doi:10.1631/FITEE.1800526

题目：基于切换和迁移多执行体架构虚拟机的云侧信道攻击防御技术

概要：云中不同租户的虚拟机共存为以信息泄露为目标的侧信道攻击创造了便利条件。然而，当前绝大多数防御技术都存在通用性或兼容性问题，无法在真实环境下实现快速部署。作为云系统固有功能之一，虚拟机迁移机制可通过在服务器之间迁移虚拟机，限制租户共存，从而提供一种具有应用前景的防御思路。本文首先建立一个统一的攻击模型，攻击者关注的目标是有效侧信道攻击。设计了一种包含多执行架构虚拟机的新型云系统：Driftor。对于其中每个虚拟机，同一时刻有且仅有一个执行体处于运行状态，并通过代理提供服务，以此降低可能泄漏的信息量。为模拟虚拟机迁移机制，系统将在虚拟机不同执行体之前周期性切换运行状态，同时通过真实迁移操作加强防御效果。为解决 CIRCUIT-SAT 求解迁移问题时的弱扩展性，本文提出一种类贪婪算法，通过逐渐扩展必须迁移的虚拟机子集搜索可行解。实验结果表明，Driftor 能有效防御快速侧信道攻击，且针对真实云应用的防御开销较小。

关键词：云计算；侧信道攻击；信息泄露；多执行体架构；虚拟机切换；虚拟机迁移