行为分析
在系统异常检测领域的应用

聂　森
苗　甦
罗世龙

Who are we?

- 浓厚兴趣
- 良好的编程水平
- 良好的团队合作精神
- 参加过第十三次微软项目实践
- 有一定的系统安全防护软件开发基础

Background

- 特征码比对技术无法解决未知威胁
- 启发式扫描一旦被突破后果不堪设想
- 主动防御代价太大，尚不能构建有效的专家系统
- 希望通过底层特权实现安全防护注定是个无底洞
- 云安全仅仅停留在概念阶段

No Silver Bullet

基于行为分析的系统安全防护
已经成为现在研究的热点

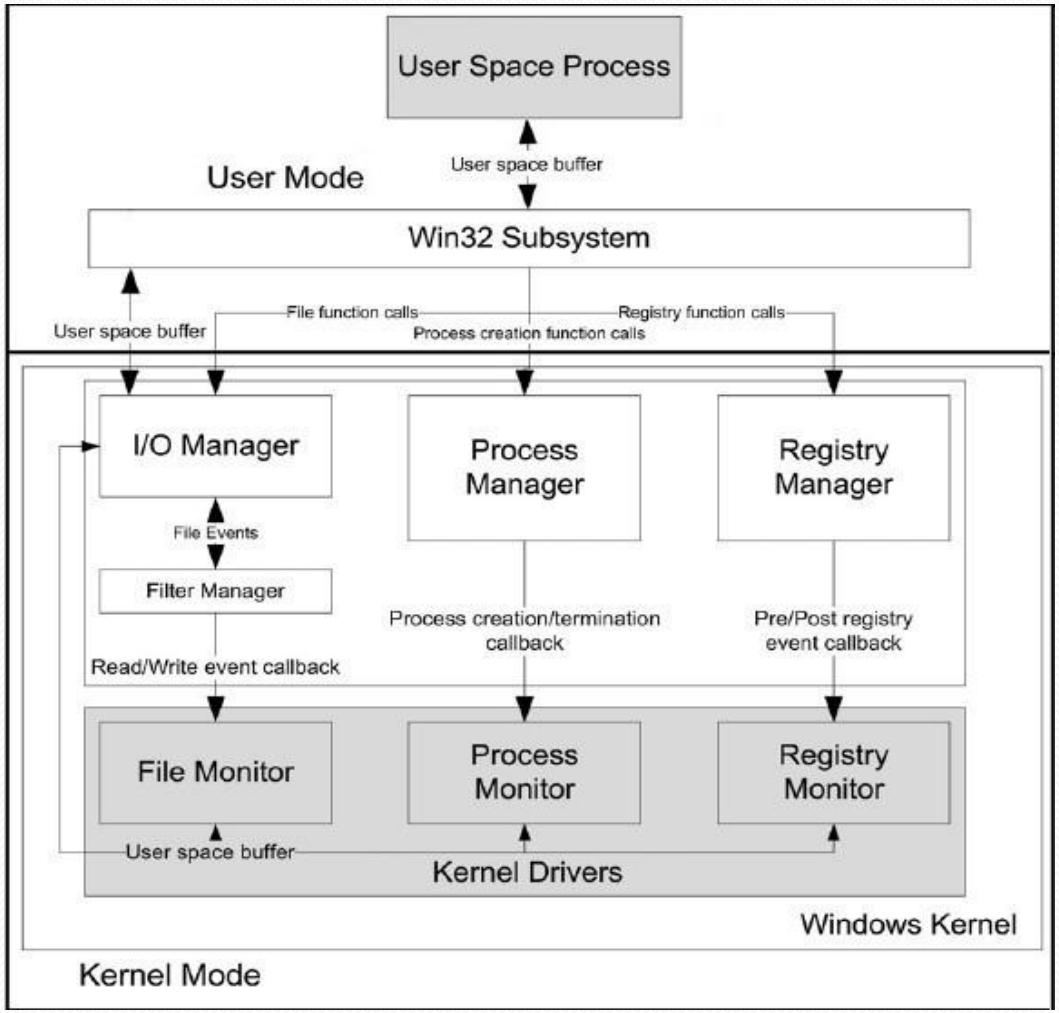
Definition

- 计算机中程序在执行过程中产生的各种系统调用称为行为
- 对这些系统调用的上下文进行分析，判断是否属于恶意行为，并进行拦截、报警或日志记录

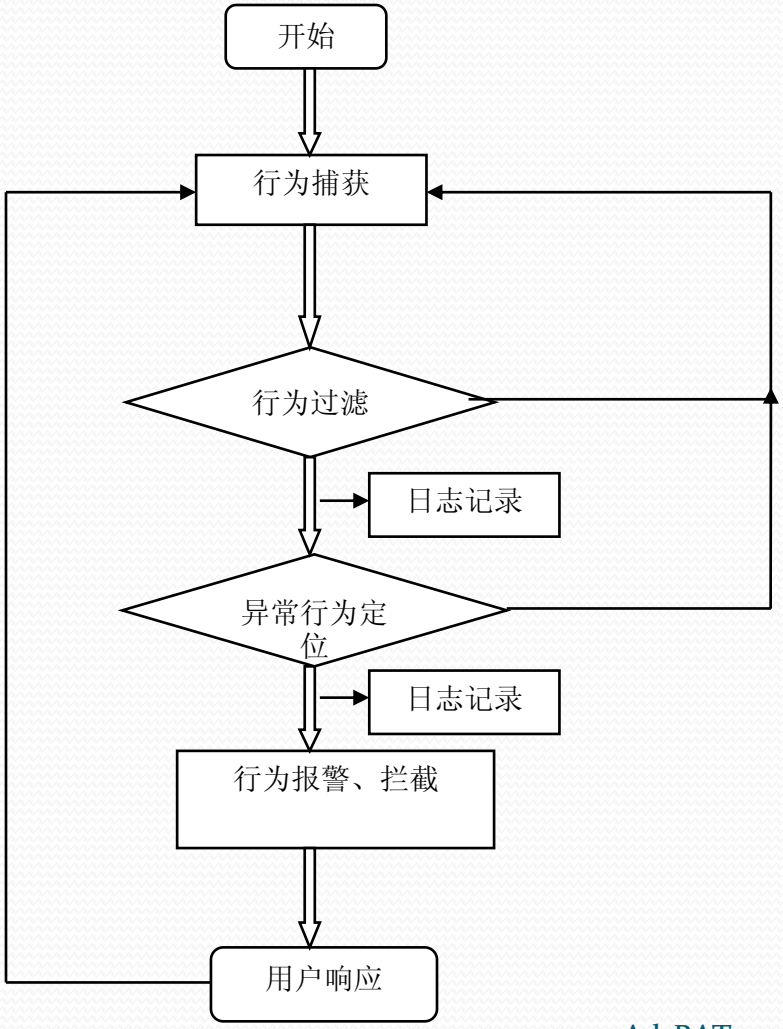
Our Idea

本项目首先对行为分析理论进行学习，研究行为分析理论在系统安全尤其是系统异常检测领域的应用，接着在理论研究基础上开发一个基于行为分析的系统异常检测系统（Advanced Behavioral Analysis Tool, 以下简称Ad-BAT）

Ad-BAT Architecture



Ad-BAT Architecture



Ad-BAT Advantages

- 高可信模型
- 有效的过滤机制
- 可移值性
- 不可见

Timeline

- 第一阶段：业务和需求分析
- 第二阶段：关键技术与核心算法研究
- 第三阶段：**Ad-BAT**项目开发与测试
- 第四阶段：撰写项目研究结题报告、提交项目管理委员会验收

Thank you

Q&A