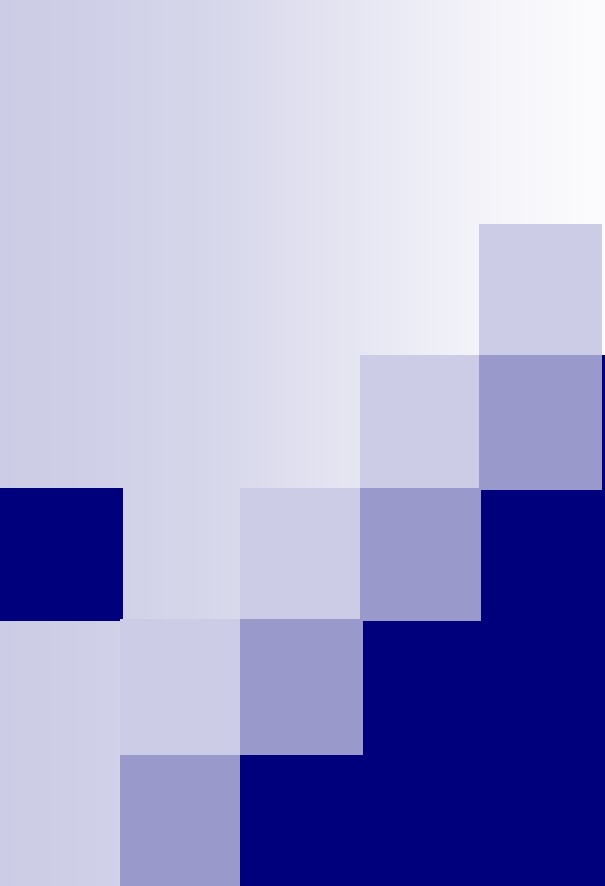




保密平安与密码技术

第八讲 入侵检测系统IDS

课程内容

- 入侵知识简介
- 入侵检测技术
- 入侵检测系统的选择和使用



课程目标

- 了解入侵检测的概念、术语
- 了解入侵检测产品部署方案
- 了解入侵检测产品选型原则
- 了解入侵检测技术开展方向



入侵知识简介

■ 入侵 (Intrusion)

- 入侵是指未经授权蓄意尝试访问信息、篡改信息，使系统不可靠或不能使用的行为。
- 入侵企图破坏计算机资源的完整性、机密性、可用性、可控性

■ 入侵者

- 入侵者可以是一个手工发出命令的人，也可是一个基于入侵脚本或程序的自动发布命令的计算机。

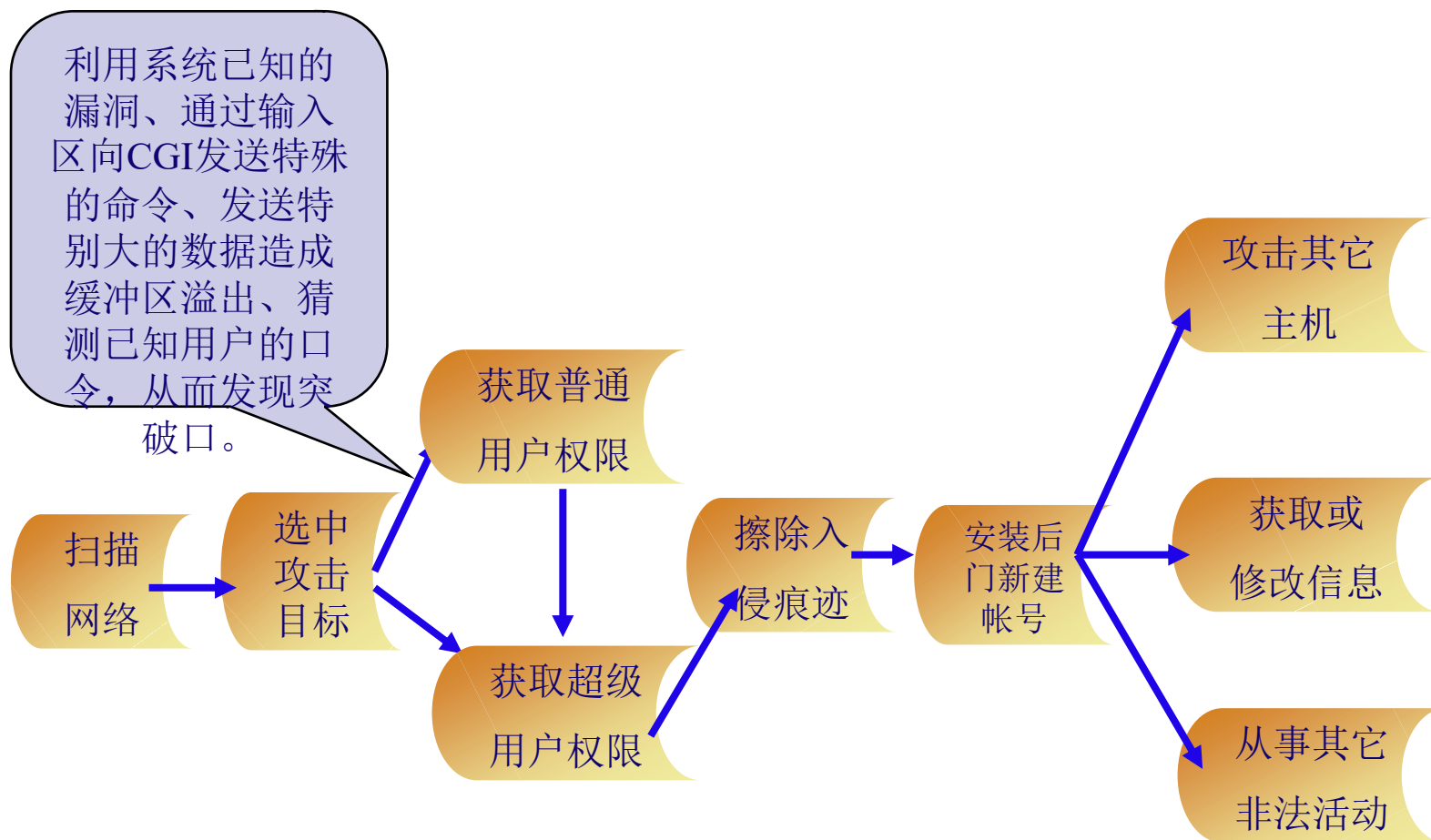
入侵知识简介

- 目前主要漏洞：
 - 缓冲区溢出
 - 拒绝效劳攻击漏洞
 - 代码泄漏、信息泄漏漏洞
 - 配置修改、系统修改漏洞
 - 脚本执行漏洞
 - 远程命令执行漏洞
 - 其它类型的漏洞
- 侵入系统的主要途径
 - 物理侵入
 - 本地侵入
 - 远程侵入

网络入侵的一般步骤

- 进行网络攻击是一件系统性很强的工作，其主要工作流程是：
- 目标探测和信息收集
- 自身隐藏
- 利用漏洞侵入主机
- 稳固和扩大战果
- 去除日志

网络入侵步骤总览



入侵检测系统概述

■ 概要

□ 背景介绍

□ 入侵检测的提出

□ 入侵检测相关术语

□ 入侵检测系统分类

□ 入侵检测系统构件

□ 入侵检测系统部署方式





背景介绍

信息社会出现的新问题

信息时代到来，电子商务、电子政务，网络改变人们的生活，人类进入信息化社会

计算机系统与网络的广泛应用，商业和国家机密信息的保护以及信息时代电子、信息对抗的需求

存储信息的系统面临的极大的平安威胁

潜在的网络、系统缺陷危及系统的平安

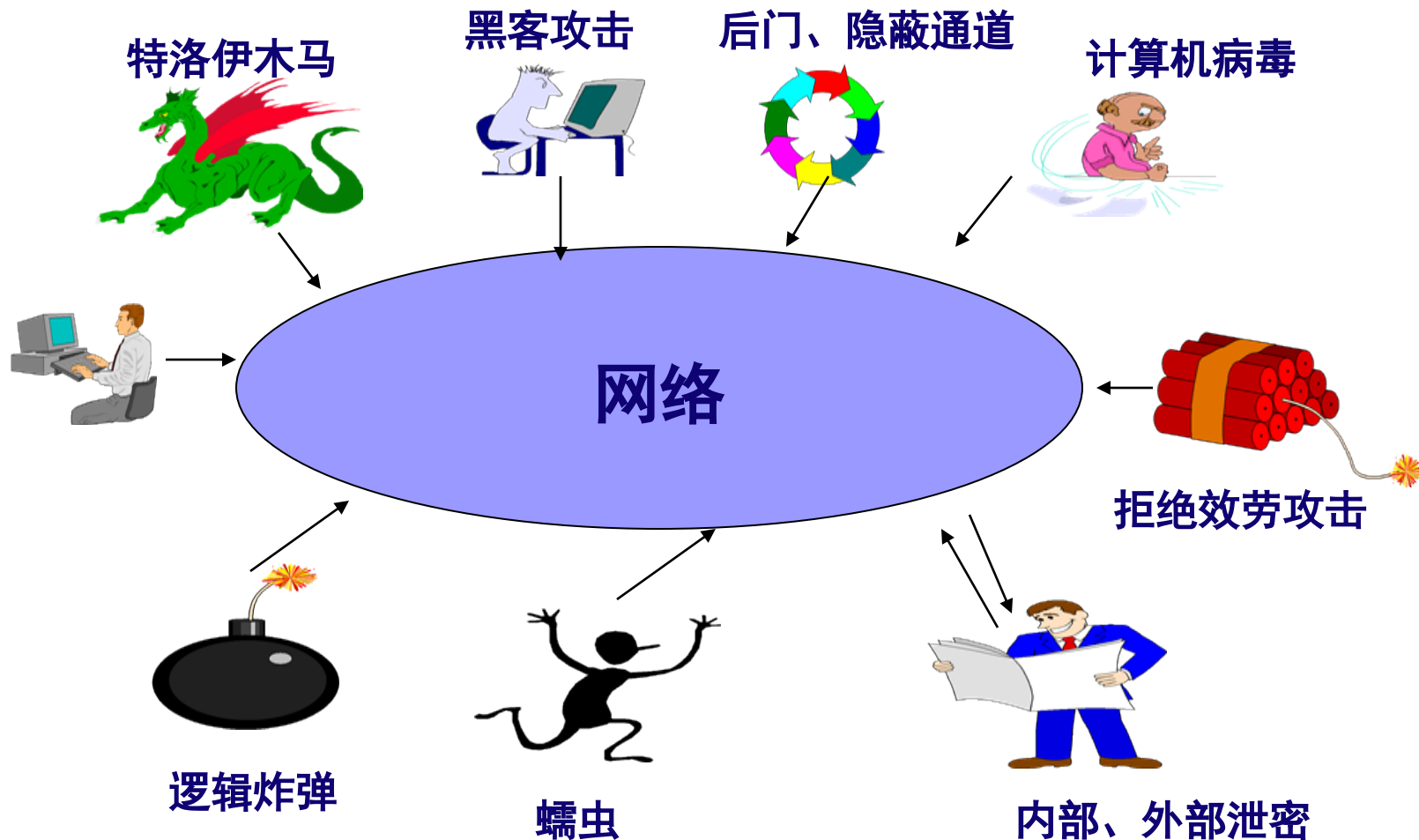
传统的平安保密技术都有各自的局限性，不能够确保系统的平安

信息系统的平安问题

操作系统的脆弱性

计算机网络的资源开放、信息共享以及网络复杂性增

黑客攻击猖獗



背景介绍

我国平安形势非常严峻

1998年2月25日：黑客入侵中国公众多媒体通信网广州蓝天**BBS**系统并得到系统的最高权限，系统失控长达**15**小时。为国内首例网上黑客案件。

1998年9月22日，黑客入侵扬州工商银行电脑系统，将**72**万元注入其户头，提出**26**万元。为国内首例利用计算机盗窃银行巨款案件。

1999年4月16日：黑客入侵中亚信托投资公司上海某证券营业部，造成**340**万元损失。

1999年11月23日：银行内部人员通过更改程序，用虚假信息从本溪某银行提取出**86**万元。

背景介绍

我国平安形势非常严峻〔续〕

2000年2月1日：黑客攻击了大连市赛伯网络效劳有限公司，造成经济损失**20**多万元。

2000年2月1日至2日：中国公共多媒体信息网兰州节点——“飞天网景信息港”遭到黑客攻击。

2000年3月2日：黑客攻击世纪龙公司**21CN**。2000年3月6日至8日：黑客攻击实华开**EC123**网站达**16**次，同一时期，号称全球最大的中文网上书店“当当书店”也遭到屡次黑客攻击。

2000年3月8日：山西日报国际互联网站遭到黑客数次攻击，被迫关机，这是国内首例黑客攻击省级党报网站事件。

2000年3月8日：黑客攻击中国最大的中文电子邮局——拥有

入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式





入侵检测的提出

什么是入侵检测系统

入侵检测系统是一套监控计算机系统或网络系统中发生的事件，根据规那么进行平安审计的软件或硬件系统。



入侵检测的提出

为什么需要IDS?

入侵很容易

入侵教程随处可见

各种工具唾手可得

防火墙不能保证绝对的平安

网络边界的设备

自身可以被攻破

对某些攻击保护很弱

不是所有的威胁来自防火墙外部

入侵检测的提出

入侵检测的任务

通过事先发现风险来阻止入侵事件的发生，
提前发现试图攻击或滥用网络系统的人员
检测其它平安工具没有发现的网络工具事件。
提供有效的审计信息，详细记录黑客的入侵
过程，从而帮助管理员发现网络的脆弱性。
检测来自内部的攻击事件和越权访问
85%以上的攻击事件来自于内部的攻击
防火墙只能防外，难于防内

入侵检测的提出

入侵检测的开展历史

1980年，James Anderson最早提出入侵检测概念

1987年，D. E. Denning首次给出了一个入侵检测的抽象模型，并将入侵检测作为一种新的平安防御措施提出。

1988年，Morris蠕虫事件直接刺激了IDS的研究

1988年，创立了基于主机的系统,有IDES, Haystack等

1989年，提出基于网络的IDS系统 有NSM,

入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式



入侵检测相关术语

- IDS(Intrusion Detection Systems)入侵检测系统
- Promiscuous 混杂模式
- Signatures 特征
- Alerts 警告
- Anomaly 异常
- Console 控制台
- Sensor 传感器

入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式



入侵检测系统分类

■ 概要

- Host-Based IDS

- Network-Based IDS

- Stack-Based IDS

Host-Based IDS(HIDS)

■ 基于主机的入侵检测系统，系统安装在主机上面，对本主机进行平安检测

■ HIDS优点

- 性能价格比高
- 细腻性，审计内容全面
- 视野集中
- 适用于加密及交换环境

■ HIDS缺点

- 额外产生的平安问题
- HIDS依赖性强
- 如果主机数目多，代价过大
- 不能监控网络上的情况

Network-Based IDS(NIDS)

基于网络的入侵检测系统，系统安装在比较重要的网段内

■ NIDS优点

检测范围广

无需改变主机配置
和性能

独立性和操作系统
无关性

安装方便

■ NIDS缺点

□ 不能检测不同网段的网络包

□ 很难检测复杂的需要大量计算的攻击

□ 协同工作能力弱

□ 难以处理加密的会话



Stack-Based IDS(NNIDS)

- 网络节点入侵检测系统
- 安装在网络节点的主机中
- 结合了NIDS和HIDS的技术
- 适合于高速交换环境和加密数据

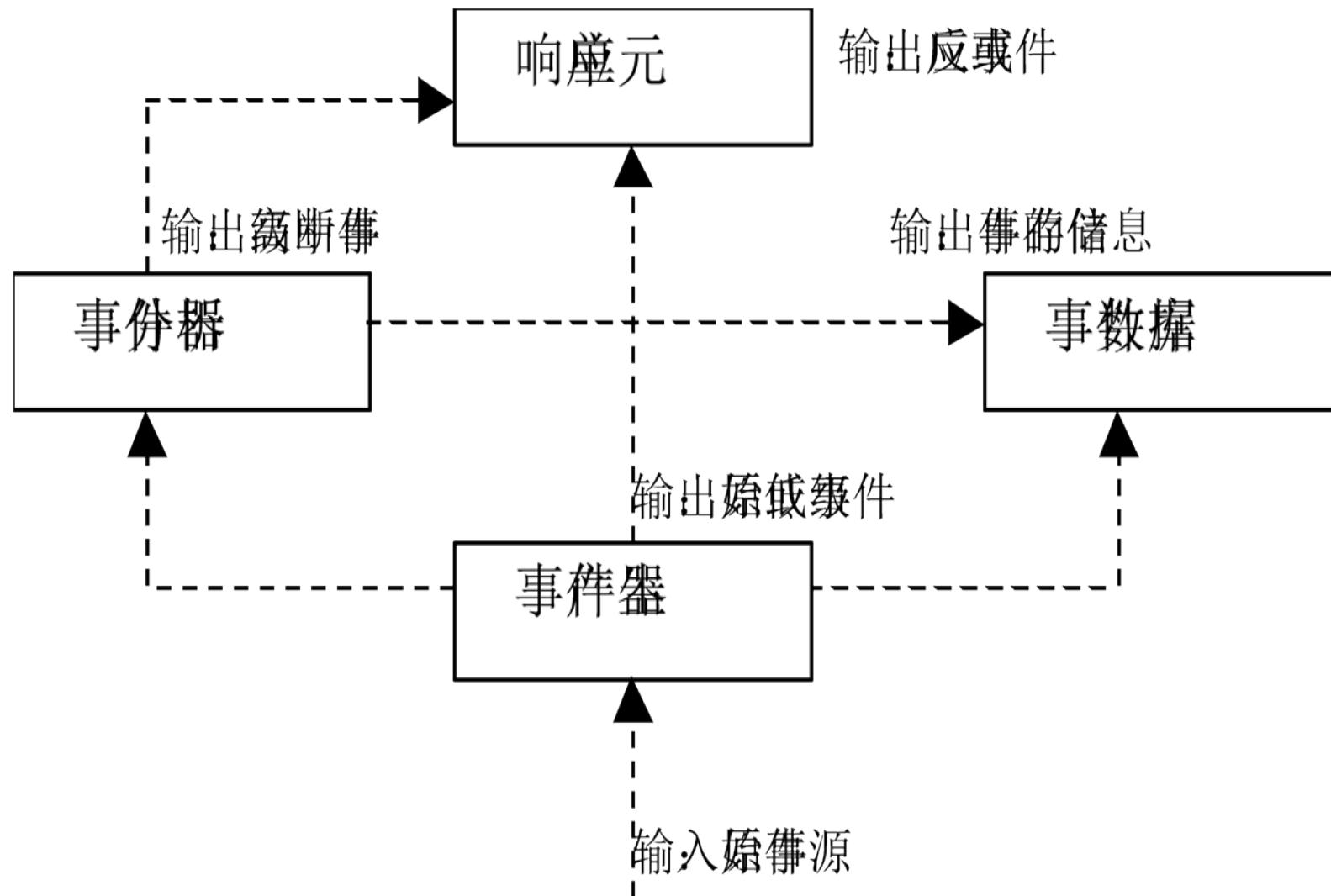
入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式



入侵检测系统构件



入侵检测系统构件

- 事件产生器(Event generators)
- 事件产生器的目的是从整个计算环境中获得事件，并向系统的其他局部提供此事件。
- 事件数据库(Event databases)
 - 事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

入侵检测系统构件

- 事件分析器(Event analyzers)

- 事件分析器分析得到的数据，并产生分析结果。

- 响应单元(Response units)

- 响应单元那么是对分析结果作出作出反响的功能单元，它可以作出切断连接、改变文件属性等强烈反响,甚至发动对攻击者的还击，也可以只是简单的报警。

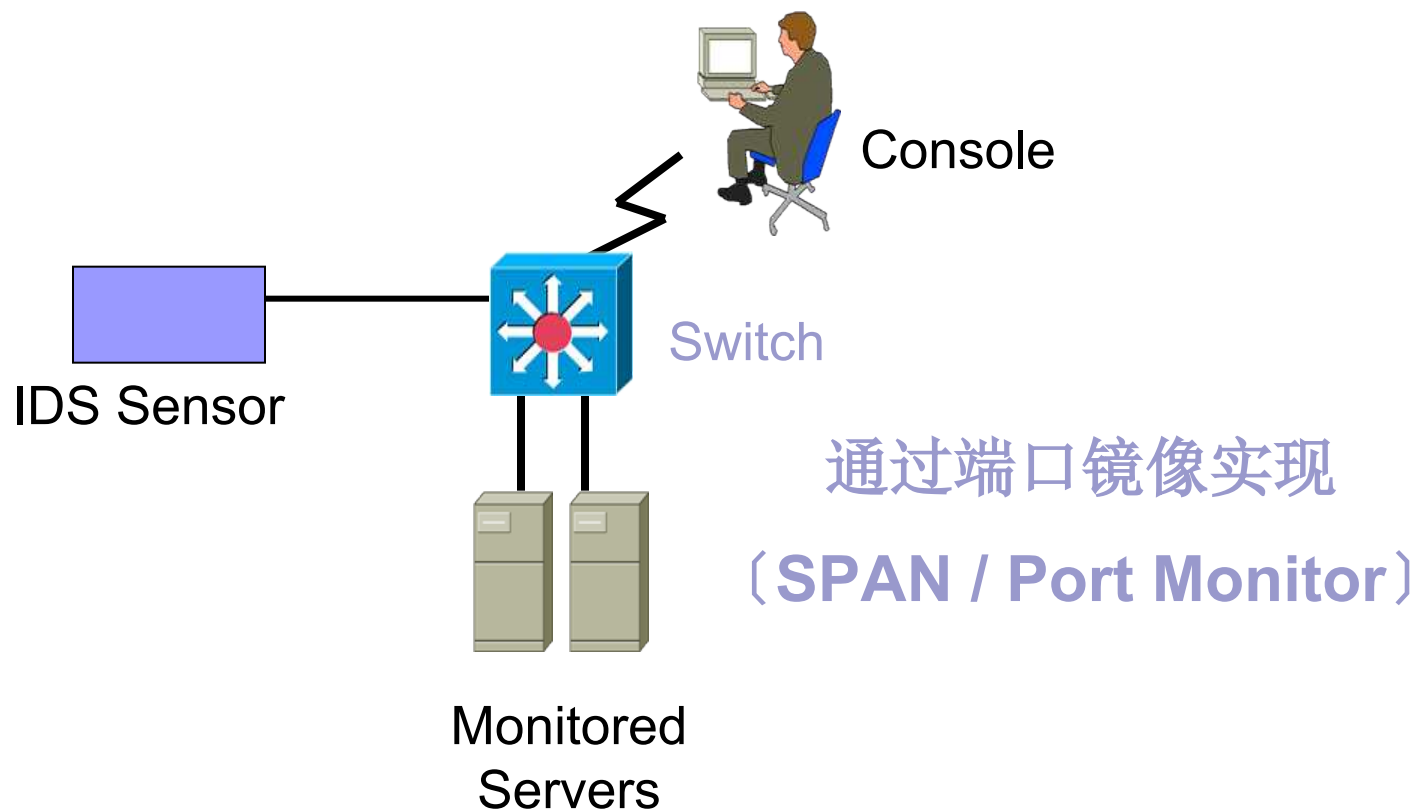
入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式



入侵检测系统部署方式

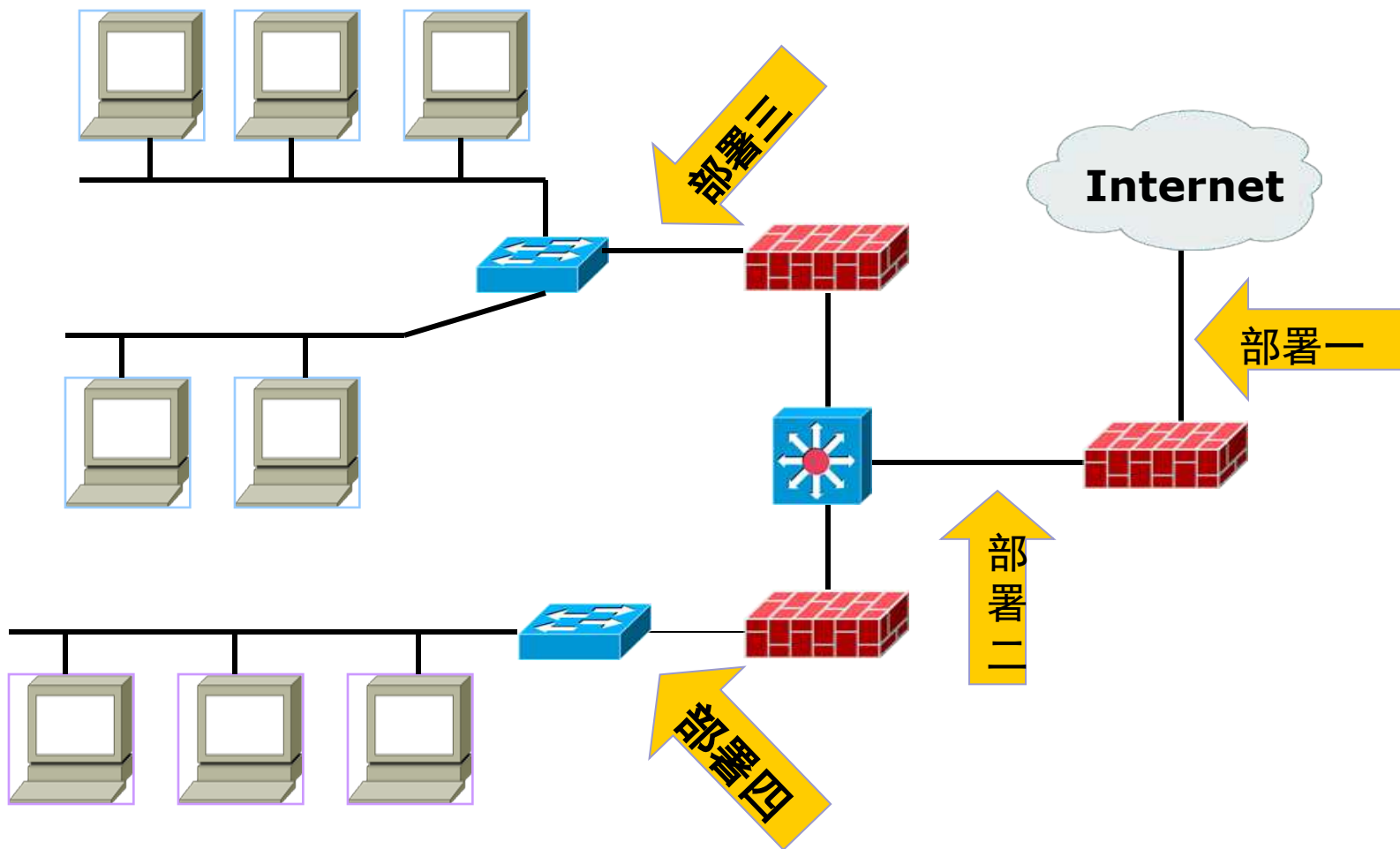




检测器部署位置

- 放在边界防火墙之内
- 放在边界防火墙之外
- 放在主要的网络中枢
- 放在一些平安级别需求高的子网

检测器部署示意图



入侵检测系统部署方式

- 检测器放置于防火墙的**DMZ**区域
 - 可以查看受保护区域主机被攻击状态
 - 可以看出防火墙系统的策略是否合理
 - 可以看出**DMZ**区域被黑客攻击的重点
- 检测器放置于路由器和边界防火墙之间
 - 可以审计所有来自**Internet**上面对保护网络的攻击数目
 - 可以审计所有来自**Internet**上面对保护网络的攻击类型

入侵检测系统部署方式

- 检测器放在主要的网络中枢
 - 监控大量的网络数据，可提高检测黑客攻击的可能性
 - 可通过授权用户的权利周界来发现为授权用户的行为
- 检测器放在平安级别高的子网
- 对非常重要的系统和资源的入侵检测

入侵检测系统概述

■ 概要

- 背景介绍
- 入侵检测的提出
- 入侵检测相关术语
- 入侵检测系统分类
- 入侵检测系统构件
- 入侵检测系统部署方式

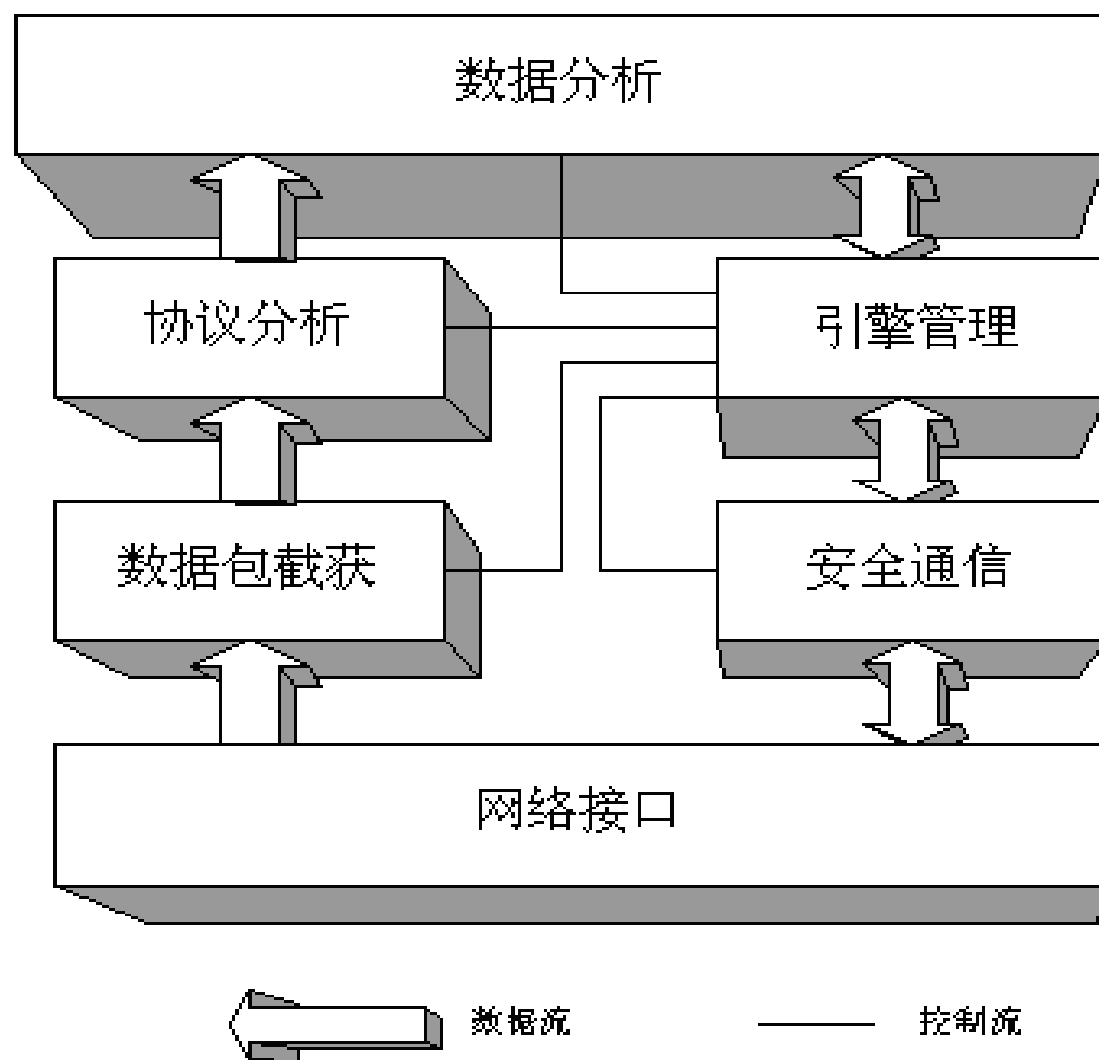


入侵检测原理与技术

- 概要
- IDS工作流程
- 入侵检测的分析方式
- 入侵检测的实现技术
- 入侵检测的缺陷
- 入侵检测的评估与测试
- 入侵检测的选型原那么
- 入侵检测的缺乏和开展趋势



入侵检测引擎工作流程



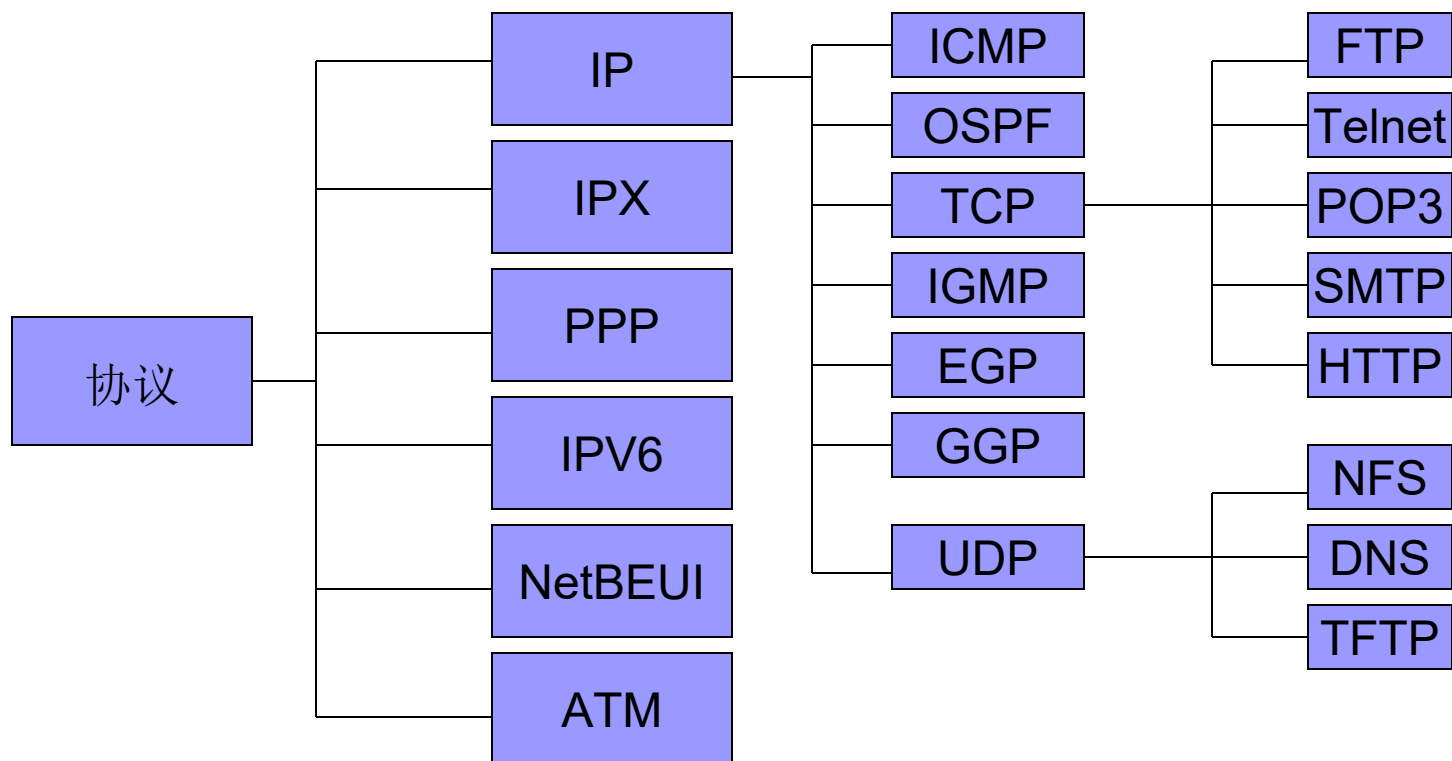
监听局部

- 网络接口混杂模式
- 根据设置过滤一些数据包
- 过滤程序的算法的重要性

监听器设置如下规那么进行过滤：

Only check the following packet
源地址为192.168.0.1

协议分析





数据分析

- 根据相应的协议调用相应的数据分析函数
- 一个协议数据有多个数据分析函数处理
- 数据分析的方法是入侵检测系统的核心
- 快速的模式匹配算法

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/065214230324011211>