Defending Side Channel Attack In Additive Layer Manufacturing Systems

Tech ID: 27617 / UC Case 2016-035-0

BRIEF DESCRIPTION

Additive layer manufacturing systems, also known as 3D printers, are a powerful tool for manufacturers in both rapid prototyping stage and full-scale production. Sensitive intellectual property is carried in the electronic information of the design files utilized by 3D printers. However, the physical characteristics of the machine in operation, including power, temperature, sounds, and motion can also reveal sensitive information that could be used to reverse-engineer a product. The inventors at UCI have demonstrated the threat posed by such side-channel attacks, and have developed countermeasures that obscure information which would otherwise be exposed during printer operation.

FULL DESCRIPTION

Additive layer manufacturing systems, or 3D printers, have become a promising technology for providing cost, time, and space effective solutions by reducing the gap between designers and manufacturers. However, security concerns for the protection of intellectual property have risen along with the widespread use of 3D printers. Relevant intellectual property is carried in the geometric design, material properties, process, and physical machine.[SR1] The inventors at UCI have shown that intellectual property information from the cyber domain (3D models, design files, etc.) can be recovered or reconstructed through non-intrusive attacks during the manufacturing process by recording a range of parameters such as power consumption, temperature profiles, acoustic information, nozzle motion, and electromagnetic emission.

The inventors at UCI have developed measures to prevent side channels from the physical domain to steal intellectual property in the cyber domain. The first measure involves machine-dependent physical process encryption. This measure injects unnecessary information into the control code in order to obfuscate the printing process from simple prediction models used by attackers. The unnecessary information can come in the form of random delays or extra movements of the motors, as well as external noise generators. The second measure is a security-aware, machine-independent 3D printing algorithm to generate a code which controls the printer. Most 3D printing algorithms are simple, being focused on optimizing for speed, material consumption, or power. As such, attackers are easily able to recreate model files from physical information. In order to prevent easy reconstruction, the proposed algorithm will generate control code differently for the same 3D object. Identical products will be made with different printer movements, masking the overall shape to the attackers.

ADVANTAGES

· First demonstration of side channel attack and security

· Sensitive intellectual property is protected on both the algorithm and physical process levels

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	10,511,622	12/17/2019	2016-035

CONTACT

Edward Hsieh
hsiehe5@uci.edu
tel: 949-824-8428.

OTHER INFORMATION

CATEGORIZED AS

- » **Computer**
  - » Security
- » **Security and Defense**
  - » Other
- » **Engineering**
  - » Robotics and Automation

RELATED CASES

2016-035-0

United States Of America	Issued Patent	10,212,185	02/19/2019	2016-035

RELATED MATERIALS

» M. A. Al Faruque et. al. Acoustic side-channel attacks on additive manufacturing systems. International Conference on Cyber-Physical Systems, 2016. - 03/03/2016

UCI Beall Applied Innovation

5270 California Avenue / Irvine,CA 92697-7700 / Tel: 949.824.2683