Side-Channels of Cyber-Physical Systems: Case Study in Additive Manufacturing

Sujit Rokka Chhetri, Mohammad Abdullah Al Faruque
University of California, Irvine

February 28, 2017

Abstract

Cyber-physical systems are prone to information leakage from the physical domain. The analog emissions such as vibration, acoustic, magnetic, and power can turn into side-channels revealing valuable cyber-domain data. An attacker capable of monitoring these analog emissions can determine the correlation between the emissions and the cyber-domain data and leverage this relation to breach the confidentiality of the system. Thus, in order to secure the system, detection of these side-channels is of paramount importance. In our work, we perform the leakage analysis on emission such as vibration, acoustic, magnetic, and power from cyber-physical additive manufacturing system. By doing so, we will effectively reveal various side-channels of the system, and highlight the importance of performing similar analysis during design time to secure the cyber-physical system.

Keywords
Cyber-Physical Systems, Security and Privacy, Side-Channels, Additive Manufacturing, Confidentiality

1 Introduction

In Cyber-Physical Systems (CPS), computational and communication cores, governed by cyber-processes, interact with physical-domain sensors and actuators. This interaction, however, has inherent vice and virtue. On one hand, it allows us to design systems capable of efficiently interacting with their surrounding, and in the other, it opens up possibilities for unique vulnerabilities [1] posing serious challenges to the system security. For example, as the information flow in the cyber-domain manifests physically in the form of energy flows in the physical-domain, it may be leaked. These energy flows may be observed in the form of various analog emissions such as *vibration, acoustic, magnetic, power*, etc. These mediums, through which unintentional leakage of information occurs, are also known as side-channels. Side-channels pose a serious threat to the *confidentiality* of the system as they may indirectly reveal the cyber-domain data. They have been previously used to break the cryptographic protocols, where attackers, rather than using brute force or attacking theoretical weakness of the algorithms, used side-channels to infer about the various system states in the cyber-domain [2]. In CPS, various side-channels may emerge due to the tight integration of cyber and physical domain components. Hence, it is important to analyze the possibility of existence of side-channels by analyzing all the observable energy flows to better secure the system. There have been various studies in understanding the information leakage in CPS [3]. However, in this article we focus on analysis of multiple analog emissions from cyber-physical additive manufacturing system to further highlight the problem of maintaining confidentiality in CPS, and encourage research in exploring side-channels to strengthen the security of the cyber-domain data.

Additive manufacturing (also known as 3D-Printers) has gained popularity due to its capability to rapidly prototype free form 3D-objects layer by layer. Wohlers forecasts that by 2020 additive manufacturing industry will generate more than $20 billion in revenue [4]. It has already been adopted in aerospace, automotive, and medical industry. However, due to its widespread, analyst group Garnter predicts that by 2018 3D printing will result in global loss of at least $100 billion per year in Intellectual Property (IP) [5]. Besides, several security challaneges for additive manufacturing have also been covered [6]. However, our work was the first to demonstrate the vulnerability of 3D-Printers to side-channel attack [7], and it was also recently reported by the Science magazine [8]. The IP in additive manufacturing consist of *geometry* of 3D-objects, *process information* (such as specific technology used), and *machine information* (such as tuning parameters for the machine) [9]. There are various types of 3D-Printers. However, Fused Deposition Modeling (FDM) technique based 3D-Printers, which deposit thermoplastic heated slightly above its melting point, are the most widely used for prototyping of plastic 3D-objects, or visualizing 3D-objects before they are sent for production. Hence, as a case study we will analyze the analog emissions from a FDM based 3D-Printer, and demonstrate how they can be used to reverse engineer the geometry of a 3D-object, potentially resulting in IP theft. Moreover, we will present a threat model that highlights IP theft during the prototyping stage, where FDM based 3D-Printers are mostly used. Securing information at this phase is crucial because the design prototypes are normally not patented during this stage, and information theft can cause the company to lose their investment in research and development of the product.

1.1 Cyber-Domain Data in Additive Manufacturing

In our threat model, even though cyber-domain data consist of any information present in the cyber-domain (for example STL, G/M-codes, firmwares, etc.,), only data consisting of the geometry of the 3D-design is considered. In additive manufacturing, the 3D design of an object is first visualized and converted to STereo-Lithography (STL) file using computer-aided design tools. Then Computer-Aided Manufacturing(CAM) tools are used to slice the STL files into layer by layer geometry description files. Then the tool-path generation algorithms selects the most efficient path (either shortest or in specific pattern to strengthen the mechanical structure) to traverse to print each layer. As a result G/M-codes are produced by the CAM tool. M-codes consist of process information such as temperature, extruder max speed, cooling fan control, etc., whereas, the G-code consist instruction to control the movement of the nozzle. Hence, throughout the digital process chain, the cyber-domain data in additive manufacturing changes its form from 3D design specification to STL file, and eventually to G/M-codes. A sample G-code, such as $G1\ F100\ X10\ Y10\ Z10\ E10$, consist of information about the travel feed-rate F in *mm/minute*, XYZ-axis coordinates in *mm*, and extrusion length E in *mm*. Hence, the IP inherent in the geometry is also present in G/M-codes, and by reverse-engineering these G/M-codes attackers will mostly likely be able to reconstruct the 3D-object. The G/M-codes consist of various parameters describing speed (V), distance (L), Axis (A), and direction (D) on each of the three axes, as well as extrusion amount (E) of the thermoplastic and temperature of the heating element (T). From an attacker's perspective the G-code can be abstracted as an angle of the line segment (θ) moving in XY-plane, travel feed-rate (V), change of layer (δ_{layer}), change of line segment(δ_{line}), extrusion amount, etc. All these cyber-domain data however, should be able to describe the geometry of the 3D-object.

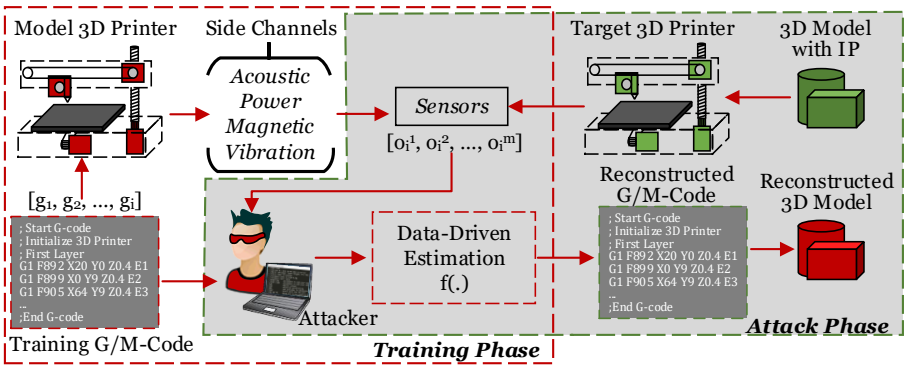

Figure 1: **Side-Channel based Threat Model.**

2 Threat Model

In our threat model (shown in Figure 1), out of various IP information, we focus on analyzing leakage of geometry information of the 3D-objects through the side-channels. For an attacker to carry out a successful attack to breach the confidentiality, the threat model should consist of three major components [10] described as follows:

1. *Threat Susceptibility:* 3D-Printers consist of various physical components. These components are actuated by the printer firmware based on the G/M-codes. While actuating, energy flows are modified and various analog emissions are emitted by the printer due to its physical property. Some of these analog emissions are unintentional and not considered as a source of information leak during design time. If these unintentional emissions have correlation (high mutual information) with the G/M-codes, they will act as side-channels and make the system susceptible to confidentiality breach by revealing the cyber-domain data $(V, L, A, D, E, T, \theta, \delta_{line}, \delta_{layer})$.

2. *Threat Accessibility:* In our threat model, we focus on non-intrusive methods in which an attacker can acquire the observable emissions from the side-channels. This includes placement of sensors such as microphone, hall effect, accelerometer, current clamp, etc., to acquire the signals $[o_1^m, o_2^m, \ldots, o_t^m]$, where m represents the specific side-channel. An attacker may simply place the sensors close to the 3D-Printer unbeknownst to the user, while they are prototyping 3D-objects. Moreover, an attacker may be an insider with a low level access to the 3D-Printer (who can only afford to be physically close to the system) or someone paid by other competing companies. We assume that an attacker has initially performed the space exploration for the optimal type (sampling rate, resolutions, etc.) and position (for example distance and angle) of the sensors for the data acquisition.

3. *Threat Capability:* Before exploiting the analog emissions, an attacker needs to determine if they can model a function $f(.)$ that can explain the relation between the analog emission and the cyber-domain data. This modeling can be done in two ways. The first methods involves modeling the physical properties using existing models (such as mechanical, electrical, etc.). However, this method is complex, and cannot encompass mechanical degradation and dynamic interaction with the environment (which are hard to predict during the design time). In the second method, an attacker can estimate the function $\hat{f}(.)$ using data-driven estimation. In such scenario, the attacker may use two steps in breaching the confidentiality of the system. The first stage, also called training phase, consist of an attacker using training G/M-codes $[g_1, g_2, \ldots, g_i]$ to acquire the analog emissions $[o_i^1, o_i^2, \ldots, o_i^m]$ corresponding to each G/M-code g_i from the potential m side-channels of the target system using a similar

model of the system. Using these data, a model function is estimated. In the next stage, called attack phase, the attacker collects all the analog emissions emitted during printing of the 3D models, and uses the estimated model functions to predict the G/M-codes. Rather than estimating model functions to map the relation of each G/M-code instructions, model functions are rather estimated for the specific parameters ($V, L, A, D, E, T, \theta, \delta_{line}, \delta_{layer}$) inherent in the G/M-code. The estimated function is specific to the given model of 3D-Printer, however, the estimation method remains same for all the 3D-Printers, slicing algorithms, and tool-path generation algorithms.

3 Leakage Analysis

In leakage analysis, the relation between the observable analog emissions and the cyber-domain data is evaluated. Let $G \rightarrow O^m$ represents the side-channels, where G represents random variable consisting of G/M-codes and O^m represent random variables for emissions from multiple channels. The G/M-code is further partitioned into random variables $[V, L, A, D, E, T, \theta, \delta_{line}, \delta_{layer}]$ for analyzing the relation between the individual parameters and the emissions rather than the whole G/M-code. For the leakage analysis, we analyze the mutual information between these variables to demonstrate the dependency among each other. Let $f_(g)$ represent the probability distribution function at g, and $f(o)$ represent the probability distribution function at o. Then, the entropy of each of these random variables can be calculated as: $H(G) = -\sum_{g \in G} f(g) log_2 f(g)$ and $H(O^m) = -\sum_{o \in O} f(o) log_2 f(o)$. If $f(g, o)$ and $f(g|o)$ are the joint and conditional probabilities of the random variables, then the conditional entropy $H(G|O^m)$ is calculated as: $H(G|O^m) = -\sum_{o \in O^m} \sum_{g \in G} f(g, o) log_2 f(g|o)$. The conditional entropy measures the amount of information required to describe the outcome of random variable G given the information about the random variable O^m. Then, the additional information required to reconstruct G will be directly related to the mutual information calculated as $I(G; O^m) = H(G) - H(G|O^m)$. The unit of mutual information is *bits*. When the random variables have high entropy, they have higher *bit* value. Mutual information can also be explained in terms of percentage of the total *bits*. For example, let a random variable X have 1 *bit* as its total entropy. Let the mutual information between random variables X and another random variable Y be 0.5 *bit*. Then, mutual information between X and Y can be written as 50%, as observing the random variable Y will reduce the entropy of the random variable X by 50%. Higher the mutual information, higher is the relation between the two random variables.

3.1 Success Rate

The mutual information gives an attacker an idea about the relation between the observable analog emissions and the G/M-code. However, to exploit the side-channels, they still need to have an accurate model estimation. To understand the vulnerability , success rate of an attacker needs to be calculated. In this paper, we will define the success rate as the capability of an attacker to accurately estimate each of the parameters of the G/M-code. Let us define a variable e_i, such that $e_i = 1$ when $|g_i - \hat{f}(o_i^m)| \leq \triangle_e$, and 0 otherwise. $\hat{f}(o_i^m)$ is as model function predicting the G/M-code (more precisely the parameters $V, L, D, E, T, \theta, \delta_{line}, \delta_{layer}$), and $\triangle_e$ is the error threshold for which the estimated partial G/M-code can be used to reconstruct the complete G/M-code. Value of $\triangle_e$ should not be greater than the process variation introduced by the 3D-Printer. However, this is only possible in case of a strong adversary. Hence, for the purpose of demonstrating the leakage analysis as a proof of concept, we will relax this constraint and set error threshold to be the most accurate prediction value that can be achieved among all the side-channels with the given threat model. Then, we define success rate in estimating of

G/M-code G as follows:

$$SR_{(m)} = \frac{\sum_{i=1}^{n} e_i}{N} \tag{1}$$

Where N gives the total number of G/M-code instructions used in describing the 3D-object. As mentioned earlier, in this article we will analyze the success rate in terms of how accurately the analog emissions can predict the various parameters of the G/M-code.

4 Analog Emissions

In this section, we will briefly describe the principle behind production of various analog emissions in FDM based 3D-Printers and how it might describe various parameters of G/M-code.

4.1 Vibration

Treating the 3D-Printer as a cartesian robot, the equation describing the general dynamics can be written as follows [11]:

$$M(q)\ddot{q} + C(q,\dot{q})\dot{q} + g(q) + f(\tau,\dot{q}) = \tau \tag{2}$$

where, $q = [q_1, q_2, \ldots, q_n]$ is a vector describing the n joints of the Cartesian robot. $M(q) \in \mathbb{R}^{n\times 1}$ is the inertial matrix, $C(q,\dot{q}) \in \mathbb{R}^{n\times n}$ is the torque matrix, and $g(q) \in \mathbb{R}^{n\times 1}$ is the vector gravity torque, $\tau \in \mathbb{R}^{n\times 1}$ is the torque produced by each of the stepper motors in the joints, and $f(\tau,\dot{q}) \in \mathbb{R}^{n\times 1}$ is the friction vector. Solving equation 2, the natural frequency of the 3D-Printer can be determined. The movement of 3D-Printer however is coordinated and controlled by the G/M-codes. Hence, an attacker may model the relation between the vibration and the various G/M-code parameters to use it as a side-channel. Besides the system vibration, the hybrid stepper motors present in 3D-Printer act a major source of vibration. This is due to the fluctuating radial force acting on the stator core of the stepper motor. This radial forces per unit area can be abstracted and expressed as follows:

$$p_r(\alpha,t) = P_r cos(r\alpha - \omega_r t) \tag{3}$$

where r is the order of the force wave, ω_r is the angular frequency of the force of the r_{th} order, α is the angular distance from the given axis, and P_r is the amplitude of the radial force pressure in N/m^2. The angular frequency of the force depends on the current passing through the winding, which are determined by the G/M-codes. Hence, the vibration in each stepper motor is a direct result of the various parameters of the G/M-code.

4.2 Acoustic

Acoustic emissions are a direct result of vibration produced in the 3D-Printer. However, it is not guaranteed that all the mechanical vibration will produce the acoustic signal. Assuming a cylindrical stator core of the stepper motor, the power radiated from a single hybrid stepper motor can be expressed as follows [12]:

$$P = 4\rho c\pi^3 f^2 {A_{rd}}^2 r l I_{rel} \tag{4}$$

Where P is the radiated sound power (W), ρ is the density of the medium (kg/m^3), c is the speed of the sound in the medium (m/s), f is the excitation frequency of the vibration with multiple harmonics (Hz), A_{rd} is the surface vibratory displacement (m), r is the radius of the cylindrical stator (m), l is the length of the stepper motor (m), and I_{rel} is the relative sound

intensity. I_{rel} depends on the mode of stator vibration R, the radius, and the length-diameter ratio. The radiated sound power is higher when the stepper motor vibrates with the natural oscillation frequency. The stator natural frequency is dependent on the mechanical structure it is attached to, and it is given as follows:

$$\omega_{np}^2 \approx \frac{K_m^{(c)} + K_{mn}^{(f)}}{M_c + M_f} \tag{5}$$

Where $K_m^{(c)}$ is the lumped stiffness of the stator core, $K_{mn}^{(f)}$ is the lumped stiffness of the frame, and M_c and M_f are the mass of the stator and the frame respectively, m is the circumferential vibration mode, and n is the axial vibration mode of the frame. Equation 5 has been derived by assuming that the lumped stiffness of the core and the frame are in parallel. Equation 5 shows that, the mechanical structure to which each stator motor is connected affects the natural frequency. Hence, due to this different stator motors withing the 3D-Printer have the possibility to produce different acoustic signature for similar G/M-code parameters. When the stepper motor is rotating with the harmonic frequency of the natural frequency such as $..., \frac{\omega_{np}}{4}, \frac{\omega_{np}}{3}, \frac{\omega_{np}}{2}, 2\omega_{np}, 3\omega_{np}, 4\omega_{np}, ...$ the vibration is more prominent due to resonance. Apart from radial stator vibration, torque ripple also introduces vibration in the stepper motor. Even though microstepping is used to minimize the ripple, due to non-conformity of the microstepping to ideal sine waves, some torque ripples are still introduced in the rotor of the stepper motor.

4.3 Magnetic

Production of magnetic field in any device where there is varying electric field is given by the Maxwell-Ampere's equation as follows:

$$\nabla \times \vec{\mathcal{H}} = \vec{\mathcal{J}}_f + \frac{\partial \vec{\mathcal{D}}}{\partial t} \tag{6}$$

Where $\vec{\mathcal{H}}$ denotes the magnetic field intensity in A/m, $\vec{\mathcal{J}}_f$ denotes current density in A/m^2, and $\vec{\mathcal{D}}$ represents electric flux density expressed in C/m^2. 3D-Printer consist of four to five stepper motors to enable movement in X, Y, and Z axes. Each of them rely on varying current (controlled by G/M-codes) flowing through the stator to produce the mechanical force necessary for the movement of the rotor core. Besides the stepper motors, there are various conductors where the variable rate of current flow through them. All of these components produce magnetic field, which can be used an attacker to learn about the cyber-domain data.

4.4 Power

The major components consuming power in 3D-Printer are heating element, stepper motors, DC motor fan, heated bed, and the main circuit board itself. Out of all these components the stepper motor has fluctuating power consumption depending on the varying current passing through it's stator winding. For two phase hybrid stepper motors the electrical model can be written as follows:

$$v_A = i_A R + L_A \frac{di_A}{dt} + M \frac{di_B}{dt} + e_A \tag{7}$$

$$v_B = i_B R + L_B \frac{di_B}{dt} + M \frac{di_A}{dt} + e_B \tag{8}$$

Where, i_A and i_B are the current flowing through the coil A and B of the two phase stepper motor, L_A and L_B are the coil inductance, v is the terminal voltage, e is the back electromotive force (emf), and M is the mutual inductance between coil A and B. The instantaneous power consumption by the motor is given by $\int_0^t V \times i dt$. Most of these 3D-Printers have constant

voltage DC power supply. Hence, a DC current clamp can be placed to monitor the varying current flow to determine the power consumption in the 3D-Printer based on various parameters of the G/M-code.

5 Experimental Results

To perform the leakage analysis, in our experiment we will present two versions of the threat model described in Section 2. In the first, the major focus will be in acoustic analog emissions, and how various parameters in the G/M-codes can be extracted. We will then present an example of the reconstruction of the 3D-object. The 3D-Printer chosen for the experiment is Printrbot simple wood version. The audio recorder (which can be a smart phone) is placed at 20 cm from the 3D-Printer at an angle of 45^o to the X and Y axis. The audio is recorded at 96 kHz sampling frequency, it is passed through digital band pass filter (with pass band between 100 Hz and 20 kHz) to remove high and low frequency noise. Then various time and frequency domain features such as *zero crossing rate (f1)*, *Energy Entropy (f2)*, *Spectral Entropy (f3)*, and *Mel Frequency Cepstral Coefficients (MFCC) (f4-f10)* are extracted by dividing the audio into a fixed size frame of 10-50 ms. The number of features extracted depends on the number of MFCCs. Based on this setup, we performed the leakage analysis to determine the relation between the various parameters and the acoustic analog emission.

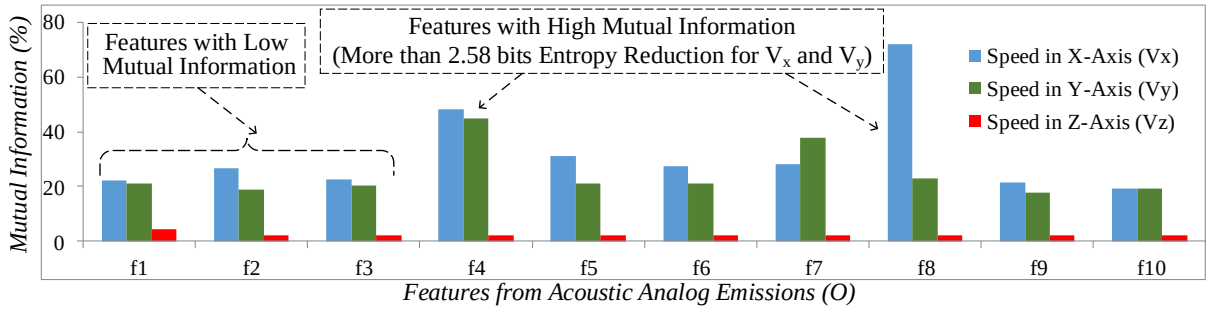

Figure 2: **Mutual Information between Features from Acoustic Signals and Speed .**

Speed (V): In order to analyze the mutual information between the random variable $V = [V_x, V_y, V_z]$ and the acoustic emission, the speed is varied from 1000 $mm/minute$ to 4500 $mm/minute$ with the step size of 100 $mm/minute$. V_x, V_y, and V_z represent speed in each of the axes. Assuming uniform distribution, the total entropy of the speed is $log_2(36) \approx 5.17$ bits. This range is specific to the given Printrbot 3D-Printer. As seen in Figure 2, the mutual information between various features and the V_x, V_y is larger compared to V_z. This is expected as for the given 3D-Printer, speed in Z-axis does not vary and is constant. The high mutual information is due to the fact that to increase the angular speed of the stepper motor, the stepping rate is increased. This in turn increases the frequency of the radiated force acting upon the stator of the stepper motor. Hence, the stator vibrates with hgher frequency. Using similar results and more features (210 *in total*) with higher mutual information, we were able to design an attack model to reconstruct the 3D-object by just utilizing acoustics side-channel.

Table 1: **Mutual Information Between Acoustic Signal Features and Axis (A).**

	Mutual Information (%)									
Parameters/Features	$f1$	$f2$	$f3$	$f4$	$f5$	$f6$	$f7$	$f8$	$f9$	$f10$
A	52.79	74.64	16.38	67.35	57.71	62.81	62.80	83.24	62.80	67.36

Axis (A): For measuring the leakage of axis information, mutual information between random

variable A and various features is calculated. Since there are 3 axis movement (X, Y, Z), the entropy is $log_2(3) \approx 1.58$ $bits$. As expected, higher mutual information is obtained for the axis information. We can also notice that the same feature $f2$ that had lower mutual information with speed ended up having higher mutual information with the axis. The variation in acoustic emissions is due to the fact that even though the same stepper motors might have been used in the 3D-Printer, most of the time the loads carried by each of the stepper motor is different. Furthermore, the mechanical structure to which the various X, Y and Z stepper motors are attached to are also different. Variation in the load affects the rotor oscillation and the vibration, whereas, the variation in the mechanical structure affects the natural frequencies as given by equation 4. Hence, this results in variation in the amplitude of frequency components of the vibration of the stepper motors even when they are rotating with the same angular speed.

Direction (R) and **Extrusion (E):** When the 3D-Printer's nozzle is moving in X and Y direction, the intensity of the sound decreases drastically with the square of the distance from the sound source. If P is the power of the sound source and r is the distance from the sound source then we have: $I = \frac{P}{4\pi r^2}$. It is trivial to show that, during single axis movements the direction of the nozzle will be leaked in the acoustic side-channel by the intensity of the sound. However, during multiple axis movement too, variation in the natural frequencies of the various stepper motor core due to mechanical frame and load can be leveraged to monitor intensity of specific frequencies unique to the stepper motor for deciphering the direction. The extrusion amount depends on the nozzle speed, layer height (movement in $Z - axis$) and the nozzle diameter. Layer height and the nozzle diameters are fixed for the given 3D-Printer, and nozzle speed can be calculated by monitoring the V_x and V_y. Furthermore, it just remains to classify if the printer is extruding the thermoplastic or just aligning the nozzle. However in state-of-the-art tool-path generation algorithms, to improve the printing time, aligning motion occurs with a high speed in 3D-Printer. Hence, the task of classifying whether the printer is extruding or not becomes the task of finding the printing speed. Nevertheless, the extruder motor is active during printing, and acoustic emissions (collected using better sensors) from it may be used to determine if the printer is printing or just aligning.

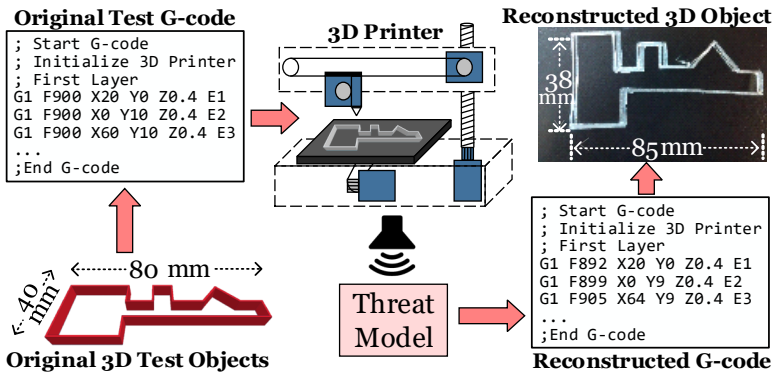

Figure 3: **Acoustic Side-Channel Attack on 3D-Printer [7].**

Based on the extracted features, multivariate regression learning algorithms were used to estimate the speeds in various axis, and multivariate classification learning algorithms were used to estimate the axis movement. And the test was performed on simple test objects such as square, triangle, and key like structure (printed at lower travel feed-rate of 900 mm/min) with five layers (see Figure 3). The average mean absolute percentage error for the regression models was 17.82%, and average accuracy for the classification was 78.35%. Moreover, the perimeter accuracy for reconstructing the key like structure was 89.72% (for details see our

previous work [7]).

In the second version of the threat model, rather than reconstructing the whole 3D object, we calculated the success rate in terms of accuracy in predicting the parameters of the G/M-code such as θ, δ_{line}, and δ_{layer}. Where $\delta_{line} \in \{0, 1\}$ and $\delta_{layer} \in \{0, 1\}$, with 1 denoting change of either the line segment or the layer. We also upgraded the 3D-Printer to Printrbot simple metal with higher average travel feed-rate. In desktop 3D-Printers the average printing speed is normally fixed to achieve the best quality. This speed is specific for each of the 3D-Printers. Assuming that an attacker has this knowledge, then the threat model just needs to estimate the parameters θ, δ_{line}, and δ_{layer}. For these parameters, we varied the angle from 0^o to 360^o with a step angle of 9^o, and calculated the mutual information for a travel feed-rate of 2400 *mm/min* which is around the average travel feed-rate. We used acoustic sensor (*Audio-Technica AT2021*), AC/DC current clamp (*PIC0 TA018*) for power measurement, magnetic field sensor (*HMC5883L*), and accelerometer (*uxcell ADXL335*) for vibration measurement. As features, 501 power spectral density values are extracted for all the analog emissions after passing it through low pass filter with cut-off frequency of 10 kHz. For calculating a single mutual information value, principal component analysis is performed on the 501 features, and the mutual information between the first principal component and the G/M-code parameters is performed. From the experiment we found that $\triangle_e$ for the angle prediction (θ) is 3^o, which is the average accuracy for the estimated functions using vibration analog emission. This error may be reduced if the step angle is reduced during the training phase of the threat model. The mutual information value and the success rate for this experiment is presented in Table 2. From the table it can be observed that the vibration analog emission has highes mutual information and success rate for predicting the angle θ, magnetic emissions has the highest mutual information and success rate for detecting both the change of layer (δ_{layer}) and change of line segment (δ_{line}). Out of all the analog emissions, the power signal reveals the least information about the parameters θ, δ_{line}, and δ_{layer} of the G/M-code.

Table 2: Mutual Information and Success Rate.

	Acoustic	Power	Vibration	Magnetic
θ	2.1732	1.0555	2.6203	2.2438
δ_{line}	0.0019	0.0013	0.0014	0.0320
δ_{layer}	0.0022	0.0003	0.0010	0.2843

Entropy(θ)=5.32 bits *Entropy(δ_{line})=1 bit* *Entropy(δ_{layer})=1 bit*

(a) Mutual Information (in bits)

	Acoustic	Power	Vibration	Magnetic
θ	0.5761	0.0978	0.7522	0.6729
δ_{line}	0.4622	0.5793	0.3536	0.9581
δ_{layer}	0.4746	0.5467	0.4068	0.8318

Complete Success=1

(b) Success Rate

6 Summary

This article provides an insight into how various analog emissions of cyber-physical additive manufacturing system have the potential to become a side-channel and reveal various cyber-domain information. As a case study, fused deposition modeling based 3D-Printer is selected, and analog emissions such as *vibration, acoustic, magnetic,* and *power* are analyzed. We demonstrate how acoustic analog emissions in itself can behave as a side-channel and reveal parameters such as speed, direction, axis, extrusion, etc. Moreover, we also present how different analog emissions reveal cyber-domain data in a controlled experiment. This work serves as a proof of concept for necessity of exploring different analog emissions of cyber-physical systems that are capable of leaking information and weakening the *confidentiality* of the system.

References

[1] M. Al Faruque, F. Regazzoni, and M. Pajic, "Design methodologies for securing cyber-physical systems," in *Proceedings of the 10th International Conference on Hardware/Software Codesign and System Synthesis*, pp. 30–36, IEEE Press, 2015.

[2] F.-X. Standaert *et al.*, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology-EUROCRYPT 2009*, pp. 443–461, Springer, 2009.

[3] L. Feng, "Quantification of information flow in cyber physical systems," PhD Thesis, Missouri University of Science and Technology, 2015.

[4] T. Wohlers, "Wohlers report 2014-3D printing and additive manufacturing-state of the industry," *Wohlers Associates*, 2014.

[5] J. Rivera, "Gartner reveals top predictions for it organizations and users for 2014 and beyond," 2013. http://www.gartner.com/newsroom/id/2603215.

[6] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3d printing," *JOM*, pp. 1–10, 2016.

[7] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *International Conference on Cyber-Physical Systems (ICCPS)*, IEEE, 2016.

[8] M. Hvistendahl, "3D printers vulnerable to spying," *Science*, vol. 352, no. 6282, pp. 132–133, 2016.

[9] M. Yampolskiy *et al.*, "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*, p. 7, ACM, 2014.

[10] J. Hughes and G. Cybenko, "Three tenets for secure cyber-physical system design and assessment," in *SPIE Defense+ Security*, International Society for Optics and Photonics, 2014.

[11] P. Sánchez-Sánchez and F. Reyes-Cortés, *Cartesian Control for Robot Manipulators*. INTECH Open Access Publisher, 2010.

[12] L. T.-P. Timár-P and P. Tímár, *Noise and vibration of electrical machines*, vol. 34. North Holland, 1989.

Sujit Rokka Chhetri Sujit Rokka Chhetri is a PhD candidate pursuing Computer Engineering at the University of California Irvine. His research is focused on big data analysis, sensor fusion, data-driven modeling, and security of Cyber-Physical Systems. He received Distinguished Best Poster Award at NDSS 2016.

Mohammad Abdullah Al Faruque is currently with the University of California Irvine (UCI), where he is a tenure track assistant professor. He received his BSc degree in CSE from the Bangladesh University of Engineering and Technology (BUET) in 2002, and the MSc and PhD degrees in CS from Aachen Technical University and Karlsruhe Institute of Technology, Germany, in 2004 and 2009, respectively. He received best paper awards at DATE 2016, DAC 2015, and ICCAD 2009 among others. Dr. Al Faruque is the recipient of the IEEE CEDA Ernest S. Kuh Early Career Award 2016.