

Accepted Manuscript

Title: Security of Additive Manufacturing: Attack Taxonomy and Survey

Author: Mark Yampolskiy Wayne E. King Jacob Gatlin Sofia Belikovetsky Adam Brown Anthony Skjellum Yuval Elovici



PII: S2214-8604(17)30502-X
DOI: <https://doi.org/doi:10.1016/j.addma.2018.03.015>
Reference: ADDMA 311

To appear in:

Received date: 2-11-2017
Revised date: 13-2-2018
Accepted date: 14-3-2018

Please cite this article as: Mark Yampolskiy, Wayne E. King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, Yuval Elovici, Security of Additive Manufacturing: Attack Taxonomy and Survey, *Additive Manufacturing* (2018), <https://doi.org/10.1016/j.addma.2018.03.015>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Security of Additive Manufacturing: Attack Taxonomy and Survey

Mark Yampolskiy^{a,*}, Wayne E. King^b, Jacob Gatlin^a, Sofia Belikovetsky^c,
Adam Brown^a, Anthony Skjellum^{d,e}, Yuval Elovici^{c,f,g}

^aUniversity of South Alabama

^bLawrence Livermore National Laboratory

^cBen-Gurion University of the Negev

^dUniversity of Tennessee at Chattanooga

^eAuburn University

^fCyber Security Research Center

^gSingapore University of Technology and Design

Abstract

Additive Manufacturing (AM) is a rapidly growing, multibillion dollar industry. AM is increasingly being used to manufacture functional parts, including components of safety critical systems in aerospace, automotive, and other industries. This makes AM an attractive attack target. AM Security is a fairly new field of research that addresses this novel threat.

This paper serves dual purposes: For researchers just entering AM Security, we provide an in-depth introduction to this highly multi-disciplinary research field. And, for active researchers in the field, this paper provides a comprehensive, structured survey of the state of the art as well as our proposal for attack taxonomies.

Keywords: Additive Manufacturing, 3D Printing, AM Security, Taxonomy, Survey

1. Introduction

Industry 4.0 [1] envisions fully automated manufacturing environments, driven by computerized manufactured equipment—Cyber-Physical Systems (CPS). Additive Manufacturing is a core component in this vision, enabling both manufacturing automation and the creation of parts with properties that could not
5 be achieved with the traditional subtractive manufacturing.

*Corresponding author

Email addresses: yampolskiy@southalabama.edu (Mark Yampolskiy), king17@llnl.gov (Wayne E.King), jrg1222@jagmail.southalabama.edu (Jacob Gatlin), sofia.belikovetsky@gmail.com (Sofia Belikovetsky), ajb1425@jagmail.southalabama.edu (Adam Brown), tony-Skjellum@utc.edu (Anthony Skjellum), yuval_elovici@sutd.edu.sg (Yuval Elovici)

Download English Version:

<https://daneshyari.com/en/article/7205969>

Download Persian Version:

<https://daneshyari.com/article/7205969>

[Daneshyari.com](https://daneshyari.com)