Survey of Hardware Security in Modern CPU and GPGPU

Meet Udeshi - 14D070007

IIT Bombay

October 14, 2018

Contents

Introduction

- Modern multi-thread, multi-core hardware focus on sharing computing resources among different programs.
- In cloud, VM and sandbox technology is used as software level security measure. But they share the same hardware.
- Programs running on current hardware inevitable leave fingerprints of their execution in power traces, EMI spectrum, caches, etc. [**?**]
- Attackers with knowledge of hardware can obtain these fingerprints and extract sensitive information.

The End