# 第一章 信息安全概述

## 信息及其特征

定义概括：

信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征

信息安全的基本要求——信息安全基础三角形C.I.A.

机密性（Confidentiality）防止未经授权使用信息：确保信息没有非授权的泄漏，不被非授权的个人、组织和计算机程序使用。

完整性（Integrity）防止对信息的非法修改和破坏：确保信息没有遭到篡改和破坏

可用性（Availability）确保及时可靠地使用信息：确保拥有授权的用户或程序可以及时、正常使用信息

信息安全的其他方面

信息的不可否认性（Non-repudiation ）要求无论发送方还是接收方都不能抵赖所进行的传输

真实性（truth）对信息的来源进行判断，能对伪造来源的信息予以鉴别。

可控制性（controllability）对信息的传播及内容具有控制能力。

可审查（Accountability）确保实体的活动可被跟踪

可靠性（Reliability）系统在规定的条件下和规定的时间内完成指定功能的概率

## 安全策略包括

包括 制度、技术、管理

与安全相关的黄金法则

第一，有连通性(Connectivity)就意味着风险

第二，安全是相对的概念

第三，必须从整个系统的角度去考虑安全问题

第四，实施安全的措施必须简单

第五，安全的实现必须注意性能价格比

基于时间的PDR模型

信息安全相关活动，都要消耗时间

P：防护(Protection)，PT：防御时间

D：检测(Detection)，DT：检测时间

R：响应(Reaction)，RT：响应时间

P2DR安全模型：策略、防护、检测、响应

# 第二章 网络威胁、攻击与网络协议安全性

## 攻击和威胁

攻击（Attack）

任何违背、危及信息安全的行为

威胁（Threat）

信息或信息系统潜在的安全漏洞

安全威胁分类

从信息流动的角度

中断、截取、修改、捏造

从威胁的来源看可分为

内部威胁和外部威胁 。自然和人为两类。

从攻击者的行为上看可以分成

主动威胁和被动威胁

从威胁的动机上看分为

偶发性威胁与故意性威胁

## 攻击类型

被动攻击——对受害者无影响

未经用户同意和认可，将信息泄露给攻击者，但不对数据信息做任何修改。

常见手段：搭线监听、无线截（取）获、其他截获。

攻击方式：消息内容分析、通信量分析

通信量分析：测定通信主机的位置和标识，观察被交换消息的频率和长度。

特点：不易被发现。

预防措施：重点在于预防 ，如使用虚拟专用网（VPN）、加密保护

主动攻击——对受害者有影响

篡改数据流、或产生虚假流。

通常分为：

假冒：一个实体假装为一个不同的实体。

重放：被动获取一个数据单元，然后重传，以产生一个未授权的效果。

篡改：一个合法消息的某些部分被改变，或消息被延迟或改变顺序，以产生一个未授权的效果。

拒绝服务：防止或禁止通信设施的正常使用或管理。

特点：能够检测出来，不易有效防止。

预防措施：自动审计、入侵检测和完整性恢复。

## 主机扫描技术

目的：

确定在目标网络上的主机是否可达

应用层

传输层

网络层

数据链路层

DNS欺骗，SMB中间人攻击

SYN Flood攻击，IP欺骗

ICMP重定向攻击，IP分片攻击

ARP欺骗

物理层

## 拒绝服务(Denial of Service)

攻击者通过某手段，导致目标机器或网络停止向合法用户提供正常服务或资源访问。

利用网络协议漏洞或其他系统及应用软件的漏洞

耗尽被攻击的计算机或网络的资源，使其无法正常提供服务，直至系统停止响应甚至崩溃。

## Land 自握手

## 死ping(ping of death)

## SYN Flood（IP欺骗）

## Smurf（反射攻击）

DOS防御

Land 补丁，加固协议栈，丢弃源、目的IP相同的包

Ping of death 打补丁，防火墙拦截

Teardrop 加入条件判断，对这种异常的包特殊处理，打补丁

Smurf 拦截广播

SYN Flood拦截困难，抗击打

DDOS攻击过程

两个步骤：

攻占代理主机、向目标发起攻击

具体步骤：

探测扫描大量主机以寻找可入侵主机；

入侵有安全漏洞的主机并获取控制权；

安装攻击所用的客户进程或守护进程；

向客户进程发出命令，操纵代理主机进行协同入侵。

## 缓冲区溢出攻击

利用目标程序的缓冲区溢出漏洞，向缓冲区写超其长度的内容，造成缓冲区溢出

1. 破坏程序的堆栈

超出部分写入（覆盖）其他缓冲区，

数据、下一条指令指针，函数返回地址或是其他程序输出内容，

2. 使程序转而执行其它指令

目标系统指令

恶意代码shellcode：通过缓冲区溢出注入

## 恶意代码的分类

病毒：

* 能自我传播、需用户干预触发执行的破坏性程序或代码。
* 如CIH、爱虫、新欢乐时光、求职信、恶鹰、rose…

蠕虫：

* 能自我传播、不需用户干预即可触发执行的破坏性程序或代码。如红色代码、SQL蠕虫王、冲击波、震荡波、极速波…

特洛伊木马：

* 看起来具有正常功能，但实际上隐藏着很多用户不希望功能的程序。
* 通常由控制端和被控制端两端组成。
* 如冰河、网络神偷、灰鸽子……

后门：

* 那些绕过安全性控制而获取对程序或系统访问权的程序方法。

木马与后门的防范方法

技术手段：

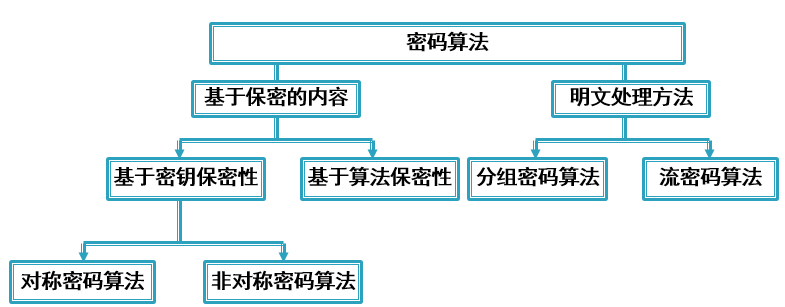
* 运行实时监控程序：
* 防火墙、防病毒软件
* 端口扫描
* 查看连接

## 安全意识：

* 不要随意打开来历不明的邮件
* 不要随意下载来历不明的软件
* 及时修补漏洞和关闭可疑的端口
* 尽量少用共享文件夹
* 经常升级系统和更新病毒库

# 第三章 密码学基础与加密技术

## 密码算法分类



按照保密的内容分:

受限制的（restricted)算法：算法的保密性基于保持算法的秘密。

基于密钥（key-based)的算法：算法的保密性基于对密钥的保密。

基于密钥的算法，按照密钥的特点分类：

对称密码算法（symmetric cipher)：

* 加密和解密密钥相同，或从一个易于推出另一个。又称秘密密钥算法或单密钥算法。
* DES、AES

非对称密钥算法（asymmetric cipher)：

* 加密密钥和解密密钥不相同，从一个很难推出另一个。又称公开密钥算法（public-key cipher) 。
* RSA、ECC

按照明文的处理方法：

分组密码（block cipher)

将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。

流密码（stream cipher)

又称序列密码.序列密码每次加密一位或一字节的明文。

## 典型加密技术

代换（代替Substitution）

置换（换位Transposition or Permutation）

乘积密码（Product Ciphers）

## 代换密码破译的三大要素

* 频率特征
* 连接特征
* 重复特征

## RSA算法

**RSA的主要缺点**

* 1）运算速度慢
  + 大数计算，RSA最快也比DES慢上100倍，一般只用于少量数据加密。
* 2）产生密钥烦琐
  + 受素数产生技术的限制

## 对称-非对称密码

* 对称
  + 优点：
    - 计算开销小，算法简单，密钥较短，加密速度快，目前用于信息加密的主要算法。
  + 缺陷：
    - 规模复杂
    - 通信前安全密钥交换
    - 没法鉴别，无法签名
* 非对称
  + 优点：
    - 密钥数量很小；密钥发布不成问题；数字签名。
  + 缺点：
    - 密钥尺寸大，加密／解密时的速度慢。

公开密码：少量数据加密

对称密码：大量数据加密

**加密功能的实施方式**

* 链到链加密
* 端到端加密

# 第四章 密钥管理与分配

密钥管理：

密钥管理是一种指导密钥生命期内相关技术问题的安全策略，以抵御各种潜在的威胁

### 密钥分级

* 初级密钥：加解密实际数据
  + **初级文件密钥**：生存周期与其保护的文件一样长
  + **初级通信（会话）密钥**：一个密钥使用一次或多次，生存周期很短（原则上一次一密）
* 二级密钥：保护初级密钥
  + 密钥加密密钥
* 主密钥：保护二级密钥进行
  + 最高级密钥
  + 生存周期很长

### 门限密钥保存方案

* 也称秘密共享或秘密分享。
  + 将秘密（密钥）被分割成几份，一定份额结合才能恢复秘密。

### 密钥分配体制

* 集中式
  + 基于中心服务器（密钥分配中心KDC，Key Distribute Center）
* 分布式
  + 用户之间直接密钥交换

## 密钥分配技术

* 直接分配（分布式）
* 密钥分配中心方式
* Diffie-Hellman方法
* 分级密钥分配

## 公钥密码体制的密钥管理

密钥形式

* 对称：随机数或随机序列；
* 公钥：单向陷门函数（数学难题）；

机制

* 对称：密钥保密、分发或协商
* 公钥：私钥自己保管、公钥公开

## 公钥管理解决方案

* 将公钥与身份绑定
  + 数字（公钥）证书
* 由可信第三方做担保
  + 权威机构（CA）管理、签名（盖章）、颁发
* 其他用户验证证书
  + 验证签名

## 公钥证书

* 数据结构
  1. 用户标识
  2. 公钥
  3. CA签名
* 存储和分配无需保护

用户通过公钥证书交换各自公

## 证书的类型

* 从证书的最终使用者看，
  1. 系统证书，CA系统自身的证书
  2. 用户证书，各种用户的证书
* 从证书的用途来看，
  1. 签名证书，对用户信息进行签名，确保不可否认性
  2. 加密证书，对用户传输信息进行加密，确保真实性，完整性

在使用中必须为用户配置两对密钥（加密、签名）和相应的证书

## PKI(Pubic Key Infrastructure)公钥基础设施

管理公开密钥和证书（生成、存储、分发、使用、验证和撤销等）的标准公开密钥管理平台。为所有网络应用透明地提供加密和签名所需密钥和证书管理。

## CA功能

负责用户密钥或证书发放、更新、废止、认证等管理工作:

1）颁发证书

2）废除证书

3）证书更新：

4）证书验证：

5）密钥管理：

# 第五章 消息认证与数字签名

## 消息（报文）认证

* 消息接收者证实收到的消息来自可信的源点且未被篡改的过程
  1. 真实性：发送者真实非假冒——信源鉴别；
  2. 完整性：消息在传送或存储过程中没被篡改、重放、乱序或延迟等；
* 目的：使接收者能识别报文的源、内容的真伪、时间有效性等。
* 防止主动攻击重要技术，防止如下一些攻击 ：
  1. 假冒：
  2. 内容修改：
  3. 顺序修改：
  4. 计时修改：

## 认证函数

消息加密函数(Message encryption)

消息认证码MAC(Message Authentication Code)

散列函数(Hash Function)

### 消息加密函数认证缺点

* 消息的密文为认证标识
* 消息有多长，认证标识就有多长

### MAC优缺点

* 优点：认证标识（码）大小固定且短
* 缺点：需要密钥，不需要从MAC解密出m

### 散列函数

消息摘要、哈希函数、数字指纹、杂凑函数

* 输入（不需密钥）：
  1. 任意长度的消息M
* 输出：
  1. 一个固定短长度散列值H(M)
* 单向函数：
  1. 正向计算容易，反向计算困难
* 不同消息不同指纹，用作消息标识
  1. 消息M的所有位的函数：消息中的任何一位或多位的变化都将导致该散列值的变化。

## 几种常用的HASH算法

* MD5
* SHA-1
* RIPEMD-160

## 数字签名需求

* 防止源点或终点否认（抵赖）的认证技术
* 传统（笔迹）签名的模拟，传统签名基本特点：
  1. 能与被签的文件在物理上不可分割
  2. 签名者不能否认自己的签名
  3. 签名不能被伪造
  4. 容易被验证
* 数字签名是传统签名的数字化，基本要求：
  1. 能与所签文件“绑定”
  2. 签名者不能否认自己的签名
  3. 签名不能被伪造
  4. 容易被自动验证

## 数字签名算法

* 1. RSA
  2. DSS/DSA

## 消息认证与数字签名的区别

* 消息认证：验证消息真实性及完整性，防范第三者；
* 数字签名：收发双方产生利害冲突时，防止纠纷。

# 第六章 身份认证

* 认证( authentication ) ：
  1. 证实主体的真实身份与其所声称的身份是否相符的过程。

## 身份认证攻击

* 数据流窃听(Sniffer)：
  1. 攻击者窃听网络数据，辨析认证数据，提取用户名和口令。
* 拷贝/重传：
  1. 非法用户截获信息，然后再传送给接收者。
* 修改或伪造：
  1. 非法用户截获信息，替换或修改信息后再传送给接收者，
  2. 非法用户冒充合法用户发送信息。

## 身份认证依据

* 用户所知Something the user know
  1. 密码、口令等
  2. 简单，开销小，容易泄密，最不安全；
* 用户所有Something the user possesses
  1. 身份证、护照、密钥盘等
  2. 泄密可能性较小，安全性高于第一类，系统相对复杂；
* 用户特征Something the user is (or How he behaves)
  1. 指纹、笔迹、声音、虹膜、DNA等
  2. 第
  3. 安全性最高，如窃取指纹很困难，涉及更复杂算法和实现技术。

## 身份认证机制

* 非密码
  1. 口令等
* 基于密码算法
  1. 对称密码算法
  2. 公开密码算法
  3. 密码校验函数
* 零知识证明协议

## 非密码身份认证

* 口令机制
* 基于地址的认证机制
* 基于生物特征的认证机制
* 个人令牌认证机制

## 口令攻击

* 字典攻击：
* 穷举攻击：
* 窥探：
* 社交工程：
* 垃圾搜索：

## 明文口令机制攻击

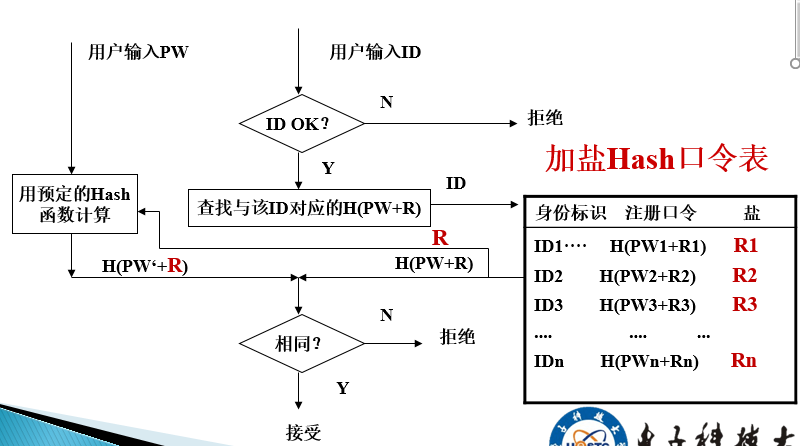
* 监听解析口令
* 重放攻击
* 获取口令文件

## hash口令机制攻击

* 重放攻击
  + 重放攻击（Replay Attacks）又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者发送一个目的[主机](http://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)已接收过的包，特别是在认证的过程中，用于认证用户身份所接收的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的安全性。
* 字典攻击

## 加盐

就是一个随机生成的字符串。我们将盐与原始密码连接（concat）在一起（放在前面或后面都可以），然后将concat后的字符串加密。采用这种方式加密密码，查表法就不灵了（因为盐是随机生成的）。



## 采用对称密码的认证机制

* 基于对称密码加解密处理构造认证协议
* 通信双方共享一个对称密钥（通常存储在硬件中），该密钥在询问—应答协议中处理或加密信息交换。

## 采用公开密码算法的机制

* 声称者用声称（他拥有）的签名密钥（私钥）来证实身份。
  1. 使用签名密钥签署某消息；
  2. 签名包含一非重复值以抵抗重放攻击。
* 验证者用声称者的有效公钥（公钥证书）验证身份。

## Kerberos 认证协议

* 基于对称密码技术**集中式**的身份认证框架结构。
  1. 使用DES加密算法
  2. 引入可信第三方
  3. 采用基于Needham-Schroeder协议
  4. 实现用户与服务器间的相互认证。

# 第七章 访问控制

## 访问控制的概念

* 网络安全防护的主要**安全策略**之一
* 依据授权规则，对提出的资源访问加以控制。
  1. 限制访问主体（用户、进程、服务等）对任何资源（计算资源、通信资源或信息资源）进行**未授权访问**，使计算机系统在合法范围内使用；
     + 非法用户使用
     + 合法用户滥用权限

决定用户能做什么，或代表用户的程序能做什么。

## 访问控制一般策略

自主访问控制、强制访问控制、基于角色的访问控制

## 访问控制三要素

主体Subject、客体Object、安全访问策略

## MAC优缺点

* 优点
  1. 严格，便于控制和管理
  2. 特别适用于军事领域
* 缺点
  1. 不灵活
  2. 用户、资源多时配置工作量大

## 下读/上写

* 向下读（Read Down，rd）
  1. 主体高于客体时允许读
  2. 低级别用户不能读高敏感度的信息
* 向上写（Write Up，wr）
  1. 主体低于客体时允许写
  2. 不允许高敏感度的信息写入低敏感度区域
* 保证数据机密性
  1. 信息流只能从低级别流向高级别
  2. 如，下级向上级汇报工作或情况

## 上读/下写

* 向上读（Read Up，ru）
  1. 主体低于客体时允许读操作
  2. 低信任级别的用户能够读高敏感度的信息
* 向下写（Write Down，wd）
  1. 主体高于客体时允许写操作
  2. 允许高敏感度的信息写入低敏感度区域
* 保证数据完整性
  1. 信息从高级别流向低级别
  2. 如,上级像下级下发文件、精神

## BLP应用：防火墙

* **下读/上写 (不上读/不下写)**
* **保证机密性**
* 安全级别
  1. 内部网络：机密
  2. 外部Internet：公开
* 隔离内外部网络——单向访问机制
  1. 不上读：阻止Internet访问内部网络，仅允许由内向外发起的数据流通过
  2. 不下写：不允许敏感数据从内部网络流向Internet

## Biba应用：Web服务器

* 安全级别
  1. Web服务器上资源安全级别为“秘密”
  2. Internet用户级别为“公开”
* 上读/不上写，保障Web数据完整性
  1. Internet上的用户只能读取服务器上的数据而不能更改它

上读/下写：完整性，eg，web server

下读/上写：机密性，eg，email server

## 自主/强制访问控制策略的问题

* 自主式太弱
  1. 配置的粒度小；配置的工作量大，效率低
  2. 无法控制信息（权限）的流动
* 强制式太强
  1. 配置的粒度大；缺乏灵活性
* 二者工作量大，不便管理
  1. 例：1000主体访问10000客体，须1000万次配置。如每次配置需1秒，每天工作8小时，就需
  2. 10，000，000/（3600\*8）=347.2天

# 第八章 防火墙

网络安全“老三样**”**

* 防火墙
* IDS
* 防病毒

## 防火墙概念

* 高级网络访问控制设备（一系列部件的组合）
  + 位置：位于不同网络安全域之间
    - 可信（内部）网络与不可信（外部）网络
  + 功能：唯一通道，执行访问控制策略
    - 允许、拒绝、监视、记录进出网络的访问行为
    - 只有经过授权的流量才可以通过防火墙
  + 目的：防止外部网络用户以非法手段进入内部网络访问内部55网络资源，保护内部网络操作环境。
* 类似：门禁、门卫。

## 防火墙技术

* 包过滤（工作在网络层）
  + 检查每个包头部信息，依据一套规则决定丢弃或者放行该数据包
  + 包头
    - IP包头：IP地址、协议类型、IP选项（分段）
    - TCP/UDP头信息：端口号
  + 规则
    - 预设规则
    - 规则匹配
  + 在标准的路由器上以及专门的防火墙设备上执行。

**包过滤优点**

* 不用改动应用程序对用户透明
* 可在路由器上实施，能协助保护整个网络
* 速度快、效率高

**包过滤缺点**

* 维护困难：
  + 正确制定规则困难：随着应用深化，规则表变大、复杂，难以测试，
  + 规则表结构出现漏洞的可能性也会增加
* 安全性低：
  + 发生故障或配置错误时容易让数据直接通过；
  + 不能防止IP欺骗
* 不能根据状态信息进行控制
* 不能处理网络/传输层以上的信息
  + 检查报文头部字段，功能简单，一些应用协议不适合于数据包过滤
  + 对位于网络更高协议层的信息不具理解能力
* 无法对网络上流动的信息提供全面的控制
* 无法执行某些安全策略
  + 不支持有效的用户认证
* 应用代理防火墙（工作在应用层）
  + 代理（应用层网关）技术：
    - 与包过滤技术完全不同，完全“阻隔”网络通信流
    - 理解应用协议，代理用户与服务器的连接
    - 接收、分析服务请求，允许则代理用户（应用）去取得网络信息——内外网间不直接通信。
  + 为每种应用服务编制专门的代理程序
    - * 对应用程序的数据进行检查，实现比包过滤路由器更严格的安全策略
  + 充当防火墙
    - 限制内外网间的相互访问
  + 节省IP开销
    - 所有用户对外只占用一个IP，所以不必租用过多的IP地址
  + 提高访问速度：
    - 本身带宽较小，通过带宽较大的proxy与目标主机连接。
    - 代理缓冲——网络缓存。
  + 优点
    - 理解应用的具体内容，能过滤数据内容；
    - 完全控制会话，安全性比包过滤防火墙高；
    - 可提供详细的日志和安全审计功能；
    - 代理可以方便地与其它安全手段集成，认证、加密
    - 可被配置成惟一的可被外部看见的主机，防止对外网暴露内网；
    - 解决合法IP地址不够用的问题。

缺点

* 难于配置
  1. 每个应用都要求单独的代理进程，要求理解每项应用协议的弱点，并合理配置安全策略
  2. 因此配置繁琐，难于理解，容易出现配置失误，最终影响内网的安全防范能力。
* 处理速度慢
  1. 一个连接改为两个两个连接
  2. 每个应用会话都需开一个单独的代理进程，处理延迟会很大，能处理的会话或连接性有限
* 对用户不透明；
* 代理服务不能保证免受所有协议弱点的限制；
* 代理不能改进底层协议的安全性；
* 电路级网关（传输层）
  + 工作在（会话层）传输层，监控内外主机间TCP握手信息，决定会话是否合法。
  + 常用于向外连接：
  + 优点：堡垒主机可设成混合网关：
    - 电路层网关：对外连接支持电路层功能，方便内部用户访问Internet服务
    - 应用层网关：对入连接支持应用层或代理服务，提供保护内部网络免于外部攻击的防火墙功能
* 状态检测包过滤防火墙（应用层）
  + 采用基于连接的状态检测机制
    - 在包过滤的同时，检察数据包之间的关联性
    - 将同一连接的所有包作为一个整体的数据流看待(连接发起到结束全过程)，构成连接状态表
    - 检查包括链路层、网络层、传输层、应用层的各种信息，结合规则表和状态表决定是否允许包通过。
  + 动态连接状态表：
    - 以前的通信信息
    - 或相关应用程序信息
  + 支持多种协议和应用，可方便地实现应用和服务扩充。

## 防火墙局限性

* 可能被绕开
* 不能防范内部攻击
* 不能防范没有安全意识的管理员授予某些入侵者临时网络访问权限
* 不能防止传送被病毒感染的程序或者文件、邮件等
* 性能瓶颈、单点失效
* 不能防备新的网络安全问题

# 第9章 入侵检测

## IDS基本结构

* 入侵检测系统包括三个功能部件

### 信息收集

* 在网络或系统的若干不同关键点（不同网段和不同主机）收集
  1. 尽可能扩大检测范围
  2. 从一个来源的信息有可能看不出疑点
* 入侵检测很大程度上依赖于收集信息的可靠性和正确性
  1. 要保证信息收集软件（组件）的完整性
  2. 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

### 信息分析

* 模式匹配
* 统计分析
* 完整性分析，往往用于事后分析

### 结果处理-响应

* 简单报警
* 切断连接
* 封锁用户
* 改变文件属性
* 最强烈反应：回击攻击者

## 入侵检测性能关键参数

* 误报(false positive)：
* 漏报(false negative)：

## 入侵检测分类

* 检测方法
  + 异常检测模型（Anomaly Detection ，统计分析)：
    - 统计正常操作应具有特征（用户轮廓），定时采样，包括会话登录、退出、CPU和内存占用，硬盘使用等
    - 用户活动与正常行为有重大偏离——入侵 。
  + 误用检测模型（Misuse Detection，模式匹配）)：
    - 收集非正常操作的行为特征，建立（入侵或攻击）特征库
    - 监测用户或系统行为与特征库中记录匹配——入侵