Forensic Science International: Digital Investigation 44 (2023) 301510

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 EU - Selected papers of the Tenth Annual DFRWS Europe Conference

FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process

Muhammad Haris Rais*, Muhammad Ahsan, Irfan Ahmed

Virginia Commonwealth University, Richmond, VA, 23284, USA

ARTICLE INFO

Article history:

Keywords:
CPS forensics
Forensic readiness
Fused filament fabrication
3D printing
Material extrusion

ABSTRACT

Additive manufacturing (a.k.a., 3D printing) materializes an object by stacking thin layers of material from ground zero. It is increasingly utilized in industry to print critical components of automobiles, airplanes, etc. Failure of a 3D printed part (such as a turbine blade) during operation may incur immense damage to the system and the surroundings, incentivizing cyberattacks on the printed object. A forensically ready printing setup facilitates a post incident investigation. Currently, no forensic readiness model exists for an additive manufacturing (AM) process in the literature, whereas conventional cyber-domain specific models do not consider AM processes and may be ineffective in investigating 3D printed parts in a crime scene. This paper presents a forensic readiness framework, FRoMEPP for the material extrusion-based 3D printing process to acquire and preserve forensic data after identifying important information sources in the printing process chain. FRoMEPP framework provides practical technical guidance to the organizations striving for a forensically ready printing environment. It also benefits the regulatory bodies in formalizing compliance criteria for critical 3D printing setups. We implement FRoMEPP framework on a typical material-extrusion printer, Ultimaker-3, and evaluate it through a case study by implementing three sabotage attacks involving thermal profile manipulation, internal voids, and printing timing integrity compromise. The evaluation results show that FRoMEPP can effectively investigate and present traces of the attacks against 3D printed parts.

1. Introduction

Digital forensic readiness (DFR) (Rowlingson et al., 2004) prepares an organization for a potential forensic investigation through a well-planned timely acquisition of information that may not remain available after an attack or incident (Singh et al., 2019). Forensic readiness of different computing infrastructures comprises different sets of evidence, information sources, and evidence retrieval methods. Any major leap in technology mandates a reassessment of applicability and effectiveness of existing forensic methods. For example, National Institute of Standards and Technology (NIST) identified 65 challenges in applying conventional techniques to cloud forensics (N. C. C. F. S. W. Group, 2014), resulting in the development of dedicated forensic readiness models for cloud environment (Raju and Geethakumari, 2016; Pichan et al., 2015). For the same reason, dedicated research is required to explore suitable forensic models for additive manufacturing (AM) processes.

With the emergence of Industry 4.0, the rising AM market has gained further significance (Dilberoglu et al., 2017). More functional components are now 3D printed, raising incentive for attackers to attack the printed objects. The research community is actively working on exploring new vulnerabilities and defense techniques, but there is no published work about making an AM process forensically ready. This paper is an attempt to fill this gap.

AM or 3D printing is a manufacturing method that materializes an object from ground-zero by adding material, typically by stacking thin layers. Fig. 1 presents a 3D printed object life cycle. To print an object, its computer-aided design (CAD) file is converted into an outer surface geometry representation, typically in stereolithography (STL) format. Utilizing the STL file and the user-defined design parameters, a slicer software produces printer-specific sequence of instructions (G-code). G-code commands are sent to the printer where the firmware sequentially executes them to print the object. Around this core process, there are supporting processes like procurement and job provisioning.

A 3D printed object can be attacked at various stages of its

* Corresponding author.
E-mail address: raismh@vcu.edu (M.H. Rais).

https://doi.org/10.1016/j.fsidi.2023.301510
2666-2817/

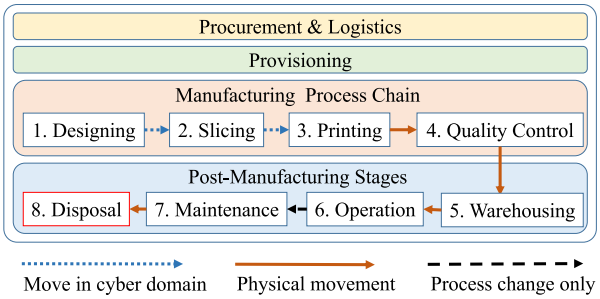


Fig. 1. 3D printed object life cycle.

lifecycle (refer to Fig. 1), including attacks on provisioning service (e.g., the computer network of a printing service provider) or during procurement and logistics (Gupta et al., 2020; Mohd Ali et al., 2019; Sturm et al., 2014). This paper focuses on the forensics of *manufacturing process chain* consisting of designing, slicing, printing, and quality control. Note that the manufacturing process covers the cyber-physical boundary and is more vulnerable to cyberattacks on printed objects than the warehousing or operation phase.

A sabotage attack on a 3D printed part aims at modifying its physical properties, such as the fit & form, and strength (Yampolskiy et al., 2018). Recently, researchers have demonstrated that planned tiny deviations within printer's specification tolerances can still degrade the mechanical strength of the printed parts (Rais et al., 1314). Low magnitude attacks are more likely to pass the non-destructive quality checks. If an attacked part fails during operation, the investigator will have to identify the intruder and prove that the intruder's actions have caused the defect leading to the accident. Therefore, a DFR solution for AM is not complete without acquiring physical-domain information to correlate between a cyberattack and manipulations in a printing environment and 3D object.

This paper presents a DFR framework, FRoMEPP (Forensic Readiness for Material Extrusion based Printing Process) to identify attack traces on a 3D printing setup and subsequent impact on a targeted 3D object. Material extrusion is the most widely used 3D printing method (Gibson et al., 2021). FRoMEPP discusses the useful information sources in cyber and physical domain of the printing process chain, highlighting the importance of capturing critical physical sub-processes (such as kinetics and thermodynamics) for a forensic investigation. It presents forensically sound and verifiable methods to acquire AM-specific details, such as the printing process instantaneous state parameters. It lays down a criteria to select and deploy a suitable process monitoring scheme aligned with specific printing environment requirements.

We implement and evaluate FRoMEPP on a real-world 3D printer against sabotage attacks, and further present post-incident log analysis to demonstrate FRoMEPP effectiveness; the analysis involves extracting forensically useful artifacts from FRoMEPP dataset and presenting them in comprehensible format for forensic investigation.

The contributions of this paper are three-folds.

- We present a novel DFR framework, FRoMEPP for material extrusion-based 3D printing.
- We demonstrate FRoMEPP's implementation on Ultimaker-3, a real-world material extrusion printer.
- We implement three existing sabotage attacks on printed parts and show that a forensic investigation using FRoMEPP successfully discovers attack traces.

The rest of the paper is organized as follows. Section 2 discusses the related work, followed by the proposed framework in Section 3. FRoMEPP implementation on Ultimaker 3 is presented in Section 4. Section 5 demonstrates FRoMEPP capabilities in conducting post-incident forensic analysis. Section 6 presents a case study to evaluate FRoMEPP against the known attacks, followed by the future work and the conclusion.

2. Related work

To the best of our knowledge, there is no work in the literature discussing the DFR model for an AM process. This section briefly mentions the relevant work on IT forensic readiness, AM forensics, and cyber-physical systems (CPS) forensics.

Rowlington proposes a ten-step process for organizations to achieve DFR, and presents its advantages for organizations and law enforcement agencies (Rowlingson et al., 2004). Grobler et al. split DF into proactive, live, and post-incident phases and discuss various dimensions of proactive forensics to present an overall picture of a forensic readiness framework (Grobler et al., 2010). Valjarevic et al. organize DFI into four process groups, where the first group comprises forensic readiness processes. Moving down from high-level abstraction, they split the readiness group into three chronological sub-groups: planning, implementation, and assessment processes (Valjarevic and Venter, 2013). Using a different approach, Elyas et al. propose a DFR framework to produce evidence that fulfills regulatory compliance, legal proceedings, and the organization's internal investigation goals (Elyas et al., 2014).

Although researchers have proposed the use of 3D printing to facilitate forensic investigations in various domains (Chaudhary et al., 2018; Carew et al., 2019; Foster et al.), the forensics of AM process itself is minimally explored. Forensically sound data acquisition for embedded devices is a challenging task due to the lack of standardized methods and tools (Conti et al., 2018; Stoyanova et al., 2020). Garcia et al. present an experiment to extract forensic information from the PC running the printer control software. Using a standard forensic software, they analyze the changes in files and registry entries after executing a printing task (Garcia and Varol, 2018).

As a 3D printer is a CPS, we briefly cover the forensics of CPS relevant to our work. Within different types of CPS, industrial control systems (ICS) (Ahmed et al., 2016) has been actively researched with a focus on forensically analyzing network traffic, and device data (Ahmed et al., 2012, 2017; Qasim et al., 2019, 2020; Awad et al., 2018; Rais et al., 2022; Zubair et al., 2022; Senthivel et al., 2017; Ayub et al., 2021). These approaches rely on extracting information from cyber domain and do not involve independent measurement of physical process parameters. Ab Rahman et al. present a framework based on *forensics by design* approach for the cyber-physical cloud system, emphasizing the importance of incorporating forensic requirements in the design phase (Ab Rahman et al., 2016). Extracting artifacts from a CPS has been done in the past (but not for 3D printers). Rais et al. propose a hardware-based approach to reliably extract the memory contents of ICS devices (Rais et al., 2021a).

Most of the above-discussed papers only explore information sources in cyber domain. Interestingly, AM security researchers have used physical-domain knowledge in exploring new attacks and defense techniques. Examples of monitoring physical-domain parameters include capturing filament heat signatures through thermal cameras, nozzle temperature monitoring, extruder movement tracking through stepper motors' acoustic signals, electric current, and accelerometers (Faruque, 2016; Miao et al., 1007; Belikovetsky et al., 2017; Gatlin et al., 2019; Chhetri et al., 2016). Although these studies do not discuss AM forensics, they confirm

the feasibility of gathering the physical-domain information.

3. FRoMEPP forensic readiness framework

3.1. Material-extrusion based 3D printing process

Material-extrusion, commonly known as fused filament fabrication, is the most widely used additive manufacturing method (Gibson et al., 2021). In a typical material-extrusion printer, continuous filament is pushed through a heated nozzle onto the printing bed. As the nozzle extrudes the filament, it follows a planned path to deposit a thin layer of material on the printing bed. Once one layer is printed, the relative distance between the nozzle and the printing bed is increased to create space for the next layer.

Material extrusion is a complex process to mathematically model due to its dependency on a number of factors such as printing sequence, layer thickness, printing orientation, infill pattern, solidification of the extruded material, etc. For instance, as the hot molten filament is extruded, its heat energy creates bonding with the existing material on the bed before getting solidified. The bonding process depends on a host of factors, including the extrusion rate, the shape and size of the nozzle, the extrusion pattern, the nozzle and the printing bed heating profile, and cooling fans speed. The process complexity offers opportunities to the attackers who are finding higher incentives in attacking 3D printing process.

3.2. Attack model

We assume an advanced attacker that has access to expert-level knowledge of material-extrusion based AM process to design inconspicuous and sophisticated attacks. The attacker can compromise the 3D printing process by either exploiting the cyber domain components of the process chain or by installing a malicious firmware through a USB drive or a SD-card. The purpose of these tough yet realistic assumptions is to design a forensic framework that caters for sophisticated attacks.

This work focuses on active attacks and assumes that the attacker will sabotage the primary printing process at any stage. Passive attacks such as intellectual property theft via side-channel monitoring (Yampolskiy et al., 2013) are not in scope.

3.3. DFR requirements for material extrusion-based AM environments

Before creating the DFR framework, it is imperative to understand its objectives. We analyze the complete AM process chain to identify the potential indicators of compromise and formulate the below-mentioned set of requirements that an effective AM-specific DFR solution should address. Literature review confirms that these requirements engulf all the existing attacks.

1 Monitor the printing process in both the cyber and the physical domains
2 Acquire operating system and application level forensic information from all involved cyber-domain actors.
3 Acquire the object specific cyber-domain artifacts (such as CAD/STL/G-codes)
4 Acquire the inter-stage network traffic captures
5 Capture the printer's view of the process by extracting forensically important logs from the printer
6 Independently monitor the printing operation with no or minimal (within operational tolerances) intrusion
7 Correlate a printed object to its corresponding logs
8 Offer capability to analyze the process on intuitive boundaries, such as per layer or per instruction basis
9 Facilitate an interruption-free printing operation during any post-incident forensic investigation
10 Preserve the dataset in accordance with standard forensic soundness guidelines

3.4. FRoMEPP - proposed DFR framework for AM process

This section presents an overview of the proposed framework outlined in Fig. 2. The left column represents generic DFR tasks at a higher abstraction level, and the right side details the information and activities to accomplish the task for AM DFR.

The first step in creating a forensically ready printing setup is to identify the useful data sources in the process chain. Cyber-domain data sources are classified as OS, Network, and Applications. As cyber-domain logs alone do not provide the required details to authentically answer all the forensic questions, critical AM-specific physical processes are identified and monitored. From the forensic perspective, we categorize the physical processes as the primary (directly influenced through cyber manipulations) and the secondary processes. FRoMEPP framework suggests monitoring all independent primary processes. The second step is to establish a monitoring criteria and a compliant acquisition scheme for data retrieval. To ensure forensic soundness, out-of-band sensors are deployed in the physical domain. For the cyber domain, network data acts as an independent source to scrutinize the OS and the applications logs.

FRoMEPP assigns a unique identifier to every printed object. The physical and the cyber logs are also assigned identification tags to correlate with the printed object logs. The information collected from various cyber and physical sources is standardized and converted to comprehensible formats for analysis. The consolidated and correlated data set from both the domains along with the metadata are preserved and archived.

4. Framework implementation and illustration on a real-world 3D printer

This section elaborates the FRoMEPP framework through an implementation study on a material extrusion-based 3D printer - Ultimaker-3. Presented in Fig. 3, Ultimaker-3 is a dual-nozzle cartesian coordinates 3D printer comprising one stepper motor for each x/y/z/filament axes. The printer is controlled through an open-source software - Cura, that receives an STL file and converts it into Ultimaker-compatible G-code commands. The control PC hosting Cura is connected to the printer over LAN. We use Comsol Multiphysics 5.4 and AutoCAD 2019 tools to create design files.

4.1. Identify the information of interest

We examine AM elements in both cyber and physical domains as candidates for information sources.

4.1.1. Cyber-domain information

Information sources in the cyber domain are classified under three main categories; operating systems, computer networks, and relevant applications.

4.1.1.1. Operating system logs. An attack may use the OS of a cyber-domain device as a launching pad, leaving important traces of unlawful activities. Information about user sessions, file activities, jump lists, and OS-level security event logs help understand the attack mechanism (Saidi et al., 2013; Singh and Singh, 2016).

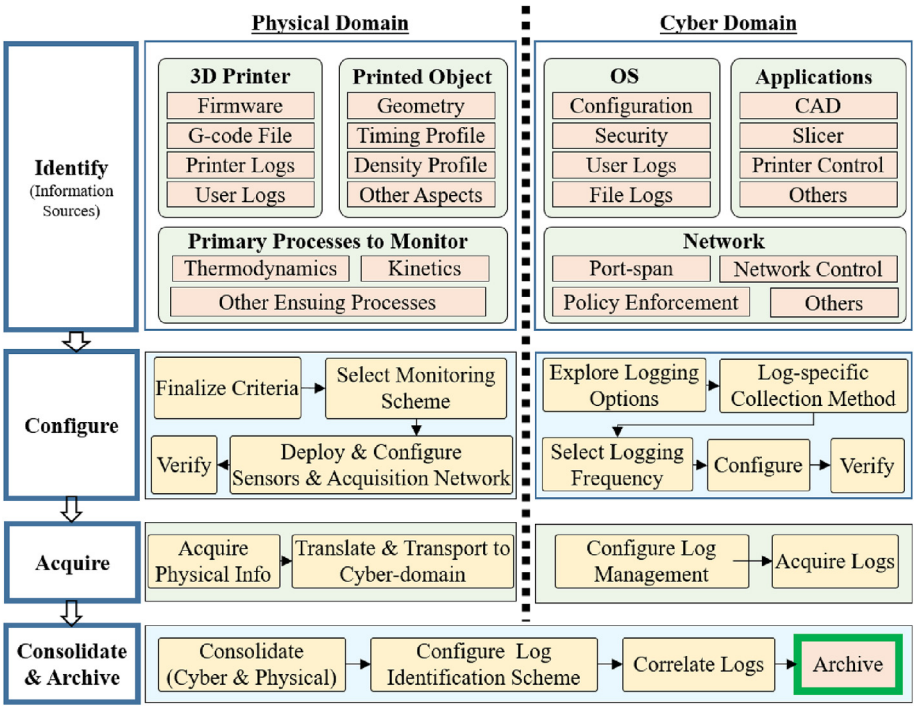


Fig. 2. Forensic readiness framework, FRoMEPP for material extrusion based additive manufacturing (3D printing) environment.

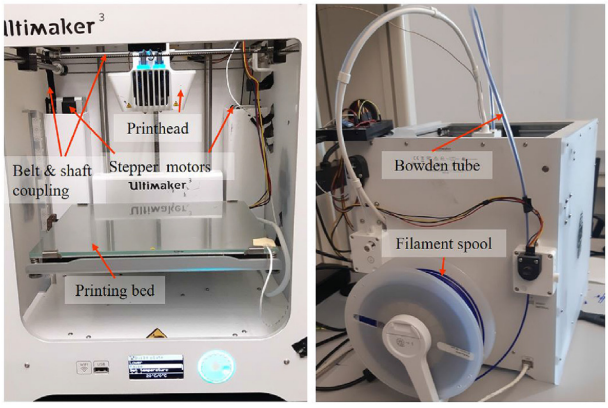


Fig. 3. Ultimaker-3 material extrusion-based 3D printer.

Interested readers may refer to (Garcia and Varol, 2018) for the OS level forensic traces in AM environment.

4.1.1.2. Network logs. For OS and application layer attacks, the network logs present an independent and forensically sound evidence. Network traffic between the printer and the external world includes Cura communication over HTTP and user connections over SSH protocol or HTTP. This implementation uses Wireshark software to capture Control PC Ethernet traffic.

4.1.1.3. Application logs. Generally, OS logs offer details about the attacker and the attack path but less information about the attack. If the traffic between two nodes is encrypted, information extraction from their network traffic becomes more challenging (van de Wiel et al., 2018). On the other hand, application logs often offer detailed and comprehensible information about the attacker's manipulations. Main applications in the 3D printing process include CAD, slicer, and printer control applications. Printing service providers have other supporting software such as provisioning and billing application.

In this implementation, we utilize the auto-save, backup files, and log files generation options in AutoCAD software to attain helpful traces of anomalous or unauthorized activity. For slicing and printer-control functions, we use Cura version 4.10.0 software. Cura generates informational and error log files saved in temporary folders. These files reveal important information, including configuration changes, error logs, and the recent printed files list.

4.1.2. Physical-domain information

Although the intrusion traces may be discovered in cyber logs, they cannot offer conclusive evidence to pin the responsibility of the component's failure on the attacker. Physical-domain data extraction fills the missing link. Being later in the process chain and not in control of the attacker in most cyberattacks, physical-domain data about the printing state is more reliable than cyber-domain logs.

4.1.2.1. Printer logs. A 3D printer is an advanced embedded system available in various hardware architectures and firmware. Basic level printers use a single controller for printing and user-interface. Ultimaker-3 uses A20-OLinuXino-LIME2 as the printer's mainboard, running a custom Linux OS based on the Debian Jessie release. The real-time kinetic and thermodynamic functions are offloaded to a separate controller with dedicated firmware. An essential aspect of the printer's security is firmware integrity. This implementation periodically extracts the running firmware, list of recent printed files, event messages, and user login details from the printer.

4.1.2.2. Printed object logs. The outcome of 3D printing process is the printed object. Being the most common target of attack (Yampolskiy et al., 2018), the state of the printed object is measured throughout the printing. Monitoring the object's state is more than

mere visual inspection. Some attacks (such as thermodynamic attacks) cause no visual deformation but still damage the printed object (Rais et al., 2021b). Material extrusion is a complex process involving kinetics, thermodynamics, crystallization (Yu et al., 2019), glass transition (Spoerk et al., 2018), microstructure-related and other properties. FRoMEPP recommends to monitor the primary or direct−manipulable processes.

4.1.2.3. Direct−manipulable processes in material extrusion-based printing. In material extrusion, kinetics and thermodynamics are the processes that a cyberattacker can exploit. As all the remaining processes are their subsequent effects, monitoring kinetics and thermodynamics covers cyber-manipulations targeted towards other properties. Fig. 4 represents the direct−manipulable processes of material extrusion-based printing, along with the components controlling them. The three sub-processes of kinetics, i.e., filament kinetics, nozzle kinetics, and printing-bed kinetics, are controlled through filament motor, x,y, or ρ, θ axes motors, and z-axis motor, respectively. The thermodynamic process is influenced by the nozzle heater, printing bed heater, and cooling fans. Environmental temperature and airflow may also slightly impact the thermodynamic process. Monitoring the instantaneous state of the components mentioned in Fig. 4 during printing is analogous to monitoring the object being printed, and thus adequate in investigating attacks on the object.

4.2. Configure the information sources for logging

After identifying the information sources, we configure them for log retrieval. Being extensively researched, the cyber-domain configuration is briefly discussed here. We only focus on AM-specific applications and network logs. We collect the network traffic directly from the Ethernet interface card of the control PC through Wireshark version 3.6.2. Traffic capturing is configured as a permanent process, and a new file is created on hourly basis.

Cura logs exhibit multiple retention patterns; such as cyclic (most recent retained or periodic erasure). We configure the logging on a *pull* basis at a frequency in accordance with the retention period and the log's buffer size. By default, Cura saves an error log file at '*C:/users/username/AppData/Roaming/Cura/*' with the name '*stderr.log*'. Another important file named '*cura.log*' placed at '*C:/users/username/AppData/Roaming/Cura/version/*' contains Cura configuration parameters values, ten most recent files, and other active configuration details.

From a logging perspective, the printer and the printed object are constituents of the physical domain. Logging configuration for the printer depends upon the provisioning options provided by the vendor. Ultimaker-3 offers Secure Shell (SSH) access to the printer for configuration and code changes. A user can add a suitable code to push the desired logs, such as important event details.

Measuring the printed object state for forensics is a less researched topic. Therefore, we discuss the four-step 'configure' task presented in Fig. 2 in detail.

4.2.1. Finalize the monitoring criteria

Numerous methods are available to observe the printed object state during printing. To evaluate the performance and suitability of a monitoring scheme for a printing setup, FRoMEPP recommends the following five points criteria.

4.2.1.1. Sensing system resolution and feasible parameters. The choice of the printing state sensing scheme depends on the required resolution for each monitored component. We set an expected resolution of 0.1 mm for the printhead, 0.05 mm for the printing bed, and 1^oC resolution for the thermal components. These values are derived in consideration with the printer specifications.

4.2.1.2. Observing the end effect. AM process transitions through multiple stages before accomplishing a printed object. If the actual printing is at Stage_n and the observation point is at Stage_i where $i < n$, the manipulations at Stage_{i+j} where $0 < j < n - i$, will go unobserved. Thus, it is natural to move the observation point as close to the end effect as feasible.

Fig. 5 elaborates this concept using Ultimaker-3 kinetic process example. When the printer executes a move instruction, the firmware calculates the per-axis distance, converts it to electrical signals, and applies them to the stepper motors. The motors transform electrical energy to magnetic energy, and rotate the driving shaft. Mechanical coupling translates shaft rotation to the printhead movement. Stage 2 to Stage 5 of Fig. 5 offer independent provision to measure the printhead state. Stage 5 is the most appropriate choice, if feasible, as it rules out the intermediate-stages errors.

4.2.1.3. Noise resilience. Noise negatively impacts the accuracy and the resolution of a monitoring scheme and may increase its algorithmic complexity and processing overhead. Some monitoring approaches are more resilient to specific environmental noises than others. For instance, unlike the electric current, magnetic field measurement suffers from the interference of other motors'

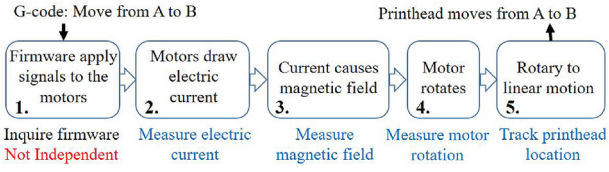


Fig. 5. Kinetics process stages with kinetic measurement options.

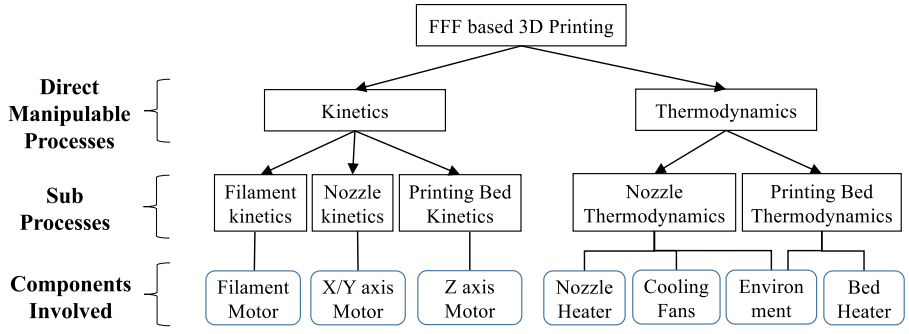


Fig. 4. Direct−manipulable processes and controlling components.

magnetic fields or external sources. For this implementation, we set a criterion that the selected scheme should be resilient to the magnetic interference, routine sounds in the lab, and minor vibrations in the platform (printer table).

4.2.1.4. Non-intrusiveness and simplicity of deployment. Intrusiveness is evaluated from deployment and operational perspectives. Measuring the electric current does not interfere with its operation, but the deployment involves partial disassembly and rewiring. On the other hand, measuring the printed object state through a camera (by iteratively pausing the printing) offers non-intrusive deployment. However, the 'pause' operation modifies the timing and thermodynamic profile. FRoMEPP recommends process monitoring to be operationally non-intrusive.

4.2.1.5. Independent monitoring. Forensic soundness of the acquired information is vital for any DFR solution. Information acquired from an actor under attack loses its evidentiary weight as a sophisticated attacker can modify its generated logs (Falliere et al.). FRoMEPP recommends out-of-band sensors to measure the process state.

4.2.2. Select a suitable monitoring scheme

After formalizing the criteria, we evaluate seven schemes for monitoring the kinetic processes, including in-band firmware query, accelerometers, magnetometers, optical encoders, acoustic sensors, camera imaging, and measuring the electric current drawn by kinetic components. Each approach has its merits and limitations. Features are split into mandatory and non-mandatory categories. Overall score of a scheme is calculated using Equation (1), where S_i is the score of i^{th} monitoring scheme, r_{ik} is the binary result of k^{th} mandatory feature, w_{ij} and s_{ij} are the respective weight and the score of a j^{th} feature for the i^{th} scheme. To ensure forensic soundness, we elevate two features as mandatory; monitoring should be (1) independent and (2) operationally non-intrusive. The remaining features are assigned an equal weight (for simplicity).

$$S_i = \left(\prod_{k=1}^{m} r_{ik} \quad * \quad \sum_{j=1}^{n} w_{ij} * s_{ij} \right) \tag{1}$$

Two approaches are rejected for not fulfilling mandatory requirements; (1) 'Inquiring the firmware' for being in-band and thus not forensically sound, and (2) 'camera imaging (as available to us)' for being operationally intrusive. 'Resolution' and 'Noise resilience' features of the schemes are assessed in view of the results in the existing literature. For these features, optical encoders and electric current measurement schemes get the highest points. Camera imaging tops the 'Observing the end effect' feature, as it rules out all possible machine issues. Overall, the optical encoder-based sensing scheme gets the highest points in our scenario and is selected for the kinetic processes monitoring, followed by the electric current sensing, accelerometers, acoustic sensors, and magnetometers.

Although the scoring is applicable to generic material-extrusion-based setups, we recommend a re-scoring for each unique criterion and printing environment. For the thermodynamics process monitoring as per Fig. 4, we restrict the scope to the nozzle and printing platform thermal profile measurement using a thermocouple and a thermistor, respectively.

4.2.3. Deploy and configure acquisition system

Rotary optical encoders are deployed on the printhead connecting shafts for the printhead kinetics. A linear encoder is installed to track the printing bed. A k-type thermocouple is deployed at the tip of the heated nozzle, and a surface-mount thermistor is annexed to a corner of the heated platform. An Arduino board energizes the sensors and collects the data. Interrupt routines are used for the high-velocity kinetic data, and the slow-varying thermodynamic data is polled periodically. The data is further sent to the project PC over a USB interface. Sensors specifications and installation procedure is detailed here (Rais et al., 2021c).

4.2.4. Evaluate the forensic soundness of the system

Unlike the established practices in the cyber domain, the forensic soundness of the proposed physical-domain monitoring methods needs to be ascertained. Reference data, physical measurements and in-system readings (where possible) are used to verify monitoring scheme data. Data acquired from the printer uses standard SSH connection, or REST APIs over HTTP. The biggest artifact in size is the firmware that matches exactly with the copy securely attained from the vendor. The printed object's logs are verified through test cases covering the operational spectrum of the unit under test. For instance, rotary encoders data is verified in small steps over one complete rotation to rule out deployment errors such as axial play and runout.

4.3. Acquire the logging data

After configuring the physical and the cyber-domain data extraction schemes, data collection is started. For a large scale setup, standard logging management suite may be used to handle the variety of logs. For this demonstration, we develop a small piece of software to manage and preserve the logs. While the cyber-domain and the printer logs follow a standard or a proprietary format, no data format exists for the external sensors network. We develop two structures for the printed object data. To avoid overloading of Arduino board, we use a small data structure for the high velocity kinetic data, and a bigger structure for the consolidated data from the entire sensors network.

4.4. Consolidate and archive

DFR software receives the physical-domain data, pre-processes it and utilizes interpolation functions to fill in the missing data fields to standardize the data set. At this point, the physical and the cyber domain data is available as a cyber domain resource. Consolidation of logs from both domains offers operational ease in the post-incident investigation. Each logging category has a different frequency, ranging from 5 ms for the fast-moving kinetic data to a day for retrieving firmware copy. To correlate among various logs, an identification mechanism is required.

4.4.1. Unique identifier for logs correlation

An identification scheme connects each unique printed object to its corresponding logs. Identification schemes can utilize on-the-object or off-the-object marking methodology. Although on-the-object schemes (such as 3D watermarks) are more scalable and

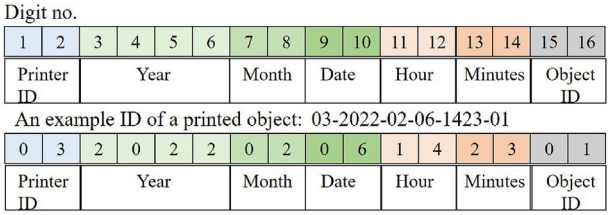


Fig. 6. 16 digit unique identifier for printed object and its logs.

error-resistant, their integration with the current process chain is not readily available. From a forensic perspective, an organization may employ any suitable object tagging mechanism. Printing an object (or a batch of objects) is a unique event in the time domain, making timing information a feasible object identifier. A unique ID is assigned to the physical object, and also to all the log categories having a one-to-one relationship with the printed object. ID tag in this study has 6 fields and 16 decimal digits. The first two digits represent the unique printer on the farm. Digits 3 to 14 mark the printing start time. The last two digits are used to disambiguate among multiple objects within a single print job having the same start time. ID 03-2022-02-06-1423-01 presented in Fig. 6 refers to the first object printed through printer 3 at 2:23 PM on Feb 6, 2022.

4.4.2. Archiving

The data set in our study is archived using a four-tier functional hierarchy: log category, organizational structure, raw logs, and extracted artifacts. Five log categories are defined; printer, printed object, OS, applications, and network logs. The organizational structure of logs is aligned with the identification scheme. To archive a new log, the software traverses the repository tree from the root down to the node hosting that log. Any non-existent node in the path is created during this operation. For example, the software extracts Cura logs on an hourly basis. At 2:00 PM (1400 hrs), the software traverses the repository from *Root/Application logs/Cura ID/Date/*. A new directory *1400* is created, and the logs are saved.

5. Post-incident forensic log analysis

A malicious intrusion in 3D printing process may be aimed to disrupt the printing service or sabotage the printed object. Inducing obvious defects in an object, such as modifying its shape and size, is a simple sabotage attack. A sophisticated sabotage attack may induce non-obvious defects in the object, so that it may pass the quality assurance check and be installed in a critical system where its premature failure can cause more damage. In this section, we present how FRoMEPP data set helps identify traces of simple and sophisticated attacks including information about the attack mechanism and the attacker. Generally, the raw logs require further analysis to identify useful evidence. Analyzing the physical-domain logs require different tools than conventional IT.Fig. 7 presents a formalization of the forensic artifacts extraction process used in our implementation. Three categories of logs are applied to the relevant extraction methods that utilize process knowledge and correlation algorithms to extract useful information. These algorithms return important artifacts such as printed object geometry and density profile, thermodynamic profile, timing profile, printer firmware, design files, and session and error logs.

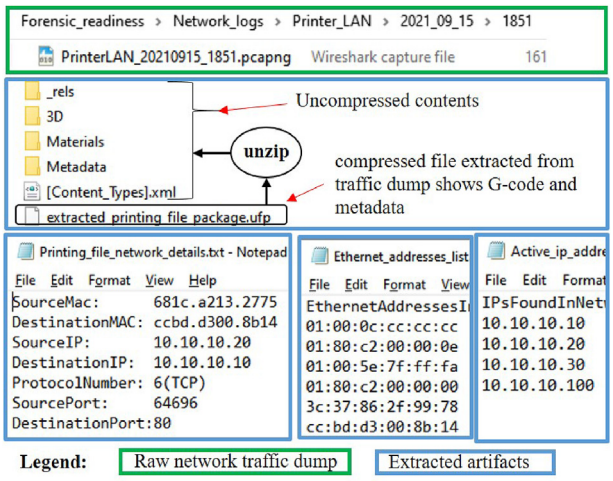


Fig. 8. Forensic artifacts extracted from network-traffic dump.

5.1. Network artifacts

Fig. 8 presents a few artifacts extracted from the network traffic. An unencrypted compressed file found in the dump comprises the G-code file and other metadata related to the printing request. We also discover the user machine MAC and IP addresses, and TCP port numbers. The active IP and Ethernet addresses shown in the figure can help in identifying suspicious users. Ultimaker-3 also hosts a web server offering unauthenticated view-only access. The network traces will capture all access events.

5.2. Cura artifacts

A few forensically important Cura logs are discussed here. The log file *stderr.log* contains error messages with the timestamp and an assigned severity level. The contents are flushed when Cura restarts. Fig. 9 displays a part of the information present in another log file, *cura.cfg*, indicating the printer's IP address, the default file path, and the ten most recent files processed by Cura. A subfolder, *quality_changes*, tracks the changes in the printing configuration profiles.

5.3. Printer artifacts

Ultimaker-3 offers a set of Representational State Transfer (REST) APIs to control and monitor the printer. We utilize selected APIs to iteratively extract the information of interest. Fig. 10 presents a snapshot of the printer logs showing the printing job name, its status, and the important timestamps related to the job. Using

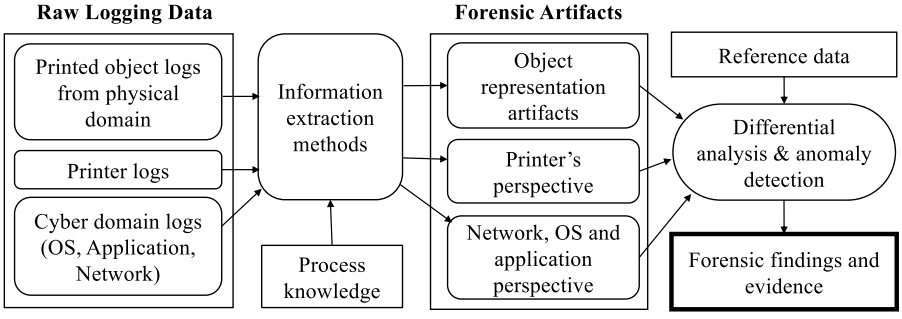


Fig. 7. Forensic information and artifacts extraction process.

```
[um3networkprinting]  [local_file]
manual instances = ,  dialog_save_path = C:/Users/SAFE-COMSOL/Desktop/3D_printer/Gcod
10.10.10.10           dialog_load_path = C:/Users/SAFE-COMSOL/Desktop/3D_printer/STLs

recent_files =
C:/Users/SAFE/Desktop/3D_printer/STLs/open_box_cut.stl;C:/Users/SAFE/Desktop/3D_print
/current/gcode_input/single_layer_noInfill_box.gcode;C:/Users/SAFE/Desktop/3D_printer
levator drum hollow at28mm cavity.stl;C:/Users/SAFE/Desktop/3D printer/STLs/Solid Bar
```

Fig. 9. cura.cfg excerpt showing IP address, paths and recent files.

datetime_started : 2021-04-06T18:03:57	datetime_started : 2021-04-07T14:08:19
name : UM3_Traxxas_pinion_28_v2	name : UM3_Propeller_Hubsan_X4_H107C_c
reprint_original_uuid : null	reprint_original_uuid : null
result : Failed	result : Finished
source : WEB_API/Ultimaker-008b14/Cura	source : WEB_API/Ultimaker-008b14/Cura
time_elapsed : 0	time_elapsed : 428.327814
time_estimated : 0	time_estimated : 0
time_total : 0	time_total : 0

Fig. 10. Printer logs showing job name, status, and timestamps.

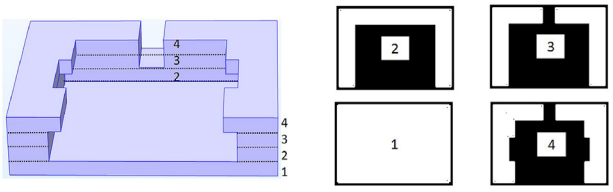


Fig. 11. A four layers model and its 2D slices.

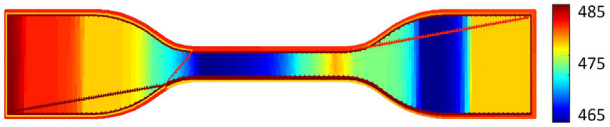


Fig. 13. Thermodynamic profile showing ± 10^{o}C variation in nozzle temperature at targeted locations.

SSH connection, we extract the printer firmware and the list of prints located at*/usr/share/griffin/griffin/machines/jedi.hex* and*/var/spool/cluster/../*, respectively.

5.4. Printed object artifacts

A layer-change event naturally splits 3D printing operation, motivating us to analyze the process on a per-layer basis. Through FRoMEPP data set, we recreate the geometry of each layer to examine the process in space domain. As two similar-looking geometries may have been accomplished using different toolpath sequences, we also analyze the printing process in the time domain.Fig. 11 presents the slices of a four layers model as 2D bitmap images. This presentation style is commonly used by slicer software, making the comparison between the actual print and the intended design simplified, detailed, and demonstrable. Although these xy plane slices, shown in Fig. 11, align with the printing direction, bitmaps of xz and yz plane cross-sections can also be extracted from the acquired data. Fig. 12 represents an accurate recovery of the printed hexagon through FRoMEPP.

The thermodynamic profile of the printed object is mainly driven by the filament temperature at the time of extrusion. A cyberattacker can manipulate the nozzle temperature to cause weak bonding or residual thermal stresses. Fig. 13 reflects the nozzle temperature at the instant when the pixel received the filament. The heatmap shows a temperature fluctuation of approximately ±10^{o}C.

The timing profile for the entire printing job or a single layer can be presented by plotting individual printing parameter values against time. Users may also employ other intuitive and beneficial techniques to view the process details such as recovering a 3D animation of the printing job from the sensors data set.

Fig. 12. Slicer representation (left), actual printed object (center), and accurate image recovered from FRoMEPP dataset (right).

6. FRoMEPP case study on sabotage attacks

Damaging the printed object is a key motive in attacking 3D printing process. This study evaluates FRoMEPP on three practical sabotage attacks in the literature (Belikovetsky et al., 2017; Rais

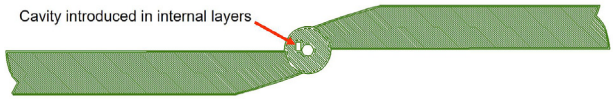


Fig. 14. Space domain representation of an internal layer of drone propeller showing a malicious cavity.

et al., 2021b).

6.1. Attack Scenario

An important printing facility receives complaints of premature failure of three critical parts (a car wheel, a drone propeller and a drive shaft) printed a few months ago. The facility owner ordered a forensic investigation. The facility had already implemented FRoMEPP framework on Ultimaker 3 as guided in Section 4 and 5 and provides its access to the forensic investigator. The investigator attains the unique identifiers for the suspected and corresponding known-good prints.

6.2. Investigating printed object logs

The suspicion of sabotage of the printed parts encouraged the forensic expert to initiate the investigation with the object logs. The expert analyzes them from three distinct standpoints: space-domain or geometrical analysis, thermodynamic analysis, and time-domain analysis.

6.2.1. Space-domain analysis

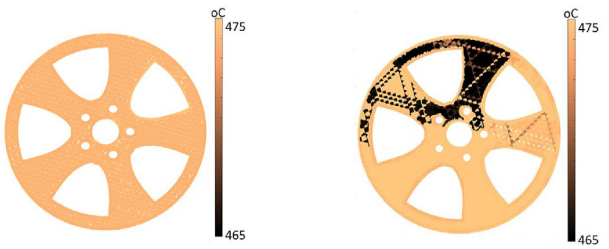
As presented in Section 5, the space-domain or the geometrical information for every layer is archived as a bitmap file, where each pixel of the bitmap represents 0.01 mm^2 area of the layer's geometry. The size and shape of the car wheel and the drive shaft match their non-attacked counterparts, but the drone propeller shows signs of a malicious cavity in the internal layers. Fig. 14 presents the bitmap image of the sixteenth layer showing a malicious cavity near the center. The cavity size is measurable by counting the pixels (as bitmaps are accurate and to the scale), and found to be 1 mm $\times$ 2 mm in 80% of the internal affected layers.

6.2.2. Thermodynamic profile analysis

The thermodynamic profile of the car wheel presented in Fig. 15b highlights a suspicious pattern. One of the spokes is printed at a different temperature than the rest of the wheel. Although a few degrees of thermal variation is expected during printing, a 10^oC reduction in temperature at a specific location is not a random error. The pattern is reinforced in all internal layers. Repeated reduction and reversion at a specific location in selected layers rule out hardware issues with the heating system. Manipulating the thermal profile may induce residual thermal stress causing strength reduction and warping (Rais et al., 2021b). The original G-code file did not contain temperature modification instructions. The thermodynamic analysis of the other two objects does not reveal any anomaly.

6.2.3. Timing profile analysis

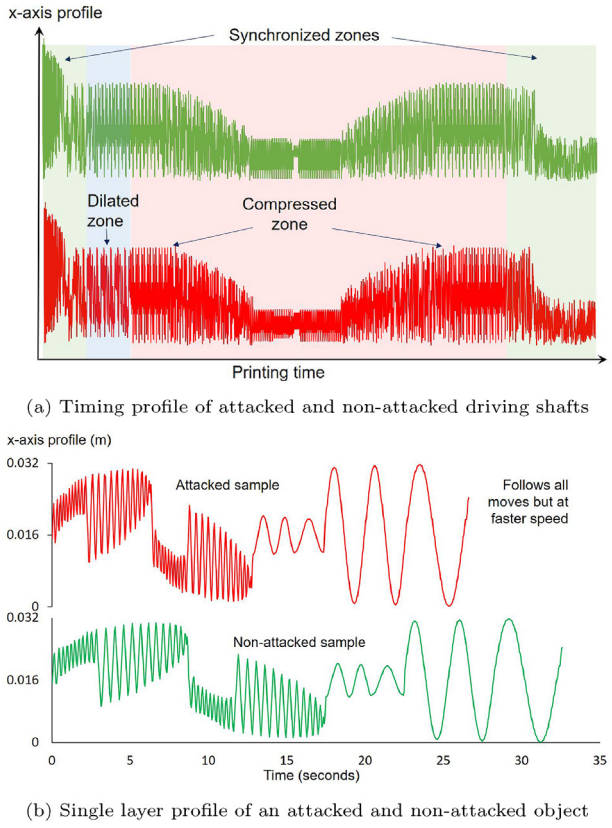
The space domain and the thermodynamic profile analysis of the driving shaft do not reveal any abnormality. The timing profile also does not offer any hint of malicious action. However, some synchronization issues are observed on examining the timing profile against known-good logs. The x-axis kinetic profile presented in Fig. 16a shows that the overall printing time is unchanged but the two profiles are not locally synchronized. To further drill down, the investigator compares per-layer timing profiles and finds that the time taken to print an internal layer is less than the default time. On the contrary, the initial layers were printed slowly. Other axes' kinetic profiles manifest similar patterns. Fig. 16b presents a comparison of a single-layer timing profile of suspected and non-attacked objects. This behavior shows that the critical zones were printed at a higher speed to influence the part's strength (Miazio, 2019), and the non-critical ones were slowed down to compensate for the time gain. The printed objects logs confirm malicious modifications in all three objects.



(a) Expected profile with minimal temperature variations

(b) Attacked object shows 10^oC reduction at one part

Fig. 15. Recovered heatmaps of attacked and non-attacked objects.



(a) Timing profile of attacked and non-attacked driving shafts

(b) Single layer profile of an attacked and non-attacked object

Fig. 16. Timing profiles of the attacked and non-attacked shafts.

6.3. Investigating the printer logs

To identify the attack mechanism and the attacker's details, the expert examines the logs from the printer. A few suspicious login attempts are discovered in the logs. The attempts were made from two source IP addresses using default usernames. As the user updated the default root password, no attempt to the root was successful. However, access to a non-root default user was successful. Fig. 17 captures a few of the login attempts. As a non-root user does not provide adequate process modification privileges, the suspected attacker did not pursue the attack through the printer. One of the IP addresses is linked to a printer control computing machine. The other IP address is assigned to the computer of an employee who is not authorized to connect to the printing setup.

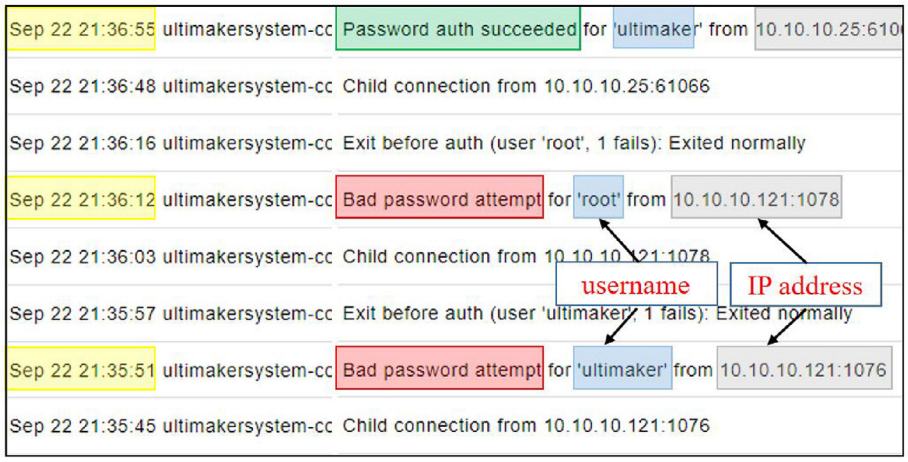


Fig. 17. Login attempts status logs extracted through REST API.

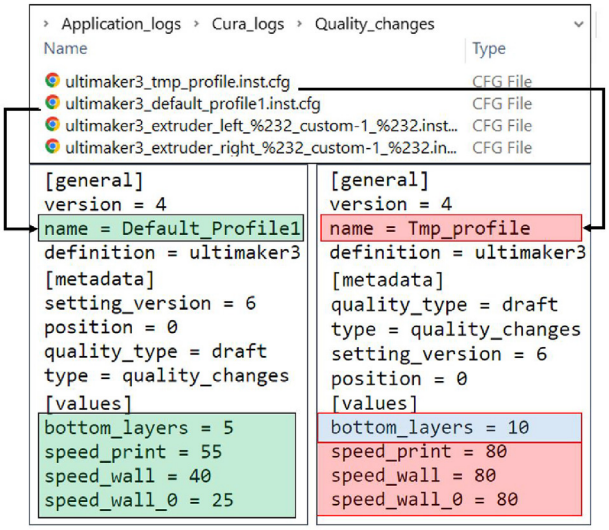


Fig. 18. Cura logs shows new or modified profiles and parameters.

6.4. Investigating cura and the network logs

Examination of the network dump provides the G-code files corresponding to the three objects under investigation. These files were sent from the IP address of the control machine. The control machine also hosts the Cura slicer software. All three recovered files were modified implying that either the control machine IP address was spoofed or the machine was hijacked. Ethernet (MAC) address associated with the IP address in the network dump confirms that the printing instructions were issued from the correct machine. Cura 'Recent files' logs show that two input files were fed to Cura software from a different path than the actual working directory. The third object file (driving_shaft.stl) was launched from the correct path. 'Cura profile logs' reveals that the printing profile in Cura software was modified and then reverted back. A suspicious printing profile, named 'Tmp_profile' increased the printing speed and the number of bottom layers from 5 to 10 as presented in Fig. 18. The modified parameter does not apply to the top and bottom layers printing speed. Slicing a design file with the modified profile results in faster printing of the intermediate layers, whereas increasing the number of low-speed bottom layers compensates for the time difference.

7. Future work

Preserving the evidence is a standardized task in the conventional IT domain and the entire ecosystem, including researchers, vendors, operators, and regulators, is well acquainted. With the increasing use of AM in the critical manufacturing, we expect to see more interest in all facets of AM forensics. Instead of relying on conventional IT forensics, it is helpful to research the methodologies and processes best suited for AM. Our proposed framework, FRoMEPP and its illustration focus on material extrusion-based printing. In the future, we intend to conduct studies on other AM techniques. An essential aspect of our proposed approach is the inclusion of physical processes in the monitoring system. A future direction is to utilize this approach to create a generic forensic readiness framework applicable to all CPS.

As commercial decision-makers often overlook security and forensics, a practical challenge is to suggest compliance criteria for the AM equipment, service providers, and customer setups.

8. Conclusion

This paper presented a forensic readiness framework, FRoMEPP, for material extrusion-based AM process incorporating the cyber and the physical domain information sources. FRoMEPP is explained through an implementation on a common printer - Ultimaker-3. The study formalized the physical-domain data acquisition process by identifying direct-manipulable sub-processes, and ranking the available acquisition options based on a set of mandatory and discretionary features. The implementation also discussed the forensic artifacts extraction process from the acquired data. Some of the extracted forensic artifacts include per-layer geometry, timing and thermodynamic profiles of the printed object, copy of the running firmware, design files, recent user-activity lists, and configuration changelogs.

Through a case study of three sophisticated sabotage attacks, we demonstrated the effectiveness of FRoMEPP in identifying information about the attack, the attacker, and the attack mechanism. The presented artifacts can help find answers to the forensic questions related to the printing deviations and the failure causes, making this implementation a strong candidate to be replicated in important 3D printing setups. The study also serves as a foundational work to facilitate the standardization and regulatory organizations in creating compliance criteria and forensic readiness standards for AM echo cycle.

References

Ab Rahman, N.H., Glisson, W.B., Yang, Y., Choo, K.-K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. 3 (1), 50–59. https://doi.org/10.1109/MCC.2016.5.

Ahmed, I., Obermeier, S., Naedele, M., Richard III, G.G., 2012. SCADA systems: challenges for forensic investigators. Computer 45 (12), 44–51.

Ahmed, I., Roussev, V., Johnson, W., Senthivel, S., Sudhakaran, S., 2016. A scada system testbed for cybersecurity and forensic research and pedagogy. In: Proceedings of the 2nd Annual Industrial Control System Security Workshop. ICSS '16, Association for Computing Machinery, New York, NY, USA, pp. 1–9. https://doi.org/10.1145/3018981.3018984.

Ahmed, I., Obermeier, S., Sudhakaran, S., Roussev, V., 2017. Programmable logic controller forensics. IEEE Secur. Priv. 15 (6), 18–24.

Awad, R.A., Beztchi, S., Smith, J.M., Lyles, B., Prowell, S., 2018. Tools, techniques, and methodologies: a survey of digital forensics for scada systems. In: Proceedings of the 4th Annual Industrial Control System Security Workshop, pp. 1–8.

Ayub, A., Yoo, H., Ahmed, I., 2021. Empirical study of plc authentication protocols in industrial control systems. In: 2021 IEEE Security and Privacy Workshops. SPW, pp. 383–397. https://doi.org/10.1109/SPW53761.2021.00058.

Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., Elovici, Y., 2017. dr0wned–cyber-physical attack with additive manufacturing. In: 11th USENIX Workshop on Offensive Technologies (WOOT 17). USENIX Association, Vancouver, BC. URL. https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky.

Carew, R.M., Morgan, R.M., Rando, C., 2019. A preliminary investigation into the accuracy of 3d modeling and 3d printing in forensic anthropology evidence reconstruction. J. Forensic Sci. 64 (2), 342–352.

Chaudhary, R.K., Doggalli, N., Chandrakant, H., Patil, K., et al., 2018. Current and evolving applications of three-dimensional printing in forensic odontology: a review. Int. J. Forensic Odontol. 3 (2), 59.

Chhetri, S.R., Canedo, A., Al Faruque, M.A., 2016. Kcad: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. In: 2016 IEEE/ACM International Conference on Computer-Aided Design. ICCAD, pp. 1–8.

Conti, M., Dehghantanha, A., Franke, K., Watson, S., 2018. Internet of things security and forensics: challenges and opportunities. Future Generat. Comput. Syst. 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060. https://www.sciencedirect.com/science/article/pii/S0167739X17316667.

Dilberoglu, U.M., Gharehpapagh, B., Yaman, U., Dolen, M., 2017. The role of additive manufacturing in the era of industry 4.0, Procedia Manufacturing. In: 27th International Conference on Flexible Automation and Intelligent Manufacturing, vol. 11, pp. 545–554. https://doi.org/10.1016/j.promfg.2017.07.148. FAIM2017, 27-30 June 2017, Modena, Italy.

Elyas, M., Maynard, S.B., Ahmad, A., Lonie, A., 2014. Towards a systemic framework for digital forensic readiness. J. Comput. Inf. Syst. 54 (3), 97–105. https://doi.org/10.1080/08874417.2014.11645708 arXiv.

Falliere, N., Murchu, L.O., Chien, E.. W32.stuxnet dossier. URL. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Faruque, M.A., 2016. Forensics of Thermal Side-Channel in Additive Manufacturing Systems.

K. Foster, P. J. Bills, L. Blunt, X. Jiang, R. Leary, The Use of Additive Manufacturing for the Presentation of Ballistic Toolmark Evidence in Court.

Garcia, V., Varol, C., 2018. Digital forensics of 3d printers. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, pp. 1–8.

Gatlin, J., Belikovetsky, S., Moore, S.B., Solewicz, Y., Elovici, Y., Yampolskiy, M., 2019. Detecting sabotage attacks in additive manufacturing using actuator power signatures. IEEE Access 7, 133421–133432.

Gibson, I., Rosen, D., Stucker, B., Khorasani, M., 2021. Material Extrusion. Springer International Publishing, Cham, pp. 171–201. https://doi.org/10.1007/978-3-030-56127-7_6.

Grobler, C., Louwrens, C., von Solms, S., 2010. A framework to guide the implementation of proactive digital forensics in organisations. In: 2010 International Conference on Availability, Reliability and Security, pp. 677–682. https://doi.org/10.1109/ARES.2010.62.

Gupta, N., Tiwari, A., Bukkapatnam, S.T.S., Karri, R., 2020. Additive manufacturing cyber-physical system: supply chain cybersecurity and risks. IEEE Access 8, 47322–47333. https://doi.org/10.1109/ACCESS.2020.2978815.

G. Miao, S.-J. Hsieh, J. Segura, J.-C. Wang, Cyber-physical system for thermal stress prevention in 3d printing process, Int. J. Adv. Manuf. Technol. 100. doi:10.1007/s00170-018-2667-5.

Miazio, L., 2019. Impact of print speed on strength of samples printed in fdm technology. Agric. Eng. 23, 33–38. https://doi.org/10.1515/agriceng-2019-0014.

Mohd Ali, M., Rai, R., Otte, J.N., Smith, B., 2019. A product life cycle ontology for additive manufacturing. Comput. Ind. 105, 191–203. https://doi.org/10.1016/j.compind.2018.12.007. https://www.sciencedirect.com/science/article/pii/S0166361518301647.

N. C. C. F. S. W. Group, 2014. Nist cloud computing forensic science challenges. https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf.

Pichan, A., Lazarescu, M., Soh, S.T., 2015. Cloud forensics: technical challenges, solutions and comparative analysis. Digit. Invest. 13, 38–57.

Qasim, S.A., Lopez, J., Ahmed, I., 2019. Automated reconstruction of control logic for programmable logic controller forensics. In: Information Security. Springer International Publishing, Cham, pp. 402–422.

Qasim, S.A., Smith, J.M., Ahmed, I., 2020. Control logic forensics framework using built-in decompiler of engineering software in industrial control systems. Forensic Sci. Int.: Digit. Invest. 33, 301013.

Rais, Muhammad Haris, Muhammad, Ahsan, Vaibhav, Sharma, Radhika, Barua, Rob, Prins, Irfan, Ahmed, Jason, Staggs, Sujeet, Shenoi, 2022. In: LOW-MAGNITUDE INFILL STRUCTURE MANIPULATION ATTACKS ON FUSED FILAMENT FABRICATION 3D PRINTERS. Critical Infrastructure Protection XVI, Springer Nature Switzerland, Cham, ISBN 978-3-031-20137-0, pp. 205–232. https://doi.org/10.1007/978-3-031-20137-0_8.

Rais, M.H., Awad, R.A., Lopez, J., Ahmed, I., 2021a. Jtag-based plc memory acquisition framework for industrial control systems. Forensic Sci. Int.: Digit. Invest. 37, 301196. https://doi.org/10.1016/j.fsidi.2021.301196. https://www.sciencedirect.com/science/article/pii/S2666281721001049.

Rais, M.H., Li, Y., Ahmed, I., 2021b. Dynamic-thermal and localized filament-kinetic attacks on fused filament fabrication based 3d printing process. Addit. Manuf., 102200 https://doi.org/10.1016/j.addma.2021.102200. https://www.sciencedirect.com/science/article/pii/S2214860421003614.

Rais, M.H., Li, Y., Ahmed, I., 2021c. Spatiotemporal g-code modeling for secure fdm-based 3d printing. In: Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems, ICCPS '21. Association for Computing Machinery, New York, NY, USA, pp. 177–186. https://doi.org/10.1145/3450267.3450545.

Rais, M.H., Awad, R.A., Lopez Jr., J., Ahmed, I., 2022. Memory forensic analysis of a programmable logic controller in industrial control systems. Forensic Sci. Int.: Digit. Invest. 40, 301339.

Raju, B.K.S.P.K., Geethakumari, G., 2016. An advanced forensic readiness model for the cloud environment. In: 2016 International Conference on Computing, Communication and Automation. ICCCA, pp. 765–771. https://doi.org/10.1109/CCAA.2016.7813819.

Rowlingson, R., et al., 2004. A ten step process for forensic readiness. Int. J. Digit. Evid. 2 (3), 1–28.

Saidi, R.M., Ahmad, S.A., Noor, N.M., Yunos, R., 2013. Windows registry analysis for forensic investigation. In: 2013 the International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE). IEEE, pp. 132–136.

Senthivel, S., Ahmed, I., Roussev, V., 2017. Scada network forensics of the pccc protocol. Digit. Invest. 22, S57–S65.

Singh, B., Singh, U., 2016. A forensic insight into windows 10 jump lists. Digit. Invest. 17, 1–13. https://doi.org/10.1016/j.diin.2016.02.001. https://www.sciencedirect.com/science/article/pii/S1742287616300202.

Singh, A., Ikuesan, A.R., Venter, H.S., 2019. Digital forensic readiness framework for ransomware investigation. In: Breitinger, F., Baggili, I. (Eds.), Digital Forensics and Cyber Crime. Springer International Publishing, Cham, pp. 91–105.

Spoerk, M., Gonzalez-Gutierrez, J., Sapkota, J., Schuschnigg, S., Holzer, C., 2018. Effect of the printing bed temperature on the adhesion of parts produced by fused filament fabrication, Plastics. Rubber Compos. 47 (1), 17–24. https://doi.org/10.1080/14658011.2017.1399531 arXiv:

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (iot) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials 22 (2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586.

Sturm, L., Williams, C., Camelio, J., White, J., Parker, R., 2014. Cyber-physical vunerabilities in additive manufacturing systems. Context 7 (8), 951–963.

Valjarevic, A., Venter, H., 2013. Implementation guidelines for a harmonised digital forensic investigation readiness process model. In: 2013 Information Security for South Africa, pp. 1–9. https://doi.org/10.1109/ISSA.2013.6641041.

van de Wiel, E., Scanlon, M., Le-Khac, N.-A., 2018. Enabling non-expert analysis of large volumes of intercepted network traffic. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics XIV. Springer International Publishing, Cham, pp. 183–197.

Yampolskiy, M., Horvath, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J., 2013. Taxonomy for description of cross-domain attacks on cps. In: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, HiCoNS '13. Association for Computing Machinery, New York, NY, USA, pp. 135–142. https://doi.org/10.1145/2461446.2461465.

Yampolskiy, M., King, W.E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A., Elovici, Y., 2018. Security of additive manufacturing: attack taxonomy and survey. Addit. Manuf. 21, 431–457. https://doi.org/10.1016/j.addma.2018.03.015.

Yu, W., Wang, X., Ferraris, E., Zhang, J., 2019. Melt crystallization of pla/talc in fused filament fabrication. Mater. Des. 182, 108013. https://doi.org/10.1016/j.matdes.2019.108013. https://www.sciencedirect.com/science/article/pii/S0264127519304514.

Zubair, N., Ayub, A., Yoo, H., Ahmed, I., 2022. Pem: remote forensic acquisition of plc memory in industrial control systems. Forensic Sci. Int.: Digit. Invest. 40, 301336.