C3PO: A Security Analysis Tool for Networked 3D Printers

Matthew McCormack, Sanjay Chandrasekaran, Tianlong Yu,
Sandra DeVincent Wolf, Vyas Sekar

May 21, 2019

CMU-CyLab-19-002

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

C3PO: A Security Analysis Tool for Networked 3D Printers

Matthew McCormack, Sanjay Chandrasekaran, Tianlong Yu, Sandra DeVincent Wolf, Vyas Sekar
Carnegie Mellon University
{mmccorm1,sanjayc,tianlony,vsekar}@andrew.cmu.edu,sandradevincentwolf@cmu.edu

ABSTRACT

Advanced manufacturing has brought networked devices and 3D printing to the manufacturing domain. While these changes have increased efficiency, they have simultaneously introduced new security risks. For example, networked 3D printers can be exploited by an attacker to steal proprietary design data, modify safety-critical parts, or halt operations. Furthermore, attackers can use other compromised devices on the network to launch attacks against these networked 3D printers. In this work, we present C3PO, a network security assessment tool that systematically identifies security threats to 3D printers in advanced manufacturing deployments. C3PO identifies an individual 3D printer's potential network-based vulnerabilities (e.g., determines if encryption is used when transmitting data). The second phase identifies possible multistage attack paths for achieving a specific goal on a given network deployment. As a use case, we applied C3PO to analyze 8 types of 3D printers in 3 real-world deployments to identify network security trends in commercial 3D printers and provide insights on how to secure these machines after they are deployed.

CCS CONCEPTS

• **Security and privacy → Network security**; **Vulnerability scanners**.

KEYWORDS

Network security, 3D printing

1 INTRODUCTION

Manufacturing centers are replacing stand-alone, manually operated devices with networked manufacturing devices. Additionally, Industrial Internet of Things (IIoT) devices are being deployed to increase efficiency and provide process insights [16],[23]. This has increased the need for network security in the manufacturing domain [25],[28],[46]. For example, Boeing's airplane production facility was impacted when networked manufacturing machines were infected with malware [33].

The manufacturing industry is also incorporating networked additive manufacturing machines, commonly referred to as 3D printers. Aviation and other safety-critical applications desire to utilize 3D printed parts [11], [43]. However, there are concerns about the safety and security of 3D printed parts due to the potential for network attacks on 3D printers [10],[22],[63]. Specifically, an attacker could produce parts with "undetectable" defects (where a part has the correct outward appearance but significantly different physical properties) [10]. Additionally, these networked 3D printers have created new vectors for stealing proprietary data [68] and disrupting operations by making machines unavailable [59].

Prior work has demonstrated that an attacker can cause a 3D printer to make "undetectable" defective parts by modifying the input files [53], [58], [10]. Others have demonstrated that sensitive data on a 3D printer (e.g., printing instructions) can be accessed by a network attacker [18]. However, these works have the following limitations: (1) they only identified a limited set of vulnerabilities on a 3D printer (e.g., data exfiltration and not defective parts), (2) they only analyzed 3D printers from a single vendor (currently there are 50+ vendors [6]), and (3) they did not consider the security implications of other devices on the network. Thus, a security assessment tool is needed. Existing tools are insufficient as they only provide partial coverage of 3D printer vulnerabilities. It is challenging due to the plethora of 3D printer vendors and their use of proprietary protocols.

To address these limitations, we developed a security assessment tool, Connected 3D Printer Observer (C3PO) [1], which systematically identifies potential security vulnerabilities in deployed 3D printers that an attacker on the network could use for printing defective parts, stealing data, or rendering 3D printers unavailable. C3PO is composed of two parts. One part uses a vendor agnostic approach for identifying security vulnerabilities on individual 3D printers, covering key recommendations from industry standards [24] and best practices [39]. The other part identifies attack paths an attacker could follow to achieve their attack goals for a given network deployment and set of 3D printer vulnerabilities (e.g., what are the security implications of deploying an IIoT camera with a 3D printer?).

C3PO's individual 3D printer analysis emulates a network attacker and identifies any possible security issue. It performs a security audit, using a network capture of benign network traffic to the 3D printer as an input. It inspects this network capture, looking for security properties (e.g., encryption). Next, it probes for security vulnerabilities using existing vulnerability scanning tools that search for susceptibility to known exploits. It continues its vulnerability search by modifying and replaying legitimate network traffic. Specifically, the network capture is used for generating fuzzing inputs to identify malicious inputs to the 3D printer application. Additionally, multiple iterations of the network capture are replayed simultaneously to identify potential Denial of Service (DoS) conditions. The results from each of these tests are used to identify potential security risks for an individual 3D printer.

As a demonstration of C3PO, we ran the individual 3D printer analysis on 8 different 3D printer models from 7 vendors, spanning 3D printer costs and printing processes. We found 28 vulnerabilities, our specific findings are:

- None used authentication or encryption for transferring data
- All 8 were vulnerable to a DoS attack (e.g., SYN flood)
- 6 of 8 exposed unused network services (e.g., open ports)
- 3 of 8 were vulnerable to known exploits (e.g., [34])
- 3 of 8 allowed inputs that crashed the printing application

The second part of C3PO identifies multistage attacks that allow an attacker to achieve their goal against a 3D printer (e.g., printing

defective parts, stealing data, or making the 3D printer unavailable). An example multistage attack is an attacker compromising an IIoT camera using default credentials and using the camera to launch a DoS attack against the 3D printer. C3PO takes a 3D printer's security risks (can be generated by C3PO's individual 3D printer analysis) and a network blueprint to generate all possible attack paths using the attack graphing tool MulVAL [38]. This provides a holistic view of how an attacker could target a specific 3D printer, and gives insights on how additional networked devices (e.g., IIoT cameras) can impact the security of a networked 3D printer.

We continued our demonstration by running C3PO's system-wide security analysis on 3 different, real-world 3D printer deployments, covering multiple network sizes and complexities. Each deployment was analyzed with 19 theoretical scenarios that assumed the presence of different vulnerabilities on devices in a 3D printer's network (e.g., IIoT cameras with default credentials, PCs running Windows 95, etc.). We made the following observations.

- The majority of devices in 3D printer deployments were embedded devices (e.g., IIoT cameras)
- Key devices bridged subnets and were a part of the majority of potential attack paths
- Previously ignored devices (i.e. network hardware, other 3D printers) could be used by an attacker

Road map: §2 provides a background on 3D printing, our attack model, and motivates the need for a security analysis tool. Next, we discuss the design of our open source security analysis tool (C3PO) and measurement methodology in §2. We provide details about using the tool to evaluate 8 commercial 3D printers in §4, and 3 different manufacturing deployments in §5. We leverage these findings to provide insights into creating defenses for networked 3D printers in §6. Finally, we discuss related work and conclude.

2 BACKGROUND AND MOTIVATION

We provide an overview of the 3D printing workflow and a generic network deployment to define our network attacker. These are used to motivate the need for a security analysis tool that identifies both an individual 3D printer's vulnerabilities and network deployment vulnerabilities.

2.1 3D Printing

Additive manufacturing (AM), often referred to as 3D printing, fabricates an object by sequentially joining layers of deposited material, enabling the fabricating of complex internal structures that are not possible using traditional (subtractive) manufacturing methods [63]. 3D printing is integral to the future of manufacturing as it shortens the time between design and final product delivery, enables on-demand production, and allows for greater customization.

The process of 3D printing an object generally follows the four-step workflow in Fig. 1. Each step transforms the data into a new representation and can occur on a different physical machine, resulting in multiple data transfers.

(1) **Generate CAD representation**. Create a digital representation of the object, often as a stereolithography file (*.STL).
(2) **Convert to layer representation**. Divide the object into vertical layers, often as a slice layer interface file (*.SLI).

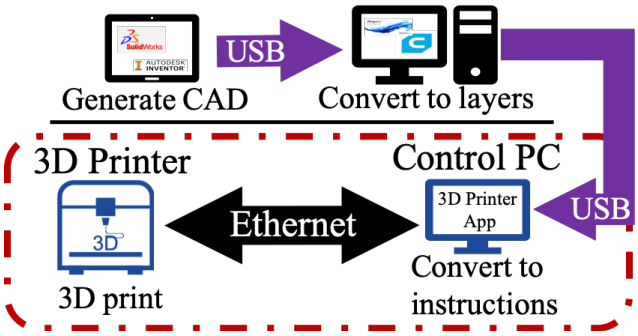


Figure 1: Abstract 3D printing workflow. Our work focuses on analyzing the security of the bottom half.

(3) **Convert to printer commands**. Generate machine-specific printing instructions specifying machine operations and settings (e.g., material depositing speed) for each layer. These instructions can be stored in many formats, the most commonly used is G-code (RS-274 [56]).[1]
(4) **3D Print**. The machine-specific printing instructions are transferred to the 3D printer. The commands might be executed automatically or after an explicit user interface (UI) action.

Our work focuses on evaluating the security of connecting 3D printers to a network, specifically wired Ethernet networks. To better understand the security challenges in these networks, we briefly describe their structure.

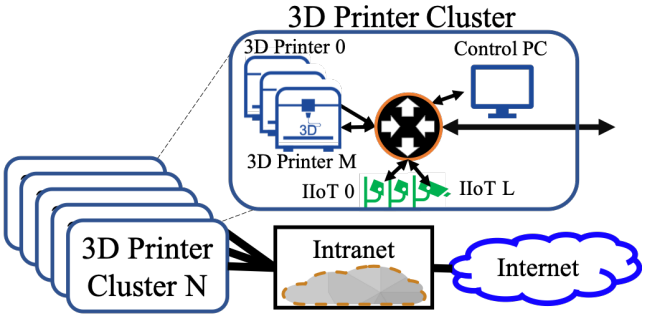


Figure 2: Generalized advanced manufacturing deployment, containing clusters of 3D printers, potentially with IIoT sensors and control PCs.

Advanced manufacturing deployments of 3D printers generally conform to the model depicted in Fig. 2. Each deployment has 1 to N 3D printer clusters connected to an intranet. These clusters typically contain 1 to M copies of a single type of 3D printer, as different types might utilize different processes/materials.[2] Additionally, each cluster can include a control PC for sending printing instruction files to the 3D printers as well as various other networked devices (e.g., IIoT cameras). While each 3D printer cluster might be on its own subnet, they are often accessible from other subnets on the intranet to enhance productivity.

[1] G-code was used by 3 of the 8 3D printers we analyzed.
[2] For example, a stereolithography 3D printer might use photopolymer resin while a fused filament fabrication 3D printer might use polylactic acid filament.

2.2 Attack Model

Security is a top concern for manufacturing centers as they migrate to smart factories [25]. Our work focuses on systematically analyzing the network security of networked 3D printers. Thus, we consider a network attacker without physical access to the 3D printers who is not concerned about being stealthy on the network. Based upon 3D printer attack taxonomies [40], [63], our attacker has one of the following goals:

(1) Create defective parts[10]
(2) Steal proprietary information/data[68]
(3) Cause machine downtime[59]

We limit our attacker's access to the 3D printer to only be over the network (i.e. no physical access). An attacker can achieve network access through various means. If we consider a network with a single 3D printer, an attacker can start with network access (e.g., insider threat) or can gain network access by compromising a device on the network. For example, an attacker could gain access to a control PC using an e-mail with a malicious link [10], an IIoT device using default credentials [8]), or a networking switch using unpatched vulnerabilities [57]. Thus, the security of 3D printer deployments must consider the other devices on the network with the 3D printer.

2.3 Motivating Scenarios

We provide two hypothetical attack scenarios to motivate the need for a systematic security analysis tool. The first scenario shows the need to identify security vulnerabilities on an individual 3D printer, when an attacker already on the network (e.g., insider threat) makes a 3D printer unusable through a DoS attack. The second highlights the need to incorporate the network deployment in the security analysis of a 3D printer. In this scenario, an attacker utilizes a multistage attack to create a man in the middle (MitM) situation, allowing her to modify printing instructions as they are transmitted to the 3D printer–resulting in defective parts being printed.

2.3.1 DoS Attack to Stop Production. A rapid prototyping manufacturer might have a 3D printer with a DoS vulnerability where the 3D printer can only process 1,000 simultaneous status requests before its compute resources are exhausted, prohibiting the 3D printer from receiving any new printing instruction files. A disgruntled employee uses a computer with network access to the 3D printer and continuously generates 1,000s of simultaneous status requests, effectively DoSing the 3D printer and stopping manufacturing operations, potentially costing the company thousands of dollars in lost time [59]. If the company had a tool to identify vulnerabilities such as this, they could have implemented defenses to block attacks similar to these DoS attacks (e.g., rate limiting 3D printer requests).

2.3.2 Multistage MitM Attack to Print Defective Parts . A safety critical component manufacturer might install an IIoT camera to enable remotely monitoring 3D printing operations. This camera is connected to the same network as the 3D printer due to its physical location and existing network infrastructure. Additionally, the camera is accessible over the internet and the default credentials were not changed. This allows an attacker on the internet to compromise the camera (similar to [8]).

The manufacturer's 3D printer does not utilize authentication or encryption when receiving printing instructions, allowing any host on the network to send printing instructions to the 3D printer. Furthermore, the control PC uses broadcast messages to identify the 3D printer prior to sending printing instructions, allowing an attacker to masquerade as the 3D printer and receive the printing instructions. This combination of vulnerabilities allows an attacker on the internet who has compromised the IIoT camera to create a MitM situation between the control PC and the 3D printer. An attacker could use this to modify the printing instructions for safety critical components as they are in transit from the control PC to the 3D printer, creating components with hidden, internal weaknesses that will result in latent failures (similar to [10] or [53]). If companies had a tool for evaluating the security implications of adding an IIoT camera to a 3D printer deployment, they could have ensured that defenses were placed to mitigate the risks or that the camera was on a separate network.

These two examples do not represent a comprehensive list of attack paths; the combination of 3D printer vulnerabilities and devices on the 3D printer's network create an array of possible attack paths. Our C3PO tool aims to systematically identify 3D printer vulnerabilities and attack paths an attacker could use to achieve her goals for a given 3D printer deployment.

2.4 Limitations of Prior Work

Prior work has either qualitatively analyzed potential attacks on 3D printers [62], [63], [65] or demonstrated a specific attack against a single vendor's 3D printer (create defective parts: [10], [22], [49], [53], [58]; data exfiltration: [18]). Many attack demonstrations have focused on modifying files prior to printing instructions being generated by the control PC (e.g., before Step 3 from the workflow in §2.1) [10], [53]. Tools that have analyzed the network security of 3D printers have been limited to only analyzing a single vendor's 3D printers and to only identifying data exfiltration vulnerabilities and they might miss vulnerabilities leading to attacks such as DoS (e.g., §2.3.1) [18]. Prior works are limited in their generalizability to multiple vendor's 3D printers and ability to identify multiple types of vulnerabilities. Furthermore, they only consider 3D printers in isolation, missing attacks that depend upon the network deployment (e.g., §2.3.2).

3 C3PO OVERVIEW AND METHODOLOGY

The goals of C3PO are to (1) systematically identify an individual 3D printer's potential security vulnerabilities and (2) identify how a 3D printer's network deployment impacts an attacker's ability to make defective parts, steal proprietary information/data, or cause 3D printer downtime.

3.1 C3PO Overview

To achieve both of these goals, we divided our tool into two parts. One part scans for vulnerabilities on an individual 3D printer; the other analyzes the network deployment to identify potential attack paths. These two parts can be used independently or in conjunction, where a 3D printer's vulnerabilities are fed into its network deployment analysis.

3.1.1 Individual 3D Printer Vulnerability Analysis. The goal for our individual 3D printer vulnerability analysis tool was for it to systematically find vulnerabilities that a network attacker could exploit for achieving any of her goals (§2.2). Additionally, we wanted the tool to support an array of 3D printer vendors by being protocol-agnostic (e.g., not limited to only analyzing 3D printers that transmit print instructions using G-code).

We approached this security analysis from the perspective of a network attacker. First, we wanted to identify known vulnerabilities (e.g., CVEs). Many existing penetration testing tools exist to scan for these known vulnerabilities. However, this does not give a complete view of all possible vulnerabilities (e.g., DoS vulnerabilities in the 3D printer application). Next, we asked what an attacker could glean if she could observe network traffic to the 3D printer. Observing this network traffic gives insights about the 3D printer's operating assumptions (e.g., is network data implicitly trusted) and details about its protocol (e.g., is it running a web server). Armed with this knowledge of the protocol format, potentially malicious inputs can be generated (e.g., fuzzing) and legitimate exchanges can be replayed in a stress test to identify potential DoS conditions. Thus, we used an attacker perspective to systematically evaluate the security of a 3D printer without knowing its protocol (§4.2).

3.1.2 Network Deployment Security Analysis. The goal of our system-wide security analysis tool was to identify how a 3D printer's network deployment impacts its security (e.g., §2.3.2 where an IIoT camera causes defective parts to be printed). Many other devices are simultaneously being added to manufacturing networks (e.g., IIoT). Our assumption is that these devices might have poor security properties, and are likely not being administered as carefully as traditional IT infrastructure. Thus, we aimed to identify how all of these devices could be used by an attacker against a 3D printer.

First, we need a network blueprint detailing all of the devices that have network access to the 3D printer. We approximated this by mapping the 3D printer and the control PC's subnet, to identify devices that could directly access the 3D printer. Second, we chose to use attack graphing to systematically identify all possible paths an attacker could follow through the network to attack the 3D printer. However, the completeness of the results produced by attack graphing is directly correlated to the depth of one's knowledge about the network devices (e.g., knowing each device's specific vulnerabilities). In the absence of this knowledge, attack graphing is still beneficial for evaluating theoretical scenarios based upon assumed device vulnerabilities (§5.2).

3.1.3 Scope: Our C3PO tool identifies vulnerabilities a network attacker could exploit; thus it does not identify every possible vulnerability. For example, fuzzing the application will likely not exercise the 100% code coverage that binary analysis might be able to achieve for a firmware image. However, some 3D printer vendors limit access to their firmware and these firmware images can be designed to run on non-x86 architectures, limiting the ability to use binary analysis. C3PO is a generic network security assessment tool; it could be used for evaluating other networked devices (e.g., IIoT devices), we use 3D printers as a demonstration of the tool.

3.2 Methodology

We used C3PO to both identify individual 3D printer vulnerabilities and analyze 3D printer deployments.

3.2.1 Individual 3D Printer Evaluation. The individual 3D printer security assessment was performed on 8 different commercially available 3D printers. These 3D printers ranged from low-cost, desktop polymer machines to $100K+, industrial metal printers as shown in Table 1. This set of printers exercised our tools' ability to be protocol-agnostic, as we observed 5 different protocols. During our evaluation we transferred printing instructions for the same part to each 3D printer. C3PO was able to identify a total of 28 security vulnerabilities.

Table 1: 3D printers evaluated.

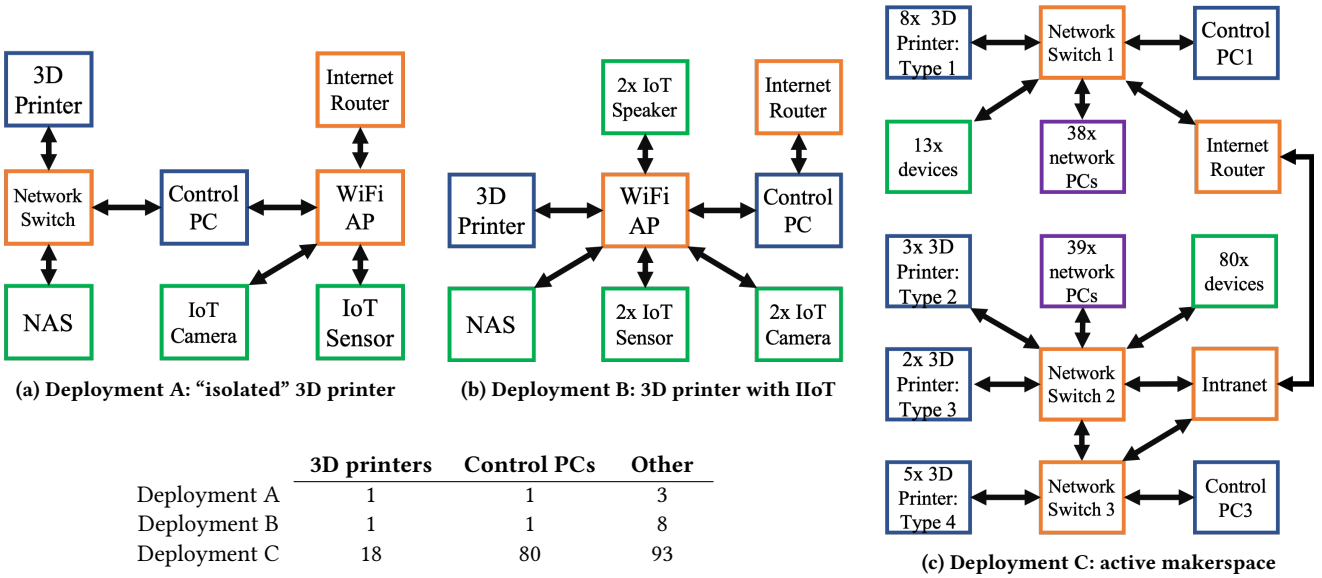
Redacted Name	Approx. Cost (US$)	Year Released	Material	Printing Protocol
Machine A	300	2015	Polymer	G-code
Machine B	1,400	2019	Polymer	G-code
Machine C	2,850	2015	Polymer	proprietary
Machine D	4,200	2016	Polymer	compressed G-code
Machine E	17,000	2017	Polymer	compressed proprietary
Machine F	31,900	2007	Polymer	compressed proprietary
Machine G	150,000	2016	Metal	proprietary
Machine H	~1,000,000	2014	Metal	proprietary

Note: Machines E & F were from the same manufacturer.

3.2.2 3D Printer Deployment Evaluation. C3PO's system-wide security analysis was performed on 3 different 3D printer deployments, depicted in Fig. 3. These three deployments were representative of the following categories:

- An "isolated" single 3D printer (e.g., a company experimenting with 3D printing)
- A 3D printer with many IIoT devices (e.g., a company experimenting with IIoT to improve its 3D printing)
- A large manufacturing environment with multiple 3D printers and 100s of other devices (e.g., a smart factory)

We evaluated each of these deployments using the specific 3D printer vulnerabilities identified by C3PO's individual 3D printer assessment to identify all attack paths that allowed an attacker to print defective parts, exfiltrate proprietary data, or deny manufacturing operations on a 3D printer. Due to a lack of knowledge about all of the device's vulnerabilities (e.g., IIoT device vulnerabilities), attack graphs were generated for 19 theoretical situations, including assumed vulnerabilities on the control PCs, network hardware, and other network devices. This analysis was performed once assuming that the attacker was on the local network (e.g., an insider threat) and repeated for a remote attacker. C3PO analyzed networks with up to 190 total devices (18 of them 3D printers), identifying an average of 5 attack paths per insecure device on the network.



(a) Deployment A: "isolated" 3D printer

(b) Deployment B: 3D printer with IIoT

(c) Deployment C: active makerspace

	3D printers	Control PCs	Other
Deployment A	1	1	3
Deployment B	1	1	8
Deployment C	18	80	93

Figure 3: Real-world 3D printer network deployments.

4 MACHINE-LEVEL ANALYSIS

C3PO's individual 3D printer security analysis systematically characterizes the security issues of a 3D printer using a synthesis of existing penetration testing tools and our custom-built tools.

4.1 Tool

4.1.1 Tool Requirements. The tool needs to be protocol-agnostic, capable of analyzing 3D printers using different protocols. The tool needs to systematically search for vulnerabilities a network attacker could exploit. To identify the minimum coverage requirements, we referenced security standards [24] and best practices [39] for networked devices (additional details can be found in Appendix A). We pruned areas that were not applicable to the manufacturing domain (e.g., privacy) and others that could not be evaluated with only network access (e.g., physical hardening). We grouped the remaining areas into four general categories: (1) data transfer, (2) network services, (3) insecure applications, and (4) availability, as shown in Table 2.

4.1.2 Existing Off-the-Shelf Tools. Existing network security tools do not comprehensively cover all of these vulnerability categories. Tools exist for analyzing data transfer (e.g., Wireshark [14]) and others for identifying network services (e.g., Nmap [31]). Still others determine a host's susceptibility to known vulnerabilities in network services (e.g., Nessus [55], openVAS [21], Metasploit [45], Nikto [54], etc.); while others find application vulnerabilities (e.g., Mutnity [51], BooFuzz [41], etc.). Finally, some provide limited insights on availability (e.g., hping [48]). However, none of these existing tools comprehensively analyze all of the vulnerability areas highlighted by the standards and best practices. Furthermore, some of these tools require manual inspection or only provide partial coverage of vulnerability risks within a given category, as shown in Table 3.

Table 2: Security assessment categories for networked devices from industry standards from IEC 62443-4-2 Foundational Requirements (FR) [24] and best practices from OWASP IoT Top 10 [39].

Category	Description	Reference	In scope
1: Data Transfer	Authentication	OWASP #1 IEC FR 1 & 3	✓
	Encryption	OWASP #7 IEC FR 3 & 4	✓
2: Network Services	Network access	OWASP #2 IEC FR 1 & 5	✓
	Outdated libraries	OWASP #5	✓
3: Insecure Applications	Insecure applications	OWASP #3 IEC FR 2 & 3	✓
	Insecure updates	OWASP #4 IEC FR 3	✓
4: Availability	Robust to DoS	IEC FR 3 & 7	✓
5: Out of Scope	Insufficient privacy	OWASP #6	X
	Lack of device management	OWASP #8 IEC FR 1-3 & 6	X
	Insecure default settings	OWASP #9 IEC FR 7	X
	Lack of physical hardening	OWASP #10 IEC FR 3 & 7	X

4.1.3 Tool Design. The C3PO's individual 3D printer analysis synthesizes existing tools to provide a more complete security assessment and augments these with custom tools for identifying application-specific vulnerability details. It requires a network connection to the 3D printer under test, and a network capture of the

Table 3: Capabilities of existing network security tools.

Tool	Data Transfer	Network Services	Insecure Application	Availability
Wireshark [14]	◐[manual analysis]			
Nmap [31]		◐[only ID]		
Nessus [55]		●		
Metasploit [45]		●		◐[basic DoS]
Mutiny [51]			◐[crash input]	
hping [48]				◐[basic DoS]

●: complete coverage ◐: partial coverage [limitation]

3D printer receiving printing instructions.[3] C3PO systematically analyzes each vulnerability category identified in the standards and best practices before outputting a report of its vulnerability findings. An overview of the tool is given in Fig. 4. Next we will briefly discuss the module for each vulnerability category.

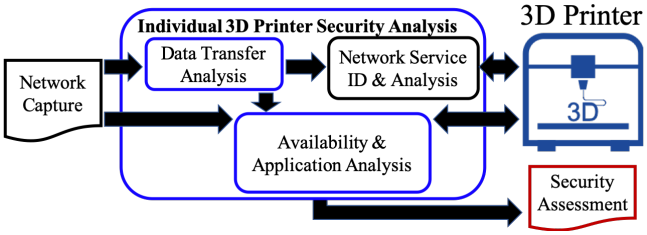


Figure 4: Overview C3PO's individual 3D printer security analysis tool.

Data Transfer Analysis: Analyzes the input network capture to determine the presence of: (1) encryption and (2) authentication. Encryption is determined by calculating the percentage of printable characters in the data segment of each packet after removing any padding. It was assumed encrypted packets would have a normal distribution of values (approximately 37% printable characters[4]), while an unencrypted packet would contain a higher proportion of printable characters (at least double, >75%). We excluded packets that contained data matching known formats (e.g., PNG, GZ, etc.). The lack of encryption and authentication allows an attacker to send instructions for printing defective parts (similar to [10]).

Identify Network Services: We leveraged existing network mapping tools (e.g., Nmap [31]) to identify network services running on the 3D printer. Open ports identified by the tool are compared to the ports used in the network capture to identify potentially unnecessary open ports on the 3D printer. These unused open ports could be indicators of insecure design or a compromised machine (e.g., attacker installed backdoor). We augmented this with a tool to infer the 3D printer's subnet mask. This was performed by sweeping the tool's IP address across subnets and checking for responses to ICMP requests. This identifies potential vectors an attacker could use to access the 3D printer.

Insecure Network Services Analysis: We further leveraged existing network scanning tools (e.g., openVAS [21], Nessus [55], etc.) to identify susceptibility to known vulnerabilities (e.g., published CVEs). These identify vulnerabilities such as those used on Boeing's aircraft factory [33].

Insecure Applications: To identify potential vulnerabilities within the 3D printer's application software, we used an existing mutational fuzzer that generates inputs based upon a network capture [51]. Fuzzed inputs were transmitted for 30 minutes while a benign status request message was used to identify an input that caused the application to crash and no longer respond properly.

Additionally, if the printer allowed for firmware updates to be performed over the network, a network capture of this operation was collected and analyzed by the data transfer module for use of encryption and authentication to determine the potential for an attacker to send malicious firmware images (such as in [22]).

Availability Analysis: For security countermeasures we analyzed robustness to DoS attacks. We checked for susceptibility to basic DoS attacks (e.g., TCP SYN flood), stress tests (e.g., sending a large number status requests in parallel) and incomplete protocol exchanges (e.g., not sending all of the printing instructions). All payloads were derived from the input network capture. Additionally, we checked if the application was vulnerable to a slowloris type attack [13] where minimal data are sent to the 3D printer just before the connection times out. All DoS conditions were verified by attempting to send new printing instructions to the 3D printer from a control PC and resulted in either the control PC not being able to connect to the 3D printer or the printing instructions not arriving at the 3D printer (despite the control PC application reporting the file was successfully transferred).

Our tool performs the following basic DoS attacks: SYN flood (using the hping tool [48]) and TCP connection exhaustion. For TCP connection exhaustion, we generate simultaneous TCP connections to the 3D printer and continue adding new connections until the 3D printer stops accepting them. Initially, no data are sent to identify if the 3D printer implements a timeout for inactivity. This is then repeated except with random data being periodically sent to stop a timeout from occurring.

The stress tests and incomplete protocol exchanges follow the same basic format as the TCP connection exhaustion tests where the number of simultaneous TCP sessions is increased until no additional connections can be established. For the stress test, a benign status request message from the input network capture is replayed by each TCP session. The data are initially replayed continuously to identify resource exhaustion when the 3D printer can no longer respond to the multiple requests. Next, we emulated a slowloris attack where each byte is sent just before the TCP timeout. For the incomplete protocol exchange, a portion of the printing instructions from the network capture is replayed simultaneously by each session. First, the replay stops to identify if the 3D printer application can be placed into a state where it will continuously wait for the protocol to complete. Next, after stopping the replay, random data are sent to check if the 3D printer checks the correctness of the input data.

Limitations: C3PO does not assess the security of a 3D printer's wireless networking capabilities or of the 3D printer's client application running on the control PC. Additionally, it does not provide a complete assessment of the 3D printer's application.

4.2 Findings

C3PO's individual 3D printer assessment tool was used to analyze 8 commercially available 3D printers. Vulnerabilities were identified in all 4 categories: data transfer, network services, 3D printer application, and availability.

[3]Other network captures could be used but would limit the tool's evaluation.
[4]As 95 of the 255 values are printable characters, this equates to 37.25%

4.2.1 Data transfer.

Observation 1: ***All 8 3D printers surveyed did not use authentication or encryption during data transfer (e.g., an attacker on the local network could impersonate the 3D printer and steal data).***

The input network capture was used to identify if authentication and/or encryption are used for transferring data to the 3D printer. Authentication was not used by any of the 3D printers analyzed, and it is unlikely any used encryption when transmitting data (reference Table 4). For those with a low percentage of printable packets received but a high percentage of sent packets (e.g., Machine C), we assumed this was caused by the protocol for specifying printing commands having a binary data format. These protocols can be vendor-specific, and not required to use printable characters. However, it is possible that the control PC is sending encrypted data, while the network communication is not encrypted.

Table 4: Findings on data transfer security.

Redacted Name	Used Auth	Used Encryp	% Printable (Sent / Recv)	Files Detected
Machine A	No	No	100% / 100%	G-code
Machine B	No	No	100% / 100%	G-code
Machine C	No	Possible	100% / 6%	PNG
Machine D	No	No	100% / 99%	Gzip
Machine E	No	No	99% / 100%	Gzip, JPEG
Machine F	No	Possible	89% / 11%	-
Machine G	No	No	100% / 100%	ASCII
Machine H	No	Possible	100% / 1%	-

None of the analyzed 3D printers used authentication. Some identifying information was included with the instructions sent to the 3D printer; however, these data could be changed by an attacker and was not always verified. For example, the data might include the sender's hostname, but the 3D printer application might not compare this value with the network data.

It is unlikely that any of the analyzed 3D printers used encryption, as the majority of all packets sent to a 3D printer had data payloads containing >85% printable characters after accounting for null byte padding and recognizable file formats (e.g., PNG to Machine C).

4.2.2 Network Services.

Observation 2: ***6 out of 8 3D printers surveyed had unnecessary network services exposed such as unused open ports and public IP addresses (e.g., an attacker could remotely control the 3D printer using an open telnet port [8]).***

Network services were identified by the Nmap tool [31]. Specifically, open network ports and any services they were running were identified. This was performed by scanning all possible TCP ports and the 100 most common UDP ports on the 3D printer. Additionally, we checked if the 3D printer was on a public or private IP address. Finally, the 3D printer's subnet mask was inferred. The majority of 3D printers surveyed had unused, open TCP ports and some had public IP addresses or wild card subnet masks accepting packets from any host IP address. A summary of our findings can be found in Table 5.

Table 5: Findings on network services.

Redacted Name	Open / Used Ports	IP address	Accessible from
Machine A	1 / 1	Private	Its subnet
Machine B	4 / 1	Private	Its subnet
Machine C	1 / 1	Private	Any IP
Machine D	3 / 2	Public	Any IP
Machine E	5 / 1	Private	Its subnet
Machine F	2 / 1	Private	Its subnet
Machine G	64,538 / 1	Private	Its subnet
Machine H	25 / 3	Private	Its subnet

While comparing the ports identified by Nmap to those used by the 3D printer during the network capture, we found that 6 out of 8 3D printers exposed more ports than were required, with some exposing more than 20 unused, open ports. Interestingly, we found that in general higher cost 3D printers had more unused, open ports. This is likely due to the increased complexity printing operations of the higher cost 3D printers and the smaller number of users identifying these vulnerable conditions.

In analyzing the 3D printers' accessibility on the network, the majority were configured to be on a private network and only accessible by other devices on the same subnet. However, one 3D printer was given a public IP address. This was not required for its operation. Using the Censys [2] and Shodan search engines [5], 49 additional 3D printers from the same manufacturer were found with publicly accessible IP addresses, allowing anyone on the internet to view the 3D printers' camera output.

Observation 3: ***3 out of 8 3D printers surveyed had network services vulnerable to known exploits, often from running out of date libraries (e.g., an attacker could utilize a published attack to gain root access on the 3D printer [33]).***

Multiple existing tools were used to perform vulnerability scans of the 3D printer's network services. These tools checked for susceptibility to Metasploit attack modules[30], Common Vulnerabilities and Exposures (CVEs) [21], and web server vulnerabilities [54]. Few known vulnerabilities were identified (reference Table 6), likely due to the limited number of network services on the 3D printers. Note, some scans were unable to run because the 3D printer limited the number of simultaneous TCP connections it would receive data from, causing the vulnerability scans to not make any progress.[5]

We observed a disconnect between software updates for a 3D printer's application software and the supporting libraries. On some machines, when the firmware was updated no supporting libraries were updated (e.g., no OS patches were applied). This left the 3D printer vulnerable to known/released exploits (e.g., WannaCry [34]). Additionally, we noted that all 3D printers running a Windows OS were vulnerable to known exploits that allowed a network attacker to execute arbitrary code.

Two 3D printers were found to be utilizing outdated libraries. One of the 3D printers was running a FTP server where the software

[5]The 3D printer would establish the connection but not send any replies to packets, causing the scanner to send scan packets and wait indefinitely.

Table 6: Network service vulnerabilities identified by scanning tools.

Redacted Name	Metasploit attacks	CVEs	Web server attacks	Old Libraries
Machine A	None	None	N/A	None
Machine B	None	3	None	FTP server
Machine C	None	None	N/A	None
Machine D	None	None	None	None
Machine E	Unable to run		N/A	None
Machine F	Unable to run		N/A	None
Machine G	2	None	N/A	None
Machine H	1	9	N/A	File server

was from a release that was >6 versions behind the current release (~4 years old). These outdated libraries had multiple CVEs allowing for attacks such as DoS and privilege escalation [3].

4.2.3 3D Printer Application.

Observation 4: ***3 out of 8 3D printers surveyed had insecure 3D printer applications, lacking input filtering and using insecure firmware updates (e.g., an attacker could send a malformed input and crash the 3D printer).***

Vulnerabilities in the 3D printer's application were identified using an open source mutational fuzzer [51]. The input network capture was input into the fuzzer to generate test inputs that followed the 3D printer's protocol message sequences. The 3D printer's physical UI and control PC client program were used to check the liveness of the 3D printer application. Additionally, if a firmware update was available, we analyzed it with the data transfer module. A summary of our findings are in Table 7.

Table 7: 3D printer application vulnerabilities identified.

ID	Crashing Inputs	Update Process	Update Analysis
A	✓	Only via USB	N/A
B	✓	Not analyzed*	N/A
C	✓	Pushed from control PC req. physical UI action	No encryption or authentication
D		Pulled from remote server req. physical UI action	No encryption or authentication
E		Pushed from control PC req. physical UI action	No encryption or authentication
F		Not analyzed*	N/A
G	Not tested†	Not analyzed*	N/A
H		Pushed from control PC	Weak encryption

† Not tested due to safety concerns.

* No firmware updates available during analysis window

While most 3D printer applications did not crash when given a fuzzed input, the 3 lower-cost machines all experienced a crash from malformed inputs. For example, one expected an HTTP PUT request of 'GETPRINTERINFO', while slightly modifying this request by adding garbage characters to the beginning (e.g., 'GRINTERINFINFOGETPRINTERINFO') caused the machine to crash. On one the physical UI remained operational, but the control PC client could no longer connect to the 3D printer. Additionally, for the 3D printers that accepted compressed files, we tested if sending a file that decompressed to be multiple GBs would cause the 3D printer application to crash [32]. None were found to be vulnerable to these decompression bombs.

We noted that there can be a significant delay in applying firmware updates (5 of 8 3D printers analyzed had out of data firmware installed). One 3D printer only had updates applied every 6 months, to align with its hardware calibration cycle. Multiple processes were employed for performing firmware updates. Most required an action on the 3D printer's physical UI (e.g., clicking 'yes' to install). Most did not employ a secure channel for transmitting updates to the 3D printer; however, at least one 3D printer downloads a digital signature for the firmware image, presumably for identifying invalid firmware images.

4.2.4 Availability.

Observation 5: ***All 8 3D printers surveyed were vulnerable to traditional denial of service attacks (e.g., an attacker can simultaneously transmit 1,000+ status requests, rendering the 3D printer unable to receive new printing instructions).***

The input network capture was used for generating messages that would be replayed in separate TCP connections simultaneous for identifying availability vulnerabilities. Specifically, we evaluated 4 situations: (1) SYN flood, (2) TCP connection flood, (3) replaying status request, and (4) partially replaying printing instructions.

Table 8: Findings on Denial of Service vulnerabilities.

ID	SYN flood	TCP flood	Replay Request	Partial data
A	●*	● Only allows 1 session		
B	●*	◐[340 sec]* 1,194 sessions	● 1,169 requests	○
C	○	● 998 sessions		●* 520 transfers
D	○	◐[40 sec] 4,000 sessions	● 576 requests	● 767 transfers
E	●	◐[2,760 sec] 33 sessions		
F	●	◐[2,760 sec] 33 sessions		
G	●*	●* Only allows 6 sessions		
H	○	○	◐[10 sec] 10 requests	● 10 transfers

○: No impact ◐: DoS for [x] seconds ●: Indefinite DoS

* 3D printer required power cycling after DoS attack

While some 3D printers were robust to simple DoS attacks, five 3D printers were unable to handle a SYN flood (with three needing a power cycle to restore operation). Additionally, most 3D printers were designed to handle multiple, simultaneous connections; however, each had a limit of <5,000 simultaneous connections with the majority only capable of supporting <35 simultaneous connections.

This was further complicated as multiple 3D printers either completely lacked timeout logic or had states that did not impose a timeout. On one 3D printer, this allowed an attacker to send <8 kB over any duration in order to create a DoS condition, while

another 3D printer would keep inactive connections alive instead of resetting them.

Multiple 3D printers exhibited a slowloris type vulnerability [13]. The 3D printers expected a certain size data input, and would wait for the input buffer to fill before processing the received network traffic, allowing for DoS conditions of >30 minutes by transmitting one byte per packet.

4.2.5 Summary. C3PO identified 28 specific security vulnerabilities on the eight 3D printers evaluated (our consolidated findings are given in Fig. 5 ordered by pervasiveness of the security issue). All lacked authentication and did not encrypt network traffic (though three may send already encrypted data). Six 3D printers had unused, open ports. Three were susceptible to known attacks. Another three had applications susceptible to malformed inputs. Finally, all surveyed 3D printers exhibited vulnerabilities to DoS attacks, resulting in the machines being unavailable until they were power cycled.

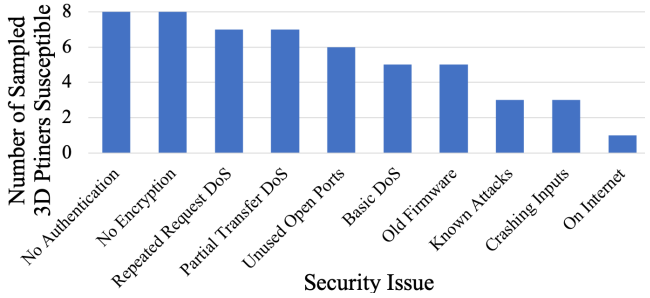


Figure 5: Summary of all findings, common security issues.

5 SYSTEM-WIDE SECURITY ANALYSIS

The network into which a 3D printer is deployed into has implications on its security. We aim to evaluate how an attacker can achieve their goals (§2.2), based upon a 3D printer's specific vulnerabilities[6] and a network blueprint obtained through a network scan. We want to automate this process to enable the evaluation to scale and ensure that potential attack paths are not skipped.

5.1 Tool

Manufacturing deployments will often isolate their 3D printers on a local intranet to protect them from attackers. However, a manufacturing deployment might add an internet connected camera on the 3D printer's subnet in order to remotely monitor the printing process, and thereby create the potential for a multistage attack from an attacker on the internet to the 3D printer via the camera. Our C3PO tool aims to identify these attack paths.

5.1.1 Tool Capabilities. Our tool systematically identifies all device interactions for a given network that lead to an attacker exploiting one of the 3D printer's specific vulnerabilities. This requires knowledge of the other devices on the network with access to the 3D printer. Additionally, the tool must know what device interactions can lead to an attacker achieving her goal.

[6]These could be identified by the first part of C3PO (§4) or from another source.

5.1.2 Limitations of Off-the-Shelf Tools. MulVAL is an attack graphing tool for identifying multi-host, multi-stage vulnerabilities [38]. It uses logical programming to determine if any set of input facts result in producing the specified attacker goal. Two key components limit our ability to directly apply MulVAL: (1) generating the inputs and (2) lack of models for attacks in the manufacturing domain.

5.1.3 Tool Design. We extended MulVAL by adding an input generation front-end and defining a set of models for attacks within the manufacturing domain. An overview of the tool is shown in Fig. 6, and the modules we extended are discussed below.

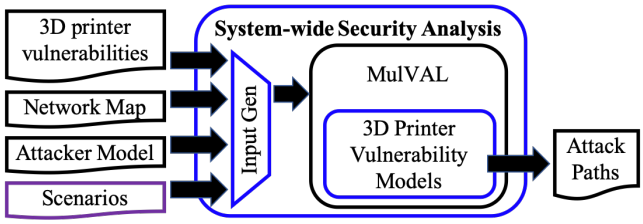


Figure 6: Overview of C3PO's system-wide security analysis tool.

Input Generation: C3PO uses 4 categories of input information: (1) 3D printer vulnerabilities, (2) network map, (3) attacker model, and (4) evaluation scenarios. 3D printer-specific vulnerabilities are either provided by C3PO's first stage (§4) or user input. The network map is collected by running a network scan (using Nmap [31]) on the 3D printer's subnet as well as the control PC's subnet to generate an estimate of all the devices with access to the 3D printer. The attacker model consists of the attacker goals (§2.2), the set of 3D printers to evaluate, and the attacker's starting location (i.e. same local network or a remote network).

With these basic inputs, MulVAL is able to identify if an attacker can achieve any of her attack goals on the 3D printer(s) being evaluated. However, a complete solution requires knowledge of all the vulnerabilities on every host. To improve C3PO's completeness, we added an additional input–scenario(s). These scenarios can be based upon common vulnerabilities for categories of devices (e.g., IIoT cameras having default credentials [8]). However, they can also be based upon data from vulnerability scans of specific devices on the network to increase the tool's fidelity. This enables performing "what-if" analysis for a given deployment (e.g., what attack paths exist if all IIoT cameras on the network have default credentials).

Manufacturing-Specific Interaction Rules: We extended the existing MulVAL interaction rules and incorporated additional manufacturing-specific rules in order to cover how an attacker could achieve her attack goals (§2.2). We extended the base MulVAL interaction rules to include sending defective parts, exfiltrating data, and creating a DoS condition.

5.2 Findings

We used part two of C3PO to identify possible attack paths an attacker could utilize in 3 real-world 3D printer deployments (shown in Fig. 3). These deployments included a small, research-focused additive manufacturing lab environment and a university makerspace.

For each deployment, the network devices were placed into 4 categories: (1) 3D printers, (2) PCs, (3) other devices (e.g., IIoT), and

Table 9: Network security evaluation scenarios.

Category	Scenario	Description
Baseline	0	No assumed vulnerabilities
PCs	1	Malicious USBs (e.g., [29])
	2	Malicious links (e.g., Phishing)
	3	Old OS (e.g., Win 95)
Network H/w	4	Exploitable firmware (e.g., [57])
Other devices (e.g., IIoT)	5	Default credentials (e.g., [8])
	6	Exploitable firmware
PCs & Network H/w	7	Scenario 1 & 4
	8	Scenario 2 & 4
	9	Scenario 3 & 4
Network H/w & other devices	10	Scenario 4 & 5
	11	Scenario 4 & 6
PCs & other devices	12	Scenario 1 & 5
	13	Scenario 1 & 6
	14	Scenario 2 & 5
	15	Scenario 2 & 6
	16	Scenario 3 & 5
	17	Scenario 3 & 6
All	18	Scenario 1, 2, 3, 4, 5 & 6

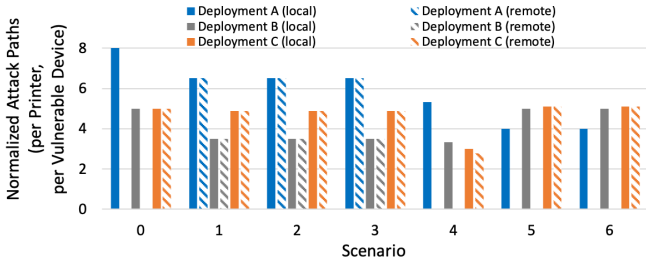
(4) network hardware. We ran a total of 19 simulated situations, where each scenario had a different assumed set of vulnerabilities (e.g., network hardware had a code execution vulnerability [57], other devices had default credentials [8], etc.). The complete list of scenarios can be found in Table 9. Each scenario was analyzed once with an attacker on the local network and again with an attacker on a remote network. The total number of attack paths for each goal was tallied for each scenario. The total number of attack paths for all attacker goals were normalized based upon the number of 3D printers and vulnerable devices on the network, which is shown in Fig. 7.

5.2.1 *3D Printer Deployment Analysis.*

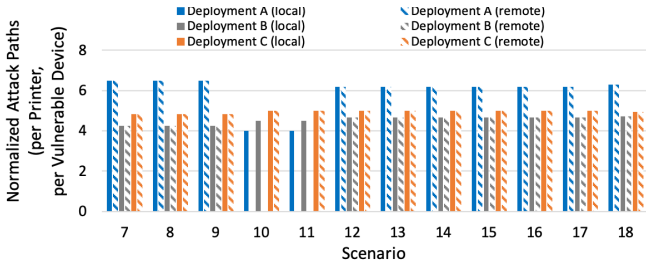
Observation 6: ***All 3 surveyed 3D printer network deployments were composed of >50% embedded devices (e.g., IIoT, paper printers, building automation, etc.). These devices often have weak security properties, creating the potential for many attack paths (e.g., in Deployment B, 66% of all possible attack paths included an embedded device).***

As the manufacturing domain seeks to increase the quantity of IIoT devices deployed [19], the appeal of these devices to attackers will increase. In each deployment we surveyed, the majority of devices were embedded devices (e.g., "other" devices). This led to the largest number of attack paths leveraging these devices. This is most notable in Deployment B, where > 66% of the theoretical attack paths identified leveraged one of these devices.

It is critical that these embedded devices be considered security threats, as networked cameras were used to launch DoS attacks [8]. Additionally, these devices are often employed inside the protected network perimeter, giving them easy access to critical machines such as 3D printers. For example, one subnet in Deployment C contained 120 devices, most of which were located in physically



(a) Vulnerabilities assumed in independent device categories.



(b) Vulnerabilities assumed in combinations of device categories.

Figure 7: Normalized number of attack paths identified for Deployment A, Deployment B, and Deployment C. Results are normalized per printer and per number of devices with assumed vulnerabilities.

separate spaces. This large number of connected devices created the potential for >800 attack paths per 3D printer.

5.2.2 *Critical Device Identification.*

Observation 7: ***2 out of 3 surveyed 3D printer network deployments had a device that bridged subnets. If this device had a vulnerability, it amplified the number of possible attack paths (e.g., in Deployment A, 54% of attack paths required the control PC be compromised).***

In Deployment A, the 3D printer appeared to be on an isolated network. However, the control PC bridged multiple networks, some of which eventually accessed the internet. Thus if a remote attacker could compromise this host (e.g., using a malicious link in an e-mail [10]), it would enable her to access the 3D printer as if she were on the local network. This can be observed in our simulation data where the total number of possible attack paths are equal between the local and remote attacker if the control PC is vulnerable. Conversely, in scenarios that assume the control PC was not vulnerable, there is a difference in the number of possible attack paths between a local and a remote attacker.

This analysis aids in identifying which devices are most critical to secure, as they are a part of the largest number of attack paths. Defenders can use this type of analysis to prioritize security efforts and resources to minimize the threats to a 3D printer.

5.2.3 *Ignored Devices.*

Observation 8: ***A compromised 3D printer could be used to launch attacks on other 3D printers in the network (e.g., a 3D***

printer compromised by an attacker could launch a DoS attack on other 3D printers on the network).

A 3D printer can also be a part of an attacker's multistage attack. Larger deployments often have multiples of the same type of 3D printer within a 3D printer cluster (e.g., Deployment C). If one of these 3D printers is compromised by an attacker (e.g., out of date firmware) it can be used for attacking other 3D printers in the cluster or potentially other 3D printers in different clusters. This is similar to how an IIoT device could be used by an attacker to launch attacks on 3D printers. While a situation such as this was not identified, combining different deployments could have created this situation. Thus, adding a new type of 3D printer could alter the threats posed to existing 3D printers in a manufacturing center.

5.2.4 Summary. C3PO demonstrated its ability to analyze real-world 3D printer deployments. All of the surveyed 3D printer network deployments were found to contain a majority of non-traditional IT devices (e.g., IIoT). C3PO was able to use theoretical attack scenarios to identify devices, which if compromised, result in the greatest increase in the number of possible attacks paths. Finally, we noted that potentially overlooked devices such as network switches and other 3D printers could be used by an attacker.

6 DISCUSSION AND RECOMMENDATIONS

Today's commercially available 3D printers expose a number of security vulnerabilities from not being designed with a defense in depth approach. Our C3PO tool highlighted 5 specific vulnerabilities, shown in Table 10.

Table 10: Identified vulnerabilities, their security implications, and our recommendations.

Vulnerability	In	Implication	Recommendation
No encryption or authentication	8 / 8	Steal data print defects	Place 3D printer on a VPN
Unused network services exposed	6 / 8	Increased attack surface	Drop traffic to unused services
Vulnerable to known exploits	3 / 8	Mod firmware, print defects	Implement patch in the network
Bad inputs crash application	3 / 8	Stop printing operations	Drop improperly formatted inputs
Vulnerable to trad. DoS attacks	8 / 8	Block access to 3D printer	Limit concurrent sessions

Manufacturing centers cannot adopt a single, fixed security solution, as they often need 3D printers from different vendors to support technologies (e.g., printing polymers vs. printing metals). Thus, manufacturing centers need a flexible defense that can be tailored to the specific needs of their specific 3D printers. Additionally, as manufacturing centers increasingly incorporate new connected devices (e.g., IIoT) the security risk of attackers using these devices as part of multistage attacks against critical assets (e.g., their 3D printers) increases. The increased productivity and efficiency of Industry 4.0 is predicated on incorporating these devices [23]; however, there is currently not a plan for securing these new, connected devices.

6.1 Proposed Defenses

We posit that the network can prevent a device's security vulnerabilities from being exploited. The network has a universal vantage point for all communications going to and from these connected devices. Defenses in the network can be deployed without modifying the connected device's operation. Additionally, network defenses do not require in-depth knowledge of vendor-specific protocols.

However, existing network defenses (e.g., firewalls) are often too coarse-grained and only deployed at the network perimeter. To combat these weaknesses, we propose a new network security paradigm that uses low-cost, software-defined security gateways to protect connected devices (similar to [26] for wireless IoT deployments). Each connected device's traffic is routed through a security gateway, which leverages advances in software-defined networking and network function virtualization to implement agile and specific security functions for that device (à la [66]).

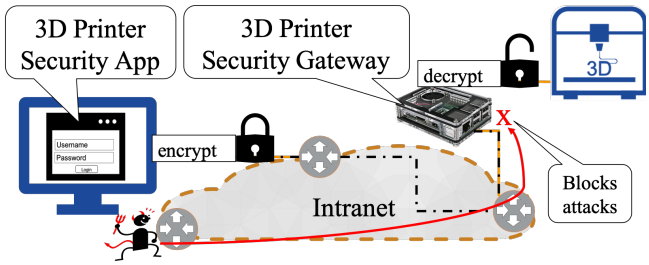


Figure 8: Conceptual overview of security gateway system for 3D printer security.

To counter the security vulnerabilities detected by C3PO, we envision the system architecture in Fig 8, where a security gateway is used in conjunction with a security app on the control PC.

- Encryption and authentication are provided by a VPN tunnel between the control PC app and the security gateway
- Unused network services are filtered by a firewall running on the security gateway
- Known exploits are patched in the network by the security gateway running an IPS which drops traffic matching known exploit signatures
- Malformed inputs are dropped by an input filter at the security gateway that only allows data payloads that match the 3D printer's expected protocol
- Traditional DoS attacks are mitigated by the security gateway limiting the number of simultaneous connections each host may have with a 3D printer

Thus, the use of security gateways could allow security to be "bolted-on" after the devices are deployed.

6.2 Future Work

The manufacturing domain is beginning to migrate towards manufacturing as a service, where a network of globally distributed 3D printers are used to have products printed at locations where 3D printers are idle or are closer to the delivery location. Companies have already deployed networks of 100+ 3D printer across multiple countries [27]. Additionally, cloud printing services are connecting low-cost 3D printers to a cloud service and controlled from the

internet [4]. The methodology of the C3PO tool could be used for analyzing these types of deployments.

7 RELATED WORK

Related work has been performed in the following areas: attacks on 3D printers, security assessments, and threat modelling.

7.1 3D Printer Attacks

Significant work has been done to qualitatively analyze possible attacks on 3D printers, with multiple attack taxonomies being created [40], [61], [63], [65]. Our work builds on these taxonomies and uses them to specify our attacker goals. An attack that these taxonomies mention, which our work identifies that has not been demonstrated in previous work, is the vulnerability of 3D printers to Denial of Service (DoS) attacks to make the printer unavailable.

Beyond these taxonomies, the preponderance of work looking at attacks on 3D printers has analyzed the production of defective parts from broad qualitative analysis [64] to specific attack demonstrations [10]. Proof of concept attacks include: injecting internal voids in the STL files on the control PC before print instructions are sent over the network [53], modifying the 3D printer's firmware [22], [36], manipulating the in-situ feedback on the 3D printer [50], changing the part's printing orientation on the control PC [67], and replacing good parts (saved on the control PC) with ones that will fail prematurely while passing a visual inspection [10]. These works are complimentary to ours as they highlight multiple strategies an attacker could employ for creating defective parts.

Data exfiltration from a network perspective was analyzed for 3D printers from a single vendor [18]. Our approach is similar, but our work analyzes 7 different vendors, identifies vulnerabilities beyond data exfiltration, and provides insight about the network deployment's impact on a 3D printer's security.

7.2 Security Assessments

Significant work has been done to assess the security of networked devices, looking at the manufacturing domain as well as other domains (e.g., office printers and IoT).

7.2.1 Manufacturing Domain. Within the manufacturing domain, numerous security assessments have been conducted. Some have focused on qualitative assessments to identify all possible security issues [17], [20], [42], [62]. Others conducted a user study evaluating if part deviations from a cyber attack would be noted [58].

Similar to our work, some of these assessments have utilized the security guidelines given in industry standards [60]; however, they have only looked qualitatively and not at specific devices. An experimental security analysis was performed on an industrial robot controller [44]; this work primarily focused on safety and was limited to a single manufacturer's device.

Orthogonal to our work, analysis has been performed on 3D printer firmware and related software applications that run on the control PC [35]. These tools could be used to identify additional vulnerabilities in 3D printers that our network analysis tool could use for identifying attack paths.

7.2.2 Other Networked Devices. Researchers have also investigated the security of other networked devices. Similar to our work, a number of office printers were evaluated in [37]; however, this work primarily leveraged a common language interpreted by most office printers.

Researchers have also investigated the security of IoT deployments, as IoT devices have gained notoriety for having security issues [15]. Most similar to our work was a survey of multiple IoT devices common to a home IoT deployment identifying common security issues [7]. This work differs from ours in only considering individual devices and not considering the system security for a deployment of devices.

7.3 System-wide Security Analysis

Prior researchers have investigated applying system-level security analysis for improving the overarching security posture and analysis. It was specifically applied to manufacturing in [12] to identify ways of increasing resiliency, and in [47] to identify the trust assumptions between sensors and actuators in cyber physical systems. The latter differs from ours in its application to a single machine (e.g., a car); while the former aims to increase a system's robustness to a failure.

Threat modelling was applied by the New York City Cyber Command that enabled the identification of new aspects that were never before considered [52]. This work differs from ours in that it primarily looked at the impact of applying the technique of threat modelling, and not on the security analysis of a specific deployment.

In an orthogonal effort, researchers have developed tools to emulate a complex deployment of cyber physical systems [9], allowing simulation of different deployments for evaluating different attacks and defenses.

8 CONCLUSIONS

Our C3PO tool allows for systematic security evaluations of networked devices and their deployments. We presented a use case example where we analyzed the security of 8 different 3D printers and 3 active manufacturing deployments where these machines were being used. We identified 28 vulnerabilities related to lack of encryption and authentication, unnecessary network services exposed, public IP addresses, unpatched known vulnerabilities, out of date libraries and firmware, crashing inputs, and multiple types of DoS. Next, we demonstrated how these vulnerabilities coupled with the 3D printer's network deployment could be used by a network attacker to launch a multistage attack in 19 simulated scenarios, identifying devices that are critical to the 3D printer's network security, the preponderance of non-traditional IT devices in these deployments, and the potential for 3D printers to be both targets and launch points for attacks. With the diversity and scale of networked devices in manufacturing deployments, we envision that the ideal way to secure these devices is to push security into the network.

REFERENCES

[1] 2019. C3PO. https://github.com/3DPrinter-Security/C3PO.
[2] 2019. Censys. https://censys.io. Accessed on 2019-02-25.
[3] 2019. CVE Details: The ultimate security vulnerability datasource. https://www.cvedetails.com/index.php. Accessed on 2019-02-27.
[4] 2019. Polar Cloud. https://polar3d.com. Accessed: 2019-05-06.
[5] 2019. Shodan. https://www.shodan.io. Accessed on 2019-02-13.

[6] 3Dnatives. 2019. Directory of 3D Printer Manufacturers. https://www.3dnatives.com/en/3d-printing-directory/categories/3d-printers-manufacturer. Accessed: 2019-05-09.

[7] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. 2018. SoK : Security Evaluation of Home-Based IoT Deployments.

[8] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[9] Daniele Antonioli and Nils Ole Tippenhauer. 2015. MiniCPS: A Toolkit for Security Research on CPS Networks. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC '15)*. ACM, New York, NY, USA, 91–100. https://doi.org/10.1145/2808705.2808715

[10] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. 2017. dr0wned – Cyber-Physical Attack with Additive Manufacturing. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. USENIX Association, Vancouver, BC. https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky

[11] Henry Canaday. 2018. Additive manufacturing could disrupt a lot of aerospace markets. http://aviationweek.com/optimizing-engines-through-lifecycle/additive-manufacturing-could-disrupt-lot-aerospace-markets. Accessed: 2018-11-19.

[12] Sutanay Choudhury, Luke Rodriguez, Darren Curtis, Kiri Oler, Peter Nordquist, Pin-Yu Chen, and Indrajit Ray. 2015. Action Recommendation for Cyber Resilience. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '15)*. ACM, New York, NY, USA, 3–8. https://doi.org/10.1145/2809826.2809837

[13] Cloudflare. 2019. What is a Slowloris DDoS Attack. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/. Accessed on 2019-02-10.

[14] Gerald Combs. 2019. Wireshark. https://www.wireshark.org. Accessed: 2019-05-03.

[15] Geremy Condra. 2015. A Plea for Incremental Work in IoT Security. In *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices (TrustED '15)*. ACM, New York, NY, USA, 39–39. https://doi.org/10.1145/2808414.2808424

[16] Lydia DePillis. 2019. GM is gone. Now come 3D printers and robots. https://www.cnn.com/2019/03/07/economy/future-of-manufacturing-youngstown/index.html. Accessed on 2019-03-07.

[17] Zach DeSmit, Ahmad E. Elhabashy, Lee J. Wells, and Jaime A. Camelio. 2016. Cyber-physical Vulnerability Assessment in Manufacturing Systems. *Procedia Manufacturing* 5 (2016), 1060 – 1074. https://doi.org/10.1016/j.promfg.2016.08.075 44th North American Manufacturing Research Conference, NAMRC 44, June 27-July 1, 2016, Blacksburg, Virginia, United States.

[18] Q. Do, B. Martini, and K. R. Choo. 2016. A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers. *IEEE Transactions on Information Forensics and Security* 11, 10 (Oct 2016), 2174–2186. https://doi.org/10.1109/TIFS.2016.2578285

[19] GE. 2019. GE Remanufacturing Facility Digitally Transforms Operations. https://www.ge.com/digital/video/ge-remanufacturing-facility-digitally-transforms-operations. Accessed: 2019-05-02.

[20] D. Glavach, J. LaSalle-DeSantis, and S. Zimmerman. 2017. *Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems*. Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9_7

[21] Greenbone Networks GmbH. 2019?. OpenVAS - Open Vulnerability Assessment System. http://openvas.org. Accessed: 2019-04-03.

[22] Xiao Zi Hang. 2013. Security Attack to 3D Printing. http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf Keynote at XCon2013.

[23] M. Hermann, T. Pentek, and B. Otto. 2016. Design Principles for Industrie 4.0 Scenarios. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*. 3928–3937. https://doi.org/10.1109/HICSS.2016.488

[24] IEC. 2018. IEC 62443: Network and system security for industrial-process measurement and control. https://www.isasecure.org/en-US/Documents/Authentication-Required-Specifications/EDSA-3-0-0/CSA-311-Functional-security-assessment-for-compone. Accessed: 2018-11-18.

[25] Ateeq Khan and Klaus Turowski. 2016. A Survey of Current Challenges in Manufacturing Industry and Preparation for Industry 4.0. In *Proceedings of the First International Scientific Conference Intelligent Information Technologies for Industry (IITI '16)*, Vol. 1. 15–26. https://doi.org/10.1007/978-3-319-33609-1_2

[26] Ronny Ko and James Mickens. 2018. DeadBolt: Securing IoT Deployments. In *Applied Networking Research Workshop*. Montreal, Quebec, Canada. https://mickens.seas.harvard.edu/files/mickens/files/deadbolt.pdf

[27] Bill Koenig. 2019. Jabil Establishes New 3D Printing Network. https://advancedmanufacturing.org/jabil-establishes-new-3d-printing-network/. Accessed: 2019-05-06.

[28] Lora Kolodny. 2018. Elon Musk emails employees about 'extensive and damaging sabotage' by employee. https://www.cnbc.com/2018/06/18/elon-musk-email-employee-conducted-extensive-and-damaging-sabotage.html. Accessed: 2019-04-12.

[29] David Kushner. 2013. The Real Story of Stuxnet. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed on 2019-02-13.

[30] Strategic Cyber LLC. 2019. Armitrage - Cyber Attack Management for Metasploit. http://www.fastandeasyhacking.com/index.html. Accessed: 2019-04-03.

[31] Gordon Lyon. 2018. Nmap. https://nmap.org. Accessed: 2018-11-19.

[32] Cara Marie. 2016. I Came to Drop Bombs: Auditing the Compression Algorithm Weapons Cache. https://bomb.codes. Accessed: 2019-05-14.

[33] Lee Mathews. 2018. Boeing is the latest wannacry ransomware victim. https://www.forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim/#9b1382d66344. Accessed: 2018-11-19.

[34] Microsoft. 2017. Microsoft Security Bulletin MS17-010 - Critical. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. Accessed: 2018-11-19.

[35] S. Moore, P. Armstrong, T. McDonald, and M. Yampolskiy. 2016. Vulnerability analysis of desktop 3D printer software. In *2016 Resilience Week (RWS)*. 46–51. https://doi.org/10.1109/RWEEK.2016.7573305

[36] Samuel Bennett Moore and William Bradley Glisson. 2016. Implications of Malicious 3 D Printer Firmware.

[37] J. MÃijller, V. Mladenov, J. Somorovsky, and J. Schwenk. 2017. SoK: Exploiting Network Printers. In *2017 IEEE Symposium on Security and Privacy (SP)*. 213–230. https://doi.org/10.1109/SP.2017.47

[38] Xinming Ou, Sudhakar Govindavajhala, and Andrew W. Appel. 2005. MulVAL: A Logic-based Network Security Analyzer. In *Proceedings of the 14th Conference on USENIX Security Symposium - Volume 14 (SSYM'05)*. USENIX Association, Berkeley, CA, USA, 8–8. http://dl.acm.org/citation.cfm?id=1251398.1251406

[39] OWASP. 2018. OWASP Internet of Things Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project. Accessed: 2018-11-18.

[40] Yao Pan, Jules White, Douglas C. Schmidt, Ahmad Elhabashy, Logan Sturm, Jaime A. Camelio, and Christopher Williams. 2017. Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems. *IJIMAI* 4 (2017), 45–54.

[41] Joshua Pereyda. 2017. boofuzz: Network Protocol Fuzzing for Humans. https://boofuzz.readthedocs.io/en/latest/. Accessed: 2019-05-08.

[42] Gregory Pope and Mark Yampolskiy. 2017. A Hazard Analysis Technique for Additive Manufacturing. *CoRR* abs/1706.00497 (2017). arXiv:1706.00497 http://arxiv.org/abs/1706.00497

[43] James Pozzi. 2019. Airbus Seeing Value of 3D Printed Parts. https://www.mro-network.com/maintenance-repair-overhaul/airbus-seeing-value-3d-printed-parts. Accessed: 2019-05-15.

[44] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero. 2017. An Experimental Security Analysis of an Industrial Robot Controller. In *2017 IEEE Symposium on Security and Privacy (SP)*. 268–286. https://doi.org/10.1109/SP.2017.20

[45] Rapid7. 2019. metasploit. urlhttps://www.metasploit.com. Accessed on 2019-02-10.

[46] IBM Research. 2018. IBM X-Force Threat Intelligence Index 2018. https://www.ibm.com/downloads/cas/MKJOL3DG. Accessed on 2019-03-21.

[47] Ivan Ruchkin, Ashwini Rao, Dionisio De Niz, Sagar Chaki, and David Garlan. 2015. Eliminating Inter-Domain Vulnerabilities in Cyber-Physical Systems: An Analysis Contracts Approach. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC '15)*. ACM, New York, NY, USA, 11–22. https://doi.org/10.1145/2808705.2808714

[48] Salvatore Sanfilippo. 2006. hping. http://www.hping.org. Accessed: 2019-05-10.

[49] Andrew Slaughter, Mark Yampolskiy, Manyalibo Matthews, Wayne E. King, Gabe Guss, and Yuval Elovici. 2017. How to Ensure Bad Quality in Metal Additive Manufacturing: In-Situ Infrared Thermography from the Security Perspective. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17)*. ACM, New York, NY, USA, Article 78, 10 pages. https://doi.org/10.1145/3098954.3107011

[50] Andrew Slaughter, Mark Yampolskiy, Manyalibo Matthews, Wayne E. King, Gabe Guss, and Yuval Elovici. 2017. How to Ensure Bad Quality in Metal Additive Manufacturing: In-Situ Infrared Thermography from the Security Perspective. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17)*. ACM, New York, NY, USA, Article 78, 10 pages. https://doi.org/10.1145/3098954.3107011

[51] James Spadaro and Lilith Wyatt. 2019. Mutiny Fuzzer. https://github.com/Cisco-Talos/mutiny-fuzzer. Accessed: 2019-05-03.

[52] Rock Stevens, Daniel Votipka, Elissa M. Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L. Mazurek. 2018. The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 621–637. https://www.usenix.org/conference/usenixsecurity18/presentation/stevens

[53] Logan D. Sturm, Christopher B. Williams, Jamie A. Camelio, Jules White, and Robert Parker. 2017. Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. *Journal of Manufacturing Systems* 44 (2017), 154 – 164. https://doi.org/10.1016/j.jmsy.2017.05.007

[54] Chris Sullo and David Lodge. 2019. Nikto2. https://cirt.net/Nikto2. Accessed: 2019-04-03.

[55] Tenable. 2019. Nessus. https://www.tenable.com/downloads/nessus. Accessed: 2019-05-03.

[56] Frederick M. Proctor Thomas R. Kramer and Elena Messina. 2000. *The NIST RS274NGC Interpreter - Version 3.* Technical Report NISTIR 6556. National Institute of Standards and Technology. https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=823374

[57] Liam Tung. 2018. Cisco critical flaw: At least 8.5 million switches open to attack, so patch now. https://www.zdnet.com/article/cisco-critical-flaw-at-least-8-5-million-switches-open-to-attack-so-patch-now/. Accessed on: 2019-02-07.

[58] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, and R. Parker. 2015. Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks? *IEEE Security Privacy* 13, 3 (May 2015), 40–47. https://doi.org/10.1109/MSP.2015.60

[59] Erin Vadala and Christen Graham. 2019. Downtime costs auto industry $22k/minute - survey. https://news.thomasnet.com/companystory/downtime-costs-auto-industry-22k-minute-survey-481017. Accessed on 2019-02-13.

[60] Yubo Wang, Oleg Anokhin, and Reiner Anderl. 2017. Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0. *Procedia CIRP* 63 (2017), 207 – 212. https://doi.org/10.1016/j.procir.2017.03.142 Manufacturing Systems 4.0 - Proceedings of the 50th CIRP Conference on Manufacturing Systems.

[61] Mingtao Wu and Young B. Moon. 2017. Taxonomy of Cross-Domain Attacks on CyberManufacturing System. *Procedia Computer Science* 114 (2017), 367 – 374. https://doi.org/10.1016/j.procs.2017.09.050 Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 - November 1, 2017, Chicago, Illinois, USA.

[62] Mark Yampolskiy, Todd R. Andel, J. Todd McDonald, William B. Glisson, and Alec Yasinsac. 2015. Towards Security of Additive Layer Manufacturing. arXiv:cs.CR/1602.07536

[63] Mark Yampolskiy, Wayne E. King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, and Yuval Elovici. 2018. Security of additive manufacturing: Attack taxonomy and survey. In *Additive Manufacturing*, Vol. 21. 431–457. https://doi.org/10.1016/j.addma.2018.03.015

[64] Mark Yampolskiy, Lena Schutzle, Uday Vaidya, and Alec Yasinsac. 2015. Security Challenges of Additive Manufacturing with Metals and Alloys. In *Critical Infrastructure Protection IX*, Mason Rice and Sujeet Shenoi (Eds.). Springer International Publishing, Cham, 169–183.

[65] Mark Yampolskiy, Anthony Skjellum, Michael Kretzschmar, Ruel A. Overfelt, Kenneth R. Sloan, and Alec Yasinsac. 2016. Using 3D printers as weapons. *International Journal of Critical Infrastructure Protection* 14 (2016), 58 – 71. https://doi.org/10.1016/j.ijcip.2015.12.004

[66] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV)*. ACM, New York, NY, USA, Article 5, 7 pages. https://doi.org/10.1145/2834050.2834095

[67] Steven Zeltmann, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. 2016. Manufacturing and Security Challenges in 3D Printing. *JOM* 68 (05 2016). https://doi.org/10.1007/s11837-016-1937-7

[68] Righard Zwienenberg. 2012. ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage. https://www.welivesecurity.com/2012/06/21/acadmedre-10000s-of-autocad-files-leaked-in-suspected-industrial-espionage/. Accessed on 2019-02-13.

A STANDARDS AND BEST PRACTICES

Table 11: Industry standards. IEC 62443-4-2 Foundational Requirements (FR) [24].

Category	Description
IEC FR 1	Identification and Authentication Control (e.g., Authentication)
IEC FR 2	Use Control (e.g., Remote session termination)
IEC FR 3	System Integrity (e.g., Protection from malicious code)
IEC FR 4	Data Confidentiality (e.g., Encryption)
IEC FR 5	Restricted Data Flow (e.g., Network segmentation)
IEC FR 6	Timely Response to Event (e.g., Audit logs)
IEC FR 7	Resource Availability (e.g., DoS Protection)

Table 12: Best practices. OWASP IoT Top 10 - 2018 [39].

Category	Description
OWASP #1	Weak, Guessable, or Hardcoded Passwords
OWASP #2	Insecure Network Services (e.g., Unneeded network services)
OWASP #3	Insecure Ecosystem Interfaces (e.g., No input filtering from mobile app)
OWASP #4	Lack of Secure Update Mechanism (e.g., Unencrypted in transit)
OWASP #5	Use of Insecure or Outdated Components (e.g., Use of deprecated software libraries)
OWASP #6	Insufficient Privacy Protection
OWASP #7	Insecure Data Transfer and Storage (e.g., Lack of encryption)
OWASP #8	Lack of Device Management
OWASP #9	Insecure Default Settings
OWASP #10	Lack of Physical Hardening

B 3D PRINTER EVALUATION DATA

Table 13: Compilation of all findings across all 3D printers analyzed.

	Data Transfer		Network Services			3D Printer Application			Availability					
Redacted Name	**Auth.**	**Encrypt.**	**Unused Open Ports**	**IP addr**	**Known Vulns.**	**Bad Input**	**Compr. Bomb**	**Update**	**SYN Flood**	**TCP Conn. Flood**	**Replay Request**	**Partial Transfer**	**Stop cmd**	**Total**
Machine A	None	None	0	Private	None	✓	N/A	N/A	Off-line	Only allows 1 connection			✓	8
Machine B	None	None	3	Private	3	✓	N/A	N/A	Off-line	Off-line for 340 seconds >1,194 conns	Off-line indefinitely >1,169 conns	No impact	✓	9
Machine C	None	Unlikely	0	Private	None	✓	No impact	No encryp No auth	No impact	Off-line indefinitely >998 connections		Off-line indefinitely >520 conns	No	7
Machine D	None	None	1	Public	None	None	No impact	No encryp No auth	No impact	Off-line for 40 seconds >4,000 conns	Off-line indefinitely >576 conns	Off-line indefinitely >767 conns	✓	9
Machine E	None	Unlikely	4	Private	Unable to run	None	N/A	No encryp No Auth	Off-line	Off-line after 33 connections			No	8
Machine F	None	Unlikely	1	Private	Unable to run	None	N/A	N/A	Off-line	Off-line after 33 connections			No	7
Machine G	None	None	64,537	Private	2	Not tested	N/A	N/A	Off-line	Only allows 6 simultaneous connections			No	8
Machine H	None	Unlikely	22	Private	9	None	N/A	Weak encryp	No impact	No impact	Off-line for 10 seconds >10 conns	Off-line indefinitely >10 conns	No	7
Total	8	8	6	1	3	3	0	4	5	7	8	7	3	63

Table 14: Details on all findings across 3D printer deployments analyzed.

Scenario	Deployment A						Deployment B						Deployment C				
	Data Exfil		Defects		DoS		Data Exfil		Defects		DoS		Data Exfil	Defects		DoS	
0	2	0	3	0	3	0	1	0	2	0	2	0	18	36		36	
1	3		5		5		1		3		3		1,404	2,862		2,862	
2	3		5		5		1		3		3		1,404	2,862		2,862	
3	3		5		5		1		3		3		1,404	2,862		2,862	
4	4	0	6	0	6	0	2	0	4	0	4	0	54	108	98	108	98
5	4	0	6	0	6	0	8	0	16	0	16	0	1,710	3,420		3,420	
6	4	0	6	0	6	0	8	0	16	0	16	0	1,710	3,420		3,420	
7	6		10		10		3		7		7		1,458	2,975	2,970	2,975	2,970
8	6		10		10		3		7		7		1,458	2,975	2,970	2,975	2,970
9	6		10		10		3		7		7		1,458	2,975	2,970	2,975	2,970
10	6	0	9	0	9	0	9	0	18	0	18	0	1,746	3,497	3,492	3,497	2,392
11	6	0	9	0	9	0	9	0	18	0	18	0	1,746	3,497	3,492	3,497	2,392
12	7		10		10		8		17		17		3,096	6,246		6,246	
13	7		10		10		8		17		17		3,096	6,246		6,246	
14	7		10		10		8		17		17		3,096	6,246		6,246	
15	7		10		10		8		17		17		3,096	6,246		6,246	
16	7		10		10		8		17		17		3,096	6,246		6,246	
17	7		10		10		8		17		17		3,096	6,246		6,246	
18	10		17		17		10		21		21		3,132	6,318	6,323	6,318	6,323