Securing Manufacturing Systems

Sixth Annual Cyber-Physical Systems – PI's Meeting

Dr. Jaime Camelio
Rolls-Royce Commonwealth Professor for
Advanced Manufacturing
Virginia Tech

Dr. Jules White
Assistant Professor of Computer Science
Vanderbilt University

VANDERBILT UNIVERSITY

VirginiaTech
Invent the Future®

Motivation

Modeling & Design Automation Critical
in Advance Systems

Design solution spaces are so complex it is impossible or extremely complex for humans to find solutions that meet desired constraints

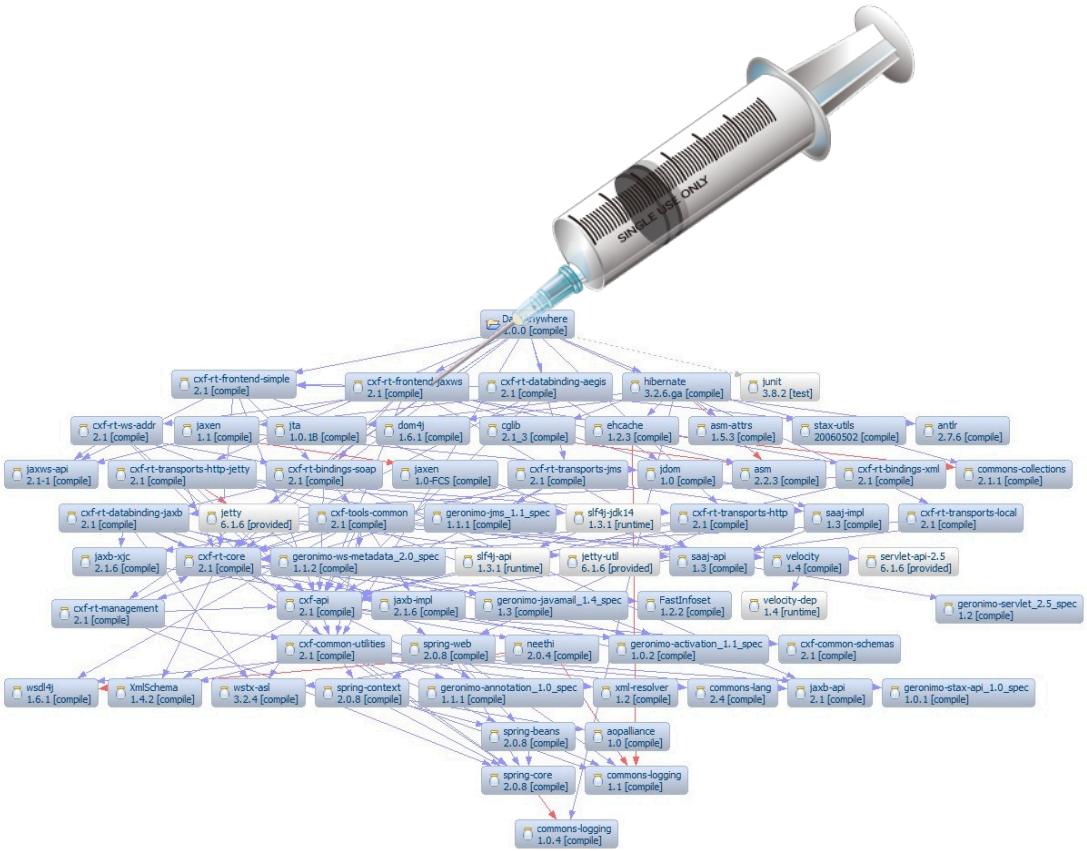
- Advanced manufacturing systems
  - Tool path code production from 3D designs, finite element analysis
- Synthetic biology
  - Oligo design
- Vehicle design (DARPA AVM)
- Oil & Gas exploration

Software Systems Increasingly
Under Attack

Attacks target the ***software construction process*** as well as deployed software

- Dilletante injects vulnerabilities into Java libraries downloaded with most common build tools
- Ken Thompson compiler virus injects backdoor into all software

If you can't compromise it, inject flaws into its construction



Toyota Settlement Over Acceleration

Problems to Top $1 Billion - NBC

How do we know that the Toyota acceleration problem wasn't a design flaw injected by an attacker?

Defect still unclear:

- "a single bit flip which can be caused by cosmic rays could cause unintended acceleration "- NASA
- Possible mechanical design flaw caused sticking

Red Team Tasks

Example TCP Stream Analysis

1. Objet data included three main configuration directories
   1. Configs
   2. Modes
   3. ServiceTools
2. Each contains config files:

Print Start Config

```
ActivationOverShoot=0
ActiveMarginInPercent=10
ActiveTanks=1,3,2
AdvanceFireTest=0
AdvanceFire_1200DPI=9
AllowEmulationDelay=0
AmbientFanControlByPass=1
AmbientLog=1
AmbientTemperatureByPass=0
AmbientTemperatureFanControl=383
AtLeastDelayTimeBetweenLayers=0
AutoPrintCurrentZLocation=0
BumperBypass=0
BumperCalibrationPermissiveArray=
```

Head Heater Config

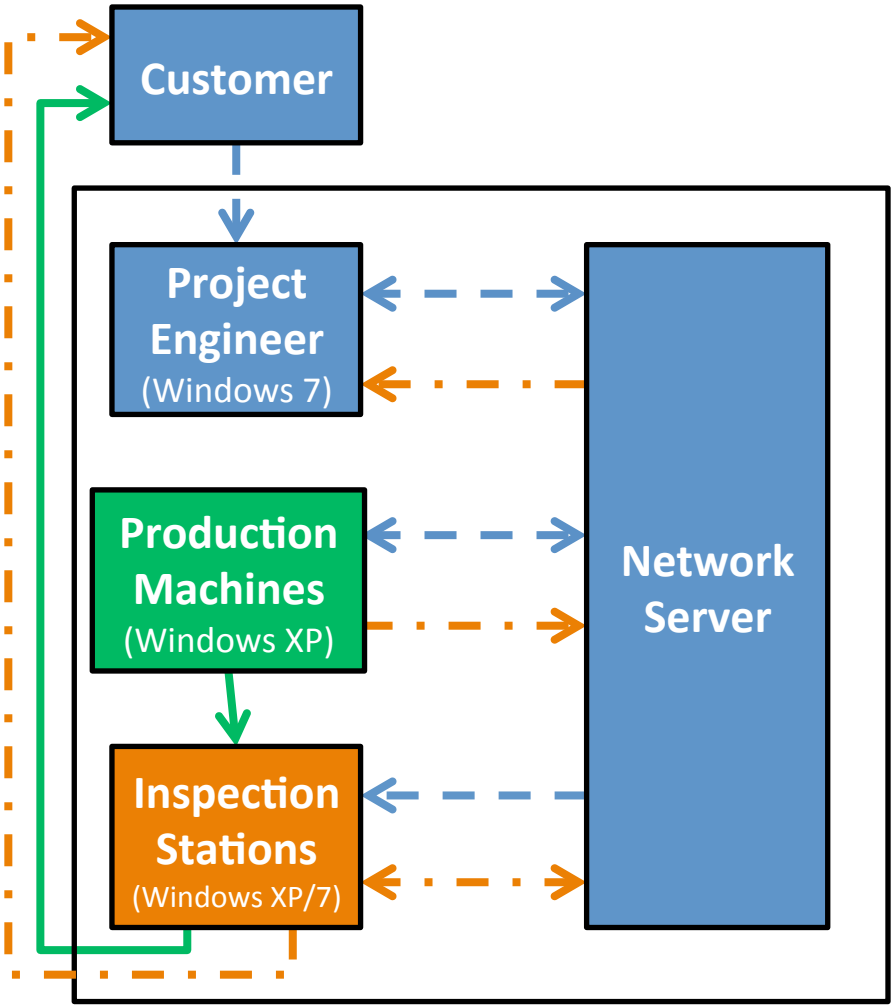
```
4000=20
3000=28.1
2900=30
2800=31.2
2700=33.5
2600=34.6
2500=35.2
2400=36.6
2300=38.4
2200=40.4
2100=41.6
2000=43.1
```

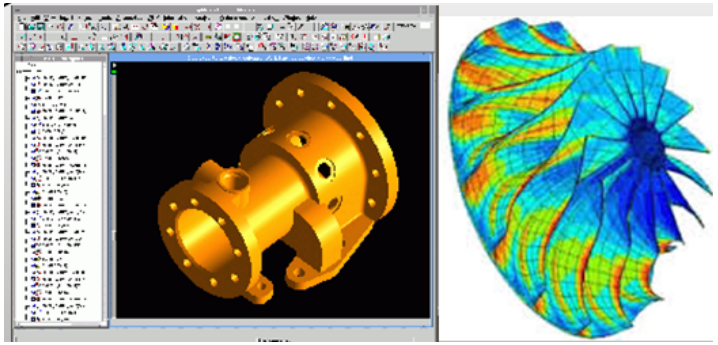
```
output/zip » ls tmp-00000001.zip
Configs  Modes  ServiceTools

output/zip » ls tmp-00000001.zip/Configs
AmbientTemperature.txt  q2rt.cfg
follow - up log.txt     q2rt.cfg.bak
HeadHeater.txt          q2rt.ref
Maintenance.bak         QSHR.bak
Maintenance.dat         QSHR.tmp
Print End Params.cfg    recover.bak
Print End Params.ref    recover.bin
Print Start Params.cfg  SensorVacuum.txt
Print Start Params.ref  Tray.txt

output/zip » cat tmp-00000001.zip/Configs/
AmbientTemperature.txt
335=3.201
400=56.468
460=105.63
```

Objet Configuration Data
Can be Detected and Modified

Is this a real problem?
AM Production Example

Additive Manufacturing Process Evaluation





CPSS – Pilot Approach

- Focus on attacking the most widely used open standards (i.e. CNC, CMM, STL, P-Code)
- Attack a common, familiar, well characterized test part (i.e. dogbone)
  - Difficult to hide attack effects
- Observe the behavior of designers unknowingly subjected to cyber physical system attack

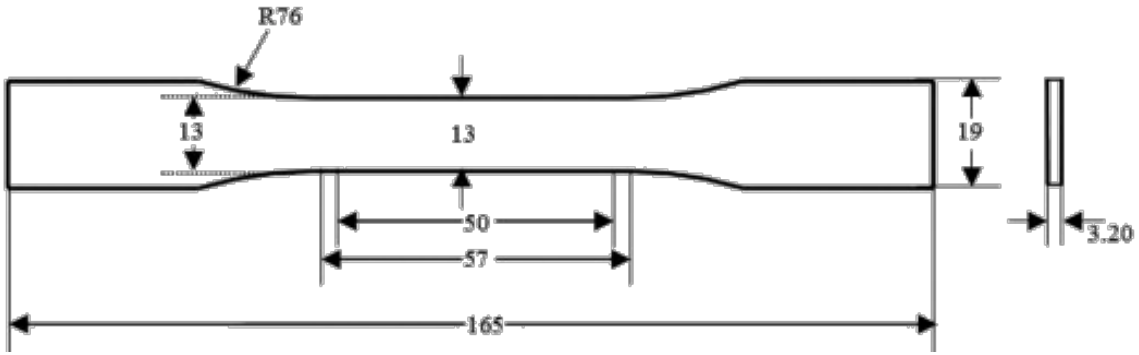
CPPSS – Pilot Teams

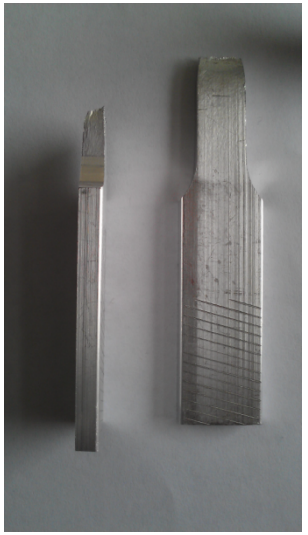
- **Two Distinct Thrusts**
  - Additive Manufacturing Team (Williams)
    - **Insert undetectable active electronics into the manufacturing process**
    - **Strategically insert microscopic voids to cause lifecycle failures in additive parts**
  - Subtractive Manufacturing Team (Camelio)
    - **Teams of mechanical designers attempt to design, build and test simple "dogbone" test article while Red Team attacks machine files and measurement devices**
- **Red Team (White)**
  - Create malicious attack delivery mechanisms
    - **Thumb drives, network, wireless attacks**
    - **Deliver mechanisms not detectable by cyber security techniques**
  - Analyze VT AM networks and intercept sensitive design data and machine control data
  - Cyber-physical defense approaches and best practices

Subtractive Manufacturing

Standard Test Part

- Dog-Bone Tensile Test Specimen
  - **Used to Determine Material Properties**
  - **Easy to Design, Machine, Inspect, & Test**
    - But VERY difficult to attack without detection
  - **Known Performance**
  - **All Necessary Equipment is Available (at one location)**
    - Material is Easy to Obtain
  - **Fits Well with Manufacturing Processes (ISE-2204)**





Subtractive Manufacturing

Phase 1 Organization

- **Two Teams**
  - Blue Team
    - Engineering Students (operating under an IRB)
    - Design, Manufacture, Inspect, and Test Part
    - Works Directly with Engineering Graduate Student
    - Ability to Detect Abnormalities is Continuously Monitored
    - Unaware of the Red Team
  - Red Team
    - Develops Malicious Software
    - Works Directly with Engineering Graduate Student

- **Engineering Graduate Student**
  - Guides Blue Team Through Product Development
  - Monitors Blue Team Behavior
  - Helps Identify Vulnerabilities
  - Implements Malicious Software

Subtractive Manufacturing

Tool Path Attack

- **Seven independent Student Teams design Standard Test Part, create P-code**
- **Machine tool paths are sent to the mill controller via ASCII files**
- **Red Team swaps ASCII files to create incorrect tool paths**
  - Insertion of thumb drive with design file detected, file on thumb drive remains unmodified but file on computer is altered on the fly as it is read in
- **Parameters modified**
  - One line changes thickness by .02”
  - 20 lines (of 135) reduce contour by .05”
  - **20% performance decrease, same file length**
- **Incorrect part is machined and tested**

```
%
:O5000
N2G70G90G40G49G17G80G53G00
N4G1X0.Y0.S3819M03
N5G43H1Z1.0T2
N6M08
N7Z0.1
N8G01Z-1.0F22.91
N9G41D1Y-5.0F45.83
N10X4.0
N11G03X5.0Y-4.0I0.J1.0
N12G01Y4.0
N13G03X4.0Y5.0I-1.0J0.
N14G01X-4.0
N15G03X-5.0Y4.0I0.J-1.0
N16G01Y-4.0
N17G03X-4.0Y-5.0I1.0J0.
N18G01X0.
N19G40Y0.
N20G00Z1.0
N21G91G28Z0M09
N22G00X0.Y0.
N23M06
N24G90G00G1X-0.036Y0.536S4965M03
N25G43H2Z1.0T1
```

Subtractive Manufacturing

Experimental Results – Blue Team Reactions

- **Teams 1-3**
  - Did not notice the 20% change in performance even when prompted with calipers
- **Teams 4-7**
  - When instructed to measure the part, these teams detected some anomaly
  - Team 4 finds file abnormality, diagnosis as “weird” computer problem in file transfer
  - Team 5 finds file abnormality , diagnosis as “weird” computer problem where “old file never left”
  - Team 6 finds file abnormality, wrongly guesses the problem is a part design problem in CAD process – not validated
  - Team 7 has no clue after measuring part, unidentifiable error

Subtractive Manufacturing

Measurement Attack Result

```
PNT4      =FEAT/POINT,RECT
          THEO/1.5,-0.2415,0.1,0,0,1
          ACTL/1.5,-0.2415,0.1,0,0,1
          CONSTR/POINT,OFFSET,,1.5,-0.2415,0.1
          ASSIGN/V1 = 0
          ASSIGN/V2 = 0
CS1       =SCRIPT/FILENAME= C:\PCDMISW\SCRIPTS\DOG_BONE.BAS
          FUNCTION/Main,SHOW=YES,,
          STARTSCRIPT/
          ENDSCRIPT/
          ASSIGN/PNT1.X = PNT3.X+V1
          ASSIGN/PNT1.Y = PNT3.Y
          ASSIGN/PNT1.Z = PNT3.Z
          ASSIGN/PNT2.X = PNT4.X+V2
          ASSIGN/PNT2.Y = PNT4.Y
          ASSIGN/PNT2.Z = PNT4.Z
```

IN	DIM WIDTH= 3D DISTANCE FROM POINT PNT3 TO POINT PNT1 TRUE					
AX	NOMINAL	+TOL	-TOL	MEAS	DEV	OUTTOL
M	0.5000	0.0100	0.0100	0.4982	-0.0018	0.0000

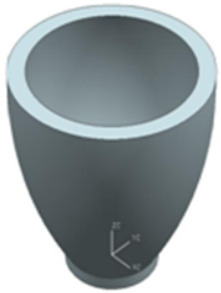
IN	DIM THICK= 3D DISTANCE FROM POINT PNT2 TO POINT PNT4 TRUE					
AX	NOMINAL	+TOL	-TOL	MEAS	DEV	OUTTOL
M	0.2000	0.0100	0.0100	0.1966	-0.0034	0.0000

```
Sub Main
Dim App As Object
Set App = CreateObject ("PCDLRN.Application")
Dim Part As Object
Set Part = App.ActivePartProgram
Dim Var1 As Object
Set Var1 = Part.GetVariableValue ("V1")
Dim Var2 As Object
Set Var2 = Part.GetVariableValue ("V2")
Dim T As Double
Dim W As Double
TMean=0.2
TStd=TMean*0.01
WMean=0.5
WStd=WMean*.01
X1=Rnd()
X2=Rnd()
Y1=Sqr(-1*Log(X1))*Cos(2*3.14159*X2)
Y2=Sqr(-1*Log(X1))*Sin(2*3.14159*X2)
T=Y1*TStd+TMean
W=Y2*WStd+WMean
Var1.DoubleValue= Var1.DoubleValue+ W
Var2.DoubleValue= Var2.DoubleValue+ T
Part.SetVariableValue "V1", Var1
Part.SetVariableValue "V2", Var2
End Sub
```

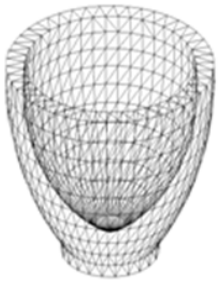
Attack Causes Reporting of Statistically Varied, Within Tolerance, But Erroneous Measurement Values

The AM Digital Thread

- File interception / augmentation
- Bring part out of specification
- Add unwanted features

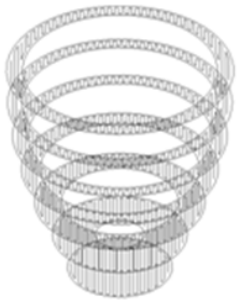


3D Cad Model

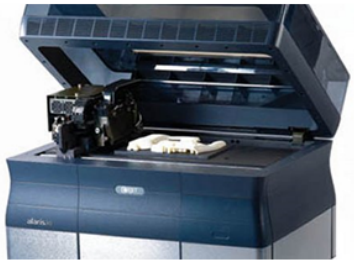


.STL File

Slicing Software



Layer Slices & Tool Path



3D Printer

3D Object

Additive Manufacturing

Phase 1 Attack Vectors

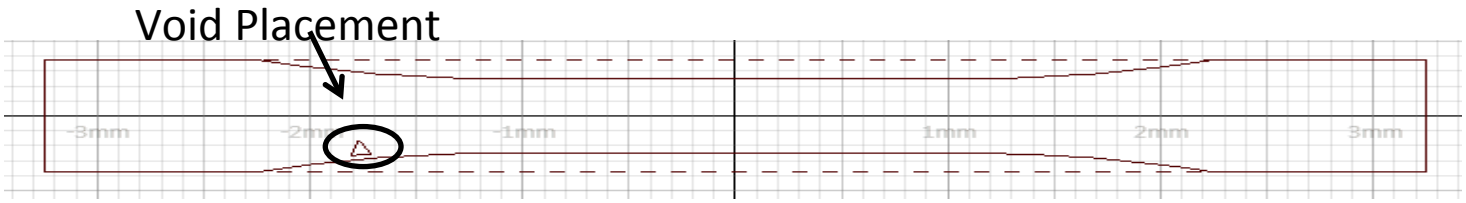
- STL Attack
  - Intercept file and rewrite to include:
    - **Small random voids to reduce structural integrity**
    - **Large voids for component embedding**

- Build Attack
  - Simulate build pause and embedding procedure
    - **Following "large void" STL attack, operator embeds component and then resumes build**

Stratasys Dimension
3-D printer

Additive – STL Attack:

Volume Analysis



- Determine where to place a void
  - Stress concentration areas
    - "Virus" automatically searches for densest mesh areas (most likely to be stress concentration points)
  - Inside/outside

    Ray tracing used to determine if a point is within the mesh
- Algorithm Updates
  - First algorithm generated long slender voids
    - Checking angles of triangle resulted in better voids
  - Tetrahedron void shape adds only four triangles to a file (minimal file size impact and appears as just another of thousands of triangles)

Additive Manufacturing

Phase 1 STL Attack Results

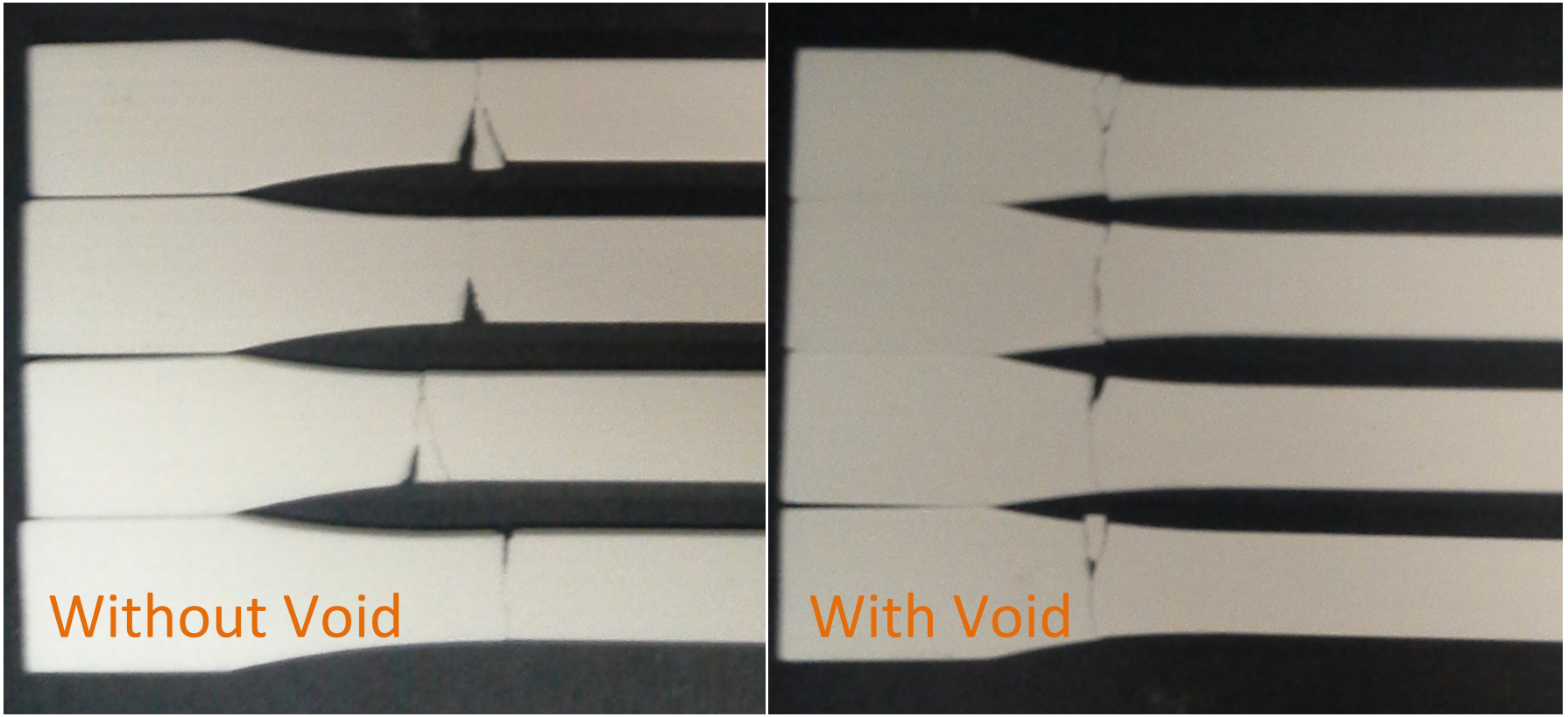
- STL exploit successfully automatically attacked STL files to insert voids

Build paused halfway to show void

Finished Part

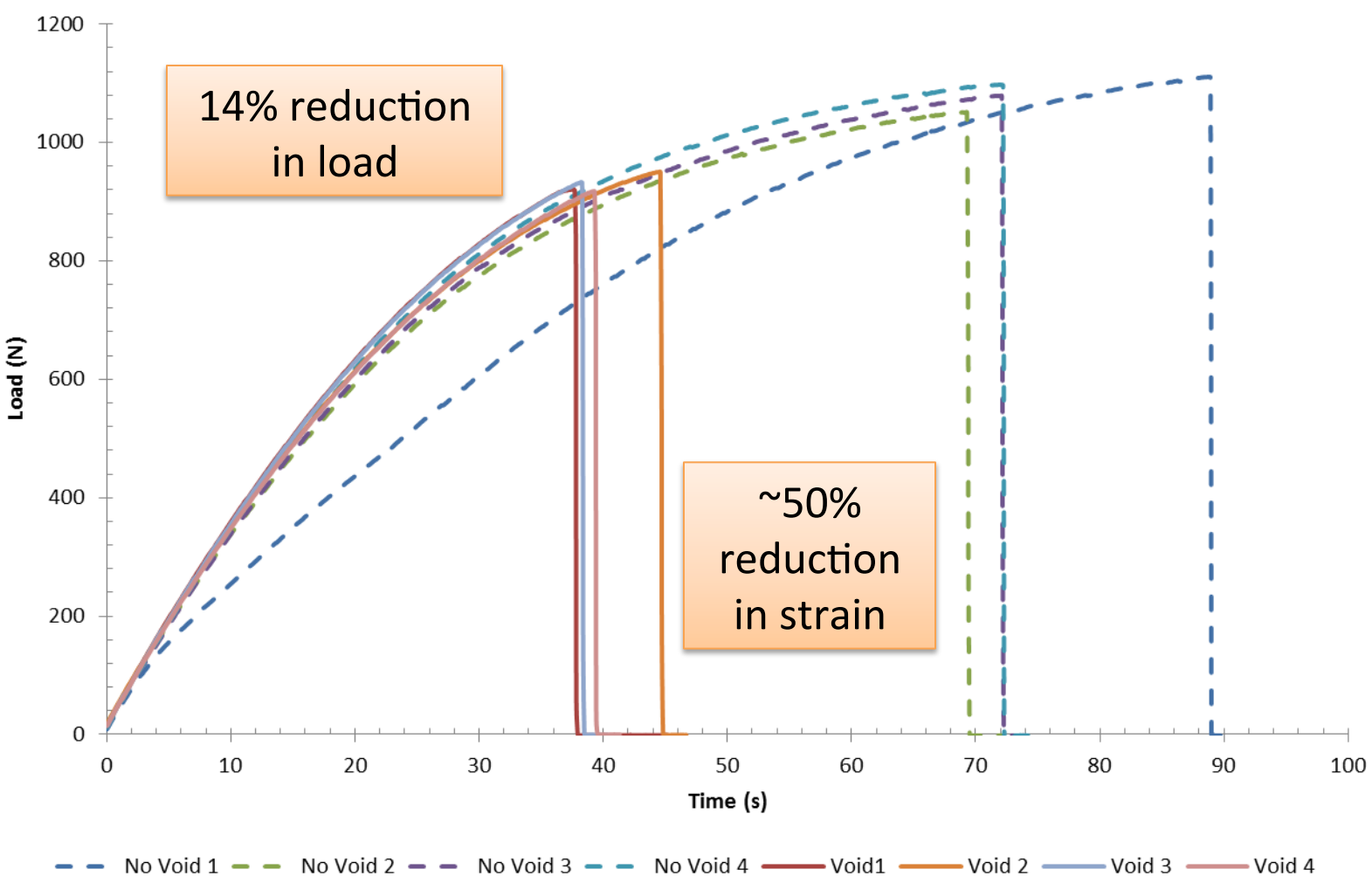
Additive Manufacturing

Phase 1 STL Attack Results – Yield Testing



Fractures occur at the void locations

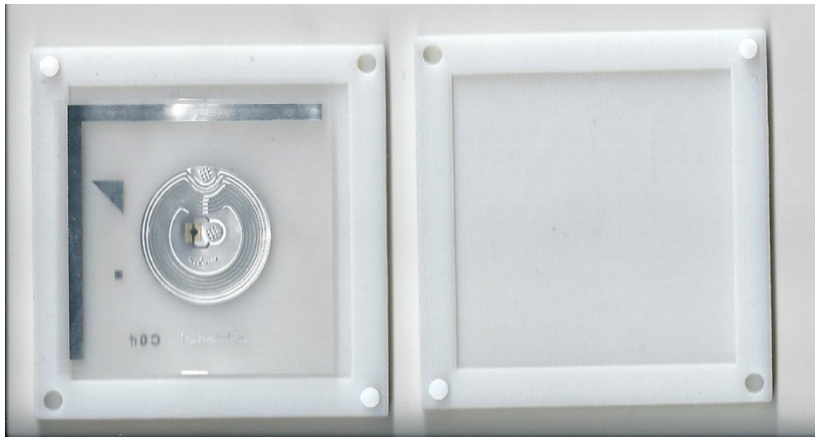
Effects on Part Strength



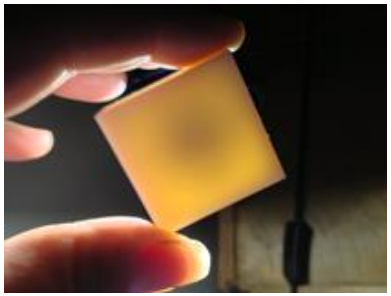
Additive Build Attack

Embedding Process

- Cavity attenuation test fixtures fabricated with Objet VeroWhitePlus on a Connex 350. UV cured photopolymer
- Functioning tags (shadow in lower photo) embedded with Stratasys Dimension SST 768
- Phase 1 Achievements
  - Build successfully halted and resumed
  - Build process did not harm tag functionality
  - Material provided no measureable attenuation to RFID signals



Signal Attenuation Test Fixture

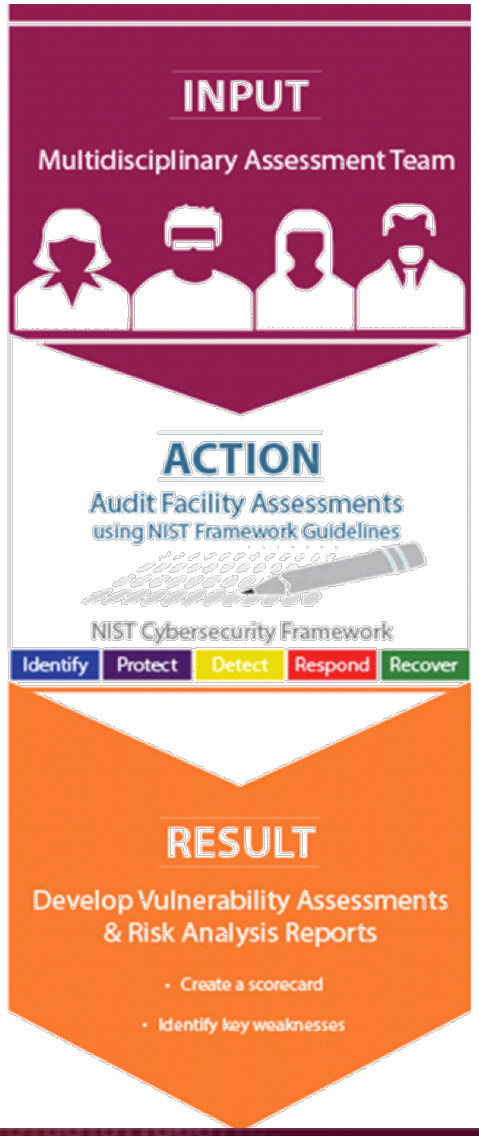


Functioning Embedded RFID tag (horizontal cavity)

Current Research

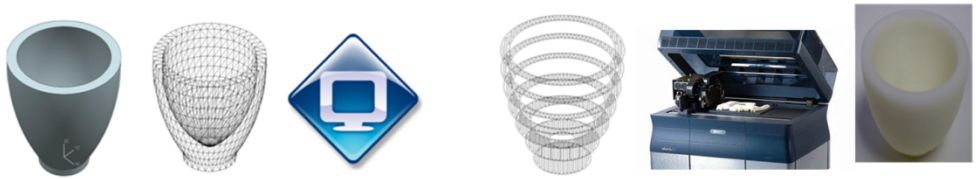
Decision Theory & Vulnerability Discovery

- **A Game Theory Approach to Cyber-Physical Security**
  - Motivate manufacturers to secure their production processes from cyber-physical attacks using game theory.
- **Cyber-Physical Vulnerability Assessment Tool**
  - Create a tool that autonomously identifies cyber-physical vulnerabilities within all levels of a manufacturing organization.
- **Cyber-Physical Vulnerability Database**
  - Create a database of cyber-physical vulnerabilities seen commonly in industry, and provide a roadmap to recovery.

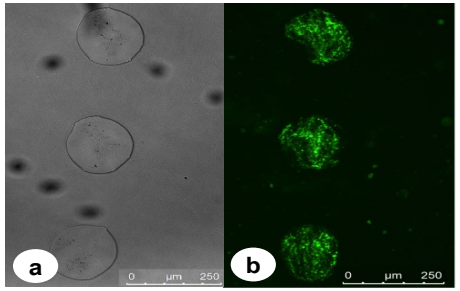


AM Current Research

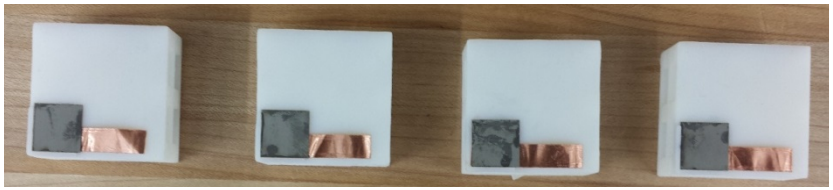
Process Chain Risk Assessment

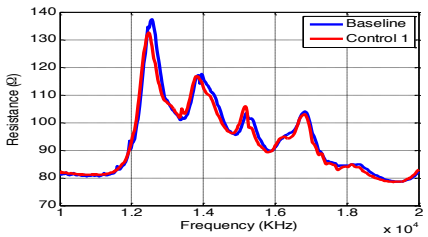


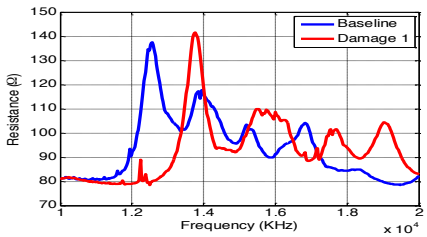
Physical Security Measures



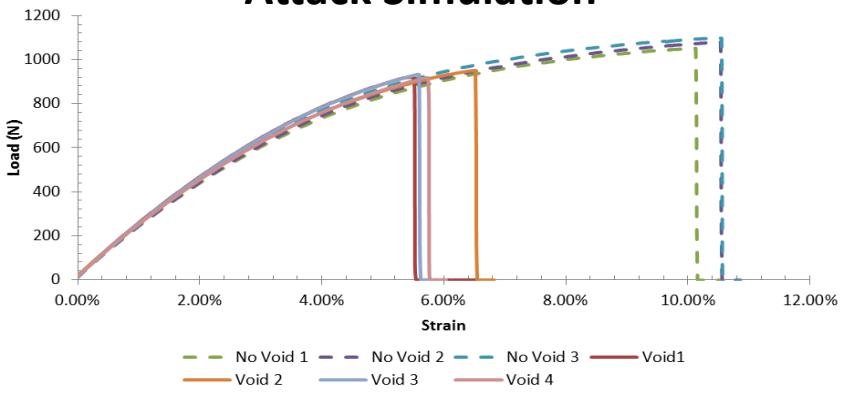
Piezoelectric Sensing and Monitoring

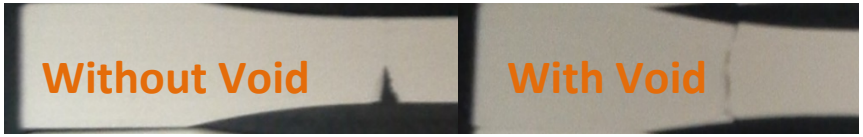






Attack Simulation





Contact Info

Dr. Jaime Camelio

Virginia Tech

Email: jcamelio@vt.edu

Dr. Jules White

Vanderbilt University

Email: jules@dre.vanderbilt.edu