Security Analysis of Networked 3D Printers

Matthew McCormack*, Sanjay Chandrasekaran†, Guyue Liu*, Tianlong Yu*, Sandra DeVincent Wolf*, Vyas Sekar*
*Carnegie Mellon University
{mmccorm1, guyuel, tianlony, sdwolf, vsekar}@andrew.cmu.edu
†University of California, Santa Barbara
{sanjaychandrasekaran}@ucsb.edu

***Abstract*—Networked 3D printers are an emerging trend in manufacturing. However, many have poor security controls, allowing attackers to cause physical hazards, create defective safety-critical parts, steal proprietary data, and halt costly operations. Prior work has given limited attention to identifying if a network attacker is able to achieve these goals. In this work, we present C3PO, an open-source network security analysis tool that systematically identifies security threats to networked 3D printers. C3PO's design is guided by industry standards and best practices, identifying potential vulnerabilities in data transfer, the printing application, availability, and exposed network services. Furthermore, C3PO analyzes how a network deployment impacts a 3D printer's security, such as an attacker compromising an IoT camera in order to send malicious commands to a networked 3D printer. We use C3PO to analyze 13 networked 3D printers and 5 real-world manufacturing network deployments. We identified 8 types of network security vulnerabilities such as a susceptibility to low-rate denial of service attacks, the transmission of unencrypted data, and publicly accessible network deployments.**

	Attack Location		
Attacker Goal	CAD Files	3D Printer	**Network**
Physical hazard		Modify firmware [10]	Hazardous cmd combination
Print defect	Add void [3], [33]	Modify firmware [24], [30]	Modify files on-the-wire
Steal data	CAD stealing malware [44]	Side-channels [6], [31]	Spoof printer [9]
DoS			Printer unavailable

TABLE I: 3D printer attack landscape, characterized by attacker goal and location. The shaded cells are new contributions we make, demonstrating the attacks in red.

I. Introduction

Additive manufacturing (also referred to as 3D printing) is a key enabler of agile manufacturing [5], [11]. While there is a significant potential for impact (e.g., excitement surrounding the advent of a "Fourth Industrial Revolution" [11]), there are also significant security concerns [14], [17]. For example, malware on networked manufacturing machines stopped production at an airplane factory [19]. Cyber vulnerabilities in the manufacturing domain have high monetary costs, many escalating to over $1M in damages per incident [12].

Indeed, prior work on 3D printer attacks (illustrated in Table I) has demonstrated that an attacker can create defective parts by modifying the computer-aided design (CAD) files [3], [33] or the 3D printer's firmware [10], [30]. Additionally, networked 3D printers create new vectors for stealing data [44] and halting operations. Most attacks have either directly tampered with the CAD files on a PC or the 3D printer's firmware. However, as these deployments are increasingly interconnected, we should also be concerned about threats from *network attackers* (e.g., network connected hosts that can steal data, create denial of service, etc.).

Unfortunately, there are few if any tools for identifying if a 3D printer is susceptible to these types of attacks. Existing tools lack: (1) coverage of multiple categories of vulnerabilities (e.g., identify out-of-date services but not availability vulnerabilities), (2) support for multiple vendors/protocols, and (3) consideration of other devices on the network (i.e., the network deployment). These limitations highlight the need for a security analysis tool that can identify multiple potential vulnerabilities across 3D printer protocols while also analyzing the security impacts of the network deployment.

To this end, we designed and implemented an open-source security analysis tool, Connected 3D Printer Observer (C3PO) [4], to systematically identify potential security vulnerabilities on networked 3D printers guided by key recommendations from industry standards [13] and best practices [8], [27]. C3PO is composed of two parts:

- The first part identifies machine-specific vulnerabilities on standalone 3D printers (i.e., the printer in isolation).
- The second part demonstrates a practical application of attack graphing for identifying intermediate nodes (e.g., IoT cameras) that impact the security of a 3D printer.

We used C3PO to analyze 13 networked 3D printers, representing 9 vendors, across a spectrum of costs and printing processes (including polymer fused deposition modeling and steriolithography to metal selective laser sintering and binder jetting). Additionally, we used C3PO to analyze five real-world 3D printer network deployments, covering multiple network sizes and complexities. Each network deployment was analyzed with 19 scenarios, each assuming the presence of different vulnerabilities (e.g., default credentials on IoT cameras, PCs running Windows 95, etc.). Details of our complete findings can be found in our technical report [20].

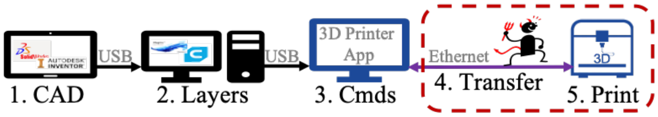

Fig. 1: A general 3D printing workflow. Our work focuses on analyzing the security inside the red dashed box.

Findings: Our key vulnerability findings are:

- *Standalone Networked 3D Printers:* All 13 networked 3D printers analyzed were vulnerable to simple DoS attacks (e.g., SYN flood [1]), some requiring a power-cycle to recover. Most (12 of 13) did not encrypt data in transit. 10 of 13 were easily spoofable (not authenticating themselves to users), and 3 executed commands without authenticating the sender. 4 of 13 allowed network inputs that crashed the machine. Finally, 4 of 13 were vulnerable to a published exploit (e.g., WannaCry [22]).
- *3D Printer Network Deployments:* 2 of 5 network deployments inadvertently placed 3D printers on publicly accessible networks. All deployments contained a significant proportion (>41%) of embedded devices (e.g., IoT cameras) that could potentially be used as launchpads for attacks.

Disclosure and Impact: We have disclosed our findings with all of the device vendors, and some have requested additional analysis of their new 3D printers to improve their product's security. Since our initial pilot studies, our tool has been requested by manufacturing center administrators and used to understand and improve their security posture.

II. Background and Motivation

We provide an overview of the 3D printing workflow and define our attacker goals. Additionally, we discuss prior work to motivate the need for a security analysis tool.

A. Background on 3D Printing Workflow

Additive manufacturing, often referred to as 3D printing, creates a physical object by sequentially joining layers of deposited material. This process enables fabricating structures that are not possible with traditional manufacturing methods [43]. The future of manufacturing relies on 3D printing as it reduces the cost of building complex parts, allows rapid design iteration, and enables on-demand production [5].

Workflow: The 3D printing workflow (shown in Fig. 1) consists of the following five steps (where the first three steps can be performed on the same host).

1) *Generate CAD representation.* Create a digital representation, often as a stereolithography file (STL).
2) *Convert to layers.* Divide vertically into layers.
3) *Convert to printing commands.* Generate machine-specific commands for each layer (e.g., G-code [35]).[1]
4) *Transfer commands.* Place commands in a file and send over the network to the 3D printer.
5) *3D Print.* Execute commands to create physical object.

The 3D printer deployments surveyed often had multiple networked 3D printers for each dedicated control PC. Additionally, the operating model for 3D printers differs from many IoT devices (e.g., [2]) in three ways: (1) 3D printers lack mobile apps,[2] (2) the majority of network traffic remains on the local network, and (3) all networked 3D printers exposed at least one listening TCP-based service.

B. Prior Work and Motivation

We group prior 3D printer attacks (e.g., [43]) based upon the attacker's goal and the attack vector (shown in Table I). We highlight three main attack vectors: (1) the CAD files, (2) the 3D printer, and (3) the network. Prior work has given limited attention to security risks arising from the network.

As such, most demonstrated attacks have ignored the network as an attack vector. Some modified STL files at the control PC before they were sent over the network (e.g., [3], [33]). Others assumed physical access to allow modifying the printer's firmware (e.g., [10], [30]). Network security analysis of 3D printers has been limited to a single vendor and only identified data transfer vulnerabilities–missing availability vulnerabilities [9]. Furthermore, most of the prior work does not identify multiple types of vulnerabilities and does not scale to multiple vendors/protocols. Moreover, the 3D printer's network deployments have been ignored, missing potential multistage attacks (e.g., those leveraging other devices on the network). We revisit prior work in §VI.

C. Attacker Model

Our work evaluates the security vulnerabilities related to connecting a 3D printer to a network (i.e., red box in Fig 1). We limit our attacker to only accessing the 3D printer over the network (i.e., no physical access). We do not consider attackers who are seeking to be stealthy or evade countermeasures. An attacker can start with network access (e.g., insider threat) or gain it by compromising a device on the network. For example, an attacker could gain access to a PC on the network through a phishing e-mail [3]. Based on prior work (e.g., [28], [41]–[43]), we envision an attacker with one of the following goals:

- **Causing physical hazards** [16]. An attacker could manipulate components (e.g., high-power lasers, high-temperature heaters, etc.) to cause a physical hazard (e.g., starting a fire).
- **Creating defective parts** [3]. A network attacker could intercept and modify printing commands, so that the printed part appears correct but will fail prematurely.
- **Stealing proprietary data** [44]. Often new printing tasks are sent to the first available machine. An attacker could advertise fake 3D printers in order to steal designs.
- **Halting printing operations** [15]. An attacker can overwhelm a networked 3D printer blocking its ability to receive new files from legitimate users, resulting in a loss of productivity that potentially costs thousands of dollars [36].

[1] G-code was used by 3 of the 13 networked 3D printers analyzed.

[2] Some vendors are beginning to release mobile apps for remote monitoring.

The combination of a 3D printer's vulnerabilities and its network deployment creates a multitude of possible attack paths for causing a physical hazard, creating defective parts, stealing data, or halting operations. C3PO, our security analysis tool, aims to be a generic tool for identifying a 3D printer's susceptibility to network attacks.

III. C3PO Tool Design

In this section, we present C3PO [4], an open-source security analysis tool for networked 3D printers and their deployments. We describe our tool's requirements, and present C3PO's design for achieving these requirements.

A. Tool Requirements

Network security analysis of 3D printers has been limited to manual analysis of a single vendor where only data transfer vulnerabilities were identified–missing availability vulnerabilities [9]. We are not aware of any 3D printer specific network analysis tools. While many generic network security tools exist, they do not identify multiple types of vulnerabilities or support multiple vendors/protocols. For example, existing IoT tools can only detect a small set of vulnerabilities (e.g., PENTOS [37] focuses on wireless security), and others are protocol specific (e.g., PRET [25] for PJL and PostScript). Moreover, the 3D printer's network deployments have been ignored, missing potential multistage attacks (e.g., those leveraging other devices on the network).

To address these limitations, we identified three requirements:

- **R1: Increased coverage of vulnerabilities.** The tool should cover multiple vulnerabilities as attacks often require combinations of vulnerabilities (e.g., an unauthenticated broadcast query and a lack of encryption allow an attacker to steal data by spoofing a printer).
- **R2: Protocol-agnostic.** The tool should support multiple vendors, including those using closed-source, proprietary protocols (e.g., more than just G-code).[3]
- **R3: Analyze network deployments.** The tool should consider how other devices in the network impact the security of a 3D printer.

B. C3PO Overview

At a high level, C3PO consists of two stages. First, the standalone 3D printer analysis stage identifies machine-specific vulnerabilities. Second, a network deployment analysis stage that uses attack graphing to identify potential multistage attack paths. We discuss the first stage and show how its results are fed into the second stage for analyzing network deployments.

1) Standalone 3D Printer Security Analysis: To provide coverage of vulnerabilities (R1), we ensure our tool identifies network security attributes in security standards [13] and best practices [8], [27]. After pruning categories that were not applicable to the manufacturing domain (e.g., privacy) or could not be evaluated with only network access (e.g., physical hardening), we grouped the resulting attributes into four categories: (1) data transfer, (2) printing application, (3) availability, and (4) exposed network services. These are mapped to four corresponding modules in C3PO's first stage as shown in Fig. 2. Each module takes a protocol-agnostic approach (R2) to identify potential vulnerabilities by using the input network traffic to infer protocol attributes.

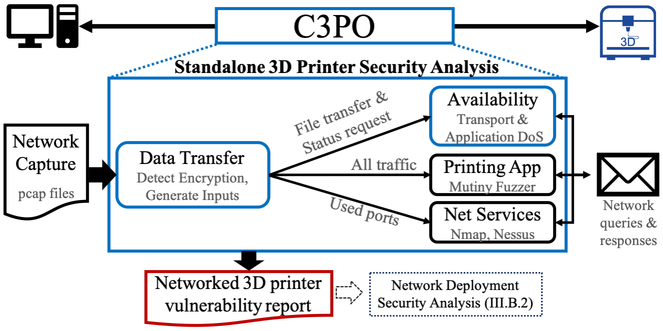

Fig. 2: C3PO's standalone networked 3D printer vulnerability analysis tool. Blue boxes represent our additions.

C3PO takes in a network capture (e.g., pcap file). We assume no prior knowledge (e.g., protocol format, printer vendor) about the capture. The network capture is analyzed by the *Data Transfer* module which determines whether encryption is used and generates a specific input to each of the following modules, as denoted in Fig. 2. Possible printing commands (e.g., file transfer, status requests) are sent to the *Availability* module, which replicates these commands to test both network and application layer availability limitations. The *Printing Application* module takes the entire network capture and feeds it into Cisco's Mutiny fuzzer [32] to create potentially malicious inputs for the printing application. The *Network Services* module uses Nmap [18] to scan for exposed network services and Nessus [34] to identify known vulnerabilities on exposed network services. A list of ports used in the network capture is used to identify potentially unused network services. Finally, C3PO collects the results from each module in order to generate a vulnerability report for the 3D printer under test. Next, we briefly discuss key modules.

Data Transfer: As many networked 3D printers use a closed-source, proprietary format to encode their printing commands, it is challenging to differentiate encryption from packed binary data. To overcome this challenge, we leverage prior work (e.g., ent and [38]) to determine if the data are encrypted based upon the results of three per-packet tests: (1) entropy of >6.75 bits per byte, (2) chi-squared test for a uniform distribution has a p-value >0.01, and (3) serial correlation coefficient is <0.3. We discard packets with identifiable file headers (e.g., Gzip, JPEG, etc.). If the majority of packets exchanged in both directions pass these tests we assume an encrypted channel is used.

Availability: Analyze DoS conditions at two network layers.

- Transport layer: Analyzes the underlying network layer capabilities of the 3D printer. We test with a SYN flood (using hping) and TCP connection exhaustion (e.g., maximum simultaneous TCP sessions).

[3] In our survey, 5 of 9 vendors used distinct proprietary protocols.

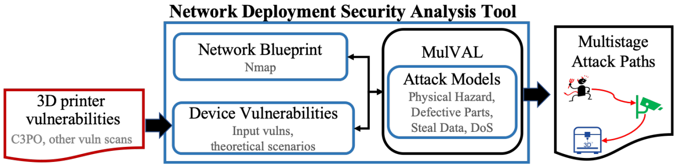
Network Deployment Security Analysis Tool
3D printer vulnerabilities
C3PO, other vuln scans
Network Blueprint
Nmap
Device Vulnerabilities
Input vulns, theoretical scenarios
MulVAL
Attack Models
Physical Hazard, Defective Parts, Steal Data, DoS
Multistage Attack Paths
3D

Fig. 3: C3PO's network deployment analysis tool, extending prior attack graphing tools.

TABLE II: Networked 3D printers evaluated.

	3D Printer	Cost (US$)	Released	Material	Protocol
Desktop	Machine A	300	2015	Polymer	G-code
	Machine B	1,400	2019	Polymer	G-code
	Machine C	1,500	2014	Polymer	proprietary
	Machine D	2,850	2015	Polymer	proprietary
	Machine E	4,200	2016	Polymer	G-code
Industrial	Machine F*	17,000	2017	Polymer	proprietary
	Machine G*	18,900	2008	Polymer	proprietary
	Machine H*	31,900	2007	Polymer	proprietary
	Machine I	50,000	2007	Polymer	STL
	Machine J	150,000	2016	Metal	proprietary
	Machine K†	600,000	2010	Metal	proprietary
	Machine L*	750,000	2011	Polymer	proprietary
	Machine M†	~1,000,000	2014	Metal	proprietary

*: Same vendor, different models $\quad$ †: Same vendor, different models

- Application layer: Use the input network capture to generate protocol-compliant inputs. We perform a stress test (e.g., sending multiple, concurrent status requests) and partial data exchange (e.g., only sending the first 100 bytes of a file, while keeping the connection open).

We assumed repeated messages to be status requests and replayed them to test the printing applications ability to handle multiple concurrent requests. Similarly, we assumed that the file to be printed was in the stream sending the largest amount of data to the 3D printer. The first 100 bytes of this were replayed while the connection was kept open to identify DoS conditions when only part of the file was transmitted.

2) Network Deployment Security Analysis: Identifying a 3D printer's vulnerabilities is the first step, but it does not convey the complete security picture. Other devices (e.g., IoT cameras, sensors, etc.) in the manufacturing network could be used to launch attacks against networked 3D printers. C3PO's network deployment analysis addresses this by identifying possible network attack paths (R3). Two inputs are required: (1) a list of devices with a network connection to the 3D printer(s) and (2) each device's vulnerabilities. However, this is challenging due to complex network deployments, with a diversity of devices, and a lack of domain specific attack models. To address these challenges, our network deployment component includes the modules shown in Fig. 3.

C3PO's *Network Blueprint* module creates a network topology for all the devices one hop from the 3D printer using Nmap. The *Device Vulnerability* module maps vulnerabilities to each device in the network topology. The networked 3D printer's vulnerabilities are provided by C3PO's standalone 3D printer analysis. For other devices, either known vulnerabilities (e.g., from a vulnerability scan) or theoretical vulnerabilities from test scenarios can be applied. These test scenarios can come from known common vulnerabilities (e.g., IoT cameras having default credentials) or from operator experiences (e.g., use of personal USB drives or lack of software updates). The outputs from the previous two modules as well as the set of networked 3D printers to evaluate, the attacker goals, and the attacker's starting location (i.e., local or remote network) are fed into the MulVAL attack graphing tool [26].

We extended MulVAL with our *Attack Models* module which maps vulnerabilities to 3D printer specific attacks by defining the necessary preconditions for an attack to succeed. For example, to identify attack paths that allow an attacker to halt printing operations the attacker must be able to send messages from a device with network access to a 3D printer which does not require authentication prior to executing commands received over the network. The output attack graph can be used to identify network devices that impact the security of a networked 3D printer.

IV. 3D Printer Evaluations

In this section, we present C3PO's findings on 13 networked 3D printers, identifying a total of 8 types of vulnerabilities.

A. 3D Printers Evaluated

The 13 networked 3D printers evaluated ranged from low-cost desktop polymer machines to $1M+ industrial metal 3D printers as shown in Table II. We selected desktop machines that were among the top 10 sold on Amazon and industrial models from the top vendors by sales.

B. Key Findings on Standalone 3D Printers

We highlight key findings from our analysis of 13 networked 3D printers below. These findings have been reported to the vendors who are currently working on updates. Our complete findings can be found in [20].

Observation 1: ***Network 3D printers are susceptible to simple and low-rate DoS attacks (e.g., SYN flood).***

Availability is an area that prior work has not explored for networked 3D printers. DoS attacks were possible at both the network and application layers on all surveyed 3D printers.

Limited simultaneous TCP connections: Most networked 3D printers (10 of 13) assumed a small number of concurrent clients (~20), allowing an attacker to easily create a temporary DoS condition. In general, the industrial printers were easier to adversely affect via DoS, requiring <100 simultaneous connections. Making this worse, five (two desktop, three industrial) of the 10 vulnerable networked 3D printers did not implement a timeout for inactive TCP connections, allowing the attack to persist without continuous network traffic.

Slowloris: Three industrial 3D printers exhibited susceptibility to a Slowloris-type attack [7]. These machines accepted data transferred one byte per packet (with a five second timeout between bytes), and would not process the data until a complete protocol message was received (a minimum of 64 bytes). Parallel status requests could be used to DoS the printer for up to 45 minutes, sending ~290bps per connection.

Partial Data Transfer: Three (two desktop, one industrial) networked 3D printers were vulnerable to incomplete file transfers. These machines disabled their TCP timeout when receiving a file, rendering the 3D printer unavailable as long as the attacker's TCP connections remained established (without requiring any data be sent). Furthermore, one of the desktop machines required a power-cycle to recover from this attack, as the DoS continued after the TCP connections were closed.

SYN Flood: Two (one desktop, one industrial) networked 3D printers required a power-cycle to recover from a SYN flood.

Observation 2: ***Most networked 3D printers do not provide confidentiality for data in transit (exposing proprietary data).***

None of the networked 3D printers encrypted data both to and from the 3D printer. Most had low entropy ($<$5.48 bits per byte) and a high serial correlation ($>$0.38) in at least one direction. Additionally, only two had a majority of their packets pass a chi-squared test for a uniform distribution, which encrypted data should pass. Based upon these results, only two may be encrypting files prior to sending them over a plaintext channel, potentially allowing an attacker to view file meta-data (e.g., filenames, length, etc.).

To put this in context, we also ran C3PO on 11 home IoT devices (e.g., Amazon Alexa, D-Link camera, etc.), and six out of 11 utilized encryption when transferring data (e.g., TLS). This suggests networked 3D printers are behind the state-of-the-art for encrypting data in transit. This is particularly surprising for industrial 3D printers, as it risks high-cost, proprietary data being stolen.

Observation 3: ***Most networked 3D printers do not authenticate themselves to users (vulnerable to spoofing).***

Only one PC application surveyed authenticated the networked 3D printer identified by its broadcast query (e.g., mDNS, LLMNR, SSDP, etc.) before sending printing commands. At a minimum, these protocols provide the PC with the hostname and IP address for each networked 3D printer; some additionally include details such as firmware version or printing material. In the event of multiple replies for the same networked 3D printer, the PC only utilizes the first reply it receives. Thus, an attacker can impersonate a networked 3D printer by replying to the PC's broadcast query before the networked 3D printer. The attacker then only needs a listening TCP socket to spoof the 3D printer and receive printing commands from the PC.

Observation 4: ***3 out of 13 networked 3D printers execute unauthenticated commands received over the network.***

Three desktop 3D printers allowed an unauthenticated user to issue start/stop commands. An attacker can use this ability to delay a part's production. Furthermore, one desktop 3D printer executed actuator commands (G-code) sent over the network without either authenticating the sender or checking if a file was midway through printing. The printer performed the malicious commands (e.g., increase heater temperature, drive print nozzle into part, etc.) at its current location in a print file (potentially creating defects, shown in Fig. 4).

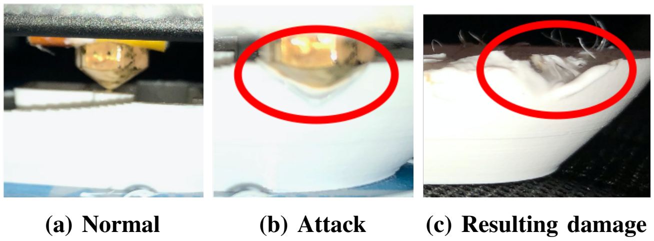
(a) Normal (b) Attack (c) Resulting damage

Fig. 4: Executing unauthenticated actuator commands while printing allows an attacker to create defects.

Observation 5: ***4 of 13 networked 3D printers lacked input filtering (e.g., a malformed input crashed the firmware).***

Three desktop and one industrial machine crashed from malformed inputs. Similar to well-known injection attacks against web servers, slightly modifying a PUT request by adding garbage characters caused one 3D printer's firmware to crash. Once the firmware crashes, the current printing operations are halted and cannot be recovered upon reboot, requiring that the task be restarted from the beginning (potentially wasting hours of printing operations). In a related manner, while most machines generated unique filenames at the 3D printer; one industrial 3D printer used the client provided filename. Filename collisions caused the firmware to crash (persisting across reboots). The machine could only be recovered by starting it in a "safe-mode" (where the 3D printer application is not started) and the file deleted.

Observation 6: ***4 of 13 networked 3D printers had unused network services vulnerable to known exploits (e.g., [22]).***

Six out of 13 networked 3D printers exposed more network services than were utilized during normal operations, with some exposing up to 10 unused services. A number of these exposed network services were running outdated libraries, as we observed a disconnect between software updates for a 3D printer's application and the supporting libraries (e.g., no OS patches applied). For example, one 3D printer was running a FTP server with software that was ~4 years old. These out-of-date libraries resulted in four networked 3D printers being susceptible to known/released exploits (e.g., WannaCry [22]).

C. Summary

In summary, C3PO identified 8 types of vulnerabilities across the 13 networked 3D printers evaluated, representing both desktop and industrial machines. Additional details and discussion on all of our findings can be found in [20]. All networked 3D printers were vulnerable to DoS attacks (basic, slowloris, partial file transfer), some remaining unavailable until they were power-cycled. Twelve did not encrypt network traffic (though two may send already encrypted data). Ten

TABLE III: Attacks demonstrated on networked 3D printers, illustrating a range of attacker goals.

		Attack			
	3D Printer	Hazard	Modify print	Crash app	DoS
Desktop	Machine A	✓		✓	✓
	Machine B		✓	✓	✓
	Machine C		✓	✓	✓
	Machine D		✓		✓
	Machine E		✓		✓
Industrial	Machine F		✓		✓
	Machine G		✓		✓
	Machine H		✓		✓
	Machine I		✓		✓
	Machine J				✓
	Machine K				✓
	Machine L		✓		✓
	Machine M		✓	✓	✓

utilized broadcast protocols (e.g., mDNS, SSDP, LLMNR) without authentication which allow an attacker to spoof a networked 3D printer and create a man in the middle situation between a PC and the 3D printer. Further, three executed unauthenticated commands received over the network. Four had applications that were susceptible to malformed inputs, requiring a power-cycle to recover. Finally, four were vulnerable to published exploits. Combinations of these vulnerabilities allowed the attacks in Table III.

In analyzing our findings, we noted a couple of trends. As the cost of a networked 3D printer increased, there was no significant reduction in the number of identified vulnerabilities. A part of this is likely due to pervasive issues such as lack of encryption and susceptibility to DoS. The higher-cost industrial machines were more likely to run additional services vulnerable to published exploits, while desktop machines were more likely to crash from a malformed input. The year a networked 3D printer model was released did not impact the number of vulnerabilities identified. Even recently released machines (e.g., 2019) did not follow known best practices. This creates significant security risks as these machines have lifespans of 10+ years (potentially never being patched). We next identify how the network deployment allows an attacker to exploit these vulnerabilities.

V. Network Deployment Evaluations

We evaluated five real-world 3D printer network deployments to better understand how different deployments affect the security of networked 3D printers.

A. 3D Printer Deployments Evaluated

The five real-world 3D printer network deployments ranged from small deployments with a single networked 3D printer (e.g., a small, lab environment) to large makerspaces with four types of networked 3D printers placed on multiple subnets with over 100 networked devices.

For each network deployment, the devices identified during the network scan were placed into four categories based upon their MAC address: (1) networked 3D printers, (2) PCs, (3) other devices (e.g., IoT), and (4) network hardware. Other devices accounted for at least 41% of all the devices on each network deployment.

We analyzed 19 scenarios, where each scenario had a different set of assumed vulnerabilities (e.g., devices with remote code execution, or PCs compromised by phishing). These scenarios were generated from prior attacks (e.g., Stuxnet) and discussions with operators (e.g., legacy systems on the network). The complete list of scenarios can be found in [20]. Each scenario was analyzed for both a local attacker (e.g., an insider threat) and a remote attacker (i.e., starting on a public network). On average, C3PO identified 5 multistage attack paths to each networked 3D printer per insecure device.

B. Key Findings from Network Deployments

Across all network deployments, we noted a lack of network isolation, with a large number of unnecessary devices (e.g., office PCs) on the 3D printer's network.

Observation 7: ***Multiple surveyed network deployments made 3D printers easily accessible to a network attacker (e.g., placing 3D printers on the public internet).***

Most networked 3D printers were configured to be on a private network and only accessible by other devices on the same subnet. However, one network deployment gave 3D printers public IP addresses, which were not required for operation. A search using the Censys and Shodan search engines identified 49 additional 3D printers configured with public IP addresses, potentially allowing anyone on the Internet to remotely stop 3D printing jobs. Similarly, other researchers found over 3,700 publicly accessible hosts running a popular web interface for 3D printers in 2018 [21]. Many were configured to not require authentication prior to executing printing commands or accessing its camera.

The surveyed 3D printer network deployments contained a majority of non-traditional IT devices (e.g., IoT). C3PO ran theoretical attack scenarios to identify which device categories (e.g., PCs, network hardware), if compromised, resulted in the greatest number of possible attack paths. We grouped the total number of attack paths a remote attacker could perform based upon the vulnerabilities assumed for each device category (depicted in Fig. 5). We normalized the data for the number of networked 3D printers in the deployment as well as the number of devices with assumed vulnerabilities to allow for comparison between networks of different sizes. We note that two of the deployments isolated the networked 3D printers behind a PC, in a Purdue enterprise reference architecture [40]. In these deployments the network security of the 3D printer is based upon this PC, which in some deployments was Internet-connected and managed by the manufacturing technicians (as opposed to the institution's IT department).

Summary: The deployment with the best network isolation was contingent on an internet-connected PC remaining secure. In the larger, operational deployments we noted a plethora of unnecessary devices on the 3D printer's network (e.g., office PCs, conference room equipment, etc.). Additionally, we noted the presence of legacy devices that were not intended for network operations (e.g., machines running Windows 95 with

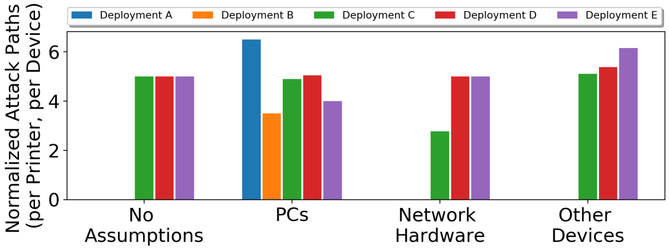

Fig. 5: Normalized number of attack paths for vulnerabilities assumed within a single device category.

added USB-WiFi adapters to connect them to the network). These risks were further elevated when these networks were connected to publicly accessible networks. Thus, having a tool such as C3PO can help inform manufacturing center operators about risks from their network deployments.

VI. Related Work

We discuss two categories of related work: 3D printer attacks and security assessments of networked devices.

A. 3D Printer Attacks

Prior works on 3D printer attacks have largely ignored network-based attacks. Most have analyzed creating defects or stealing data by either attacking the PC where the files are stored or modifying the 3D printer's firmware, such as researchers using static analysis on a sampling of 3D printers' firmware and PC applications [23].

Creating defects: 3D printed parts are susceptible to an attacker injecting undetectable voids in the part, changing its mechanical properties and causing it to fail prematurely [3], [33]. Similarly, an attacker that modifies the 3D printer's firmware can cause defective parts to be printed [10], [24], [30]. These works are complementary to ours as they highlight the potential for an attacker to create defective parts. However, none of these prior works leveraged the network.

Stealing Data: ARP spoofing was used to steal data from a single vendor's networked 3D printer [9]. The work was limited to a specific vendor's protocol and only discussed stealing data over the network. While our approach similarly relies on analysis of the network protocol, we propose a protocol-agnostic tool for identifying multiple security vulnerabilities.

B. Security Assessments

Others have looked at assessing the security of networked devices, in manufacturing as well as other domains (e.g., IoT).

Manufacturing Domain: Within the manufacturing domain, qualitative assessments have been guided by industry standards [39]; however, they did not analyze networked 3D printers. Others performed a detailed analysis of the security risks to an industrial robot controller impacting human safety [29].

Other Networked Devices: Researchers have also investigated the security of other networked devices. Similar to our work, a tool was developed for analyzing office printers [25]. However, this work leveraged common languages interpreted by most office printers (i.e., PJL and PostScript). Networked 3D printers do not currently share a common language, requiring a different security analysis tool. Researchers have also investigated the security of IoT, as IoT devices have gained notoriety for having security issues. Most similar to our work was a survey of multiple commodity IoT devices, identifying common security issues using an amalgamation of existing network security tools [2]. However, most IoT devices have mobile apps and cloud servers, which are rare for 3D printers.

VII. Conclusions

Our C3PO security analysis tool allows for the systematic security evaluation of networked 3D printers and their network deployments. We analyzed the security of 13 networked 3D printers and 5 active manufacturing network deployments. We identified 8 types of vulnerabilities related to multiple types of DoS, lack of encryption and authentication, susceptibility to being spoofed, crashing inputs, and unpatched known vulnerabilities. Next, we demonstrated a practical application of attack graphing for identifying potential multistage attack paths in 3D printer network deployments. Analyzing 19 simulated scenarios, we identified 3D printers on public networks, the preponderance of embedded devices in these network 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 networks, we envision that the ideal way to secure these devices is to push security into the network.

Acknowledgment

This work was supported in part by NSF award CNS-1564009. This work was also supported in part by the CONIX Research Center, one of six centers in JUMP, a Semiconductor Research Corporation (SRC) program sponsored by DARPA. This research was also supported by the Carnegie Mellon University (CMU) Manufacturing Futures Initiative, made possible by the Richard King Mellon Foundation. The authors would like to thank the CMU NextManufacturing Center and Todd Baer in particular for support and technical expertise. Additionally, we would like to thank the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense, for support and guidance.

References

[1] 21 ca-1996-21: Tcp syn flooding and ip spoofing attacks. https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf#page=123, 2000.

[2] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. Sok: Security evaluation of home-based iot deployments. In *2019 2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019.

[3] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici. dr0wned – cyber-physical attack with additive manufacturing. In *11th USENIX Workshop on Offensive Technology (WOOT 17)*. USENIX, 2017.

[4] C3po. https://github.com/3DPrinter-Security/C3PO, 2019.

[5] T. CAMPBELL, C. WILLIAMS, O. IVANOVA, and B. GARRETT. Could 3d printing change the world? atlanticcouncil.org/images/files/publication_pdfs/403/101711_ACUS_3DPrinting.PDF, 2011.

[6] S. R. Chhetri, S. Faezi, and M. A. A. Faruque. Fix the leak! an information leakage aware secured cyber-physical manufacturing system. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, 2017.

[7] Cloudflare. What is a slowloris ddos attack. cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/, 2019.

[8] J. Day, R. Shepherd, P. Kearney, and R. Storer. Secure design best practices guidelines. iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf, 2018.

[9] Q. Do, B. Martini, and K. R. Choo. A data exfiltration and remote exploitation attack on consumer 3d printers. *IEEE Transactions on Information Forensics and Security*, 2016.

[10] X. Z. Hang. Security attack to 3d printing. XCon Keynote 13.

[11] M. Hermann, T. Pentek, and B. Otto. Design principles for industrie 4.0 scenarios. In *HICSS*, 2016.

[12] T. Huelsman, E. Powers, S. Peasley, and R. Robinson. Cyber risk in advanced manufacturing. deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing, 2016.

[13] IEC. Iec 62443: Network and system security for industrial-process measurement and control. isasecure.org/en-US/Documents/Authentication-Required-Specifications/EDSA-3-0-0/CSA-311-Functional-security-assessment-for-compone, 2018.

[14] A. Khan and K. Turowski. A survey of current challenges in manufacturing industry and preparation for industry 4.0. In *IITI*, 2016.

[15] E. Kovacs. Flaw exposes mitsubishi plcs to remote dos attacks. securityweek.com/flaw-exposes-mitsubishi-plcs-remote-dos-attacks.

[16] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9(3):49–51, May 2011.

[17] J. Lorincz. Cyber secure manufacturing is smart manufacturing. advancedmanufacturing.org/cyber-secure-smart-manufacturing/, 2018.

[18] G. Lyon. Nmap. https://nmap.org, 2018. Accessed: 2018-11-19.

[19] L. Mathews. Boeing is the latest wannacry ransomware victim. forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim, 2018.

[20] M. McCormack, S. Chandrasekaran, G. Liu, T. Yu, S. D. Wolf, and V. Sekar. C3po: A security analysis tool for networked 3d printers. Technical report, CMU-CyLab, 2020. https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab20001.pdf.

[21] X. Mertens. 3d printers in the wild, what can go wrong? isc.sans.edu/forums/diary/3D+Printers+in+The+Wild+What+Can+Go+Wrong/24044/, 2018.

[22] Microsoft. Microsoft security bulletin ms17-010 - critical. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010, 2017. Accessed: 2018-11-19.

[23] S. Moore, P. Armstrong, T. McDonald, and M. Yampolskiy. Vulnerability analysis of desktop 3d printer software. In *2016 Resilience Week (RWS)*, 2016.

[24] S. B. Moore and W. B. Glisson. Implications of malicious 3 d printer firmware. In *Hawaii International Conference on System Sciences*, 2016.

[25] J. Müller, V. Mladenov, J. Somorovsky, and J. Schwenk. Sok: Exploiting network printers. In *2017 IEEE Symposium on Security and Privacy (SP)*.

[26] X. Ou, S. Govindavajhala, and A. W. Appel. Mulval: A logic-based network security analyzer. In *Proceedings of the 14th Conference on USENIX Security Symposium - Volume 14*, SSYM'05, pages 8–8, Berkeley, CA, USA, 2005. USENIX Association.

[27] OWASP. Owasp internet of things project. owasp.org/index.php/OWASP_Internet_of_Things_Project.

[28] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm, J. A. Camelio, and C. Williams. Taxonomies for reasoning about cyber-physical attacks in iot-based manufacturing systems. *IJIMAI*, 4:45–54, 2017.

[29] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero. An experimental security analysis of an industrial robot controller. In *2017 IEEE Symposium on Security and Privacy (SP)*, 2017.

[30] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, and Y. Elovici. 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*. ACM, 2017.

[31] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu. My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3d printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16.

[32] J. Spadaro and L. Wyatt. Mutiny fuzzer. https://github.com/Cisco-Talos/mutiny-fuzzer, 2019. Accessed: 2019-05-03.

[33] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker. Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .stl file with human subjects. *Journal of Manufacturing Systems*, 2017.

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

[35] F. M. P. Thomas R. Kramer and E. Messina. The nist rs274ngc interpreter - version 3. Technical Report NISTIR 6556, National Institute of Standards and Technology, 2000.

[36] E. Vadala and C. Graham. Downtime costs auto industry $22k/minute - survey. news.thomasnet.com/companystory/downtime-costs-auto-industry-22k-minute-survey-481017, 2019.

[37] V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart, and S. Chotivatunyu. Pentos: Penetration testing tool for internet of thing devices. In *TENCON 2017 - 2017 IEEE Region 10 Conference*, 2017.

[38] R. Wang, Y. Shoshitaishvili, C. Kruegel, and G. Vigna. Steal this movie: Automatically bypassing DRM protection in streaming media services. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, 2013.

[39] Y. Wang, O. Anokhin, and R. Anderl. Concept and use case driven approach for mapping it security requirements on system assets and processes in industrie 4.0. *Procedia CIRP*, 2017.

[40] T. J. Williams. The purdue enterprise reference architecture. *Comput. Ind.*, 24(2-3):141–158, Sept. 1994.

[41] M. Wu and Y. B. Moon. Taxonomy of cross-domain attacks on cybermanufacturing system. *Procedia Computer Science*, 2017.

[42] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac. Towards security of additive layer manufacturing, 2015.

[43] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici. Security of additive manufacturing: Attack taxonomy and survey. In *Additive Manufacturing*, 18.

[44] R. Zwienenberg. Acad/medre.a 10000's of autocad files leaked in suspected industrial espionage. welivesecurity.com/2012/06/21/acadmedre-10000s-of-autocad-files-leaked-in-suspected-industrial-espionage.