Offensive and Defensive Perspectives in Additive Manufacturing Security

Rohith Yanambaka Venkata, Nathaniel Brown, Daniel Ting and Krishna Kavi

Presented by Nathaniel Brown, University of North Texas
nathanielbrown@my.unt.edu

IARIA

UNT® UNIVERSITY OF NORTH TEXAS®

The Presenter

- Undergraduate Researcher at the University of North Texas (UNT)
- Member of the Computer Systems Research Lab (CSRL) at UNT
- Research applied and conceptual Additive Manufacturing (AM) security

Nathaniel Brown

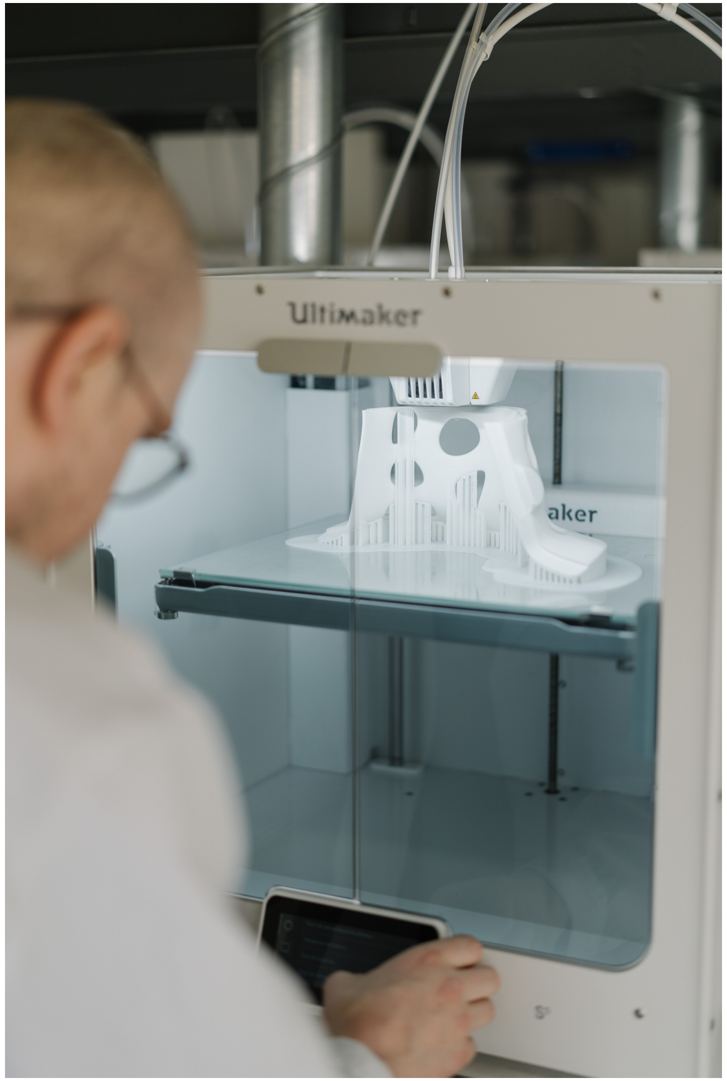
Our Research Interests

- Additive Manufacturing Security
- Internet of Things (IoT) Security
- Hardware and System-Level Security Enhancements
- Processing-in-Memory and Memory Analysis

https://csrl.cse.unt.edu/

What is Additive Manufacturing?

- Key component of Industry 4.0
- Produces materials in a layer-wise fashion
- Decentralizes the manufacturing and distribution process
- Many techniques:
  - Vat Photopolymerization
  - Material Extrusion
  - Material Jetting
  - Powder Bed Fusion



A 3-D Printer

AM Vulnerabilities

- Cyber-physical nature leads to many informational and physical dependencies, leading to vulnerabilities such as:
    - Side-channel attacks
    - Attacks aiming to create minor deficiencies
    - Alter printing orientation
    - Target insecure methods of file transfer
    - Exploit code vulnerabilities
    - Target quality assurance systems

Our Strategy

- Summarize the state-of-the-art in AM security from:
  - The view of the attacker
  - The view of the defender
- Use Microsoft’s STRIDE security model to categorize threats.
- Enumerate mitigative measures based on NIST cyber-physical security recommendations as a launchpad for securing AM systems.

Attacker’s Perspective

Intent of the Attacker

- Can be broadly classified into three categories:
    - Technical Data Theft
    - AM Sabotage
    - Illegal Part Manufacturing

Technical Data Theft

- Side-channel attacks
- Targeting insecure information transfer methods
- Outsourcing risks

- Examples:
    - Machine learning models can recreate 3D models from printer sounds
    - Insecure data transfer methods can leak valuable IP

AM Sabotage

- Creation of minute voids
- Altered printing orientation
- Purposefully damage the machine
- Human externalities

- Examples:
  - Altered printing orientation can affect manufactured products' structural integrity
  - Altered firmware can spread defects to a variety of different printed parts

Illegal Part Manufacturing

- Synthesis of illicit medical products or drugs
- Manufacture of illegal gun parts

Defender’s Perspective

STRIDE Threat Model

- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- Mature
- Widely used for cyber-physical systems

NIST Cyber-Physical Security Recommendations

- Guide to Industrial Control Systems (ICS) Security
- Framework for Improving Critical Infrastructure Cybersecurity
- Security and Privacy Controls for Federal Information Systems

- *Included on the following slides are a sample of relevant recommendations for each threat category*

Spoofing

- *Claiming a false identity in order to gain unauthorized access to resources.*
- Potential risks:
  - Spoof a printer of computer’s identity to intercept 3D models
  - Gain an entry to launch a large-scale attack on an AM system
- Security recommendations:
  - Physical Access Authorizations
  - Session Authenticity
  - Least Functionality

Tampering

- *Malicious modification of data or processes.*
- Potential risks:
  - Insertion of invisible voids
  - Altered printing settings
  - Installation of malicious firmware
- Security Recommendations:
  - Continuous Monitoring
  - Information Input Validation
  - Customized Development of Critical Components

Repudiation

- *Falsely denying the occurrence of an action or event.*
- Potential risks:
  - Hijack insecure logging systems to prevent discovery of alterations
  - Targeting of other tracing systems and modification of relevant data
- Security Recommendations:
  - Network Disconnect
  - Adaptive Identification and Authentication

Information Disclosure

- *Data leaks or breaches that violates the confidentiality requirements of a system*
- Potential Risks:
  - Theft of valuable 3D models
  - Side-channel attacks that recreate models
- Security Recommendations:
  - Information in Shared Resources
  - Wireless Link Protection
  - Boundary Protection Devices

Denial of Service

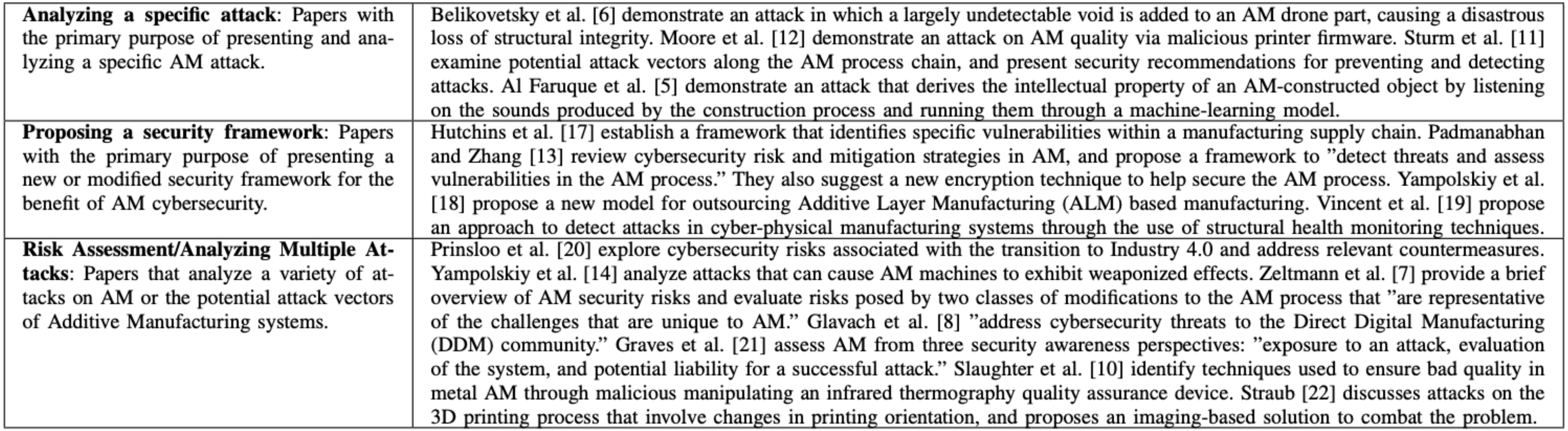
- *Disruption of a service or network resource that prevents users from accessing the network service*
- Potential Risks:
  - *In-situ* interruption of printing processes
  - Interruption of information transfer
- Security Recommendations:
  - Error Handling
  - Application Partitioning

Elevation of Privilege

- *Unauthorized access to system resources by violating the authorization requirement of a system*
- Potential Risks:
  - Stepping stone to launch attacks with greater effects
  - Especially relevant for systems that implement hierarchical authorization
- Security Recommendations:
  - (Proper Authentication + Authorization Mechanisms)
  - Memory Protection

Categorization of Papers by Purpose

TABLE I. CATEGORIZATION OF PAPERS BY PURPOSE



Analyzing a specific attack: Papers with the primary purpose of presenting and analyzing a specific AM attack.	Belikovetsky et al. [6] demonstrate an attack in which a largely undetectable void is added to an AM drone part, causing a disastrous loss of structural integrity. Moore et al. [12] demonstrate an attack on AM quality via malicious printer firmware. Sturm et al. [11] examine potential attack vectors along the AM process chain, and present security recommendations for preventing and detecting attacks. Al Faruque et al. [5] demonstrate an attack that derives the intellectual property of an AM-constructed object by listening on the sounds produced by the construction process and running them through a machine-learning model.
Proposing a security framework: Papers with the primary purpose of presenting a new or modified security framework for the benefit of AM cybersecurity.	Hutchins et al. [17] establish a framework that identifies specific vulnerabilities within a manufacturing supply chain. Padmanabhan and Zhang [13] review cybersecurity risk and mitigation strategies in AM, and propose a framework to ”detect threats and assess vulnerabilities in the AM process.” They also suggest a new encryption technique to help secure the AM process. Yampolskiy et al. [18] propose a new model for outsourcing Additive Layer Manufacturing (ALM) based manufacturing. Vincent et al. [19] propose an approach to detect attacks in cyber-physical manufacturing systems through the use of structural health monitoring techniques.
Risk Assessment/Analyzing Multiple Attacks: Papers that analyze a variety of attacks on AM or the potential attack vectors of Additive Manufacturing systems.	Prinsloo et al. [20] explore cybersecurity risks associated with the transition to Industry 4.0 and address relevant countermeasures. Yampolskiy et al. [14] analyze attacks that can cause AM machines to exhibit weaponized effects. Zeltmann et al. [7] provide a brief overview of AM security risks and evaluate risks posed by two classes of modifications to the AM process that ”are representative of the challenges that are unique to AM.” Glavach et al. [8] ”address cybersecurity threats to the Direct Digital Manufacturing (DDM) community.” Graves et al. [21] assess AM from three security awareness perspectives: ”exposure to an attack, evaluation of the system, and potential liability for a successful attack.” Slaughter et al. [10] identify techniques used to ensure bad quality in metal AM through malicious manipulating an infrared thermography quality assurance device. Straub [22] discusses attacks on the 3D printing process that involve changes in printing orientation, and proposes an imaging-based solution to combat the problem.

Detailed Citations found in Paper

Conclusion

- As the push for Industry 4.0 continues, the importance of properly securing AM systems is only increasing.
- Questions we would like to see answered:
    - *To what extent have manufacturers secured their AM systems against the wide variety of attacks? Should we push for more manufacturer openness about their security methodologies?*
    - *What additional properties unique to AM could an attacker exploit?*

Miscellaneous

- Photos from Unsplash

Click to add text

The authors would like to acknowledge the infrastructure and support of Center for Agile & Adaptive and Additive Manufacturing funded through State of Texas Appropriation (#190405-105-805008-220).