

2002-2003年度北京大学工程硕士研究生课程

网络与信息安全

王 昭

北京大学计算机系信息安全研究室

wangzhao@cs.pku.edu.cn

infosec

概论

- 网络与信息安全的重要性与严峻性 ←
- 信息安全的定义
- 信息安全问题的起源和常见威胁
- 网络信息安全的理论和技术
- 信息安全标准、法规和政策
- 本课程的安排

关于信息化

- 信息革命是人类第三次最伟大的生产力革命
- 四个现代化，那一化也离不开信息化。

——江泽民

日常生活中的信息化

- 电视
- 电话
- 手机
- 计算机
- 信息家电
- 银行业务
- 邮局业务
- 网络: 求职、购物、电子邮件、聊天
-

伴随信息化出现的问题

- 网上信息的可信度
- 病毒
- 攻击
-

信息安全的严峻形势

1. 2000年问题总算平安过渡
2. 黑客攻击搅得全球不安
3. 计算机病毒两年来网上肆虐
4. 白领犯罪造成巨大商业损失
5. 数字化能力的差距造成世界上不平等竞争
6. 信息战阴影威胁数字化和平

信息安全事件统计

CERT有关安全事件的统计

年份	事件报道数目
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	52658

信息安全事件统计

- CERT有关安全事件的统计

年度	报道事件数目	与软件漏洞相关事件数目
2002上半年	43136	2148
2001	52658	2437
2000	21756	1090

信息安全是信息化可持续发展的保障

- 信息是社会发展的**重要战略资源**。
- 网络信息安全已成为急待解决、影响国家大局和长远利益的重大关键问题，信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国在奋力攀登的制高点。
- 网络信息安全问题如果解决不好将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

-----沈昌祥

infosec

信息化与国家安全

—— 政治安全

由于信息网络化的发展，已经形成了一个新的思想文化阵地和思想政治斗争的战场。

- 以美国为首的西方国家，始终认为我们是他们的敌对国家。一直没有放弃对我们的西化、分化、弱化的政策。
- 去年年初，美国国务卿奥尔布莱特在国会讲：“中国为了发展经济，不得不连入互联网。互联网在中国的发展，使得中国的民主，真正的到来了。”
- 香港《广角镜》月刊7月号文章：
中情局对付中国的 < 十条诫令 >

帶有政治性的網上攻擊

过去两年，我们国家的一些政府网站，遭受了四次大的黑客攻击事件。

- 第一次在99年1月份左右，但是美国黑客组织“美国地下军团”联合了波兰的、英国的黑客组织，世界上各个国家的一些黑客组织，有组织地对我们国家的政府网站进行了攻击。
- 第二次，99年7月份，台湾李登辉提出了两国论。
- 第三次是在2000年5月8号，美国轰炸我国驻南联盟大使馆后。
- 第四次在2001年4月到5月，美机撞毁王伟战机侵入我海南机场

信息化与国家安全

—— 经济安全

一个国家信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也越高。

- 我国计算机犯罪的增长速度超过了传统的犯罪
97年20几起，98年142起，99年908起，2000年上半年1420起。
- 利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。

近几年已经破获和掌握100多起。涉及的金额几个亿。

安全事件造成经济损失

- 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。
 - 2月7日10时15分，汹涌而来的垃圾邮件堵死了雅虎网站除电子邮件服务等三个站点之外的所有服务器，雅虎大部分网络服务陷入瘫痪。
 - 第二天，世界最著名的网络拍卖行电子湾（eBay）也因神秘客袭击而瘫痪。
 - 美国有线新闻网CNN的网站随后也因遭神秘客的袭击而瘫痪近两个小时；顶级购物网站亚马逊也被迫关闭一个多小时。
 - 在此之后又有一些著名网站被袭击：ZDnet，Etrade，Excite，Datek.....到2月17日为止，黑客攻击个案已增至17宗，而且可能有更多网站受袭而未被察觉
 - 引起美国道穷斯股票指数下降了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。

安全事件造成的经济损失

- 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。
- 据美国加利福尼亚州的名为“电脑经济”的研究机构发布的初步统计数据，“爱虫”大爆发两天之后，全球约有4500万台电脑被感染，造成的损失已经达到26亿美元。今后几天里，“爱虫”病毒所造成的损失还将以每天10亿美元到15亿美元的速度增加。
- 1995年计算机安全杂志在全球抽样调查了300家典型的公司，69%的公司报告上年度遇到过计算机网络安全问题，59%的公司报告，上述安全问题造成的损超过1万美元。

信息化与国家安全

——社会稳定

互连网上散布一些虚假信息、有害信息对社会管理秩序造成的危害，要比现实社会中一个造谣要大的多。

- 99年4月，河南商都热线一个BBS，一张说交通银行郑州支行行长协巨款外逃的帖子，造成了社会的动荡，三天十万人上街排队，挤提了十个亿。
- 网上治安问题，民事问题，进行人身侮辱。

针对社会公共信息基础设施的攻击严重扰乱了社会管理秩序

- 2001年2月8日正是春节，新浪网遭受攻击，电子邮件服务器瘫痪了18个小时。造成了几百万的用户无法正常的联络。
- 广东163.net免费邮箱，黑客进去以后进行域名修改，打开邮箱就向美国去了，造成400多万用户不能使用。

网上不良信息腐蚀人们灵魂

- 色情资讯业日益猖獗
- 网上赌博盛行

信息化与国家安全

—— 信息战

信息战指双方为争夺对于信息的获取权、控制权和使用权而展开的斗争。是以计算机网络为战场，计算机技术为核心、为武器，是一场智力的较量，以攻击敌方的信息系统为主要手段，破坏敌方核心的信息系统，是现代战争的“第一个打击目标”。

通常来说它利用的手段有计算机病毒、逻辑炸弹、后门（Back Door）、黑客、电磁炸弹、纳米机器人和芯片细菌等。

信息战重要实例

- 1990年海湾战争，被称为“世界上首次全面信息战”，充分显示了现代高技术条件下“制信息权”的关键作用。美军通过向带病毒芯片的打印机设备发送指令，致使伊拉克军队系统瘫痪，轻易地摧毁了伊军的防空系统。多国部队运用精湛的信息技术,仅以伤亡百余人的代价取得了歼敌十多万成果。
- 在科索沃战争中，美国的电子专家成功侵入了南联盟防空体系的计算机系统。当南联盟军官在计算机屏幕上看到敌机目标的时候，天空上其实什么也没有。通过这种方法，美军成功迷惑了南联盟，使南联盟浪费了大量的人力物力资源。
- 同样的方法还应用到南联盟首领米洛舍维奇的头上，美军雇佣黑客闯入瑞士银行系统，调查米氏的存款情况并加以删除，从心理上给予米氏以沉重的打击。

信息战的特点

战略信息战是一场没有前线的战斗。

兰德公司《战略信息战》的报告综合了信息战的特点：


- 信息攻击花费低
- 传统边界模糊
- 管理观念的困难
- 战略情报的不可靠性
- 战术警报/攻击估计极端困难
- 建立和维持合作关系变得更为复杂
- 无安全的战略后方

兰德公司的对华建议策略

- 兰德公司于1999年6月份向美国政府提出的建议报告：
美国的对华战略应该分三步走：
 - 第一步是西化、分化中国，使中国的意识形态西方化，从而失去与美国对抗的可能性；
 - 第二步是在第一步失效或成效不大时，对中国进行全面的遏制，并形成对中国战略上的合围；
 - 第三步就是在前两招都不能得逞时，不惜与中国一战，当然作战的最好形式不是美国的直接参战，而是支持中国内部谋求独立的地区或与中国有重大利益冲突的周边国家。

信息时代的国际形势

- 在信息时代，世界的格局是：一个信息霸权国家，十几个信息主权国家，多数信息殖民地国家。
- 在这样的一个格局中，只有一个定位：反对信息霸权，保卫信息主权。

- 信息安全的重要性
- 信息安全的定义 
- 信息安全问题的起源和常见威胁
- 网络信息安全的理论和技术
- 信息安全标准、法规和政策
- 本课程的安排

信息安全的含义

通信保密（COMSEC）：60-70年代

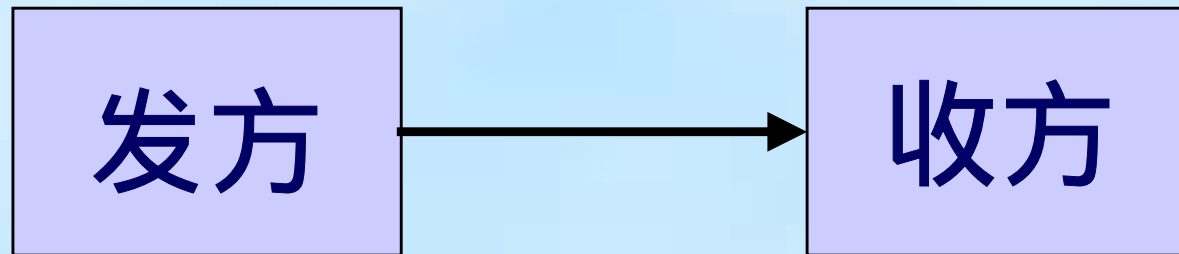
信息保密

信息安全（INFOSEC）：80-90年代

机密性、完整性、可用性、可控性、不可否认性

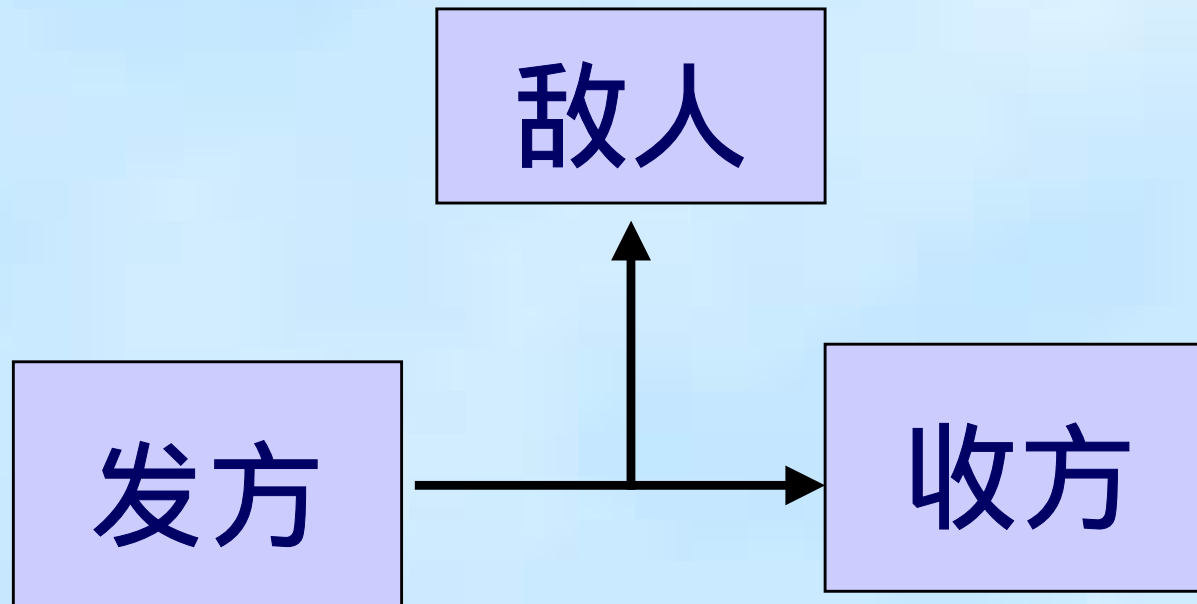
信息保障（IA）：90年代-

- 基本的通讯模型



信源编码
信道编码
信道传输
通信协议

- 通信的保密模型
通信安全-60年代 (COMSEC)



信源编码
信道编码
信道传输
通信协议
密码

信息安全的含义 (80-90年代)

- 信息安全的三个基本方面
 - 保密性 Confidentiality
即保证信息为授权者享用而不泄漏给未经授权者。
 - 完整性 Integrity
即保证信息从真实的发信者传送到真实的收信者手中，传送过程中没有被他人添加、删除、替换。
 - 可用性 Availability
即保证信息和信息系统随时为授权者提供服务，而不要出现非授权者滥用却对授权者拒绝服务的情况。

- 信息的可控性：

即出于国家和机构的利益和社会管理的需要，保证管理者能够对信息实施必要的控制管理，以对抗社会犯罪和外敌侵犯。

- 信息的不可否认性：

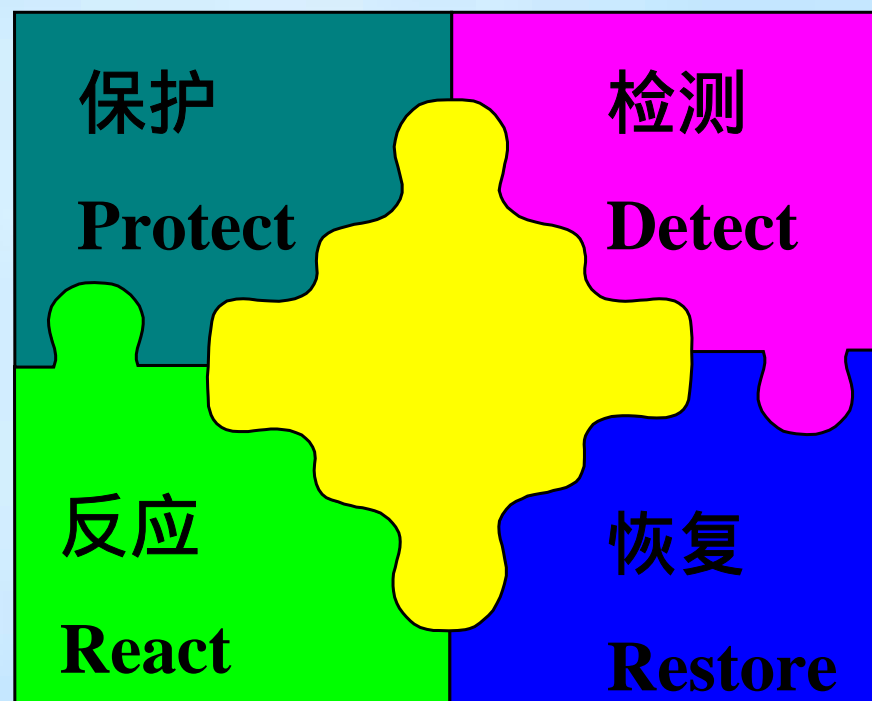
即信息的行为人要为自己的信息行为负责，提供保证社会依法管理需要的公证、仲裁信息证据。

信息保障

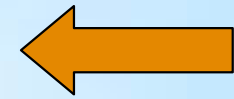
- 美国人提出的概念:

Information Assurance

- 保护 (Protect)
- 检测 (Detect)
- 反应 (React)
- 恢复 (Restore)



- 信息安全的重要性
- 信息安全的定义
- 信息安全问题的起源和常见威胁
- 网络信息安全的理论和技术
- 信息安全标准、法规和政策
- 本课程的安排



网络安全脆弱性的原因

- 内因

- 人们的认识能力和实践能力的局限性

- 系统规模

- Windows 3.1 ——300万行代码

- Windows 2000 ——5000万行代码

- **Internet**从建立开始就缺乏安全的总体构想和设计
- **TCP/IP**协议是在可信环境下，为网络互联专门设计的，缺乏安全措施的考虑

CERT/CC关于系统脆弱性的报告

年份	报告的脆弱性数目
1995	171
1996	345
1997	311
1998	262
1999	419
2000	774
总数	2280

外因

国家安全威胁	信息战士	减小美国决策空间、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

Insider（内部人员）威胁必须引起高度重视

国内外从事信息安全的专业人士，通过调查逐步认识到，媒体炒得火热的外部入侵事件，充其量占到所有安全事件的20%-30%，而70%-80%的安全事件来自于内部。

通信系统典型攻击

1)消息篡改

当所传送的内容被改变而未发觉，并导致一种非授权后果时出现消息篡改。

2)旁路

攻击者发掘系统的缺陷或安全脆弱性。

3)服务拒绝

当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行它们的正当功能的时候便发生服务拒绝。

4) 窃听

信息从被监视的通信过程中泄露出去。

5)完整性破坏

数据的一致性通过对数据进行未授权的创建、修改或破坏而受到损坏。

6)冒充

冒充就是一个实体（人或系统）假装成另一个不同的实体。冒充经常和某些别的攻击形式一起使用，特别是消息的重演与篡改。

7)重演

当一个消息或部分消息为了产生非授权效果而被重复时就出现重演。

8)抵赖

在一次通信中涉及到的那些实体之一不承认参加了该通信的全部或一部分。

9) 业务流分析


通过对通信业务流模式进行观察而造成信息被泄露给未授权的实体。

10) 陷阱门

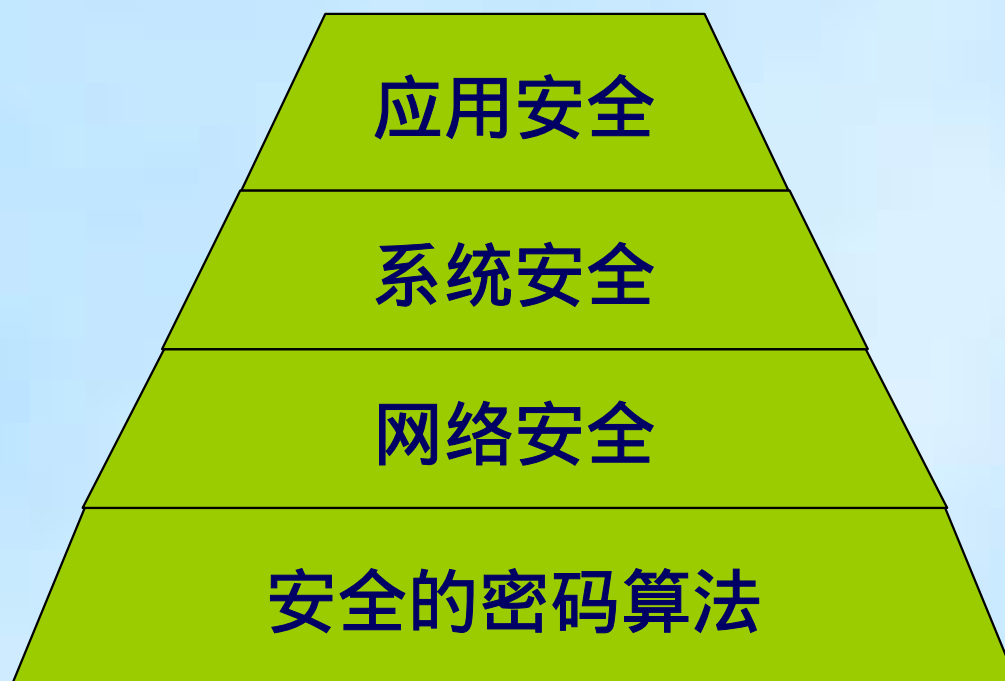
当系统的实体受到改变致使一个攻击者能对命令，或对预定的事件或事件序列产生非授权的影响时，其结果就称为陷阱门。

11) 特洛伊木马

对系统而言的特洛伊木马，是指它不但具有自己的授权功能，而且还具有非授权功能。

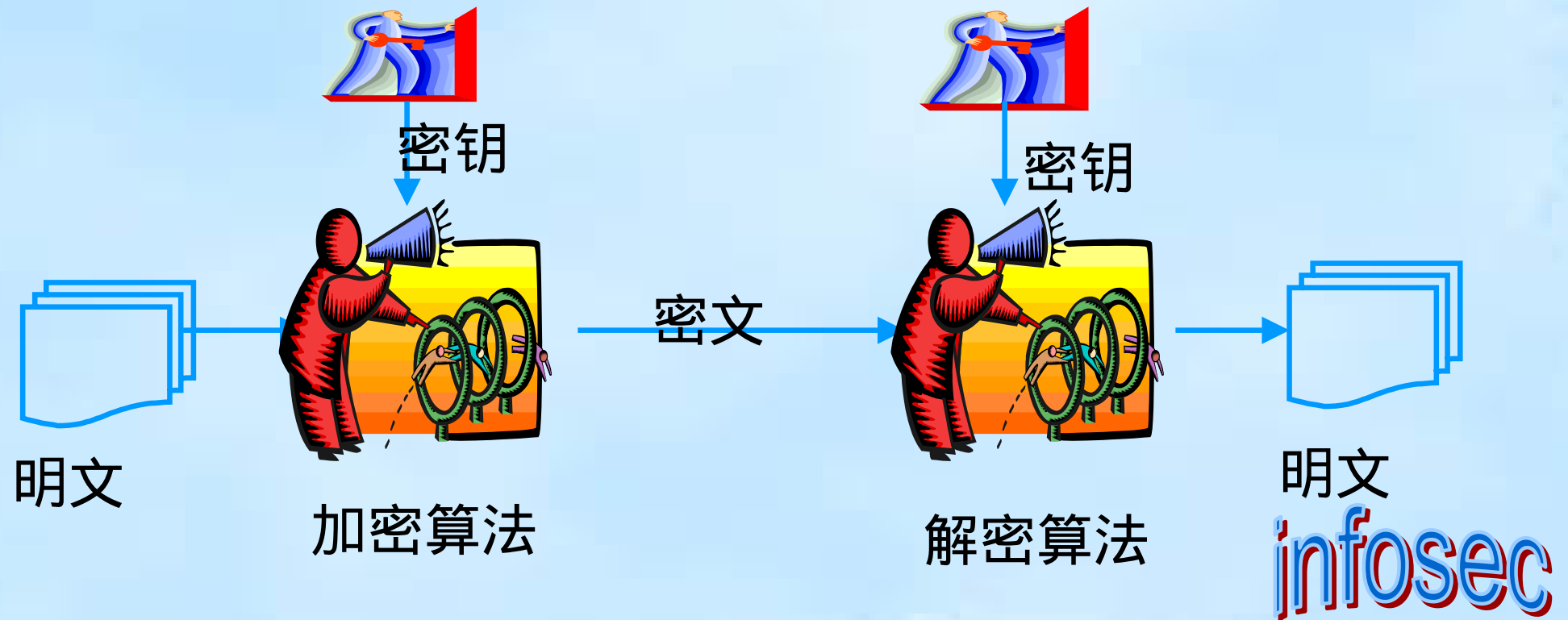
- 信息安全的重要性
- 信息安全的定义
- 信息安全问题的起源和典型攻击
- 网络信息安全的理论和技术 
- 信息安全标准、法规和政策
- 本课程的安排

安全层次



密码算法

- 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。



算法分类

- 经典密码 classical
 - 代替密码：
 - 简单代替 多名或同音代替
 - 多表代替 多字母或多码代替
 - 换位密码：
- 对称加密算法： Symmetric
 - 分组密码： DES AES
 - 流密码：
- 非对称（公钥）算法 Public-key
 - RSA、背包密码、椭圆曲线ECC

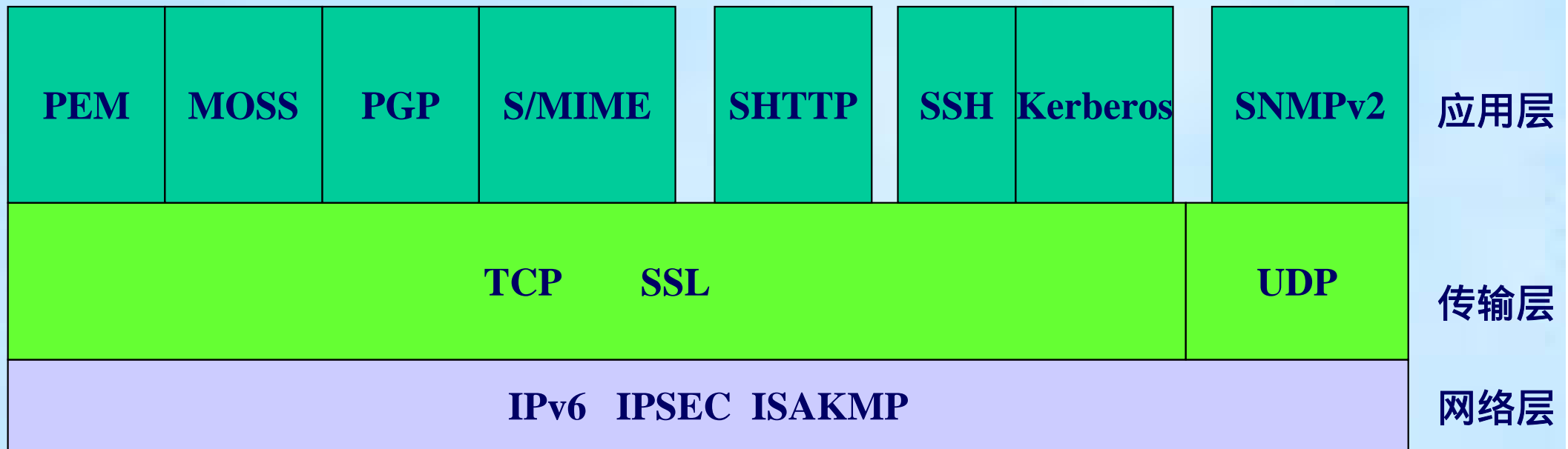
ISO7498-2 , 信息安全体系结构

- 1989.2.15颁布 , 确立了基于OSI参考模型的七层协议之上的信息安全体系结构
 - 五大类安全服务(鉴别、访问控制、保密性、完整性、抗否认)
 - 八类安全机制(加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公证)
 - OSI安全管理

ISO7498-2到TCP/IP的映射

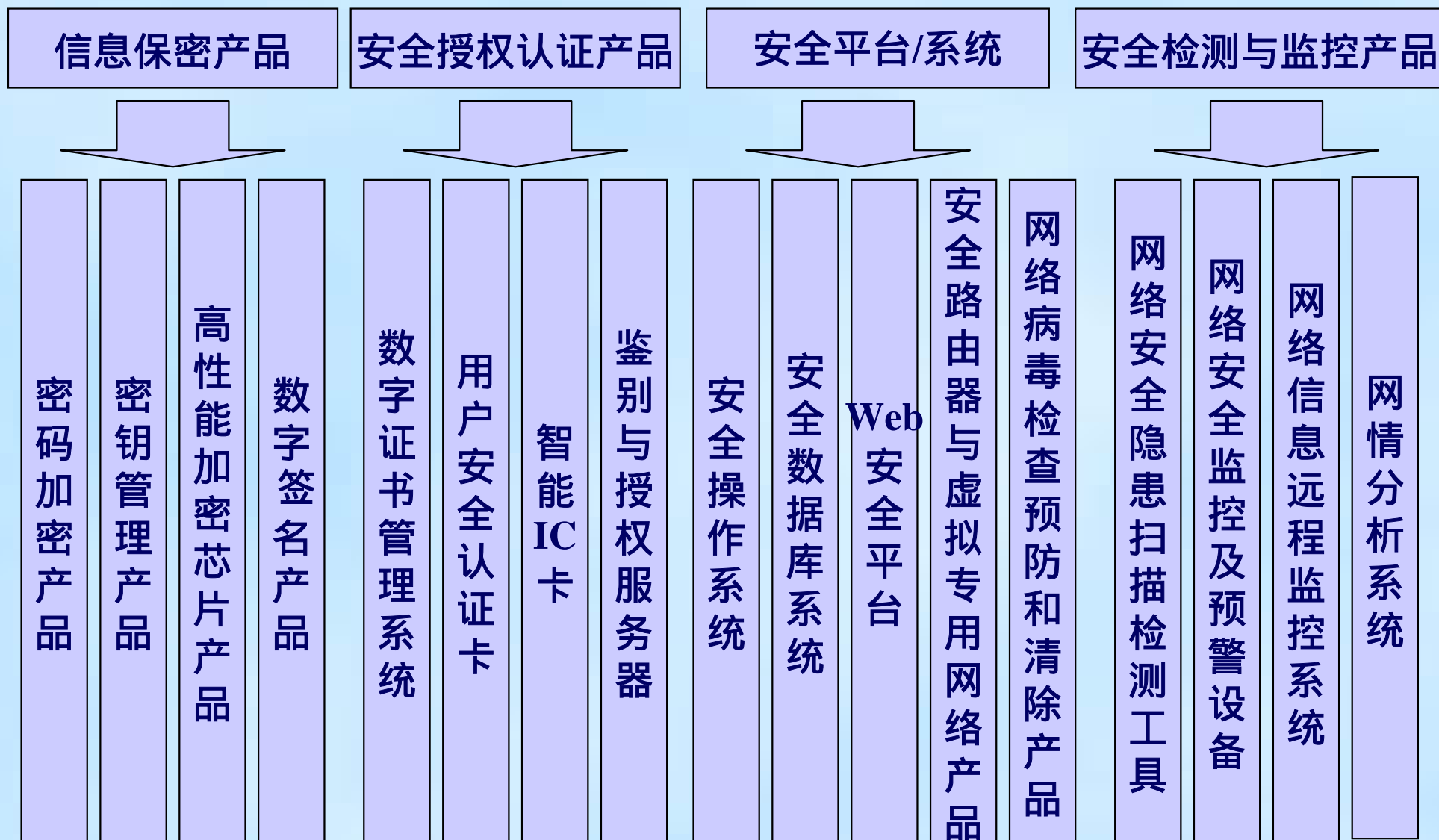
安全服务	TCP/IP 协议层			
	网络接口	互联网层	传输层	应用层
对等实体鉴别	-	Y	Y	Y
数据源鉴别	-	Y	Y	Y
访问控制服务	-	Y	Y	Y
连接保密性	Y	Y	Y	Y
无连接保密性	Y	Y	Y	Y
选择域保密性	-	-	-	Y
流量保密性	Y	Y	-	Y
有恢复功能的连接完整性	-	-	Y	Y
无恢复功能的连接完整性	-	Y	Y	Y
选择域连接完整性	-	-	-	Y
无连接完整性	-	Y	Y	Y
选择域非连接完整性	-	-	-	Y
源发方不可否认	-	-	-	Y
接收方不可否认	-	-	-	Y

基于TCP/IP协议的网络安全体系结构基础框架

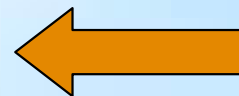


安全产品类型

- 根据我国目前信息网络系统安全的薄弱环节，近几年应重点发展安全保护、安全检测与监控类产品，相应发展应急反应和灾难恢复类产品。
 - 信息保密产品
 - 用户认证授权产品
 - 安全平台/系统
 - 网络安全检测监控设备



- 信息安全的重要性
- 信息安全的定义
- 信息安全问题的起源和典型攻击
- 网络信息安全的理论和技术
- 信息安全标准、法规和政策
- 本课程的安排



国际信息安全政策法规

美国立法情况

- 早在1987年，美国就再次修订了《计算机犯罪法》，这部法律在80年代末至90年代初一直被作为美国各州制定其地方法规的依据。
- 美国现以确立的有关信息安全的法规有：
信息自由法、个人隐私法、反腐败行经法、伪造访问设备和计算机欺骗滥用法、电子通信隐私法、计算机欺骗滥用法、计算机安全法、正当通信法（一度被确立，但后又被推翻）和电讯法。

- 1998年5月，美国发布第63号总统令，要求行政部门评估国家关键基础设施的计算机脆弱性，并要求联邦政府制定保卫国家免受计算机破坏的详细计划。
- 2000年1月发布了《保卫美国计算机空间——信息系统保护国家计划1.0》，这是一个规划美国计算机安全持续发展和更新的综合方案。

俄罗斯立法情况

- 1995年颁布了《联邦信息、信息化和信息保护法》，法规明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。
- 2000年，普京总统批准了《国家信息安全学说》，它是一部纲领性、指导性、顶层性、战略性文件，并不是学说。它明确了俄罗斯联邦信息安全建设的目的、任务、原则和主要内容，第一次明确指出了俄罗斯在信息安全领域的利益、受到的威胁，以及为保障信息安全应采取的首要措施。

- 欧洲经济共同体是一个在欧洲范围内具有较强影响力的政府间组织。其成员国从70年代末到80年代初，先后制定并颁布了各自有关数据安全的法律。
- 德国政府于1996年夏出台了《信息和通信服务规范法》（即多媒体法），为电子信息和通信服务的各种利用可能性规定了统一的基本法律框架。该国政府还通过了电信服务数据保护法，并根据需要对刑法法典、治安法、传播危害青少年文字法、著作权法和报价法作了必要的修改和补充。
- 新加坡在1996年宣布对互联网络实行管制，宣布实施分类许可证制度。它是一种自动取得许可证的制度，目的是鼓励正当使用互联网络，促进其健康发展。

- 美国是最早允许在国内社会使用密码的国家，美国国内，政府、军界、企业和个人为了各自的利益，围绕信息加密政策的争论繁多，主要是密码的使用范围和允许出口的长度。此外，多国出口控制协调委员会COCOM、欧盟和国际商务委员会等组织以及英国、法国、德国、意大利、俄罗斯、波兰、澳大利亚、香港等许多国家和地区也分别制定了自己的信息加密政策。
- 对于数字签名技术，有关国际组织、各国政府和企业为了各自的利益，很难达成一致观点。1995年，美国犹他州通过了美国历史上（也是世界历史上）第一部数字签名法。在犹他州的带动下，美国的其他一些州也确立了自己的数字签名法，但是美国联邦政府还迟迟没有立法。德国有幸成为第一个以国家名义制定数字签名法的国家。

组织机构

国际上信息安全方面的协调机构主要有计算机应急响应小组（CERT/CC）、信息安全问题小组论坛（FIRST）。

- 计算机应急响应小组是一个信息安全专家技术中心，是设在Carnegie Mellon大学软件工程研究所的联邦资助的研究开发中心，成立于1988年。该组织研究Internet的脆弱性、处理计算机安全事件、发布安全警告、研究网络系统的长期变化以及提供安全培训帮助你提高站点的安全性。CERT/CC成立后，很多政府、商业和学术机构都组建了信息安全问题小组，但CERT/CC始终是这一方面规模最大、最著名和最权威的组织。
- 信息安全问题小组论坛（FIRST）成立于1990年，当时只有11个成员，截止2001年年中，它的成员已超过90个。FIRST的目标是为有效解决安全事件加强各小组间的合作，作为小组之间的信息中介，促进安全技术的共享和研究活动的开展。

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。

我国的国家信息安全组织管理体系

- **国务院信息化领导小组**对Internet安全中的重大问题进行管理协调，国务院信息化领导小组办公室作为Internet安全工作的办事机构，负责组织、协调和制定有关Internet安全的政策、法规和标准，并检查监督其执行情况。
- 政府有关信息安全的其它管理和执法部门：**信息产业部、国家安全部、公安部、机要局、国家保密局、国家密码管理委员会和国务院新闻办公室等**

我国信息安全管理 的方针

基本方针“兴利除弊，集中监控，分级管理，保障国家安全”。

对于密码的管理政策实行“统一领导、集中管理、定点研制、专控经营、满足使用”的发展和管理方针。

我国立法

我国政府现有的信息安全法规政策可以分为两个层次。一是法律层次，从国家宪法和其它部门法的高度对个人、法人和其它组织的涉及国家安全的信息活动的权利和义务进行规范，例如1997年新《刑法》首次界定了计算机犯罪。其中，这一层次上的法律主要有

- 宪法、
- 刑法、
- 国家安全法
- 国家保密法。

二是行政法规和规章层次，直接约束计算机安全和Internet安全，对信息内容、信息安全技术和信息安全产品的授权审批进行规定。这一层次主要包括：

- 《中华人民共和国计算机信息系统安全保护条例》（简称《安保条例》）、
- 《中华人民共和国计算机信息网络国际互联网管理暂行规定》（简称《联网规定》）、
- 《中华人民共和国计算机信息网络国际互联网安全保护管理办法》、
- 《电子出版物管理暂行规定》、
- 《中国互联网络域名注册暂行管理办法》、
- 《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》等条例和法规。

著名国际标准化组织

- 国际标准化组织（ISO）和国际电工委员会（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。ISO和IEC的各技术委员会在共同感兴趣的领域内进行合作。与ISO和IEC有联系的其他官方和非官方国际组织也可以参与国际标准的制定工作。
- 对于信息技术，ISO和IEC建立了一个联合技术委员会，即ISO/IEC JTC1。由联合技术委员会提出的国际标准草案分发给国家成员体进行表决。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。
- 国际标准开放系统互联(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。等同文本为ITU-T建议X.200。

- 国际电报和电话咨询委员会(CCITT)

国际电报和电话咨询委员会是一个联合国条约组织，属于国际电信联盟，由主要成员国的邮政、电报和电话当局组成，主要从事涉及通信领域的接口和通信协议的制定，与ISO密切合作进行国际通信的标准化工作，在数据通信范围内的工作体现于V系列和X系列建议书。

国际信息处理联合会第十一技术委员会（IFIP TC11）

- 该组织是国际上有重要影响的有关信息系统安全的国际组织，公安部代表我国参加该组织的活动，该组织每年举行一次计算机安全的国际研讨会。该组织机构包括安全管理工作组、办公自动化安全工作组、数据库安全工作组、密码工作组、系统完整性与控制工作组、拟构成计算机事务处理工作组、计算机安全法律工作组和计算机安全教育工作组。

电气和电子工程师学会（IEEE）

- 电气和电子工程师学会是一个由电气和电子工程师组成的世界上最大的专业性学会，划分成许多部门。1980年2月，IEEE计算机学会建立了一个委员会负责制定有关网络的协议标准(802.1~9)，包括高层接口、逻辑链路控制、CSMA/CD网、令牌总线网、令牌环网、城域网、宽带技术咨询组、光纤技术咨询组、数据和话音综合网络等标准。

- 欧洲计算机制造商协会（ECMA）
- 欧洲计算机制造商协会是包括美国在欧洲供应计算机的厂商在内组成的组织，致力于适用于计算机技术的各种标准的制定和颁布，在ISO和CCITT中是一个没有表决权的成员。

Internet 体系结构委员会 (IAB)

- Internet 体系结构委员下设两个重要部门：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。

美国国家标准局（NBS）与美国商业部国家标准技术研究所（NIST）

- 美国国家标准局属于美国商业部的一个机构，现在的工作由NIST进行。发布销售给美国联邦政府的设备的信息处理标准。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。他制定的信息安全规范和标准很多，主要涉及访问控制和认证技术、评价和保障、密码、电子商务、一般计算机安全、网络安全、风险管理、电讯和联邦信息处理标准等。
- 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。

美国国家标准协会（ANSI）

- 美国国家标准协会是由制定标准和使用标准的组织联合组成的非盈利的非政府的民办机构，由全美1000多家制造商、专业性协会、贸易协会、政府和管理团体、公司和用户协会组成，是美国自发的制定与计算机工业有关的各种标准的统筹交流组织。

美国电子工业协会（EIA）

- 美国电子工业协会是美国电子公司贸易协会，属于ANSI的成员。它制定了涉及电气和电子领域的400多个标准，主要工作是建立了数据终端设备和数据通信设备间的接口标准（如RS232C等）。

美国国防部（DoD）及国家计算机安全中心（NCSC）

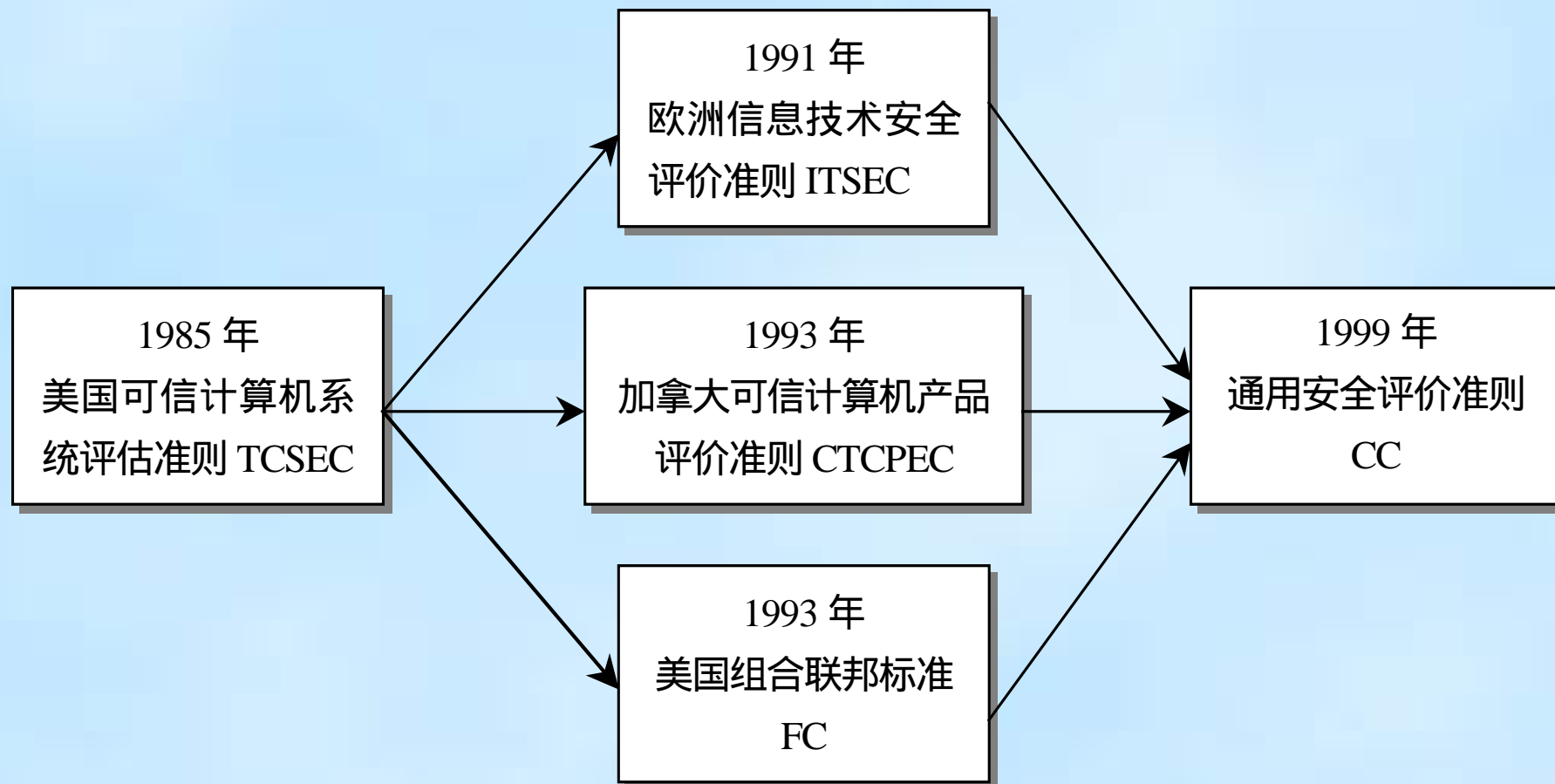
- 美国国防部早在80年代就针对计算机安全保密开展了一系列有影响的工作，后来成立的NCSC接续进行有关的工作。1983年他们公布了《可信计算机信息系统评价准则》TCSEC，以后NCSC又出版了一系列有关可信计算机数据库、可信计算机网络的指南。

其它协议

- 除了上述标准化组织，美国的一些公司也纷纷研究和提出有关规范建议，并根据建议发展产品，试图将建议变为实际的工业标准，其中一些建议或标准归纳如下表。

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

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。TNI是把TCSEC的思想用到网络上，缺乏成功实践的支持。

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）。

- 1993年，加拿大发布了“加拿大可信计算机产品评价准则”（CTCPEC）。
- 同年，美国对可信计算机系统评估准则（TCSEC）作了补充和修改，国家标准局和国家安全局合作制定了“组合的联邦标准”（简称FC），对保护框架和安全目标作了定义，明确了由用户提供其系统安全保护需求的详细框架，产品厂商定义产品的安全功能、安全目标等，但其有很多缺陷，只是一个过度准则。

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。

CC标准的读者对象

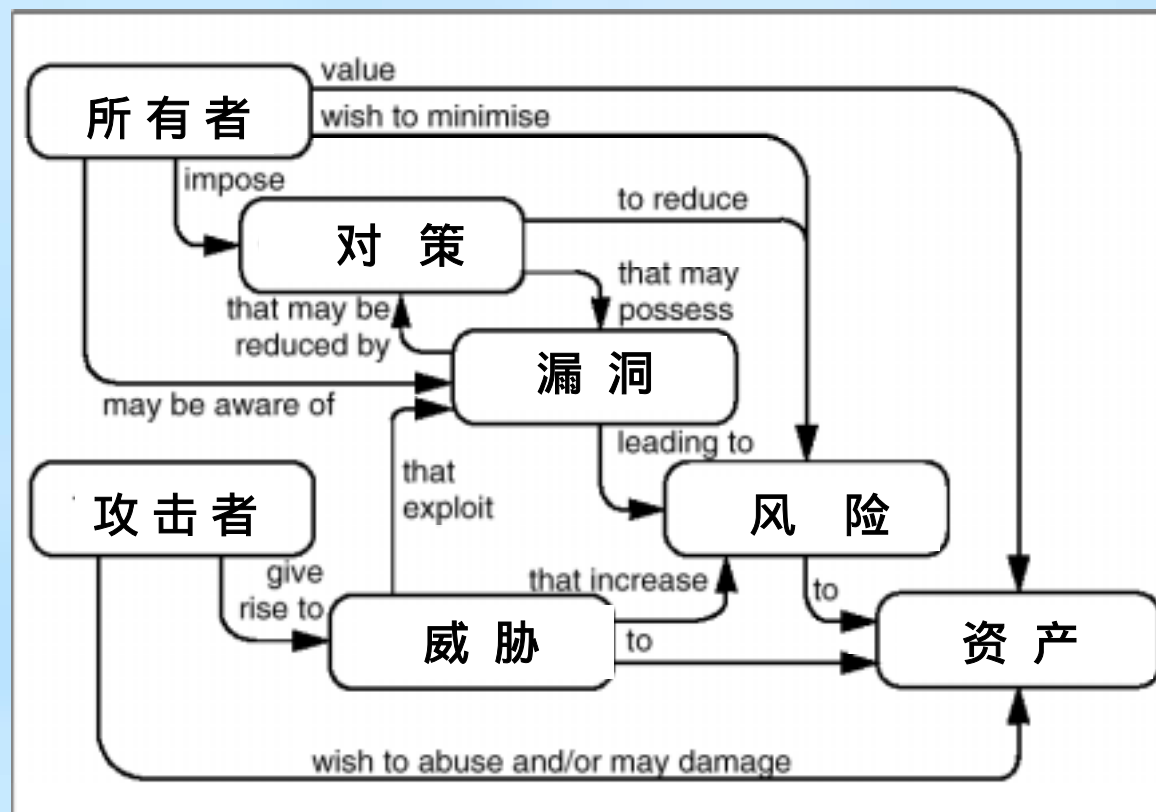
- 用户：通过风险和策略的分析，比较评价的不同产品和系统，选择适合自己使用的产品和系统。
- 开发者：支持开发者认识满足自己产品和系统的安全要求，制定保护轮廓（PP），确定安全目标（ST），支持开发者开发自己的评价目标（TOE），在评价方法学帮助开发者，以共识的评价结果评价自己开发的产品和系统。
- 评价者：正式审查评价目标时为评价者提供一个评价准则，用于评价评价目标（TOE）和安全要求的一致性
- 其它：对于对IT安全有兴趣和有责任的人起到一个导向和参考材料的作用，机构中的系统监管和安全官员确定安全策略和要求

CC评价准则的结构

- 第一部分：介绍和总体模型
 - 对CC评价准则的介绍。定义IT安全评价和描述模型的一般概念和原则，提出选择和定义说明产品和系统IT安全客体的明确的组织的安全要求。
- 第二部分：安全功能要求
 - 用标准化的方法对评价目标（TOE）建立一个明确的安全要求的部件功能集合。功能集合分类为部件（components）、族（families）和类（classes）
- 第三部分：安全保证要求
 - 用标准化的方法对评价目标（TOE）建立一个明确的安全要求的保证部件的集合。对保护方案（PP）和安全目标（ST）进行定义，并且对安全评价目标（TOE）提出安全评价保证级别（EAL）

不同评测标准的评估级别的粗略对应关系

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



CC定义的安全概念和关系模型

我国标准制定状况

- 我国是国际标准化组织的成员国，我国的信息安全标准化工作在各方面的努力下，正在积极开展之中。从80年代中期开始，自主制定和视同采用了一批相应的信息安全标准。到2000年底，已颁布的信息技术安全标准有22项，国家军用安全标准6项，涉及信息技术设备的安全、信息处理系统开放系统互联安全体系结构、数据加密、数字签名、实体鉴别、抗抵赖和防火墙安全技术等。今年，我国颁布的国家标准GB/T 18336等同采用国际标准ISO/IEC 15408。这些标准的颁布将积极推动我国的信息化建设与发展。
- 此外，在一些对信息安全要求高的行业和对信息安全管理负有责任的部门，也制定一些信息安全的行业标准和部门标准，例如金融、公安等行业和部门

国家法律

中华人民共和国主席令第6号
中华人民共和国保守国家秘密法

行政法规

- 中华人民共和国国务院令147号
中华人民共和国计算机信息系统安全保护条例
- 中华人民共和国国务院令第195号
中华人民共和国计算机信息网络国际联网管理暂行规定
- 中华人民共和国计算机信息网络
国际联网管理暂行规定实施办法
- 中华人民共和国国务院令第273号
商用密码管理条例
- 中华人民共和国国务院令第291号
中华人民共和国电信条例

安全标准

- 计算机病毒防治产品评级准则(2000-5-17发布)
- 计算机信息系统安全保护等级划分准则(1999-9-13发布)
- 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构
- 计算机信息系统安全专用产品分类原则
- 信息技术设备的无线电干扰极限值和测量方法
- 计算机机房用活动地板技术条件
- DOS操作系统环境中计算机病毒防治产品测试方法
- 基于DOS的信息安全产品评级准则
- 电子计算机机房设计规范

GB17859-1999

计算机信息系统安全保护等级划分准则

1999年9月我国制定并颁布了《计算机信息系统安全保护等级划分准则》，该准则于2001年1月1日开始实施。

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

安全要素


安全策略（ Policy ）：自主访问控制、客体重用、标记及强制访问控制、

责任（ Accountability ）：身份鉴别、可信路径和审计

保证（ Assurance ）数据完整性、隐蔽通道分析及可信恢复

安全保护等级与安全要素的对应关系

安全要素	用户自主 保护级	系统审计 保护级	安全标记 保护级	结构化保 护级	访问验证 保护级
自主访问控制	√	√	√	√	√
身份鉴别	√	√	√	√	√
数据完整性	√	√	√	√	√
审计		√	√	√	√
客体重用		√	√	√	√
标记			√	√	√
强制访问控制			√	√	√
隐蔽信道分析				√	√
可信路径				√	√
可信恢复					√

- 信息安全的重要性
- 信息安全的定义
- 信息安全问题的起源和典型攻击
- 网络信息安全的理论和技术
- 信息安全标准、法规和政策
- 本课程的安排 

先修要求

- 程序设计
- 计算机网络
- 操作系统

课程目标

- 让学生了解和掌握网络与信息安全的基本原理、技术、及最新研究成果
- 具有网络与信息安全的理论基础和基本实践能力

课程体系

- 密码学基础：经典密码、对称密码、非对称密码、密钥管理技术
- 认证理论与技术：散列算法（Hash）、数字签名、身份鉴别和访问控制
- 网络安全：电子邮件的安全、IP的安全、Web的安全、扫描、攻击与入侵检测
- 系统安全：防火墙技术、操作系统的安全、病毒
- 专题讲座：

学习用书

- 教材： William Stallings, Cryptography and network security: principles and practice, Second Edition
or
- 杨明，胥光辉等译《密码编码学与网络安全：原理与实践》（第二版），电子工业出版社，2001，4

成绩考核

考试分 平时作业(15%)+
小论文(20%)+
期末笔试(65%)

Reference

- 1) 沈昌详,信息安全工程技术, 2001年全国第五次高级计算机人才培训班讲义
- 2) 赵战生,信息安全保障的政策、法规和标准, 2001年全国第五次高级计算机人才培训班讲义
- 3) 赵战生 冯登国等,《信息安全技术浅谈》, 科学出版社, 1999
- 4) [TCSEC1985] Department of Defense of USA.
Trusted Computer System Evaluation Criteria.
(Orange book),1985

Reference

- 4) [ISO/IEC 15408-1:1998] ISO/IEC , Common Criteria for Information Technology Security Evaluation ,Part 1: Introduction and General model, Version 2.0 ,1998,5
- 5) [ISO/IEC 15408-2:1999] ISO/IEC , Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.0,1998,5
- 6) [ISO/IEC 15408-3:1999] ISO/IEC , Common Criteria for Information Technology Security Evaluation ,Part 3:Security Assurance Requirements, Version 2.0, 1998,5

End
Thank You!!