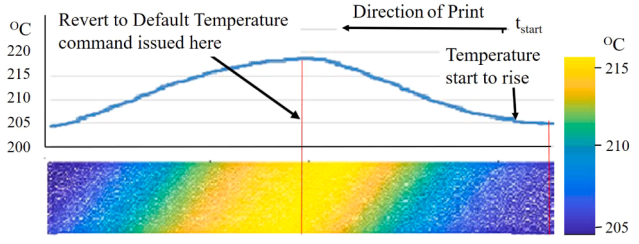
Table 2
Attack footprints from detection standpoint.

Attack category	Attack name	Visible change	Change in outer dimensions	Toolpath sequence change	Printing Time change	Weight difference
Filament-kinetic	Clean Cavity	Yes (only in internal layers during printing)	None	None	0.4 s per attacked layer	<1%
Filament-kinetic	Filament State	None	None	None	None	<1%
Filament-kinetic	Filament Speed	None	None	None	None	None
Dynamic-thermal	High Temperature	None	None	None	None	None
Dynamic-thermal	Low Temperature	None	None	None	None	None

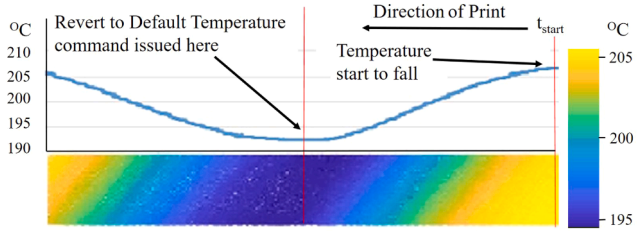
(a) Image taken after pausing the printing during middle layers

(b) Exaggerated attack magnitude results in obvious thinning of the filament

Fig. 6. Filament-kinetic attacks - parameters deviation evidence.



(a) High temperature profile Attack



(b) Low temperature profile attack

Fig. 7. Temperature profile for dynamic-thermal attacks.

bondage. The three-point bending results indicate apparent changes in the object properties based on the attack pattern. Table 4 presents the results of the three-point bending tests for the filament-kinetic attacks specimens.

6.2. Mechanical testing of dynamic-thermal attacks

6.2.1. Tensile test

Tensile tests for dynamic-thermal attacks also show a noticeable change in properties. Fig. 11a shows that the benign samples break at random locations, as expected. However, a consistent interesting trend is visible with the two attack patterns. The low-temperature attack samples, shown in the Fig. 11b, always break at the center where the temperature deviation is maximum, while the high-temperature attack samples, shown in the Fig. 11c, never break at the center. Table 5 presents the tensile tests results for the dynamic-thermal attacks samples.

Compared with the default profile, the peak stress value was reduced by 8.1% for the low-temperature attack and 3.3% for the high-temperature attack. The most impacted property was 'Strain' with −28% difference in the low-temperature profile attack. Table 6 presents the summary of the test results. Fig. 12a and 12b presents tensile test results plots for stress versus strain, and load versus time.

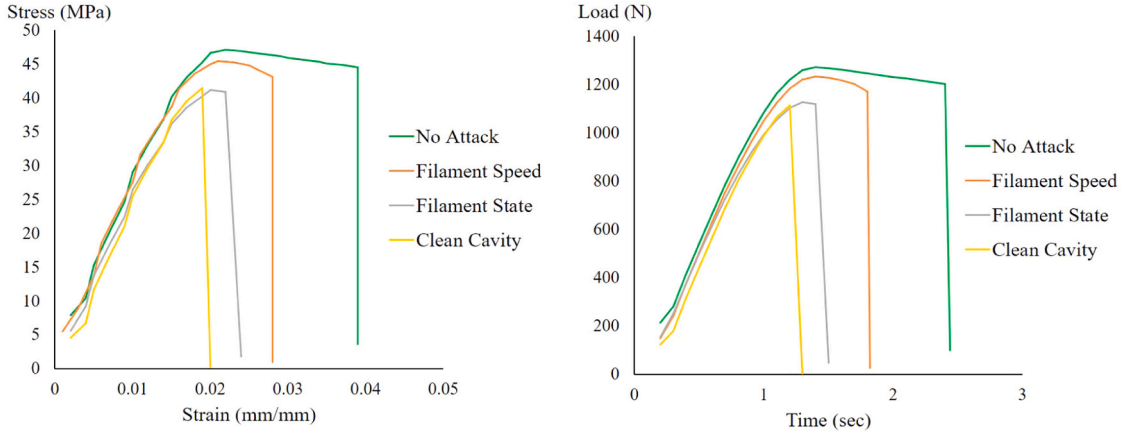
6.2.2. Three-point bending test

Fig. 13 represents the three-point bending test results for dynamic-thermal attacks.

For this test, we set a maximum extension limit of 7.5 mm. All specimens fractured before this value. For high-temperature attack samples, the specimen breaks abruptly, indicating strong inter-layer bondage in the central part. Though the specimen gets fractured earlier for low-temperature attacks, several layers remain intact till the max extension limit for all the low-temperature attack specimens. It shows the weakening of the inter-layer bondage caused by temperature reduction. The peak load value raised from 144 N (default) to 158.8 N for the high-temperature profile but reduced to 129.4 N for the low-temperature profile indicating 10–15% average deviation.

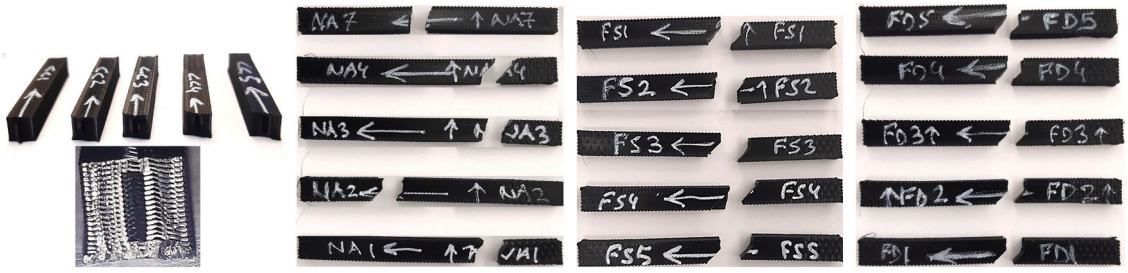
Table 3
Tensile tests summary for filament-kinetic attacks.

	Peak load (N)		Peak stress (MPa)		Peak strain (mm/mm)		Modulus (MPa)	
Attack types	Mean	Std dev	Mean	Std dev	Mean	Std dev	Mean	Std dev
No Attack	1273.252	43.380	47.140	1.856	0.023	0.001	2916.865	81.932
Clean Cavity	1123.876	81.768	41.580	3.178	0.019	0.002	2880.255	48.643
Filament State	1135.753	29.283	41.940	1.060	0.020	0.000	2779.170	68.891
Filament Speed	1230.394	36.287	45.380	1.203	0.023	0.001	2814.338	81.932



(a) Stress vs Strain (b) Load vs Time

Fig. 8. Tensile test results for filament-kinetic attacks.



(a) Filament cavity attack (b) Samples with no attack (c) Filament state attack (d) Filament speed attack

Fig. 9. Filament attacks specimens after tensile tests.

7. Attack countermeasures

The attack countermeasures can be categorized into two groups: cyber and physical domain measures.

7.1. Cyber-domain countermeasures

The proposed attacks can be launched by modifying the G-code file sent to the printer, or by compromising the printer firmware. Following paragraphs discuss some countermeasures in the cyber-domain to detect and block these attacks.

Network layer security

McCormack et al. [20] identifies most of the surveyed printers using unencrypted communication with the control PC, increasing the chances of network layer attacks. By securing the communication channel between the control PC and the printer through advanced encryption standards and authentication techniques, the network attack vector can be controlled.

Firmware attack countermeasures

Firmware of a 3D printer can be modified through an illegal upgrade activity over the network or via USB port. Network security measures and vulnerability analysis of the firmware covers the known remote exploits. To avoid an illegal USB based firmware upgrade, physical access should be controlled, and USB drives should be regularly scanned for malware. To verify the firmware of the printers, users may utilize verification schemes proposed by researchers, such as [21] based on block-chain, [22] using instructions level abstraction, etc.

7.2. Physical domain countermeasures

Monitoring the physical process is an important measure to detect cyberattacks in a CPS.

7.2.1. Realtime and out-of-band monitoring of filament-kinetics

The test results show that the presented sabotage attacks change the physical properties in various ways and magnitude. Cavity attacks through filament-kinetics created a clean cavity with a minimal footprint over the nozzle kinetics. The filament-state attack has zero

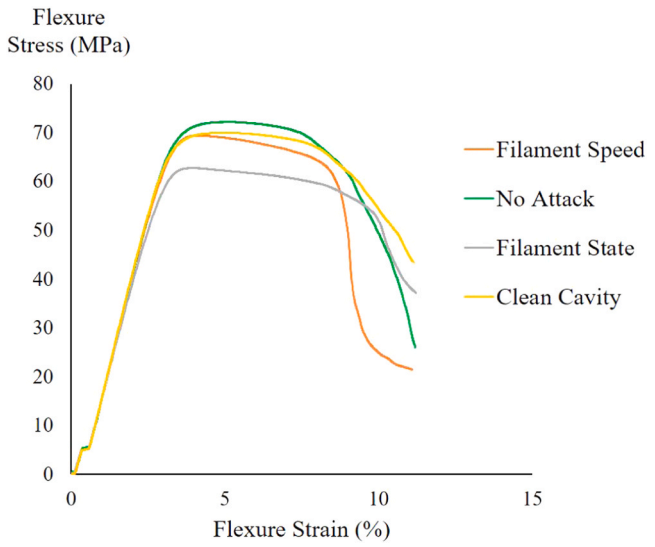


Fig. 10. Three-point bending test for filament-kinetic attacks: flexure stress vs flexure strain.

Table 4
Three-point bending tests summary for filament-kinetic attacks.

	Peak flexure stress (MPa)		Peak flexure strain %)		Peak stress / Strain (MPa)	
Attack types	Mean	Std dev	Mean	Std dev	Mean	Std dev
No attack	71.814	1.477	11.190	0.033	21.618	0.663
Clean Cavity	70.403	1.477	11.043	0.061	21.151	0.491
Filament State	65.283	1.712	11.184	0.064	19.735	0.347
Filament Density	69.361	0.484	11.152	0.062	20.881	0.112

footprint over nozzle-kinetics but a relatively bigger footprint over filament-kinetics. If the filament-kinetic state is monitored, this attack can be detected. The filament-speed attack is slow and steady. There is no footprint over nozzle-kinetics. If the magnitude of density variation is low enough, the detection could be challenging. More research can reveal new ways to launch and block these attacks. Schemes based on optical-encoders [23] or electric current measurement [11] can be utilized effectively with more research. As all the attacks incurred unique effects on the object, an interesting future study can provide unique attack signatures. These signatures can help in detection when the attack magnitudes go further low into the confusion zone of the printing process' benign deviations.

7.2.2. *Monitoring via temperature sensors or thermal cameras*

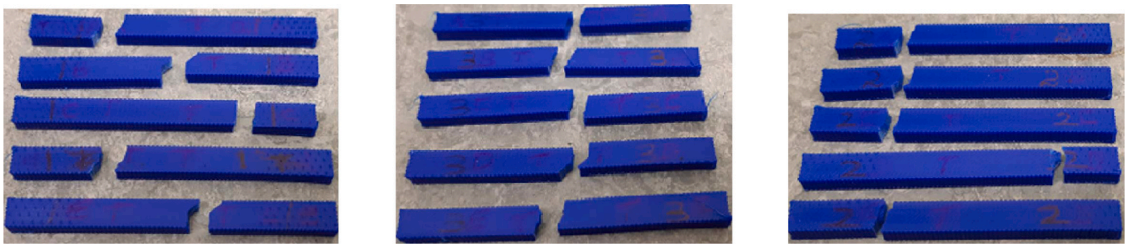
The two dynamic-thermal attack patterns used in our scheme successfully modified object properties confirming that these attacks are practical. Very low temperature deviations do not affect the object, while very high changes can cause visual deformity. Within this window, different attacks can be launched to target specific properties of the object. Monitoring the nozzle temperature through thermocouple sensors or object temperature using thermal cameras [24] can help in detecting these attacks.

8. Conclusion

We presented and evaluated localized filament-kinetic and dynamic-thermal attacks on FFF-based 3D printing process. The attacks produce no visual impairment and insignificant footprint, making them difficult to detect. With the help of tensile and three-point bending tests, we established that these attacks successfully modify the printed object's physical properties, such as peak stress and strain. The attacks that target the design or STL files usually cause big and uncontrolled printing profile changes at the slicing stage, making them obvious to simple detection schemes. On the contrary, the proposed attacks can bypass the existing detection techniques, and can still impair the normal functioning of the targeted object. To protect against these attacks, synchronized space-time analysis of the thermodynamic, nozzle-kinetic and filament-kinetic processes can be an effective way.

Table 6
Three-point bending tests summary for dynamic-thermal attacks.

Attacks	Peak flexure stress (MPa)		Peak flexure strain (%)		Peak stress /strain (MPa)	
	Mean	Std dev	Mean	Std dev	Mean	Std dev
No Attack	80.209	4.344	10.953	0.105	7.322	0.370
High Temperature	88.288	1.885	11.003	0.036	8.025	0.191
Low Temperature	70.842	3.375	11.067	0.090	6.403	0.327



(a) Default temperature profile: sample breaks at random locations

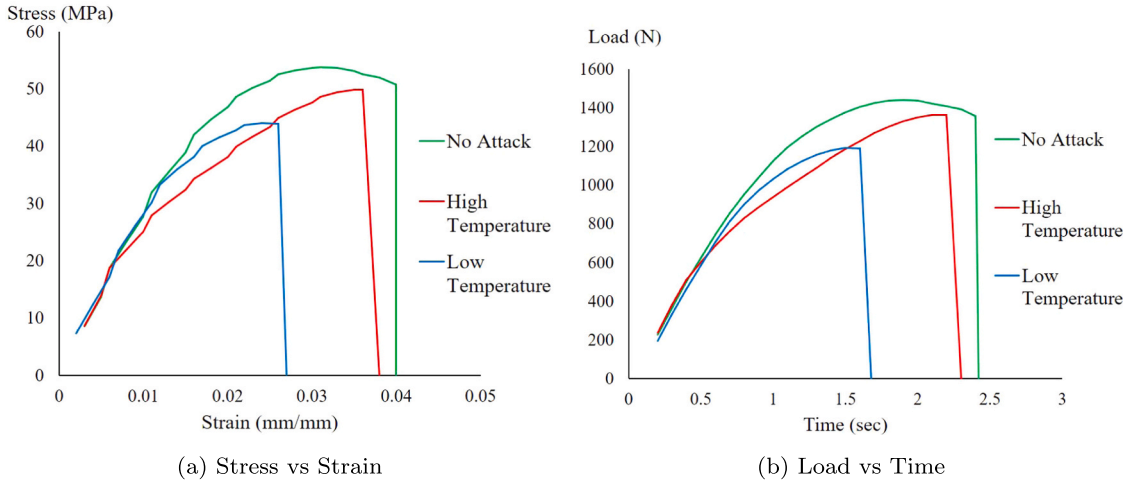
(b) Low temperature profile: specimen always break at the center

(c) High temperature profile: specimen never break at the center

Fig. 11. Dynamic-thermal attacks specimen images highlighting the break-points.

Table 5
Tensile tests summary for dynamic-thermal attacks.

Attacks	Peak load (N)		Peak stress (MPa)		Strain at break (mm/mm)		Modulus (MPa)	
	Mean	Std dev	Mean	Std dev	Mean	Std dev	Mean	Std dev
No Attack	1356.438	72.806	50.800	2.593	0.032	0.002	2939.383	223.311
High Temperature	1329.316	73.773	49.120	2.594	0.033	0.005	2845.408	259.791
Low Temperature	1268.334	43.458	46.820	1.617	0.023	0.001	2962.007	66.050



(a) Stress vs Strain (b) Load vs Time

Fig. 12. Tensile test results for dynamic-thermal attacks.

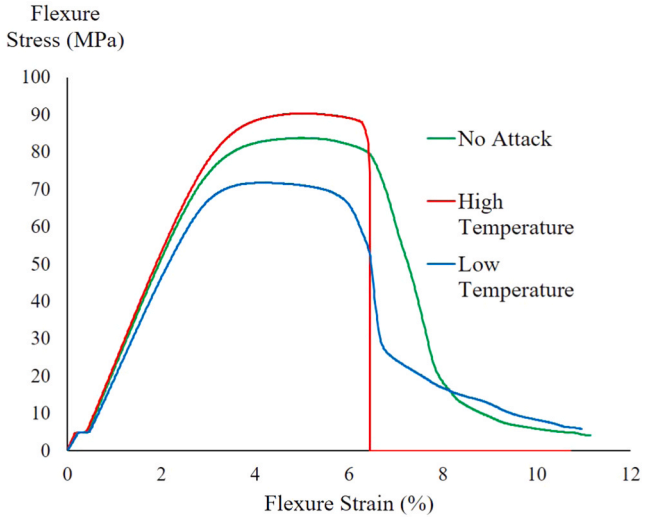


Fig. 13. Three-point bending tests for dynamic-thermal attacks: flexure stress vs flexure strain.

CRediT authorship contribution statement

Muhammad Haris Rais: Conceptualization, Methodology, Software, Investigation, Writing – original draft. **Ye Li:** Conceptualization, Methodology, Supervision, Writing – original draft. **Irfan Ahmed:** Conceptualization, Methodology, Supervision, Writing – original draft, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

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] E., Abouel Nasr, Rapid Prototyping: Theory and Practice, 2006.
[2] M. Yampolskiy, W.E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, Y. Elovici, Security of additive manufacturing: attack taxonomy and survey, Addit. Manuf. 21 (2018) 431–457, https://doi.org/10.1016/j.addma.2018.03.015.
[3] M.A., Al Faruque, S.R., Chhetri, A., Canedo, J., Wan, Acoustic side-channel attacks on additive manufacturing systems, in: Proceedings of the 2016 ACM/IEEE Seventh International Conference on Cyber-Physical Systems (ICCPS), 1–10.
[4] 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. ⟨https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky⟩.
[5] S.E. Zeltmann, N. Gupta, N.G. Tsoutsos, M. Maniatakos, J. Rajendran, R. Karri, Manufacturing and security challenges in 3d printing, JOM 68 (2016) 1872–1881, https://doi.org/10.1007/s11837-016-1937-7.
[6] 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⟩.
[7] S. Ding, B. Zou, P. Wang, H. Ding, Effects of nozzle temperature and building orientation on mechanical properties and microstructure of peek and pei printed by 3d-fdm, Polym. Test. 78 (2019), 105948, https://doi.org/10.1016/j.polymertesting.2019.105948.
[8] M. Spoerk, J. Gonzalez-Gutierrez, J. Sapkota, S. Schuschnigg, C. Holzer, Effect of the printing bed temperature on the adhesion of parts produced by fused filament fabrication, Plast. Rubber Compos. 47 (2018) 17–24, https://doi.org/10.1080/14658011.2017.1399531.
[9] M., Yampolskiy, L., Schutzle, U., Vaidya, A., Yasinsac, Security challenges of additive manufacturing with metals and alloys, in: M. Rice, S. Shenoi (Eds.), Proceedings of the Critical Infrastructure Protection IX, Springer International Publishing, Cham, 2015, 169–183.
[10] C., Bayens, T., Le, L., Garcia, R., Beyah, M., Javanmard, S., Zonouz, See no evil, hear no evil, feel no evil, print no evil- malicious fill patterns detection in additive manufacturing, in: Proceedings of the Twenty Sixth USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC, 2017, 1181–1198.
[11] J. Gatlin, S. Belikovetsky, S.B. Moore, Y. Solewicz, Y. Elovici, M. Yampolskiy, Detecting sabotage attacks in additive manufacturing using actuator power signatures, IEEE Access 7 (2019) 133421–133432.
[12] S. Belikovetsky, Y.A. Solewicz, M. Yampolskiy, J. Toh, Y. Elovici, Digital audio signature for 3d printing integrity, IEEE Trans. Inf. Forens. Secur. 14 (2019) 1127–1141.
[13] 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.
[14] S., Moore, W., Glisson, M., Yampolskiy, Implications of malicious 3d printer firmware. ⟨https://doi.org/10.24251/HICSS.2017.735⟩.
[15] X.Z., Hang, Three demos of attacking arduino and reprap 3d printers, code to keynote at xcon2013 (2013), 2016. ⟨https://github.com/secmobi/attack-arduino-and-reprap⟩.
[16] L.D. Sturm, C.B. Williams, J.A. Camelio, J. White, R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems: a case study attack on the.stl file with human subjects, J. Manuf. Syst. 44 (2017) 154–164, https://doi.org/10.1016/j.jmsy.2017.05.007.
[17] G. Miao, S.-J. Hsieh, J. Segura, J.-C. Wang, Cyber-physical system for thermal stress prevention in 3d printing process, Int. J. Adv. Manuf. Technol. 100 (2019) 553–567.

[18] L., Garcia, F., Brasser, M., Cintuglu, A.R., Sadeghi, O., Mohammed, S.A., Zonouz, Hey, my malware knows physics! attacking plcs with physical model aware rootkit, in: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, NDSS,2017, Internet Society, Reston, VA, USA, 2017. ⟨https://doi.org/10.14722/ndss.2017.23313⟩.

[19] Vosynek Petr, Navrat Tomas, Krejbychova Adela, Palousek David, Influence of process parameters of printing on mechanical properties of plastic parts produced by fdm 3d printing technology, MATEC Web Conf. 237 (2018) 02014, https://doi.org/10.1051/matecconf/201823702014.

[20] M., McCormack, S., Chandrasekaran, G., Liu, T., Yu, S., DeVincent Wolf, V., Sekar, Security analysis of networked 3d printers, in: Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW), 118–125. ⟨https://doi.org/10.1109/SPW50608.2020.00035⟩.

[21] B. Lee, S. Malik, S. Wi, J.-H. Lee, Firmware verification of embedded devices based on a blockchain, in: J.-H. Lee, S. Pack (Eds.), Quality, Reliability, Security and Robustness in Heterogeneous Networks, Springer International Publishing, Cham, 2017, pp. 52–61.

[22] B.-Y., Huang, S., Ray, A., Gupta, J.M., Fung, S., Malik, Formal security verification of concurrent firmware in socs using instruction-level abstraction for hardware*, in: Proceedings of the 2018 Fifty Fifth ACM/ESDA/IEEE Design Automation Conference (DAC), 1–6. ⟨https://doi.org/10.1109/DAC.2018.8465794⟩.

[23] M.H., Rais, Y., Li, I., Ahmed, Spatiotemporal G-Code Modeling for Secure FDM-Based 3d Printing.

[24] M.A., Al Faruque, S.R., Chhetri, A., Canedo, J., Wan, Forensics of Thermal Side-channel in Additive Manufacturing Systems, University of California, Irvine, 2016.