# 第五章 计算机网络安全

# 你的网络…安全吗？

- 不安全的原因：

  多种服务是不安全的

  协议是不安全的

- 处理的措施（使虚拟世界真实化）：

  防火墙技术

  认证和加密

# §5.1 基础知识

自然或人为

网络安全的含义：**(掌握)**

**网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶尔的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运营，网络服务不中断。**

- 网络安全又分为：
  - 运营系统安全，即确保信息处理和传播系统的安全。
  - 网络上系统信息的安全。
  - 网络上信息传播的安全。
  - 网络上信息内容的安全。

- 网

可被授权实体访问并按需求使用的特征，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运营等都属于对可用性的攻击。

或过程

共利用的特征。

数据未经授权不能进行变化的特征，即信息在存储或传播过程中保持不被修改、不被破坏和丢失的特征。

对信息的传播及内容具有控制能力。

- 网络安全的威胁

非授权访问（unauthorized access）：一种非授权的人的入侵。

信息泄露（disclosure of information）：造成将有价值的和高度机密的信息暴露给无权访问该信息的人的全部问题。

拒绝服务（denial of service）：使得系统难以或不可能继续执行任务的全部问题。

- 网络安全的威胁

计算机系统的脆弱性：

（1）计算机系统的脆弱性主要来自于操作系统的不安全性，在网络环境下，还起源于通信协议的不安全性。

（2）存在超级顾客，假如入侵者得到了超级顾客口令，整个系统将完全受控于入侵者。

（3）计算机可能会因硬件或软件故障而停止运转，或被入侵者利用并造成损失。

- 网络安全的威胁

协议安全的脆弱性：

例如：Robert Morries在 VAX机上用 C编写的一种GUESS软件，它根据对顾客名的搜索猜测机器密码口令的程序，自在1988年11月开始在网络上传播后来，几乎每年都给Internet造成上亿美元的损失

- 网络安全的威胁

人为的原因：

不论是什么样的网络系统都离不开人的管理，但又大多数缺乏安全管理员，尤其是高素质的网络管理员。

另外，缺乏网络安全管理的技术规范，缺乏定时的安全测试与检验，更缺乏安全监控。令人担忧的许多网络系统已使用数年，但网络管理员与顾客的注册、口令等还是处于缺省状态。

# 网络安全的关键技术

- 主机安全技术
- 身份认证技术
- 访问控制技术
- 密码技术
- 防火墙技术
- 安全审计技术
- 安全管理技术

- 网络安全的策略
  - 网络顾客的安全责任
  - 系统管理员的安全责任
  - 正确利用网络资源
  - 检测到安全问题时的对策

# 信息安全原则

- TCSEC

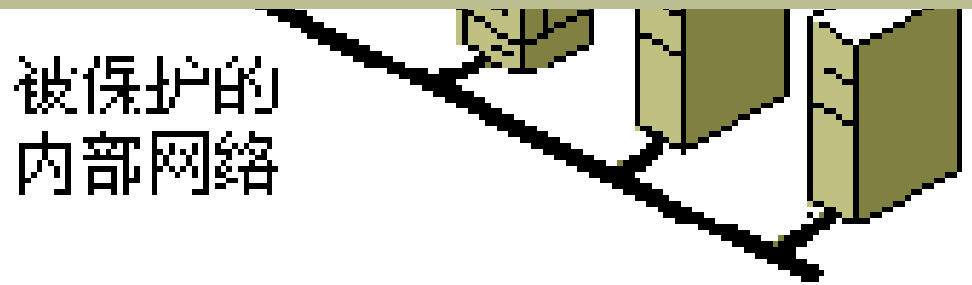
最低保护等级、自主保护等级、强制保护等级、验证保护等级

- CC

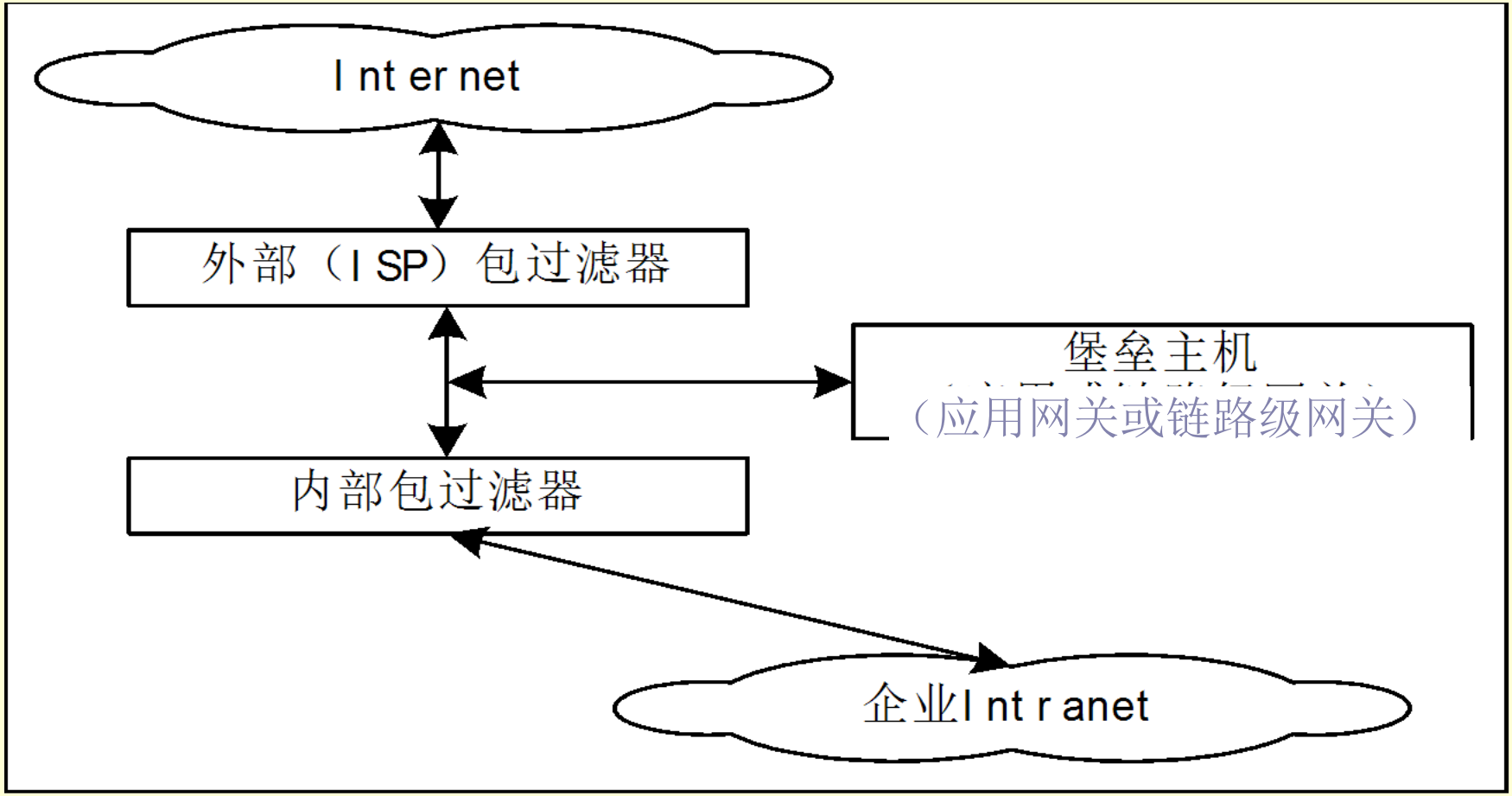
主要考虑人为的信息威胁，也可用于非人为原因造成的威胁。

# §5.2 防火墙——分组过滤装置

防火墙技术就是一种保护计算机网络安全的技术性措施，是在内部网络和外部网络之间实现控制策略的系统，主要是为了用来保护内部的网络不易受到来自Internet的侵害。



# 经典的防火墙：



# 防火墙的类型

- 电路级防火墙能够由应用层网关来完毕。电路层网关只依赖于TCP连接，并不进行任何附加的包处理或过滤。
- 一般由[illegible]的计[illegible]成。
- 应用级防火墙一般指运营代理（Proxy）服务器软件的一台计算机主机。

- 防火墙的主要功能如下：
  - 过滤不安全服务和非法顾客，禁止未授权的顾客访问受保护网络。
  - 防火墙能够允许受保护网的一部分主机被外部网访问，而另一部分被保护起来，预防不必要访问。
  - 防火墙能够统计下全部经过它的访问，并提供网络使用情况的统计数据。

- 防火墙的不足：

（1）不能防范绕过防火墙的攻击。

（2）一般的防火墙不能预防受到病毒感染的软件或文件的传播。

（3）不能预防数据驱动式攻击。

（4）难以防止来自内部的攻击。

- PC机的保护
  - 防病毒软件
  - 个人防火墙

# 防病毒软件

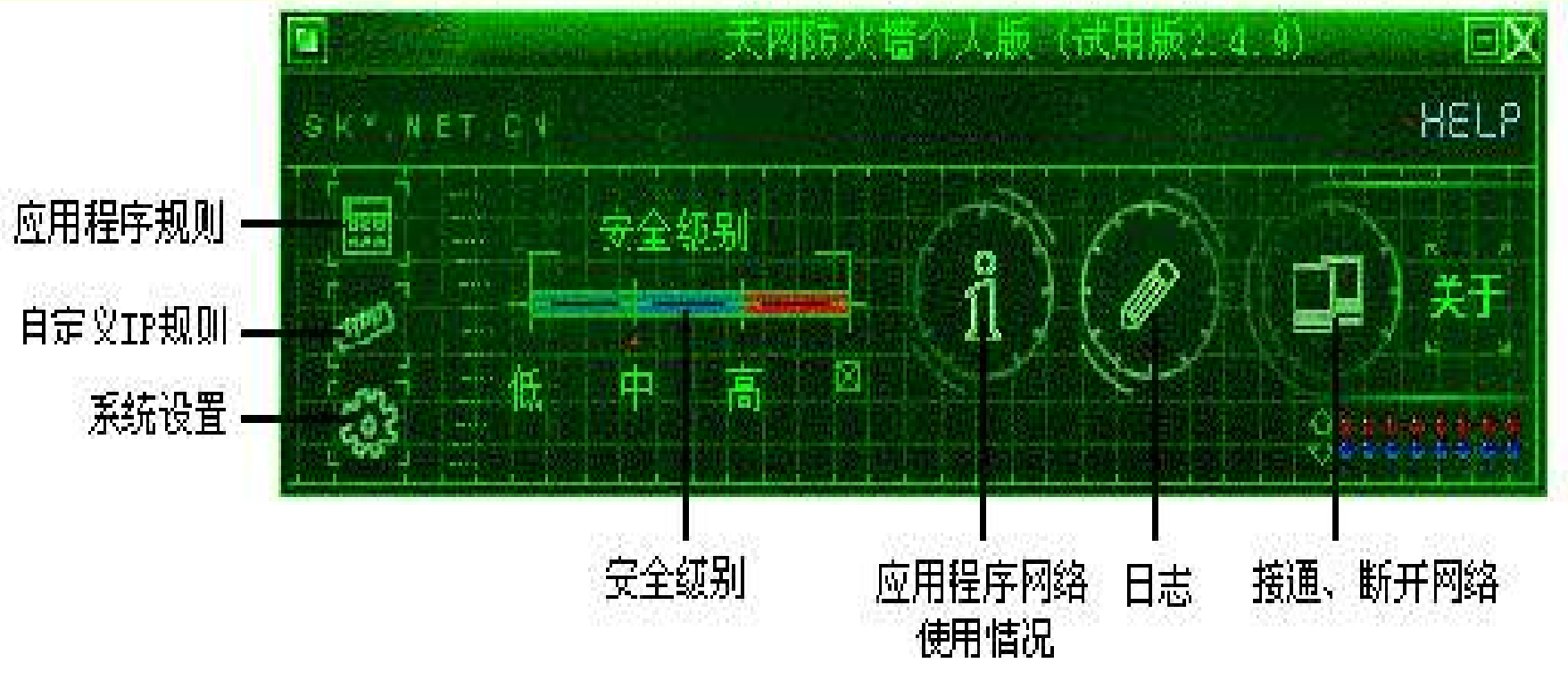

金山毒霸2003
我的金山毒霸
Kingsoft DUBA 2003
请选择查杀任务
我的电脑
我的文档
我的下载
我的硬盘
我的光盘
我的软盘
移动存储设备
自定义文件夹
闪电杀毒
全面杀毒
在线升级
病毒库版本：2004.03.26

## 构建个人防火墙

个人顾客只能使用应用级防火墙，一般都是使用包过滤和协议过滤等技术实现的。

这种防火墙能有效地预防顾客数据直接暴露在Internet中，并统计主机和Internet数据互换的情况，从而确保了顾客的安全。

# “天网防火墙”


天网防火墙个人版（试用版2.4.9）
SK.NET.CN
HELP
安全级别
低
中
高
关于
应用程序规则
自定义IP规则
系统设置
安全级别
应用程序网络使用情况
日志
接通、断开网络

# §5.3 加密技术

- 加密（cryptography）

明文 → 暗文

（plaintext） （ciphertext）

最简朴的加密技术是字母替代密码。

例如：密钥中… G-T；O-%；D-W；！-A；… …

消息：GOOD！

密文：T%%WA

## 常规密钥密码体制（单密钥）

特色：

消息被加密和解密的速度。

缺陷：

通信过程涉及若干个人时，需要密钥数量。如：两个人之间只需要一种密钥；十个人，需要45个密钥。（n×(n-1)/2）

- 定时更换密钥

# 公开密钥密码体制（双密钥）

分为公

优点：

需要密

缺陷：

加密、

简朴描述：

随机产生两个很大的质数（每一种是300位的十进制数，理想模式）。

求两个质数的乘积（公钥、密钥的一部分）

……

- RSA算法
- 不足：加密速度慢

- 数字署名过程：


使用A的密钥加密

数字署名

使用B的公钥加密

使用B的密钥解密

使用A的公钥验证数字署名

- 使用数字署名：
  - 能够表白署名者的身份
  - 发送者无法抵赖（反拒认）
  - 不能伪造

- 数字证书
  - 证明权威 CA

顾客B用CA的公钥验证CA对A的数字证书。

钥产生一种摘要，用CA的密钥署名得到数字证书。

- 因为公钥需要定时更换，使用数字证书时要验证是否失效。