Spatiotemporal G-code modeling for secure FDM-based 3D printing

Muhammad Haris Rais[1], Ye Li [2], Irfan Ahmed [1]

[1] Virginia Commonwealth University [2] Bradley University

Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems. 2021

https://dl.acm.org/doi/10.1145/3450267.3450545

Outline

- Overview of additive manufacturing process
- Categories of cyberattacks
- Processes involved
- Sophos3DP framework
- Evaluation
- Future work
- Conclusion

Additive manufacturing process chain

Designing

CAD software — Creating a CAD File

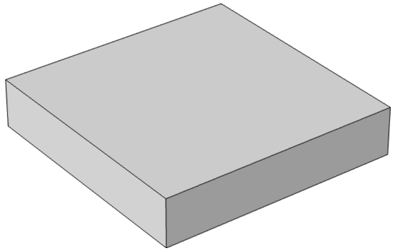
STL Editor Software — CAD to STL File

Slicing

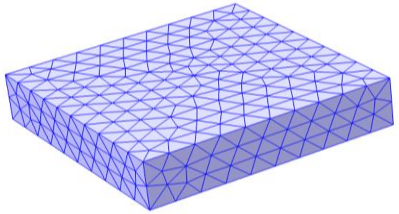
Slicer Software — Generating G-codes from STL file

Printing

3D printer firmware — Printing the object

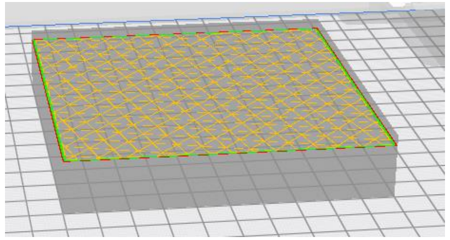


3D Model



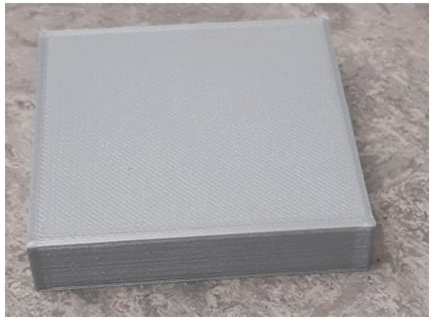
Outer surface representation

```
facet normal -0 -0 -1
outer loop
vertex 0 5 0
vertex 5 5 0
vertex 0 0 0
endloop
endfacet
```

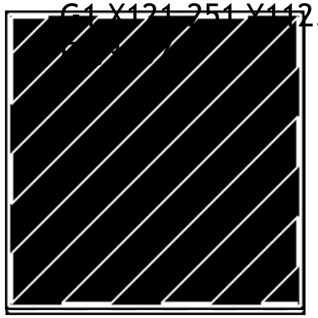


Printing instructions

```
;TYPE:WALL-OUTER
G1 F1500 X111.749 Y112.251 E1.7
G1 X111.749 Y102.749 E1.98518
G1 X121.251 Y102.749 E2.18546
G1 X121.251 Y112.251
```



Physical object



Internal Layers

Why cybersecurity of additive manufacturing?

New technology

- Fundamentally different
- Not designed with security in mind
- AM is a CPS

Less security awareness

Industry 4.0

- AM – Mass customization
- IoT
- Cloud Computing
- Big Data
- AI

Easier access to attackers

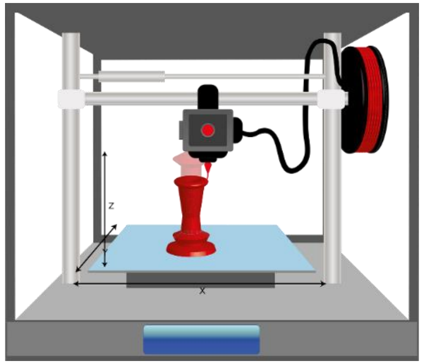
Use Cases

- Healthcare
- Aviation
- Automobile
- 24% ACGR

Higher rewards for attackers

Major attack goals

Intellectual Property Theft

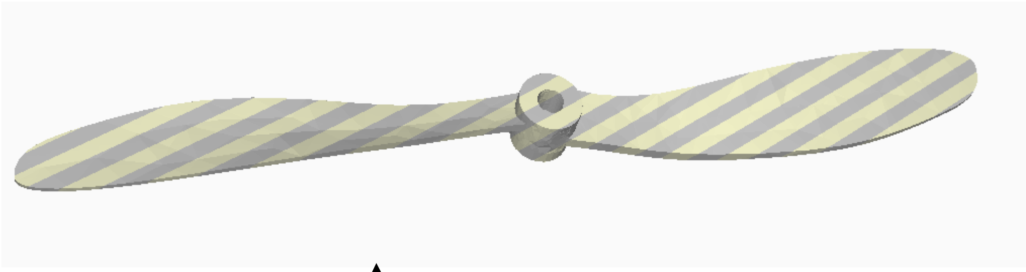


Confidentiality

Integrity

Availability

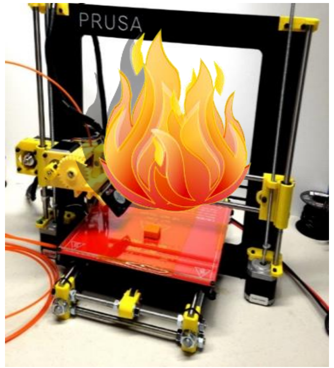
Defected printed Object



Sabotage Attacks

Focus of this paper

Denial of Service



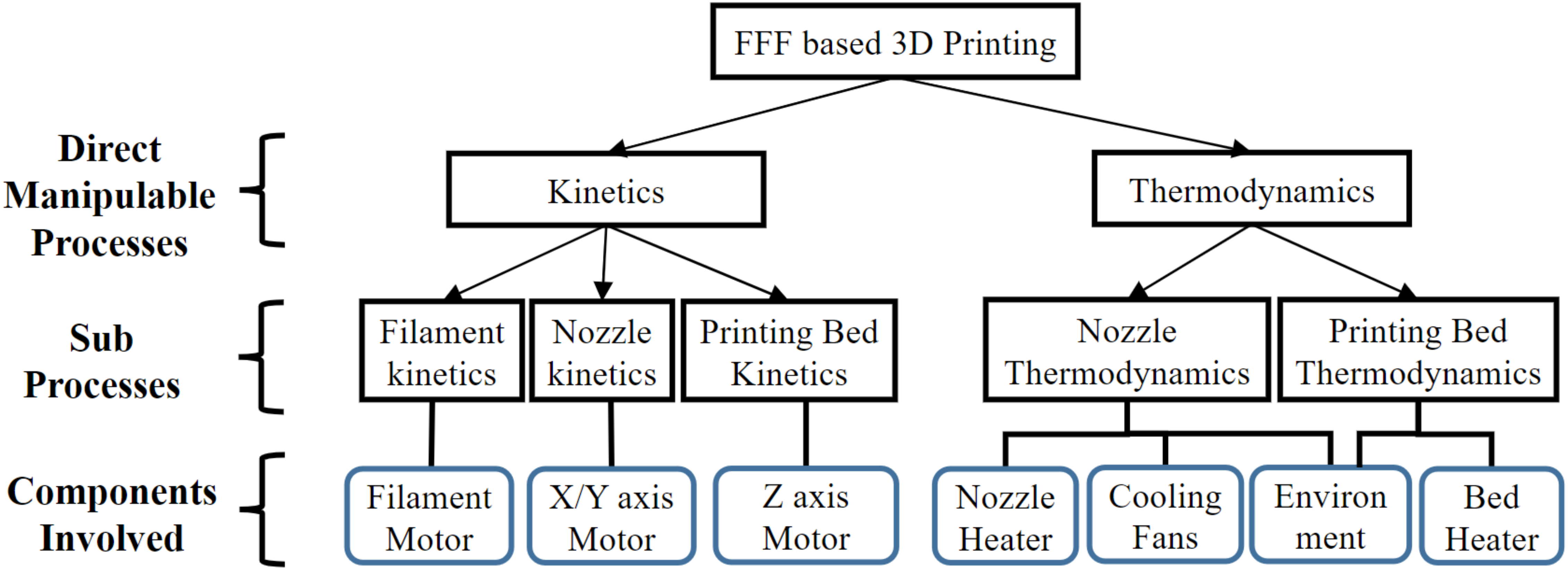
Sabotage Attacks on 3D Printing Process

Sabotage attack’s aim is to weaken, damage or destroy the printed object

Types of Sabotage Attacks

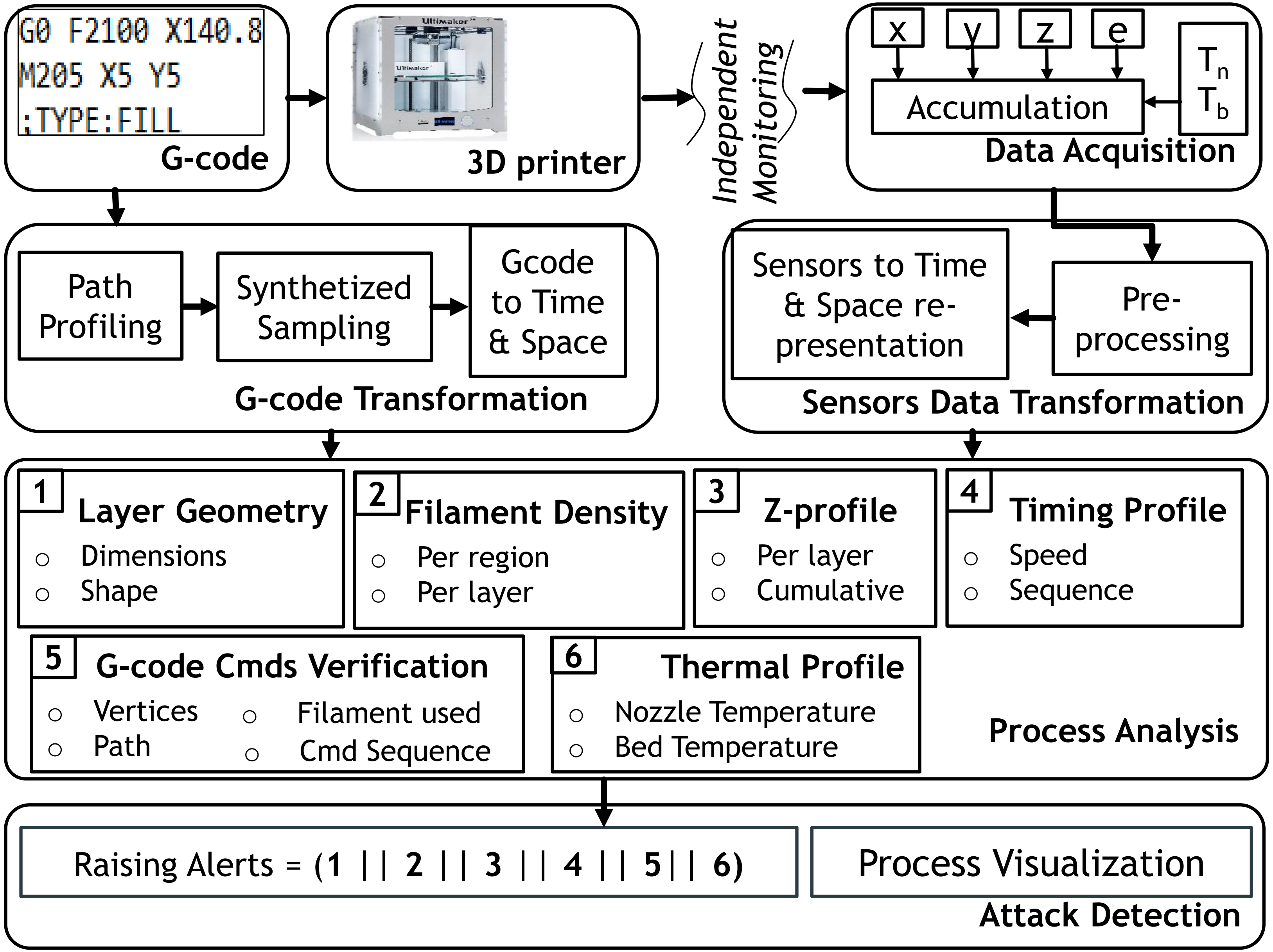
- Geometry Related
  - External
  - Internal
- Filament-density Related
- Timing Sequence Related
  - Anisotropy
  - Printing Speed
- Thermodynamics Related

Direct manipulable physical processes in FFF printing



Sophos3DP : A framework to detect sabotage attacks

Sophos3DP – A Framework for Secure FDM Printing

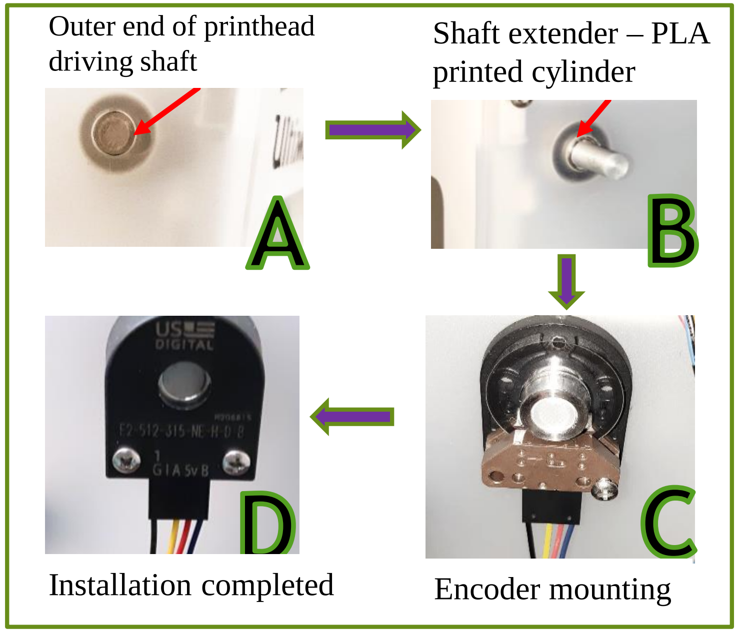


- Data Acquisition
- G-code Transformation
- Sensor Data Transformation
- Process Analysis
- Evaluation

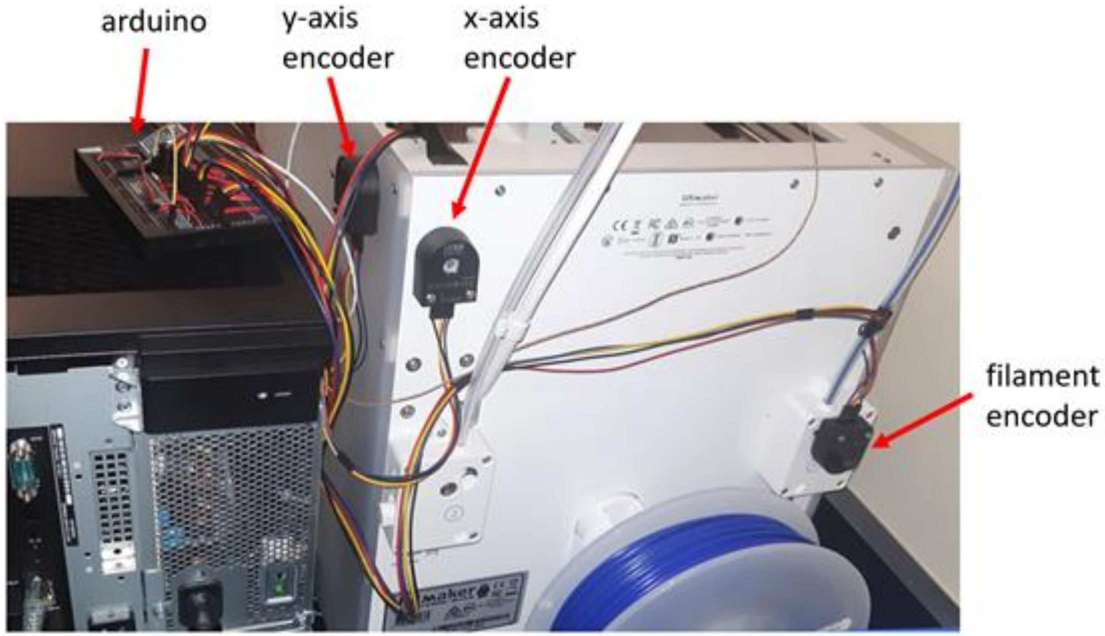
Data Acquisition - Kinetics

- Optical Encoders
- Rotary encoders for x,y, filament movement
- Linear encoder for printing bed
- Accumulation through Arduino

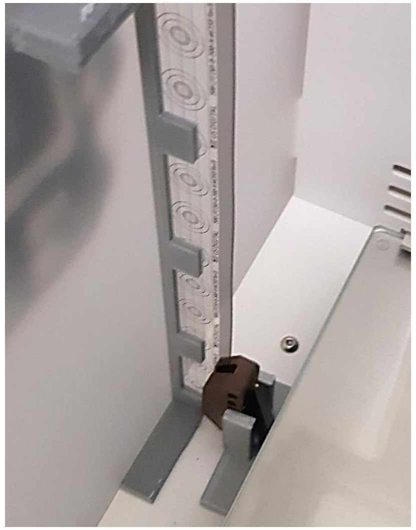
Pictures from our experiment on Ultimaker3 printer



Rotary optical encoder deployment steps



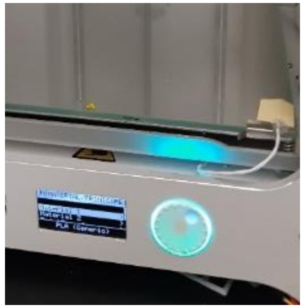
Encoders => Arduino -> control PC



Linear Strip Encoder for bed movement

Data Acquisition - Thermodynamics

Thermocouple mounted on nozzle



Thermistor mounted on printer bed

Thermocouple output

↓

MAX31855 driver to amplify signal

↓

Convert to nozzle temperature

Thermistor output

↓

Voltage Divider Circuit

↓

Convert to bed temperature

Nozzle and Bed Temperature sensors

Selected Sensors

Purpose	Sensor Type	Vendor	Model Number	Specs	Resolution as per System Deployment
X-axis	Optical-Rotary	US Digital	E2-512-315-NE-H-D-B	512 cycles/rev	0.1 mm
Y-axis	Optical-Rotary	US Digital	E2-512-315-NE-H-D-B	512 cycles/rev	0.1 mm
Z-axis	Optical-Linear Strip	US Digital	LIN-500-9.5-N	500 cycles/inch	0.012 mm
Filament	Optical-Rotary	US Digital	E2-2000-315-IE-E-D-3	2000 cycles/rev	0.0035 mm
Nozzle Temperature	Thermocouple	Adafruit	Type-k & MAX31855	Upto 500^oC	0.25^oC
Bed Temperature	Thermistor	Omega	SA1-TH-44006-40-T	Upto 120^oC	0.2^oC

Higher resolution sensors can be used for improved resolution

Go Back To Framework

G-code to synthesized data set

- Challenge
  - G-code file does not mention instruction execution time
  - Detection solution assumes no knowledge of firmware

```
222  ;TIME_ELAPSED:57.715992
223   ;LAYER:1
224   M140 S60
225 M106 S255
226 ;TYPE:FILL
227 ;MESH:single_bar_60x15x4mm_without_walls.stl
228 G1 F2400 X102.71 Y95.68 E24.93945
229 G1 X102.32 Y95.68 E24.94413
230 G1 X102.319 Y94.71 E24.95576
472   G0 F6000 X102.319 Y95.289
473   ;TIME_ELAPSED:98.312862
474   ;LAYER:2
475   ;TYPE:FILL
476;MESH:single_bar_60x15x4mm_without_walls.stl
477G1 F2400 X102.71 Y95.68 E42.42031
478 G1 X102.32 Y95.68 E42.42499
```

- Solution
  - Model the printer (firmware + hardware)
    - Linear and 2nd order derivatives based interpretation of instructions
    - Error is calculated and distributed across the layer data set after every layer

Error_{L-1} = Gcode-Time $_{L-1}$ - Modeled-Time $_{L-1}$

Error_{L-1} distributed across all data points in Dataset_{L-1}

Algorithm: G-code file to space and time profiles

Output: LayerMap and TimeProfile
Input: G-code File
while (! (End of G-code File))
    pickNextInstruction()
    if(layerEnd)
        finalize(LM,TP) for CurrentLayer
        update(z_profile)
    else if (PrintingParameter)
        Update Pms // current parameter set
    else if (MoveCommand)
        Update x2, y2, e2 $\leftarrow B_{x,y,e}$
        LM $\leftarrow$ pathProfile(x_1,y_1,e_1,x_2,y_2,e_2,LM, Pms)
        TP $\leftarrow$ timeProfile(TP, x_2,y_2,e_2 , Pms)
        Assign $x_1,y_1,z_1 \leftarrow x_2,y_2,e_2$
return LM, TP

G-code to Space-Domain

```
;START_OF_HEADER
;HEADER_VERSION:0.1
;FLAVOR:Griffin
;GENERATOR.NAME:Cura_SteamEngine
;GENERATOR.VERSION:4.0.0
;GENERATOR.BUILD_DATE:2019-03-19
;TARGET_MACHINE.NAME:Ultimaker 3
;EXTRUDER_TRAIN.0.INITIAL_TEMPERATURE:
;EXTRUDER_TRAIN.0.MATERIAL.VOLUME_USED
;EXTRUDER_TRAIN.0.MATERIAL.GUID:506c9f
;EXTRUDER_TRAIN.0.NOZZLE.DIAMETER:0.4
;EXTRUDER_TRAIN.0.NOZZLE.NAME:AA 0.4
;BUILD_PLATE.TYPE:glass
;BUILD_PLATE.INITIAL_TEMPERATURE:60
;PRINT.TIME:794
;PRINT.GROUPS:1
;PRINT.SIZE.MIN.X:106.013
;PRINT.SIZE.MIN.Y:97.005
;PRINT.SIZE.MIN.Z:0.27
;PRINT.SIZE.MAX.X:126.995
;PRINT.SIZE.MAX.Y:117.997
;PRINT.SIZE.MAX.Z:8.87
;END_OF_HEADER
;Generated with Cura_SteamEngine 4.0.0
T0
M82 ;absolute extrusion mode

G92 E0
M109 S210
G280 S1
G0 Z20.001
;LAYER_COUNT:44
;LAYER:0
M107
M204 S125
```

```
G1 X114.244 Y116.524 E2.57157
G1 X115.055 Y116.688 E2.58901
G1 X115.882 Y116.781 E2.60655
M205 X6 Y6
G0 F2100 X116.082 Y116.781
G0 X116.096 Y117.279
M205 X5 Y5
;TYPE:WALL-INNER
G1 F1500 X116.878 Y117.279 E2.62303
G1 X117.121 Y117.28 E2.62815
G1 X117.595 Y117.229 E2.6382
G1 X117.998 Y117.184 E2.64675
G1 X118.276 Y117.129 E2.65272
G1 X118.854 Y117.013 E2.66515
G1 X118.895 Y117.001 E2.66605
G1 X119.691 Y116.767 E2.68354
G1 X120.505 Y116.446 E2.70198
G1 X120.557 Y116.42 E2.7032
G1 X121.285 Y116.054 E2.72038
G1 X121.305 Y116.042 E2.72087
G1 X122.028 Y115.594 E2.7388
G1 X122.073 Y115.56 E2.73999
G1 X122.726 Y115.069 E2.75721
G1 X122.814 Y114.99 E2.7597
G1 X123.376 Y114.485 E2.77562
G1 X123.565 Y114.282 E2.78147
G1 X123.97 Y113.845 E2.79403
G1 X124.147 Y113.616 E2.80013
G1 X124.505 Y113.156 E2.81241
G1 X124.647 Y112.934 E2.81797
G1 X124.977 Y112.419 E2.83086
G1 X125.112 Y112.161 E2.837
G1 X125.382 Y111.645 E2.84927
G1 X125.548 Y111.242 E2.85846
```

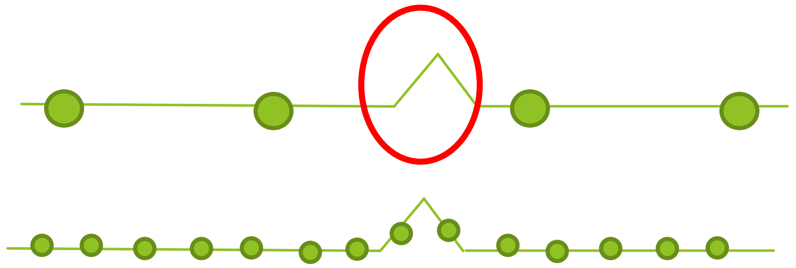
x-axis (m)	y-axis (m)	Time (sec)	Nozzle temperature (K)	Filment length (mm)	Printing Status
0.0262	0.0206	133.806	478	1279.644	1
0.0262	0.0207	133.809	478	1279.645	1
0.0262	0.0208	133.811	478	1279.646	1
0.0262	0.0209	133.813	478	1279.647	1
0.0262	0.021	136.975	478	1280.539	1
0.0262	0.0211	136.977	478	1280.54	1
0.0262	0.0212	136.978	478	1280.541	1
0.0262	0.0213	136.979	478	1280.542	1
0.0262	0.0214	136.98	478	1280.543	1
0.0262	0.0215	136.982	478	1280.544	1
0.0262	0.0216	139.523	478	1281.455	1
0.0262	0.0217	139.524	478	1281.457	1
0.0262	0.0218	139.525	478	1281.458	1
0.0262	0.0219	139.526	478	1281.459	1
0.0262	0.022	139.527	478	1281.46	1
0.0262	0.0221	139.529	478	1281.461	1
0.0262	0.0222	139.53	478	1281.462	1
0.0262	0.0223	54.613	478	1247.71	1
0.0262	0.0224	54.609	478	1247.709	1
0.0262	0.0225	54.606	478	1247.708	1
0.0262	0.0226	54.603	478	1247.707	1
0.0262	0.0227	54.601	478	1247.705	1
0.0262	0.0228	79.442	478	1259.976	1
0.0262	0.0229	79.442	478	1259.976	1
0.0262	0.023	79.442	478	1259.976	1
0.0262	0.0231	79.442	478	1259.976	1
0.0262	0.0232	141.404	478	1275	1
0.0262	0.0233	141.404	478	1275	0

Go Back To Framework

Sensors data to time and space domain profile

- Alignment move
  - $(\Delta x > 0 \;||\; \Delta y > 0)$ & $\Delta e == 0$
- Extrusion move
  - $(\Delta x > 0 \;||\; \Delta y > 0)$ & $\Delta e > 0$

- Filament moves much slower than x/y motors
- Is this an extrusion and alignment move?
- Sampling rate: the higher the better ?



$FS_{t1} = a$; $FS_{t2} = a$; $FS_{t3} = a'$; $FS_{t3} = a'$

- Solution:
  - Higher resolution sensors for low speed axis
  - Dual sampling rate introduced
  - High sampling to track nozzle movement
  - Low sampling to establish the filament extrusion state
  - Sampling rates
    - covers the printing speed limits
    - Acquisition system capacity

Raw sensors data to time domain

Starting Marker	Time (ms)	X-axis (mm)	Y-axis (mm)	Z-axis (mm)	Filament Consumed (mm)	Nozzle Temperature (C)	Bed Temperature (C)	Ending Marker
S	378200.03	201.58	302.66	9.59	88.8	198.75	59.5	T
S	378205.15	201.7	302.54					T
S	378210.09	201.84	302.42					T
S	378215.03	201.97	302.28					T
S	378220.09	202.11	302.15					T
S	378225.09	202.23	302.01					
S	378230.12	202.34	301.89					T
S	378235.03	202.46	301.8					T
S	378240.09	202.48	301.74					T
S	378245.09	202.27	301.74					T
S	378250.09	202.05	301.74	9.59	88.814	198.75	59.5	T
S	378255.09	201.97	301.76					T
S	378260.06	201.95	301.78					T
S	378265.12	201.95	301.82					T
S	378270.03	201.91	301.85					T
S	378275.12	201.84	301.91					T
S	378280.03	201.76	301.99					T
S	378285.06	201.68	302.07					T
S	378290.12	201.6	302.17					T
S	378295.03	201.5	302.25					T
S	378300.03	201.39	302.36	9.59	88.825	198.75	59.5	T
S	378305.25	201.27	302.48					T

Fast Samplesteady Samples

Time (sec)	x-axis (m)	y-axis (m)	Nozzle temperature (K)	Filment length (mm)	Printing Status
0	0.068	0.003	477.62	0	1
0	0.068	0.003	477.62	0	1
0.05	0.067	0.003	477.62	0.014	1
0.1	0.066	0.003	477.62	0.029	1
0.15	0.065	0.003	477.62	0.039	1
0.2	0.064	0.003	477.62	0.053	1
0.25	0.063	0.003	477.62	0.068	1
0.3	0.062	0.003	477.62	0.082	1
0.35	0.061	0.003	477.62	0.085	1
0.355	0.0609	0.003	477.62	0.087	1
0.36	0.0608	0.003	477.62	0.09	1
0.365	0.0607	0.003	477.62	0.093	1
0.37	0.0606	0.003	477.62	0.095	1
0.375	0.0605	0.003	477.62	0.098	1
0.38	0.0604	0.003	477.62	0.101	1
0.385	0.0603	0.003	477.62	0.103	1
0.39	0.0602	0.003	477.62	0.106	1
0.395	0.0601	0.003	477.62	0.109	1
0.4	0.06	0.003	477.62	0.111	1
0.405	0.0599	0.003	477.62	0.113	1
0.41	0.0598	0.003	477.62	0.114	1
0.415	0.0597	0.003	477.62	0.116	1
0.42	0.0596	0.003	477.62	0.117	1
0.425	0.0595	0.003	477.62	0.119	1
0.43	0.0594	0.003	477.62	0.12	1
0.435	0.0593	0.003	477.62	0.122	1
0.44	0.0592	0.003	477.62	0.123	1
0.445	0.0591	0.003	477.62	0.125	1
0.45	0.059	0.003	477.62	0.126	1

Raw sensors data to space domain

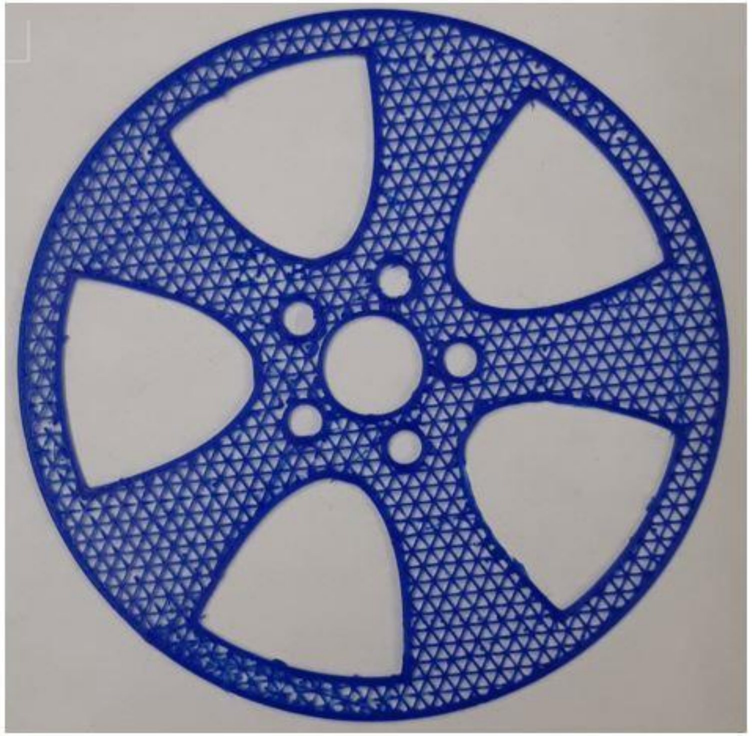
Starting Marker	Time (ms)	X-axis (mm)	Y-axis (mm)	Z-axis (mm)	Filament Consumed (mm)	Nozzle Temperature (C)	Bed Temperature (C)	Ending Marker
S	378200.03	201.58	302.66	9.59	88.8	198.75	59.5	T
S	378205.15	201.7	302.54					T
S	378210.09	201.84	302.42					T
S	378215.03	201.97	302.28					T
S	378220.09	202.11	302.15					T
S	378225.09	202.23	302.01					
S	378230.12	202.34	301.89					T
S	378235.03	202.46	301.8					T
S	378240.09	202.48	301.74					T
S	378245.09	202.27	301.74					T
S	378250.09	202.05	301.74	9.59	88.814	198.75	59.5	T
S	378255.09	201.97	301.76					T
S	378260.06	201.95	301.78					T
S	378265.12	201.95	301.82					T
S	378270.03	201.91	301.85					T
S	378275.12	201.84	301.91					T
S	378280.03	201.76	301.99					T
S	378285.06	201.68	302.07					T
S	378290.12	201.6	302.17					T
S	378295.03	201.5	302.25					T
S	378300.03	201.39	302.36	9.59	88.825	198.75	59.5	T
S	378305.25	201.27	302.48					T

Fast Samplesteady Samples

x-axis (m)	y-axis (m)	Time (sec)	Nozzle temperature (K)	Filment length (mm)	Printing Status
0.0044	9.00E-04	3.67	478	1.087	1
0.0044	0.001	3.67	478	1.087	1
0.0044	0.0011	25.465	479	8.226	1
0.0044	0.0012	25.465	479	8.226	1
0.0044	0.0013	25.465	479	8.226	1
0.0044	0.0014	25.465	479	8.226	1
0.0044	0.0015	25.465	479	8.226	1
0.0044	0.0016	999	295	0	0
0.0044	0.0017	43.27	478	12.183	1
0.0044	0.0018	43.27	478	12.183	1
0.0044	0.0019	43.27	478	12.183	1
0.0044	0.002	43.27	478	12.183	1
0.0044	0.0021	43.27	478	12.183	1
0.0044	0.0022	43.255	478	12.178	1
0.0044	0.0023	43.435	478	12.217	1
0.0044	0.0024	43.435	478	12.217	1
0.0044	0.0025	43.435	478	12.217	1
0.0044	0.0026	43.435	478	12.217	1

Go Back To Framework

Sophos3DP space domain representation



Camera image of the printed part

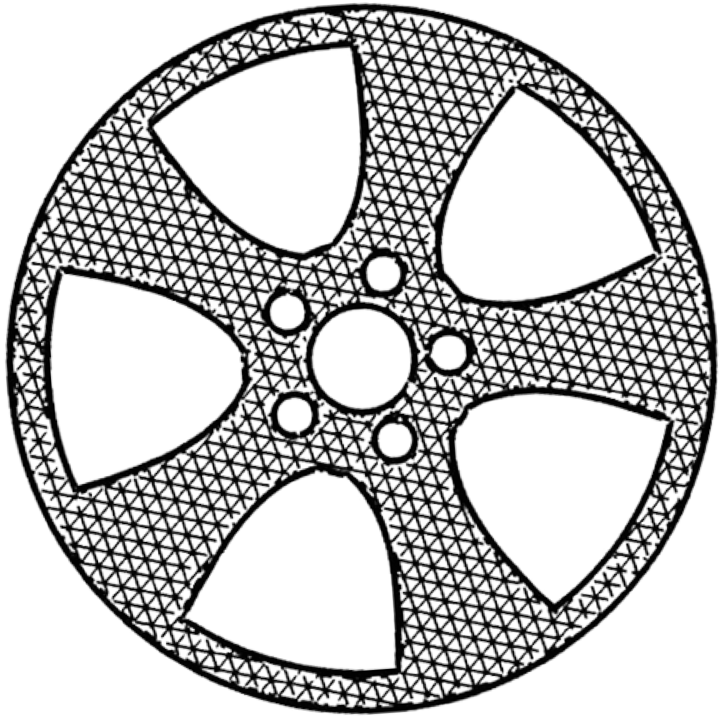


Image generated by Sophos3DP from the sensors data set (single layer)

Process analysis

- Pixel for pixel || sample for sample mapping?
- Three distinct view points
  - Time domain
  - Space domain
  - G-code instruction
- Evaluation carried out **after each layer** is printed

Aspects to Analyze	Features
Layer Geometry	Dimensions, Shape
Filament Consumption	Per layer, Per region, per G-code command
Z-profile	Layer Thickness
Timing Profile	Toolpath Sequence, Speed
Thermal Profile	Nozzle Temperature, Bed Temperature
G-code Command Verification	Vertices, Path, Filament Consumption, Command Sequence

Algorithm : G-code commands verification

Output: G-code commands integrity status

Input: G-code file , SensorData

Synchronize sample series "S" with 1st command>1mm:

move from A to B

∀ i ∈ SampleSequence

Assume $s_i = A$, if ∃ s_j s.t.

$|d_{i,j} - |AB|| \leq th_{vertex}$ // ie. B in vicinity of (s_j)

AND $slope_{AB} \equiv slope(s_i , s_j)$

if s_j NotFound → return: **Sync Failed**

else **Sync Achieved, Verify Individual Cmds**

∀ k ∈ Gcode_Mov_Cmds:

Find sample s_i corresponding to vertex A

if A found:

refineVertex(A)⟶ s_i

while B found: Chronologically test fol

1. $d(s_{i+1} - B) \leq d(s_i - B)$
2. dist $(s_i - AB) \leq th_{point\ 2line}$

if B found:

refineVertex(B)⟶ sj

else: return "**Cmd k failed** due to {Reason}"

// Filament consumption test //

if $((e(s_j)\text{-}e(s_i)) - (e_B - e_A)) \leq th_{filament}$

"**Cmd k Verified**"

else return Cmd k failed due to {Reason}

return "**Cmd verification test passed**"

Attack verdict processing

- Challenges
  - Physical process has tolerances
  - Measurement errors
  - Slicer software estimation errors
  - Modeling approximation errors
- Our approach
  - Print a set of various benign objects
  - Tweak the alert thresholds to ensure zero FP [each feature is already calibrated]
  - Print a set of attacked samples with high magnitude deviations
  - Gradually reduce the magnitude of attack parameter to the boundary of zero FN
  - Set of parameter values corresponding to zero FP and zero FN represents Sophos3DP performance

Sophos3DP detection thresholds

- Printed objects of various shapes / infills / speeds / other printing parameters
- Find out deviations b/w sensors data and corresponding G-codes
- Alert thresholds relaxed till the achievement of zero False Positives
- For a 5 cm x 5 cm-> 2500 mm^2, 1 mm^2 deviation is 0.04 %

S /No	Performance Parameters	Related Attack	Alert Thresholds
1	Single Mismatched Area	Geometry	1 mm^2
2	Cumulative mismatched area	Geometry	2% per layer, min dimension >0.2 mm
3	Nozzle Temperature Deviation	Thermodynamics	5^oC
4	Time window for sample search	Timing Profile	2 seconds
5	Samples Mismatch per Layer	Timing Profile	2%
6	Continuous Mismatch Duration	Timing Profile	500 ms
7	Max Layer Thickness Difference	Geometry	0.05 mm for 500 ms
8	Bed Temperature Difference	Thermodynamics	5^oC for 500 ms
9	Filament Consumption Deviation per move	Density, Geometry	5% diff per move
10	Filament Consumption Deviation per Layer	Density, Geometry	1% diff per layer
11	Max Nozzle Deviation	Geometry	0.75 mm $\perp$ to move path
12	Max Vertex Deviation	Geometry	0.75 mm

Performance of detection algorithms

Attack Type	Attack Mechanism	Parameters Impacted	Algorithms Performance *			Final Result and Performance Description	Existing State of the Art
			1	2	3		
Filament Status	Switched off extruder motor for 1 infill command	Filament consumption Space layout Timing Synchronization	✓	✓	✓	Detected (100ms+) 1% filament deviation / layer, 5% per command	Not Detected
Filament Density	Reduced the filament consumption for 2 infill lines	Filament consumption Space layout Timing Synchronization	✓	✓	✓	Detected 1% deviation per layer, 5% per command	Not Detected
Nozzle Temperature	Changed nozzle temperature by ±10C	Nozzle temperature profile	✓	✓	✗	Detected; Capable to detect lower deviations	Not Detected
Bed Temperature	Changed bed temperature by ±5C	Bed temperature profile	✗	✓	✗	Detected	Not Detected
Infill Pattern	Line/Triangle/Grid/ Gyroid	Space layout Timing Synchronization	✓	✓	✓	Detected	Detected [13]
Infill Density	20%,21%, 30%, 31%, 40%,41%	Space layout Timing Synchronization	✓	✓	✓	Detected; 1% verified;	Presented case: 10% deviation [15] Any deviation > 1sec [12]

1: Space domain analysis ; 2: Time domain analysis; 3: G-code command verification

Layer Thickness	Changed z-move from 0.2 mm to 0.1 mm	Z-axis Synchronization	✗	✓	✗	Detected	0.1mm with multiple sensors [17] OR if repeated over multiple layers [16]
Geometry limits (x_{min}, y_{min} – x_{max}, y_{max})	Changed outer dimensions by ±0.3mm over one axis	Space layout	✓	✗	✓	Detected; verified General rule: $1mm^2$ single area or 2% total mismatch	Not addressed as a benchmark
Cavity	No cavity, 1x1mm, 2x2mm, 3x2mm, 3x3mm cavities	Space integrity Timing Synchronization	✓	✓	✓	Detected	4 mm over one axis [17]
Toolpath Sequence	Sequence of 3 move commands modified (total $\Delta t < 1$ sec)	Relative toolpath deviation	✗	✗	✓	Detected, if vertices distance > 1mm ; $\Delta t < 1$ sec is detectable	$\Delta t \geq 2.26$ sec [12]
Toolpath Add / Delete	Single command (< 1 sec, 2mm) with no extrusion	Space layout Relative toolpath deviation	✓	✗	✓	Detected, if distance > 1mm	1 sec duration (translated to >10 mm) [12]
Toolpath Add / Delete	Two short commands 'to &fro' (< 1sec, 2mm) with no extrusion	Relative toolpath deviation	✗	✗	✓	Detected; if distance > 1mm	Not presented; we assume 1 sec (as above)
Toolpath Add / Delete	Multiple consecutive small (<1mm) commands sequence lasting for over 2 sec	Timing Synchronization	✗	✓	✗	Detected, if cumulative distance of single seq > 1 mm OR if $\Sigma (\Delta t) > 2$ sec	Not presented; we assume 1 sec (as above)
Printing Speed	w/o modifying the path, changed the printing speed to create 2 seconds difference	Timing Synchronization	✗	✓	✗	Detected, as and if cumulative time difference > 2 sec	$\Delta v \geq \pm 25$mm/s [17] 0.8 sec [12]

1: Space domain analysis ; 2: Time domain analysis; 3: G-code command verification

Sophos3DP Evaluation

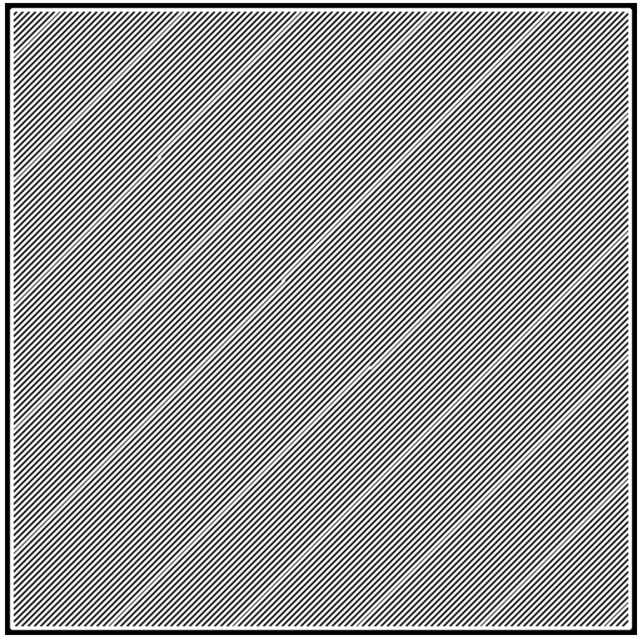
Sophos3DP Performance on Test Attacks

- 16 different types of attacks conducted
- Patterns and design files were changed BUT attack magnitudes kept bigger than the detection capability
- All attacks successfully detected

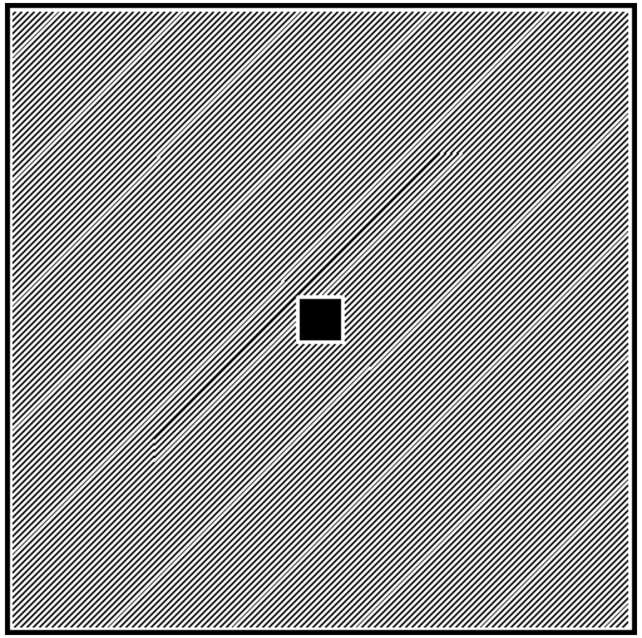
Attack Name	Attack Mechanism	Affected Domain
Filament status	Switch off the extruder for 1 infill command	FK
Filament density	Reduce the filament speed for 2 infill lines	FK
Filament-kinetic based cavity	Retract the filament for 2 infill lines 2 mm long, Path change:Nil; Time Diff:0.4 sec	FK, NK minimal
Nozzle temperature	Change the nozzle temperature by $\pm 10^{o}$C in central region of rectangular bar	THM
Bed temperature	Change the bed temperature by 6^{o}C	THM
Infill pattern	Swap among the Line/Triangle/Grid or other infill patterns	FK, NK
Infill density	Change infill density from 20% to 21% ; 30% to 31% ; 40% to 41% (1% change at different density levels)	FK, NK
Z-axis 1 layer	Change layer thickness of a single layer by 0.1 mm	ZK
Z-axis multiple layers	Change thickness of three layers by 0.04 mm each	ZK
Outer geometry	Change outer dimensions by 0.3 mm for a single axis	FK, NK
Cavity via design file	Create a cavity of 1x1 mm, 2x2 mm, 3x2 mm through design file	FK, NK
Path sequence	Modify 3 mov cmds, Δ t <1sec	FK, NK
Add/delete single move	Add 2 mm long, <1 sec cmd w/o extrusion	FK, NK
Add/delete 2 moves	Add 2 cmds of 2 mm and under 1sec duration w/o filament extrusion [A>B, B>A]	FK, NK
Add/delete multiple small moves	Insert multiple cmds <1 mm each, lasting for 2 secs	NK
Printing speed	Change printing speed to cause $\Delta t \geq 2$sec, w/o path change	FK, NK

Cavity Attack based on Design Change

- Change in design stage results in BIG attack footprint
  - G-code commands sequence
  - Space domain layout
  - Timing profile
  - Filament-kinetic profile

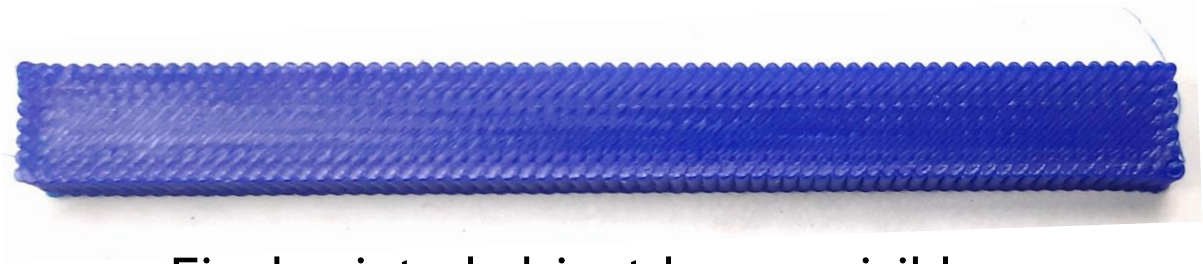


Intermediate Layer – Original File

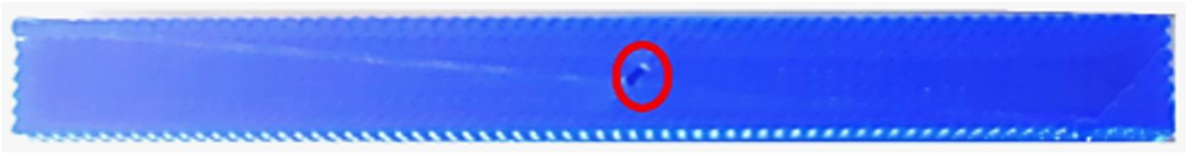


Intermediate Layer – After Attack

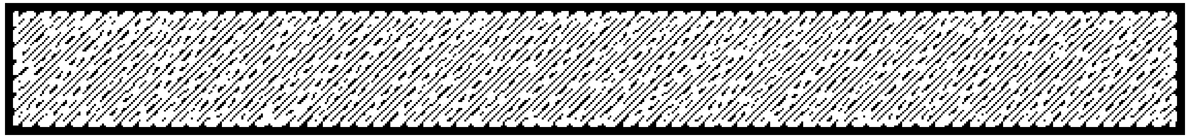
Cavity Attack based on Filament Kinetics



Final printed object has no visible deformation



Cavity seen during the printing – picture taken after printing is paused

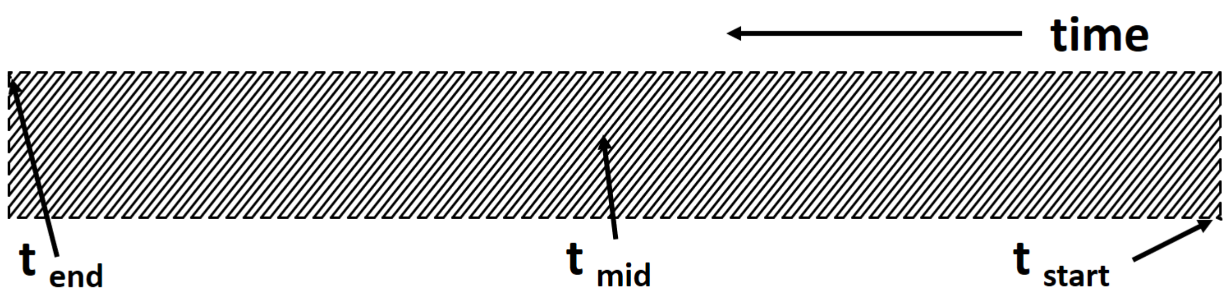


Bitmap image generated from the G-code file

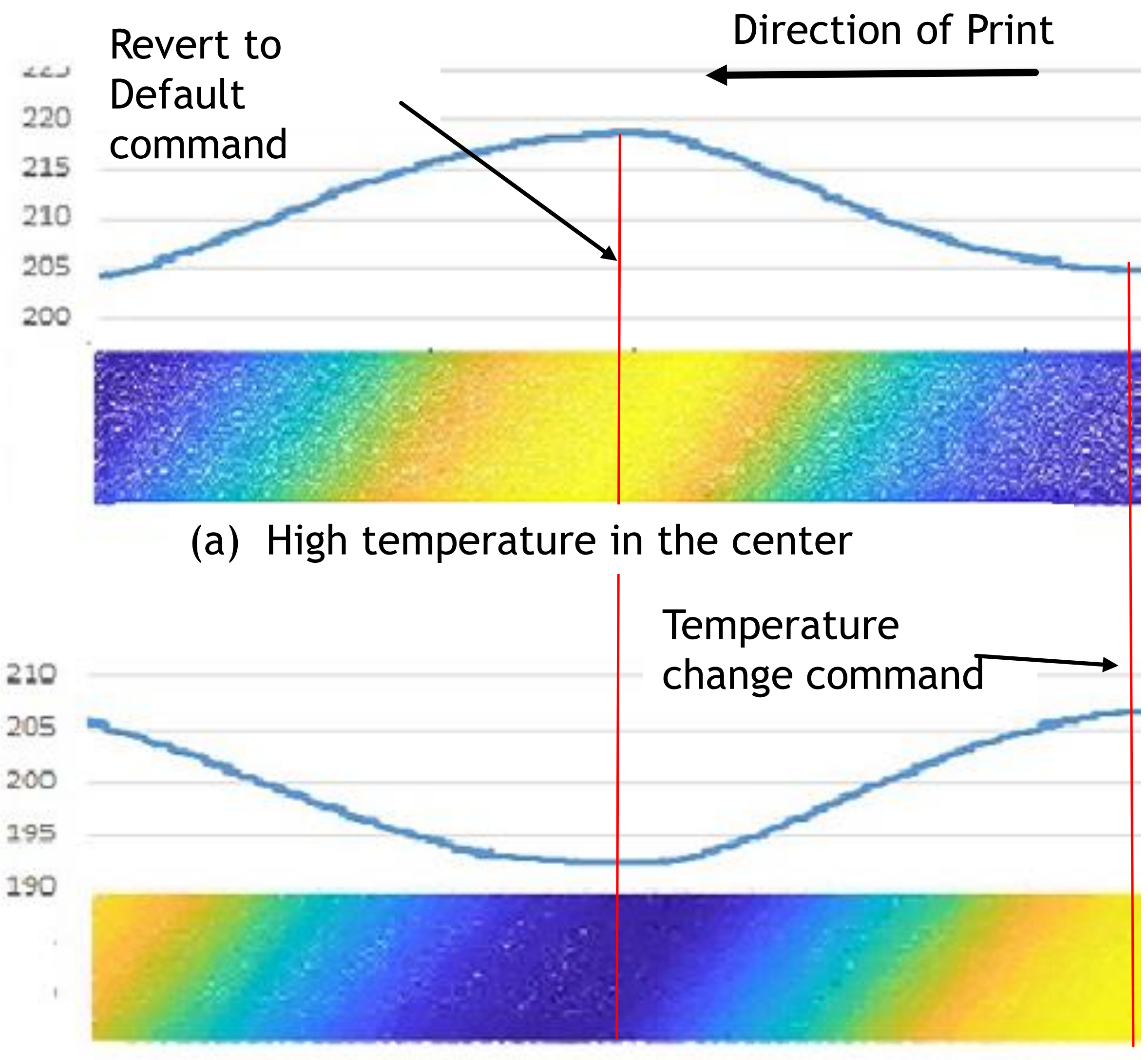
Bitmap image generated from the sensors data

Thermodynamic Attacks

- Planned temperature variations can induce thermal stresses in the object
- Two attack variations
  - Increasing the temperature
  - Reducing the temperature



Infill pattern toolpath sequence in the rectangular bar



(a) High temperature in the center

(b) Low temperature in the center

Toolpath Re-sequence Attack

- Toolpath sequence is important parameter in FDM
- Tested Sophos3DP on very small change
  - 3 commands creating corner triangle re-sequenced
- Detects on the first modified command

Original G-code

```
   G1 X92.175 Y129.844 E16.81589
1) G1 X92.175 Y131.825 E16.85359
2) G1 X94.153 Y131.823 E16.89126
3) G1 X92.174 Y129.844 E16.94456
   M205 X6 Y6
   G1 F1500 E12.44456
```

SYNCHRONIZED

3 CMDS SEQUENCE CHANGED

RE-SYNCHRONIZED

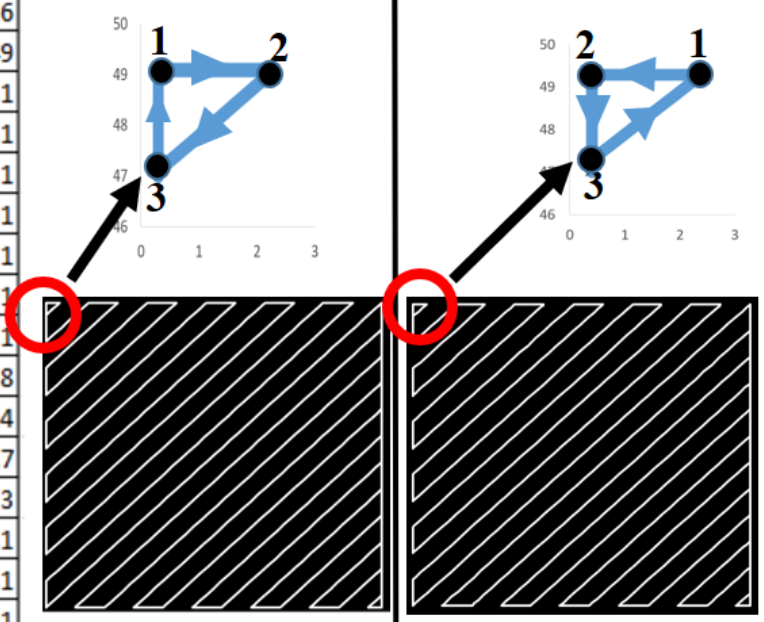
Modified Sequenced G-code

```
   G1 X92.175 Y129.844 E16.81589
2) G1 X94.153 Y131.823 E16.86915
1) G1 X92.174 Y131.823 E16.90686
3) G1 X92.174 Y129.844 E16.94456
   M205 X6 Y6
   G1 F1500 E12.44456
```

Time (sec)	x-axis (mm)	y-axis (mm)
41	0.3	47
41.05	0.3	47.9
41.1	0.3	48.6
41.15	0.3	49
41.2	0.3	49.1
41.25	0.4	49.1
41.3	0.8	49.1
41.35	1.4	49.1
41.4	2	49.1
41.45	2.2	49.1
41.5	2.3	49.1
41.55	2	48.8
41.6	1.6	48.4
41.65	0.9	47.7
41.7	0.5	47.3
41.75	0.3	47.1
41.8	0.3	47.1
41.85	0.3	47.1
41.9	0.3	47.1

$X_{trace} = X_{G\text{-}code} - 91.875$
$Y_{trace} = Y_{G\text{-}code} - 82.844$

Sophos Alerts on 1st modified command



Time (sec)	x-axis (mm)	y-axis (mm)
40.9	0.40	47.00
40.95	0.40	47.20
41	0.50	47.40
41.05	0.70	47.60
41.1	1.30	48.20
41.15	1.90	48.80
41.2	2.30	49.20
41.25	2.40	49.30
41.3	2.30	49.30
41.35	1.90	49.30
41.4	1.20	49.30
41.45	0.70	49.30
41.5	0.50	49.30
41.55	0.40	49.20
41.6	0.40	49.00
41.65	0.40	48.50
41.7	0.40	47.80
41.75	0.40	47.40
41.8	0.40	47.30

3 commands Re-sequence lasts for 0.9 secs; detected on 1st command

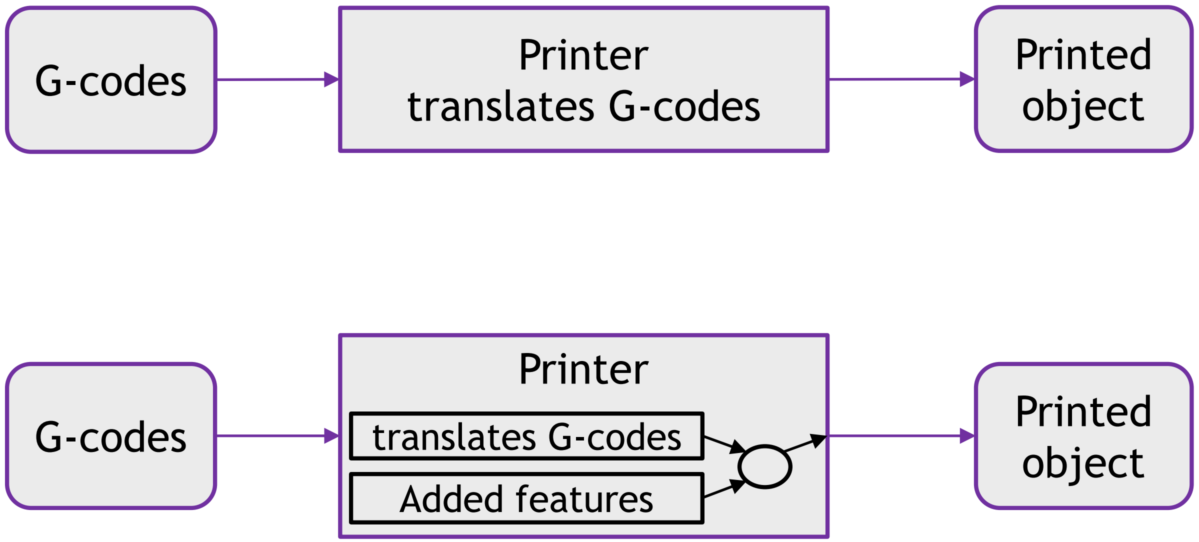
(a) Original Sequence Trace

(b) Modified Sequence Trace

Future Work

Future Work – Sophos3DP+

- Monitoring direct manipulable processes – Missing elements
- Attack may not be detectable in one layer
  - XZ, YZ, any other plane or not confined to a plane
- Features not incorporated in G-codes



Conclusion

- Sophos3DP is a modular integrity checking framework
- It utilizes ubiquitous sensors to attain printing state independent of the process chain
- Deploys multi-domain analysis to detect inconspicuous attacks
- No machine learning or profile generation required for new objects
- Aligned with Industry 4.0 vision of mass customization
- Future directions

Security & Forensics Engineering Lab

Thanks!!

Questions?

Presenter: Muhammad Haris Rais raismh@vcu.edu

Ye Li yli@bradley.edu

Irfan Ahmed iahmed3@vcu.edu