网络信息安全管理培训

2019年1月15日

一、什么是信息？

- 消息、信号、数据、情报和知识
- 信息本身是无形的，借助于信息媒体以多种形式存在或传播：
  - 存储在计算机、磁带、纸张等介质中
  - 记忆在人的大脑里
  - 通过网络、打印机、传真机等方式进行传播
- 信息借助媒体而存在，对现代企业来说具有价值，就成为信息资产：
  - 计算机和网络中的数据
  - 硬件、软件、文档资料
  - 关键人员
  - 组织提供的服务
- 具有价值的信息资产面临诸多威胁，需要妥善保护

- 不论信息的形式是什么，不论是文字、数字、图形（像）和声音等，在计算机中都转换成二进制符号‘0’和‘1’来保存和处理。

```
void main()
{

// 了解结构体的使用方法1
    char kk[10]="大家好";
    Argon *p;
    Position *q;

    p=new Argon;
    q=new Position; //如果
    q->x=1;
    q->y=2;
    q->z=3;
```

Memory

地址: kk

0012FF74	B4	F3	BC	D2	BA	C3	00	大家好.
0012FF7B	00	00	00	CC	CC	C0	FF	...烫..
0012FF82	12	00	89	13	40	00	01	....@..
0012FF89	00	00	00	60	0F	37	00	...`.7.
0012FF90	08	10	37	00	00	00	00	..7....
0012FF97	00	C8	05	93	7C	00	E0	...揩..
0012FF9E	FD	7F	21	96	4F	80	9C	?!聋..

上下文: main()

名称

信息是资产

- 企业的信息资产包括计算机和网络中的数据、硬件和软件、关键人员、组织提供的服务以及各类文档（专利、标准、商业机密、文件、图纸、管理规章等等）

- 信息是一种资产，像其他重要的业务资产一样对组织具有价值，因此需要妥善保护。

企业关注的信息类型

内部信息

组织不想让其竞争对手知道的信息

客户信息

顾客/客户不想让组织泄漏的信息

共享信息

需要与其他业务伙伴分享的信息

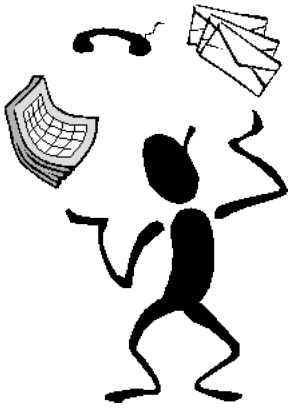
信息生命周期

- 从安全的角度去考察信息资产，并不能只停留在静态的一个点或者一个层面上。

- 信息是有生命周期的，从创建到被使用或操作，到储存，再到被传递，直至其生命周期结束而被销毁或丢弃，各个环节各个阶段都应被考虑到，安全保护应该兼顾信息存在的各种状态，不能够有所遗漏。

信息的处理方式

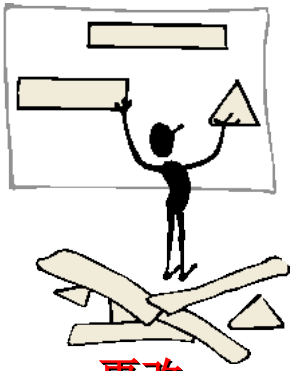
创建



使用

存 储

传递



更改

销毁


输入
创建
分类
转换
收集
处理
传送
保护
恢复
转换
管理
业务流程
存储
保护
迁移
存档
遵守法规
保留
共享
分发
格式
显示
打印
交付

二、 信息安全基本概念

- 信息安全和其保护的信息对象有关。本质是在信息的安全期内保证其在传输或静态存放时不被非授权用户非法访问。但允许授权用户访问。
  - 1. 物理安全
  - 2. 通信安全
  - 3. 辐射安全
  - 4. 系统安全
  - 5. 网络安全
  - 6. 人员安全

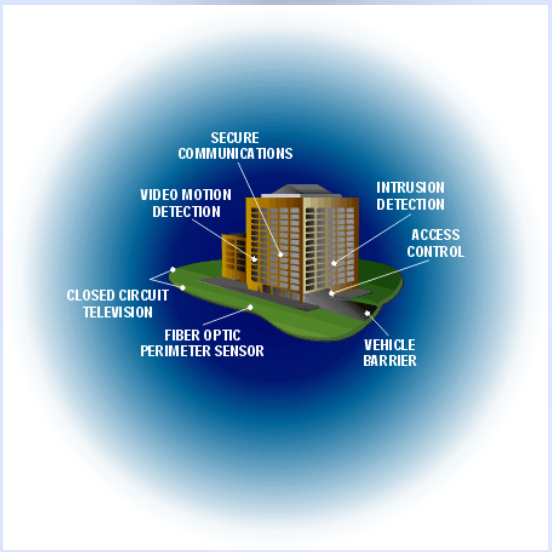
- 1. 物理安全

IBM: ASCI White超级计算机

8 192个 CPU　最大平均速度 7.304 TF (10^{12})

物理安全要点提示

- 清晰划定安全区域边界
- 围墙、门锁、照明、告警、监视系统
- 专门设立接待区，限制物理访问
- 外来人员登记及陪同
- 定期检查访问记录
- 关键设施不要放置在公共区域
- 关键区域不做显眼标记
- 防止火灾、水灾、地震、爆炸等自然或人为灾难
- 安全区域内工作，禁止摄影摄像，加强监督
- 一定要注意那些不在视野范围内的东西

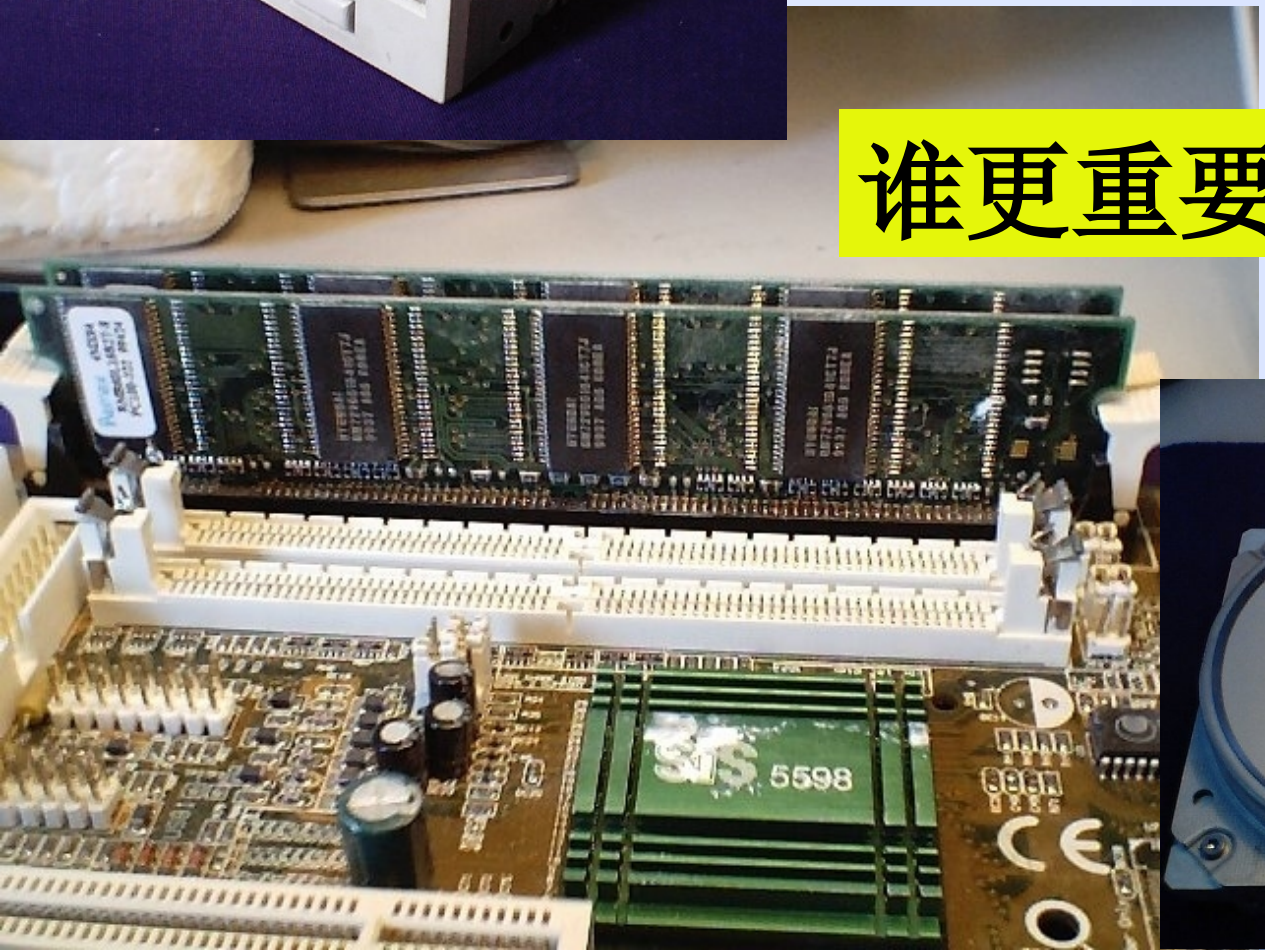


九城上海机房失火

- 2007-4-25晚上9点45分， 位于上海市浦东新区张江高科技园区碧波路690号3号楼第九城市的1号机房发生严重的火灾，并伴有零星的爆炸声；
- 10点15分上海浦东消防2中队赶来进行现场封锁和火灾扑灭工作，1区部分FWQ在此次火灾中已经烧毁，人物资料全部丢失，预计财产损失在3500万以上！


intel
pentium
w/ MMX™ tech

谁更重要？


SiS 5598


Seagate
Medalist 3210
MEDALIST
ULTRA ATA
FRAGILE

磁盘管理

- 各种信息的处理也越来越依赖于各类磁介质载体以电脑、磁盘、声像制品为主的磁介质载体已成为信息化社会中主流的信息载体。对这类新型载体的再认识和管理是做好新形势下保密工作的一项重要工作

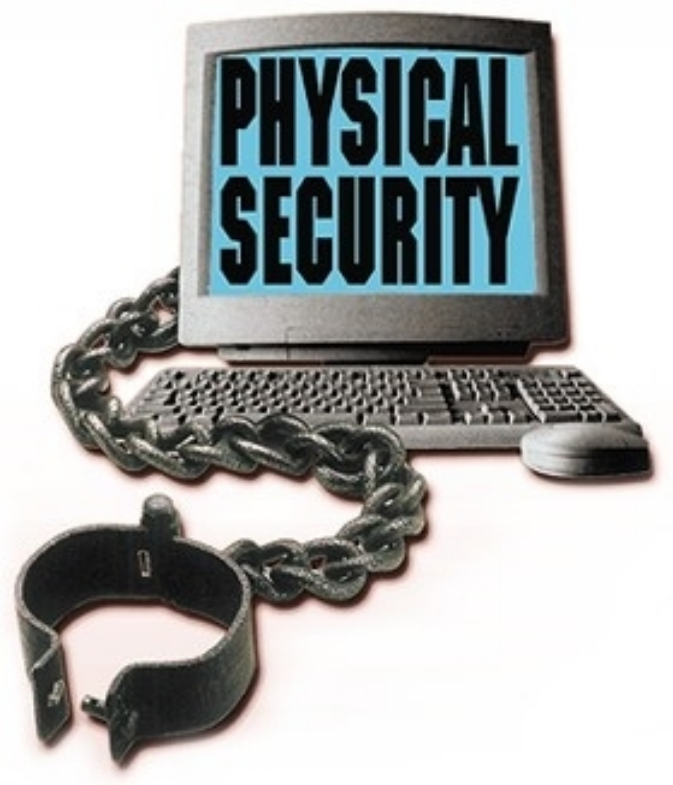
- 目前常用的计算机硬磁盘已达上百G的容量，可记载大量信息，存储密度高而体积很小的磁盘在储备传递的过程中很容易遭到窃取、篡改、伪造、销毁等不法行为的威胁。

- 计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化；

- 磁介质上记载的信息在一定程度上是抹除不净的，使用高灵敏度的磁头和放大器可以将已抹除信息的磁盘上的原有信息提取出来。

- 据一些资料的介绍，即使磁盘已改写了12次，但第一次写入的信息仍有可能复原出来。这使涉密和重要磁介质的管理，废弃磁介质的处理，都成为很重要的问题。

- 国外有的甚至规定记录绝密信息资料的磁盘只准用一次，不用时就必须销毁，不准抹后重录。



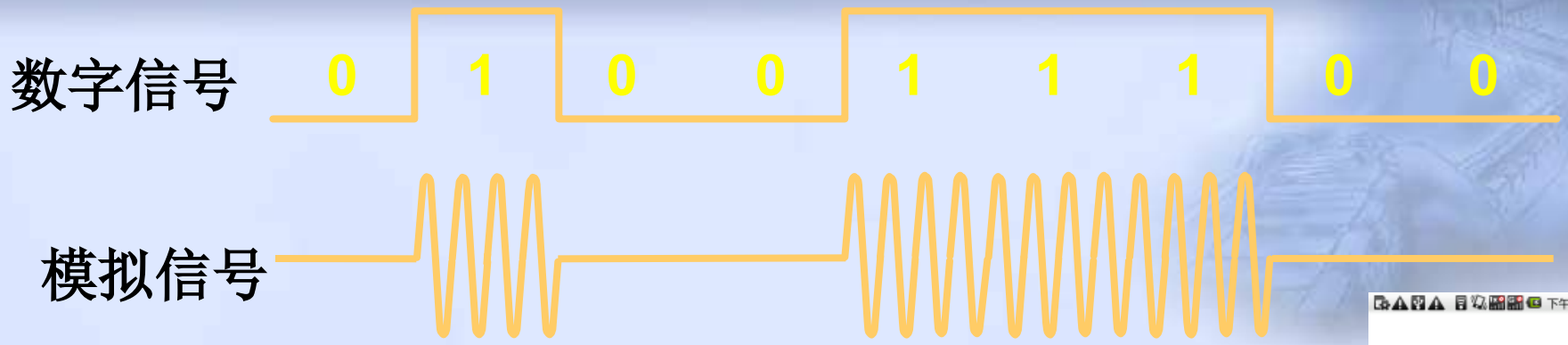
注意你的身边！

注意最细微的地方！

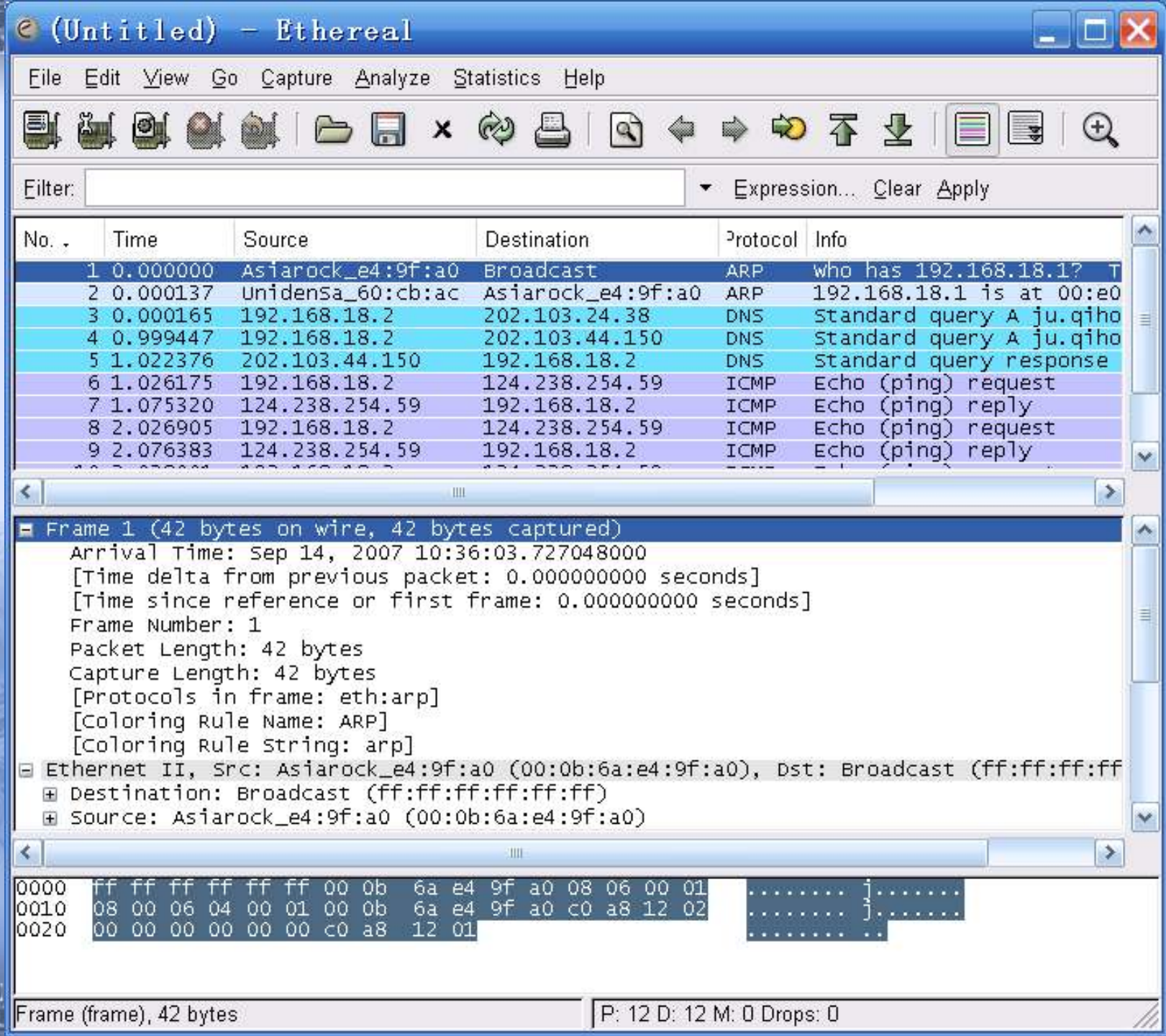
2. 通信安全

- 消息在传输过程中被截获，那么消息中的信息就可能被敌人知道。

- 其解决方法采用通信安全措施。Julius Caesar发明了恺撒密码，这种密码可以传递即使截获也无法读出的消息。



- 信号可以描述为数字，也可以描述为文字、图形、音响等.
- 在电学中具有两种稳定状态以代表0和1的东西很多。如：电压的高和低，开关的开和关，脉冲的有和无，晶体管的导通和截止等等。


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 Asiarock_e4:9f:a0 Broadcast ARP Who has 192.168.18.1? T
2 0.000137 UnidenSa_60:cb:ac Asiarock_e4:9f:a0 ARP 192.168.18.1 is at 00:e0
3 0.000165 192.168.18.2 202.103.24.38 DNS Standard query A ju.qiho
4 0.999447 192.168.18.2 202.103.44.150 DNS Standard query A ju.qiho
5 1.022376 202.103.44.150 192.168.18.2 DNS Standard query response
6 1.026175 192.168.18.2 124.238.254.59 ICMP Echo (ping) request
7 1.075320 124.238.254.59 192.168.18.2 ICMP Echo (ping) reply
8 2.026905 192.168.18.2 124.238.254.59 ICMP Echo (ping) request
9 2.076383 124.238.254.59 192.168.18.2 ICMP Echo (ping) reply
Frame 1 (42 bytes on wire, 42 bytes captured)
Arrival Time: Sep 14, 2007 10:36:03.727048000
[Time delta from previous packet: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Packet Length: 42 bytes
Capture Length: 42 bytes
[Protocols in frame: eth:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: Asiarock_e4:9f:a0 (00:0b:6a:e4:9f:a0), Dst: Broadcast (ff:ff:ff:ff
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Asiarock_e4:9f:a0 (00:0b:6a:e4:9f:a0)
0000 ff ff ff ff ff ff 00 0b 6a e4 9f a0 08 06 00 01 .... j.......
0010 08 00 06 04 00 01 00 0b 6a e4 9f a0 c0 a8 12 02 .... j.......
0020 00 00 00 00 00 00 c0 a8 12 01 ....
Frame (frame), 42 bytes
P: 12 D: 12 M: 0 Drops: 0

3　辐射安全

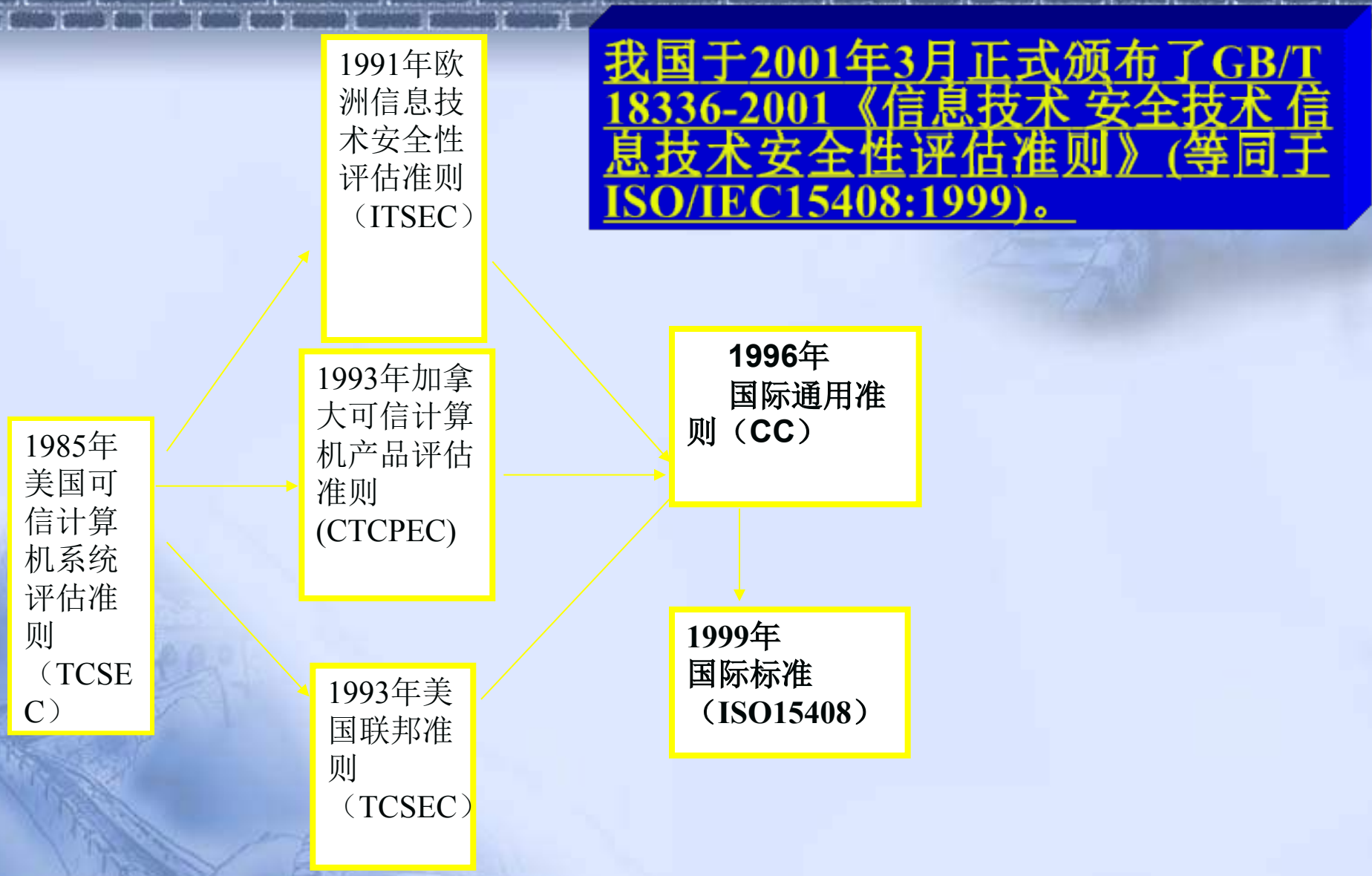
- 人机界面不能使用密码，而只能使用通用的信息表示方法，如显示器显示、打印机打印信息等。

- 信息网络系统的输入和输出端设备总是必有的，事实证明这此设备(系统)电磁泄露造成的信息泄露十分严重。

4　系统安全

- 美国国防部在1985年正式提出了可信计算系统评估标准(TCSEC，也被称为橙皮书)。橙皮书按照下列级别定义了计算机系统。

类别	级别	名称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

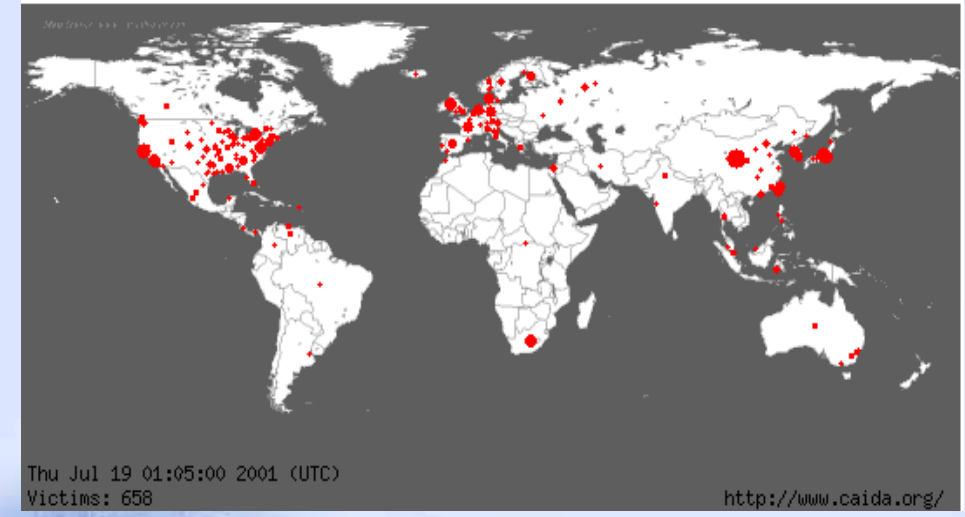

我国于2001年3月正式颁布了GB/T 18336-2001《信息技术 安全技术 信息技术安全性评估准则》(等同于ISO/IEC15408:1999)。
1991年欧洲信息技术安全性评估准则（ITSEC）
1985年美国可信计算机系统评估准则（TCSEC）
1993年加拿大可信计算机产品评估准则(CTCPEC)
1993年美国联邦准则（TCSEC）
1996年国际通用准则（CC）
1999年国际标准（ISO15408）

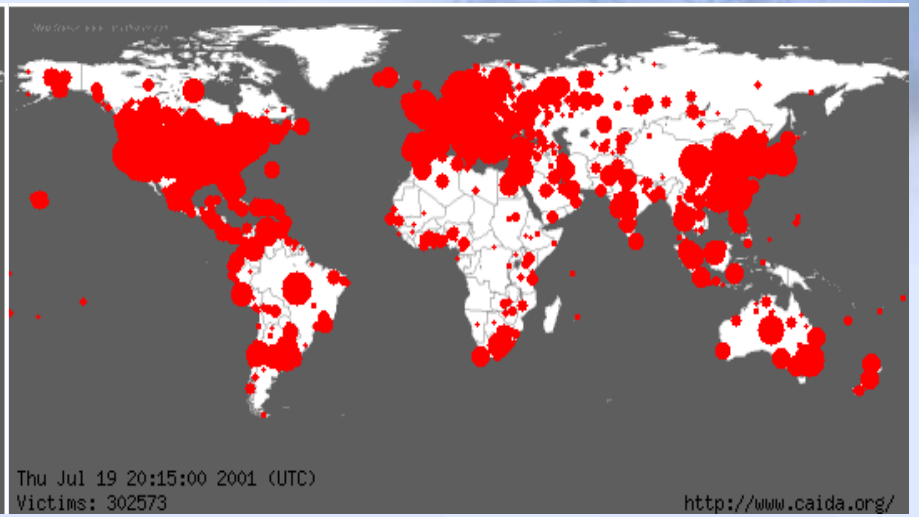
信息安全测评标准发展

5　网络安全

- 计算机相互连接形成网络时，就会出现新的安全问题，而且原有的问题也会以不同的方式出现。
- 比如信息系统联网之后，对信息的威胁就增加了来自网络更大范围的黑客攻击间翻，网络病毒的传播和破坏也不同于单机模式。

“红色代码“病毒





2001年7月19日 1点05分　　2001年7月19日 20点15分

- “红色代码”是一种计算机蠕虫病毒，能够通过网络服务器和互联网进行传播。
- 在短短不到一周的时间内，这个病毒感染了近40万台服务器，据估计多达100万台计算机受到感染。
- 损失估计：全球约26亿美元

Who are you?

网络中，我如何能相信你

6. 人员安全

福建泉州频发技术秘密被盗件 多由职工跳槽引发

http://www.sina.com.cn 2004年10月06日10:45 新华网

新华网福州10月6日电（记者陈文钊）福建泉州市一家知名公司的几名职员离职后带走公司的技术秘密另立门户，给该公司造成极大经济损失。日前，几名职员被该公司以侵犯技术秘密告上法庭。据悉，类似的技术秘密被盗案件屡屡发生，仅今年来泉州市中级法院就受理10多起，占受理案件的三分之一。

据法院人士称，今年受理的80%以上的技术秘密被盗案件，是职工跳槽带走秘密而 引发的。这些案件多数是企业技术部门员工在任职期间泄露或出卖技术秘密另谋高就；部分是在职员工带走商业秘密自立门户。另有一些企业通过高薪聘请等手段，挖走竞争对手的人才，谋取竞争对手的技术秘密或商业秘密。晋江一家通讯设备公司开发

人最常犯的一些错误

- 将口令写在便签上，贴在电脑监视器旁
- 开着电脑离开，就像离开家却忘记关灯那样
- 轻易相信来自陌生人的邮件，好奇打开邮件附件
- 使用容易猜测的口令，或者根本不设口令
- 丢失笔记本电脑
- 不能保守秘密，口无遮拦，泄漏敏感信息
- 随便在服务器上接Modem，或者随意将服务器连入网络
- 事不关己，高高挂起，不报告安全事件
- 在系统更新和安装补丁上总是行动迟缓
- 只关注外来的威胁，忽视企业内部人员的问题

人员安全重要提示

- 人员和组织安全是信息安全管理的难点，因为：
- 人本身就是一个最复杂的因素
- 信息安全的“潜在性”使得安全组织和人才培养不容易获得认可
- 信息安全人才的培养是一个高难的过程
- 信息安全组织需要和企业文化进行磨合
- 避免信息安全组织和业务组织对立

增强全员的安全意识

- 安全意识（Security awareness），泛指组织员工对安全和安全控制重要性的一般性的、集体的意识。促进安全意识，可以减少人员的非授权活动，可以增强保护控制的效率，有助于避免欺诈和对计算资源的浪费
- 员工具有安全意识的标志：
  - 认知可能存在的安全问题及其危害，理解安全所需
  - 明白自身的安全职责，恪守正确的行为方式
- 促进安全意识的方法和途径多种多样：
  - 交互性的、实时的介绍，课程，视频
  - 出版发布物品，新闻传单，张贴物，简报，布告栏，Intranet
  - 奖金和赞誉等激励机制
  - 提醒物，比如登录banner，笔、便签、鼠标垫等随身物品
- 安全意识材料应该直接、简单和清楚，易于理解，要有创新和变化

安全培训和教育

- 培训（Training）不同于意识，其目的是传授安全相关的工作技能，主要对象为信息系统管理和维护人员，通常利用一对一的课堂形式，包括：
  - 为操作者和具体用户提供的安全相关的职务培训
  - 为与敏感安全位置相关的具体的部门或人员提供的技能培训
  - 为IT支持人员和系统管理员提供的技术性安全培训
  - 为安全实践者和信息系统审计师提供的高级信息安全培训
  - 为高级管理者、职能经理和业务单位经理提供的安全培训
- 教育（Education）更为深入，其目的是为安全专业人士提供工作所需的专业技术，一般通过外部程序实现，并且应该成为职业规划的一部分
- 具体的安全软件和硬件的产品培训也很重要