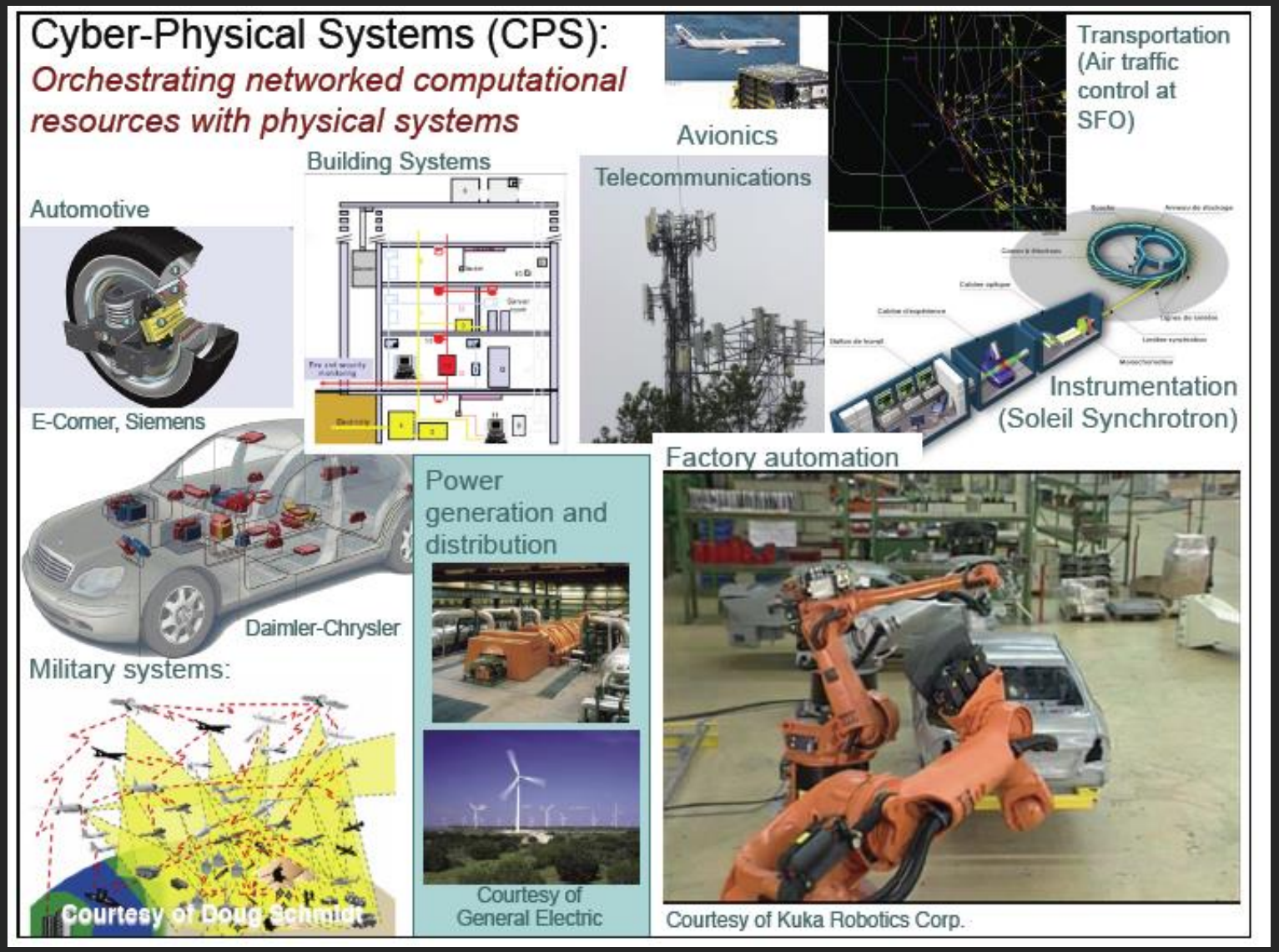
UCIrvine | The Henry Samueli School of Engineering

Cross-Domain Security of Cyber-Physical Systems

Sujit Chhetri, Jiang Wan, **Mohammad Al Faruque**

Cyber-Physical Systems

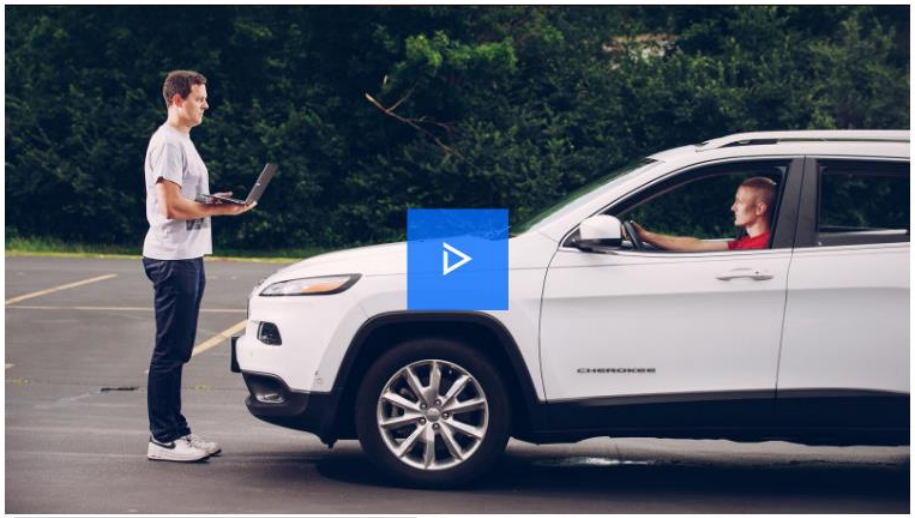


Courtesy: Professor Edward Lee

Kinetic Cyber Attacks

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



https://www.wired.com

KIM ZETTER SECURITY 11.03.14 6:30 AM

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

https://www.wired.com

Cyber-Physical Systems Security

Side-Channel Attacks → attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms → timing information, power consumption, electromagnetic leaks or even sound can be exploited to break the system.

Source: Wikipedia

Outline

- ✓ Overview
- ➢ Physical-to-Cyber-Attack – Side-Channel Attack
- ➢ Cyber-to-Physical-Attack – Kinetic Cyber Attack

Acoustic Side-Channel Attacks on Additive Manufacturing

Published in *International Conference on Cyber Physical System* 2016 (ICCPS)

This work is partially supported by NSF CPS grant CNS-1546993!

Additive Manufacturing (3D Printer)

Growth

- Airbus 350

Source: http://helicecluster.com/

Gartner: $100 Billion Losses Per Year in IP by 2018 due to 3D Printing!

- $21B industry by 2020!

Wholers

& Seating: SLS

Wheel, tires & Suspension: SLS, Inkjet, SLM

Electronics: SLS

OEM: SLM, Electronic Beam

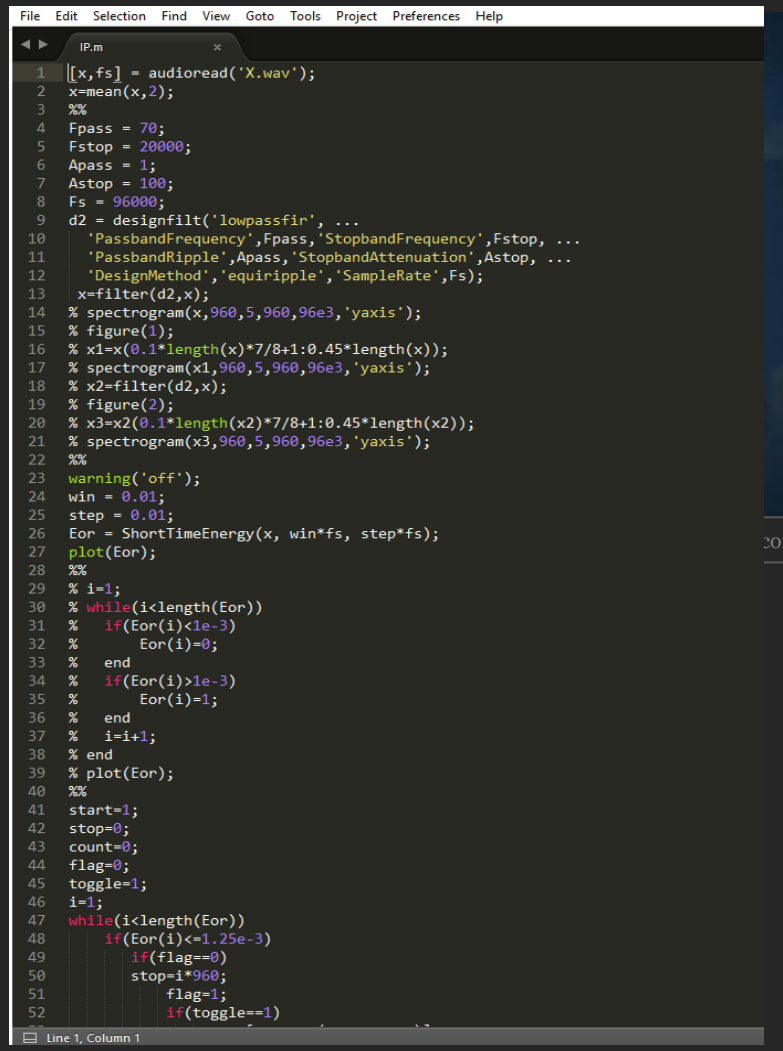
Frame: SLM

Engine: Electron Beam

Source: https://dupress.deloitte.com
Graphics: Deloitte University Press | DUPress.com

Intellectual Property (IP)

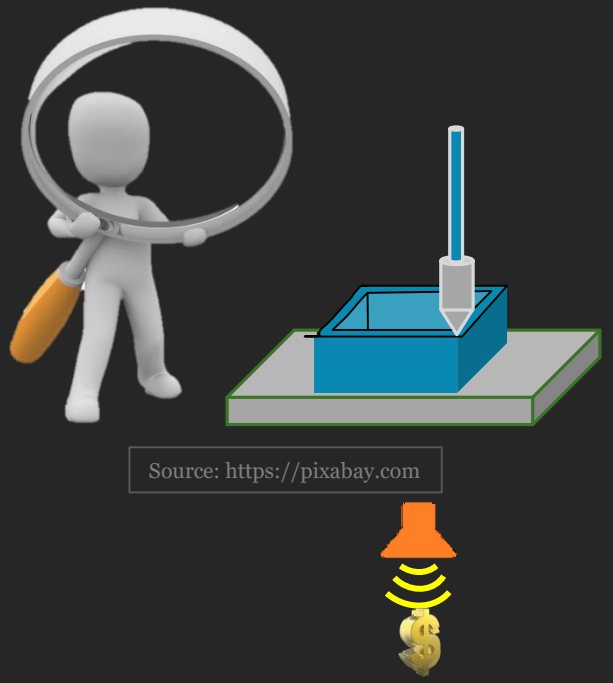
- Unique Features
- IP in Additive Manufacturing [1]
  - Geometric Shape,
  - Process Information,
  - Machine Information,
  - Stored in Cyber Domain!



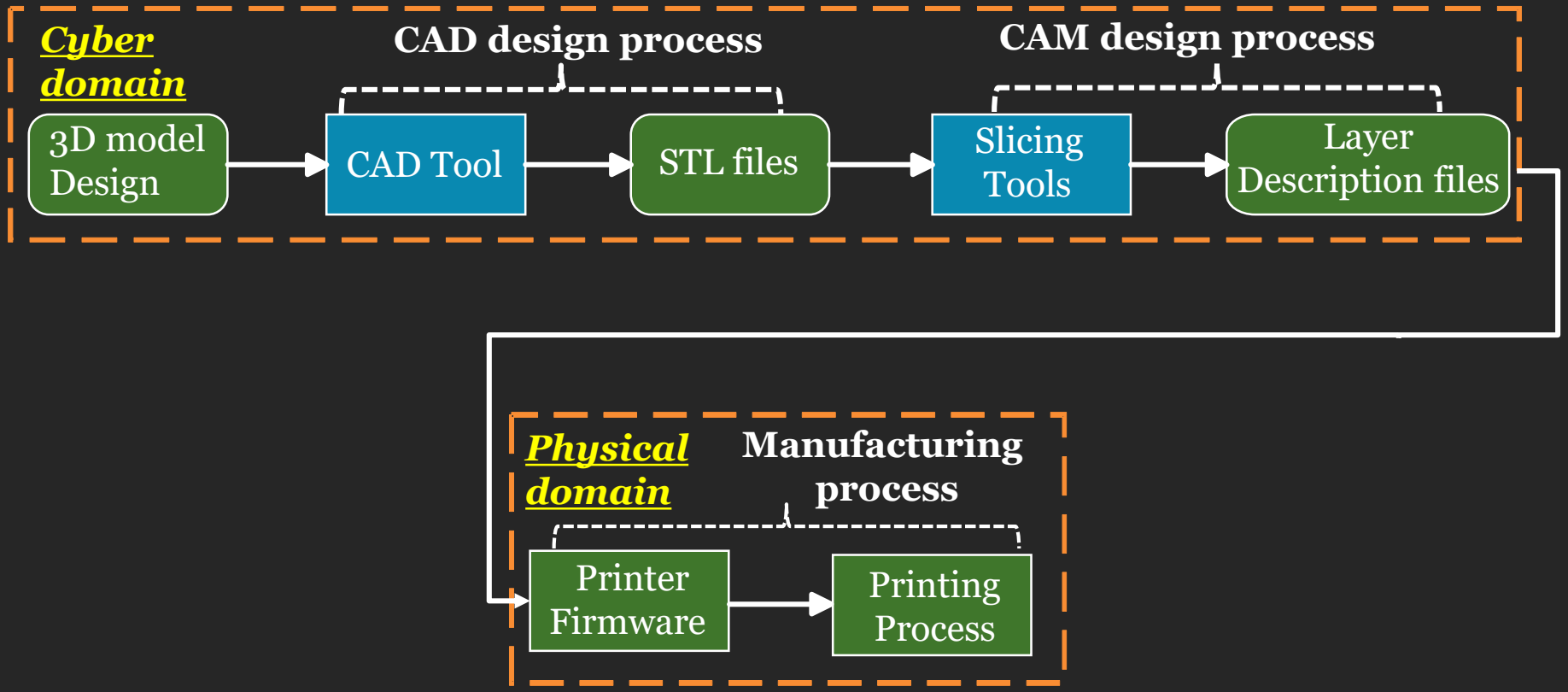
[1] M. Yampolskiy et al., "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in Proceedings of the 4th Program Protection and Reverse Engineering Workshop, p. 7, **ACM, 2014.**

Our Contribution

- Acoustic Leakage Analysis
  - Fused Deposition Modeling (FDM) based 3D Printers
- Novel Acoustic Attack Model
  - To breach confidentiality



Background - Digital Process Chain



Digital Process Chain (G-code)

- G-code Structure
  - Travel Feed rate
  - Movement Axis
  - Extrusion Amount

C:\Users\SujitRChhetri\Desktop\sample.gcode - Notepad++ [Administrator]

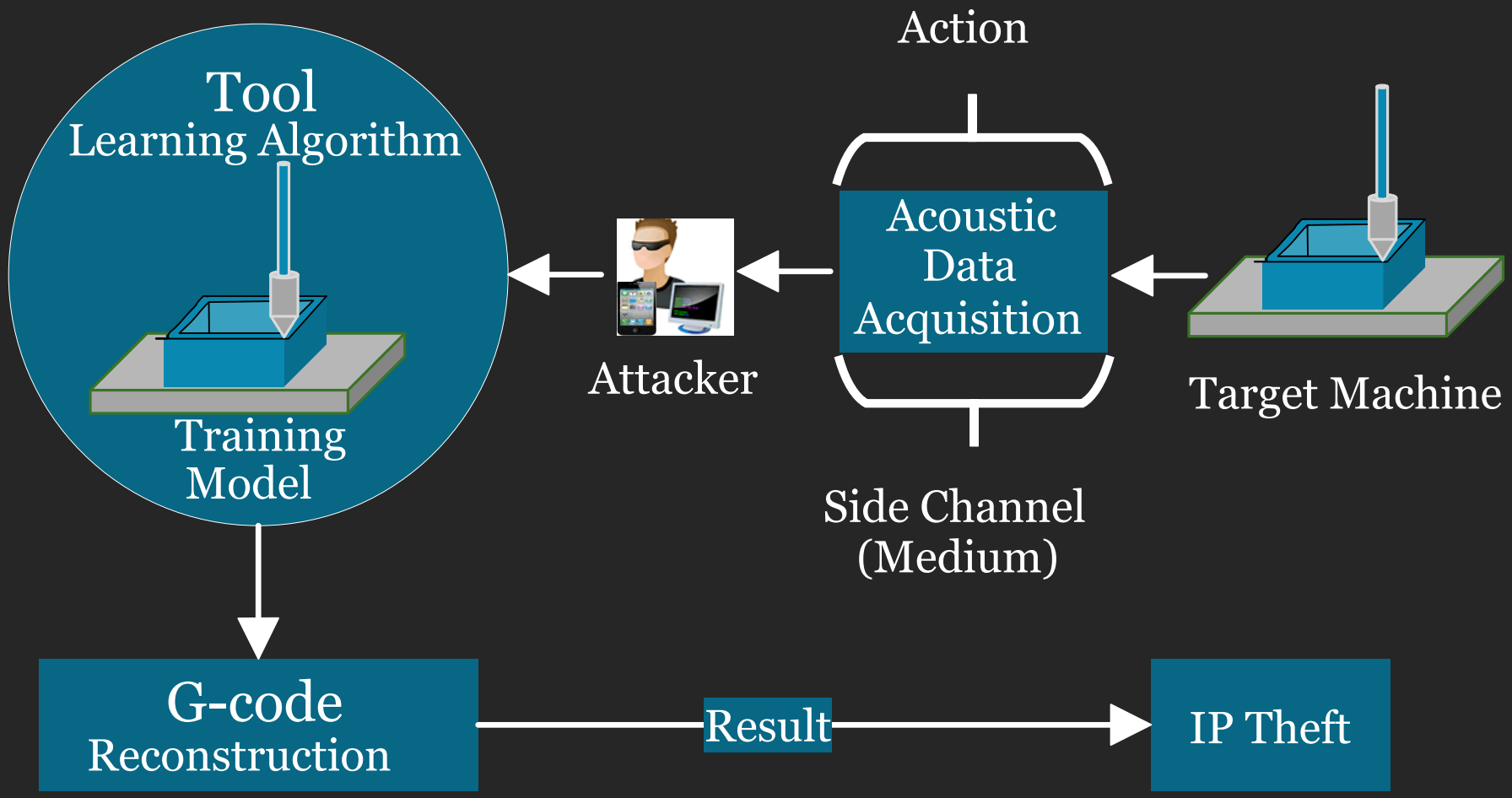
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

sample.gcode

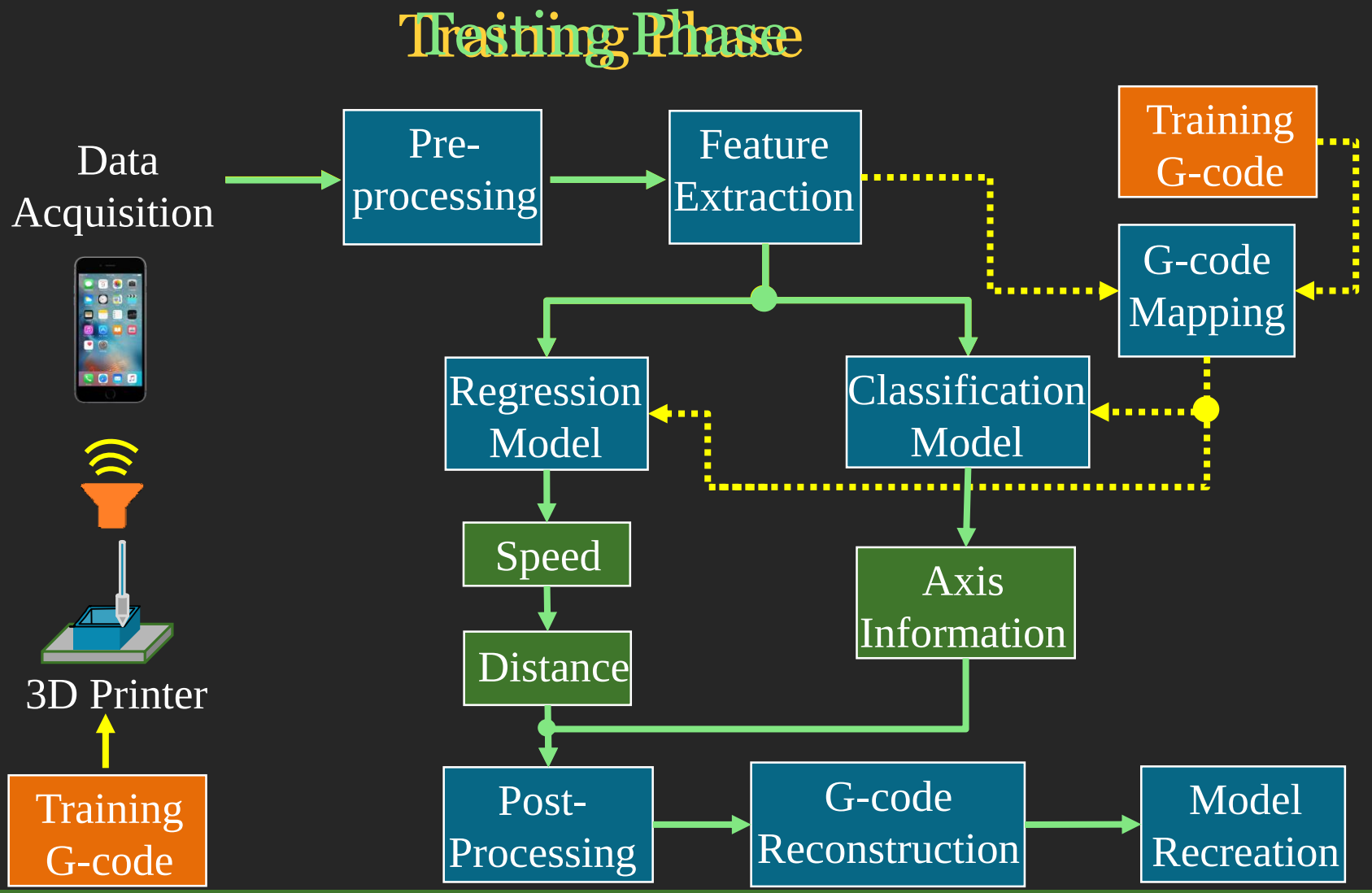
```
 M109 S200
;Sliced at: Wed 04-03-2016 11:57:57
;Basic settings:  Layer height: 0.4 Walls: 0.8 Fill: 20
;Print time: 8 minutes
;Filament used: 0.332m 0.0g
;Filament cost: None
;M190 S70  ;Uncomment to add your own bed temperature line
;M109 S100 ;Uncomment to add your own temperature line
G21        metric values
G90        ;absolute positioning
M82        ;set extruder to absolute mode
M107       ;start with the fan off
G28 X0 Y0  ;move X/Y to min endstops
G28 Z0     ;move Z to min endstops
G1 Z15.0 F4200 ;move the platform down 15mm
G92 E0                  ;zero the extruded length
G1 F200 E5              ;extrude 5mm of feed stock
G92 E0                  ;zero the extruded length again
G1 F4200
G0 F4200 X40 Y40 Z0.4
G4 P5000
M107
;Layer 1
G1 F1200 X39 Y40 Z0.4 E2.05
G1 F1200 X38 Y40 Z0.4 E2.1
```

Sliced using Slicr

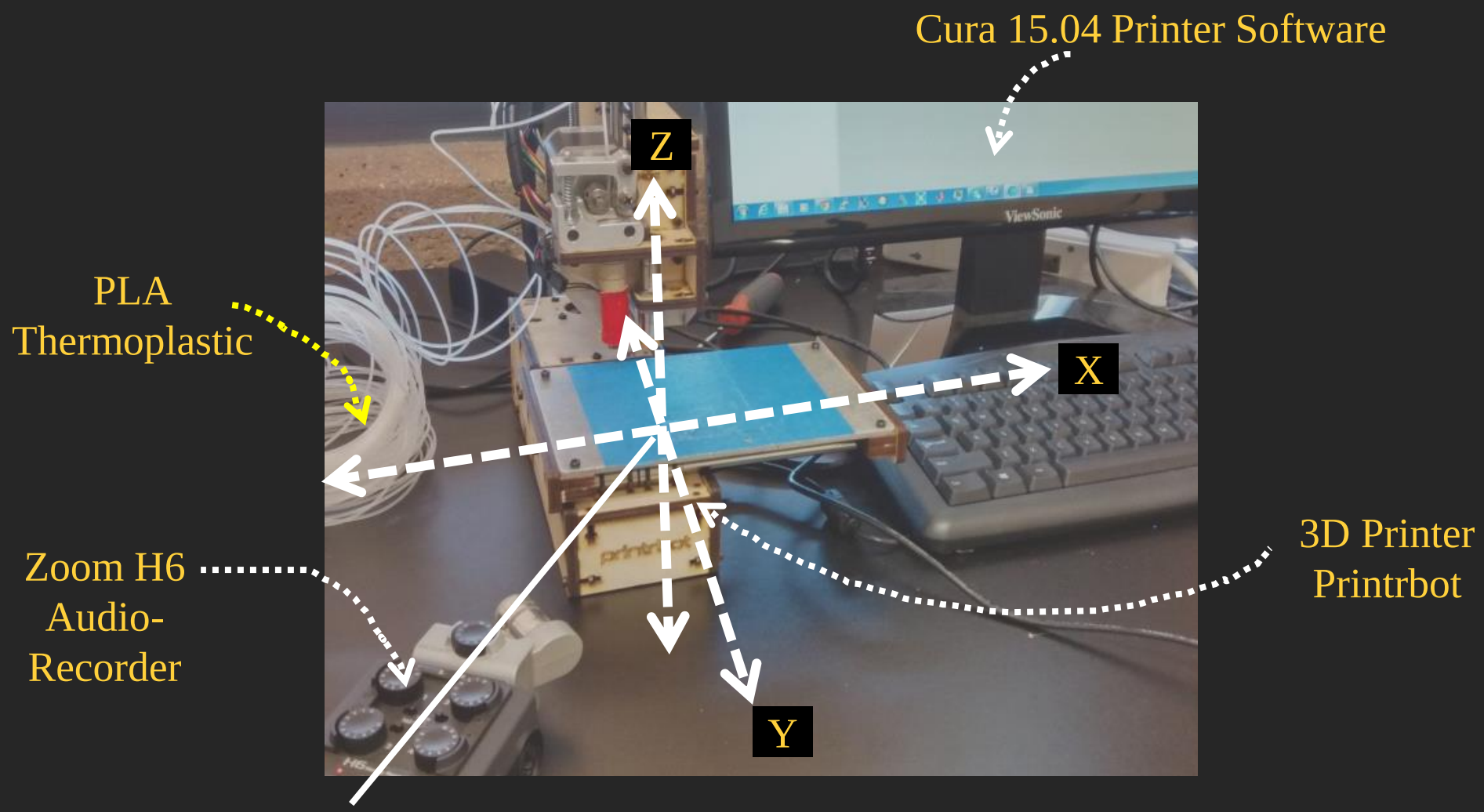
Attack Model



Attack Pipeline

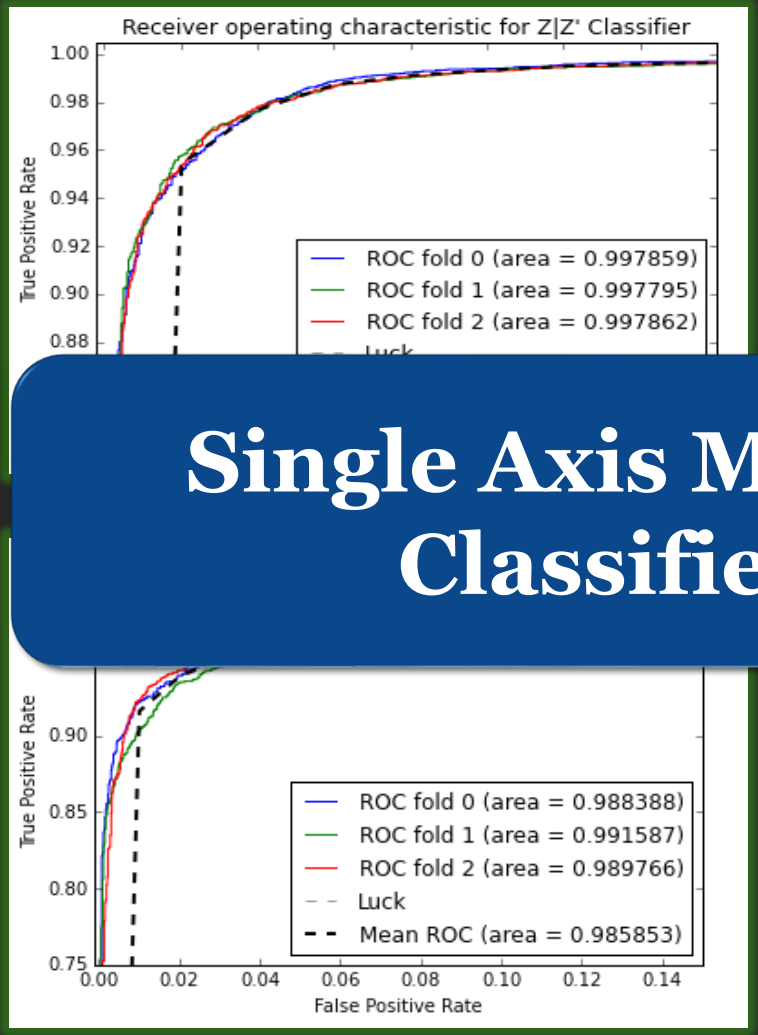


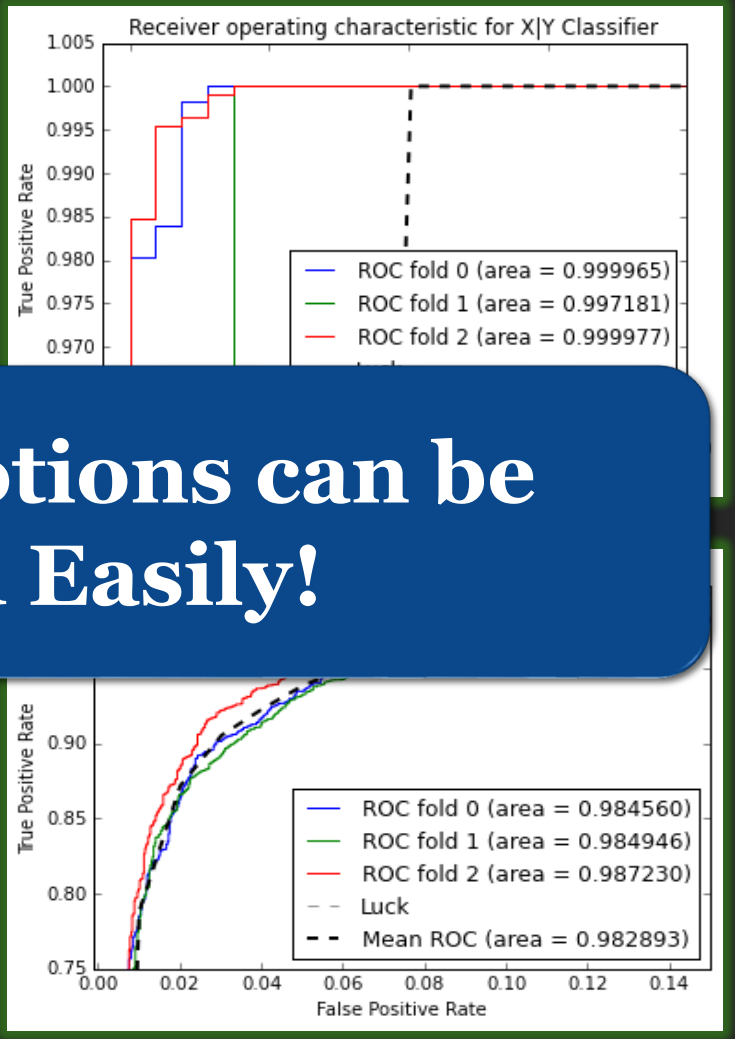
Experimental Setup



Classification Models

- Training Performance

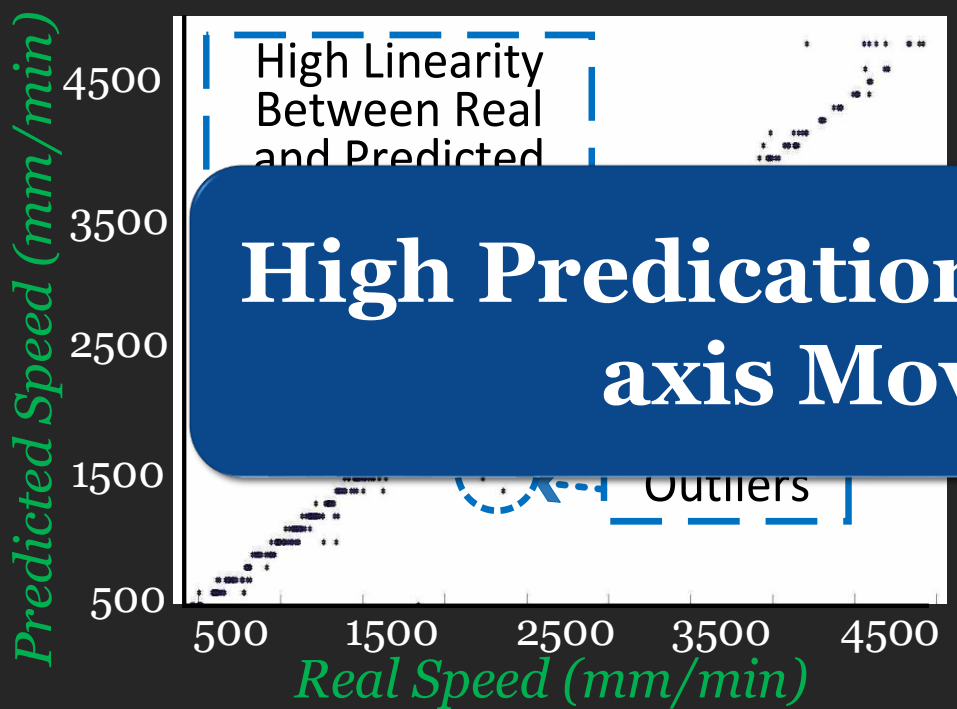




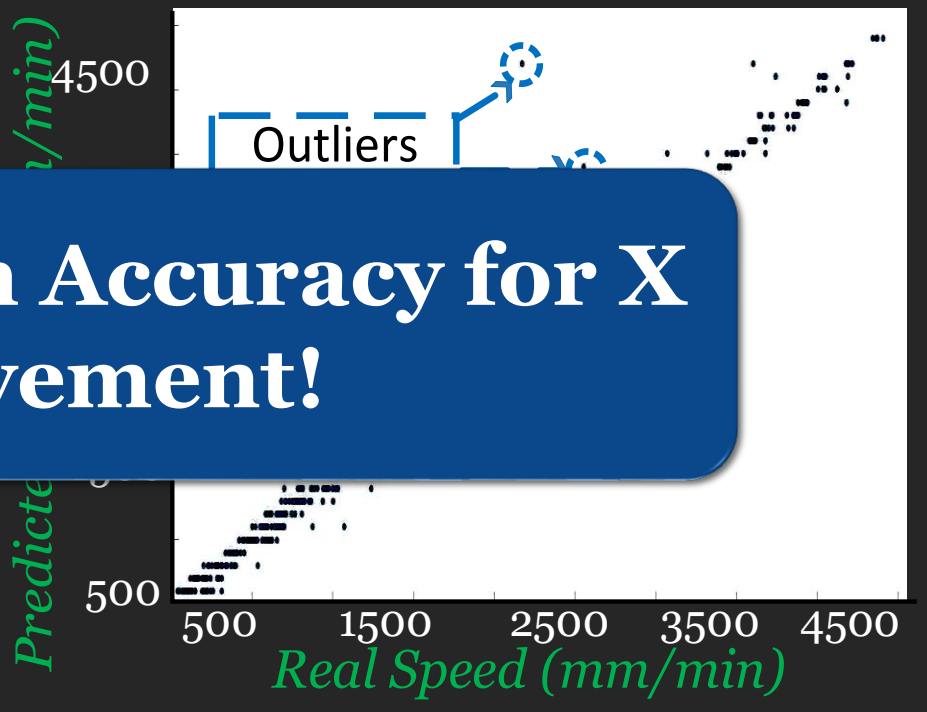
Single Axis Motions can be Classified Easily!

Regression Model

- Training Performance



i) Motion in just X Axis

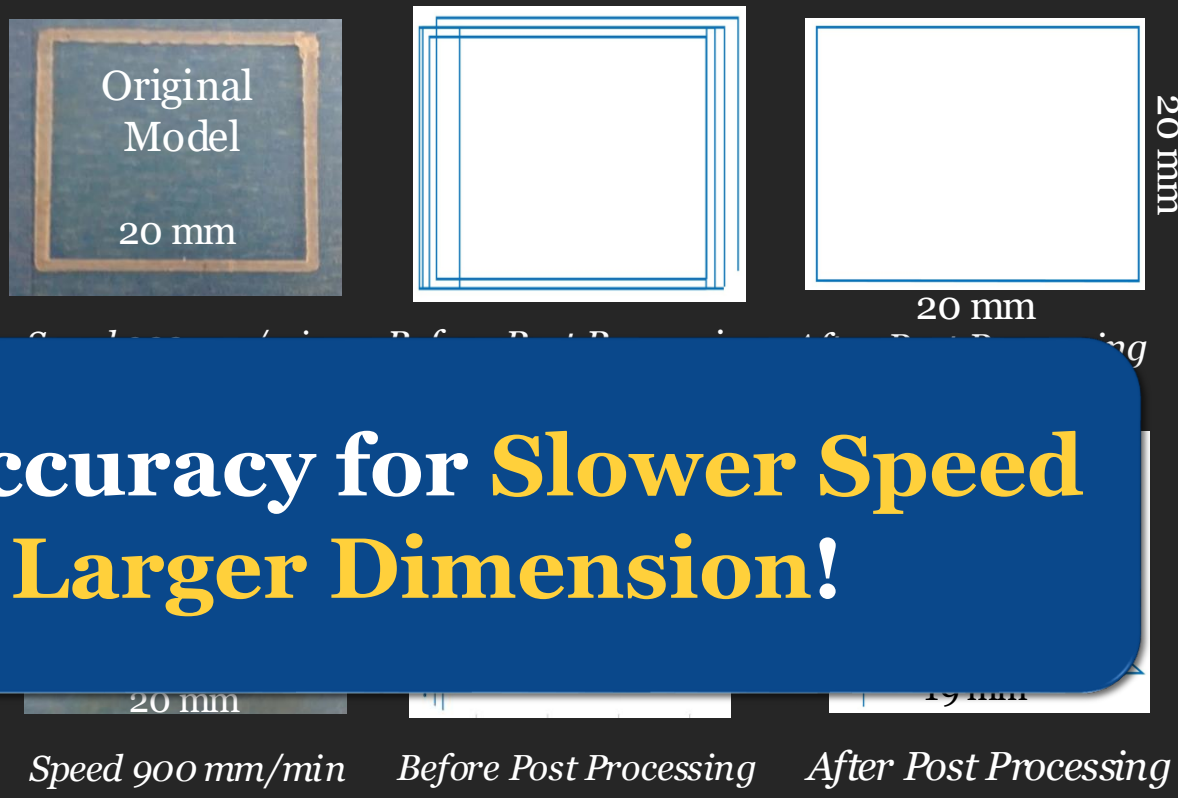


ii) Motion in just Y Axis

High Predication Accuracy for X axis Movement!

Test Parameter and Test Objects

- Speed
  - 900 to 1700 mm/min
- Multiple Axis



Higher Accuracy for Slower Speed and Larger Dimension!

- **Average Axis Prediction Accuracy: 78.35%**
- **Average Length Prediction Error: 17.82%**

Summary of Physical-to-Cyber-Attack

SHARE

IN DEPTH | INDUSTRIAL ESPIONAGE

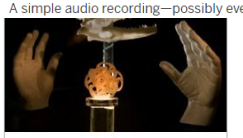
3D printers vulnerable to spying

Mara Hvistendah

Science 08 Apr 2016:
Vol. 352, Issue 6282, pp. 132-133
DOI: 10.1126/science.352.6282.132

From online shopping to social media, the power and convenience of digital technologies often come with a cost in security. Three-dimensional printing, the versatile technology that can churn out everything from engine parts to prosthetic limbs, appears to be no exception. By building objects layer by layer, rather than chiseling away at materials and assembling parts, 3D printers can make individualized products with minimal waste. But the signals that a printer sheds as it goes through its digitally controlled paces render it vulnerable to attacks, scientists have discovered.

A simple audio recording—possibly even one made by a smartphone—can be enough to



A new study by the University of California, Irvine has found three-dimentional printers emit sounds, vibrations, and other signals that present opportunities for industrial espionage.

Credit: Daniel Anderson/UCI

The team, led by Mohammad Al Faruque, director of UCI's Advanced Integrated Cyber-Physical Systems Lab, says a smartphone could be placed next to a 3D printer and capture information about the precise movements of the machine's nozzle. They warn the recording could be used to reverse-engineer the object being printed and re-create it elsewhere.

"If process and product information is stolen during the prototyping phases, companies stand to incur large financial losses," Al Faruque says.

His team achieved nearly 90% accuracy using the sound copying process to duplicate a key-shaped object in the lab.

State-of-the-art 3D printing systems build objects by converting digital information embedded in source code, which can be protected from cybertheft with strong encryption. However, once the creation process has begun, the sounds, vibrations, and other acoustic signals can expose the secrets buried in the software, the UCI team says.

ARTICLE TOOLS
Email
Print
Alerts
Citation tools

MORE NEWS & OPINI
In the Apple Case, Over Data Hits Ho
The New York Times
Apple's Deep Lear
Bloomberg Businessweek
A Call to Action fo Education to mak Principles Work
Mark Guzdial

ACM RESOURCES
Time Manageme Edition)
Courses

NEW URBANIST 11 May 2016

The perfect heists that involve stealing nothing at all

New Urbanist is **Geoff Manaugh**'s monthly column that explores how technology and design are changing our cities, homes, the built environment – and ourselves

Ulrich Baumgarten via Getty Images/Queen Nefertiti, at Egyptian Museum and Papyrus Collection in the Neues Museum Berlin

By **Geoff Manaugh**

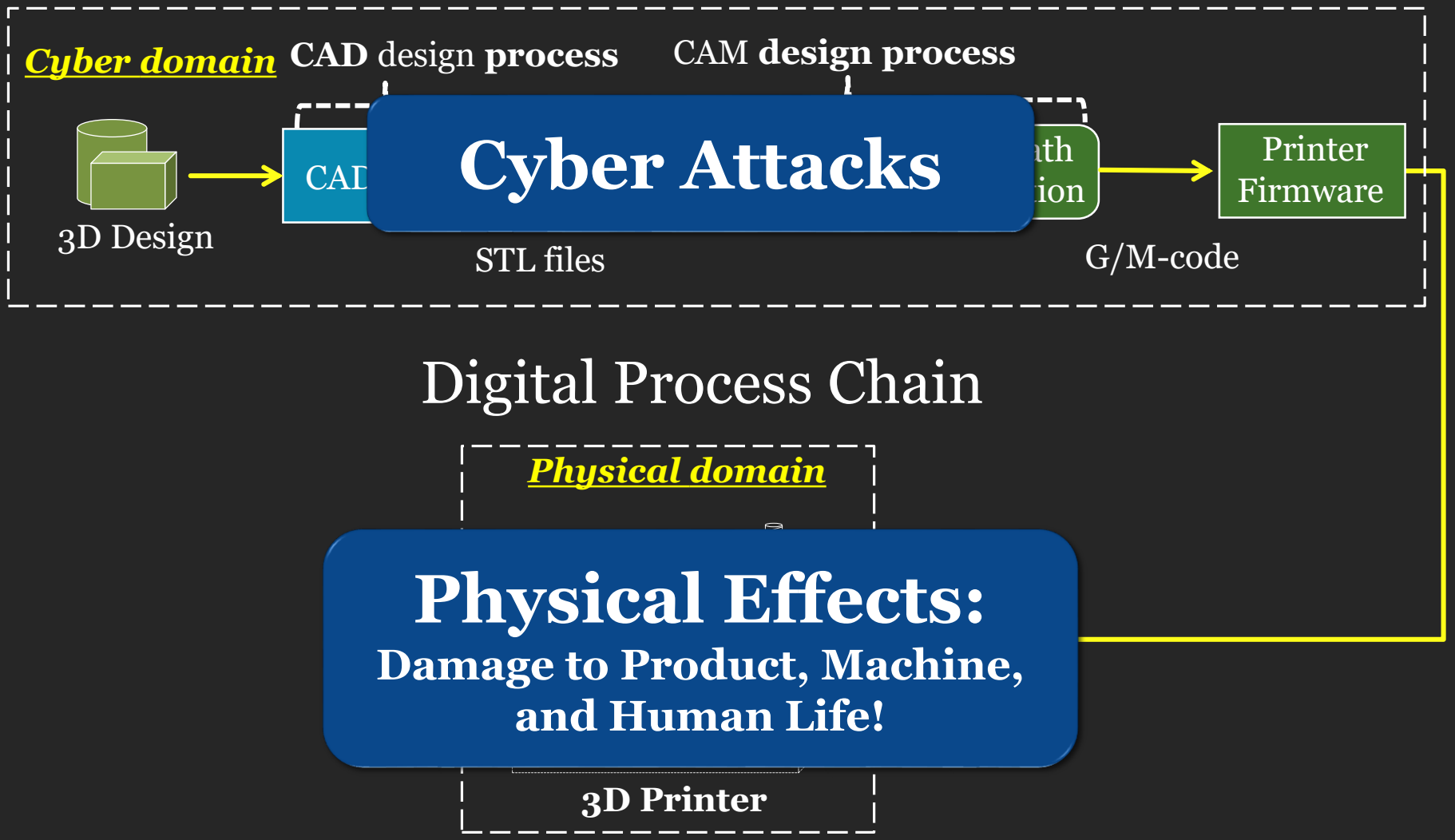
In February, two artists, Nora al-Badri and Jan Nikolai Nelles – claimed to have scanned the bust of Nefertiti in a German history museum using a handheld Kinect Sensor. They then posted the digital files online.

Their goal, they said, was to free the statue from its imprisonment inside the walls of Berlin's Neues Museum by

Outline

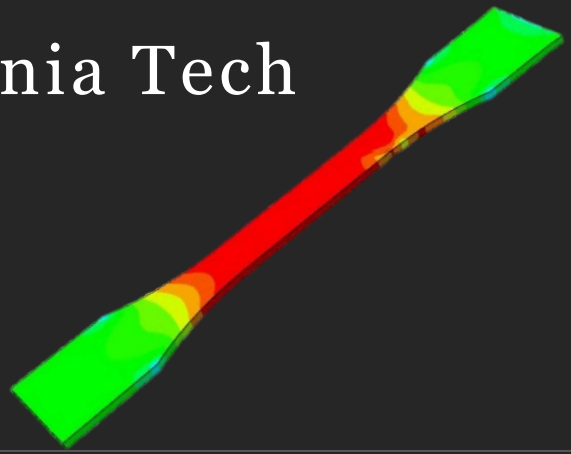
- ✓ Overview
- ➢ Physical-to-Cyber-Attack – Side-Channel Attack
- ➢ Cyber-to-Physical-Attack – Kinetic Cyber Attack

Kinetic Attacks on Additive Manufacturing



Kinetic Attacks on Additive Manufacturing

- *Zero-Day Kinetic-Cyber Attacks*
  - Void Placement in STL→ Virginia Tech
  - D638-10 Tensile Specimen[1]
  - Load Handling Capacity ↓14%



Source: https://i.ytimg.com/vi/1CPy6dLCVJ8/maxresdefault.jpg/

- *3D Printer as Weapon*
  - Attack taxonomy (3D objects, 3D Printer, environment) →University of South Alabama
- *Can Affect*
  - Aerospace, automotive!

[1] American Society for Testing and Materials (ASTM) Standard

Attack Example

Researchers sabotage 3D printer files to destroy a drone

Posted Oct 21, 2016 by John Biggs (@johnbiggs)

Researchers at Ben-Gurion University of the Negev (BGU), the University of South Alabama, and Singapore University of Technology and Design have successfully injected malicious code into a computer which, in turn, added invisible commands to a file containing a 3D

Crunchbase

Ben-Gurion University of the Negev

FOUNDED
1969

OVERVIEW
Ben-Gurion University of the Negev is one of Israel's leading research universities and among the world leaders in many fields. It has around 20,000 students and 4,000 faculty members in the Faculties of Engineering Sciences; Health Sciences; Natural Sciences; the Pinchas Sapir Faculty of Humanities and Social Sciences; the Guilford Glazer Faculty of Business and Management; the Joyce and Irving ...

LOCATION
Be'er Sheva, 01

CATEGORIES
Education, Solar

FOUNDERS
Eytan Stibbe

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Eve

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERAT

ENDPOINT

10/20/2016
05:20 PM

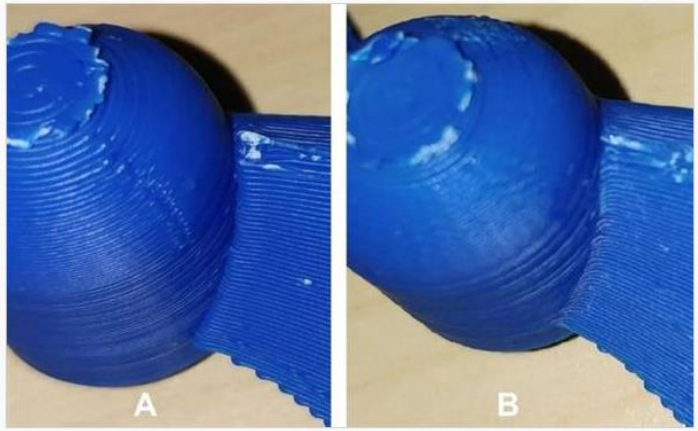
How To Crash A Drone By Hacking Its 3D Propeller Design

Researchers from Israel's Ben-Gurion University of the Negev and two other universities show how attackers can exploit 3D manufacturing processes.

Jai Vijayan
News

Researchers at Israel's Ben-Gurion University of the Negev along with their counterparts at the University of South Alabama and the Singapore University

Connect Directly



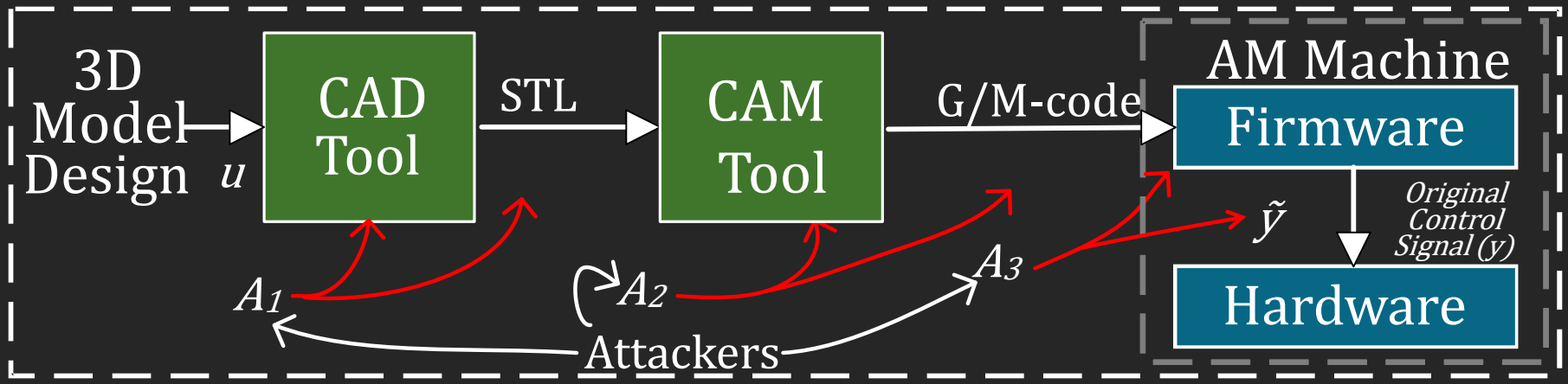
- *Code Injection into plastic propeller: Damage $1000 [2]-* Ben-Gurion University of the Negev (BGU), University of South Alabama

[2] https://techcrunch.com/2016/10/21/researchers-sabotage-3d-printer-files-to-destroy-a-drone/

Our Contribution

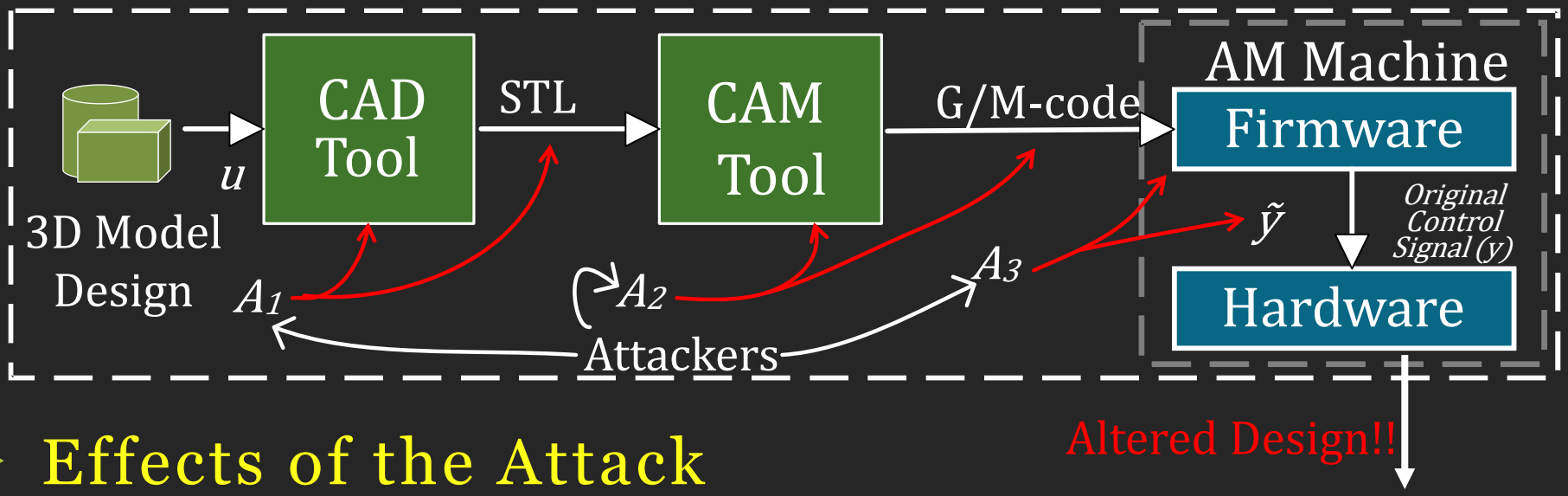
- Modeling of an Adversary
  - Define various attack points
- Data-Driven Modeling of the System
  - Statistical estimation
- Analysis of Analog Emission
  - Using mutual information

Adversary Model



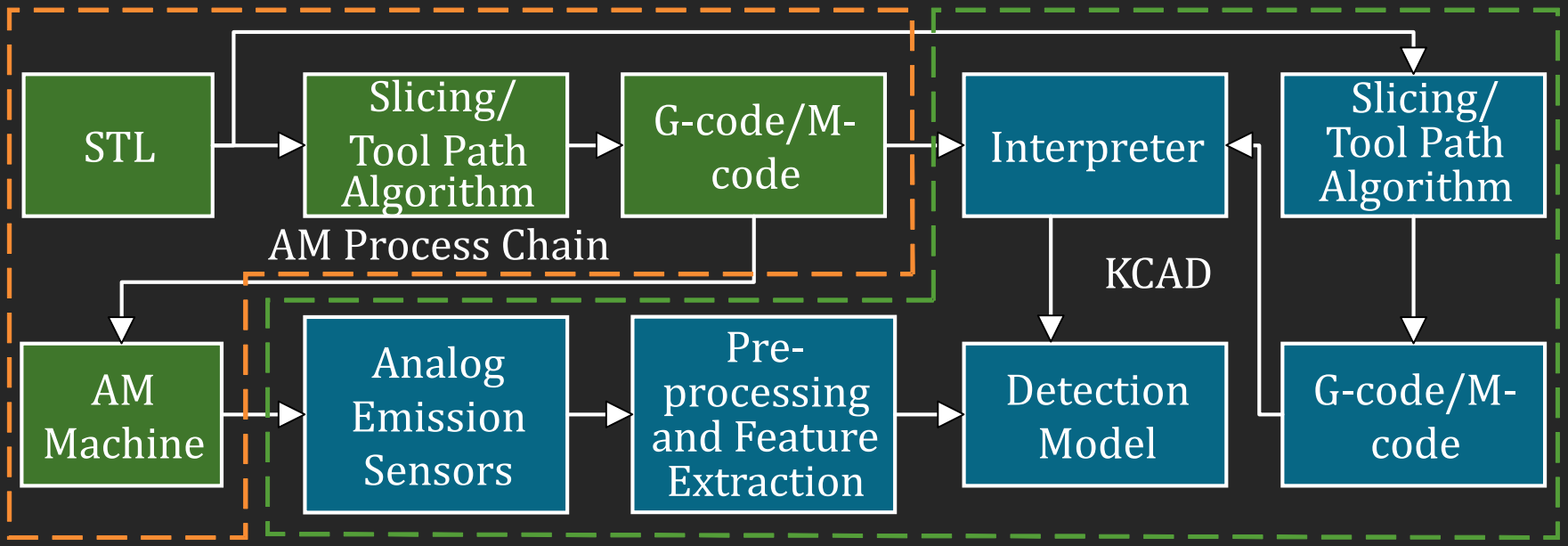
- Capability of the Attacker
  - Modify CAD tools, CAM tools
  - Intercept the network
  - Modify the firmware

Adversary Model



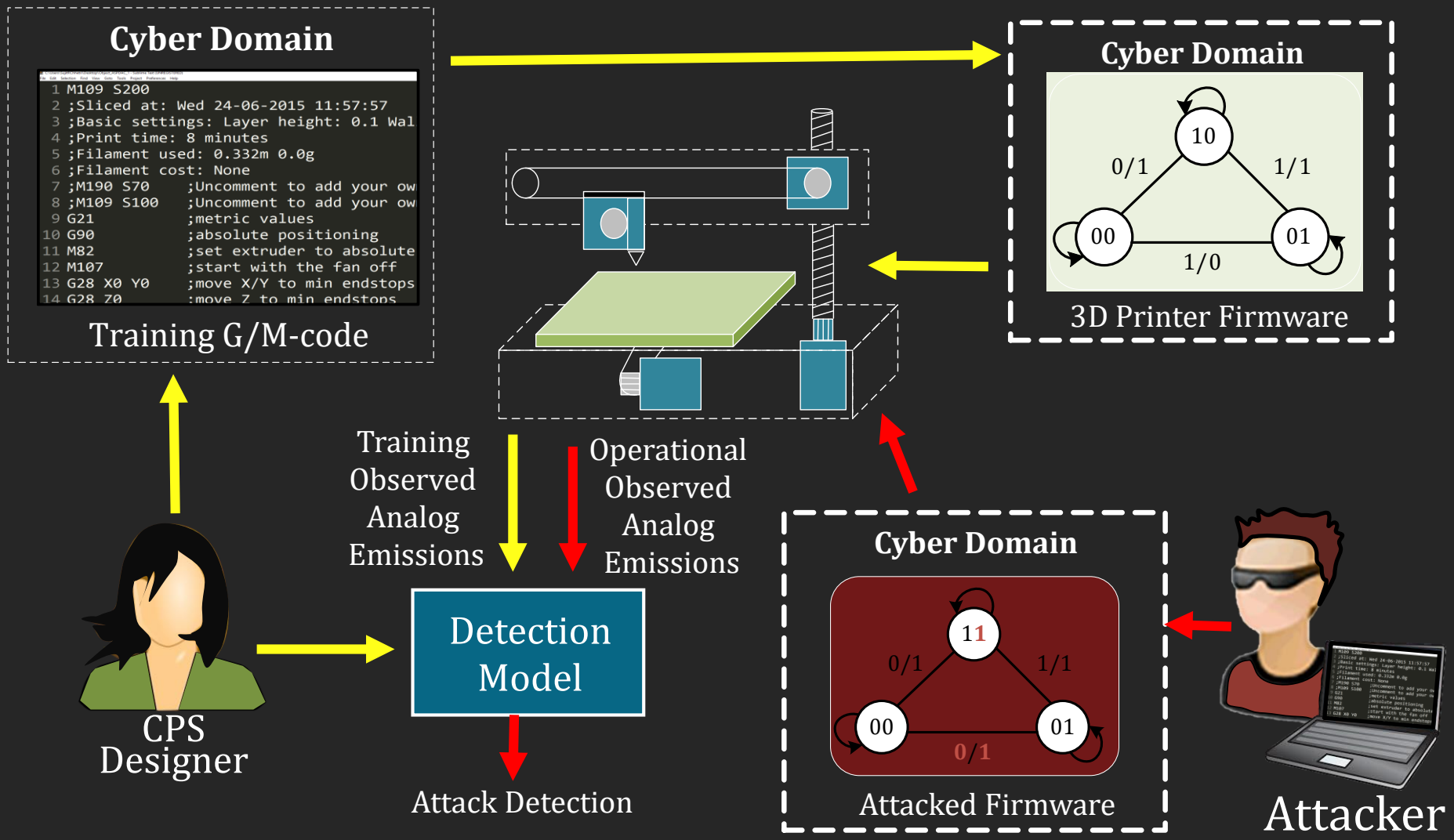
- Effects of the Attack
  - Cyber-attack introduces variation in the information flow (u).
  - Changes Control Signals y to ỹ in physical domain

KCAD Method

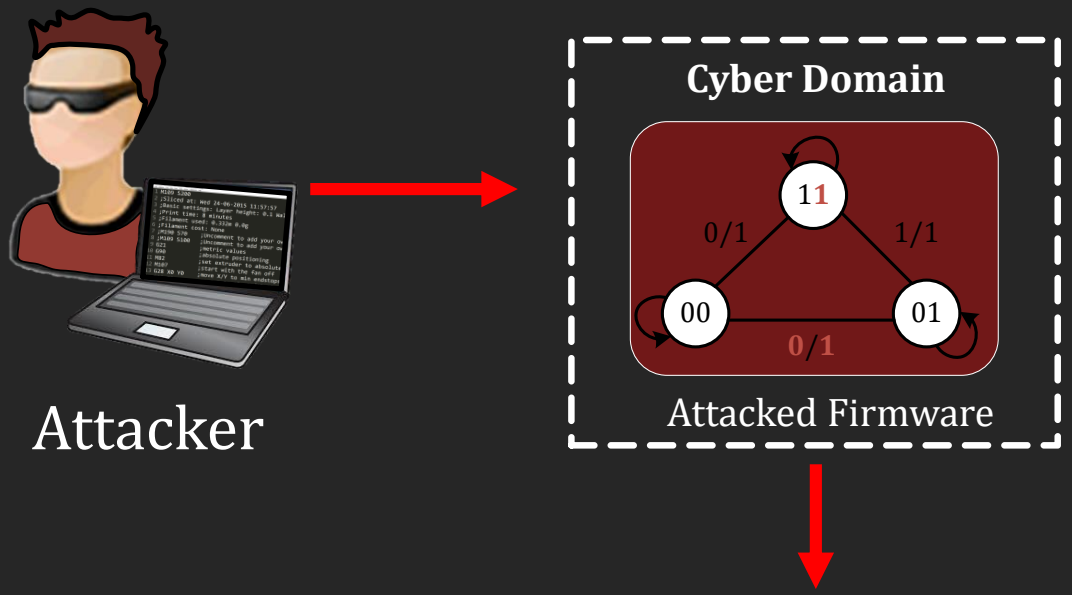


- *High Mutual Information* between control signals (y) and Energy Flow (acoustic, power, magnetic, thermal, etc.)

KCAD Method: Simplified!

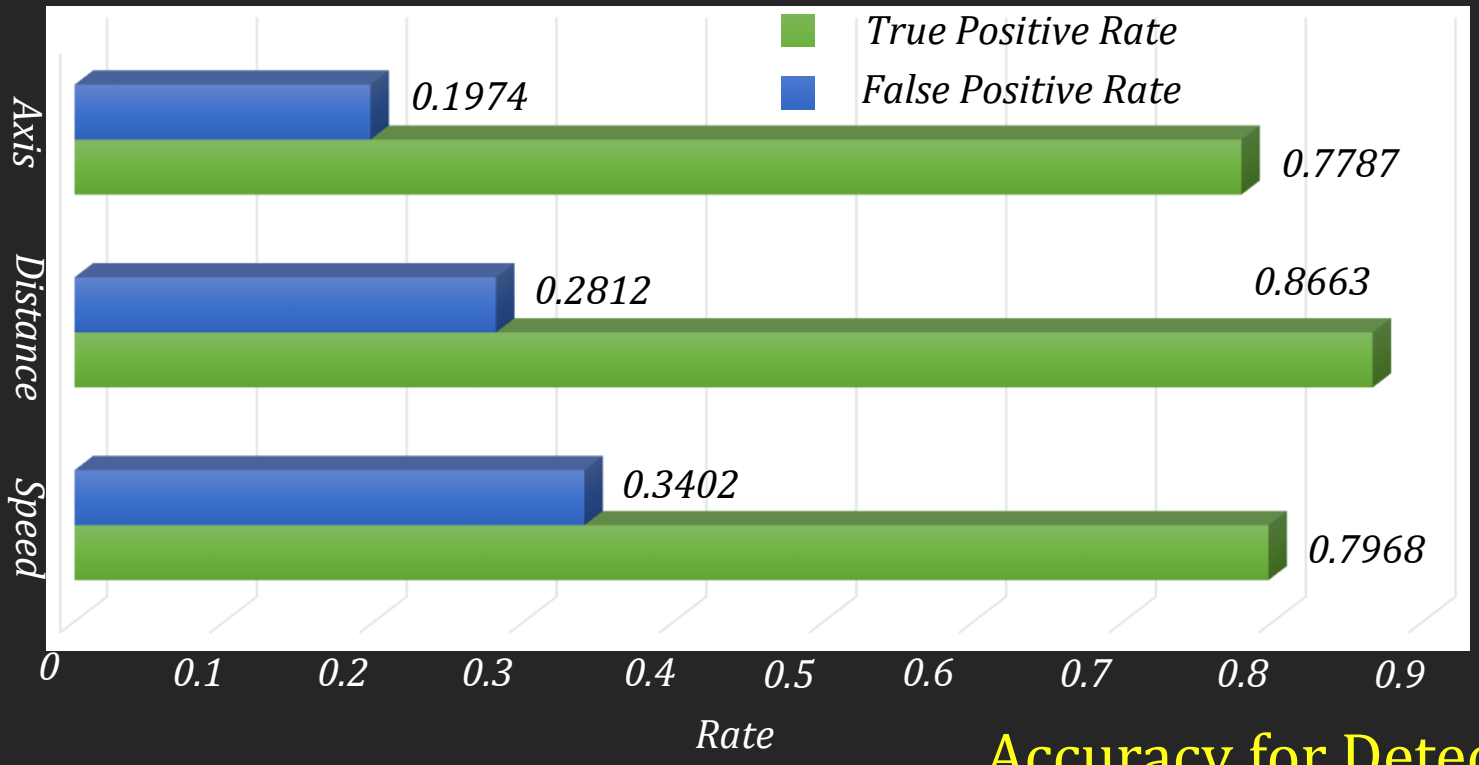


KCAD Method:



- *Introduces minutes changes which are hard to inspect without special equipment.*
  - Speed, distance, axis movement, etc.
  - Affects the structural integrity of the 3D objects.

Test Results



True Positive Rate= TP/(TP+TN)

Accuracy= (TP+TN)/Total Sample

Accuracy for Detection

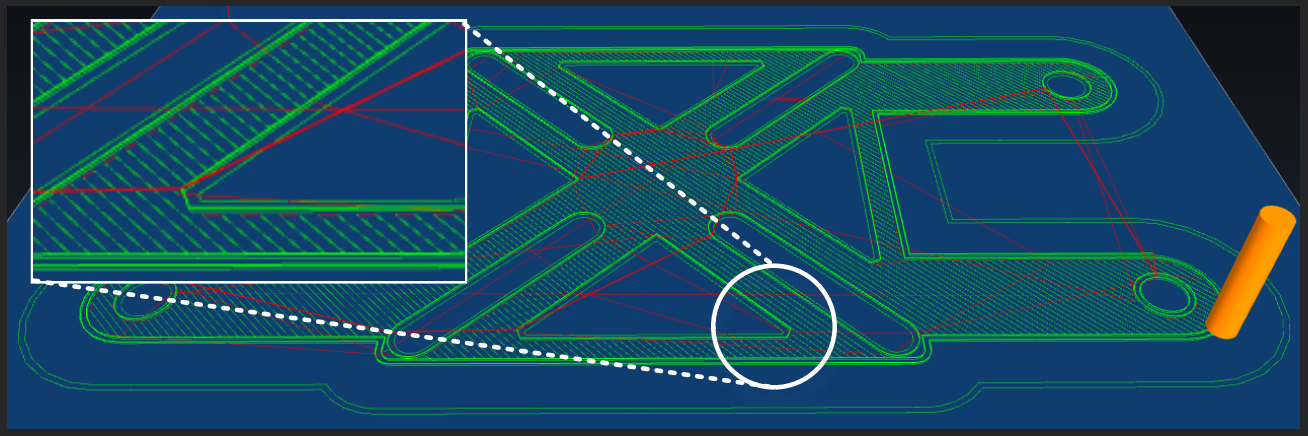
Speed = 72.83%

Distance = 79.25%

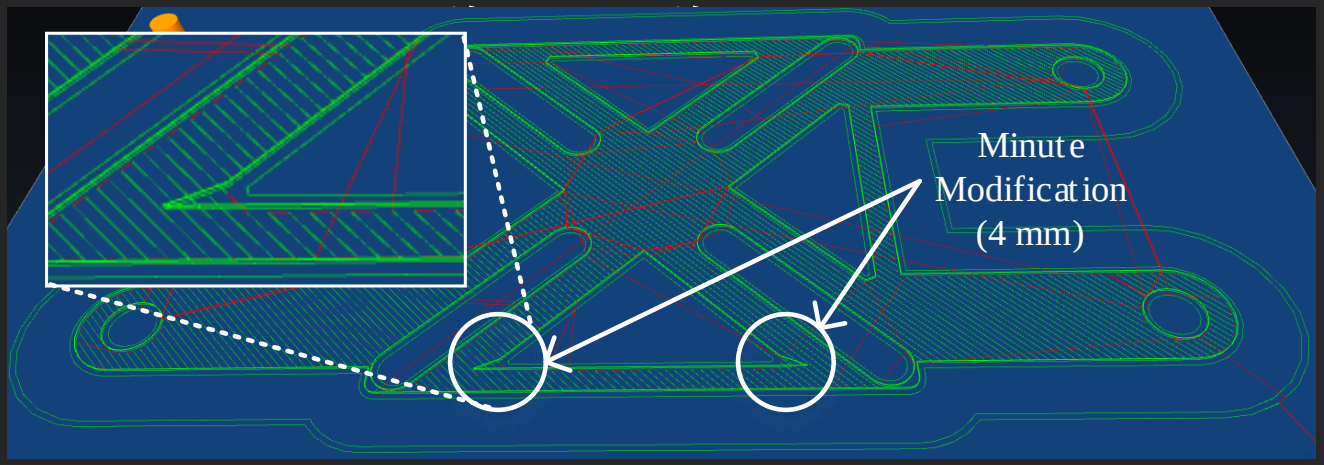
Axis = 79.07%

Average = 77.45%

Test Case: Base Plate of QuadCopter



a) Original G-code Trace.



b) G-code Trace after Kinetic Attack.

Summary

- Monitor Information Flow from any point in Digital Process Chain
- Detect any modifications that affect Dynamics
- Detection during printing stage
- Non-intrusive and hence supports Legacy Systems!

Questions

Thank You!

Cross-Domain Security of Cyber-Physical Systems