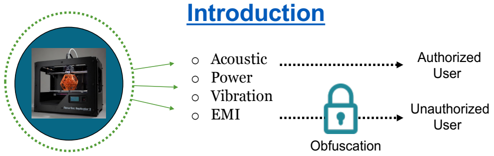
Defending Side Channel Attacks in Cyber-Physical Additive Layer Manufacturing Systems (Project Number : CNS 1546993)

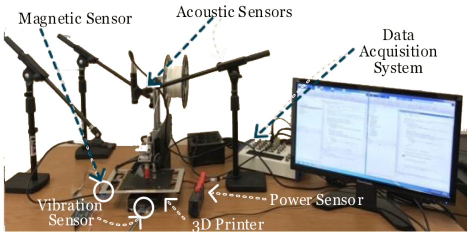
Sujit Rokka Chhetri, Sina Faezi, Mohammad Al Faruque (PI)
University of California, Irvine
{schhetri ,sfaezi, alfaruqu}@uci.edu

Introduction



Physical components of a 3D printer (such as motors, heaters, etc.) leak data in side-channels (such as acoustic, electromagnetic, power, etc.) while printing 3D objects.

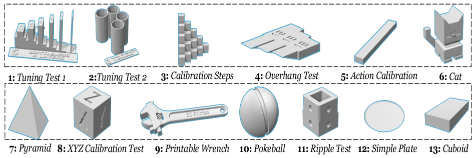
Overview



Test Bed

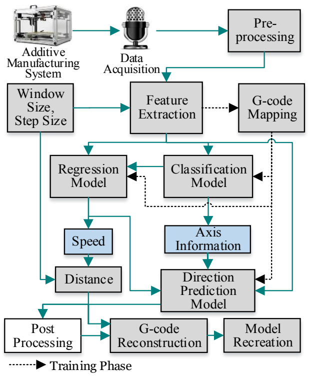
In this work, we try to analyze the side-channel emissions with various objectives, highlighted as follows:

- **Side-channel attack on AM:** We propose an attack model, using which, an attacker may reverse engineer the Intellectual property inherent in the 3D objects.
- **Secured CAM tool:** We propose a data-driven algorithm that can be used by Computer Aided Manufacturing (CAM) tools to reduce the information leakage from the side-channels.
- **Kinetic cyber attack detection:** These kind of attacks can be embedded in firmware of a 3D printer, CAM, or CAD tool and result in distortion of final output object of AM. In our work, we utilize the behavioral model of the AM created using the side-channel emissions, to detect these kind of kinetic cyber-attacks.



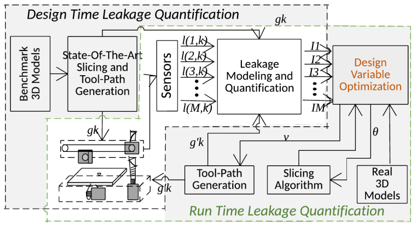
Benchmark 3D objects

Side-Channel attack on AM [1]



- ➢ **Regression Model:** Predicting continuous speed values.
- ➢ **Classification Model:** Predicting discrete axis of movement.
- ➢ **Direction Prediction:** Direction of nozzle in each axis.

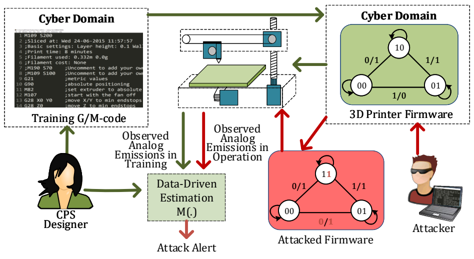
Secured CAM Tool [2]


Design Time Leakage Quantification
Benchmark 3D Models
State-Of-The-Art Slicing and Tool-Path Generation
Sensors
l(1,k)
l(2,k)
l(3,k)
l(M,k)
Leakage Modeling and Quantification
I1
I2
I3
IM
Design Variable Optimization
gk
g'k
v
θ
Tool-Path Generation
Slicing Algorithm
Real 3D Models
Run Time Leakage Quantification

We utilize the design and process parameters of 3D printing that do not not affect the quality of printed 3D objects. These parameters are as follow:

- **Speed ($\mathcal{V}$) :** Slight variation in speed does not affect the quality of the print. However, experiments show that printing with certain speeds can minimize leakage from side-channels.
- **Direction (θ) :** PCA of facets' normal is used to determine the general directionality of an object. Changing direction of the object over XY base plate has no effect on quality of print.

Kinetic Cyber-Attack Detection [3]

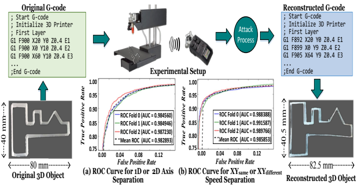


```
1 M109 S200
2 ;Sliced at: Wed 24-06-2015 11:57:57
3 ;Basic settings: Layer height: 0.1 Wal
4 ;Print time: 8 minutes
5 ;Filament used: 0.332m 0.0g
6 ;Filament cost: None
7 ;M190 S70      ;Uncomment to add your ow
8 ;M109 S100     ;Uncomment to add your ow
9 G21            ;metric values
10 G90           ;absolute positioning
11 M82           ;set extruder to absolute
12 M107          ;start with the fan off
13 G28 X0 Y0     ;move X/Y to min endstops
14 G28 Z0        ;move Z to min endstops
```

- CPS designer trains a data-driven model which models the relationship between the analog emission in the side-channel and the cyber-domain data.
- While printing, the user continuously compares the analog emissions with estimated ones. By monitoring the difference, it then warns the user about the possibility of existence of an kinetic cyber-attack in the system.

Results

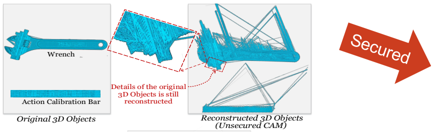
1



```
; Start G-code
; Initialize 3D Printer
; First Layer
G1 F900 X20 Y0 Z0.4 E1
G1 F900 X0 Y10 Z0.4 E2
G1 F900 X60 Y10 Z0.4 E3
...
;End G-code
```

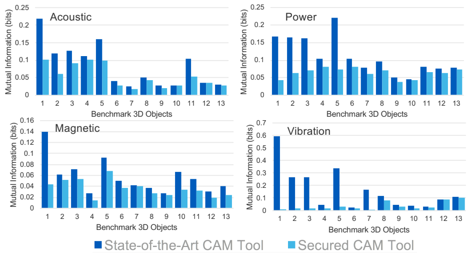
```
; Start G-code
; Initialize 3D Printer
; First Layer
G1 F892 X20 Y0 Z0.4 E1
G1 F899 X0 Y9 Z0.4 E2
G1 F905 X64 Y9 Z0.4 E3
...
;End G-code
```

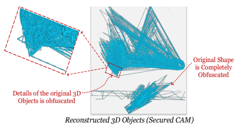
Acoustic side-channel attack for objects with simple geometry

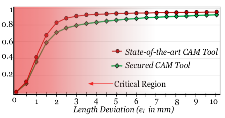

Wrench
Action Calibration Bar
Original 3D Objects
Details of the original 3D Objects is still reconstructed
Reconstructed 3D Objects (Unsecured CAM)
Secured

Multi-modality *side-channel attack for reconstructing real objects without post processing*

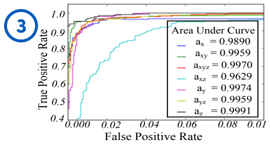
2



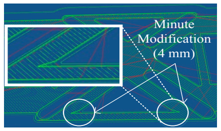

Details of the original 3D Objects is obfuscated
Original Shape is Completely Obfuscated
Reconstructed 3D Objects (Secured CAM)



3



ROC Curve for Axis Modification Detection



G-code Trace After Kinetic Attack

1. Average accuracy for axis Classification 86.00%, length. regression 88.89%, test key object reconstruction: 92.48%.
2. Average drop in mutual information 24.7% , average Increase in Time 0.58%. The success rate for reconstructing the 3D objects, when incorporating the secured CAM tool, is reduced.
3. All attacks resulted in more than 4mm deviation in the 2nd,3rd, and 5th layer were detected in quadcopter's baseplate . Average detection in range of variations: 77.45%.

Conclusion

- We provide a proof of concept that additive manufacturing systems are vulnerable to side-channel attacks.
- We presented a novel defense mechanism that can be incorporated in the CAM tools for minimizing the information leakage in the side-channels.
- We used side-channel data, in our advantage, for detecting kinetic cyber attacks on AM.

References

1. A. Faruque, M. Abdullah, et al., "Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems," ACM Transactions on Cyber-Physical Systems, 2017.
2. S. R. Chhetri et al., "Fix the leak! an information leakage aware secured cyber-physical manufacturing system," in 2017 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1408–1413, IEEE, 2017.
3. S. R. Chhetri et al., "Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems," in Computer-Aided Design (ICCAD), 2016 IEEE/ACM International Conference on, pp. 1–8, IEEE, 2016.