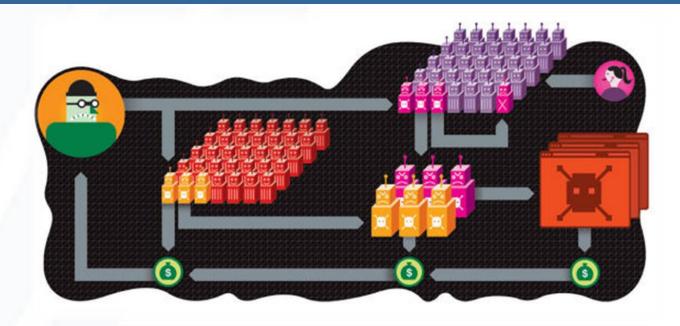


# 云取证技术研究

丁丽萍 中国科学院软件研究所



# 云环境更加脆弱





## 云环境存在的安全问题

黑客入侵云端服务器窃 取数据

云服务供应商内部员工 窃取客户敏感数据

使用同一云服务供应商 的其它客户意外取得或 窃取敏感数据 云端资源遭到恶意滥用 被用来滥发垃圾邮件或 恶意主机等

外国政府可以未经客户 授权读取当地云数据中 心内的数据

客户不易对云服务供应 商的安全控制措施和访 问记录进行审计 云服务供应商灾备管理 不完善导致服务中断

云服务供应商倒闭无法 继续提供服务

用户帐号密码被窃云服 务资源遭到盗用

#### 云环境中的安全需求

## 执行安全需求



用户的任务能够在可信的执行环境中正确地完成

#### 数据安全需求



用户的隐私数据不会被第三方以及恶意的云服务提供商 所窃取

#### 服务安全需求



用户能够在任何时间、任何地点无缝地接入云服务,并且整个接入过程是安全、可靠、可验证的

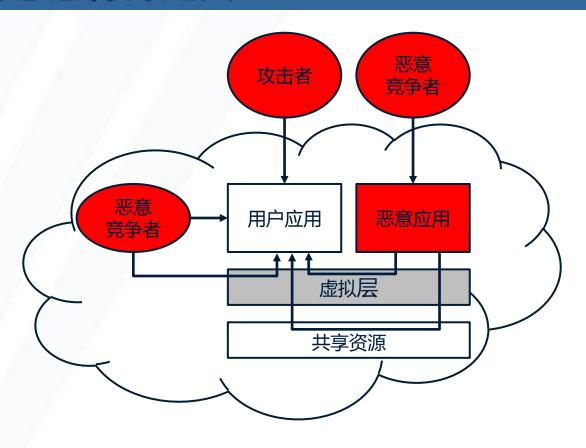
#### 诉讼维权需求



运营商和用户在云环境遭遇了安全事件后,如何获取法庭认可的电子证据提起诉讼,维护自己的合法权益



## 云环境中的恶意行为定义



#### 重要性

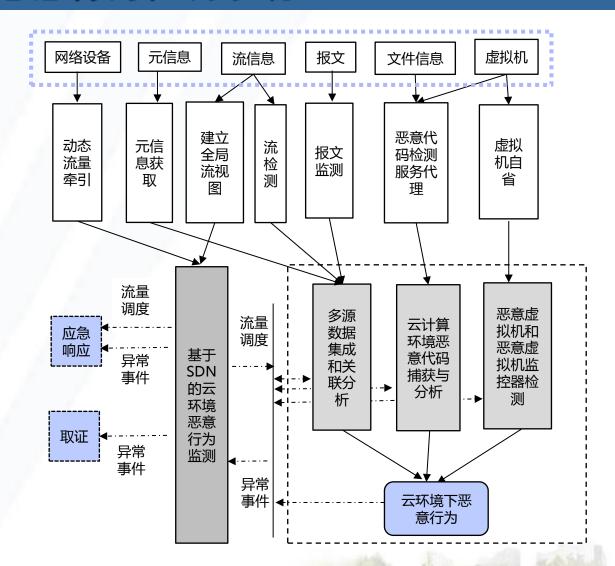
云计算环境下的恶意行为检测与取证技术研究**符合国家政策、时代 发展和科技发展的必然要求** 

云计算环境下的恶意行为检测与取证技术研究是**目前云计算安全 状况的迫切需求** 

> 云计算环境下的恶意行为检测与取证技术研究是**目前云安全、云 取证实践的迫切需求**



#### 云环境下恶意行为检测系统

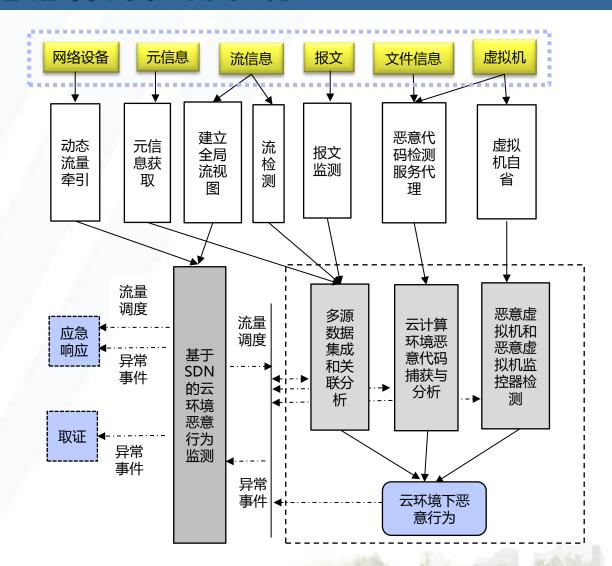


实线:表示数据

虚线:表示控制调度



#### 云环境下恶意行为检测系统

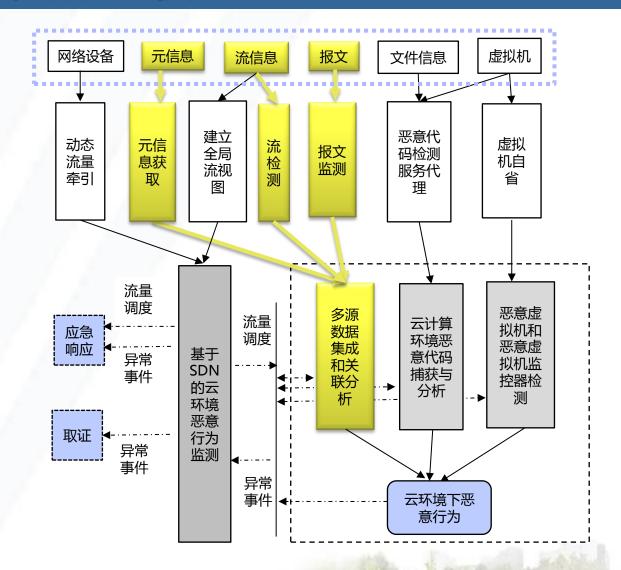


实线:表示数据

虚线:表示控制调度



#### 多源数据集成和关联分析

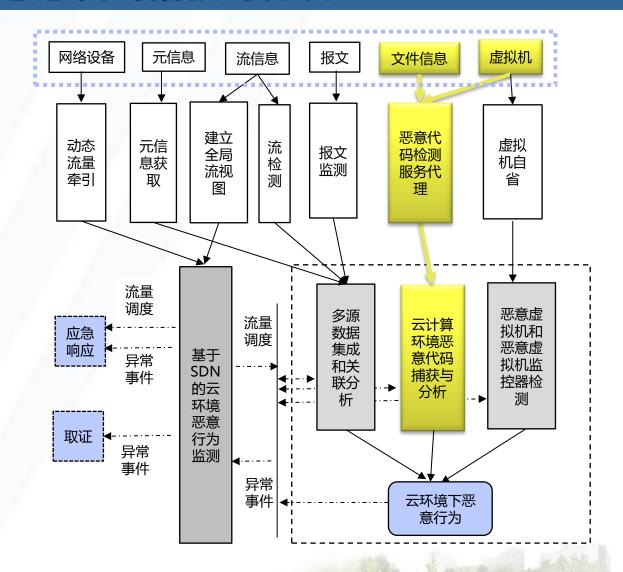


实线:表示数据

虚线:表示控制调度



## 云环境下恶意代码捕获与分析

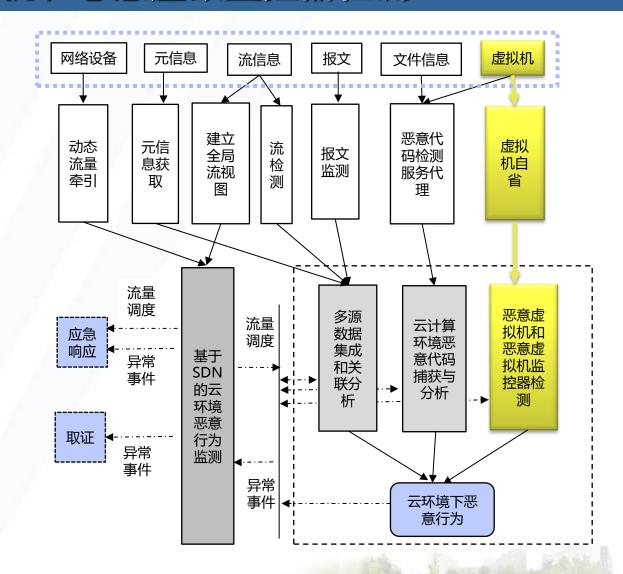


实线:表示数据

虚线:表示控制调度



#### 恶意虚拟机和恶意虚拟监控器检测

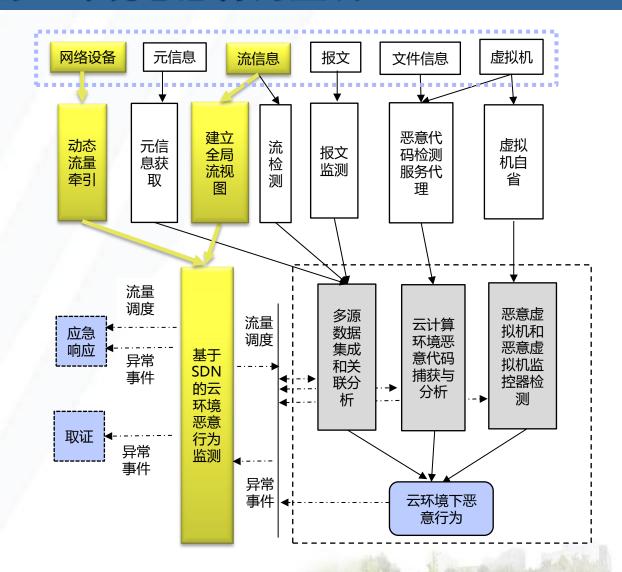


实线:表示数据

虚线:表示控制调度



#### 基于SDN的云环境恶意行为监测

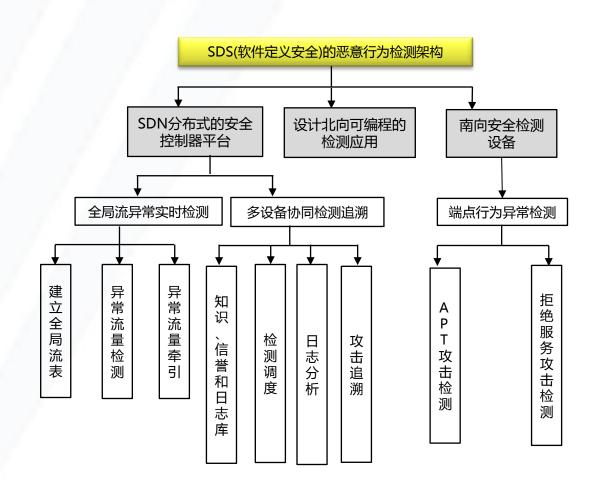


实线:表示数据

虚线:表示控制调度

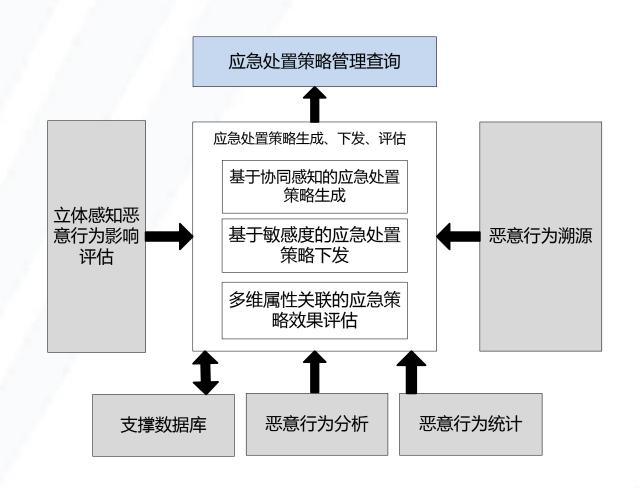


#### 基于SDS的云环境恶意行为检测技术



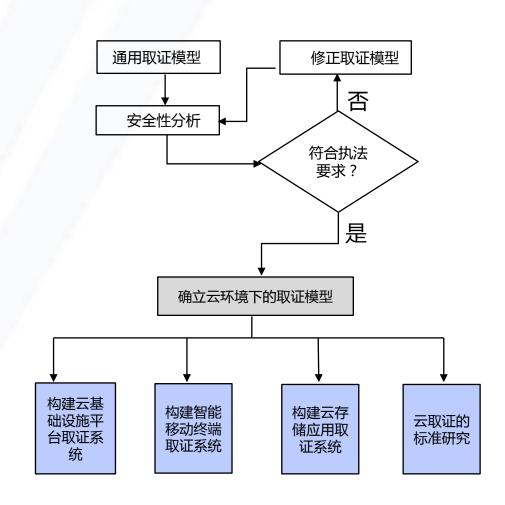


#### 云环境下的恶意行为应急处置与溯源系统



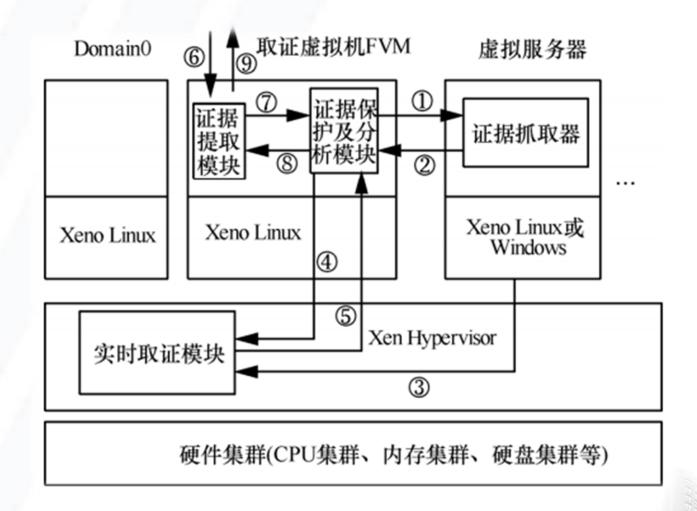


# 云环境下的取证系统





### 云基础设施平台取证系统





### 智能移动终端取证系统

#### 智能终端RAM获取分析系统

- ios
- Android
- Windows Phone

智能终端密码破解系统

智能移动终 端取证系统

智能手机存储系统 提取分析系统

智能终端证据智能化 关联分析系统



#### 云存储应用取证系统





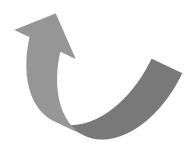
## 云取证标准



#### 前述研究成果

研究云存储证据的证据标 准及度量评价标准

理论和实践相结合的方法



结合公安计算机物证鉴定 要求



# 谢谢大家 请批评指正