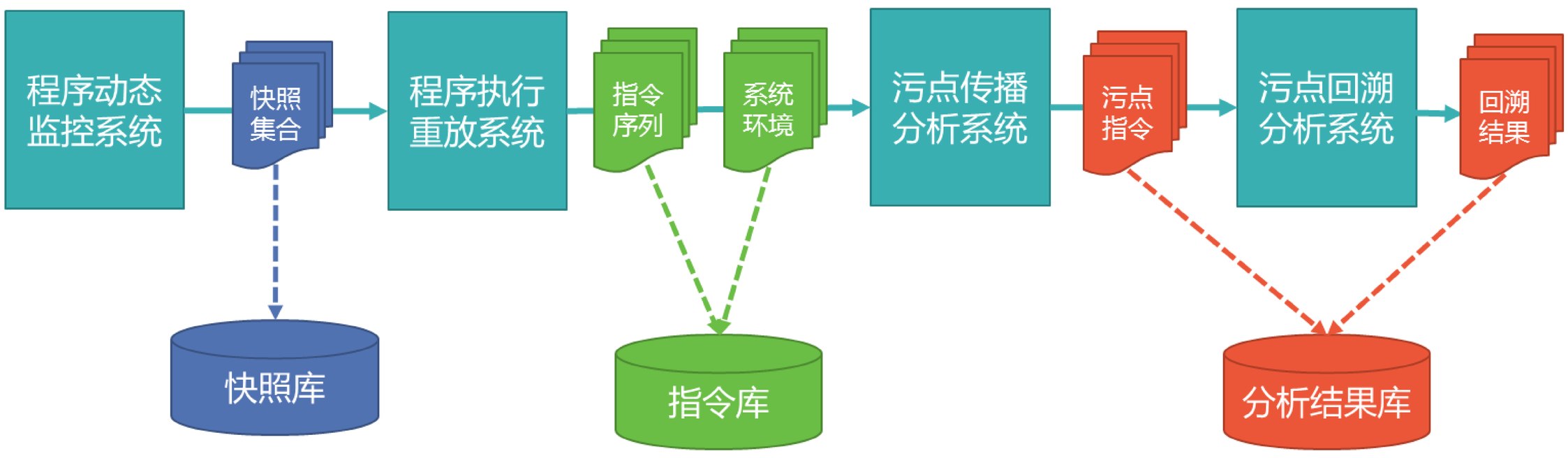
面向应用的污点分析系统
Application Oriented Taint Analysis

苏璞睿、杨轶、和亮、黄桦烽
{purui, yangyi}@iscas.ac.cn

AOTA（Application Oriented Taint Analysis）系统针对软件漏洞分析、恶意代码机理分析、协议逆向分析等工作中对软件逆向分析的需求研发，系统主要包括指令动态提取、污点传播分析、污点回溯分析、程序逆向切片等功能，具备针对Windows XP、Windows 7等操作系统上大型应用软件的动态逆向分析能力。该系统具有如下的技术特性：

1）采用基于硬件虚拟化的动态分析技术，分析透明性高；
2）具有系统级运行记录与重放机制，不受系统随机性影响；
3）基于离线式污点传播分析，时间和空间复杂度低；
4）支持多污点源回溯分析与逆向切片等功能，分析精度高。



AOTA系统得到国家自然科学基金、国家863计划、国家科技支撑计划等多个国家项目的持续支持。目前该系统已经成功应用于针对MS Office、Acrobat Reader、IE浏览器等应用软件的数十个CVE漏洞分析，SandWorm等APT攻击样本的机理分析，以及ZeroAccess、ZeusGameover等僵尸网络协议的逆向分析工作。该系统已经在公安部、部队研究所等多个部门和单位的实际工作中得到部署应用，荣获得军队科技进步二等奖1项。