Poster: Exploiting Acoustic Side-Channel for Attack on Additive Manufacturing Systems

Sujit Rokka Chhetri, Arquimedes Canedo[†], Mohammad Abdullah Al Faruque
University of California, Irvine
(schhetri, alfaruqu)@uci.edu, [†]arquimedes.canedo@siemens.com

***Abstract*—Confidentiality, Integrity and Availability (CIA) are the fundamental security requirements for Cyber-Physical Systems (CPS) such as additive manufacturing. However, unlike most security research on CPS, analysis of side-channel for detecting threat towards CIA of additive manufacturing is still at its early stage. In our work, we focus on analyzing the acoustic side-channel of Fused Deposition Modeling (FDM) based additive manufacturing systems, such as 3D-printers, to monitor the leakage of cyber domain information. This leakage can be used to breach the confidentiality inherent in the system, which can lead to the theft of Intellectual Property (IP) and trade secrets. We have found that acoustics emanated from 3D-printers carry process information (such as the G-code) that can be used to reverse engineer and reconstruct the 3D-objects being printed. To demonstrate the attack on confidentiality, we present 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 on confidentiality by reconstructing the test object and its corresponding G-code with an accuracy of 89.72%.**

I. Introduction

Additive manufacturing system build 3D objects in layers. It has gained popularity as a cost-effective solution for automated fabrication due to its rapid prototyping capability. 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. In additive manufacturing systems, confidentiality of internal and external geometry of the 3D objects, process information, and machine information, which are in fact the Intellectual Property (IP) of the system [3], is of paramount importance. An attacker motivated by industrial espionage can breach the confidentiality of the system to manipulate the IP to harm the image of the company, or even worse, cause the company to lose its IP [4]. Currently, security measures for achieving confidentiality have only been considered in the cyber domain through various mechanisms such as authentication, cryptography etc. However, in additive manufacturing systems, information leaking from the physical domain (side-channels) can compromise the confidentiality too. Side-channel information (e.g. acoustics, power dissipation etc.) have already been exploited to determine the secret keys from devices performing cryptographic computation [5]. Recently, we have successfully used the acoustic-side channel to reconstruct the G-code sent to the 3D-printer [6], thus effectively breaking the confidentiality of the system.

II. Attack Model

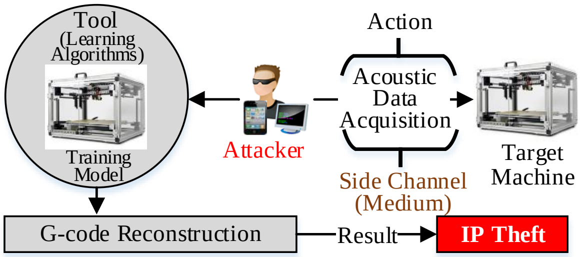


Fig. 1: Proposed Attack Model [6].

In our attack model (see Fig. 1), the attacker acquires the acoustic side-channel information via recording device placed at a close proximity to the 3D-printer. This information is passed to the attack process (see Fig. 2) to reconstruct the G-code sent to the 3D-printer, which carries the design information of the 3D object.

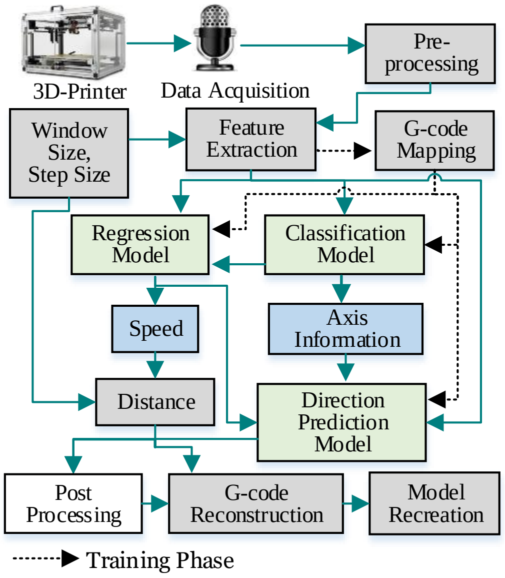
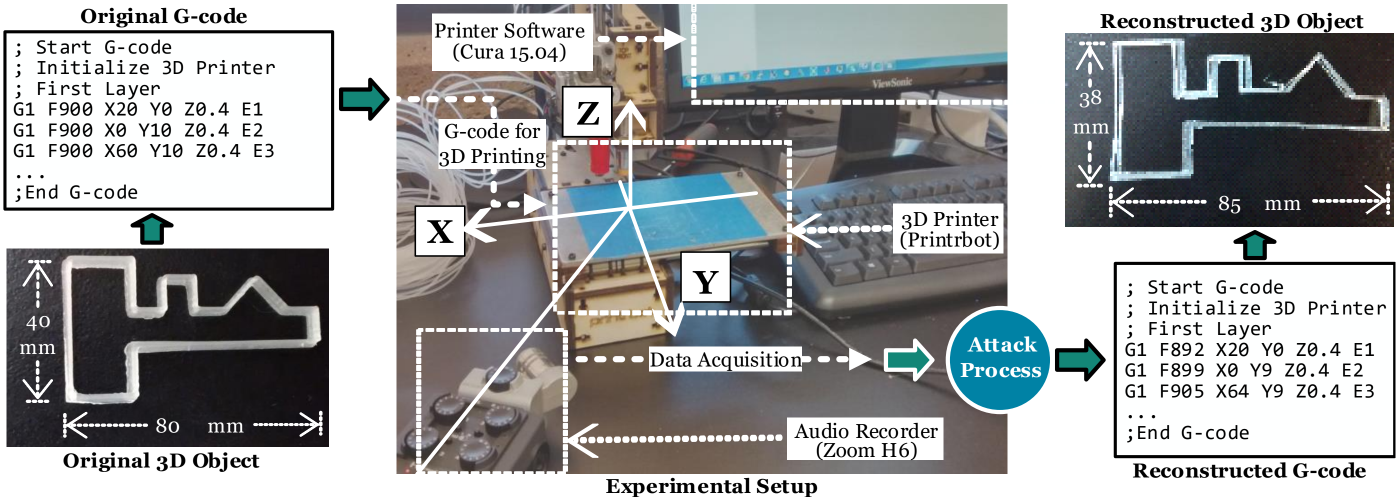


Fig. 2: Our Attack Process and Methodology [6].

Our attack methodology consists of different learning algorithms (see Fig. 2), which analyze the recorded sound to extract specific information about the G-code. The recorded sound is

NDSS '16, 21-24 February 2016, San Diego, CA, USA
Copyright 2016 Internet Society, ISBN 1-891562-41-X
http://dx.doi.org/10.14722/ndss.2016.23xxx



```
; 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).

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. The 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.

III. Experiment and Results

Our experimental setup (see Fig. 3) consists of a 3D-printer, audio recorder, and printer software. The audio device is placed within 20 cm from the 3D-printer at an angle of 45^o to both X and Y axes for better direction prediction.

TABLE I: Accuracy of Classification Models.

Classification Model	Classifying	Accuracy (%)
Φ_1	Z or ~Z Axis	99.86
Φ_2	1D or 2D Axis	99.88
Φ_3	X or Y Axis	99.93
Φ_4	XY_{same} or $XY_{different}$	98.89

We have used classification models to differentiate the axis movement such as 1) either X or Y; 2) presence or absence 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 I.

TABLE II: Accuracy of Regression Models.

Regression Model	Movement Axis	MSE (Normalized)
X	Only X	0.00616
Y	Only Y	0.01874
X	Both X and Y	0.1658
Y	Both X and Y	0.4290

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. The direction of the movement of the nozzle in X or Y axis is predicted using the intensity of the specific frequency components produced by the X and Y stepper motors respectively. Post processing is applied to improve the accuracy by utilizing the fact that printing always occurs in layers. As a test case, we designed an outline of a key (see Fig. 3) to test the accuracy of the attack model when movement occurs in multiple axes. After post processing, we were able to obtain a perimeter accuracy of 87.92% while using our attack model to reconstruct an outline of a key. As shown in Fig. 3, the reconstructed key has a very close resemblance with the original key. In our experiment, the accuracy of the attack model decreases with the increase of the printing speed and decrease of the dimension of object being printed. This is due to the fact that we have used fixed large window size while extracting the features of sound which is unable to distinguish smaller and faster movements.

IV. Conclusion

We have presented a novel attack model that exploits the acoustic-side channel of additive manufacturing systems to compromise its confidentiality by stealing the IP information of the 3D object. This work serves as a proof of concept of the vulnerability of the additive manufacturing system to physical-to-cyber domain attacks. For a key as a test case, we have obtained a perimeter accuracy of 89.72%. With this, we argue that the security in additive manufacturing systems should incorporate defensive mechanisms against not only cyber-domain, but physical-domain attacks as well.

References

[1] T. Wohlers, ”3D-Printing and Additive Manufacturing-State of the Industry,” Wohlers Associates, 2014.

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

[3] M. Yampolskiy, et al. ”Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing.” Proceedings of the 4th Program Protection and Reverse Engineering Workshop. ACM, 2014.

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

[5] Agrawal, Dakshi, et al. ”The EM sidechannel (s).” Cryptographic Hardware and Embedded Systems-CHES 2002. Springer Berlin Heidelberg, 2003.

[6] 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.