11th International Conference on Micro Manufacturing
Orange County, California, USA, March 2016

Paper#

Attacks on Confidentiality of Additive Manufacturing Systems using Acoustic Side-Channel

Sujit Rokka Chhetri[1], Mohammad Abdullah Al Faruque[1]

[1] *Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA*

Abstract

Acoustics emanated from the additive manufacturing systems, such as 3D-printers, carry process information that can be used to breach the confidentiality of the system. Moreover, this is an example of a physical-to-cyber domain attack, where information gathered from the physical domain, such as acoustic side-channel of a 3D-printer, can be used to reveal information about the cyber domain (such as the G-code used to operate the 3D-printer). To demonstrate the vulnerability of the system to such type of attacks, we are presenting a novel attack model consisting of signal processing, machine learning algorithms, and context-based post-processing. In our experiments, we have successfully conducted the attack by reconstructing the test object and its corresponding G-code with an accuracy of 89.72%. These attacks on confidentiality can pose serious threat to additive manufacturing systems as it can lead to theft of Intellectual Property (IP) and trade secrets.

Keywords: Confidentiality, Side-Channel Attack, Additive Manufacturing, 3D Printer, Security.

1. Introduction

Additive manufacturing systems have gained popularity as a cost-effective solution for automated fabrication due to their rapid capability to prototype 3D objects. In fact, the revenue of the additive manufacturing industry is expected to exceed $21B by 2020 [1]. On the other hand, as per the IBM 2015 security report [2], manufacturing has consistently been among the top three industries facing high security incident rates. Attackers who target additive manufacturing systems are motivated by either industrial espionage of Intellectual Property (IP), alteration of data, or denial of process control [3]. IP in additive manufacturing consists of the internal and external structure of the object, and the machine specific tuning parameters. If these information are stolen, they can be manipulated to harm the image of the company, or even worse, can cause the company to lose its IP. Currently, IP theft mainly occurs through the cyber domain, but IP information can also be leaked through the physical domain (side-channels). A common example of this is to use side-channel information (e.g. acoustics, power dissipation etc.) from devices performing cryptographic computation to determine their secret keys. Recently, we have successfully used the acoustic-side channel to reconstruct the object sent to the 3D-printer [4]. Our novel contribution aids the manufacturing security research by demonstrating the possibility of attack on confidentiality utilizing the acoustic side-channel.

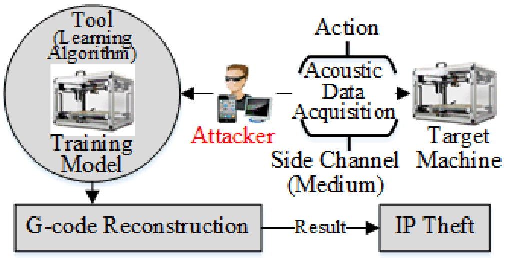


Fig. 1. Proposed Attack Model [4]

2. Attack Model

In our attack model (see Fig. 1), we assume that the attacker can acquire the acoustic side-channel information through a recording device placed at a close proximity to the 3D-printer. To produce a 3D object, design information is supplied to the manufacturing system in the form of G-code. Our attack model consists of different learning algorithms (see Fig. 2.), which analyse the recorded sound to extract specific information.

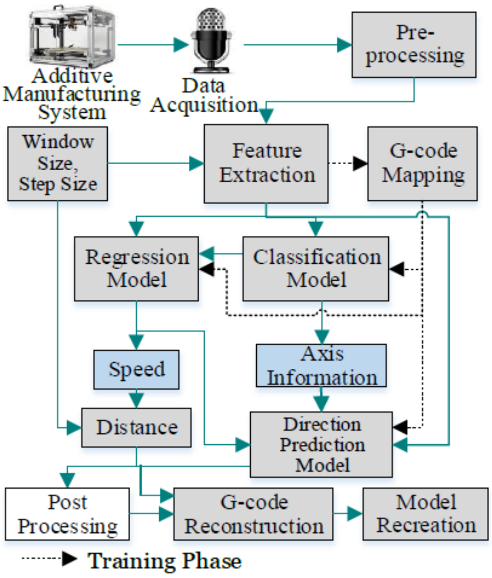


Fig. 2. Our Attack Methodology [4]

The recorded sound is first pre-processed to remove noise, then different time and frequency domain features are extracted from them. During the training phase, the extracted features are mapped to the training G-codes (to label the fingerprints) and fed to the machine learning algorithms. Learning algorithms extract information such as speed, axis of movement, and direction of movement in different axis to re-construct the G-code, and ultimately reconstruct the 3D object.

3. Experiment and Results

Our experimental setup consists of a 3D-printer, audio recorder, and a printer software (see Fig. 3.).

Table 1. Accuracy of Classification Models

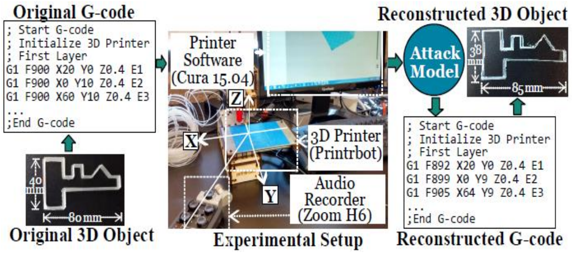
Classifier	Classifying	Accuracy (%)
1	X|Y	99.93
2	Z|Z’	99.86
3	1D|2D	99.88
4	XY_{same}|XY_{Diff}	98.89

We have used classification models to differentiate the axis movement such as 1) X or Y; 2) presence of Z axis movement; 3) movement in one or two axis; and 4) movement in X and Y axis with same speed or different speed. The combined results from these classifiers are used to predict the axis in which the nozzle is moving. The accuracy of each of these classifiers is shown in Table 1. To extract the speed information, we have used regression models. These models predict the speed of the printer in X and Y axis when movement occurs in just one or two axis. Post processing is applied to improve the accuracy by utilizing the fact that printing always occurs in layers.

Table 2. Accuracy of the Regression Models

Regression	Movement Axis	MSE
X	X	0.0061
Y	Y	0.0187
X	X and Y	0.1658
Y	X and Y	0.4290

As a test case, we were able to obtain a perimeter accuracy of 87.92% while using our attack model to reconstruct an outline of a key.



```
; Start G-code
; Initialize 3D Printer
; First Layer
G1 F900 X20 Y0 Z0.4 E1
G1 F900 X0 Y10 Z0.4 E2
G1 F900 X60 Y10 Z0.4 E3
...
;End G-code
```

```
; Start G-code
; Initialize 3D Printer
; First Layer
G1 F892 X20 Y0 Z0.4 E1
G1 F899 X0 Y9 Z0.4 E2
G1 F905 X64 Y9 Z0.4 E3
...
;End G-code
```

Fig. 3. Reconstruction of an Outline of a Key (a Case Study Analysis)

4. Conclusions

Our novel attack model serves as a proof of concept of the serious vulnerability to the confidentiality of the additive manufacturing system to the attacks leveraging acoustic side-channel. For a key as a test case, we have obtained an accuracy of 89.72%. With this, we argue that the security in additive manufacturing systems should incorporate defensive mechanisms against physical-domain attacks as well.

References

[1]T. Wohlers, “3D printing and additive manufacturing-state of the industry,” Wohlers Associates, 2014.

[2] “Cyber security intelligence index.” IBM, 2015.

[3] “Cyber Security for Advanced Manufacturing,” National Defense Industrial Association, 2014.

[4] M. Al Faruque et al, "Acoustic Side-Channel Attacks on Additive Manufacturing Systems", ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'16), Vienna, Austria, April, 2016.