

Poster Abstract: Thermal Side-Channel Forensics in Additive Manufacturing Systems

Sujit Rokka Chhetri, Sina Faezi, Arquimedes Canedo[†], Mohammad Abdullah Al Faruque
{schhetri, sfaezi, alfaruqu}@uci.edu
[†]arquimedes.canedo@siemens.com
Department of Electrical Engineering and Computer Science
University of California, Irvine, CA, USA

ABSTRACT

Additive manufacturing systems leak cyber-related information (such as G-code, M-code, etc.) from the side-channels (such as acoustic, power, thermal, etc.). In our work, we have successfully demonstrated the vulnerability of additive manufacturing to thermal side-channel attacks, where confidentiality can be breached to steal the Intellectual Property (IP) in the form of 3D design and printing parameters. We introduce a novel methodology to reverse engineer the thermal images acquired from the thermal side-channel to extract specific information (such as speed, temperature, axis of movement, etc.) present in the cyber-domain. To the best of our knowledge, this kind of forensics has not yet been explored in additive manufacturing systems.

CCS Concepts

•Computer systems organization → Embedded and cyber-physical systems; •Security and privacy → Side-channel analysis;

Keywords

Forensics, Thermal Side-Channel, Additive Manufacturing, 3D-printer, Cyber-Physical Systems

1. INTRODUCTION

Additive manufacturing systems produce 3D objects by fusing materials layer by layer. It has been adopted by several sectors for automated fabrication. However, it faces new and emerging challenges in terms of security and quality control [1]. In our work, we are analyzing the thermal side-channel of the 3D-printers to expose its vulnerability towards attacks on its confidentiality. Infrared radiation is emitted by all objects with temperature above absolute zero. 3D-printer consists of components that emit infrared radiation based on process parameters (such as temperature, nozzle movement in different axis, etc.). Thermal camera can capture this radiation with high accuracy regardless of the lighting condition of the environment, which makes it useful for extracting valuable process parameters accurately.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ICCPS '16 April 11-14, 2016, Vienna, Austria.

© 2016 ACM. ISBN 978-1-4503-2138-9...\$15.00

DOI: 10.1145/1235

2. THERMAL FORENSICS

We have designed a novel methodology to extract and analyze specific information from the 3D-printer (see Figure 1). It uses a pipeline of data acquisition, image processing, and mapping algorithms to extract specific information from the thermal images. We first acquire the thermal video using a thermal camera from a 3D-printer in operation. Next, we extract the initial region of interest, such as nozzle edges, and analyze the changes in its properties in the frame. Then, the mapping algorithms is used to map these changes to the physical movements. Finally, the information extracted by the mapping algorithms is converted into the G-code.

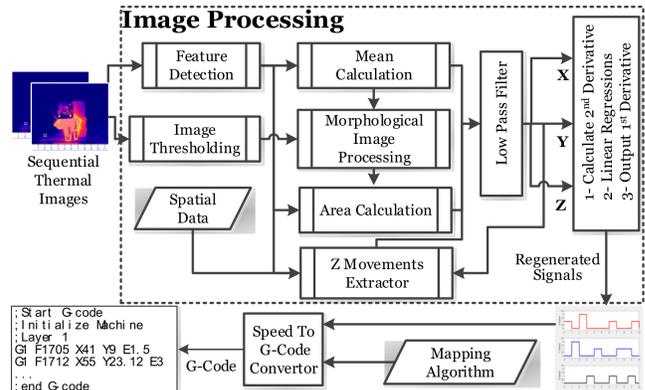


Figure 1: Forensics Methodology for 3D-Printer.

3. RESULTS

From our preliminary work, we have successfully extracted the speed of the nozzle while moving in X and Y axis along with the temperature of the nozzle. With this, we can reconstruct basic shapes involving movement in one axis at a time. Our next step is to analyze the thermal image with multiple axis movements to reconstruct complex 3D objects.

4. CONCLUSION

Our experiment serves as a proof of concept of the fact that various parameters can be extracted from the thermal side-channel of the 3D-printer. This information can be used to carry out attacks on confidentiality of the machine by attackers, or if incorporated as a feedback to the process control block, can improve the quality of the object.

5. REFERENCES

- [1] M. Al Faruque *et al.*, “Acoustic side-channel attacks on additive manufacturing systems,” in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'16)*, Vienna, Austria, April 2016.