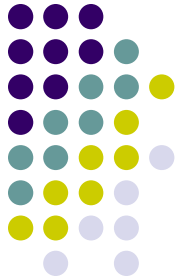
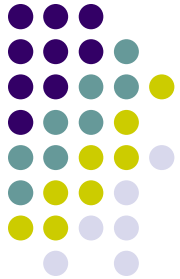


第9章 入侵检测系统

第9章 内容概要



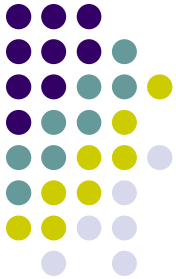
- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统

入侵检测系统基本概念

什么是入侵?

- 例如，入侵者获取Alice的用户名和密码来假冒 Alice
- 入侵者为黑客，获取合法用户登录信息并且假冒他们

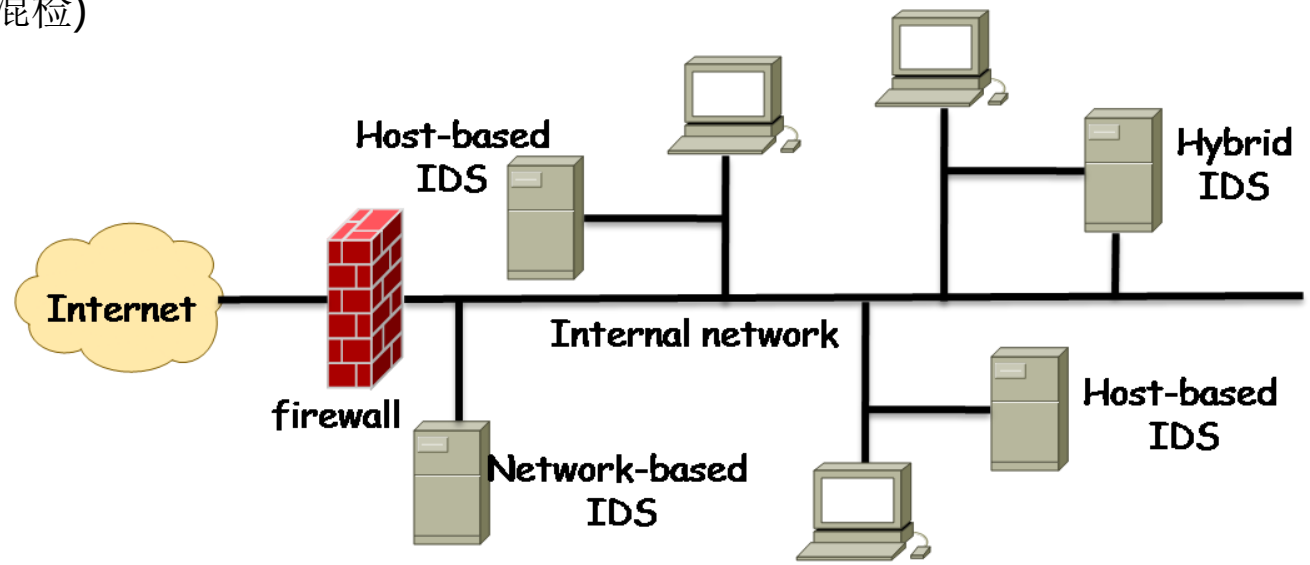
入侵检测系统基本概念



- 观测 (始于1980’s中期)
  - 入侵者行为与合法用户具有不同的行为
  - 这些行为可以通过定量的方法测量出来
- 入侵检测:
  - 尽快的识别出已发生或正在发生的入侵者行为
  - 收集入侵证据
  - 常用手段: 检测不正常行为
- 怎样构造一个自动检测工具去发现这些入侵行为? → 入侵检测系统(IDS)

基本方法

- 设立系统日志并分析之
  - 如果日志文件较小，可以手动完成。但是如果日志文件很大，可能需要复杂的工具
  - 基于通过跟踪用户用户使用主机行为和上网行为构造用户表征
    - 网检(NBD)
    - 机检(HBD)
    - 二者结合 (混检)



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

基本方法

- 安全审查
  - 分析日志常指审查
  - 两种审查
    - 安全表征实例：静态配置信息

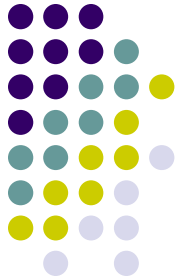
	参数	值
登录密码	最小长度(字节) 有效期 (天) 过期警告(天)	8 90 14
登录阶段	允许登录失败的次数 下一次允许登录时间间隔 (秒) 登录后什么也不做保持登录的时间(小时)	3 20 12

    - 动态事件: 动态用户事件

主体	操作	对象	意外事件	资源使用情况	时间戳
Alice Alice Alice	运行 开启 写入	cp ./myprog etc/myprog	无 无 写入失败	CPU:00001 byte-r: 0 byte-w: 0	Tue 11/06/07 20:18:33 EST Tue 11/06/07 20:18:33 EST Tue 11/06/07 20:18:34 EST

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

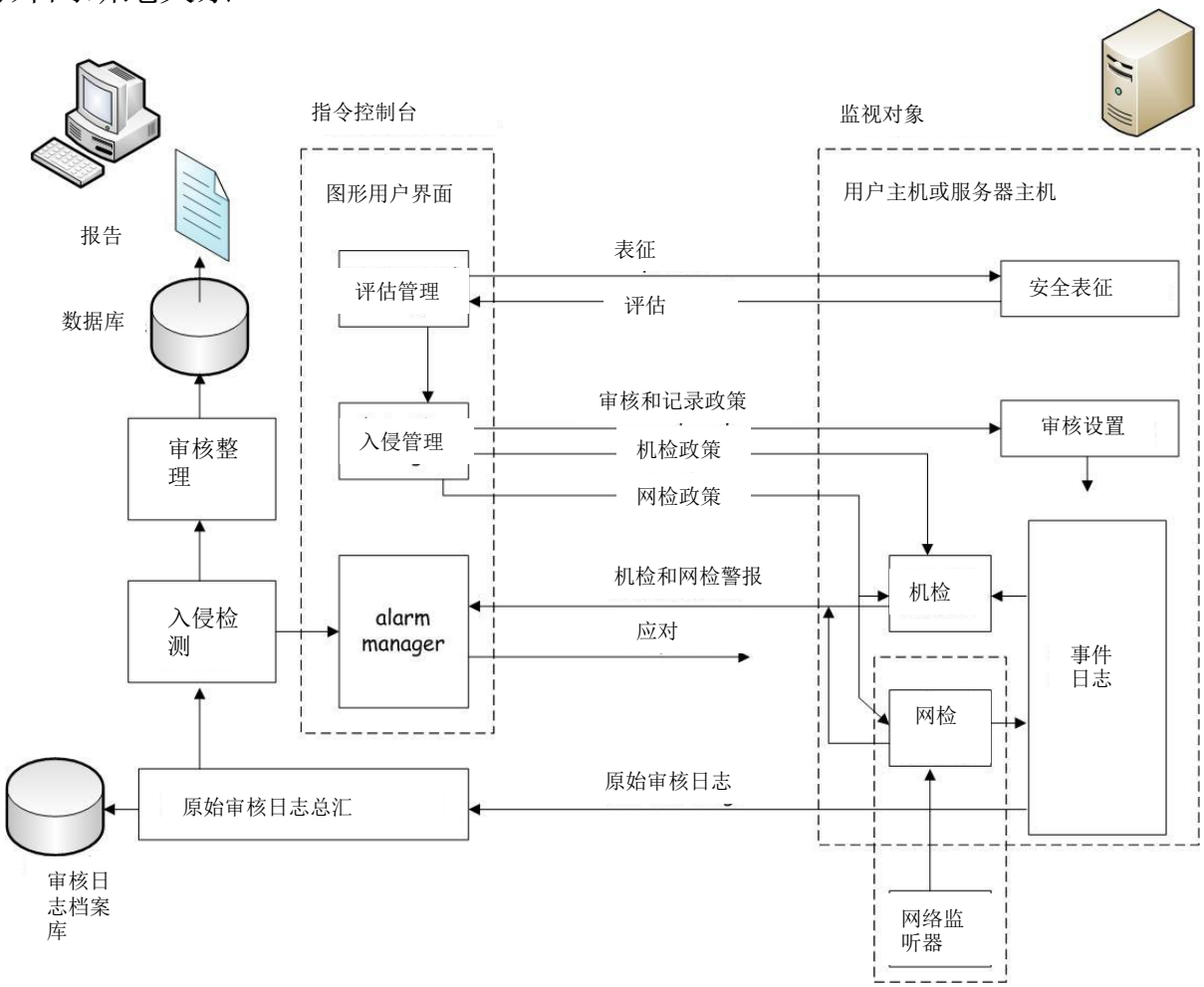
IDS 组成



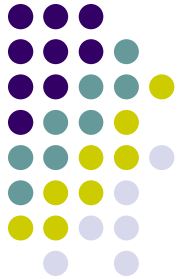
- 三部分:
  - 评估
    - 对系统的安全需求做出整体评价，并作出系统安全表征
  - 检测
    - 收集系统使用的事件并分析他们来找出入侵行为
      - 用户表征，可允许误差
  - 警报
    - 通知用户或系统管理员反常用机行为
    - 为警报分类并指示系统如何回应

IDS 体系结构

- 指令控制台
  - 控制管理目标主机
  - 与外网断绝关系
- 监视对象
  - 监视设备上的入侵行为

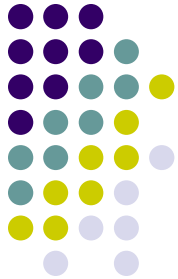


检测政策



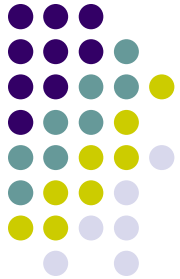
- IDP用来识别入侵行为
- 规定哪些数据必须保护以及受保护的程度
- 定义哪些是入侵行为并且在识别出后的应对
  - 错判和漏判
  - 行为分类
    - 绿灯行为: 可接受的正常行为
    - 红灯行为: 必须拒绝的不正常行为
    - 黄灯行为:基于当前信息无法判断的行为
    - 对于红灯行为和黄灯行为的应对政策:
      - 如果是黄灯行为，则收集更多信息作判断依据
      - 如果是红灯行为，终止用户登录
      - 如果是红灯行为，切断用户网络连接
      - 停机

不可接受行为



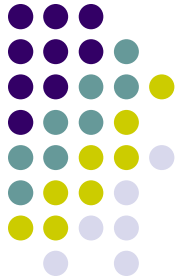
- 行为:
  - 一系列事件或者多系列事件的集合
- 可接受行为:
  - 遵循系统安全政策的一系列事件
- 不可接受行为:
  - 一系列违反系统安全政策的行为
- 问题:
  - 如何定义可接受行为和不可接受行为?
  - 怎样用定量的方法去描述和分析行为

第九章 内容概要



- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统

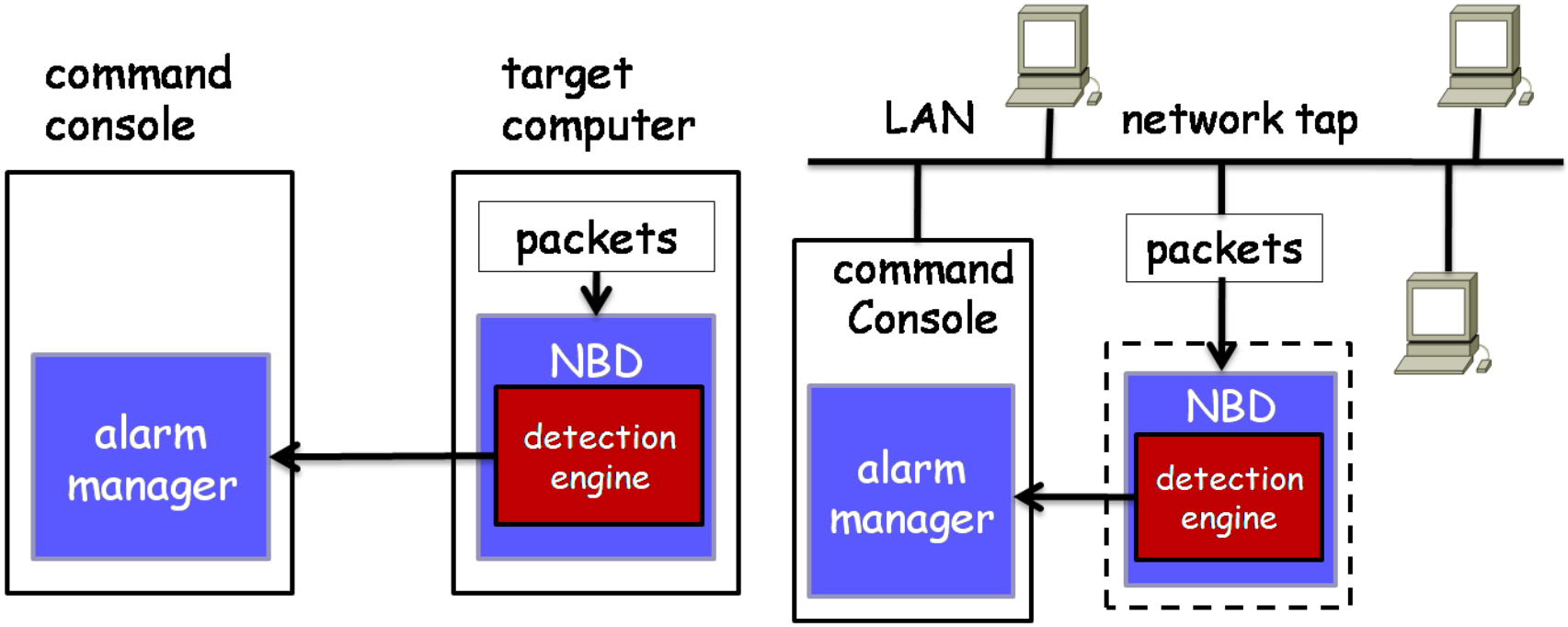
网检(NBD)



- NBD 分析网络数据包
- NBD:
  - 定义黄灯行为，红灯行为
  - 向控制台管理员发送警报信息
  - 将警报行为保存在系统日志中供日后分析用
- 主要有两种:
  - 网端检测:
    - 在特定的端点收集信息，检测网络
  - 引擎检测:
    - 分析数据包，发送警告消息

NBD 体系结构

- 网端检测
  - 检测系统设在主机内
- 网段检测
  - 网络上选定的点
  - 需要网络端点



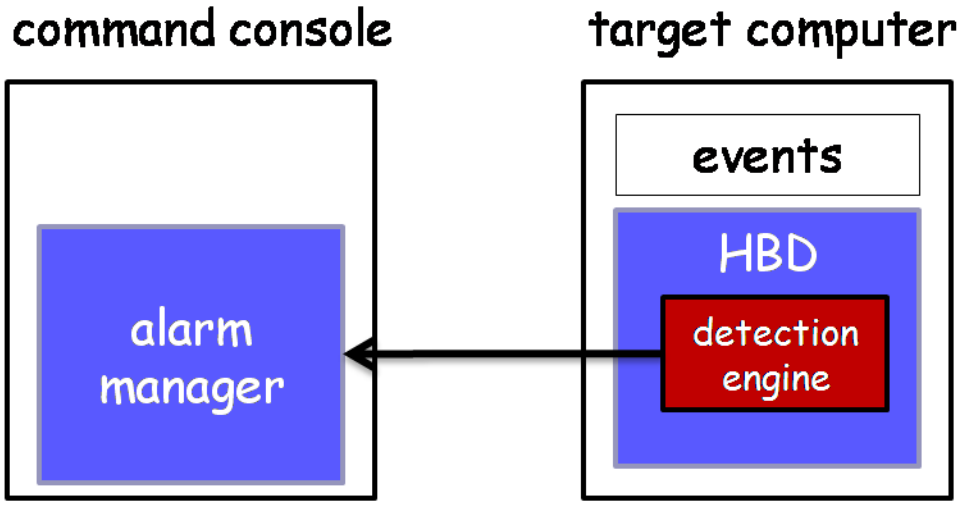
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

NBD 的优缺点

- 优点:
  - 成本低
  - 无干扰
  - 抗入侵
- 缺点:
  - 无法分析加密包
  - 网络流量大时，会无法分析数据而产生漏判
  - 某些入侵行为难以定义
  - 难以判断入侵行为是否成功

机检系统(HBD)

- HBD 分析系统事件和用户行为并且向管理员发出警告
  - 检查事件日志去定义可疑行为
  - 检查系统日志，保存系统文件记录
  - 检查系统配置
  - 为事件日志保存拷贝以防攻击者修改

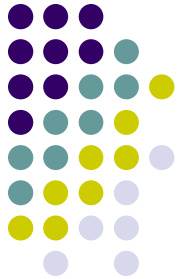


《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

HBD 优缺点

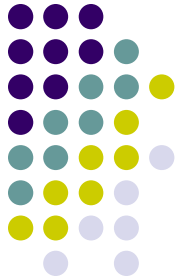
- 优点:
  - 不会因为数据在传输过程中被加密而受影响
  - 不需要特殊的硬件设备
  - 通过检查系统日志，更精确的分析系统行为
- 缺点:
  - 需要使用更多的系统管理资源
  - 消耗更多的计算资源
  - 直接危害主机操作系统的攻击会影响机检系统的执行
  - 不能安装在路由器和交换器等设备上

第九章 内容概要



- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统

特征检测

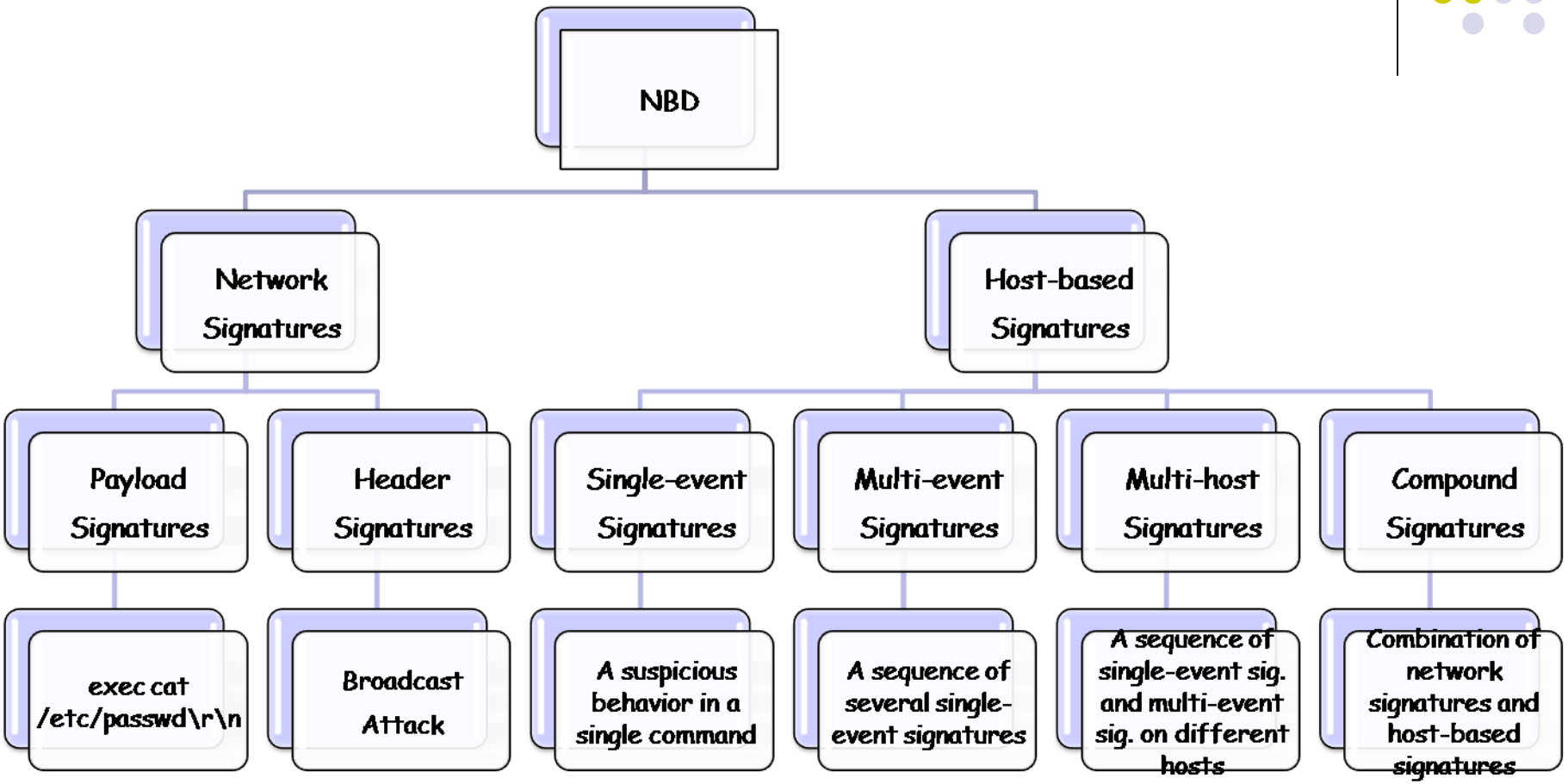


- 也称操作检测或规则检测
- 检查当前事件是否可以接受
- 两种特征检测:
  - 网络特征
    - 分析数据包的行为
  - 行为特征
    - 分析事件的用机行为

- 一系列行为规则:
  - 普通用户不能拷贝系统文件
  - 用户不能直接读写硬盘
  - 用户不应该访问其他用户的个人目录
  - 连续三次登录失败后用户不应该继续尝试登录
  - …

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

特征分类



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

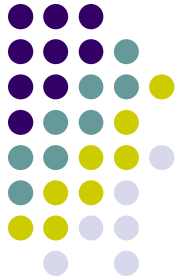
混合特征实例

网络特征	行为特征	混合特征
用户用 FTP登录后使用 cd 和 ls 指令	用户浏览\ etc目录和 passwd文件	用户从远程浏览系统文件
用户用FTP登录后使用 put 指令	上传到系统的文件有病毒和木马特征	用户从远程将可疑文件上传到主机系统
用户用FTP登录后使用 put 指令	用户修改系统文件和注册表	用户从远程修改系统文件
某种万维网攻击	读系统可执行文件	网络攻击成功

混合特征实例

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

局外人行为和局内人滥用权限

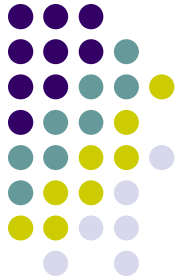


- 局内人:系统中具有登录权限的用户
- 局外人:没有登录权限的用户
- 利用局外人行为的检测:
  - 攻击者可能在目标系统中安装特洛伊木马，劫持TCP连接或尝试扫荡攻击
- 利用局内人滥用权限的检测:
  - 攻击者做通常的合法用户不会做的事

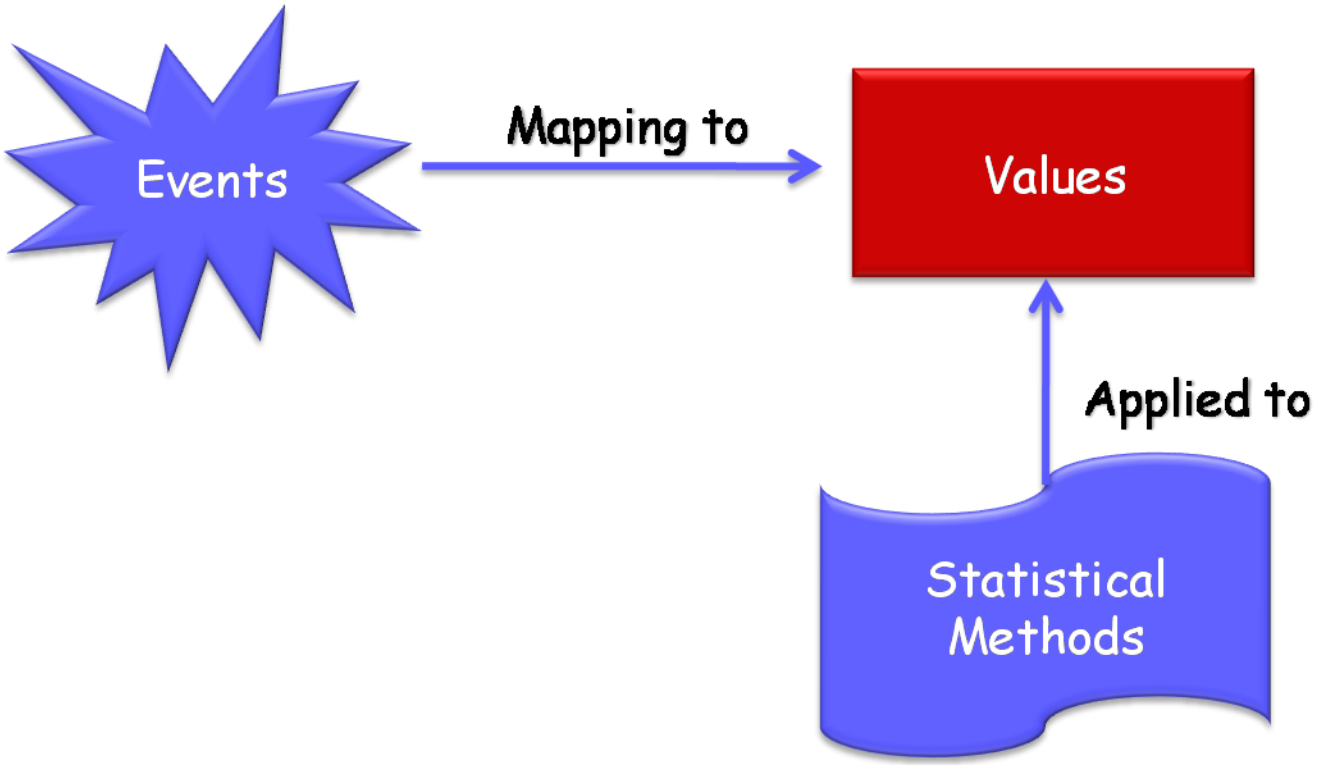
特征检测系统

- 内置系统
  - 在系统内部存储检测规则
  - 给用户提供IDS编辑器
  - 用户基于自身需要选取规则
- 程序系统
  - 有默认规则，提供程序语言
  - 允许用户选择规则和编写新规则
- 专家系统
  - 更专业更完整
  - 需领域内专家

第九章 内容概要

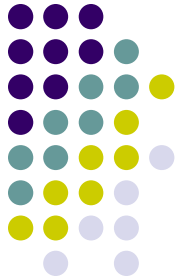


- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统



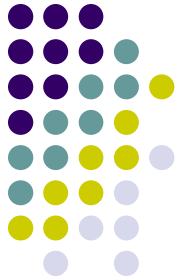
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

两种方法



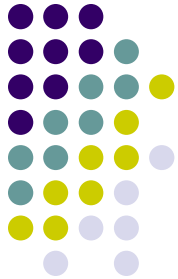
- 当可以用定量方法描述出不可接受行为与正仓行为的差别时，通常用大两种统计方法:
  - 依据临界值分析
    - 简单但不精确
    - 统计在一段时间内某种类型的事件出现的次数
  - 用户表征
    - 更精确
    - 基于定量方法收集用户用机行为，建立用户表征

事件计量器



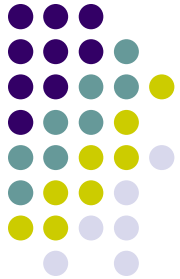
- 例子:
  - 特定事件发生的时间
  - 一段时间内特定事件发生的次数
  - 系统变量当前的值
  - 系统资源的利用率

事件计数器



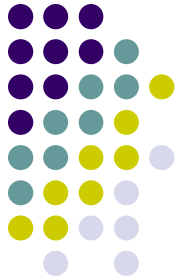
- 事件计数
  - 一个整形变量记录在一个指定的时间内同一类型数据出现的次数
- 事件表
  - 一个整形变量为系统里的每一个测试对象一个当前值
- 事件计时器
  - 为系统中两个相关事件赋予一个整数变量，用来表示从第一个事件到第二个事件的发生之间的时间间隔
- 资源利用率
  - 为每一个资源赋予一个变量，用来记录在一个指定时间段中的资源利用率

统计学方法



- 均值和方差
  - 与正常值比较
- 多变量分析
  - 同时分析两个或更多相关值，识别异常行为
- 马尔可夫过程
  - 计算系统从一种形态到另一种形态转换的概率
- 时间序列分析
  - 研究事件序列，查找异常

第九章 内容概要

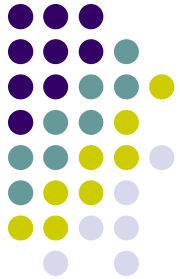


- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统

行为推理

- 行为推理研究怎样运用数据挖掘技术分析事件日志并寻求有用信息
- 数据挖掘技术
  - 数据提炼
  - 上下文演绎
  - 来源组合
  - 外围数据
  - 深挖细掘
- 行为推理实例 (p295)

第九章 内容概要

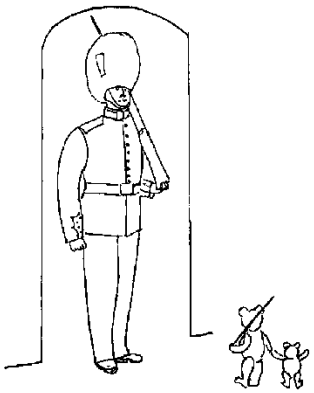


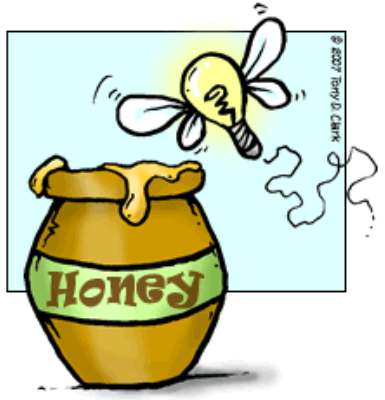
- 9.1 基本概念
- 9.2 网检和机检
- 9.3 特征检测
- 9.4 统计分析
- 9.5 行为推理
- 9.6 诱饵系统

诱饵系统

- 定义:
  - 用设备，系统，目录或文件作为诱饵，引诱攻击者，使真正重要的主机和系统免于攻击并收集入侵者行为
  - 帮助用户找到敌人
  - 牺牲自己，保全真正主机系统不受攻击

- IDS = 守卫
- Decoy System = 蜜罐





《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

诱饵系统种类

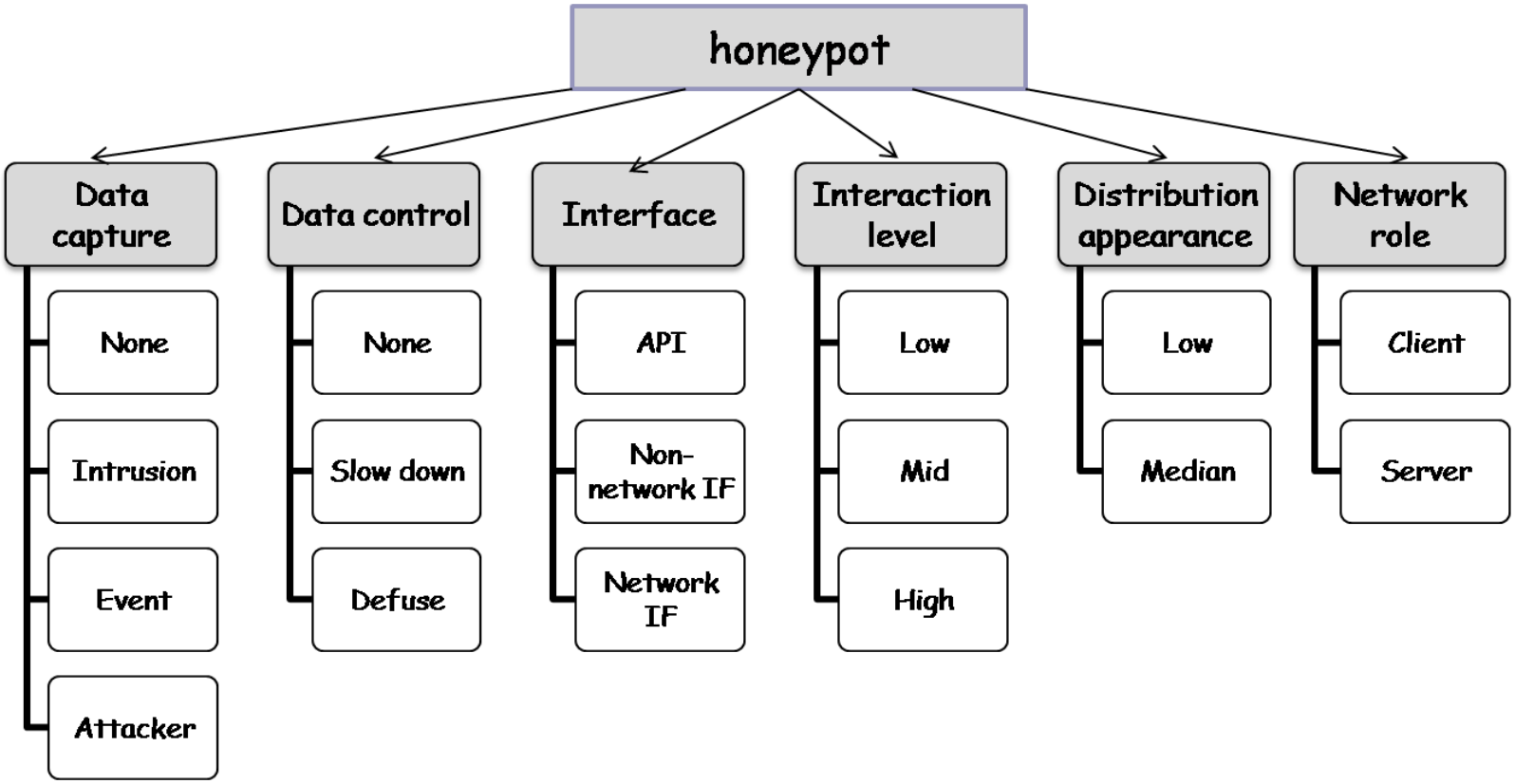
- 1990开发出来
  - 连在局域网内的主机，有真正的 IP 地址
  - 需要与操作系统进行高层互动并且用相当的精力去维护
- 1990’s后期，软件技术逐渐成熟，
  - 容易配置
  - 需要低层互动
  - 常用的虚拟诱饵系统Honeyd, KFSensor, CyberCop Sting …

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

互动层次

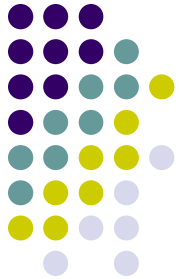
- 低层互动：
  - 运行诱饵主机的服务端程序只能往主机的硬盘上写入信息
- 中层互动：
  - 运行诱饵主机的服务端程序只能往主机的硬盘上读出和写入信息
- 高层互动：
  - 运行诱饵主机的服务端程序可以和主机的操作系统互动，并通过操作系统与主机硬盘和其他系统资源互动

诱饵系统的功能和刻画



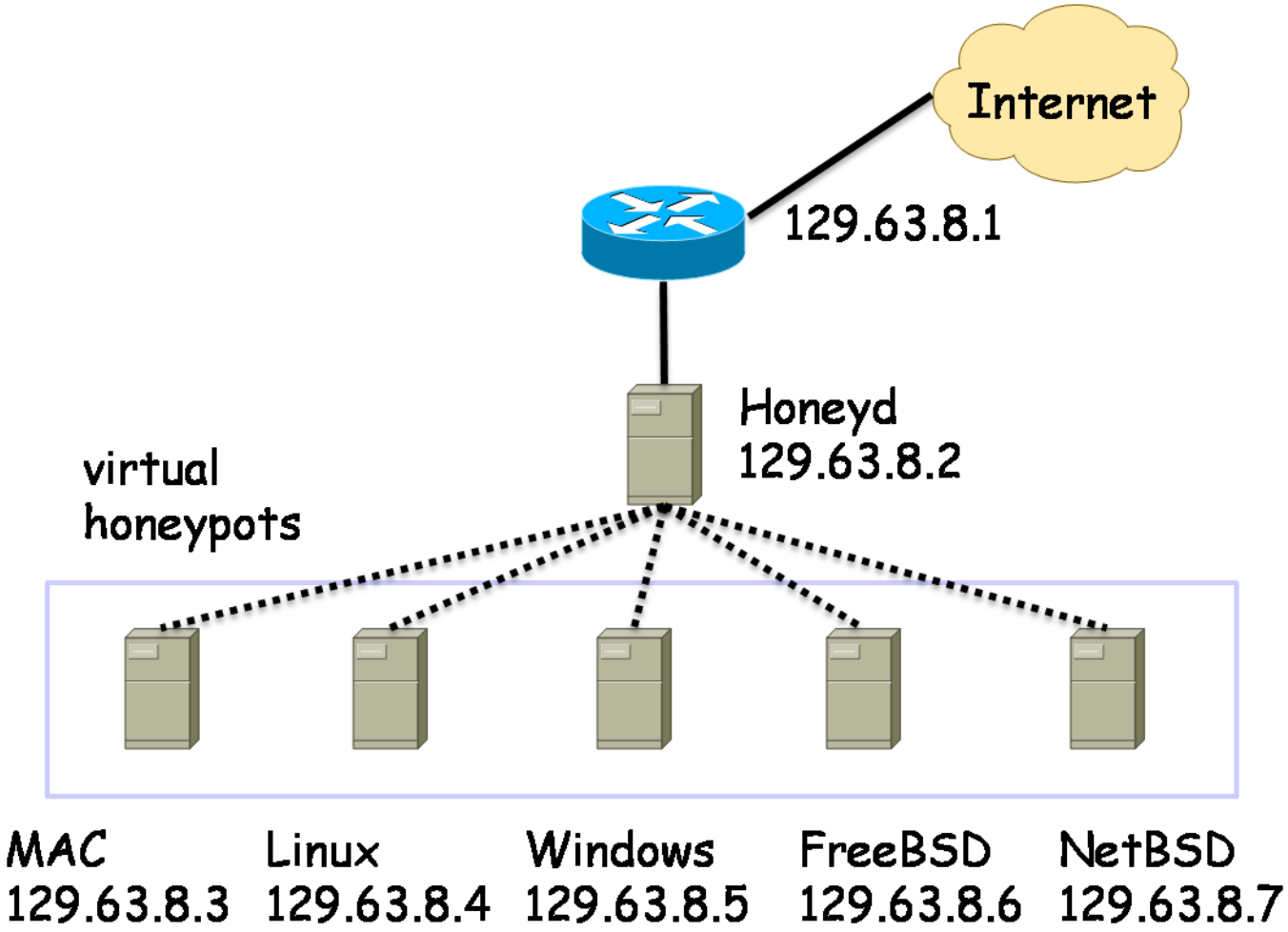
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

Honeyd



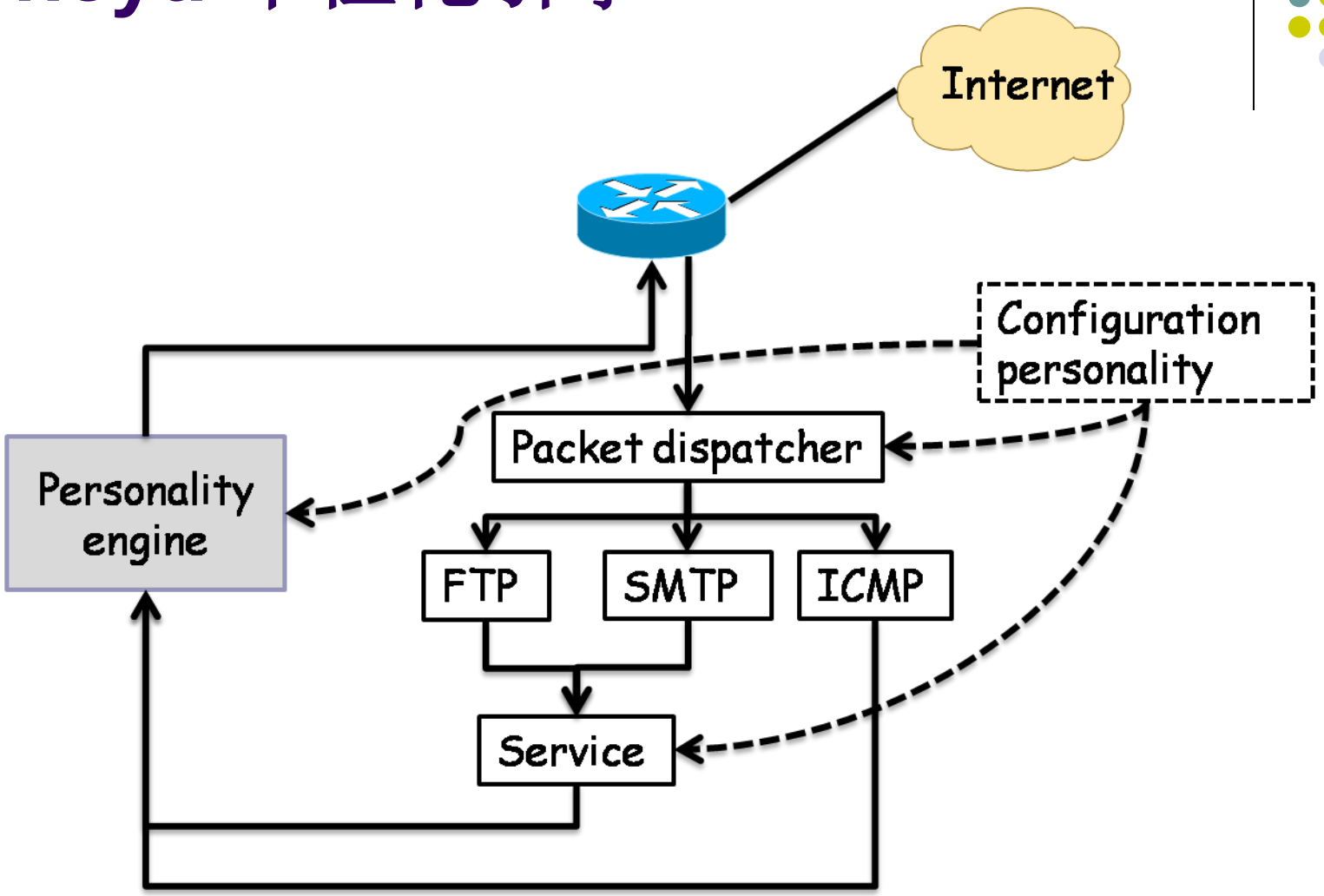
- 时并行运行虚拟IP协议集和的软件引擎
- 在网络层上建构虚拟诱饵系统提供了结构简易的框架
- 能够模拟标准网络服务在不同的虚拟主机系统上运行不同的操作系统
- 能监测并清除蠕虫， 分散入侵者注意力，组织垃圾邮件的传播

Honeyd 结构示意图



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

Honeyd 个性化引擎



A block diagram of Honeyd architecture

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

其他系统

- MWCollect 计划
- Honeynet计划
  - Honeywall CDROM
  - Sebek
  - 高层互动分析工具包 (HIHAT)
  - HoneyBow