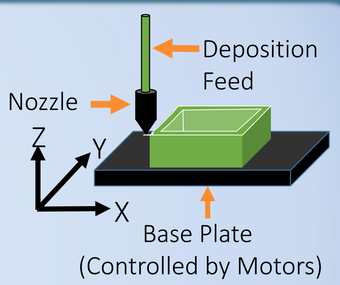
# Exploiting Acoustic Side-Channel for Attack on Additive Manufacturing Systems

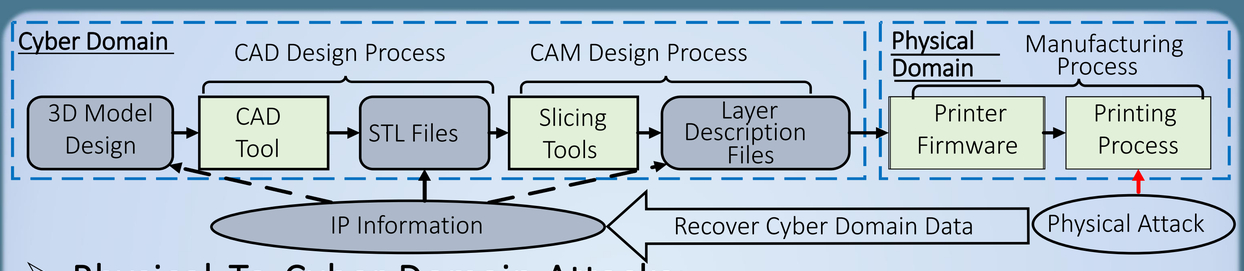
Sujit Rokka Chhetri, Arquimedes Canedo†, Mohammad Abdullah Al Faruque
University of California, Irvine
{schhetri, alfaruqu}@uci.edu, †arquimedes.canedo@siemens.com

## Introduction

- **Additive Manufacturing:**
  - Build 3D objects in layers.
  - Rapid prototyping of freeform 3D objects.
  - Disruptive technology [1]. E.g. 3D-Printers.
- **Side-Channels:**
  - Power, acoustic, electromagnetic, timing etc.
- **Intellectual Property (IP):**
  - Internal and external 3D geometry, process parameters, machine parameters [2] etc.



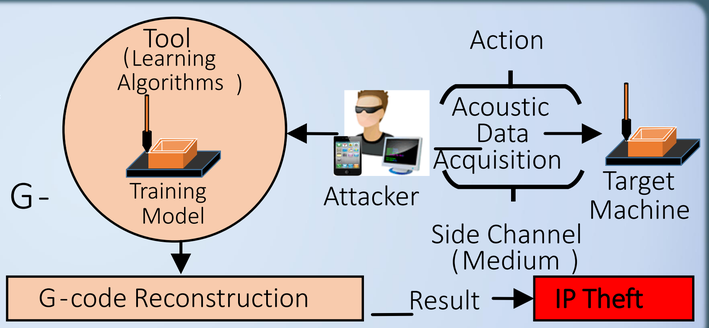

## Background and Motivation



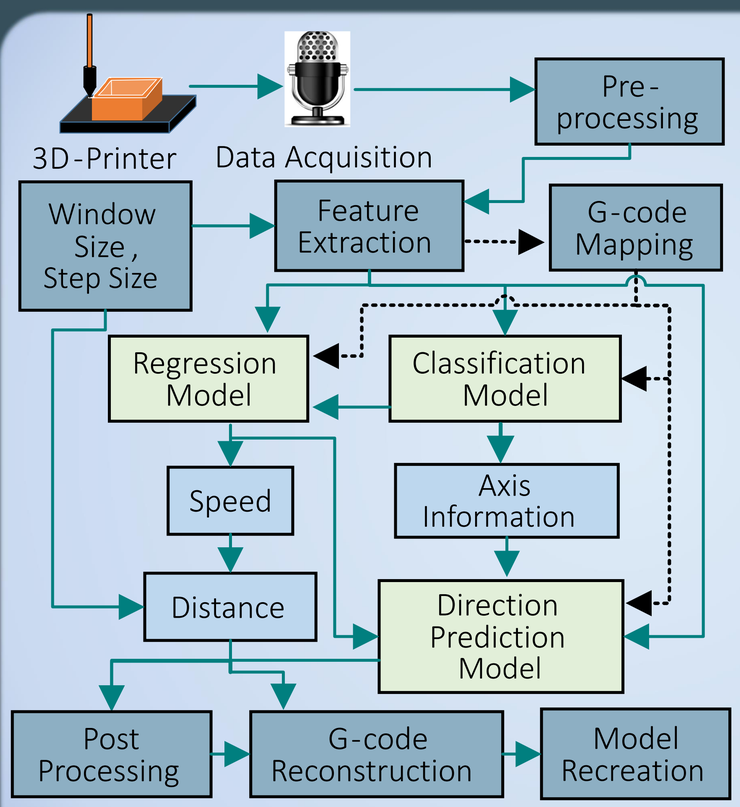

- **Physical-To-Cyber Domain Attacks:**
  - Utilize physical domain data to conduct attack on Confidentiality (steal IP), Integrity, and Availability (CIA).
- **Side-Channel Leakage in Additive Manufacturing:**
  - Acoustic signal vary in frequency and intensity according to load, speed and direction of the nozzle movement.

## Acoustic Attack Model

- **Attack Model [3]:**
  - Train Learning Algorithms.
  - Record acoustics.
  - Extract Information about G-code (Used in 3D-Printes).
  - Reconstruct the Object.

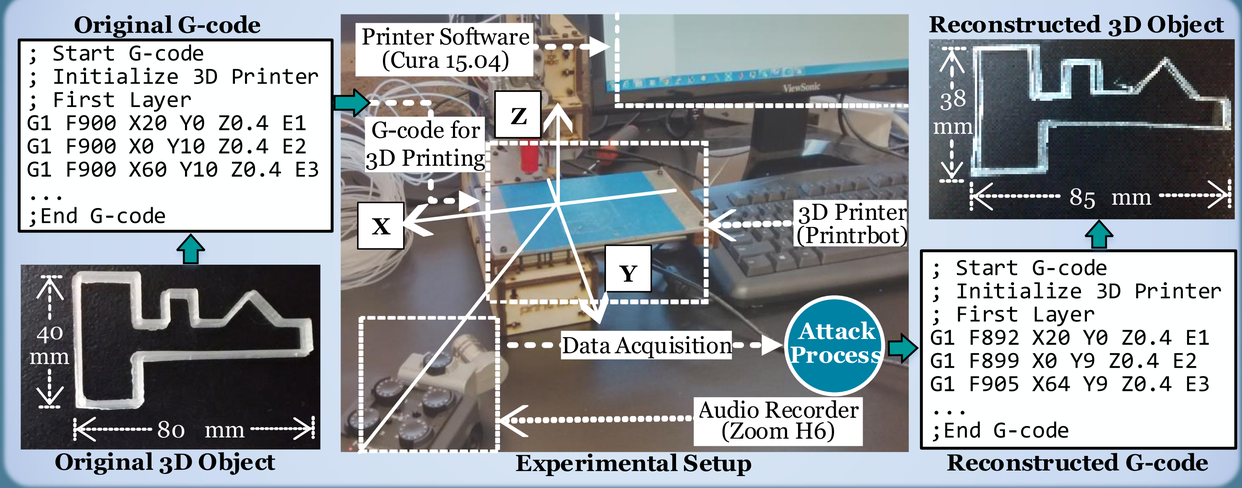



## Attack Methodology

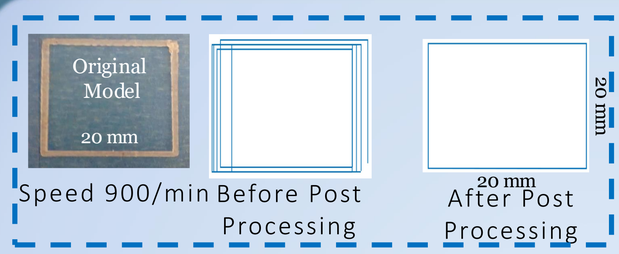


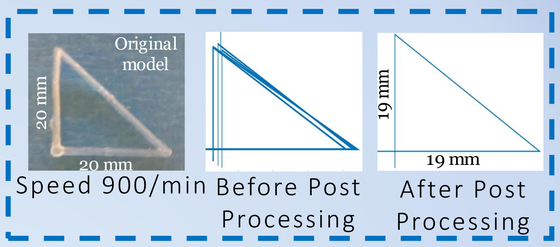

- **Attack Method [3]:**
  - Pre-process to remove noise.
  - Extract time and frequency domain features.
  - Train different learning algorithms to extract speed, axis, and direction.
  - Predict parameters.
  - Context based post-processing to improve accuracy.
  - Reconstruct G-code.

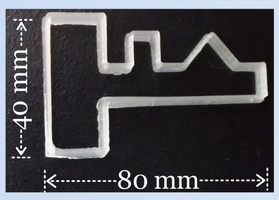
## Experimental Setup



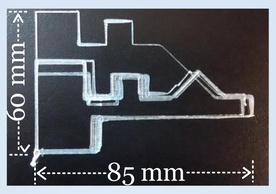

## Results



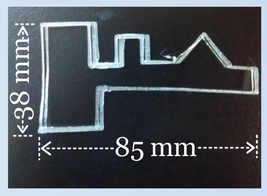




i)Original 3D-Printed Key




ii)Reconstructed Key Before Post Processing




iii)Reconstructed Key After Post Processing

- **Test Parameters:**
  - Speed, Dimension, and Complexity (Movement in Multiple Axes).
- **Average Accuracy:**
  - Axis Prediction Accuracy Classification Models: **78.35%**.
  - Length Prediction Error of Regression Models: **17.82%.**
  - **Perimeter Accuracy of a Test Case (Key): 89.72%.**

## Summary

- High correlation between physical and cyber domain data.
- Side-channel information leakage not considered in additive manufacturing systems.
- Leakage from side-channel can breach confidentiality.
- It is imperative to incorporate side-channel leakage as a parameter in design methodology for secure additive manufacturing systems (future work).

## References

1. Hopkinson, Neil, Richard Hague, et al. *Rapid manufacturing: an industrial revolution for the digital age*. John Wiley & Sons, 2006.
2. Yampolskiy, Mark, et al. "Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing." *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*. ACM, 2014.
3. M. A. Al Faruque, S. Chhetri, A. Canedo, J. Wan, "*Acoustic Side-Channel Attacks on Additive Manufacturing Systems*", accepted to be published in the ACM/IEEE International Conference on Cyber-Physical Systems (**ICCPS'16**), Vienna, Austria, April, 2016