

信息安全基础

中科院计算所教育中心

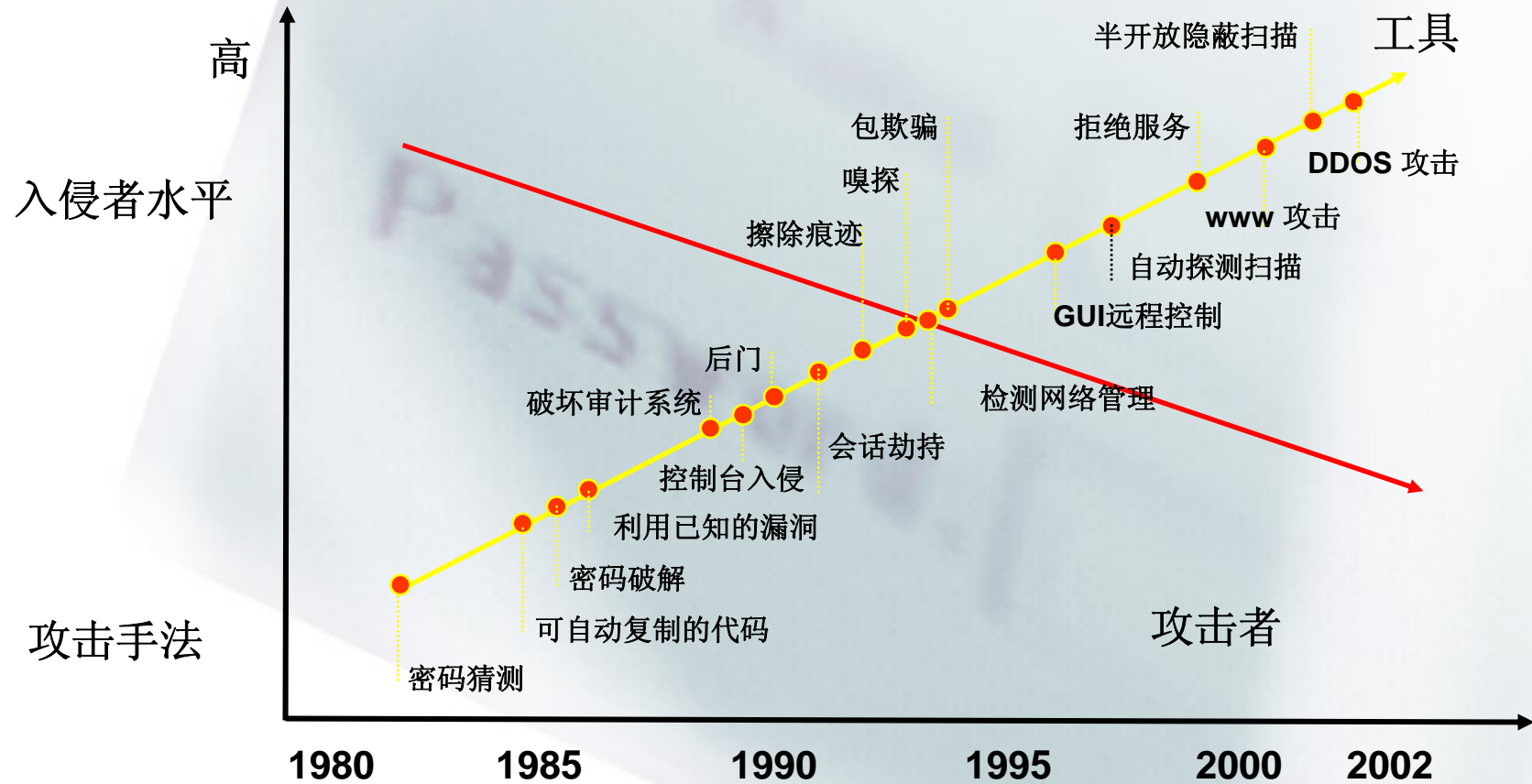


信息安全的定义

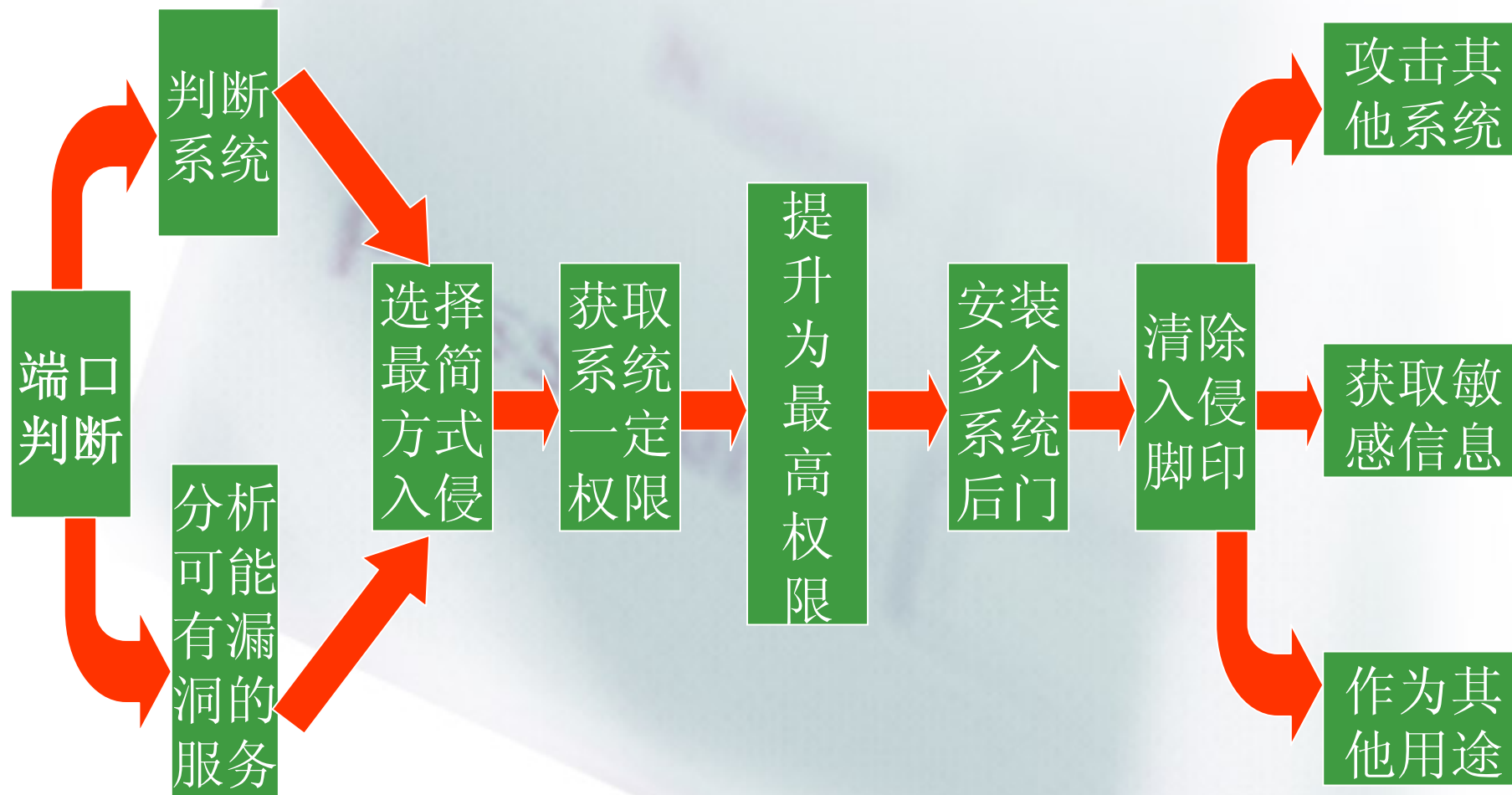
国际标准化组织(ISO)的定义为：

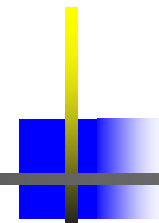
“为数据处理系统建立和采用的技术和管理的安全保护，**保护计算机硬件、软件和数据**不因偶然和恶意的原因遭到破坏、更改和泄露”。

入侵技术的发展



入侵系统的常用步骤





安全意识考验

- 你出差在外地，在一个陌生的环境里上网，试图连到自己在家里的一台服务器上。
- 使用**telnet**。开启了一个**ftp**服务，试图下载一些东西。
- 会有哪些风险出现？

很多协议明文传输

Packet Details

- General Information
- Ethernet v.2.0 MAC Head
- IPv4 Header
- TCP Header
- HTTP Client Request
 - [849 byte(s) of data]
 - 107
 - mynum=1&user=&pass=&u=s

Hex dump:

* 33 64 72 3A 30 33	[3d6310e7c, crr:03]
* 2C 70 30 35 2C 65	[, pos:08, sal:05, e]
* 64 75 2C 6D 61 72	[du:03, sta:02, mar]
* 3A 30 3A 33 32 3B	[:0, gen:M, age:32;]
* 20 53 20 53 49 44	[SINA_USER=; SID]
* 3D 3B 6C 6F 67 69	[=; userinfo_logi]
* 6E 74 34 32 39 37	[ntime=1016174297]
* 3B 20 68 61 6E 6E	[; userinfo_chann]
* 65 6C 72 69 6E 66	[el=mail; userinf]
* 6F 5F 3D 31 36 32	[o_remoteaddr=162]
* 2E 31 20 53 4D 3D	[.105. ; SM=]
* 53 69 6D 79 6E 75	[SinaMail....mynu]
* 6D 3D 73 73 3D 26	[m=1&user=&pass=&
* 75 3D 70 73 77 3D	[u= &psw=]
* 25 33 41 25	[&l=http%3A%
* 32 46 6E 61 2E 63	[2F%2Fmail.sina.c]
* 6F 6D 62 69 6E 25	[om.cn%2Fcgi-bin%
* 32 46 72 6F 64 75	[2Fmail.cgi&produ]
* 63 74	[ct=mail]

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.56.111	192.168.56.136	ICMP	Echo (ping) request
2	0.001727	192.168.56.136	192.168.56.111	ICMP	Echo (ping) reply
3	0.998885	192.168.56.111	192.168.56.136	ICMP	Echo (ping) request
4	1.000643	192.168.56.136	192.168.56.111	ICMP	Echo (ping) reply
5	2.001171	192.168.56.111	192.168.56.136	ICMP	Echo (ping) request

Frame 1 (74 bytes on wire, 74 bytes captured)

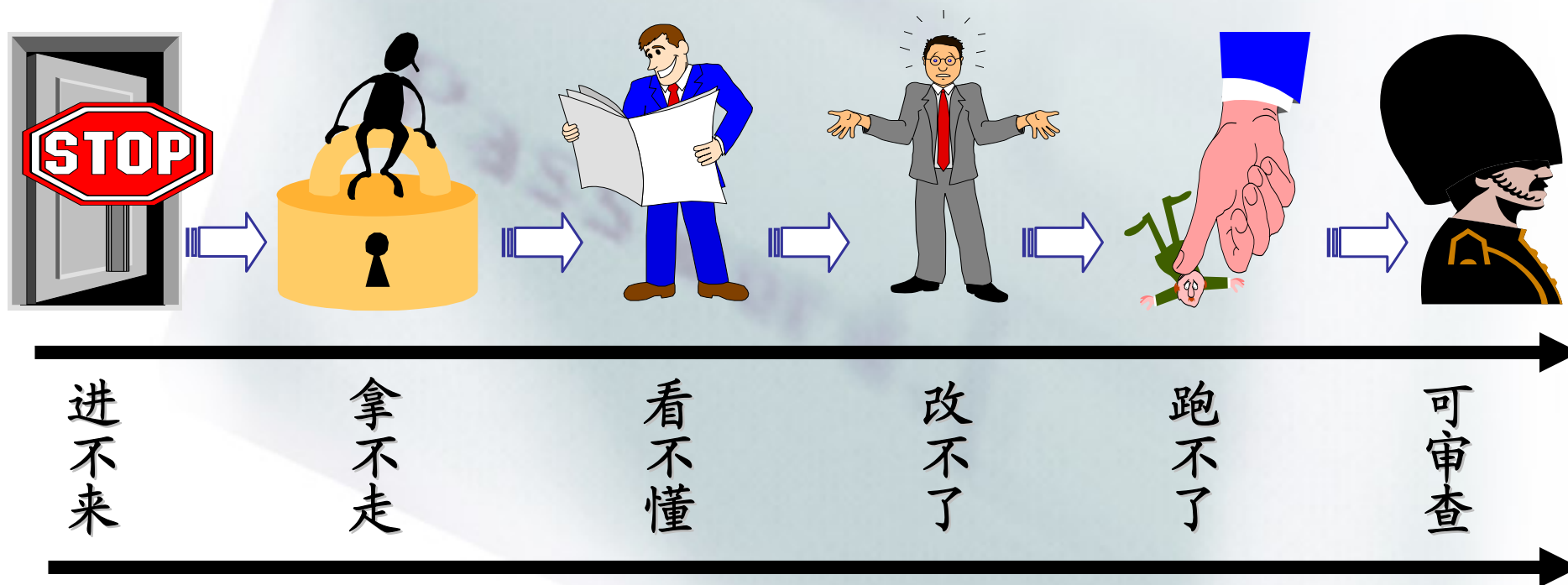
Ethernet II, Src: vmware_c0:00:01 (00:50:56:c0:00:01), Dst: vmware_c2:8d:88 (00:0c:29:c2:8d:88)
 Destination: vmware_c2:8d:88 (00:0c:29:c2:8d:88)
 Source: vmware_c0:00:01 (00:50:56:c0:00:01)
 Type: IP (0x0800)

Internet Protocol, Src: 192.168.56.111 (192.168.56.111), Dst: 192.168.56.136 (192.168.56.136)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 60
 Identification: 0x8e21 (36385)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 128
 Protocol: ICMP (0x01)
 Header checksum: 0xba57 [correct]
 Source: 192.168.56.111 (192.168.56.111)

0000	00 0c 29 c2 8d 88 00 50 56 c0 00 01 08 00 45 00	..).P V.E.
0010	00 3c 8e 21 00 00 80 01 ba 57 c0 a8 38 6f c0 a8	.<.!w..8o..
0020	38 88 08 00 41 5c 03 00 09 00 61 62 63 64 65 66	8...A\.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

Internet Protocol (ip), 20 P: 8 D: 8 M: 0 Drops: 0

信息安全的目的





一些术语

- 机密性：确保信息不暴露给未授权的实体或进程
- 完整性：确保信息未被未授权篡改或者损坏
- 实体鉴别：验证一个实体的身份
- 数据源发鉴别：验证消息来自可靠的源点
- 签名：一种绑定实体和信息的方法
- 授权：把做某件事情的许可传递给另一实体
- 访问控制：限制资源只能被授权的实体访问
- 抗否认：防止对以前行为否认的措施

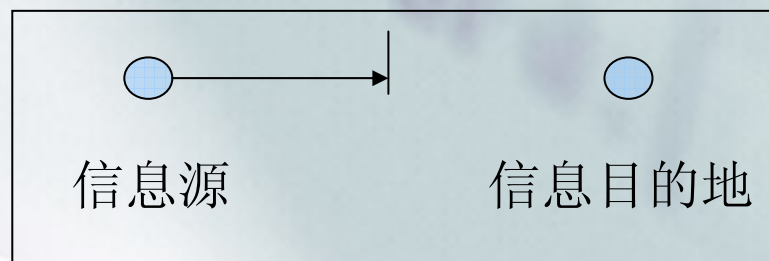


攻击

- 攻击分类：被动攻击与主动攻击
- 被动攻击,如窃听或者偷窥,非常难以被检测到,但可以防范
 - ❑ release of message content 信息内容泄露
 - ❑ traffic analysis 流量分析
- 主动攻击,常常是对数据流的修改,可以被检测到,但难以防范
 - ❑ Masquerade 伪装
 - ❑ Replay 重放
 - ❑ modification of message 消息篡改
 - ❑ denial of service 拒绝服务

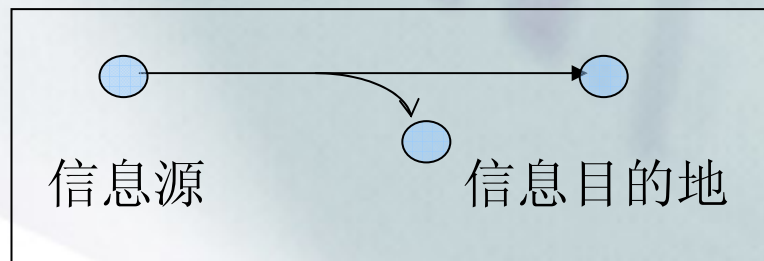
攻击者的能力-中断

- 使在用**信息系统毁坏**或不能使用的攻击，破坏可用性（**availability**）。
- 硬件的毁坏，通信线路的切断。
- **DoS**攻击，病毒导致的文件破坏，丢失。



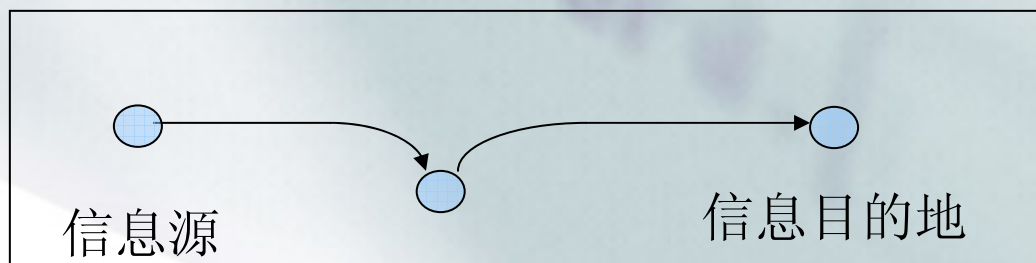
攻击者的能力-窃听

- 一个非授权方介入系统的攻击，破坏保密性 (**confidentiality**).
- 这种攻击包括搭线窃听，文件或程序的不正当拷贝。
- 密码窃听，会话劫持。



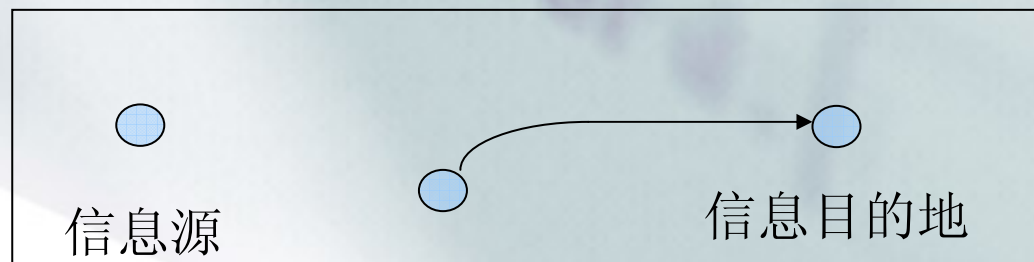
攻击者的能力-修改

- 一个非授权方不仅介入系统而且在系统中进行篡改的攻击，破坏完整性（**integrity**）。
- 这些攻击包括改变数据文件，改变程序使之不能正确执行，修改信件内容等。
- 对协议的攻击，缓冲区溢出。

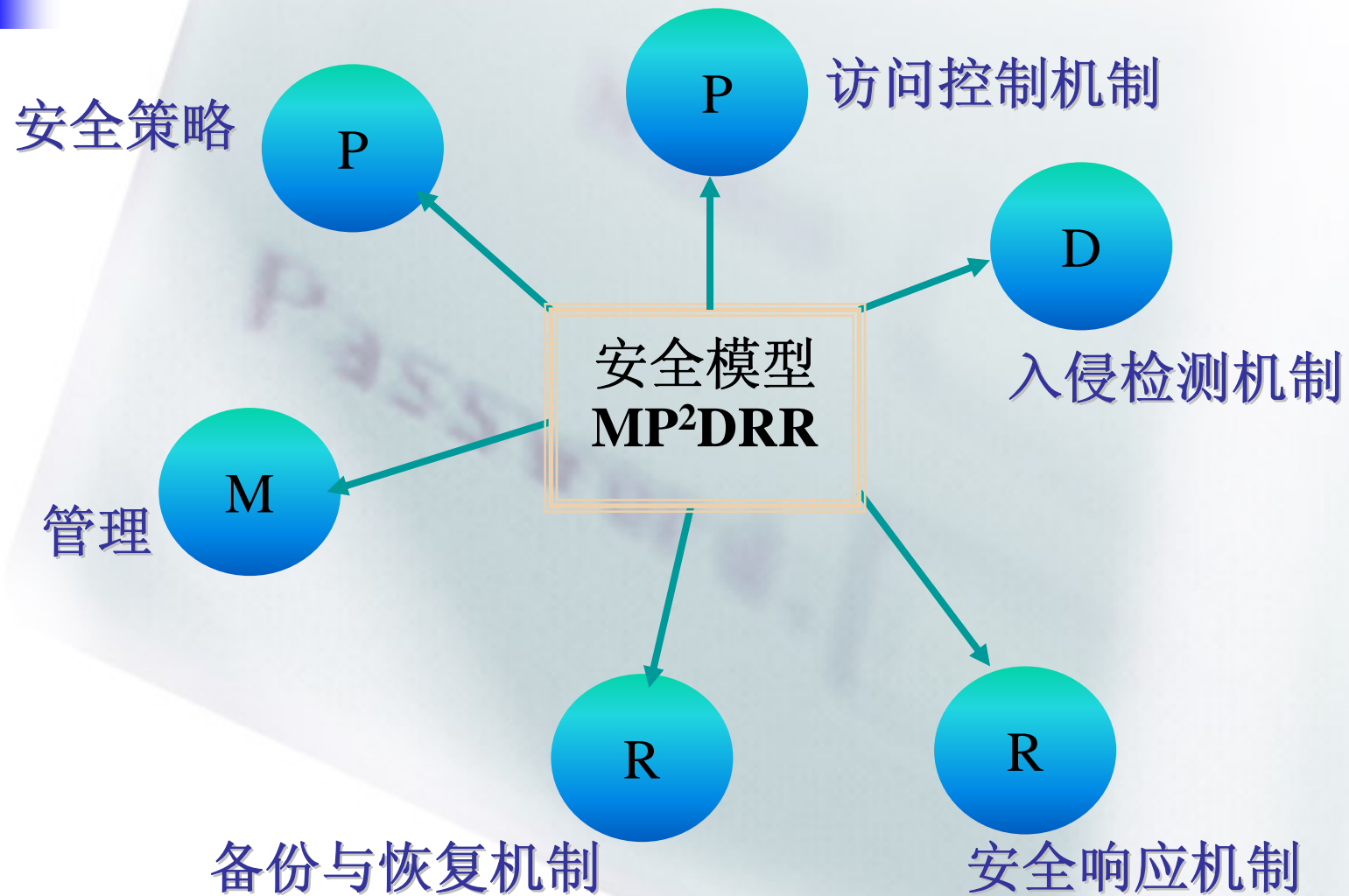


攻击者的能力-伪造

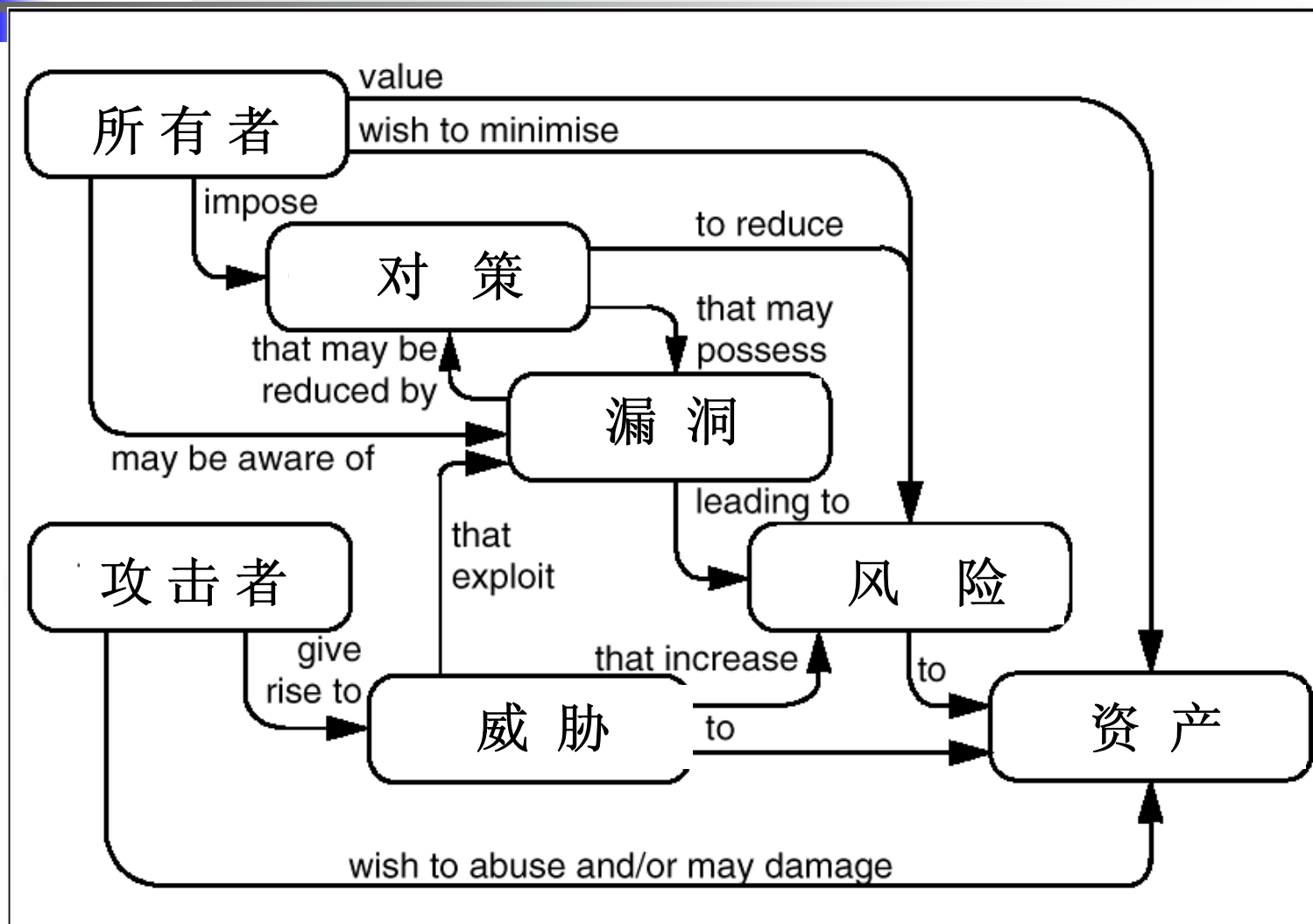
- 一个非授权方将伪造的客体插入系统中，破坏真实性（**authenticity**）的攻击。
- 包括网络中插入假信件，或者在文件中追加记录等。
- 冒充，**phishing**。



MP²DRR



CC定义的安全概念模型





可用性 Availability

- 要求包括信息、信息系统和系统服务都可以被授权实体在适合的时间，要求的方式，及时、可靠的访问。甚至在信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。
- 不要出现非授权者滥用却对授权者拒绝服务的情况。
- 硬件可用性最为直观和常见。
- 软件可用性是指在规定的时间内，程序成功运行的概率。
- 人员可用性是指人员成功地完成工作或任务的概率。

机密性(保密性) Confidentiality

- 机密性服务是用加密的机制实现的。
 - 密级文件经过加密可以公开存放和发送。
 - 构建加密通道的需要，防止搭线窃听和冒名入侵。
- 消息被称为明文。用某种方法伪装消息以隐藏它的内容的过程称为加密，被加密的消息称为密文，而把密文转变为明文的过程称为解密。
- 密码算法是用于加密和解密的数学函数

密码算法分类

- 对称密码算法：
 - 古典密码：简单代替 多名或同音代替
多表代替 多字母或多码代替
 - 现代对称分组密码： DES AES
- 非对称（公钥）算法 Public-key
RSA、背包密码、椭圆曲线ECC
- 新的领域：量子密码、混沌密码、DNA密码...



完整性 Integrity

数据完整性，未被未授权篡改或者损坏

系统完整性，系统未被非授权操纵，按既定的功能运行



消息鉴别Message Authentication

消息鉴别 (**Message Authentication**):

是一个证实收到的消息来自可信的源点且未被篡改的过程。

消息鉴别码**MAC**(**Message Authentication Code**)

公开函数+密钥产生一个固定长度的值作为鉴别标识。

散列函数(**Hash Function**)

一个散列函数以一个任意长的报文作为输入，并产生一个定长的散列码，有时也称报文摘要，作为输出。



鉴别(认证) Authentication

- **鉴别**就是确认实体是它所声明的，适用于用户、进程、系统等。
- **实体鉴别（身份鉴别）**：某一实体确信与之打交道的实体正是所需要的实体。只是简单地鉴别实体本身的身份，不会和实体想要进行何种活动相联系。
- **数据原发鉴别**：鉴定某个指定的数据是否来源于某个特定的实体。不是孤立地鉴别一个实体，也不是为了允许实体执行下一步的操作而鉴别它的身份，而是为了确定被鉴别的实体与一些特定数据项有着静态的不可分割的联系。
- **IP,口令,认证协议, 智能卡, 指纹, 面部扫描、视网膜、语音**

一个认证协议

- $A \rightarrow S: A, B, Na$
- $S \rightarrow A: \{Na, B, Kab, \{Kab, A\}Kbs\}Kas$
- $A \rightarrow B: \{Kab, A\}Kbs$
- $B \rightarrow A: \{Nb\}Kab$
- $A \rightarrow B: \{Nb-1\}Kab$

访问控制 Access Control

是针对越权使用资源的防御措施。

- 基本目标:

防止对任何资源（如计算资源、通信资源或信息资源）进行未授权的访问。从而使计算机系统在合法范围内使用；**决定用户能做什么**，也**决定**代表一定用户利益的**程序能做什么**。

- 如**unix**系统中访问控制通过**文件系统**实现，文件系统同时也是**unix**系统安全的核心。

```
❑ -rwxrwxr-x  root  root  13716 Jul  2 05:59 a.out
```

```
❑ -rw- rw-r- -  vick  vick      79 Jun 21 16:28 hello.c
```




其他性质

□ 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
- 数字签名（**Digital Signature**）是一种防止源点或终点抵赖的鉴别技术。



其他性质

☐ 审计 **Accountability**

- 确保实体的活动可被跟踪

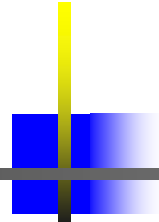
☐ 可靠性 **Reliability**

- 特定行为和结果的一致性



考虑可能的安全威胁

- 你在家通过**ADSL**上网，浏览了一会网页后，打开一家银行的网上银行系统，登录并查看自己的账户。
- 会有哪些风险？

- 
- 根据反网络钓鱼组织APWG（04年11月成立，网址为<http://www.antiphishing.org/>）最新统计指出，约有70.8%的网络欺诈是针对金融机构而来，而最常被仿冒的前三家公司为：Citibank（花旗银行）、eBay和Paypal。
 - 中国已经成为仅次于美国、世界上第二大拥有仿冒域名及网站的国家，占全球域名仿冒总份额的12%。



工行的安全措施

- 预留信息验证
- 使用U盾
- 口令卡

预留信息

登录个人网上银行，
系统自动提示设置预留验证信息

在“预留验证信息”后的输入框内输入一段特定文字（如喜爱的歌曲名称、诗句等），填写验证码和证件号码，点击“确定”即可

网上购物并进行在线支付

进入中国工商银行支付页面

输入支付卡号和验证码，点击“提交”按钮

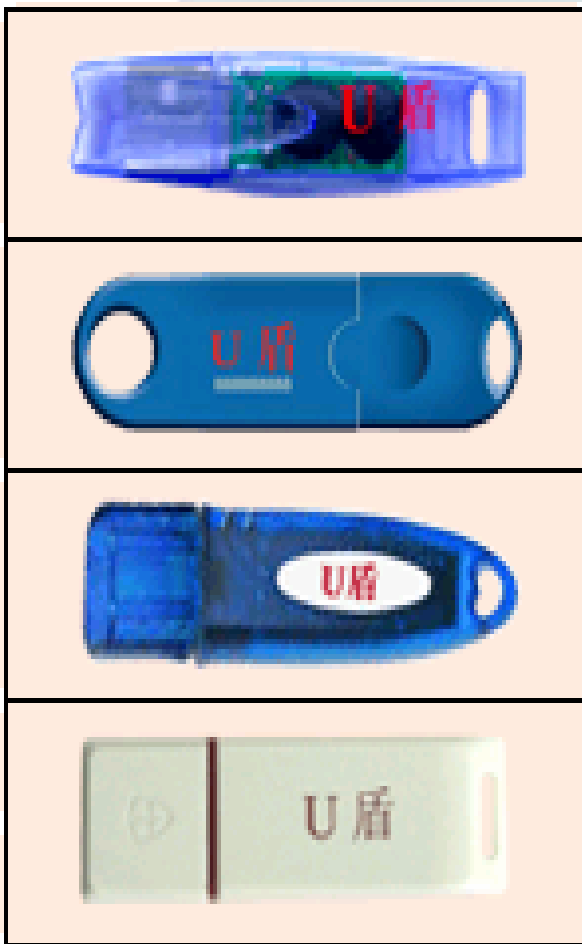
如果该商户是工商银行特约网站，页面上将显示您在网上银行中预留的信息，您核对无误后就可以放心地进行支付；如果不能正确返回信息，则说明该网站不是工行的特约网站，请您立即停止支付并致电95588咨询



U盾

- 安装**U盾**驱动程序。
- 下载证书信息，可委托网点柜员协助下载个人证书信息到**U盾**体内，也可以登录工行个人网上银行，进入“客户服务—**U盾**管理—**U盾**自助下载”，完成证书信息下载。
- 登录个人网上银行之后，如需办理转账、汇款、缴费等对外支付业务，只要按系统提示将**U盾**插入电脑的**USB**接口，输入**U盾**密码，并经银行系统验证无误，即可完成支付业务。

安全性



帐号

帐号密码

U盾

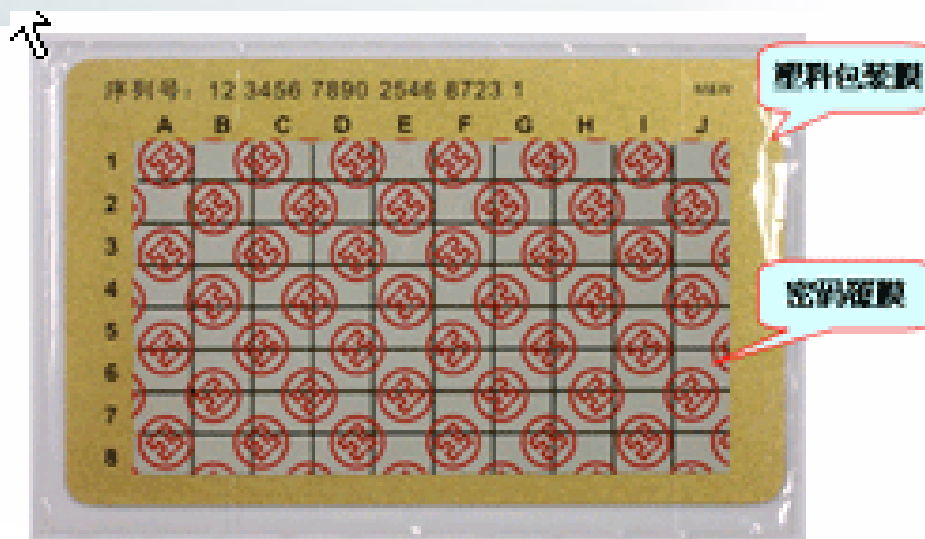
U盾密码



电子银行口令卡

- 帐户，帐户口令，口令卡不被同一个人获取，就能够保证资金的安全。
- 客户在使用电子银行进行转账、购物、缴费等支付交易时，电子银行系统会随机给出一组口令卡坐标，客户根据坐标从卡片中找到口令组合并输入电子银行系统。
- 申请口令卡后，只要登录个人网上银行，无需进行其他操作，即完成了同步激活口令卡的过程，之后即可进行网上支付。

口令卡



与U盾相比，电子银行口令卡的加密认证手段虽不如前者先进，但口令卡价格低廉、使用方便，适合对支付限额要求不高的普通客户使用。如果对网上银行的安全有较高的要求，建议申请U盾。

电子银行口令卡的使用

单笔转账汇款

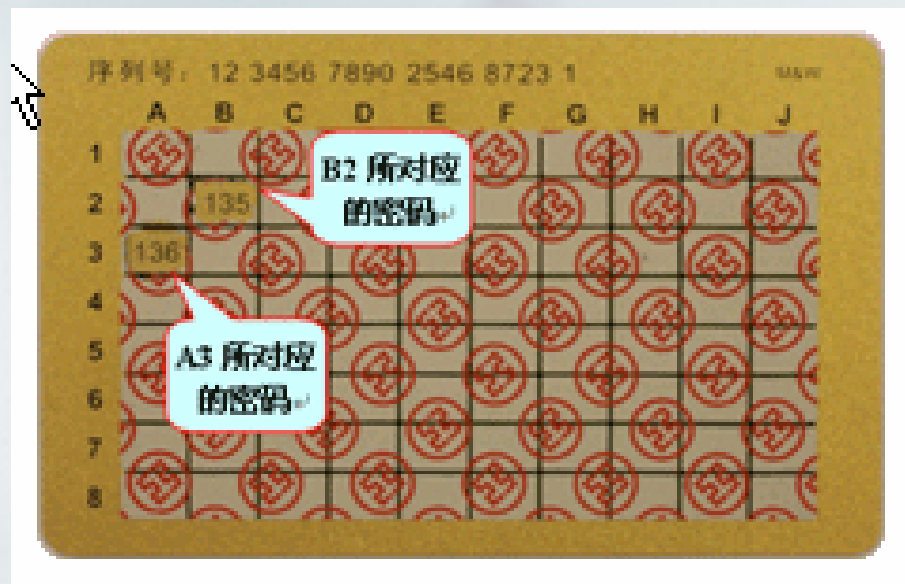
转账汇款日期：2006年09月01日

付款人	姓名：	测试	收款人	全称	陈钊钊
	卡号：	4580601024912003		账号(账号类型)	9558800200115889956 (灵通卡)
	不允许收款方查看此笔交易的付款方信息： <input type="checkbox"/>			证件类型	
				收款人所在地	
				收款网点机构名	
用途	手工录入		手工输入用途	现金	
附言					
手续费	0 元			币种：人民币	钞汇标志：现钞
请输入如下显示位置的动态密码：					
A3 B2					
<input type="text"/> (了解动态密码)					
请输入验证码： <input type="text"/> 6905					

**系统提示的
密码坐标**

确认 上一步

电子银行口令卡的使用



电子银行口令卡目前没有使用时间的限制，但有1000次的使用次数限制。

电子银行口令卡的使用

A3转账汇款

转账汇款日期：2006年09月01日

付款人	姓名：	测试	收款人	全称	陈钊钊
	卡号：	4580601024912003		账号(账号类型)	9558800200115869956(灵通卡)
	不允许收款方查看此笔交易的付款方信息： <input type="checkbox"/>			证件类型	
				收款人所在地	
		收款网点机构名			

用途	手工录入	手工输入用途	现金
附言			
手续费	0 元	总金额 1,000.00	币种:人民币 钞汇标志:现钞

请输入如下显示位置的动态密码：

A3 B2

在密码框中
输入 136135

请输入验证码：

6905

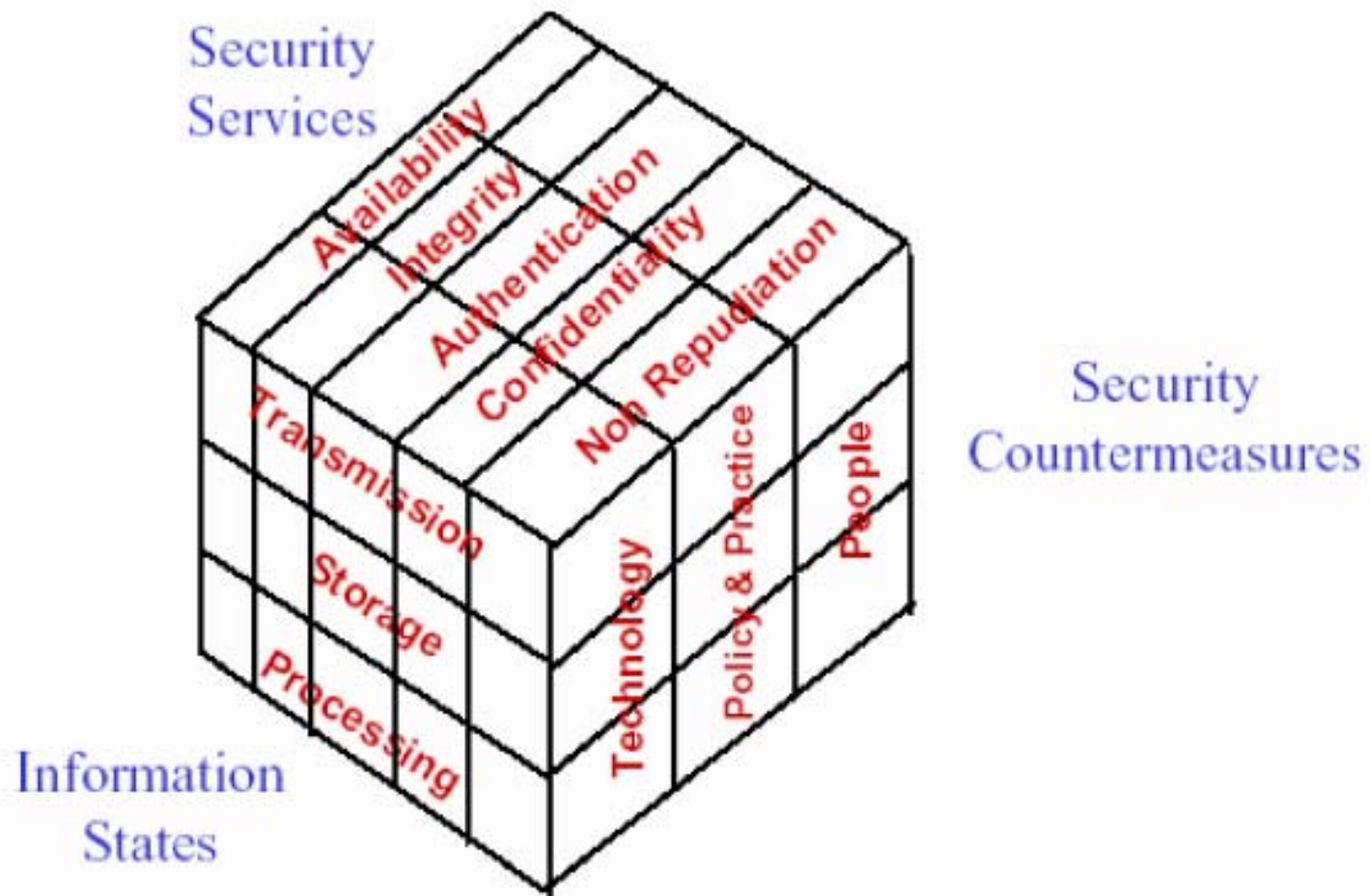
6905

输入验证码

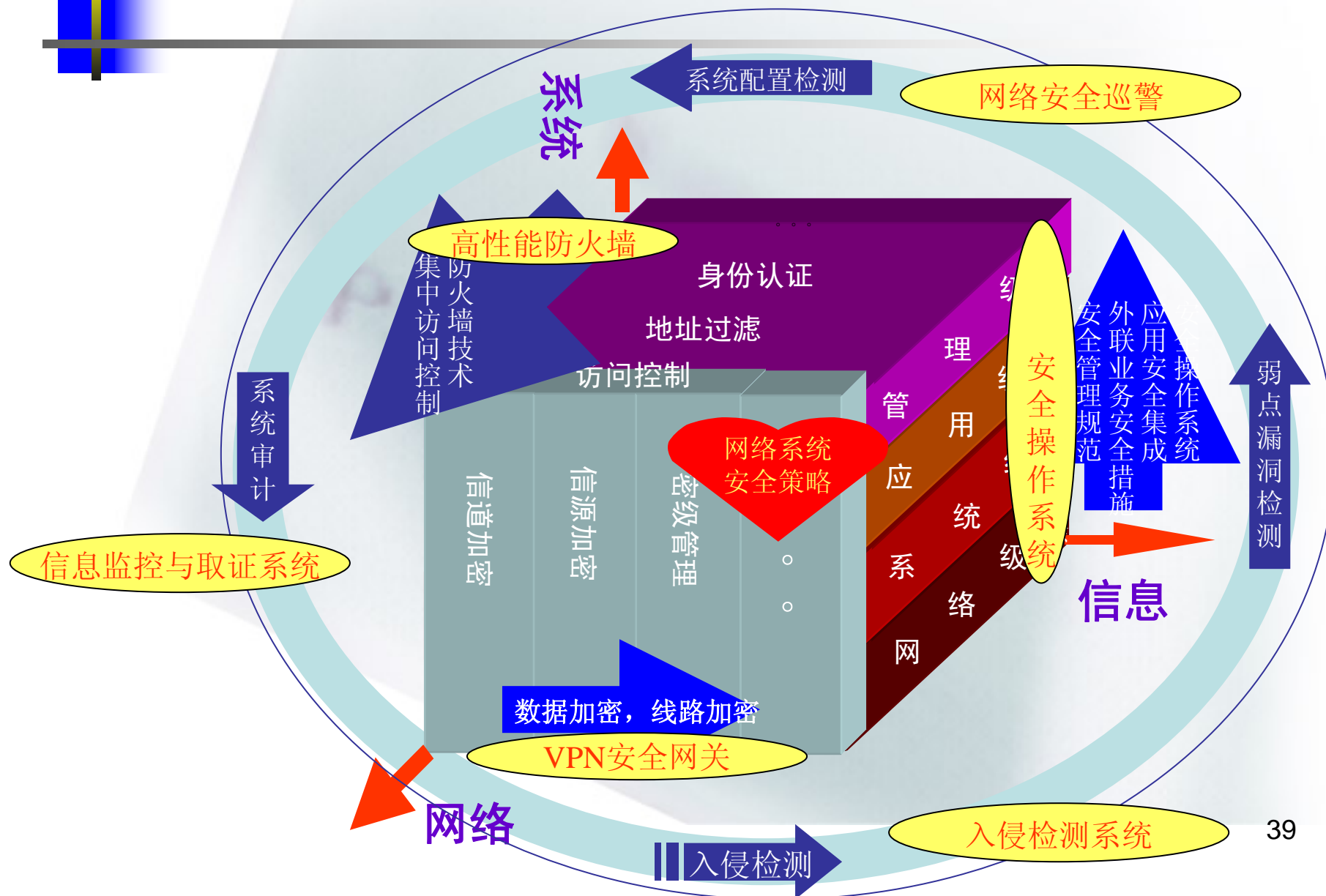
确认

上一步

三维模型



再看一个模型



威胁类型

国家安全威胁	信息战士	获得战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	恐怖分子	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的。破坏制度
局部威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战



安全事件

- **1988**年康奈尔大学的研究生罗伯特.莫里斯(**22**岁)针对**UNIX**的缺陷设计了一个“蠕虫”程序,感染了**6000**台计算机,使**Internet**不能正常运行,造成的经济损失达**1**亿美元。他因此被判三年缓刑、罚款**1**万美元、做**400**小时的社区服务。



安全事件

- **99年4月26日**，台湾人编制的**CIH病毒**的大爆发，有统计说我国大陆受其影响的**PC机**总量达**36万台**之多。有人估计在这次事件中，经济损失高达近**12亿元**。



安全事件

- **2000年2月份黑客攻击的浪潮，是互连网问世以来最为严重的黑客事件。**
 - ❑ 三天内黑客使美国数家顶级互联网站——雅虎、亚马逊、**EBAY**、**CNN**陷入瘫痪，造成直接经济损失**12亿美元**。并引起股市动荡。
 - ❑ 引起美国道琼斯股票指数下降了**200**多点。
 - ❑ 成长中的高科技股纳斯达克股票也一度下跌了**80**个点。

现状

- 占了**OS**世界市场**90%**的微软操作系统被发现的脆弱数(漏洞)快速增长。
- **NSA**认为，对美国国防部系统的成功攻击**90%**以上是利用了已知的漏洞。

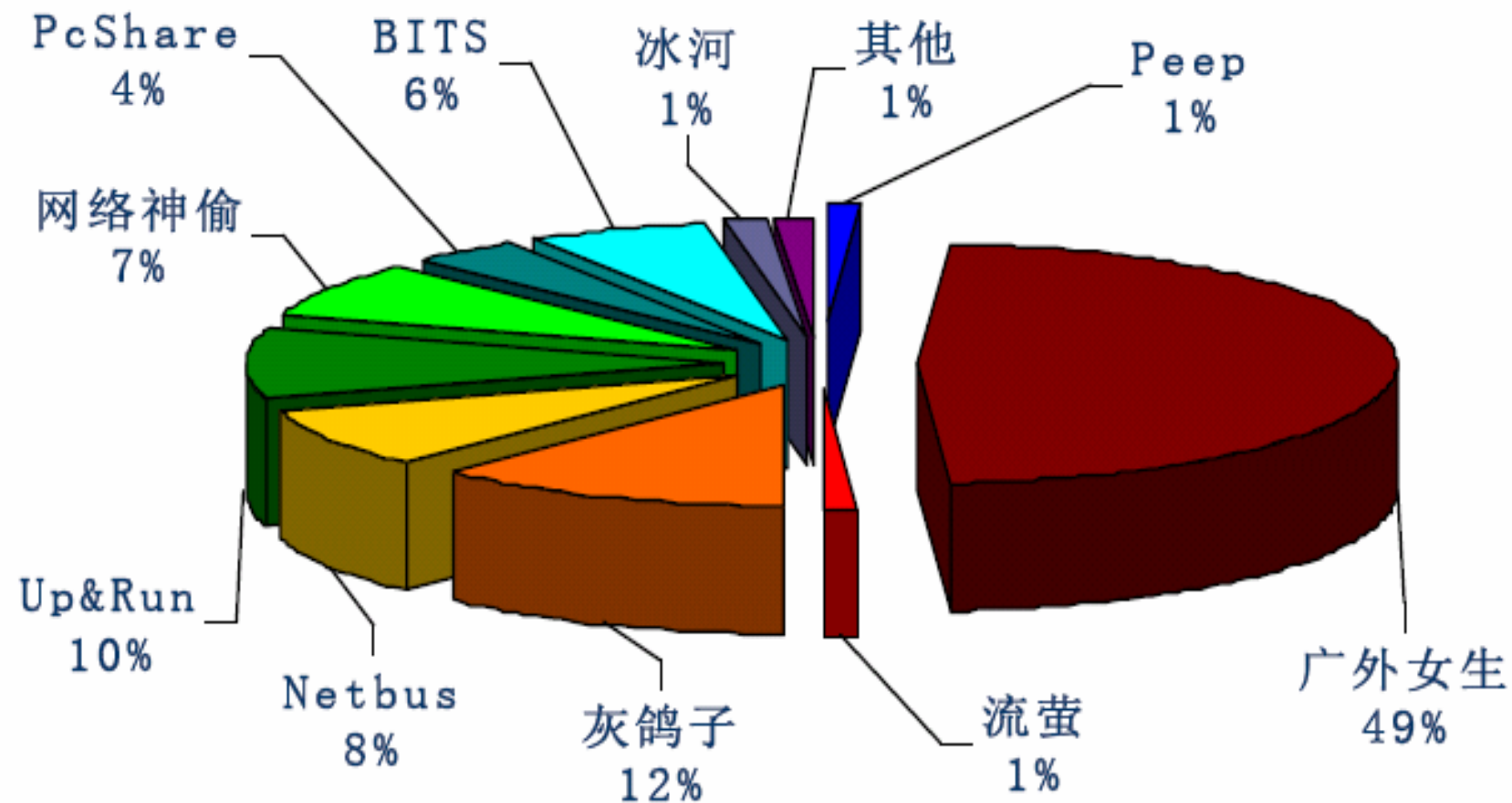




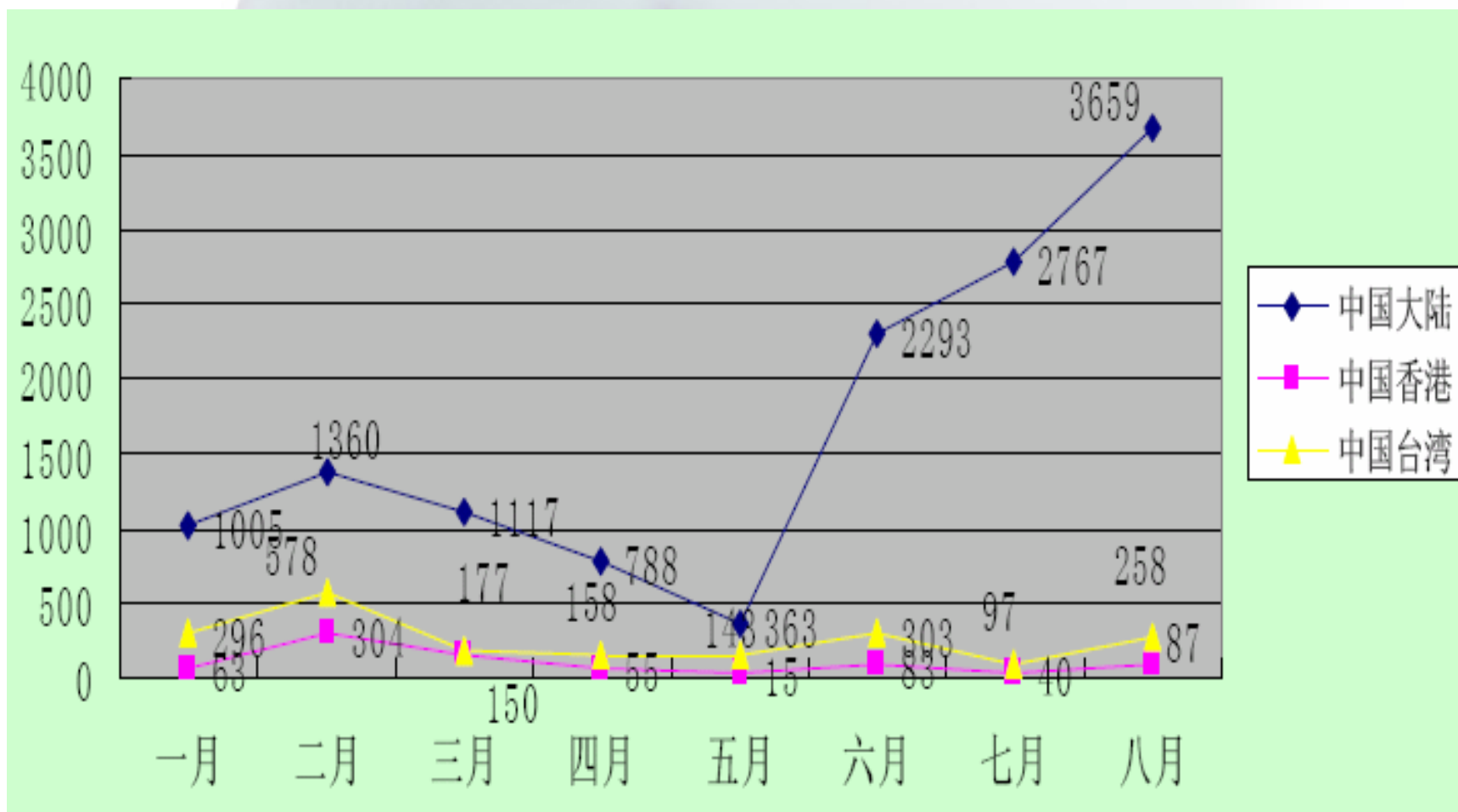
现状

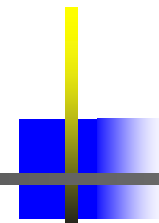
- 攻击变得容易——几乎不用或很少用到技术上的技巧就能攻击**70%**的脆弱性；
- 攻击节奏加快——以前对某一漏洞的攻击一般是发生在公布该漏洞之后的半年左右，但在**2004**年上半年的攻击却是平均发生在公布漏洞的**5.8**天之后，而**Witty**蠕虫的攻击更在该漏洞之后的**48**小时之内发生；

2005年我国木马分布抽样监测情况



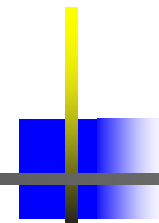
2006年前八个月中国网页被黑情况





实例：数据库安全

- 数据库**mysql**默认安装后存在**root**空口令漏洞，如果不补上的话，任意远程主机都可以使用如下命令连接你服务器上的**mysql**数据库，任意编辑，修改，删除数据库。
- **mysql -h218.184.196.9 -uroot**
- 解决方法：设置**root**密码
- **#./mysqladmin -u root password "passwd"**
- 或者：
mysql>grant select,insert,update,delete on *.* to root@"%" identified by "passwd";



实例：数据库安全

- **SQL Server**可能存在**SQL**空口令漏洞。
- 对该漏洞的可以使用**supersqlexec**工具，连接成功后，在命令行中输入：

```
net user guest /active:yes
```

```
>The command completed successfully.
```

```
net user guest 123456
```

```
> The command completed successfully
```

```
net localgroup administrators guest /add
```

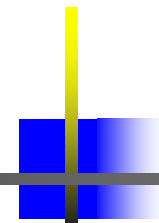
```
> The command completed successfully.
```

这几个命令意思是将**guest**用户激活，密码是**123456**，并提升为**admin**。



解决方法

- 运行**SQL Server**管理工具，给**SA**帐号加上强壮密码。
- 另外，最好执行**SQL**命令行：“**use master
sp_dropextendedproc 'xp_cmdshell'**”
这样就算攻击者获得**SA**帐号密码远程连接后，也不能调用**CMDSHELL**了。



实例：数据库安全

- 很多网站使用了**ASP**整站程序,下载稍微修改即加以使用。
- 找到数据库路径，如
`http://www.*.net/ADMIN/DATA/news30000.mdb`**
- 下载，用**MS office access**打开，双击**Admin**表，很有可能看到明文形式的密码（设计良好的程序不会以明文显示）。
- 使用网站的管理员登录入口，进入网站的后台管理页面。



解决

- 修改数据库的名称和路径，以及相应的连接。
- 可以手工修改或者采用修改工具。
- 如某论坛安装程序释放后的临时目录为 **c:\Temp**，打开**data**文件夹，可以看到一个名为“**Dvbbs7.mdb**”的数据库文件。可以将它改为“**i168love97943298you324#666.asp**”。
- 在**c:\Temp**中找到名为**CONN.asp**的文件，找到“**Db = data/Dvbbs7.mdb**”这一行，改为刚才修改后的名称。

现状

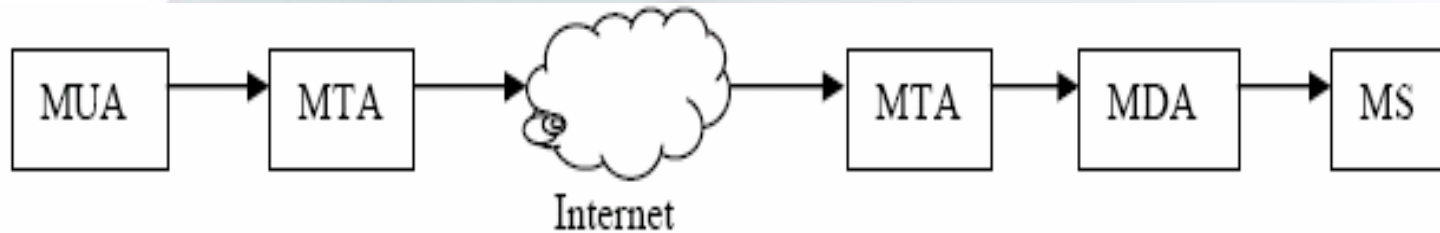
- 公安部公共信息网络安全监察局对我国 2 0 0 5 年 5 月至 2 0 0 6 年 5 月发生的网络安全事件和安全管理中存在的问题进行了调查。
- 感染计算机病毒、蠕虫和木马程序是最突出的网络安全情况，占发生安全事件总数的 8 4 %，“遭到端口扫描或网络攻击”和“垃圾邮件”分别占 3 6 %和 3 5 %。
- 调查显示，攻击或传播源来自外部的占 5 0 %，比去年下降 7 %；内外部均有的占 3 4 . 5 %，比去年上升 1 0 . 5 %。7 3 %的安全事件是由于未修补或防范软件漏洞所导致。
- 今年中国计算机用户计算机病毒感染率为 7 4 %，较上年 8 0 %的感染率呈下降趋势。



垃圾邮件

- (1) 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；
- (2) 收件人无法拒收的电子邮件；
- (3) 隐藏发件人身份、地址、标题等信息的电子邮件；
- (4) 含有虚假的信息源、发件人、路由等信息的电子邮件；
- (5) 含有病毒、恶意代码、色情、反动等不良信息或有害信息的邮件。

电子邮件工作原理



MUA: 邮件用户代理 MTA: 邮件传输代理 MDA: 邮件投递代理 MS: 邮件存储

- 用户通过**UA**（如**outlook**、**foxmail**等）书写邮件，然后由**UA**将邮件发送给**MTA**，**MTA**负责将邮件发送到目的地**MTA**，但中间可能经过多个**MTA**传递。邮件到达目的地**MTA**后，再通过**MDA**将邮件放到**MS**（也即接受用户的邮箱）中。



针对垃圾邮件的对策

- 基于信源（发信地址）的邮件过滤
- 基于规则的邮件过滤
- 基于内容的邮件过滤



黑白名单列表

- 黑白名单可在**MUA**或**MTA**中设置和维护，从白名单来的邮件都被认为是合法邮件，而从黑名单来的邮件被认定为垃圾邮件。
- 白名单通常由用户提供，也可由**MTA**自动地进行学习获得。
- 黑名单可以由用户提供，也可由相关组织机构进行统一管理，通常是按照某个地址发垃圾邮件的数量和该地址发垃圾邮件的性质来判断。如一些主动恶意发送的**MTA**或被利用的**MTA**（即**openrelay MTA**）等等。



蜜罐技术

- 为防止黑名单伤及无辜，黑名单技术常与蜜罐技术相结合，即借助设置蜜罐（无人使用的诱饵邮箱）来进一步核实黑名单。
- 实时黑名单由实时黑名单服务器提供，如 **Mail-Abuse** 的 **RBL**、**RBL+** 服务器，以及国内的反垃圾邮件联盟（<http://anti-spam.org.cn>）等。



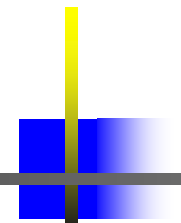
基于规则的邮件过滤

- 信头分析：一封邮件从发信人到收信人，会经过两个或多个**MTA**，每个**MTA**都会在信件头部加入一条**Received**的信息。垃圾邮件通常伪造**From**地址（即发信人地址），但无法伪造**Received**信息，故通过比较**Received**域和**From**地址可判断发信地址是否为伪造的。
- 关键词匹配：当在邮件标题或者正文中匹配到如“**free**”、“免费”、“抢注”、“热卖”、“赠送”等关键词或短语，就可判定为垃圾邮件。
- 其他特征：邮件文字较少却含有较多的超级链接，正文中包含有大量的随机字符等等；



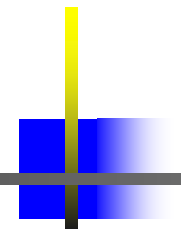
SpamAssassin

- 开源软件**SpamAssassin**规则集中有上百条规则，每条规则都设置了权重并与一个分数（正或负）相关，负分表示合法邮件的属性，正分表示垃圾邮件的属性。每个邮件可能触发多个规则，对所有匹配规则对应的分数求和后得出邮件的总分，然后根据阈值来判断是否为垃圾邮件。
- 基于规则过滤方法的优点是规则较易理解和修改，缺点是在规律性不明显的应用领域效果较差。



基于内容的邮件过滤

- 是国内外目前研究反垃圾邮件技术的热点和方向，利用机器学习的方法识别出垃圾邮件。
- 机器学习方法过滤垃圾邮件通常包含**3**个阶段：文档表示、语料训练和分类。语料训练阶段对大量的已标注邮件样本进行学习并构造分类器；分类阶段则利用分类器将未标记邮件分为垃圾邮件和正常邮件。
- 当垃圾邮件特征偏移时，必须进行批量反馈学习或完全重新学习。
- 优点是机器学习导致的自动化程度高，缺点是目前仍然没有智能性很高的算法，语料训练需要较多的时间和空间等。



网络信息安全层次

- 层次一：物理环境的安全性（物理层安全）
- 层次二：操作系统的安全性（系统层安全）
- 层次三：网络的安全性（网络层安全）
- 层次四：应用的安全性（应用层安全）
- 层次五：管理的安全性（管理层安全）



信息安全策略

- 自上而下地制定安全策略
- 最小特权原则
- 最薄弱环节（被忽视的环节）
- 失效保护机制
 - ❑ 缺省拒绝状态
 - ❑ 缺省接受状态
- 采用多防线技术
- 不要太过于依赖系统操作
- 定期备份
- 普遍参与



物理安全

- ✓ 物理安全是保护计算机网络设备、设施、介质和信息免遭自然灾害、环境事故以及人为物理操作失误或错误及各种以物理手段犯罪行为导致的破坏、丢失。
- ✓ 考虑三个方面：
 - 环境安全
 - 设备安全
 - 媒介安全



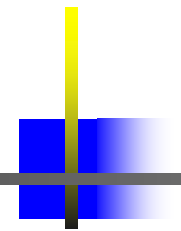
网络物理与结构安全

- ❑ 对于机房环境安全，应符合相关的国家标准：
GB50173-93 《电子计算机机房设计规范》； GB2887-89 《计算站场地技术条件》； GB9361-88 《计算站场地安全要求》等。
- ❑ 对于设备的物理安全，主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；关键网络设备和应用系统主机设备的冗余设计；员工整体安全意识的提高。
- ❑ 对于媒体安全，包括媒体数据的安全及媒体本身的安全，要防止系统信息在空间的扩散。

计算机主机的安全

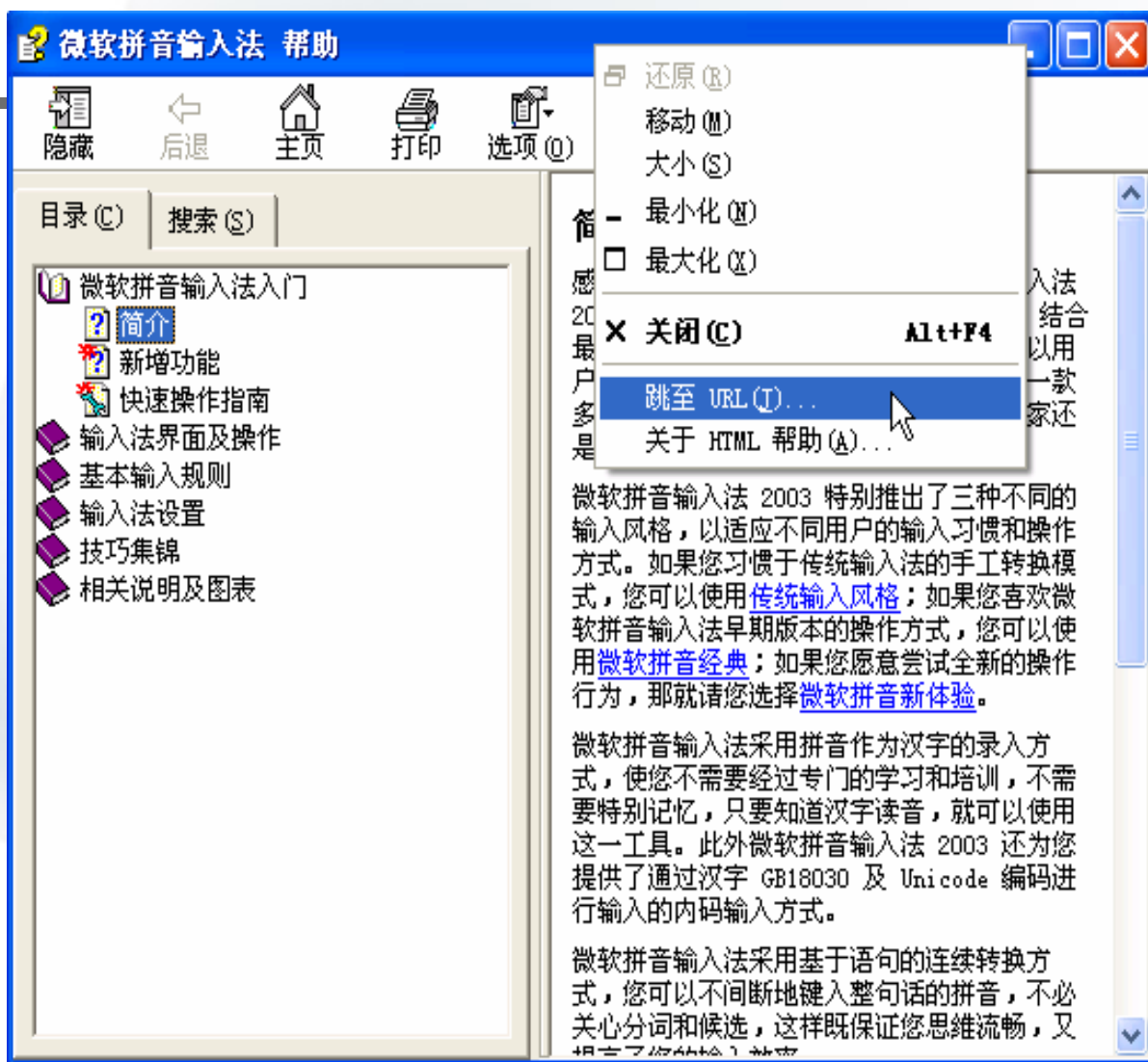
- 主机安全：主要考虑保护合法用户对于授权资源的使用，防止非法入侵者对于系统资源的侵占与破坏。

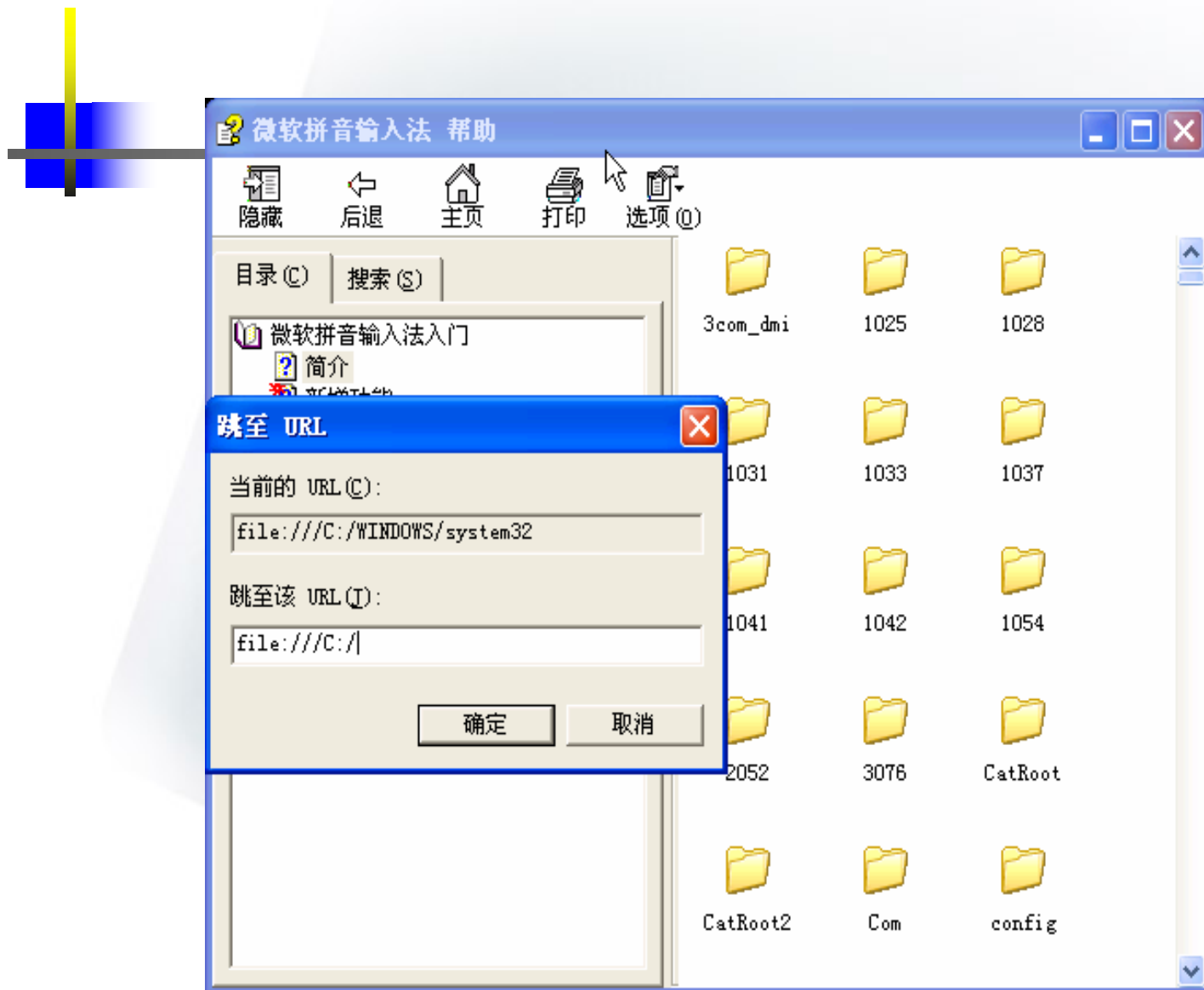




3389漏洞

- 输入法漏洞
- **windows2000**中文简体版终端服务
- 使用**mstsc**进行连接
- 登录界面出现后，使用全拼输入法，点击帮助->操作指南->在最上面右击->跳转到url->填**c:\windows\system32**或者**file:///c:**



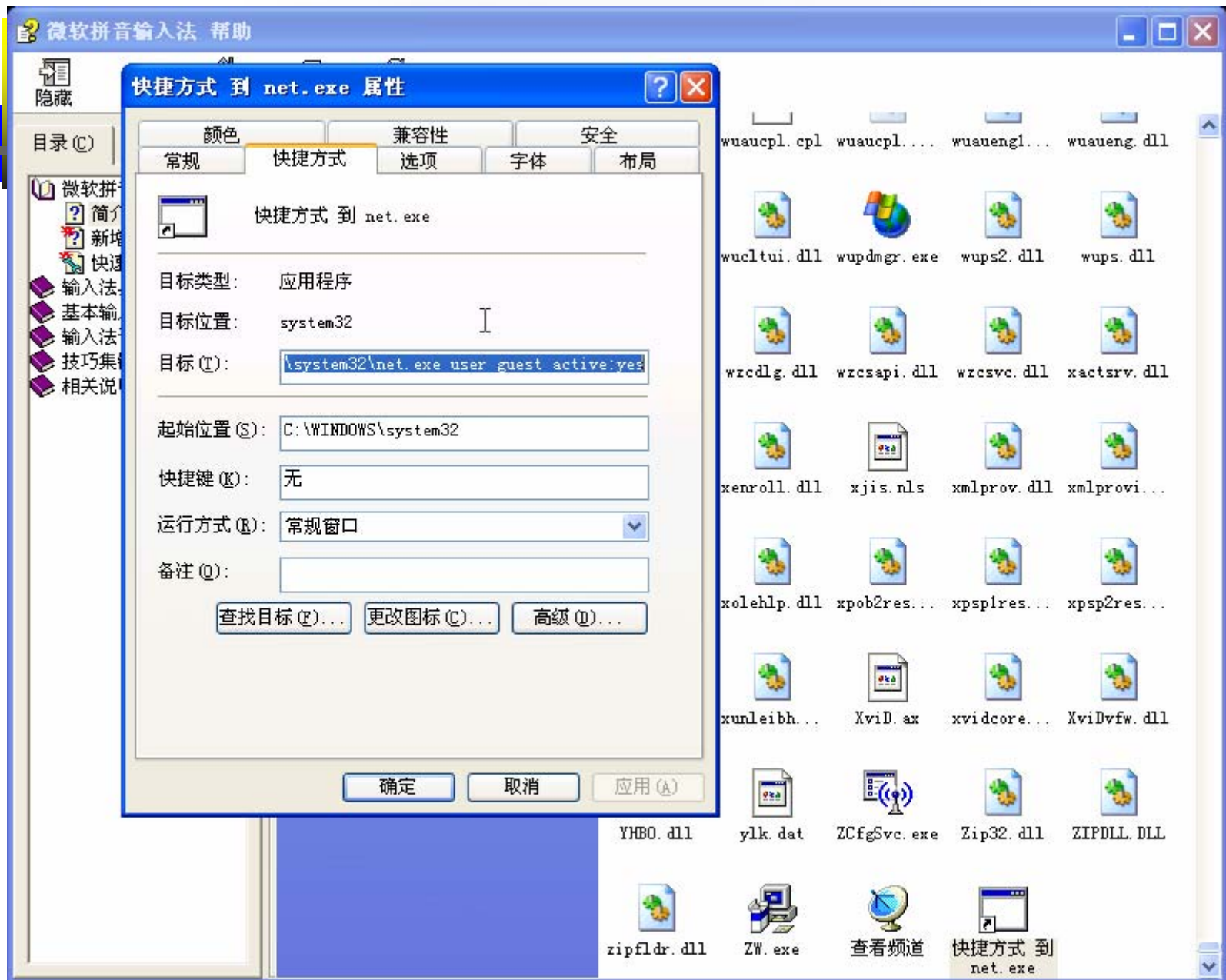


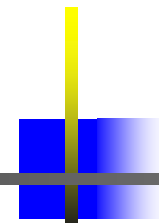
- 
- 创建**net.exe**的快捷方式
 - 属性里在**net.exe**后添加
user guest active:yes
同样的，可运行：

net user winadin /add

net user winadin "xxxx"

net localgroup administrators winadin /add





防范

- 打补丁，**sp2**以上已经没有该漏洞。
- 删除输入法的帮助文件。

c:\windows\help

winime.chm 输入法操作指南

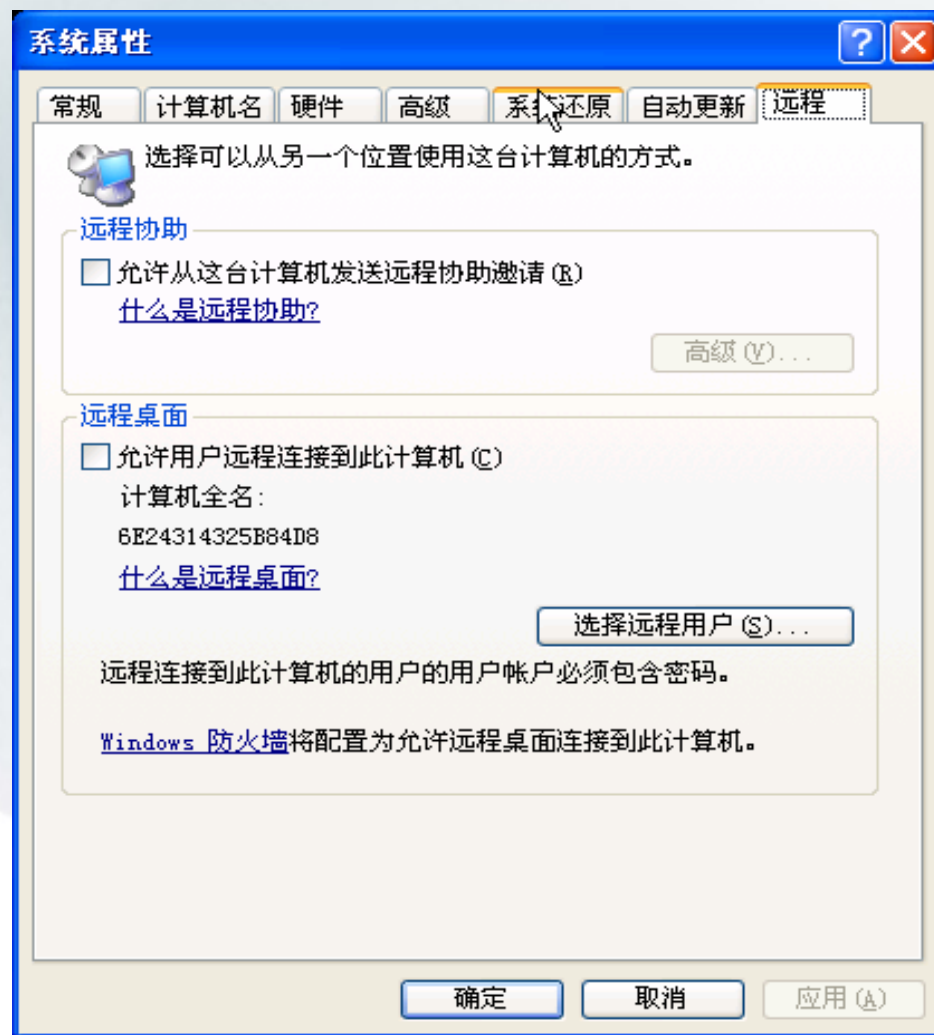
winsp.chm 双拼输入法

winzm.chm 郑码输入法

winpy.chm 全拼输入法

wingb.chm 内码输入法

关闭远程桌面服务





防范意识

- 1.及时给系统打补丁，防止绝大多数利用漏洞的攻击。
- 2.使用**netstat**查看与主机的连接，如果有可疑情况（如陌生的**IP**，端口号大于**1000**），断开网络连接，使用杀毒软件看是否有木马。
- 3.检查主机中是否多了陌生的用户，或**guest**用户是否被激活。**net user**命令查看所有用户，**net user Guest**
- 4.经常查看系统开了哪些服务，把不必要的或不认识的关掉。**net start**查看服务，**net stop "server name"**关掉服务，**services.msc**修改注册表。



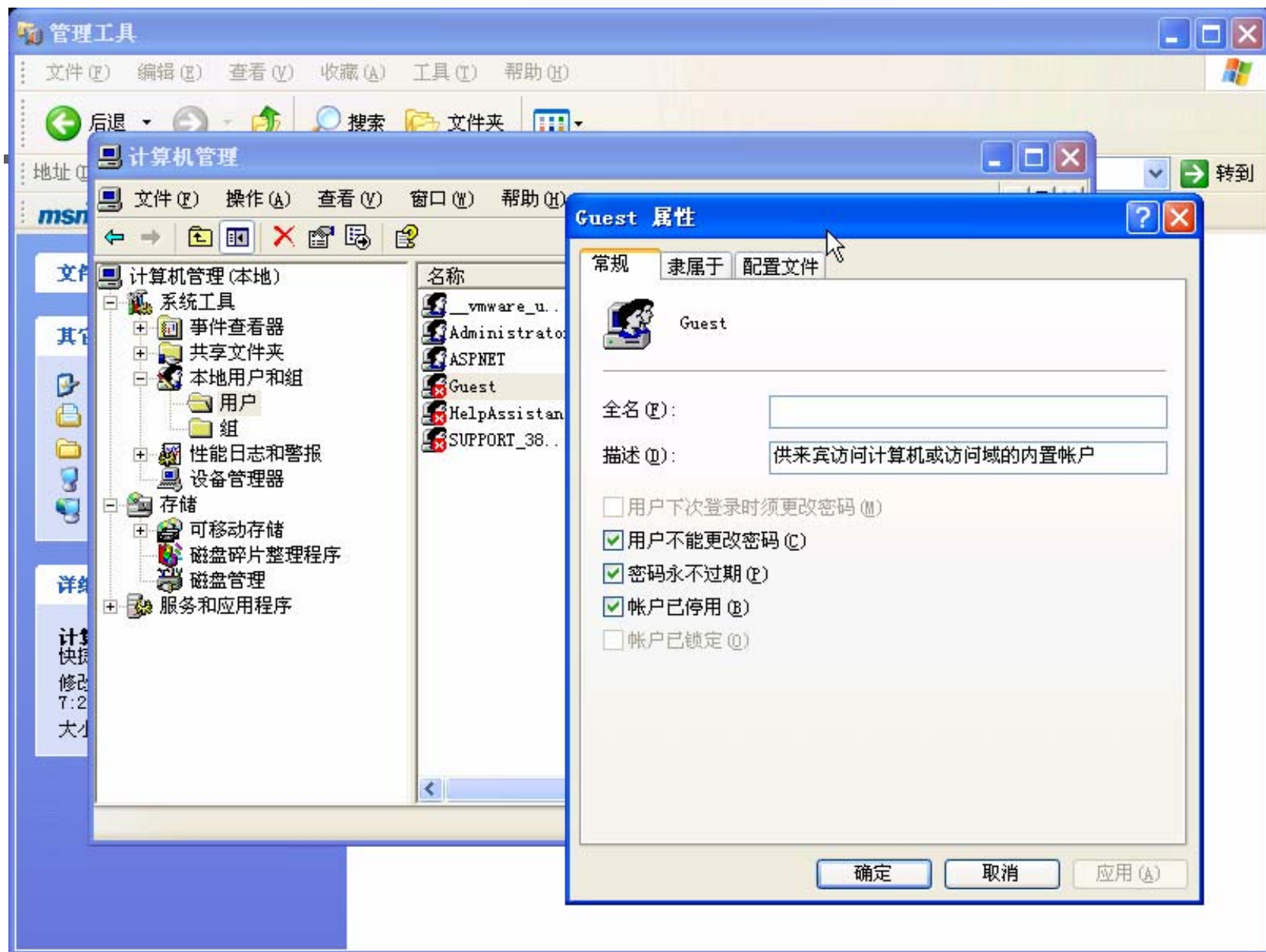
防范措施

- 1.禁用**Guest**帐号
- 2.停止共享
- 3.关闭不必要的服务
- 4.禁止建立空连接



禁用Guest帐号

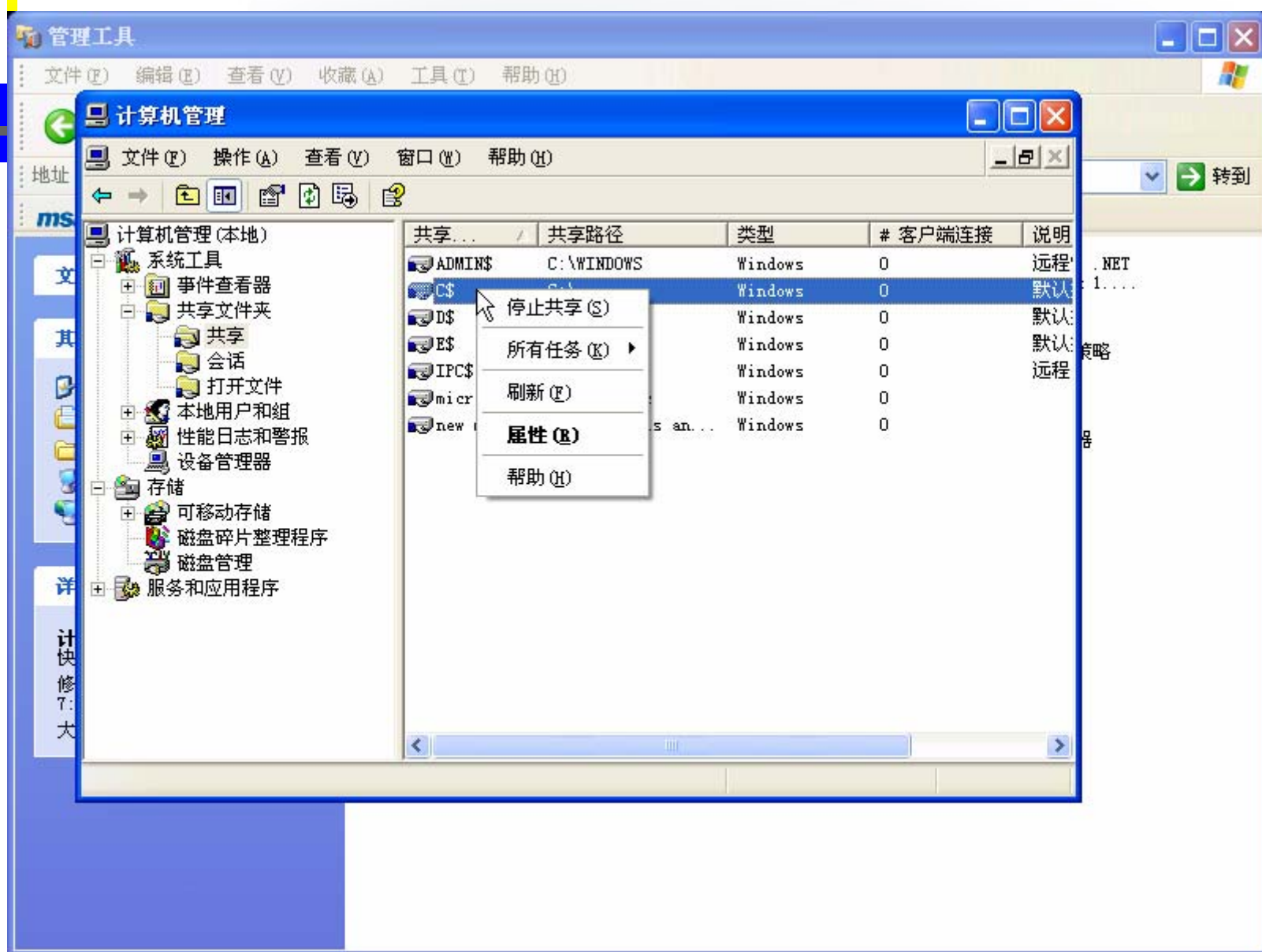
- 把**Guest**帐号禁用。有很多入侵都是通过这个帐号进一步获得管理员密码或者权限的。
- 计算机管理->本地用户和组->**Guest**帐号上面点击右键，选择属性，在“常规”页中选中“账户已停用”。





停止共享

- 点击开始→运行→**cmd**，然后在命令行方式下键入命令“**net share**”，可以查看目前的共享。
- 管理工具→计算机管理→共享文件夹→共享，在相应的共享文件夹上按右键，点“停止共享”。

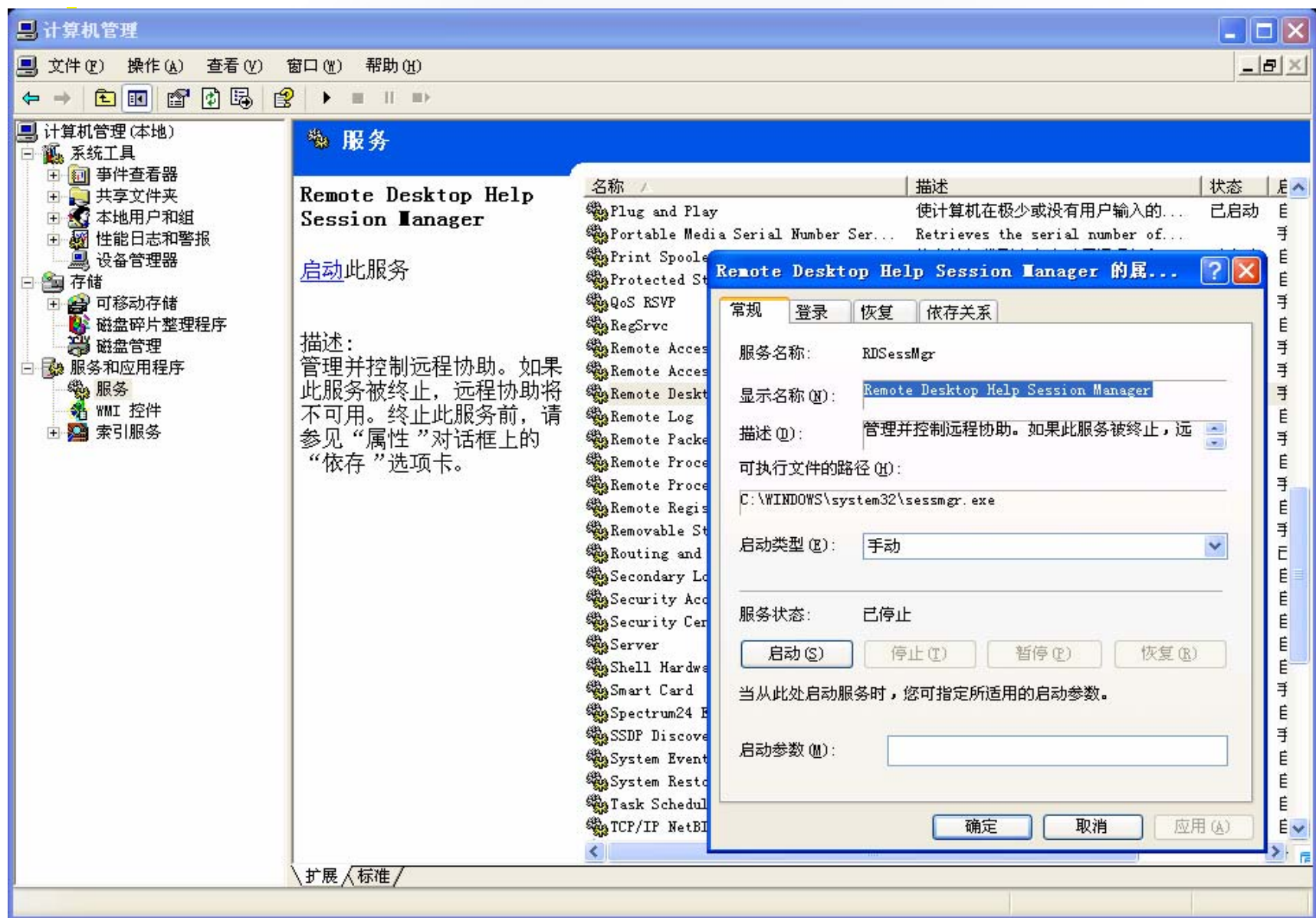


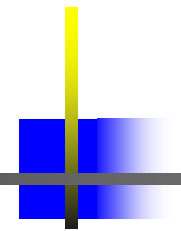
- 
- 或者
 - **net share ipc\$ /delete**
 - **net share admin\$ /delete**
 - **net share c\$ /delete**
 - **net share d\$ /delete**
 - **net share e\$ /delete**



关闭不必要的服务

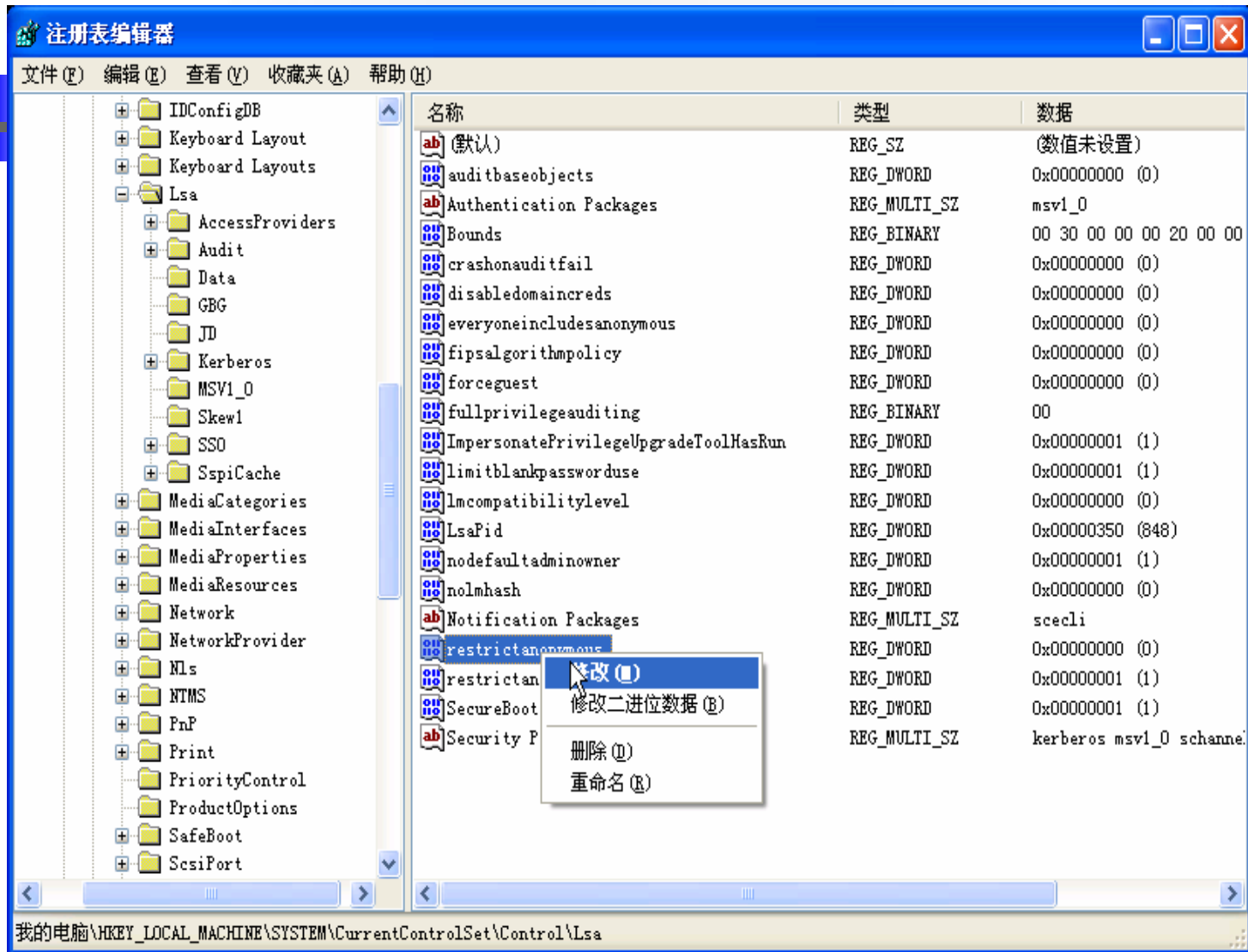
- 尽量关闭不必要的服务，如**Terminal Services**、**IIS**（如果你没有用自己的机器作**Web**服务器的话）、**RAS**（远程访问服务）等。
- 烦人的**Messenger**服务也关掉， 否则可能会收到有人发的网络广告。
- 管理工具→计算机管理→服务和应用程序→服务。
- 注意，彻底停止共享的办法是：关闭**Server**服务，也即**lanmanserver**，但如果对外提供**IIS**服务，则不要关闭这个服务。





禁止建立空连接

- 禁止建立空连接的两种方法
- (1)修改注册表：
HKEY_Local_Machine\System\CurrentControlSet\Control\LSA下，将**DWORD**值**RestrictAnonymous**的键值改成**1**。
- (2)修改Windows的本地安全策略：
设置“本地安全策略→本地策略→选项”中的**RestrictAnonymous**（匿名连接的额外限制）为“不容许枚举**SAM**账号和共享”。

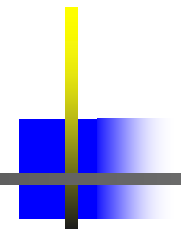




防毒软件

- 防毒软件是最为人熟悉的安全工具，可以检测、清除各种文件型病毒、宏病毒和邮件病毒等。在应对黑客入侵方面，它可以查杀特洛伊木马和蠕虫等病毒程序，但对于基于网络的攻击行为（如扫描、针对漏洞的攻击）却无能为力





网络病毒防范

考虑内部网络系统运行环境复杂，网上用户数多，同Internet有连接等，需在网络上建立多层次的病毒防护体系，对桌面、服务器和网关等潜在病毒进入点实行全面保护。

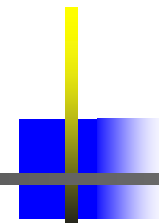
(1) 建立基于桌面的反病毒系统

在内部网中的每台桌面机上安装单机版的反病毒软件，实时监测和捕获桌面计算机系统的病毒，防止来自软盘、光盘以及活动驱动器等的病毒来源。

(2) 建立基于服务器的反病毒系统

在网络系统的文件及应用服务器（一些关键的Windows NT服务器）上安装基于服务器的反病毒软件，实时监测和捕获进出服务器的数据文件病毒，使病毒无法在网络中传播。

。



网络病毒防范

(3) 建立基于群件环境的反病毒系统

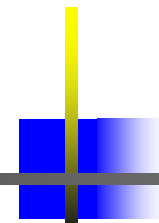
在网络系统的Louts Notes和Ms Exchange服务器上安装基于群件环境的反病毒软件，堵住夹在文档或电子邮件中的病毒。

(4) 建立基于Internet网关的反病毒系统

在代理服务器（Proxy）网关上安装基于网关的反病毒软件，堵住来自Internet通过Http或Ftp等方式进入内部网络的病毒。

(5) 建立病毒管理控制中心

在中心控制台实施策略配置和管理、统一事件和告警处理。通过自动更新、分发和告警机制，使桌面PC和服务器等设备自动获得最新的病毒特征库。



个人对病毒的防范

- 经常进行数据备份，特别是一些非常重要的数据及文件，以免被病毒侵入后无法恢复。
- 对系统引导区、**Boot**区及**FAT**表等要做好备份。
- 用**regedit**的导出和导入功能备份注册表。
- 采用一套较好的驻留式防病毒软件，以便进行实时监控，及时控制病毒的入侵,并及时、可靠地升级反病毒产品。
- 打开邮件的附件之前一定要三思而后行，即使是来自你信任的人，因为你的朋友很可能已经被病毒感染，



数据备份

- **1.标准备份：** 完全备份，如对整个**c**盘或**d**盘的备份，适用于服务器。
- **2.增量备份，** 只备份新建的文件或更新的数据。
- **3.差量备份，** 同上，区别是增量备份在备份后修改备份标志位，而差量备份不修改。
- 备份和归档不是一个概念。



背景知识：BIOS

在刚开机时，根据**X386CPU**的特性，**CS=FFFF**、**IP=0000**。这时**CPU**根据**CS**和**IP** 的值执行**FFFF0H**处的指令。**FFFF0H**已经到了基本内存的高地址顶端，此处的指令一般总是一个**JMP**指令，**jump**到**ROM BIOS** 的入口地址。然后**ROM BIOS** 进行开机自检，如检查内存，键盘等。最后，**ROM BIOS** 读取磁盘上的第一个扇区并将这个扇区的内存装入内存。



启动-MBR

硬盘的第一扇区称为主引导记录（**MBR**）。**MBR** 的长度为**512**字节。可分为两部分：第一部分为引导代码区，占了**446**个字节；第二部分为分区表，共有**66**个字节，记录硬盘的分区信息。以**BIOS**的**magic number AA55**结束。

MBR的代码要作以下的操作：

1. 确定活动分区。
2. 使用**BIOS**,将活动分区的启动扇区读入。
3. 跳到启动扇区的**0**位置。

如果用软盘启动计算机，**ROM BIOS** 读入的是软盘的引导区，既软盘的第一个扇区。



分区表

- 分区表有**4**项。叫做**4**个主分区,假如它们不够用,可以设置其中一个为扩展分区。扩展分区包含至少一个逻辑分区。
- 扩展分区的第一个扇区结构类似**MBR**,它的分区表的第一表项对应第一个逻辑分区。
- 如果存在第二个逻辑分区,那么分区表的第二个表项就包含了一个指针。这个指针指向第一个逻辑分区的起始位置,该位置又包含一个分区表。该分区表的第一表项对应第二个逻辑分区。这样就组成一个链表,从而扩展分区可以有任意多的逻辑分区。
- 每一个主分区(包括扩展区)都包含一个引导扇区。系统从活动的主分区的引导扇区启动。



备份和还原主引导扇区

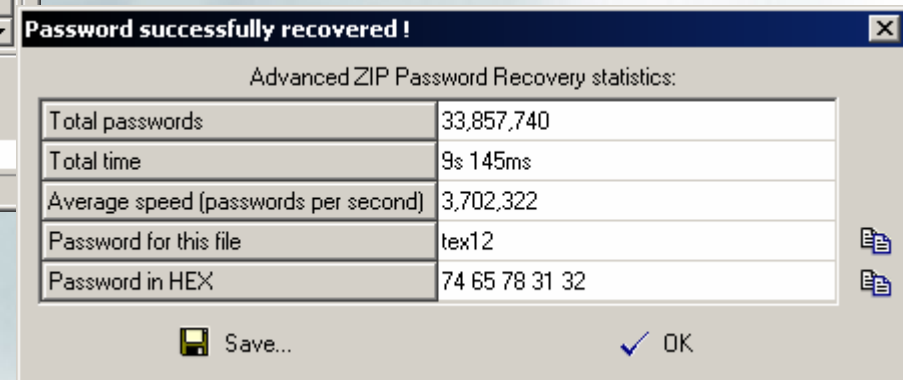
- 很多工具都可以完成这个功能
- **KV300, DISKMAN**
- **Disk Genius**的前身是**DISKMAN**, 中文图形界面, 支持鼠标操作
- 修复硬盘主引导程序最简单有效的方法, 就是利用引导盘引导系统, 然后执行“**Fdisk /MBR**”命令
- **Windows 2000/XP**安装光盘里的**Dskprob.exe**, 在\support\tools目录中。

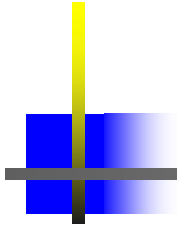


数据恢复

- **Recover Lost Data**
Handy Recovery
GetDataBack
Restorer2000 Professional
Magic Recovery
ZAR32
- **Recover My Files**
Quick Recovery
R-Studio
Stellar Phoenix
Recover It All
Data Rescue PC
- **FinalData**
- **Easyrecovery**
- **Revival**

口令破解: ZIP密码破解

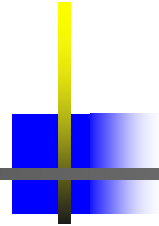


- 
- **advanced office password recovery**
 - **advanced PDF password recovery**
 - **...**



Windows帐户密码

- **Windows**采用安全账号管理器(**SAM**)机制。用户名和口令经过加密**hash**变换后存放在`%systemRoot%\System32`下的**sam**文件中。
- **L0phtCrack**通过破解**SAM**文件来获取用户名和密码。
- **LC3**, **LC5**, 字典结合暴力破解, 速度较快。

- 
- 在L0phcrack的选项中的“**Open Wordlist File**”提供字典文件的位置，并提供了“**Hybrid Attack**”(混合破解)和“**Brute Force Attack**”(野蛮破解)，混合破解会利用像“**Password12345**”这样的简单组合来测试**SAM**的密码。
 - **John**主要是用来对**UNIX**的“**Password**”进行破解的一个强大的工具，但是它同样的具有破解“**Windows NT LanManager**”散列加密值的功能。

口令攻击演示：XP/2000密码

LC3 - [me.lcs]

File View Import Session Help

User Name	LM Password	<8	NTLM Password	LM Hash	NTLM Hash	Cha
21cn		x		C22CA7D1C4A...	18FB2B3747DC...	
Administrator	?????????			423A10161A1...	B27F951CCEA7...	
cyyang	????????N			C6E6D533416...	749047F69CCA...	
ftpsur		x		176C168B35D...	967CE1620F41...	
Guest	????????4			1319B0FA23C...	0A640404B5C3...	
IUSR_TESTER				845D8411F52...	A316D9D85333...	
IWAM_TESTER				4BF231F4AB4...	03C545E2184B...	
tester1	????????L			26A8E973E43...	8CFD40B90A3B...	
__vmware_user__	* empty *	x		AAD3B435B51...	FFD635ED5500...	

Dictionary Status

words total: 98710
words done: 235007
% done: 42.003%

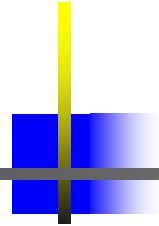
Brute Force

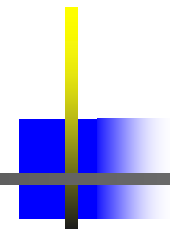
time elapsed: 0d 0h 0m 0s
time left:
% done:
current test:
keyrate:

☒ User Info Check
☒ Dictionary
☐ Hybrid
☐ Brute Force

LC3
Security Software Technologies, Inc.
securitysoftwaretech.com

Ready

- 
- 问题：系统运行后，无法直接打开和拷贝**sam**文件。
 - 从光盘或软盘启动。
 - 或者安装了多个操作系统，启动另一个系统，可接触目标系统所在盘。
 - 删除目标系统的**sam**或改名。
 - 重启动目标系统，空密码即可进入。



防范

- 1.在**bios**里禁止从软盘和光盘启动
- 2.一台机器只装一个操作系统



Windows2000

- 在**c:\winnt\repair**目录下，有一个文件叫做**SAM._**。这是**SAM**数据库的压缩版本。它是在系统安装时建立的，用**rdisk**工具运行更新。普通用户有读它的权限。
- 运行**rdisk**更新：
c:\>rdisk /s
- 进入**c:\winnt\repair**目录，将**SAM._**拷贝到另一个目录。
并键入：
c:\temp>expand SAM._ sam
- 然后，使用一个叫**SAMDump**的工具。**SAMDump**会将这个文件转换成能使用的格式：
c:\temp>samdump sam > samfile
接下来就可以运行**l0phtcrack**



windows XP

- 使用**pwdump3**导出**sam**文件。
- 运行：
- **c:\pwdump>pwdump3 127.0.0.1 pdump**
- 产生文件**pdump**
- 然后，运行**l0phtcrack**，选择**import from pwdump**，即可。

其他：如果有**admin**权限，可远程**dump**，防范：可将系统的**REMOTE REGISTRY SERVICES**关闭。

安全审计系统

- 安全审计系统通过独立的、对网络行为和主机操作提供全面与忠实的记录，方便用户分析与审查事故原因，很像飞机上的黑匣子。由于数据量和分析量比较大，目前市场上鲜见特别成熟的产品。

主动式审计（IDS部署）

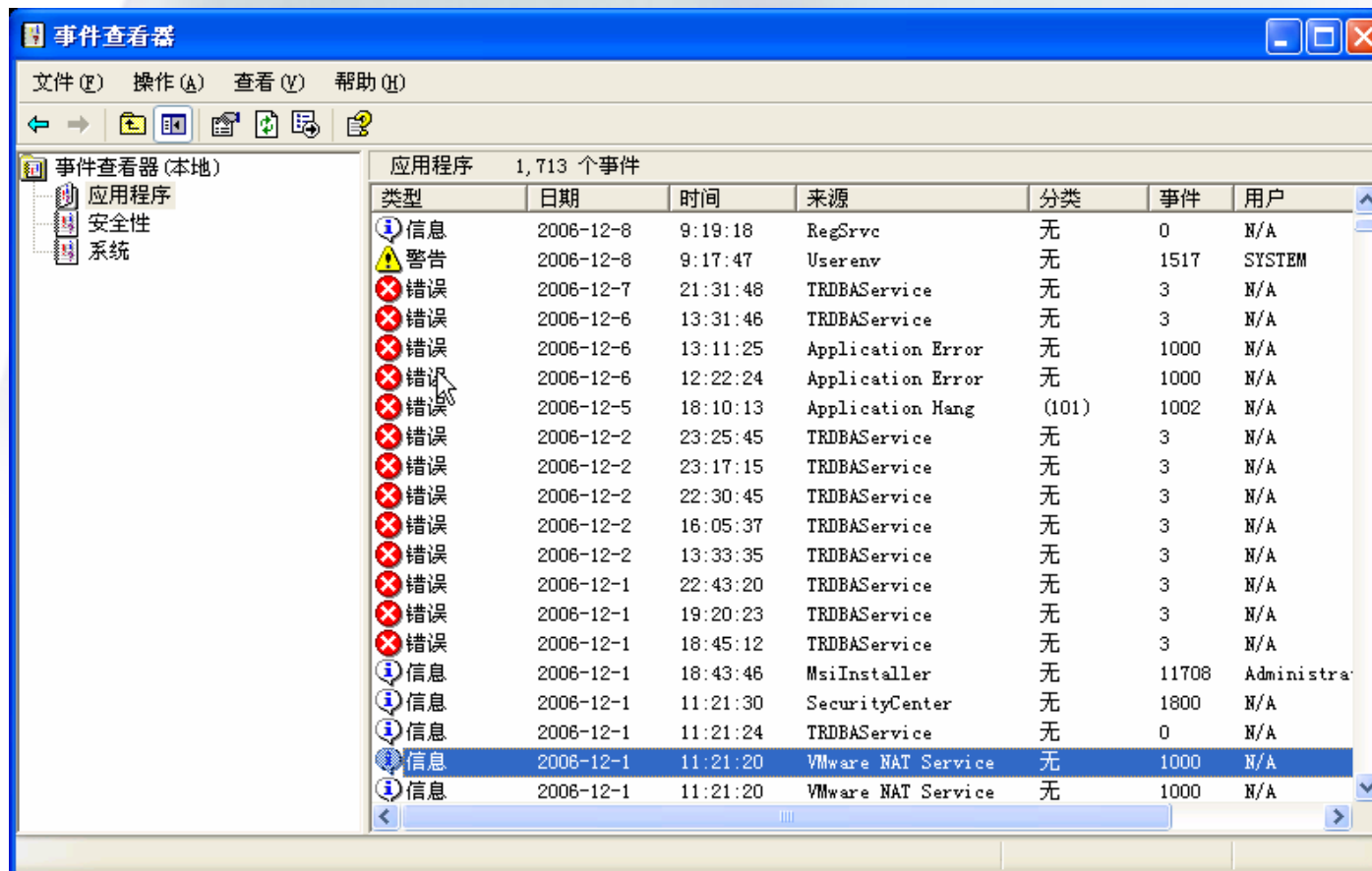
被动式审计（日志监控）

注意：和记帐不同，记帐收集和存储的是用户对各种资源使用情况的数据，而不是操作记录。



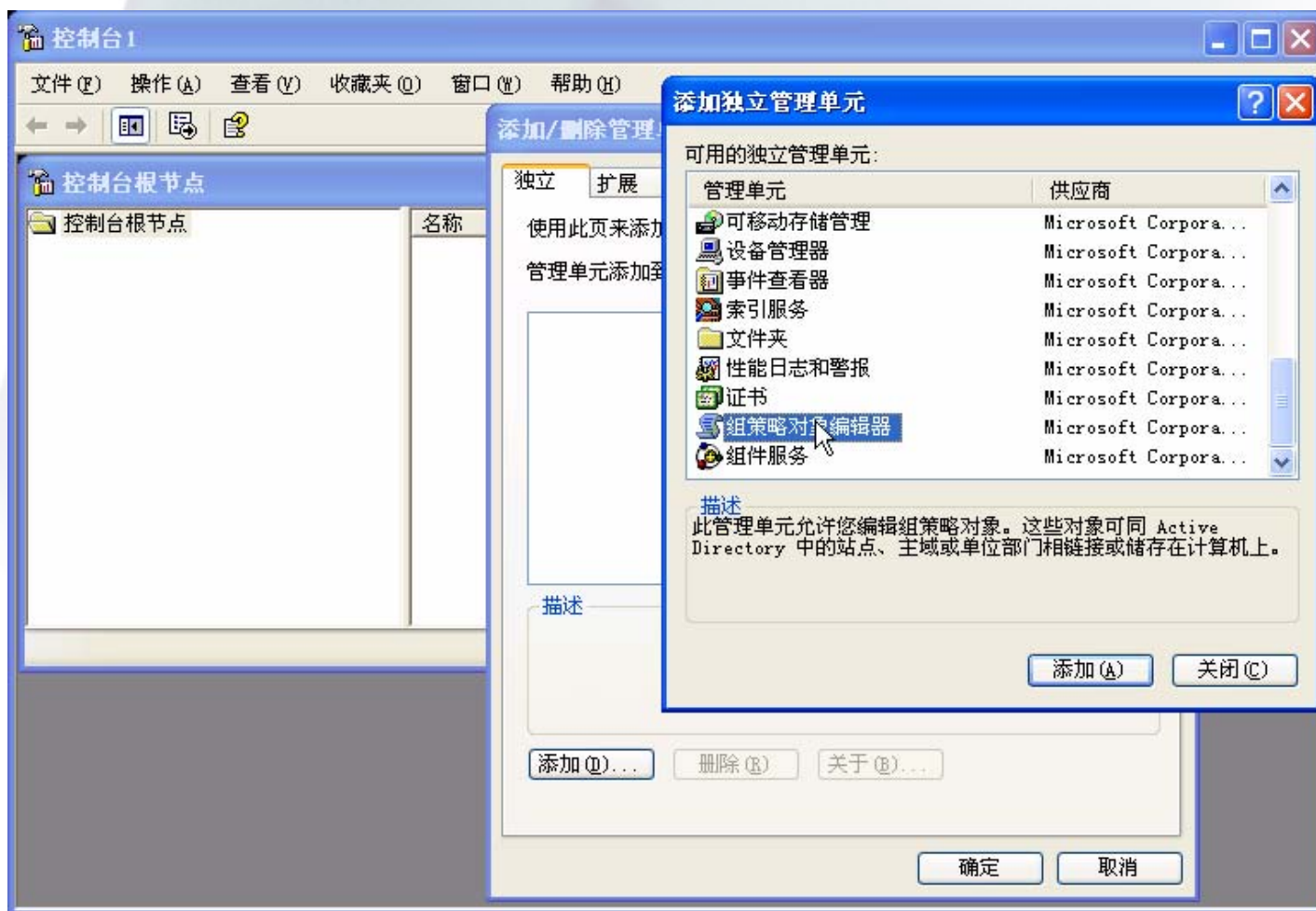
Windows的事件查看器

- 程序->控制面板->管理工具->事件查看器

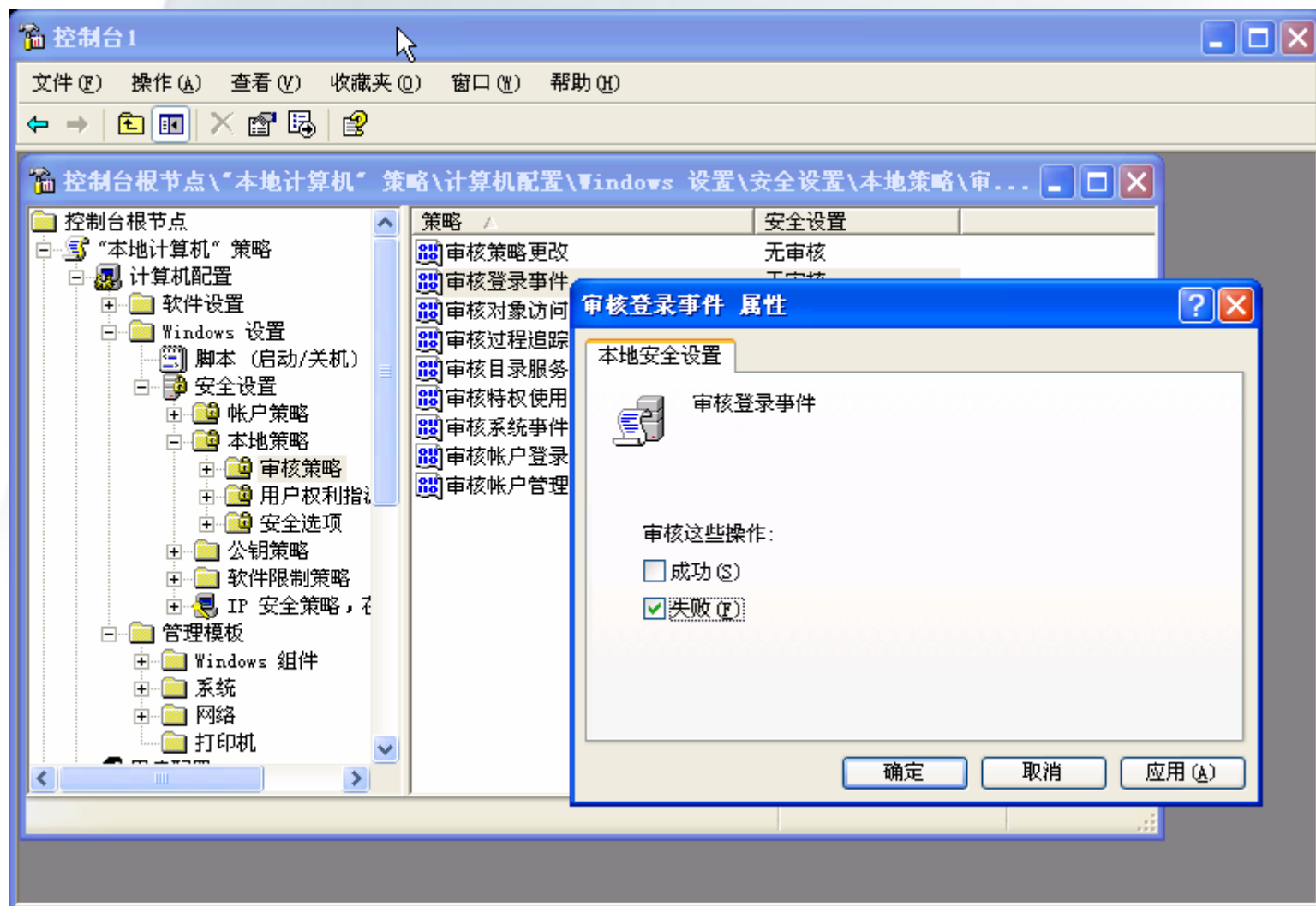


启用安全日志

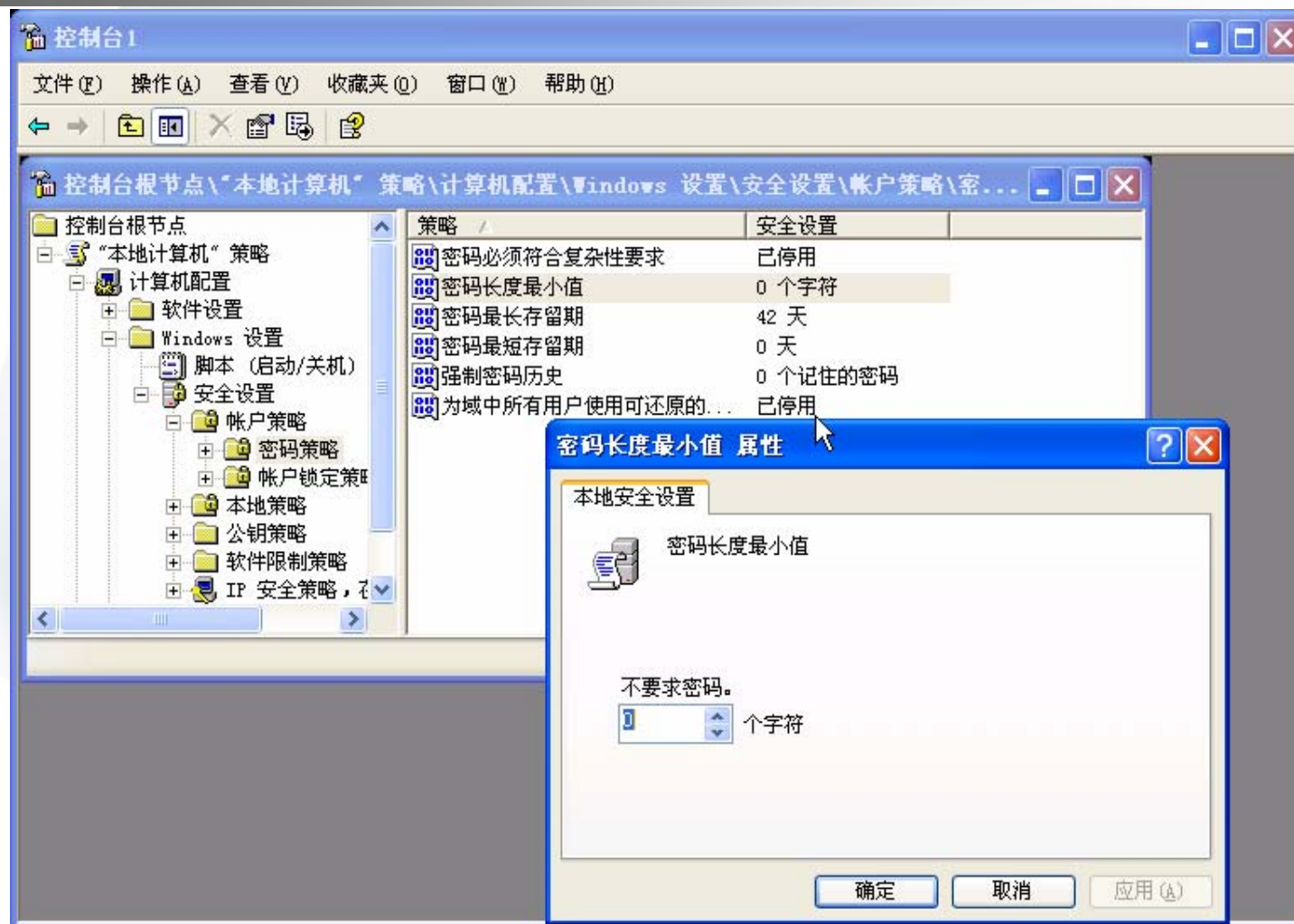
- 安全日志默认是停用的，键入`mmc /a`进行配置



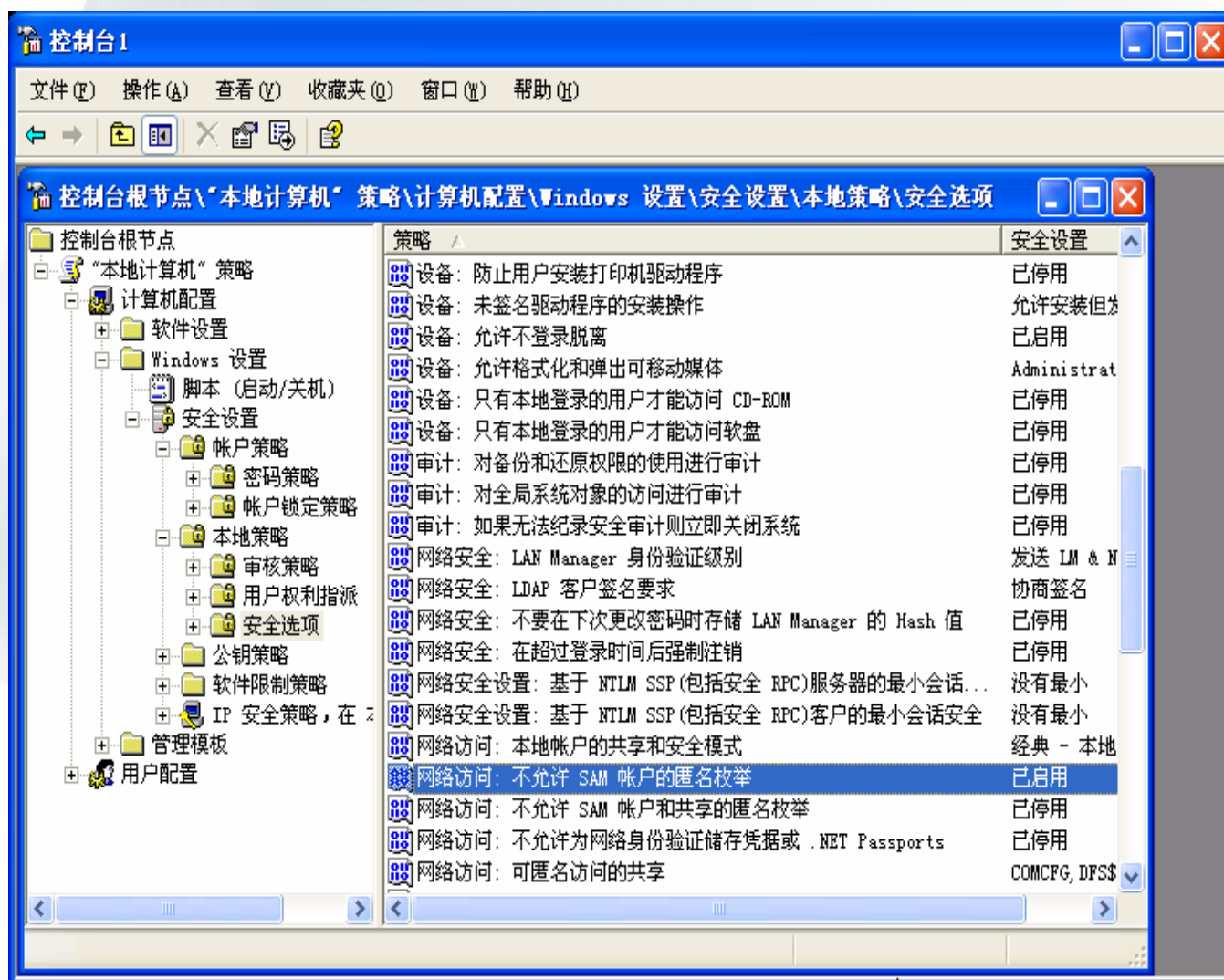
对安全事件审核



口令安全设置



其它安全选项





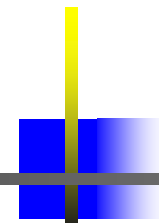
日志文件

- 系统日志，安全性日志和应用程序日志分别位于 **%systemroot%\system32\config** 目录下。
secevent.evt, sysevent.evt, appevent.evt
- 应用程序有自己的日志，如**IIS**每天生成一个日志，如文件名**ex061123**表示**06年11月23号**产生的日志，记录的是**www或ftp**的日志。
- **IIS的WWW**日志位于系统盘中
%systemroot%\system32\logfiles\w3svc1 目录下。
- **IIS的FTP**日志位于系统盘中
%systemroot%\system32\logfiles\msftpsvc1 目录下。



什么是防火墙

- 防火墙对流经它的网络数据进行扫描，以图过滤掉一些攻击，可以关闭某些不使用的端口。还能禁止特定端口的流出通信，以封锁木马。
- 防火墙有不同类型。可以是硬件，可以在一台主机上运行，作为它背后网络中所有计算机的代理和防火墙。最后，还可以个人防火墙的形态出现。



边界安全

- 防火墙作为一个阻塞点或控制点，能极大地提高内部网络的安全性。
- 美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。
- 所谓网络边界即是采用不同安全策略的 两个网络连接处。
 - 如用户网络和互联网之间连接
 - 和其它业务往来单位的网络连接
 - 用户内部网络不同部门之间的连接



防火墙特点

- 1.内部网络和外部网络之间的所有网络数据流都必须经过防火墙。
- 2.只有符合安全策略的数据流才能通过防火墙。
- 3.防火墙自身应具有非常强的抗攻击免疫力。

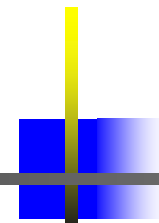
防火墙产品中，国外主流厂商为**Cisco**、**CheckPoint**、**NetScreen**等，国内主流厂商有很多。



什么是IDS

- **IDS（Intrusion Detection Systems）**依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果。

假如把防火墙比作一幢大楼的门锁，那么**IDS**就是这幢大楼里的监视系统。



IDS的部署

- **IDS**应当挂接在所有**所关注流量**都必须流经的链路上。"所关注流量"指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。
- **HUB**式的共享介质网络已经很少，**IDS**的位置一般选择在：
 - 服务器区域的交换机
 - 路由器之后的第一台交换机上
 - 重点保护网段的局域网交换机上



什么是VPN

- 分公司、经销商、合作伙伴、客户和外地出差人员要求随时经过公用网访问公司的资源,这些资源包括:公司的内部资料、办公 **OA**、**ERP**（企业资源计划）、**CRM**（客户关系管理）系统、项目管理系统等。
- **VPN（Virtual Private Network）**通过一个公用网络建立一个临时的、安全的连接，为位于不同地方的两个或多个企业内部网之间建立一条专有的安全线路，就好像是架设了一条专线一样。



VPN: IPSec vs SSL

- **SSL VPN**比较适合用于移动用户的远程接入，而**IPSec VPN**适合网对网连接。
- **SSL VPN**是基于应用层的**VPN**，**IPsec VPN**是基于网络层的**VPN**。
- **IPsec VPN**对所有的**IP**应用均透明；**SSL VPN**保护基于**Web**的应用更有优势，也支持**TCP/UDP**的**C/S**应用，例如文件共享、网络邻居、**Ftp**、**Telnet**、**Oracle**等，容易提供细粒度访问控制。



安全相关的标准

ISO IEC ITU CCITT IETF IRTF IESG DOD
NSA NIST ARPA

OSI RFC ISO/IEC13335 ISO/IEC17799
IATF TCSEC ITSEC CC



ISO IEC

- ISO(国际标准化组织)和IEC(国际电工委员会)是世界性的标准化专门机构。
- 国家成员体（他们都是ISO或IEC的成员国）通过国际组织建立的各个技术委员会参与制定特定技术范围的国际标准。
- 发布一项国际标准，至少需要75%的参与表决的国家成员体投票赞成。
- 开放系统互联(OSI)基本参考模型(ISO/IEC7498)是由ISO/IEC JTC1“信息技术”联合技术委员会与ITU-T共同制定的。
- CCITT是一个联合国条约组织，属于国际电信联盟，现在改名为ITU。



系统安全管理

- **ISO/IEC13335 《IT安全管理方针》（GMITS）系列，可以作为替代：**
 - ☐ **ISO/IEC13335-1 : 1996 《IT安全的概念与模型》**
 - ☐ **ISO/IEC13335-2 : 1997 《IT安全管理和计划制定》**
 - ☐ **ISO/IEC13335-3 : 1998 《IT安全管理技术》**
 - ☐ **ISO/IEC13335-4 : 2000 《安全措施的选择》**
 - ☐ **ISO/IEC13335-5 : 《网络安全管理方针》**



安全管理的微观粒度在加细

- **ISO/IEC17799**

- ☐ 建立机构的安全策略
 - ☐ 机构的安全基础设施
 - ☐ 资产的分类和控制
 - ☐ 人员安全
 - ☐ 物理与环境安全
 - ☐ 通信与操作管理
 - ☐ 访问控制
 - ☐ 系统开发与维护
 - ☐ 业务连续性管理
- 20多个要素120多个测试点**



IAB IETF IRTF

- Internet 体系结构委员会下设两个重要部门：Internet 工程特别工作组（IETF）和 Internet 研究特别工作组（IRTF）。发展到今天，IAB 公布的协议参考草案（RFC）已经积累到 3000 多个。
- **IAB**: 负责定义互联网的整体架构
- **IETF**: 互联网的协议施工与开发
- **IESG**: 负责 IETF 的技术管理和互联网标准化过程的技术管理



RFC

- 在**IETF**的推荐下,**RFC**被提升为标准
 - ☐可靠并且容易被理解
 - ☐技术先进
 - ☐在实际应用中具有多重独立性和可操作性
 - ☐能够赢得广泛的支持
 - ☐对互联网的部分或所有领域具有强可用性



美国的标准机构

- 美国国内与信息安全事物有关的管理机构主要有国家安全局（**NSA**）、国家标准技术研究所（**NIST**）、联邦调查局（**FBI**）、高级研究计划署（**ARPA**）和国防部信息局（**DISA**）。他们有各自授权管理的领域和业务，同时，这些机构。通过信息安全管理职责上的理解备忘录和协议备忘录进行合作。

IATF

- 美国国家安全局NSA制定的信息保障技术框架（IATF）
1998年开始，已发布V3.0

三保卫、一支撑				
保卫网络 基础设施	保卫边界和 外部连接	保卫局域 计算环境	支撑基础设施	
无线安全	Firewalls	Operating Systems	KMI/PKI	Detect and Respond
www安全	VPNs	Biometrics	PKI Protection Class 4 PKI Directory	IDS
	Peripheral Sharing Switch	Single Level Web		
	Remote Access	Tokens		
	Multiple Domain Solutions	Mobile Code		
	Mobile Code	Secure Messaging		



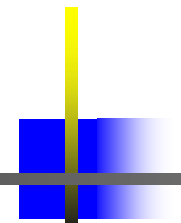
DoD NCSC

美国国防部 (DoD) 早在80年代就针对计算机安全保密开展了一系列有影响的工作，后来成立的**国家计算机安全中心** (NCSC) 接续进行有关的工作。1983年他们公布了《**可信计算机信息系统评价准则**》**TCSEC**，以后NCSC又出版了一系列有关可信计算机数据库、可信计算机网络的指南。



NIST

- NIST与NSA紧密合作，在NSA的指导监督下，制定计算机信息系统的技术安全标准。他的工作一般以NIST出版物（FIPS PUB）和NIST特别出版物（SPEC PUB）等形式发布。
- 该机构比较有影响的工作是制定公布了美国国家数据加密标准DES，参加了美国、加拿大、英国、法国、德国、荷兰等国制定的信息安全的通用评价准则（CC），在1993年制定了密钥托管加密标准EES。



一些公司的建议或标准

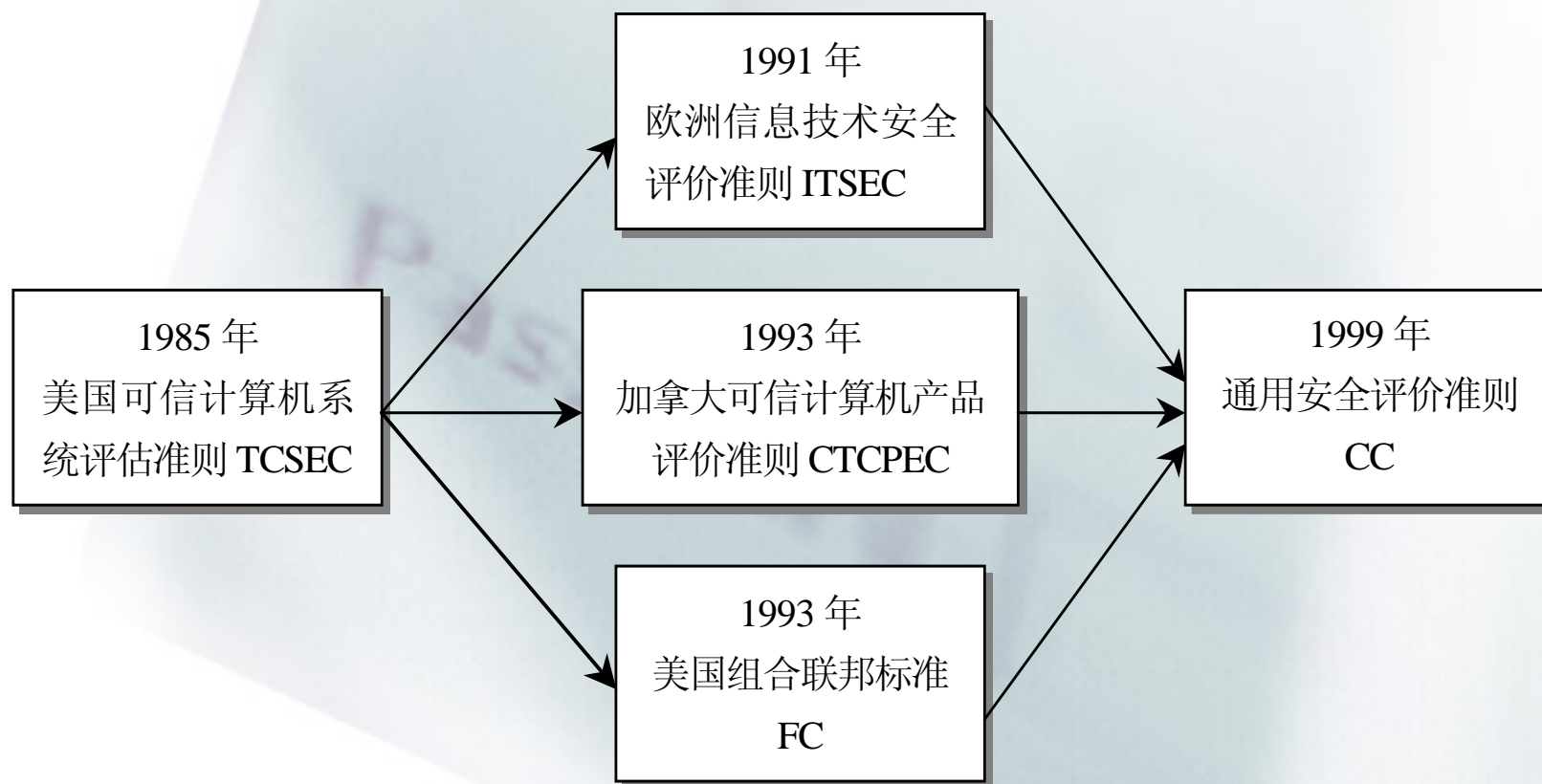
协议名	协议开发者	协议内容
PKCS	RSA 数据安全公司 RSA 实验室在 Apple , Microsoft, DEC, Lotus, Sun 和 MIT 等机构非正式的咨询合作下开发	公开密钥密码标准与 ITU-X. 509 标准兼容
SSL	Netscape	用于 WWW 上的会话层安全协议
S-HTTP	Enterprise Integration Technologies	基于 WWW, 提供保密、认证、完整性和不可否认服务
PTC	Microsoft 和 Visa	保密通信协议, 与 SSL 类似, 不同的是, 它在客户和服务器之间包含了几个短的报文数据, 认证和加密使用不同的密钥, 提供了某种防火墙功能
SET	Visa 和 Mastercard	开放网络电子支付协议



安全测评

- **80年代:**
 - ❑ 美国**DoD TCSEC**, (橘皮书。彩虹系列)
- **90年代:**
 - ❑ 英、法、德、荷**ITSEC** (白皮书)
- **90年代末至今:**
 - ❑ 六国七方: **CC (Common Criteria)**

信息系统评测标准





TCSEC

- TCSEC的第一版发布于1983年，1985年最终修订。由于使用了桔色书皮，通常人们称其为“**桔皮书**”，后来在NCSC的主持下制定了一系列相关准则，称之为彩虹系列，其中，1987年，NCSC为TCSEC提出的可依赖网络解释(TNI 1987)通常被称作“红皮书”。1991年，为TCSEC提出的可依赖数据库管理系统解释(TDI 1991)通常称作“紫皮书”。



TCSEC

- TCSEC将计算机安全从低到高顺序分为四等八级：最低保护等级（D）、自主保护等级（C1，C2）、强制保护等级（B1，B2，B3）和验证保护等级（A1，超A1），为信息安全产品的测评提供准则和方法，指导信息安全产品的制造和应用。TCSEC是针对孤立计算机系统提出的，特别是小型机和主机系统，假设有一定的物理屏障，该标准适合军队和政府，不适合企业，是一个静态模型。



ITSEC

- 在借鉴TCSEC成功经验的基础上，90年代初，西欧四国（英、法、荷、德）联合提出了信息技术安全评价准则（ITSEC）。

ITSEC定义了七个安全级别：

不能充分满足保证（E0）

功能测试（E1）

数字化测试（E2）

数字化测试分析（E3）

半形式化分析（E4）

形式化分析（E5）

形式化验证（E6）

CC

- 进入90年代中期，美国改进TCSEC与各国改进ITSEC的想法不谋而合，宣布了制定通用安全评价准则（CC）的计划，它的全称是Common Criteria for IT security Evaluation。
- CC的制定考虑了对前期标准的兼容，因而他们之间可建立如下的粗略的对应关系。

TC SEC C	D	——	C1	C2	B1	B2	B3	A1
IT SEC C	E0	——	E1	E2	E3	E4	E5	E6
CC	——	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7



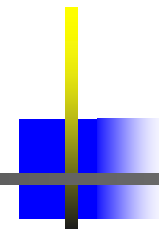
管理安全等级划分

- 国家标准《计算机信息系统安全保护等级划分准则》
- 第一级：用户自主保护级
 - 实施计划管理
- 第二级：系统审计保护级
 - 实施操作规程管理
- 第三级：安全标记保护级
 - 实施标准化过程管理
- 第四级：结构化保护级
 - 实施安全生态管理
- 第五级：访问验证保护级
 - 实施安全文化管理



信息系统安全法规

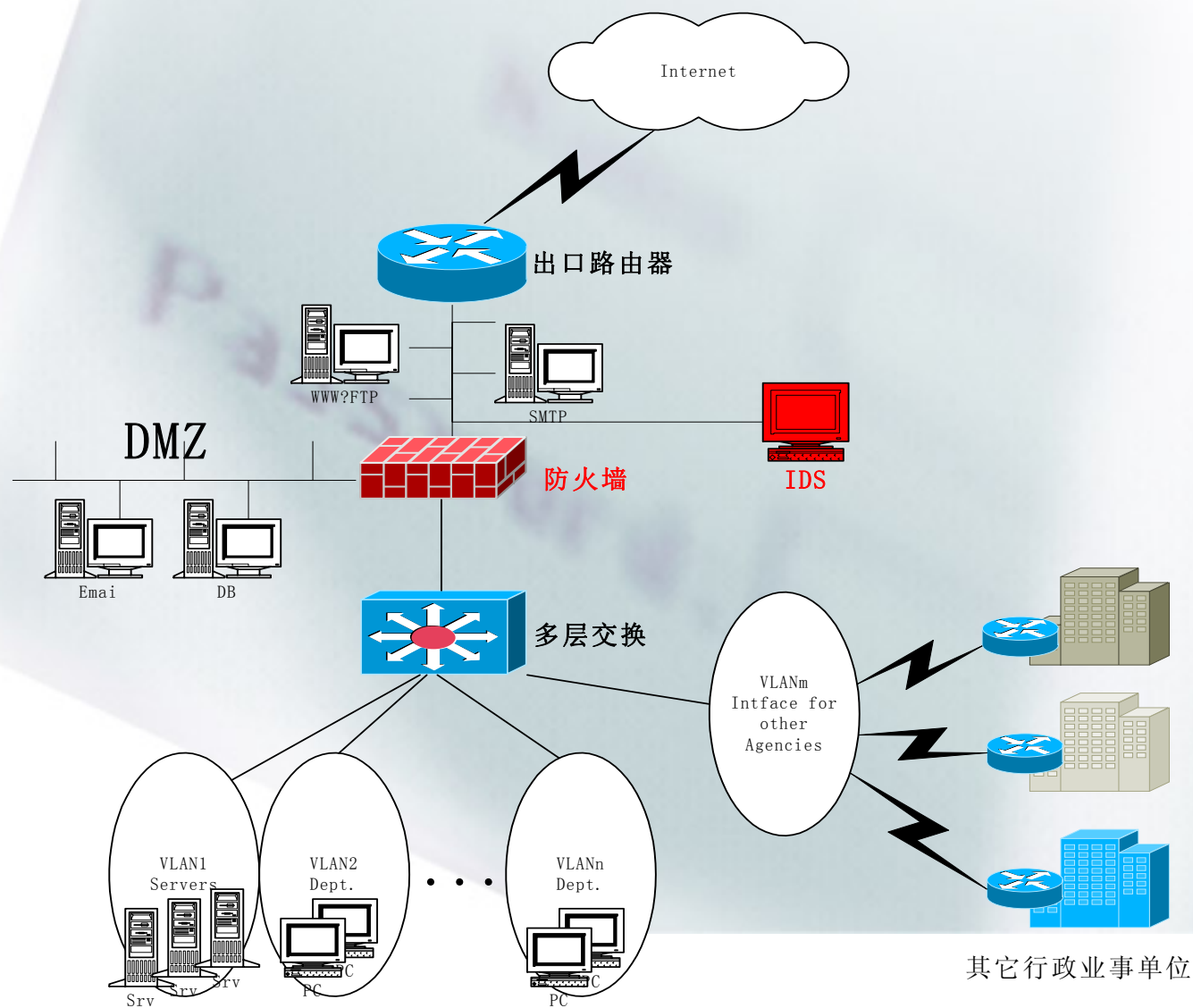
- 《计算机信息网络国际联网安全保护管理办法》由公安部于**1997年12月30日**发布的。
- 《计算机信息系统国际联网保密管理规定》，由国家保密局发布并于**2000年1月1日**开始执行。
- 《商用密码管理条例》是国务院在**1999年10月7日**发布的。
- 《计算机病毒防治管理办法》是公安部于**2000年4月26日**发布执行的。
- 《中华人民共和国电子签名法》于**2005年4月1日**正式实施。配套部门规章《电子认证服务管理办法》同时实施。



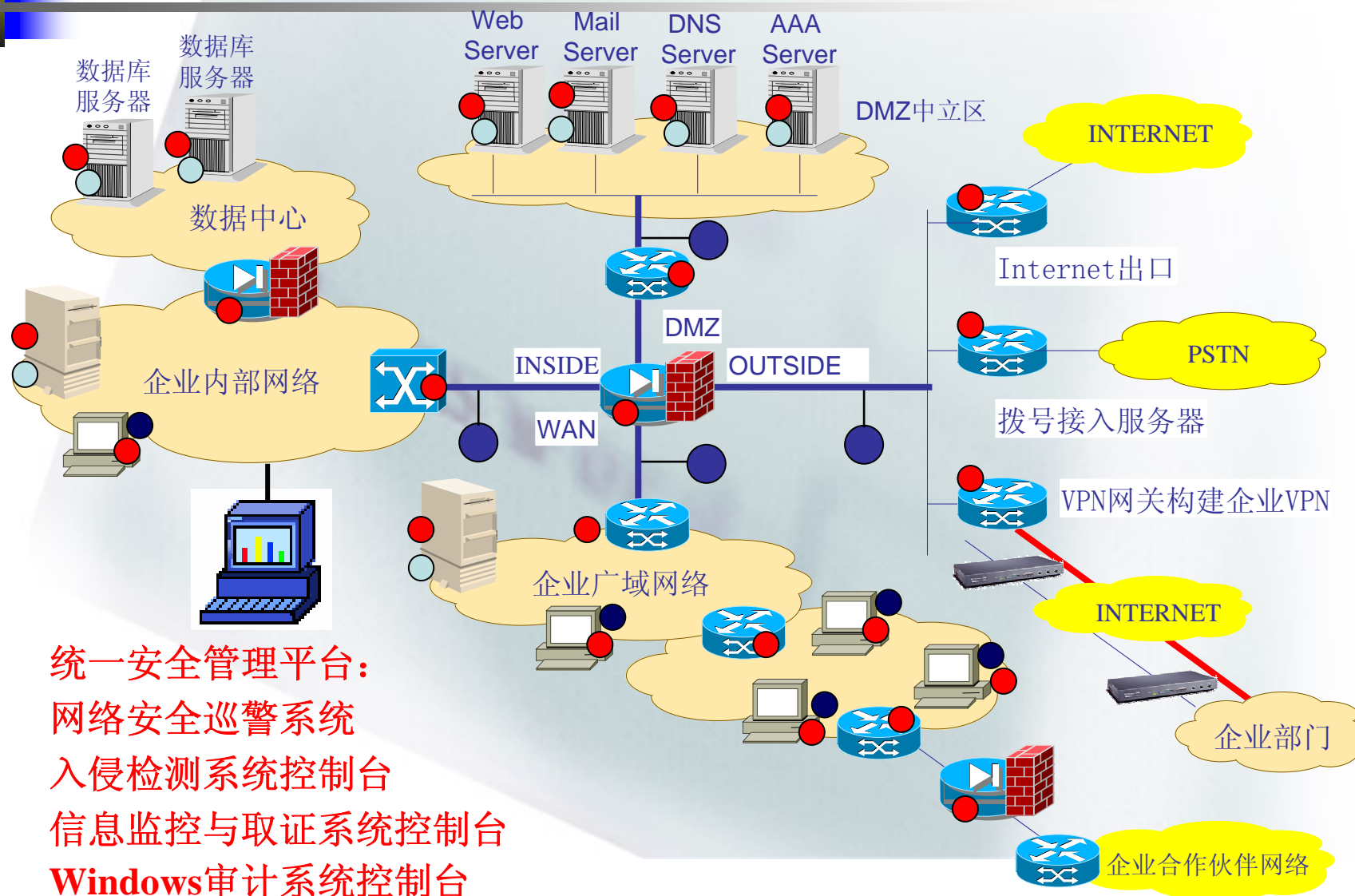
许可证制度

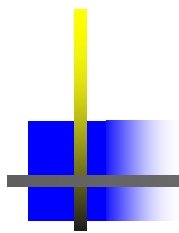
- 《计算机信息系统安全专用产品检测和销售许可证管理办法》是公安部于**1997年12月12日**发布并执行的，其主要内容如下：
- （1）我国境内的安全专用产品进入市场销售，实行销售许可证制度。
- （2）颁发销售许可证前，产品必须进行安全功能的检测和认定。
- （3）公安部计算机管理监察部门负责销售许可证的审批颁发、检测机构的审批、定期发布安全专用产品的检测通告和经安全功能检测确认的安全专用产品目录。
- （4）销售许可证只对所申请销售的安全专用产品有效，有效期为两年。

某省信息中心网络拓扑图



信息网络系统安全解决方案





Q&A

谢谢！