drown -
Cyber-Physical Attack with Additive Manufacturing

Sofia Belikovetsky
Ben-Gurion University of the Negev

Mark Yampolskiy
University of South Alabama

Jinghui Toh
Singapore University of Technology and Design

Jacob Gatlin
University of South Alabama

Yuval Elovici
Ben-Gurion University of the Negev, Singapore University of Technology and Design
Agenda

- Introduction
- Manufacturing process
- The attack
  - Goal of attack
  - Methodology
  - Results
- Scale up
Introduction
What is Additive Manufacturing?
It’s already everywhere
Motivation

“The FAA Cleared The First 3D Printed Part To Fly In A Commercial Jet Engine From GE”
Manufacturing Process
The Manufacturing Process

1 CAD
2 STL convert
3 File transfer to machine
4 Machine setup
5 Build
6 Remove
7 Post-process
8 Application
AM Cyber Threats

Violation of Intellectual property

Sabotage attacks
The Attack
Reducing the fatigue life of a 3D printed object

**Motivation:** Create delayed damage, so that the object breaks after integration into critical system

**Goals:**

- Demonstration of a NEW sabotage attack that targets the fatigue life of a manufactured part in order to damage the system the integrates the part.
- Present and experimentally validate the attack
- Generalize the attack

**Evaluation Methods:**

- Experimental lab and field testing to assess the introduced damage
Use Case: Sabotage of Replacement Propeller via a fatigue attack
Use Case: Sabotage of Replacement Propeller via a fatigue attack

3D Object Designers

STL/AMF Propeller Design

Personal Computer

3D Printer

Replacement Propeller

Quadcopter UAV

Internet

Source and Auxiliary Material Suppliers

3D Printer Owner
Systematic Analysis of attack chains

**Attack Vectors**
- Software
  - Code Injection into AM Files
  - General Infiltration Methods
- Software Supply Chain
  - Software Updates
  - Compromised Software
  - Open Source Backdoor
- Hardware / Firmware
  - Hardware Trojans
  - Firmware Updates
- Network
  - General network attacks
  - Protocol vulnerabilities

**Compromised Elements**
- External Designer
- Controller PC
- Network
  - Network Equipment
  - Network Services
  - Unrelated Assets
- 3D Printer
  - Firmware
  - Hardware

**Influenced Elements**
- Files
  - Design Files
  - Tool Path Files
- Variables
- Printing Configuration
- Slicing Configuration
- Code
  - Printer Control
- Traffic
  - Printer Instructions
  - Interference

**Influences**
- Specification Modification
  - Object Blueprint
  - Orientation
  - Material
  - ...
- Manufacturing Properties Modification
  - Layer Thickness
  - Temperature
  - Speed
  - ...

**Attack Targets**
- Sabotage of Manufactured Part
Manipulation

The Location of the Defect:
Joint connection of the blades to the cap

Iteration through Defects:
0.1 mm gaps – best for the time restraints
Lab tests

Testing setup:

- Installed a benign and sabotaged propellers on a drone in a lab
- Examined the maximal RPM and time of each
Field Trials

Testing setup:
- Replacing the propellers of a drone with AM printed copies.
- 3 benign and 1 sabotaged
- Operating the drone under regular conditions

Results:
- Breakage after 1:42 minutes of normal operation
- When the drone was mid-flight
The selected attack chain

Phishing attack → Controller PC → STL files → Insertion of Gaps → Faster development of Fatigue time => Destruction of the drone
Video

Link:
https://www.youtube.com/watch?v=zUnSpT6jSys
Yes but... Isn’t it easy to detect?

- The change in weight is less than 3%
- The change in printing time is 1 minute out of 1:17 hours
- Signing your G-code is very limiting
- It can be offline
- It can be generalized
Scale up the attack

Proposal:

- Automatic attack of G-Code files
- The files contain critical manufacturing information that stored only there
- The files are hard to verify

Automatic search for “weak spots”: find significantly smaller joint points
Scale up the attack (Cont.)

- Split printing moves into two, skipping the part that intersects with the gaps
- Integrate the script into worm for maximum reach

<table>
<thead>
<tr>
<th>Original Code</th>
<th>Split a printing move</th>
<th>=&gt; G0 X106.0 154.450</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1 X103.265 Y153.205</td>
<td>G1 X103.265 Y153.205 E959.89129</td>
<td></td>
</tr>
<tr>
<td>G1 X107.531 Y155.147</td>
<td>G1 X105.011 Y154.0 E959.89508</td>
<td></td>
</tr>
<tr>
<td></td>
<td>;G1 X106.0 Y154.450 E959.89508</td>
<td></td>
</tr>
<tr>
<td></td>
<td>G1 X107.531 Y155.147 E959.89508</td>
<td></td>
</tr>
</tbody>
</table>
Conclusions

A real threat!

- Expect to see a lot of research and developments in this field
- Opportunity to shape the security in this industry
Thank you!