



入侵检测



罗敏

13907125177

武汉大学 计算机学院

mluo@whu.edu.cn



防火墙技术 重点回顾

- 防火墙技术概述
- 防火墙的结构
- 构建防火墙
- 防火墙产品



主要内容

- 入侵检测概述
- 入侵检测的模型
- 入侵检测产品



传统的安全技术

- 预防(prevention)、防护 (protection)
 - 加密
 - 消息摘要、数字签名
 - 身份认证：口令、认证交换协议、生物特征
 - 访问控制
 - 安全协议： IPsec、SSL
 - 网络安全产品与技术：防火墙、VPN
 - 内容控制：防病毒、内容过滤等
- 遵循“正确的安全策略 → 正确的设计 → 正确的开发 → 正确的配置与使用”

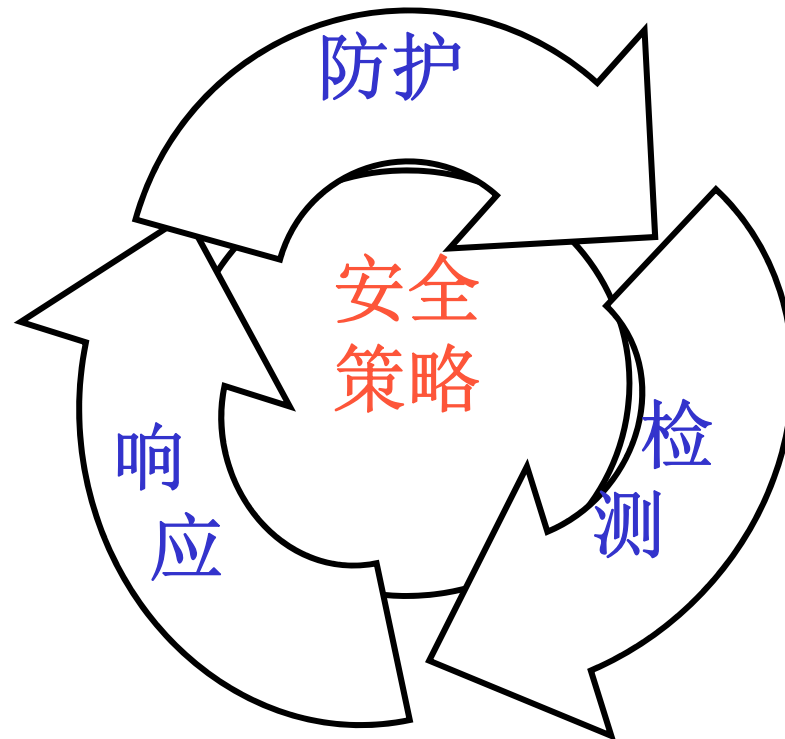


预防措施的局限性

- 预防性安全措施采用严格的访问控制和数据加密策略来防护，但在复杂系统中，这些策略是不充分的。这些措施都是以减慢交易为代价的。
- 大部分损失是由内部引起的
 - **1999年CSI/FBI (Computer security institute/Federal Bureau of Investigation)指出，82%的损失是内部威胁造成的。**

动态安全模型

- 以安全策略为核心



P2DR安全模型

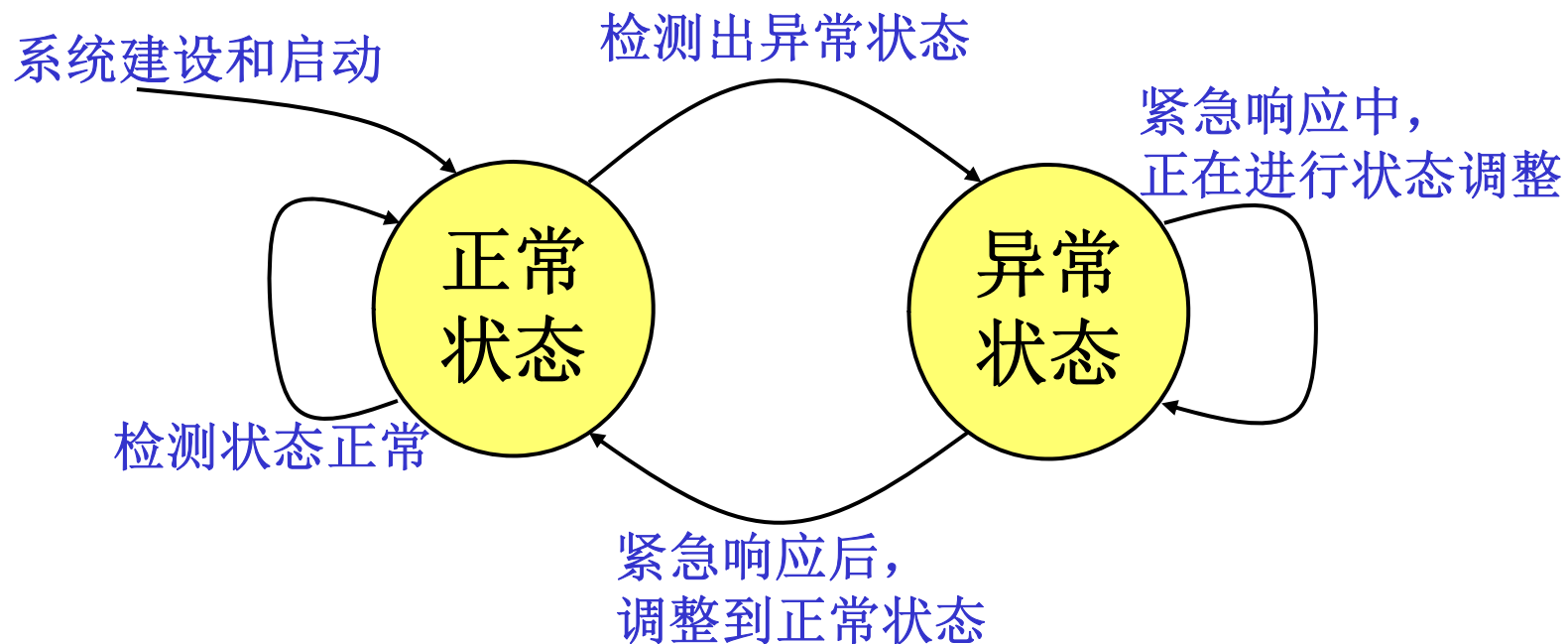


动态安全模型

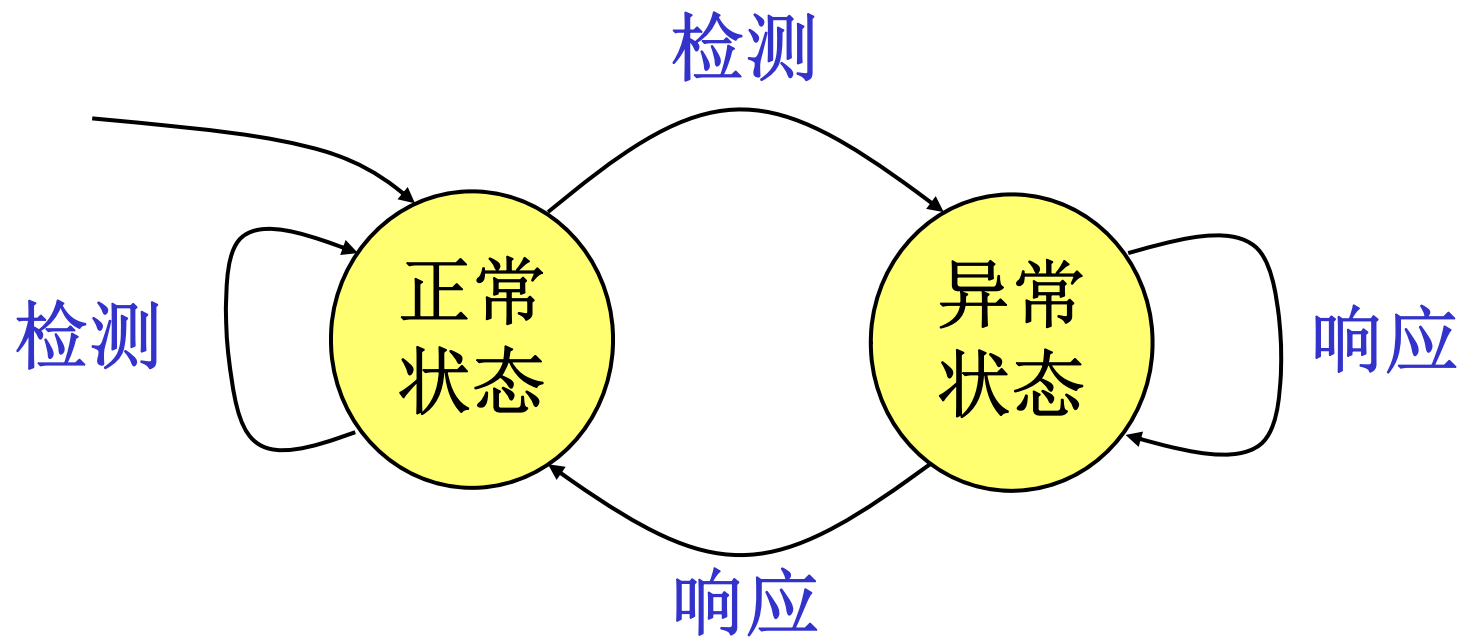
■ P2DR模型

- 策略（**Policy**）：是模型的核心，具体的实施过程中，策略意味着网络安全要达到的目标。
- 防护（**Protection**）：安全规章、安全配置、安全措施
- 检测（**Detection**）：异常监视、模式发现
- 响应（**Reponse**）：报告、记录、反应、恢复

信息安全两态论



信息安全两态论





入侵检测系统

- NSTAC (National Security Telecommunications Advisory Board, 国家安全通信委员会) 的IDSG (Intrusion Detection Sub-Group) 是一个由美国总统特许的保护国家关键基础设施的小组。
- IDSG 1997年给出了如下定义:
- **入侵 (Intrusion)** : 对信息系统的非授权访问及 (或) 未经许可在信息系统中进行操作。
- **入侵检测 (Intrusion Detection)** : 对 (网络) 系统的运行状态进行监视, 对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。



入侵检测系统

- **ICSA.net**国家计算机安全协会(ICSA)是提供安全产品的测试和事实上的行业标准的组织.
- 1998年ICSA建立了入侵检测系统协会IDSC(Intrusion Detection Systems Consortium),1999年3月给出如下定义:
- **入侵检测系统 (Intrusion Detection System)** : 该系统从多种计算机系统及网络中搜集信息,再从这些信息中分析入侵及误用特征。
- **入侵**: 由系统外部发起的攻击
- **误用**: 由系统内部发起的攻击



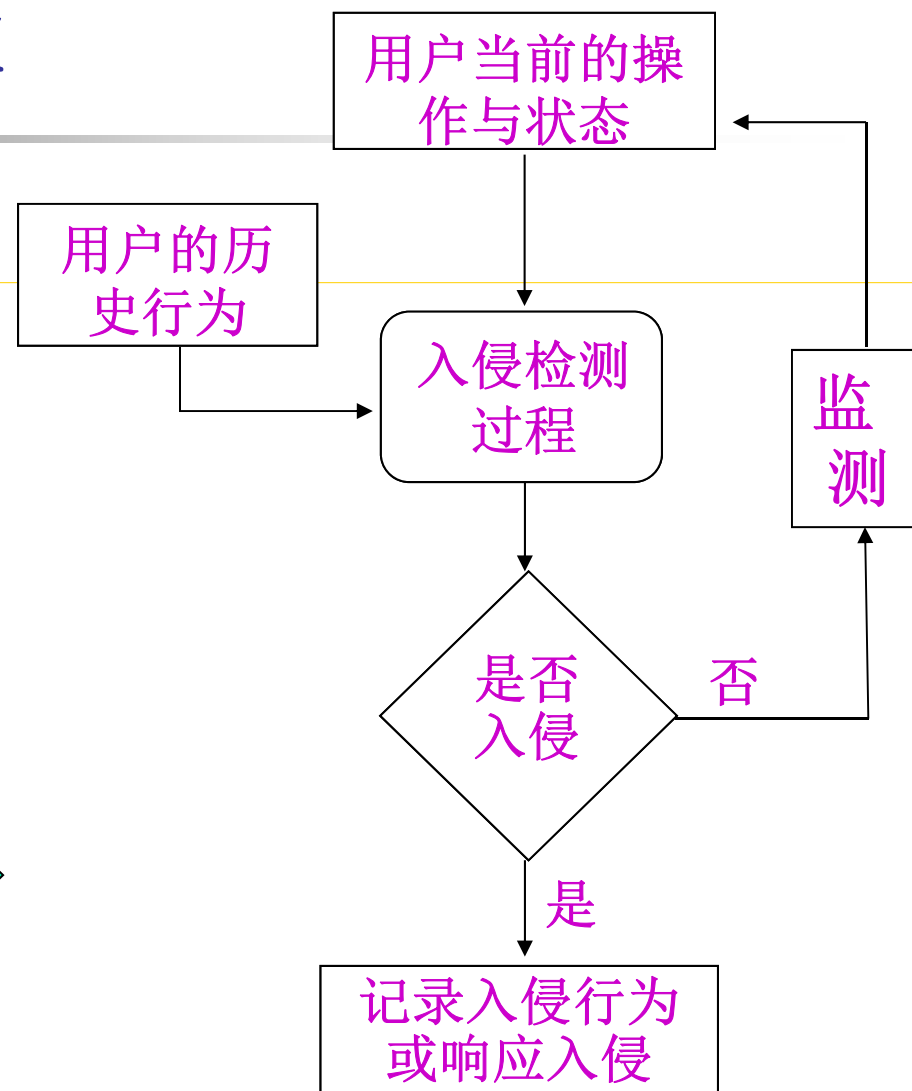
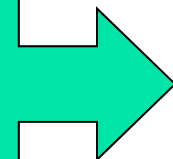
入侵检测系统

- 入侵检测是一种动态的网络安全技术
 - 利用各种不同类型的引擎，实时地或定期地对网络中相关的数据源进行分析，依照引擎对特殊的数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制。
 - 入侵检测的动态性反映在入侵检测的实时性、对网络环境的变化具有一定程度上的自适应性，这是以往静态安全技术无法具有的

入侵检测技术

- 入侵检测的内容可分为
 - 外部攻击检测
 - 内部特权滥用检测

入侵检测
技术原理



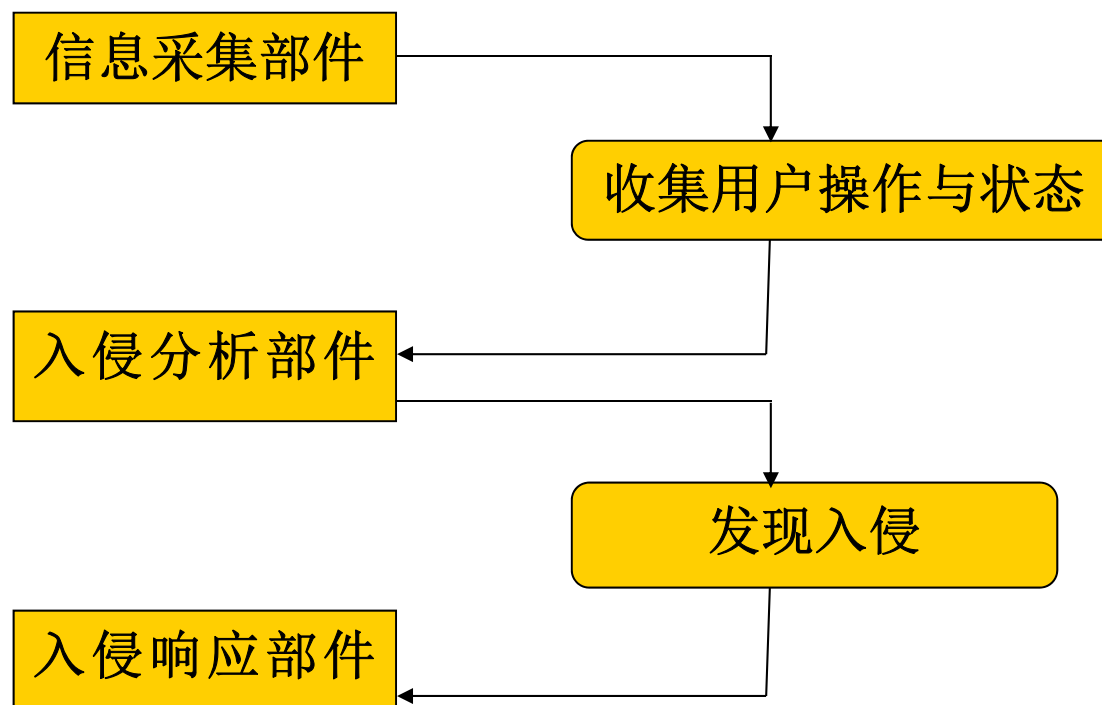


入侵检测系统的基本功能

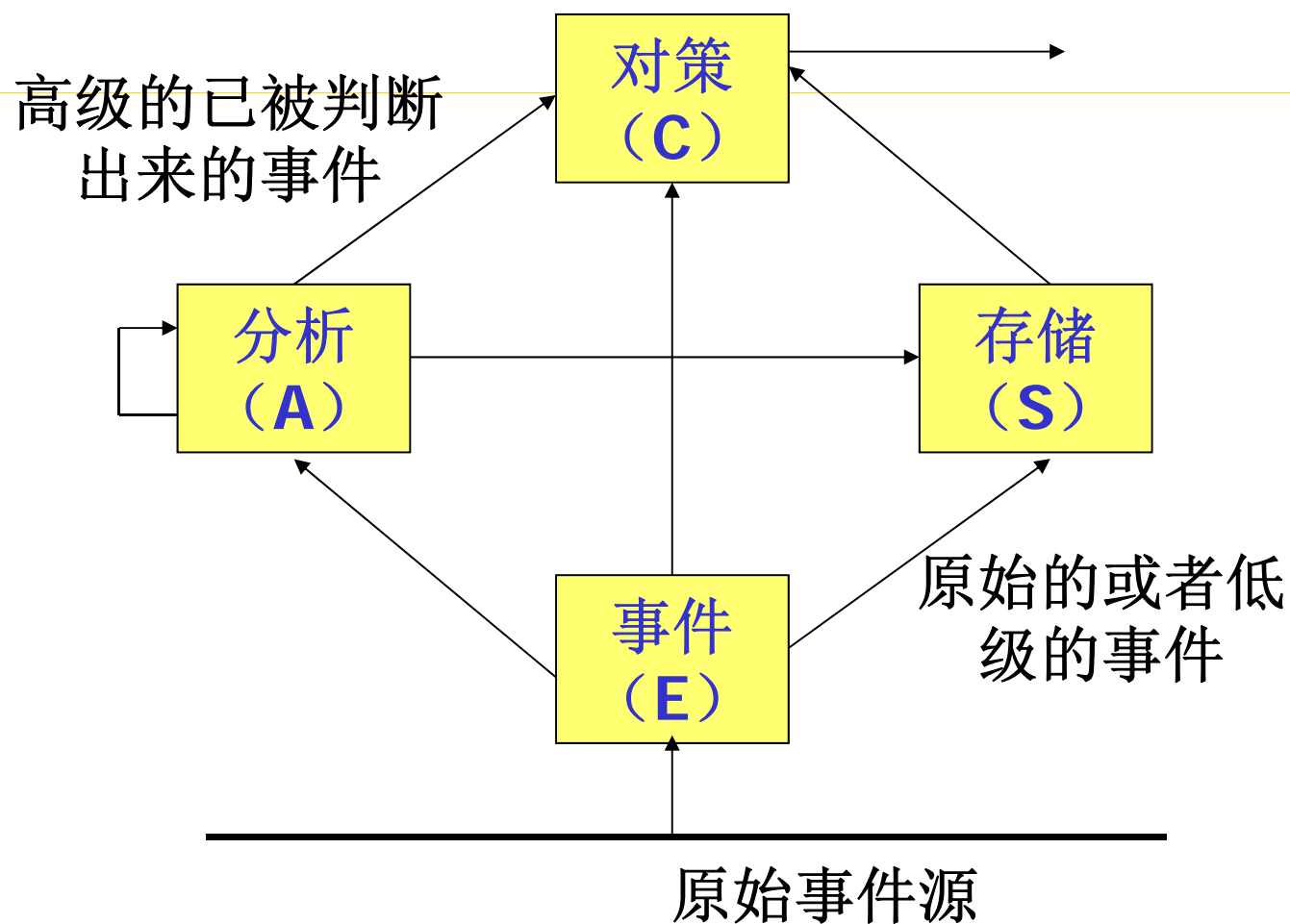
- 检测和分析用户和系统的活动
- 审计系统配置和脆弱性
- 评估关键系统和数据文件的一致性和完整性
- 识别反映已知攻击的活动模式
- 非正常活动模式的统计分析
- 操作系统的审计跟踪管理，通过用户活动的识别违规操作
- 纠正系统配置错误
- 安装、运行陷阱以记录入侵者的相关信息

入侵检测技术

■ 入侵检测系统



公共入侵检测框架





入侵分析——信息收集

- 入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为。
- 需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，
 - 尽可能扩大检测范围
 - 从一个源来的信息有可能看不出疑点



入侵分析——信息收集

- 入侵检测很大程度上依赖于收集信息的可靠性和正确性。
- 要保证用来检测网络系统的软件的完整性。
- 特别是入侵检测系统软件本身应具有相当强的坚固性，防止被篡改而收集到错误的信息。
- 在一个环境中，审计信息必须与它要保护的系统分离来存储和处理。因为
 - 防止入侵者通过删除审计记录来使入侵检测系统失效
 - 防止入侵者通过修改入侵检测器的结果来隐藏入侵的存在
 - 要减轻操作系统执行入侵检测任务带来的操作负载



入侵分析——信息收集

■ 数据来源可分为四类：

- 来自主机的：基于主机的监测收集通常在操作系统层的来自计算机内部的数据，包括操作系统审计跟踪信息和系统日志
- 来自网络：检测收集网络的数据
- 来自应用程序：监测收集来自运行着的应用程序的数据，包括应用程序事件日志和其它存储在应用程序内部的数据
- 来自目标机：使用散列函数来检测对系统对象的修改。



入侵分析——信息收集

- 黑客经常在系统日志文件中留下他们的踪迹，因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。
- 日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如记录“用户活动”类型的日志，就包含登录、用户**ID**改变、用户对文件的访问、授权和认证信息等内容。
- 显然，对用户活动来讲，不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等等



入侵分析——信息收集

■ 异常变化

- 网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。
- 入侵者经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件



入侵分析

- 误用检测（模式匹配）
- 异常检测（统计分析）
- 完整性分析，往往用于事后分析



误用检测

- 误用检测就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。
- 一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）



异常检测

- 异常检测方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。
- 测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生



完整性分析

- 完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、被安装木马的应用程序方面特别有效。



入侵检测的分类

■ 按照分析方法（检测方法）

- 异常检测模型（**Anomaly Detection**）:首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。
- 误用检测模型（**Misuse Detection**）: 收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。



异常检测

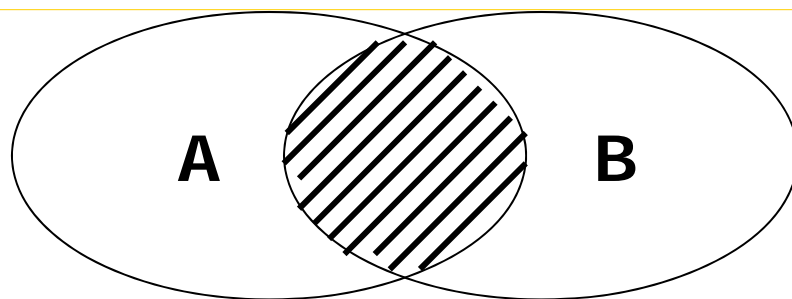
- 假定所有的入侵活动都是异常的活动。建立一个正常活动的特征文件，通过统计不同于已建立的特征文件的所有系统状态的数量识别入侵企图
- 以历史数据或期望值为基础，为各个主体、对象的行为定义变量与该变量的基值，利用加权函数组合变量，得出综合变量值，并在此基础上，将入侵定义为出现了任何与期望值相比较有不可接受的偏差。



异常检测

- 异常行为集和入侵行为集不等时产生假报和漏判
 - 不是入侵的异常活动被标识为入侵，称之为误报（**False Positives**），造成假警报
 - 入侵活动不是异常活动，这时入侵活动被标识为正常活动，称之为漏报（**False Negatives**），造成漏判

异常检测



A: 异常行为集

B: 入侵行为集



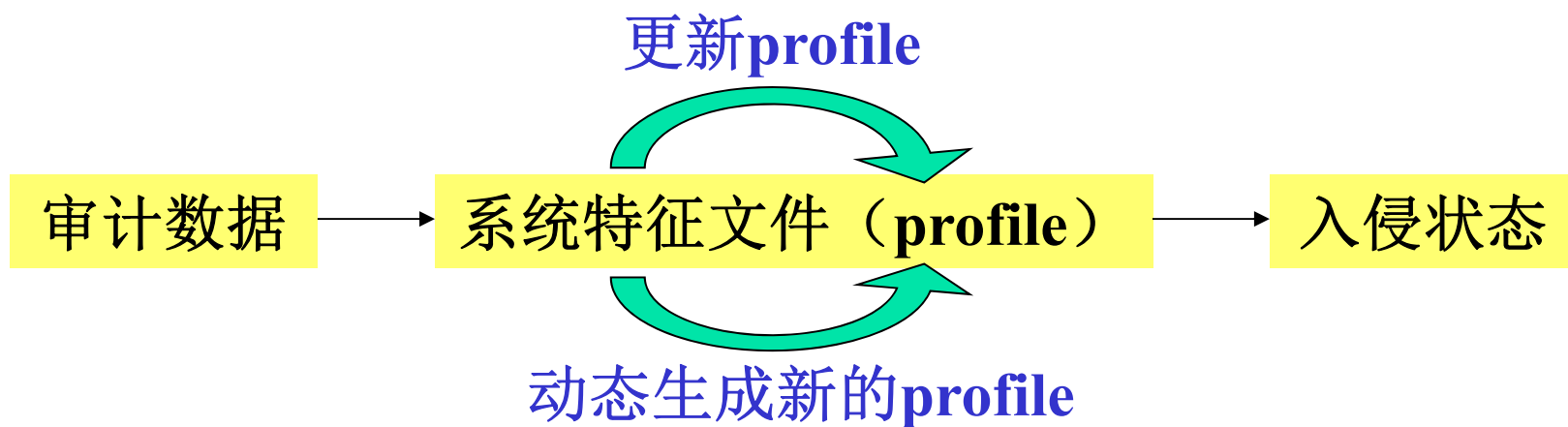
: 可正确检测C

可正确检测 $C = A \cap B$

假警报: $A - C$

漏判: $B - C$

异常检测





异常检测

- 异常检测根据使用者行为或资源使用状况判断是否入侵，而不依赖于具体行为是否出现来检测，也称为**基于行为的检测**
- 基于行为的检测方法：概率统计、预测模式、机器学习、神经网络、免疫算法、模糊技术等



异常检测

■ 概率统计方法

- 检测器根据用户对象的动作为每个用户建立一个用户特征表，通过比较当前特征与已存储定型的以前特征，从而判断是否存在异常行为
- 用户特征表根据审计记录情况不断更新
- 运用成熟的概率统计理论，但对事件发生的次序不敏感



异常检测

■ 描述特征的变量

- 操作密度：操作执行的速率
 - 审计记录分布：在最新记录中所有操作类型的分布
 - 范畴尺度：在一定动作范畴内特定操作的分布情况
 - 数值尺度：产生数值结果的操作
-
- 例子：SRI/CSL的入侵检测专家系统的特征项：
<变量名，行为描述，例外情况，资源使用，时间周期，变量类型，门限值，主体，客体，值>



入侵检测技术

■ 误用检测（**Misuses Detection**）分析方法

- 特征检测或基于知识的检测
- 利用已知的攻击方法，根据已定义好的入侵模式，通过判断这些入侵模式是否出现来进行检测。
- 模式数据库的建立，通过专有知识和实践经验结合形成具有一定及时性的入侵模式数据，并且存在着定期更新的需求。
- 基于知识的检测方法：专家系统、模式匹配与协议分析、基于模型、按键监视、模型推理、状态转换分析、**Petri网**状态转换



入侵检测技术

■ 入侵检测系统分类

- 离线和在线检测系统
- 误用检测和异常检测

优点：

- 符合数据的异常变化理论，适合事务的发展规律
- 对变量的跟踪不需要大量的内存
- 异常检查对模式匹配发现不了的某些新的攻击具有检测与响应的能力

缺点：

- 数据假设可能不合理，加权算法在统计意义上可能不准确；
- 对突发性正常事件容易引起误判断
- 对长期、稳定的攻击方法灵敏度太低
- 通常不具备自学习能力
- 攻击行为转化为模式比较困难



入侵检测技术

■ 检测数据源

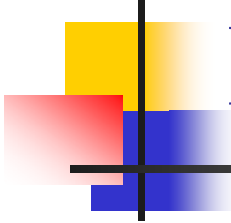
- 操作系统审计记录 (Audit Trails)
- 系统日志 (System Logs)
- 应用程序日志 (Application Logs)
- 目标信息 (Objects)



入侵检测技术

■ NT审计机制

- 以事件日志（event-logging）的形式提供数据源
- 融合了从操作系统和其它系统数据源处收集到的事件信息
- 由操作系统内部的安全参考监视器（SRM）、本地安全中心（LSA）和事件记录器（Event Logger）共同完成



NT审计机制

- NT包含7种类型的审计事件组:

- 系统
- 登录/退出
- 对象访问
- 特权使用
- 细节跟踪
- 策略更改
- 帐号管理



入侵检测技术

- NT的事件日志机制

- 系统日志

- 记录操作系统事件

- 应用日志

- 记录应用程序事件

- 安全日志

- 记录与安全相关的事件



入侵检测技术

■ NT的事件记录格式

记录头	日期	时间	主体标识	计算机名
	事件标号	事件来源	事件等级	事件类别
事件描述	事件描述区的内容取决于具体的事件，可以是事件的名称、详细说明、产生该事件的原因、建议的解决方案等信息。			
附加数据	可选数据区，通常包含可以以16进制方式显示的二进制数据。 具体内容产生事件记录的应用程序决定。			



系统日志

- 系统日志是反映各种系统事件和设置的文件；
- Unix系统提供了分类齐全的系统日志，如登录日志、进程统计日志；
- Unix提供通用的服务（syslog）用于支持产生和更新事件日志，任何程序都可以通过syslog记录事件；



系统日志

- 系统日志的来源：产生日志的软件作为一个应用程序
- 系统日志的存储方式：存储在不受保护的目录里
- 提高系统日志的安全性
 - 加密和校验机制
 - 日志重定向



系统日志

- 面向管理员而非面向计算机
- 与审计记录相比，更为人性化
- 易于浏览、便于理解



入侵检测技术

■ Unix系统日志

日志	内容	位置
lastlog	记录每个用户最近的成功登录和不成功登录	/var/adm/wtmp
loginlog	记录所有的不成功登录	/var/adm/acct/sum/loginlog
utmp(x)	记录当前登录的所有用户	/var/adm/utmp(x)
wtmp(x)	记录每个用户登录/退出的时间	/var/adm/wtmp(x)
sulog	记录su命令的使用	/var/adm/sulog
pacct	用户执行命令和资源使用情况	/var/adm/pacct
nis.trans	记录NIS名称空间的更改	/var/nis/trans.log



主机数据源

■ 优点

- 可利用操作系统本身提供的功能，因此检测效率高，速度快
- 可结合操作系统和应用程序的行为特征，得出更为准确的报告
- 可检测针对本机的入侵行为

■ 缺点

- 依赖于系统的可靠性
- 主机提供的信息有限
- 对网络层的入侵无能为力
- 必须为不同操作系统开发不同的程序
- 增加系统负荷



网络数据源

- 商业IDS最常用的信息来源
 - RealSecure,NFR,NetRanger,Snort...
- 利用以太网协议（IEEE 802.3）的广播机制



网络数据源

- 在一个共享式网络，可以监听所有的流量
- 目前有大量商业的、免费的监听工具，俗称嗅探器(sniffer)
 - 管理员可以用来监听网络的流量情况
 - 开发网络应用的程序员可以监视程序的网路情况
 - 黑客可以用来刺探网络情报



以太网的工作模式

- 网卡的MAC地址(48位)
 - 通过ARP来解析MAC与IP地址的转换
 - 用ipconfig/ifconfig可以查看MAC地址
- 正常情况下，网卡应该只接收这样的包
 - MAC地址与自己相匹配的数据帧
 - 广播包
- 网卡完成收发数据包的工作，两种接收模式
 - 混杂模式：不管数据帧中的目的地址是否与自己的地址匹配，都接收下来
 - 非混杂模式：只接收目的地址相匹配的数据帧，以及广播数据包(和组播数据包)
- 为了监听网络上的流量，必须设置为混杂模式



应用程序抓包

- **UNIX系统提供了标准的API支持**
 - **Packet socket**
 - **BPF**
- **Windows平台上通过驱动程序来获取数据包**
 - **驱动程序**
 - **WinPcap**



网络数据源

■ 优点

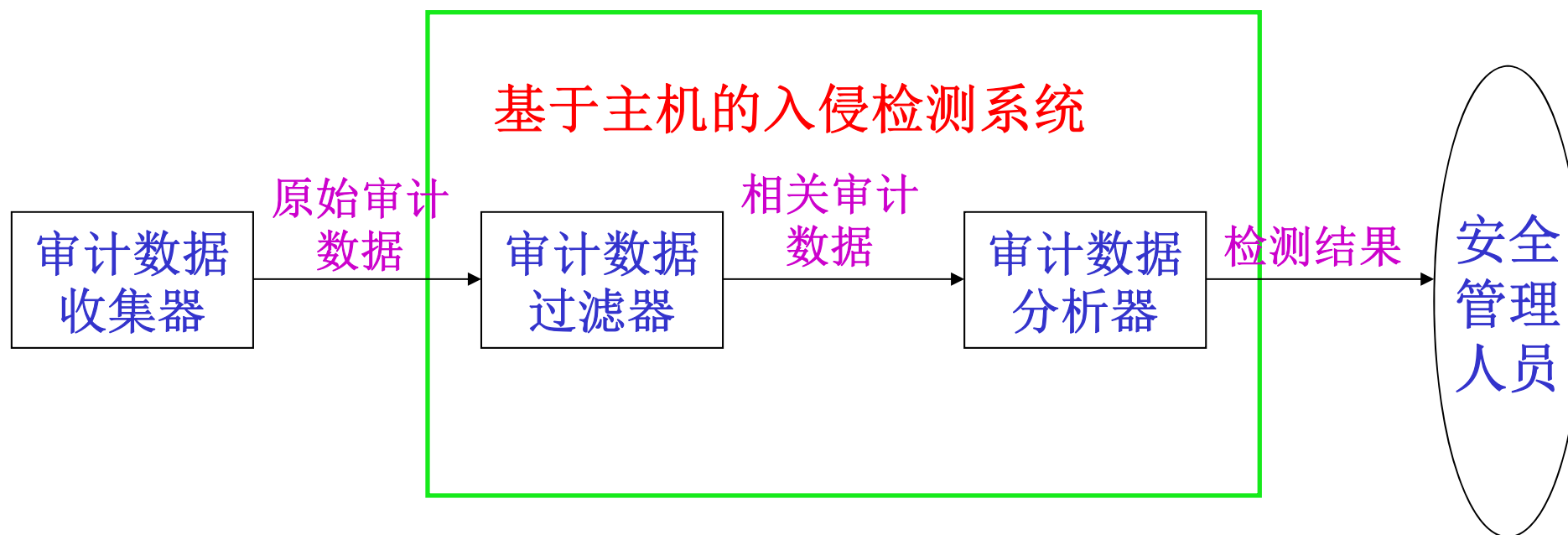
- 可以对整个子网进行检测
- 不影响现存的数据源，不改变系统和网络的工作模式
- 不影响主机性能和网络性能
- 被动接收方式，隐蔽性好
- 对基于网络协议的入侵手段有较强的分析能力

■ 缺点

- 检测效率
- 网络流量日益增大的挑战
- 虚警和漏警的平衡
- 应用于交换环境出现的问题

入侵检测系统

■ 基于主机的入侵检测系统





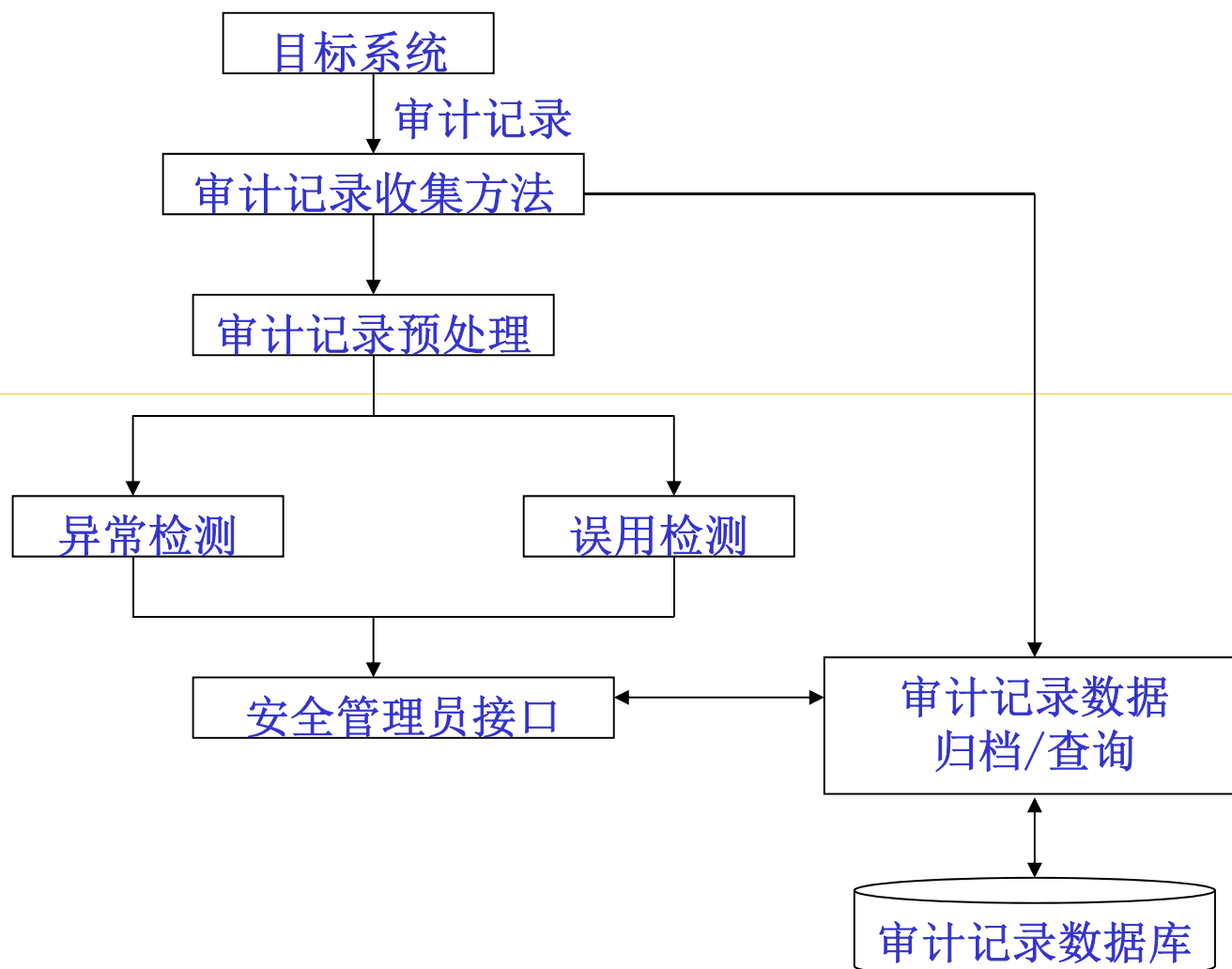
基于主机的检测威胁

- 特权滥用：当用户具有root权限、管理员特权时，该用户以非授权方式使用特权。
 - 具有提高特权的立约人
 - 前职员使用旧帐户
 - 管理员创建后门帐户
- 关键数据的访问及修改
 - 学生改变成绩、职员修改业绩、非授权泄露、修改WEB站点
- 安全配置的变化
 - 激活guest帐户



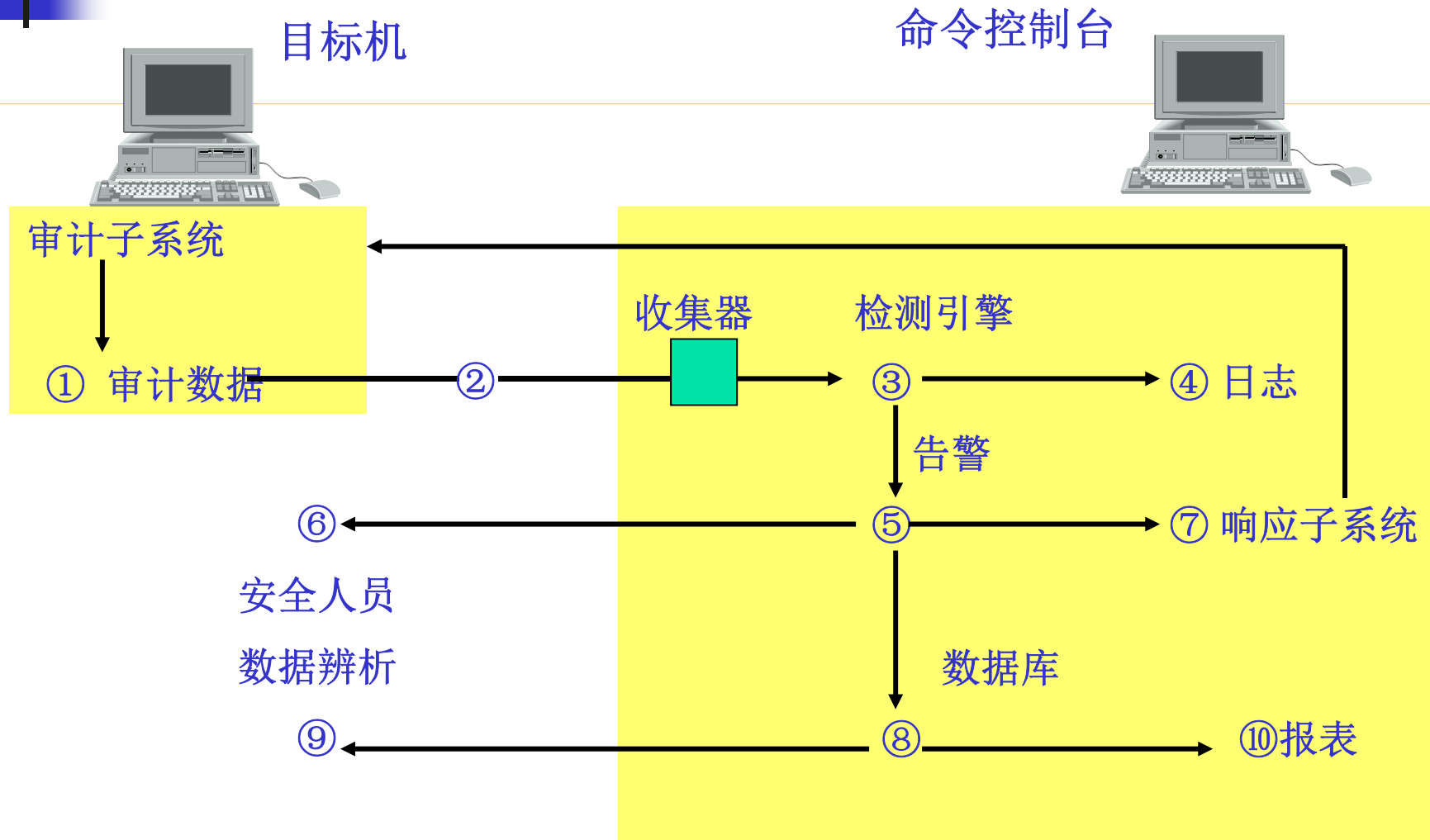
基于主机的入侵检测

- 基于主机的入侵检测系统通常是基于代理的，代理是运行在目标系统上的可执行程序，与中央控制计算机（命令控制台）通信。
 - 集中式：原始数据在分析之前要先发送到中央位置
 - 分布式：原始数据在目标系统上实时分析，只有告警命令被发送给控制台。



基于主机的入侵检测系统结构示意图

集中式的基于主机的入侵检测





集中式的基于主机的入侵检测

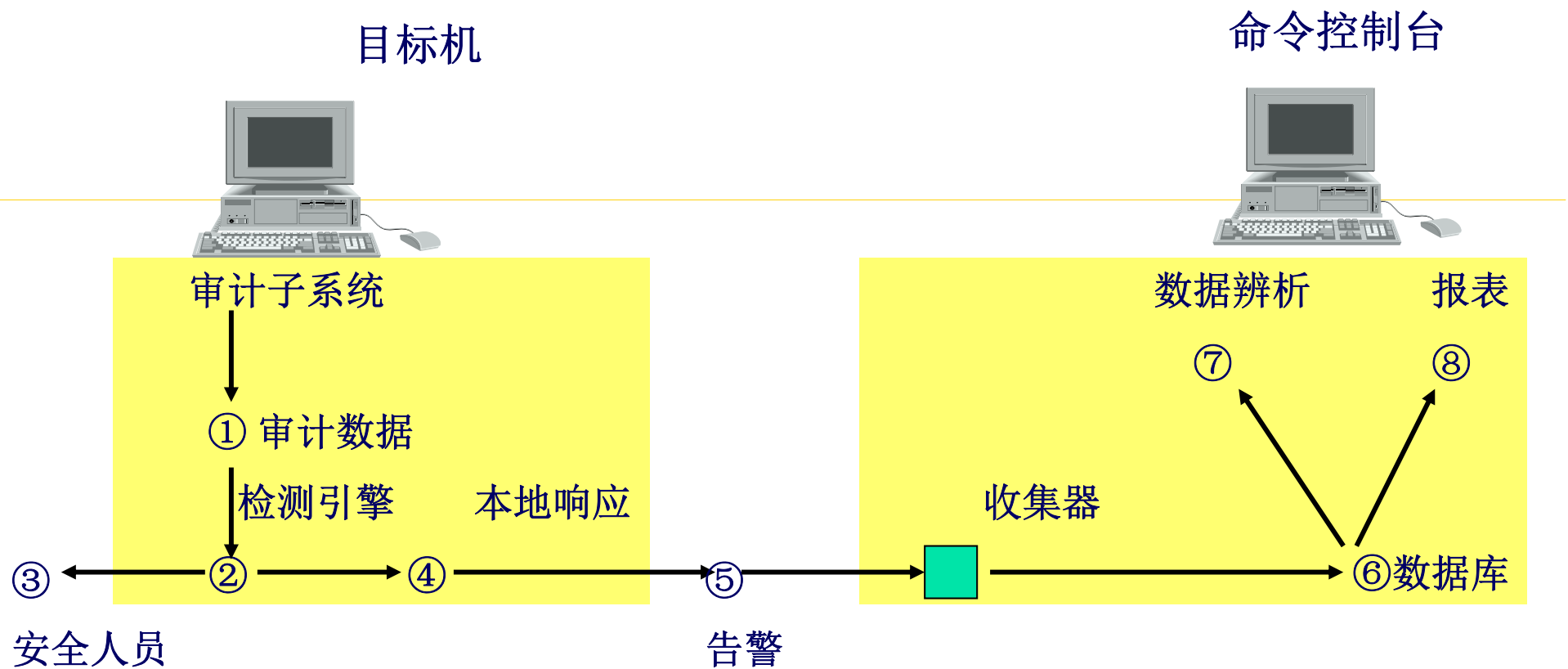
■ 优点

- 不会降低目标机的性能
- 统计行为信息
- 多主机标志、用于支持起诉的原始数据

■ 缺点

- 不能进行实时检测
- 不能实时响应
- 影响网络通信量

分布式的基于主机的入侵检测





分布式检测的优缺点

- 优点

- 实时告警
- 实时响应

- 缺点

- 降低目标机的性能
- 没有统计行为信息
- 没有多主机标志
- 没有用于支持起诉的原始数据
- 降低了数据的辨析能力
- 系统离线时不能分析数据



操作模式

- 基于主机的入侵检测系统的使用方式
 - 警告：用于检测关键任务误用
 - 监视：更尽力地观察几个主体的行为
 - 毁坏情况评估：确定计算机受损的程度
 - 遵从性：用于确定用户是否在遵守安全策略



基于主机的入侵检测

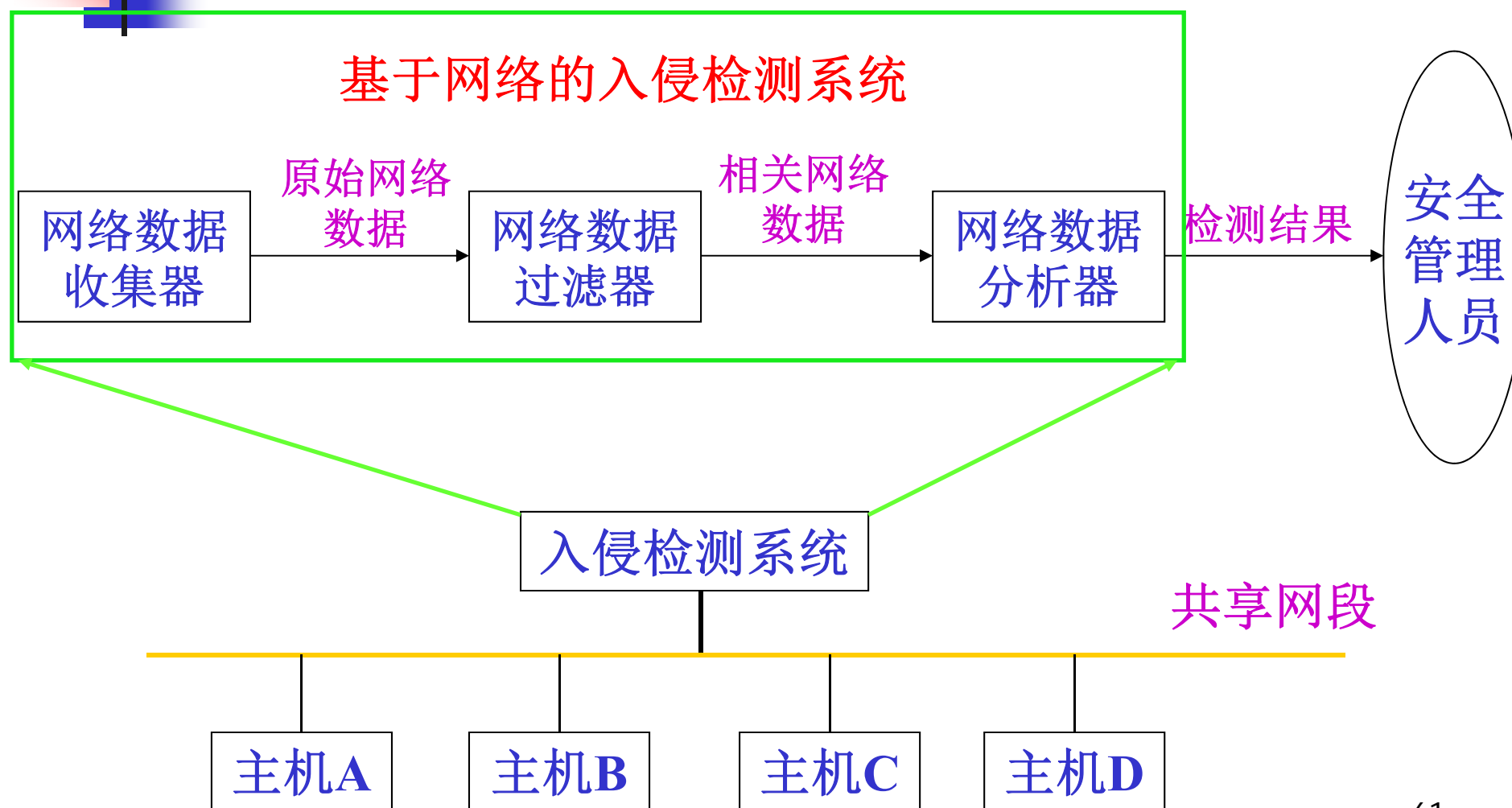
■ 优点

- 威慑内部人员
- 检测
- 通告及响应
- 毁坏情况评估
- 攻击预测
- 诉讼支持
- 行为数据辨析

■ 面临的问题

- 性能：降低是不可避免的
- 部署/维护
- 欺骗：审计源

入侵检测系统





基于网络的检测威胁

- 非授权访问
 - 非授权登录 (login)
 - 进行其它攻击的起始点
- 数据/资源的窃取
 - 口令下载
 - 带宽窃取
- 拒绝服务
 - 畸形分组: **land**
 - 分组泛洪: **packet flooding**
 - 分布式拒绝服务

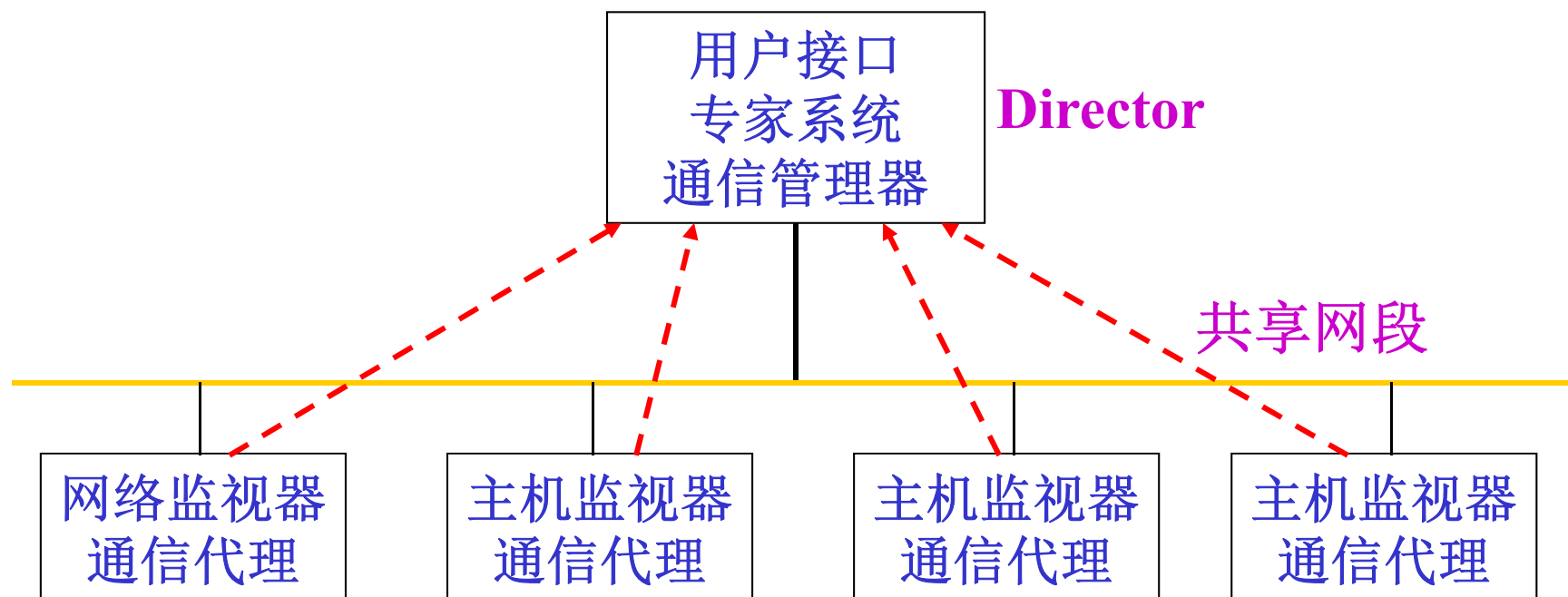


基于网络的入侵检测

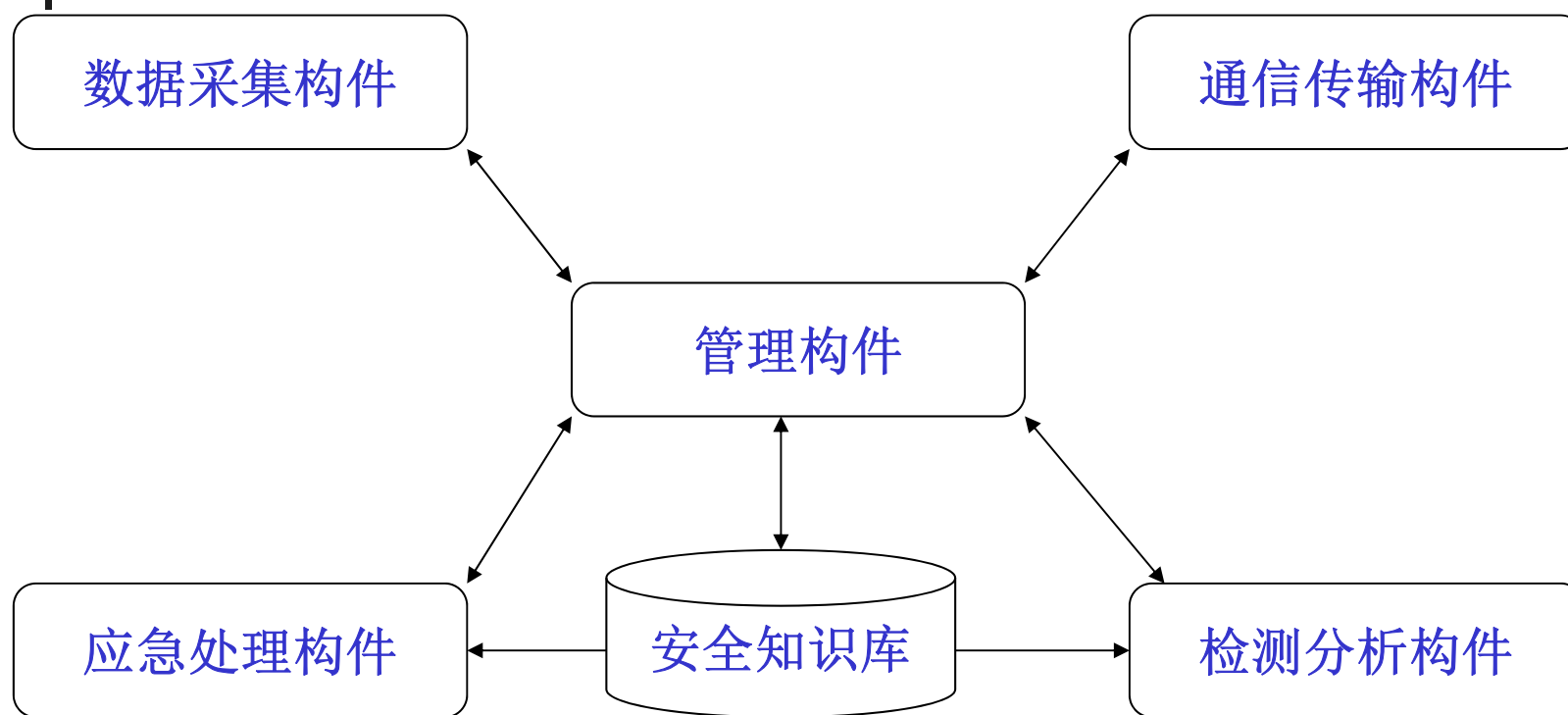
- 基于网络的入侵检测系统由遍及网络的传感器(Sensor)组成，传感器会向中央控制台报告。传感器通常是独立的检测引擎，能获得网络分组、找寻误用模式，然后告警
 - 传统的基于传感器的结构，（又被称为混杂模式网络入侵检测系统，或网络分接器(network tap)）
 - 分布式网络节点结构(network node)

入侵检测系统

分布式入侵检测系统



入侵检测系统



分布式基于网络的入侵检测系统结构



基于网络的入侵检测器的位置

- 放在防火墙之外
 - 通常放在DMZ区，无法检测到某些攻击，但可以看到自己的站点和防火墙暴露在多少种攻击之下
- 检测器在防火墙内
 - 少一些干扰，减少误报警；减少对检测器的攻击；发现防火墙的配置失误
- 防火墙内外都有检测器
 - 各有优势
- 检测器的其他位置
 - 与你有直接联系的合伙人和经常在防火墙内的供应商处
 - 高价值的地方
 - 有大量不稳定雇员的地方
 - 已被当作攻击目标的子网



操作模式

- 基于网络的入侵检测系统的使用方式
 - 警告
 - 监视
 - 辨析工作台：分析网络通信量



入侵检测器的响应

- 制订响应策略考虑的因素

- 系统用户：入侵检测系统用户可以分为网络安全专家或管理员、系统管理员、安全调查员。这三类人员对系统的使用目的、方式和熟悉程度不同，必须区别对待
- 操作运行环境：入侵检测系统提供的信息形式依赖其运行环境
- 系统目标：为用户提供关键数据和业务的系统，需要部分地提供主动响应机制
- 规则或法令的需求：在某些军事环境里，允许采取主动防御甚至攻击技术来对付入侵行为



入侵检测器的响应

- 主动响应

- 针对入侵者的措施——自动响应
- 系统修正——弥补缺陷
- 收集更详细的信息——**Honey Pot**

- 被动响应



自动响应

- 摧毁攻击
- 压制调速 (**Throttling**)
- **TCP RESET**
- 防火墙或网关的联动
- 联络攻击发起方的管理员



自动响应实例

■ 撤销连接

- 当攻击者对一个激活的端口进行连接，他向该端口发送一个或数个包，包含有攻击字符串或可开放该端口的程序。入侵检测系统检测到攻击字符串后，命令防火墙撤销连接

■ 隔离

- 如果在某一段时间段发生了足够多次的攻击，入侵检测系统就发出命令，将路由器的电源断掉



修正系统

- 针对受保护系统

- 弥补引起攻击的缺陷
- 隔离导致问题的部分

- 针对检测系统

- 改变监控范围或收集数据的粒度
- 改变分析引擎的操作方式和参数
- 添加、修改检测规则



诱骗攻击者

- 检测到入侵后，把攻击者引导到经过特殊装备的诱骗服务器上，这些服务器可以模拟关键系统的文件系统和其它系统特征，引诱攻击者进入，记录下攻击者的行为，从而获得关于攻击者的详细信息。
- 蜜罐（**Honey Pot**）技术



响应小组

- **CERT/CC**研究因特网安全漏洞以及系统脆弱性，提供事故响应和处理服务，发布安全警报，研究基于广域网环境的分布式计算问题，通过提供信息和培训来帮助提高公众的网络安全水平
- **FIRST(Forum of Incident Response Teams)**是一个国际性组织，专门致力于计算机安全事故的紧急响应及其相关问题的研究和交流



标准化

- 通用入侵检测框架**CIDF(The Common Intrusion Detection Framework)**
- **IETF**入侵检测工作组(**IDWG**)的入侵检测交换格式**IDEF(Intrusion Detection Exchange Format)**
- 漏洞和风险的标准 **CVE(Common Vulnerabilities and Exposures)**

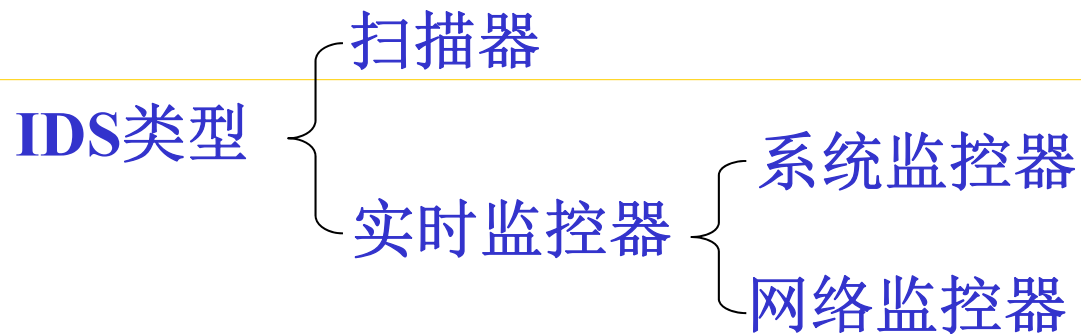


与其他安全产品的结合

- 防火墙
- 认证系统
- 访问控制系统
- 其它安全设备



入侵检测产品



- 基于统计分析的入侵检测技术
- 基于神经网络的入侵检测技术
- 基于专家系统的入侵检测技术
- 基于模型推理的入侵检测技术



入侵检测技术

■ 入侵检测产品

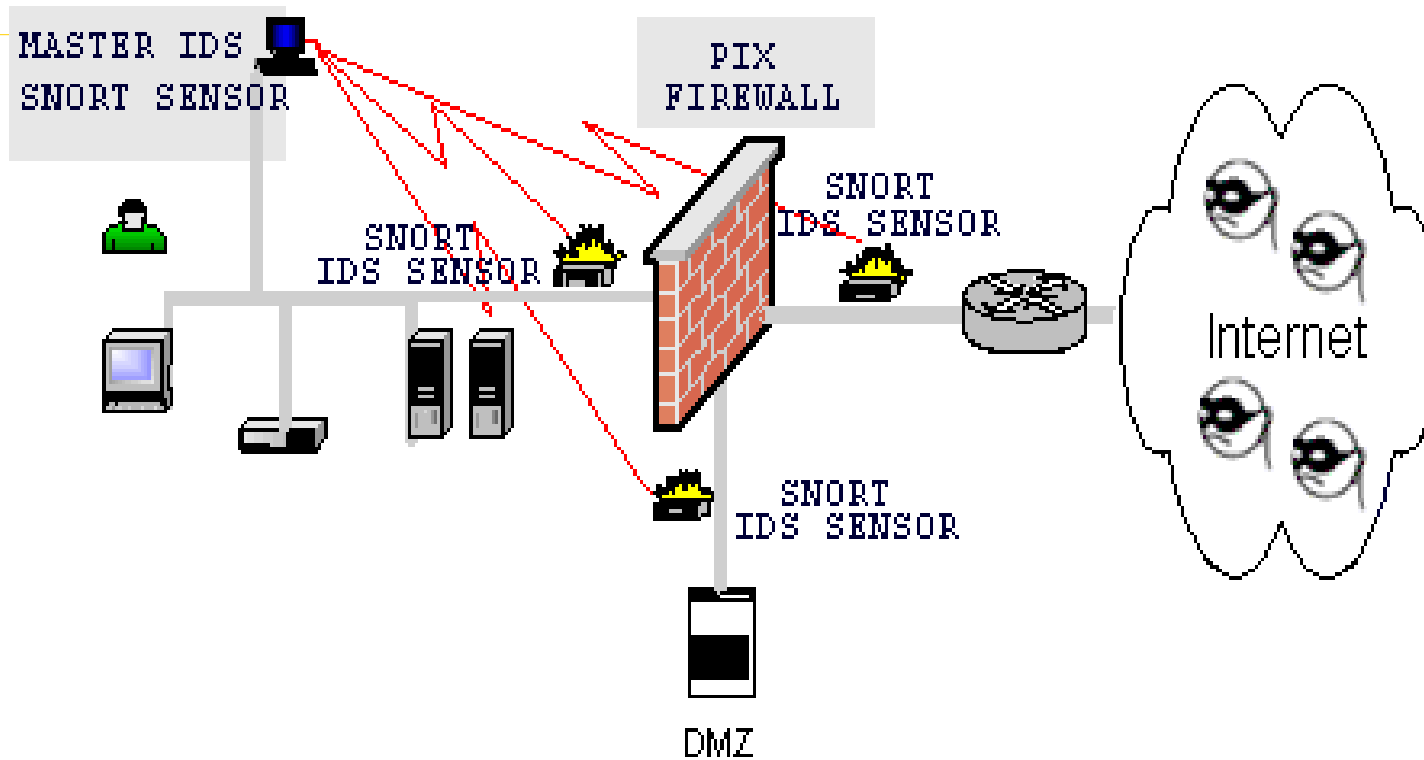
- **Snort——免费的IDS**
- **Cyber Cop IDS —NAI公司的网络安全产品**
- **NFR(NetWare Flight Recorder) —Anzen公司**
- **IERS系统（Internet Emergency Response Service）— IBM公司**
- **RIDS-100 — 瑞星公司**
- **天阆黑客入侵检测与预警系统—启明星辰信息技术有限公司**



入侵检测产品——snort

- 获取: <http://www.snort.org>
- 特点
 - 设计原则: 性能、简单、灵活
 - 包含三个子系统: 网络包的解析器、检测引擎、日志和报警子系统
 - 内置了一套插件子系统, 作为系统扩展的手段
 - 模式特征链——规则链
 - 也可以用作一个sniffer工具

Snort on Windows





入侵检测问题

- 新的入侵模式
- 大量的报警信息
- 分布式攻击
- 黑客跟踪



入侵检测问题

■ 新入侵模式

- 异常检测--- 哥伦比亚大学的WenkeLee研究小组采用数据挖掘的方法，通过关联分析、序列分析、分类算法等方法挖掘新的入侵模式，对于端口扫描、本地用户权限提升效果比较好，对于某些拒绝服务攻击和远程攻击效果不好。



入侵检测问题

■ 大量报警信息

- 数以千计的报警信息 99%报警信息
- IBM Zurich安全实验室找到根本原因(root cause)
- 很少几类的root cause占了90%的报警信息
- 这些root cause很多是误配置，无修改配置，不消除
- 找到报警信息的root cause，如果是属于上面的正常情况，不用分析。
- 例如： NAT使能的防火墙的端口扫描行为
Secondary DNS Server Zone Transfer



入侵检测问题

- 分布式拒绝服务攻击

- 问题:
 - --很容易控制数以百计的计算机
 - --攻击模式变化、难以预防
 - --从流量上检测异常（采样）
 - --ISP的责任



入侵检测问题

■ 黑客跟踪

- --检测到是否有攻击
- --确定谁在攻击
- --日志删除
- --跳板
- -----有成功的案例**Mitnick**



入侵检测问题

■ 黑客跟踪

- 1、Andrew Gross发现ISP Shimomura被侵害
- 2、ISP (Well)一用户发现奇怪的文件，中有Shimonmura。
- 3、隔离检查，检查日志，发现IP地址来自另一ISP NetCom
- 4、在NetCom安装程序，登录通知，查到电话交换机Raleigh，本想在Raleigh 查出电话号码，由于电话交换机也被攻破，没有查出。



入侵检测问题

■ 黑客跟踪

- 5、通过本地区只有两家蜂窝电话服务提供商，确定蜂窝电话服务提供商。
- 6、呼叫记录提供了蜂窝校区位置和电话的电子序列号，将范围锁定在某个蜂窝小区，直径5-8公里，电话号码是复制的，用户身份没有的。
- 7、在线监控蜂窝电话发射的信号，然后定位。



协同

- 目前**IDS**实现的功能是相对初级的
- **IDS**也需要充分利用数据信息的相关性
- **IDS**作为网络安全整体解决方案的重要部分，与其他安全设备之间应该有着紧密的联系
- **IDS**需要一种新的系统体系来克服自身的不足，并将**IDS**的各个功能模块与其他安全产品有机地融合起来，这就需要引入协同的概念



数据采集协同

- 基于网络的IDS需要采集动态数据（网络数据包）
- 基于主机的IDS需要采集静态数据（日志文件等）
- 目前的IDS将网络数据包的采集、分析与日志文件的采集、分析割裂开来，没有在这两类原始数据的相关性上作考虑。
- 在数据采集上进行协同并充分利用各层次的数据，是提高入侵检测能力的首要条件



数据分析协同

- 入侵检测不仅需要利用模式匹配和异常检测技术来分析某个检测引擎所采集的数据，以发现一些简单的入侵行为，还需要在此基础上利用数据挖掘技术，分析多个检测引擎提交的审计数据以发现更为复杂的入侵行为。



数据分析协同

- 两个层面上进行
 - 1. 单个检测引擎采集的数据：综合使用检测技术，以发现较为常见的、典型的攻击行为<—— 本地引擎
 - 2. 多个检测引擎的审计数据：利用数据挖掘技术进行分析，以发现较为复杂的攻击行为<—— 中心管理控制平台



数据挖掘

- 数据挖掘技术是一种决策支持过程，它主要基于AI，机器学习统计等技术，能高度自动化地分析原有数据，做出归纳性推理，从中挖掘出潜在的模式，预测出客户的行为
- 运用关联分析，能够提取入侵行为在时间和空间上的关联，可以进行的关联包括源IP关联、目标IP关联、数据包特征关联、时间周期关联、网络流量关联等；
- 运用序列模式分析可以进行入侵行为的时间序列特征分析；
- 利用以上的分析结构，可以制订入侵行为的分类标准，并进行形式化的描述，通过一定的训练数据集来构造检测模型；
- 运用聚类分析，能优化或完全抛弃既有的模型，对入侵行为重新划分并用显示或隐式的方法进行描述



数据挖掘

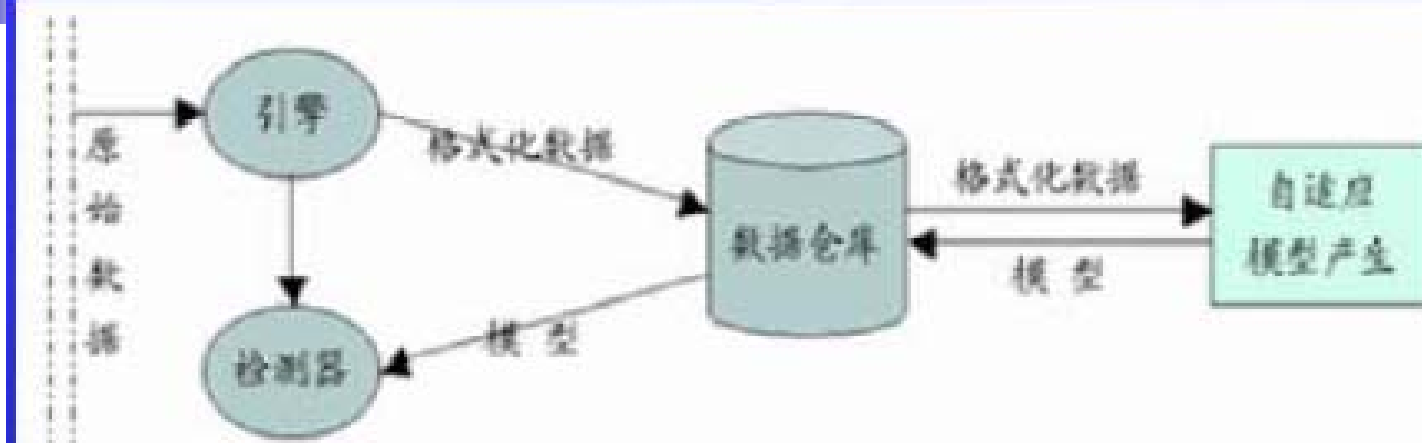
- 数据准备
- 数据清理和集成
- 数据挖掘
- 知识表示
- 模式评估



数据挖掘

- 1. 从审计数据中提取特征，以帮助区分正常数据和攻击行为
- 2. 将这些特征用于模式匹配或异常检测模型
- 3. 描述一种人工异常产生方法，来降低异常检测算法的误报率
- 4. 提供一种结合模式匹配和异常检测模型的方法

数据挖掘



- 1. 引擎观察原始数据并计算用于模型评估的特征
- 2. 检测器获取引擎的数据并利用检测模型来评估它是否是一个攻击
- 3. 数据仓库被用作数据和模型的中心存储地;
- 4. 模型产生的主要目的是为了加快开发以及分发新的入侵检测模型的速度

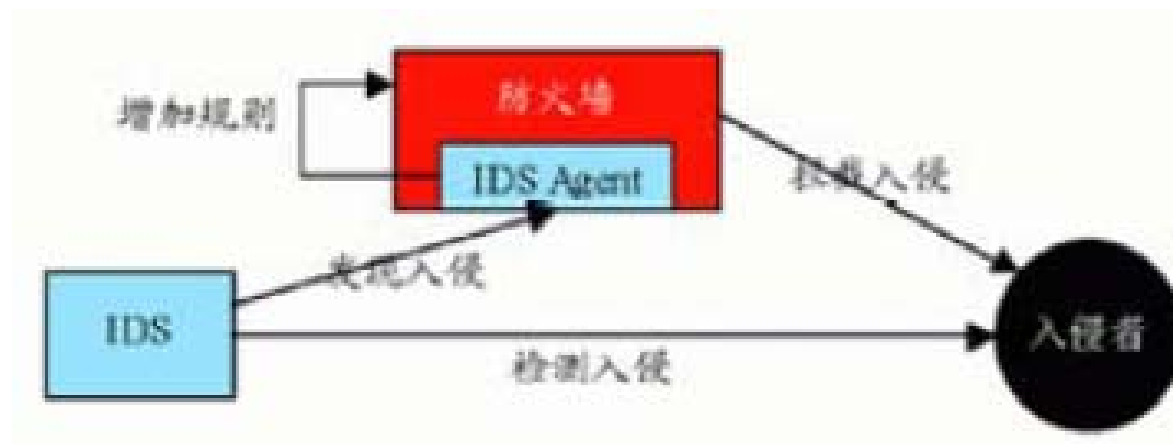


响应协同

- 理想的情况是，建立相关安全产品能够相互通信并协同工作的安全体系，实现防火墙、IDS、病毒防护系统和审计系统等的互通与联动，以实现整体安全防护
- 响应协同：当**IDS**检测到需要阻断的入侵行为时，立即迅速启动联动机制，自动通知防火墙或其他安全控制设备对攻击源进行封堵，达到整体安全控制的效果。
 - IDS与防火墙的联动，可封堵源自外部网络的攻击
 - IDS与网络管理系统的联动，可封堵被利用的网络设备和主机
 - IDS与操作系统的联动，可封堵有恶意的用户账号
 - IDS与内网监控管理系统的联动，可封堵内部网络上恶意的主机

IDS与Firewall联动

- 通过在防火墙中驻留的一个IDS Agent对象，以接收来自IDS的控制消息，然后再增加防火墙的过滤规则，最终实现联动



- Cisco CIDE(CISL)
- ISS Checkpoint




其它-报警信息融合

- 虽然目前多种网络入侵检测系统都采用了分布式结构，但对于收到的报警信息，管理器只是进行简单的统计和显示，或只能针对特定类型的事件进行关联分析，但是没有对这些来自不同网络区域的Sensor的报警信息进行汇总分析或做进一步的融合判断，因而无法检测一些复杂的攻击模式，如分布式攻击等。
- 单一的检测方法或检测系统难以检测各种复杂的攻击，综合多种检测技术和多种检测系统能够有效提高检测的准确性。这就需要对源自不同检测方法或检测系统的检测结果进行融合，得到一个综合的判别结果。
- 为了能够适应攻击者身份识别、计算机和网络的安全态势评估等更高层次的安全需求，同样也需要多个网络检测器、多个入侵检测系统的报警信息进行融合处理。



其它-网络流量异常检测

- 网络流量异常检测是网络入侵检测系统的重要组成部分。DoS、DDoS、网络蠕虫等多种攻击都会引起网络流量的异常变化。
- 以单位时间内的包数作为网络流量特征，使用神经网络检测流量异常的方法；
- 通过对多种异常报文的分析来检测各种DoS 攻击；
- 通过TCP 报文中SYN, FIN 和RST 报文之间的比例关系，使用异常点检测的方法来检测SYN Flooding 攻击；
- 对网络流数目的可视化为管理员判断是否发生网络流量异常提供决策支持；
- 通过建立基于TCP 的连接请求到达模型（Poisson 模型）来检测网络异常
- 研究使用神经网络对会话统计参数如TCP SYN 包数、TCP FIN包数，以及在统计单位时间内建立的TCP 连接数等来检测网络流量异常。



其它-攻击源追踪

- 攻击者可以轻易地获得匿名性，从而逃避惩罚，这是导致网络攻击得以泛滥的一个重要原因。
- 所谓伪造报文攻击，就是攻击者通过伪造报文的源IP 地址，来达到隐藏攻击主机地址的目的。伪造报文攻击主要用于DoS，DDoS等攻击，如SYNFlooding、Smurf、Shaft 等。在端口扫描、TCP 会话劫持、盗取主机机密信息、利用应用程序漏洞获取root 权限等网络攻击中，攻击者需要和目标主机进行交互，必须使用真实的网络地址，这时攻击者就可以采用间接攻击来隐藏自己的真实网络地址。
- 在间接攻击中，攻击者首先连接到一个存在安全漏洞或提供网络代理服务的主机CH1，再从CH1 连接到CH2，从CH2 对目标发动攻击。攻击路线图为攻击者--->CH1--->CH2--->目标。从被攻击的主机只能看到攻击主机CH2，而无法获知攻击源主机。攻击源追踪分为基于主机的攻击源追踪和基于网络的攻击源追踪两部分。



其它-基于主机的攻击源追踪

- **DIDS** (**Distributed Intrusion Detection System**) 是一个基于主机的分布式入侵检测系统，在域中的每个主机上都有一个监控程序**Host Monitor**，负责收集本机的日志信息，并对其进行分析，然后将重要的事件比如登录事件等报告给一个中央管理器**Director**。**Director** 对各个**Host Monitor** 报告的信息进行综合分析，就可以构造出用户在各个主机的登录路径，从而获得用户登录的源头。
- **Caller ID** **Caller ID** 利用反向攻击来追踪攻击的源头：假设：如果攻击者通过一些中间主机发动攻击，那么极有可能在这些中间主机上存在漏洞，从而使得攻击者可以访问这些主机。当发生攻击时，**Caller-ID** 可以沿着逆向路径攻击主机，不断获得上一个主机的地址，依次类推，最终获得攻击者的真实地址。



其它-基于网络的攻击源追踪

- 数据指纹技术在间接攻击中，假如攻击者在主机 H1，H2，H3，H4 上依次登录，其每次操作都会产生一个从H1 到H2的报文，H2 处理完后，把相应的信息再发送给H3，同样，H3 也会发送报文给H4，命令最后在H4 得以执行。由远程登录的原理可以知道，H1 和H2，H2 和H3，H3 和H4 间传递的报文内容都是相同的。如果可监测到不同主机间的所有通信内容，通过分析就可以得知它们是否属于同一登录链，再由监测到报文的时间就可以确定登录的先后顺序，从而找到登录链的源头。



其它-基于网络的攻击源追踪

- TCP Connection Chain: Kunikazu Yoda 和Hiroaki Etoh 提出了基于TCP 序列号的登录链追踪办法。通过监测记录每个网段上所有TCP 连接发送数据的序列号，就可以判断它们是否属于同一登录链。



入侵检测的发展方向

- 体系结构方面进一步研究分布式入侵检测与通用入侵检测框架
- 应用层入侵检测
- 智能的入侵检测
- 提供高层统计与决策
- 响应策略与恢复研究
- 入侵检测的评测方法
- 和其他网络安全部件的协作、与其他安全技术的结合



参考文献

- 黄传河等, 网络安全, 武汉大学出版社, 2004,6
- 韩东海、王超等,入侵检测系统及实例剖析, 清华大学出版社, 2002, 5
- **Rebeca Gurley Bace**, 入侵检测, 人民邮电出版社,2001,6
- 张世永, 网络安全原理与应用, 科学出版社, 2003,5
- **Stephen Northcutt**,网络入侵检测分析员手册, 人民邮电出版社,2000,10
- 入侵检测讲义, 北京大学信息安全研究所
- 入侵检测讲义, 上海交大陈克非