信息安全导论

第一章 信息化与信息安全

黄 玮

关于课程你需要了解…

教学团队

- 主讲教师

  —黄玮

  —信息安全博士，讲师

课程概况

- 上课地点
  - —讲授：48教 A503
- 上课时间
  - —讲授 第2周~第16周： 每周五上午 8:00~9:50
- 答疑地点
  - —教室 / 课后
- 答疑时间
  - —新浪微博 @中传黄玮 / 随时

课程概况

- 先修课程

  —无

- 参考教材

  —沈昌祥，信息安全导论，电子工业出版社，2009

- 硬件和软件环境

  —PC

在线资源

- http://cs.cuc.edu.cn/huangwei/wiki

小调查

- 你的电脑中过病毒吗?
- 你对信息安全专业的认知程度?
  - —就业?
  - —和计算机科学与技术专业的区别与联系?
- 信息安全与传媒行业的关系

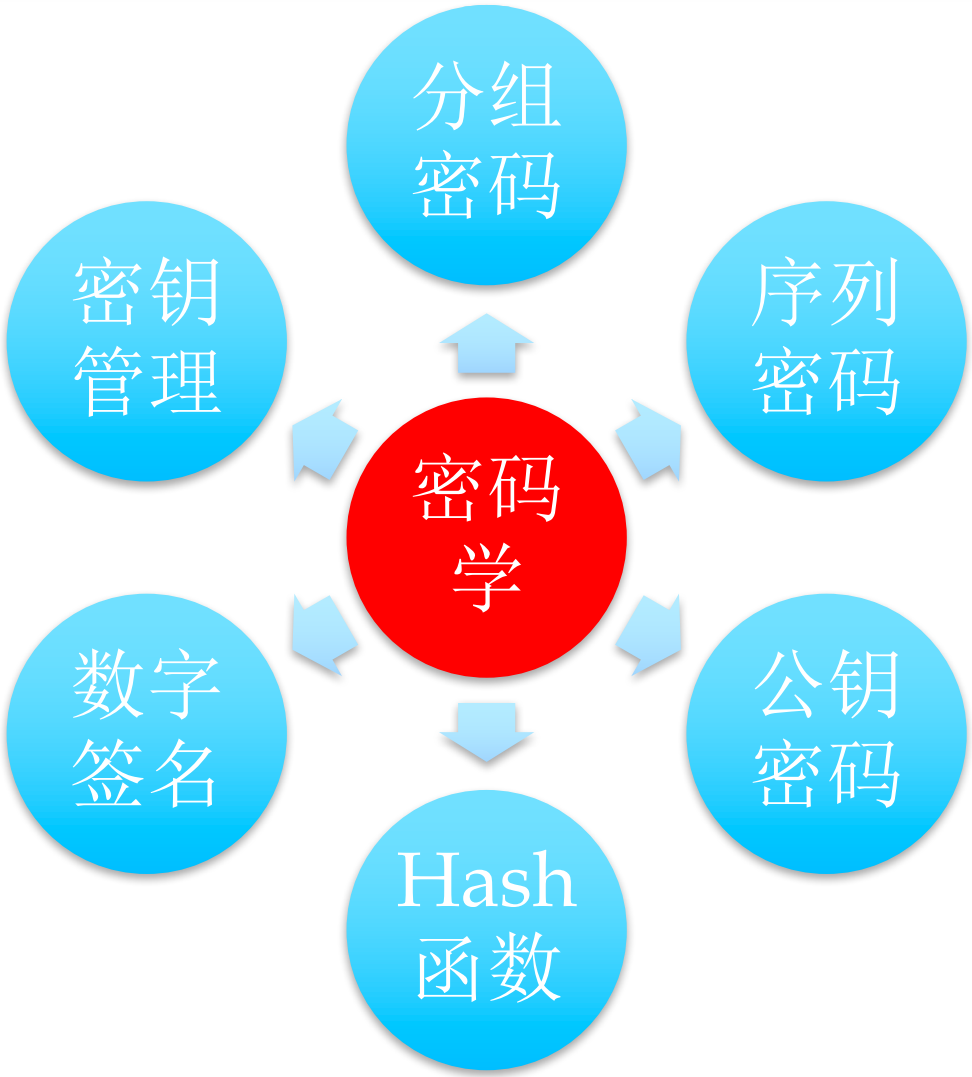
信息安全的研究内容

信息安全研究内容

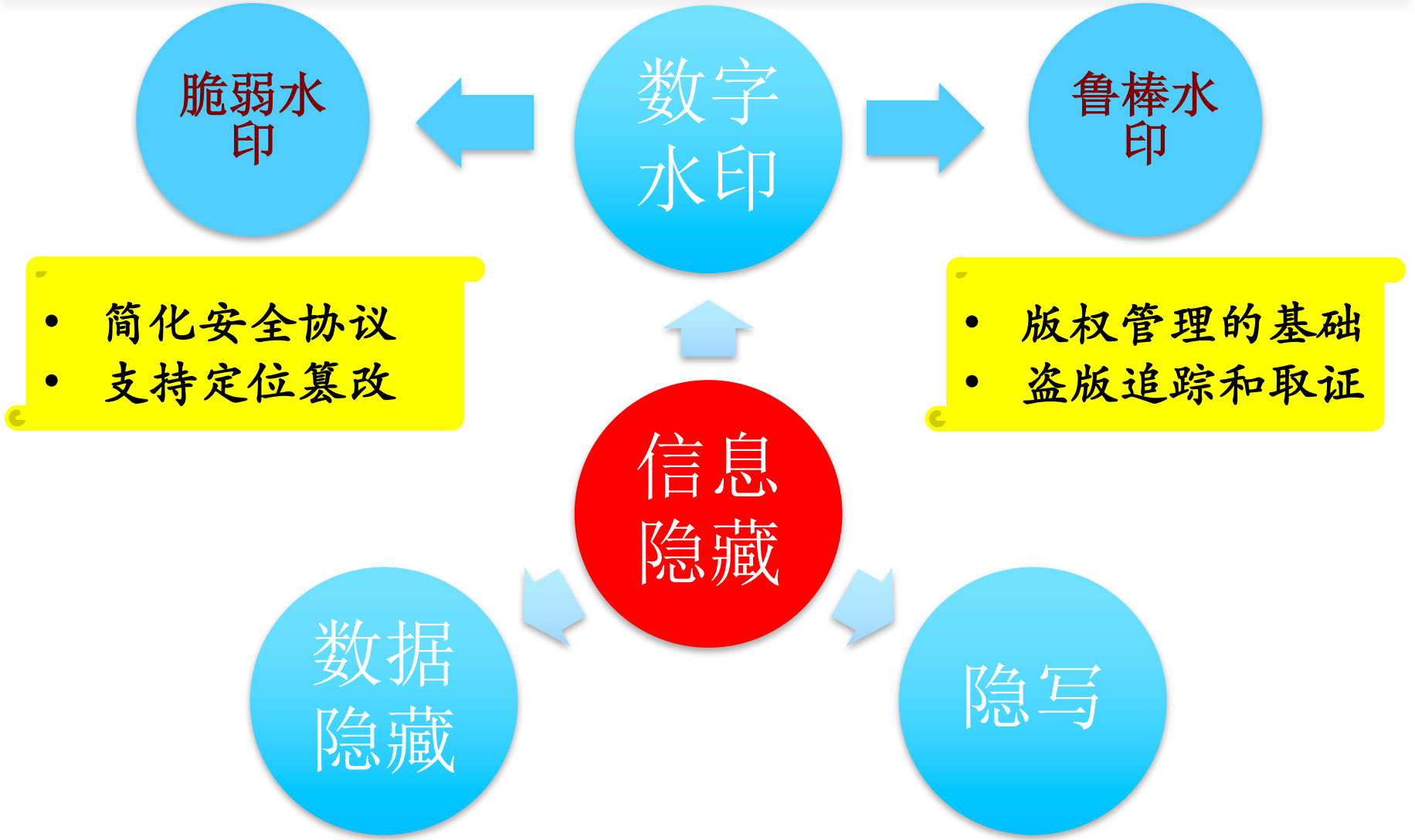
管理规范	法律和法规	管理研究
内容安全	网络与系统安全	应用研究
密码学	信息隐藏	基础研究

密码学研究内容

- 后续相关课程
  - —信息安全数学基础
  - —密码学
  - —信息论与编码原理B

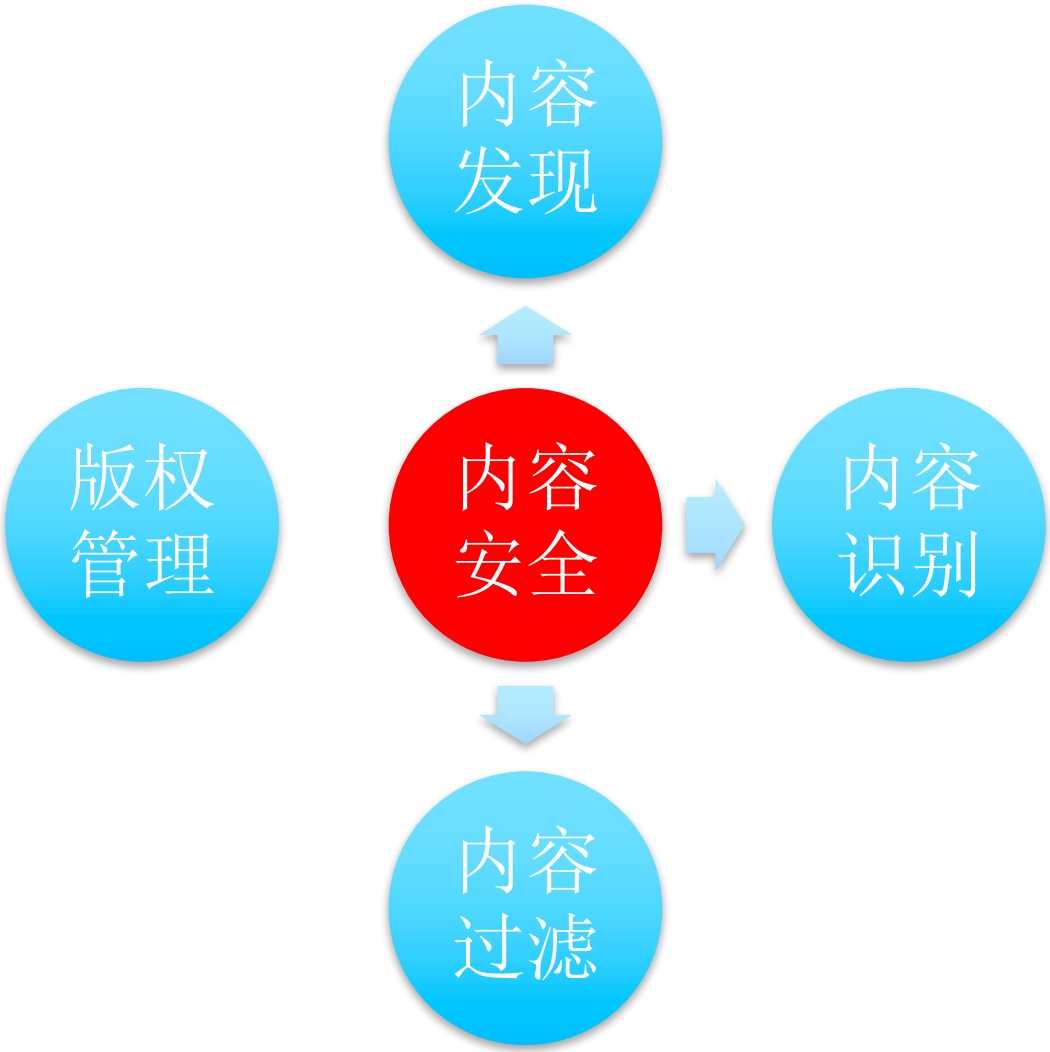


信息隐藏研究内容



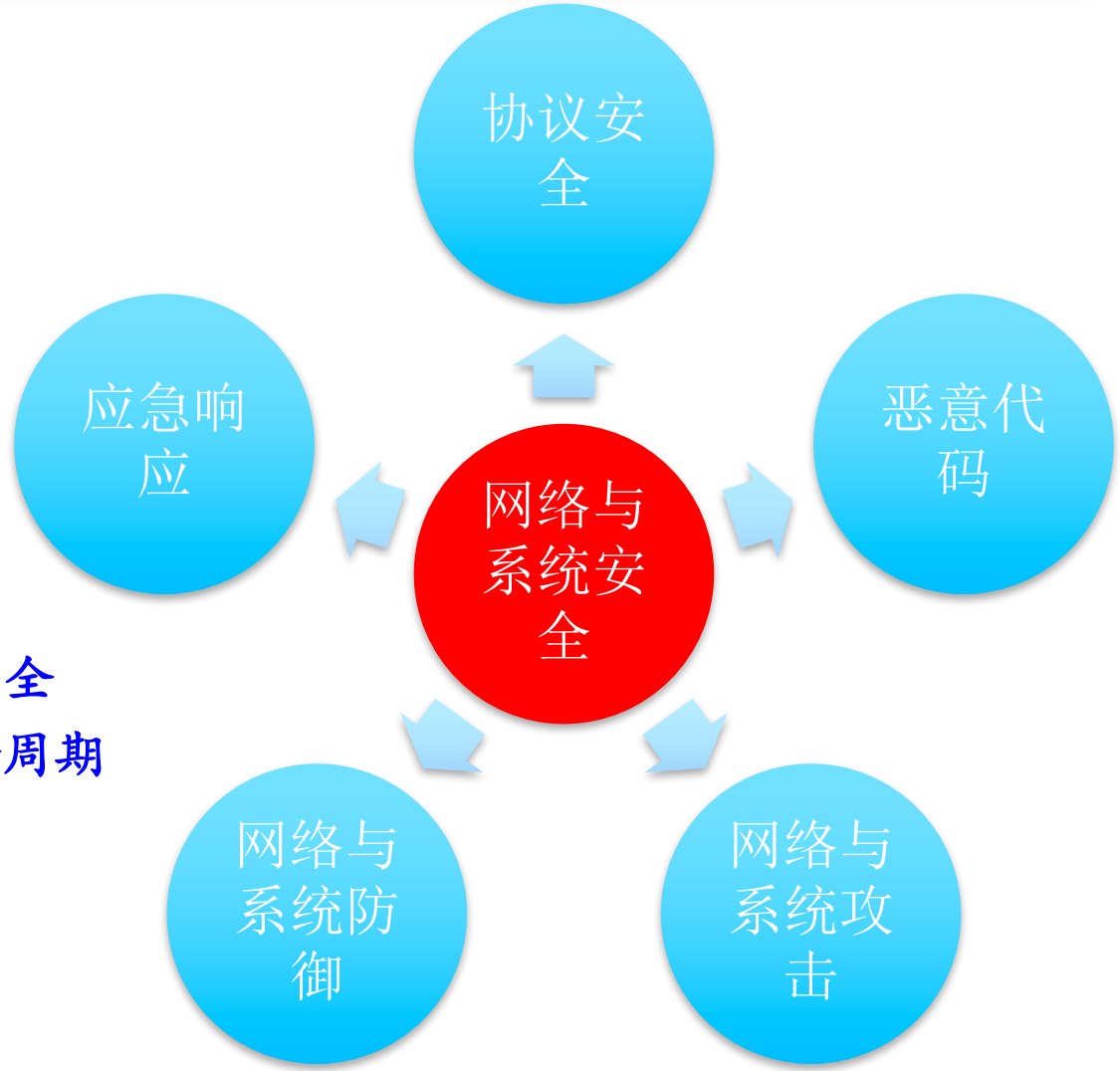
内容安全研究内容

- 后续相关课程
  - —数字内容安全
  - —数字版权保护
  - —数字媒体安全应用与实践



网络与系统安全研究内容

- 后续相关课程
  - —计算机安全与维护
  - —数据结构A
  - —编译原理
  - —网络安全
  - —移动互联网安全
  - —软件与系统安全
  - —网络传播与隐私保护
  - —电子商务与电子政务安全
  - —软件项目安全开发生命周期
  - —信息系统容灾技术
  - —信息安全新技术讲座

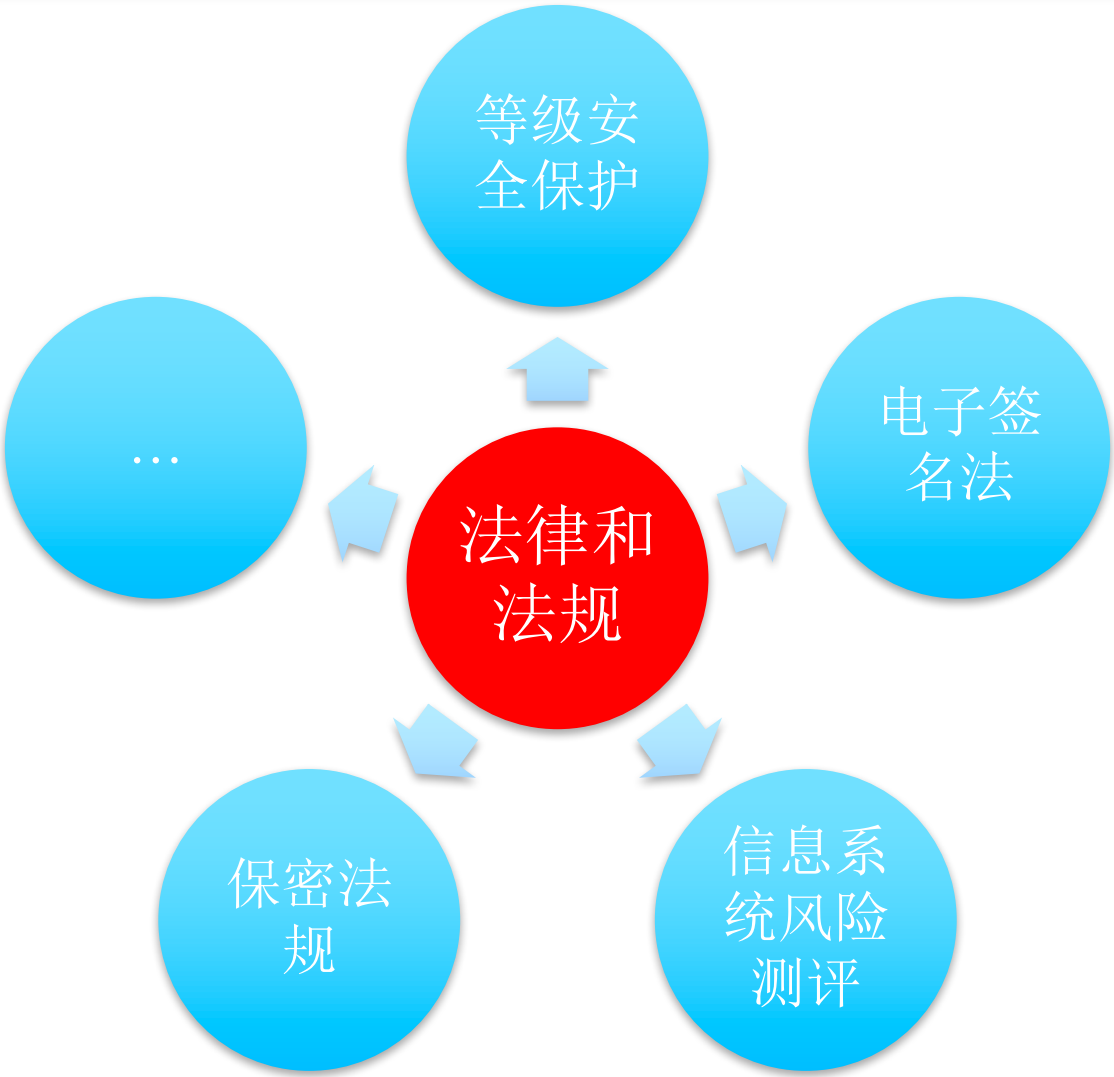


管理规范研究内容

- **后续相关课程**

  —信息安全管理

法律和法规研究内容



课程目的

- 通过本课程的讲授
  - —你能了解到
    - 信息安全的基本概念、原理和知识体系
    - 信息安全专业的主要研究内容
  - —你不能了解到
    - 如何编写恶意代码
- 激发专业兴趣，培养学习方法

课程体系

4学时	6学时	12学时	8学时
信息化与信息安全	密码学基础 2学时	操作系统安全 2学时	信息安全等级保护 2学时
信息安全基础	公钥密码与散列函数 2学时	网络安全 2学时	信息系统安全工程 2学时
	可信计算 2学时	Web安全 2学时	信息安全管理 2学时
		恶意代码 2学时	信息安全事件应急处理和灾难恢复 1学时
		信息隐藏技术 2学时	信息安全法规和标准 1学时
		数字水印技术 2学时	
课程概述	信息安全理论	信息安全技术	信息安全管理

考核方式

- 平时成绩
  - 占总评成绩的百分比为20%
  - 主要包括以下形式：
    - 上课考勤，作业、测验
- 期末考试
  - 闭卷
  - 占学期总成绩80%

第一章 信息化与信息安全

本章学习目标

- 了解信息化发展与信息安全的关系
- 掌握信息安全的基本属性
- 了解信息安全概念的演变历程
- 理解信息安全的非传统安全特点
- 了解我国信息安全保障工作的总体要求和主要原则

本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

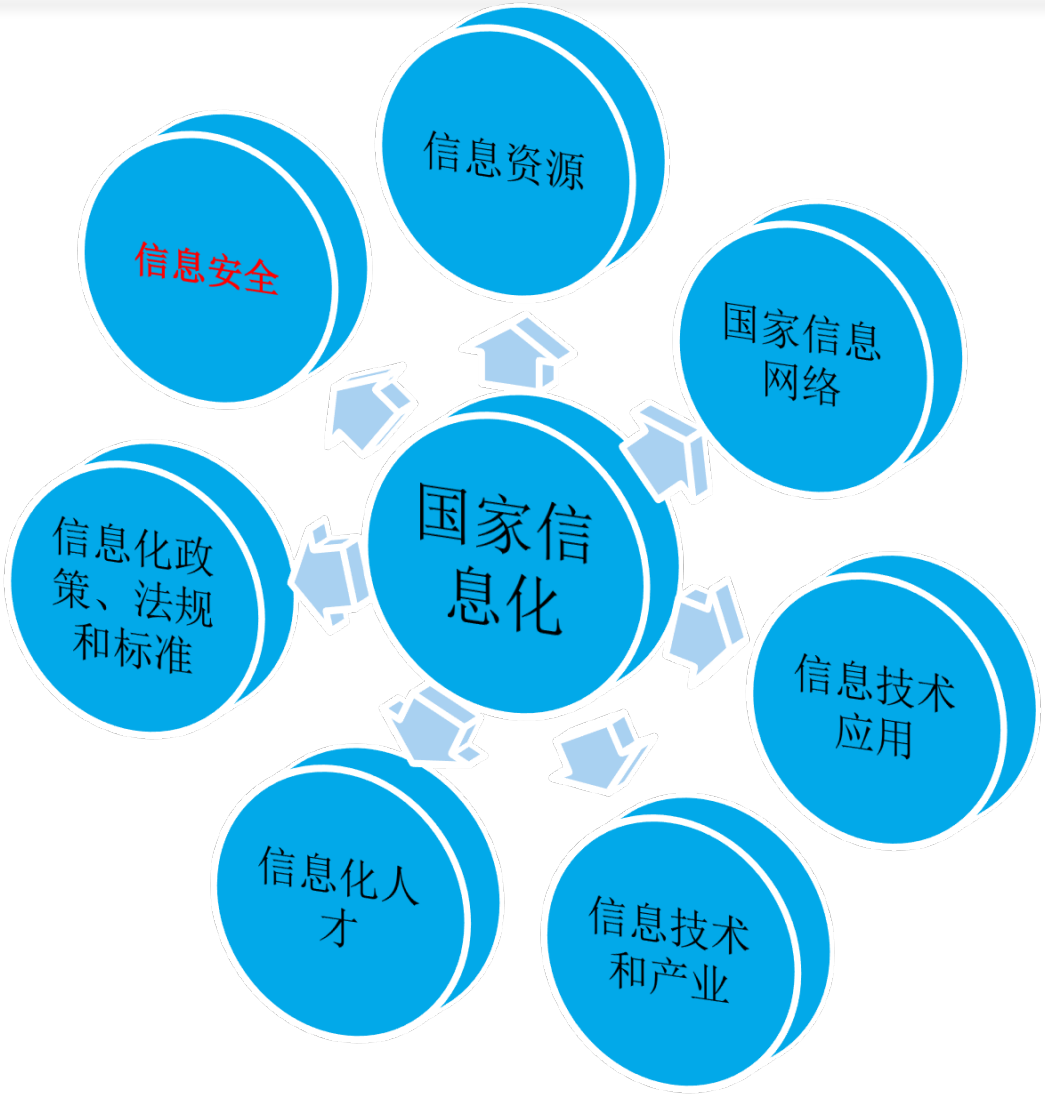
本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

信息化内涵

- 信息化是充分利用**信息技术**，开发利用**信息资源**，促进信息交流和知识共享，提高经济增长质量，推动经济社会发展转型的历史进程

我国国家信息化体系



我国信息化发展现状

- 政务信息化
  - —金盾、金关、金财、金税、金审、金农
- 信息化与工业化融合
  - —装备、船舶、汽车、家电、有色、纺织
- 信息化与文化传媒行业
  - —文化部“十二五”规划：文化与科技融合
  - —三网融合
  - —新媒体与社会化网络

身边的信息化

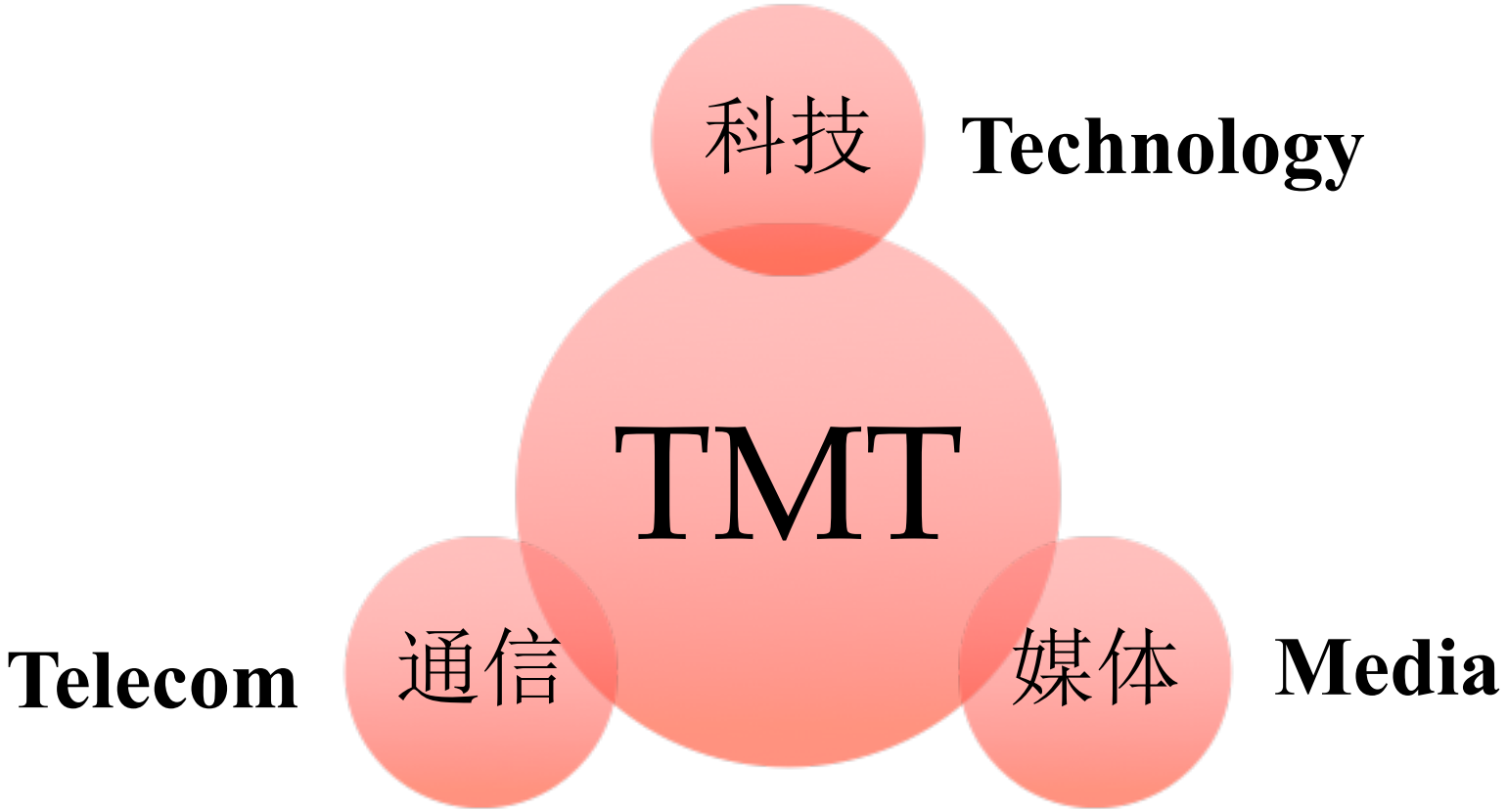
- 无纸化办公
  - —电子档案代替纸质档案
  - —MIS/ERP/CRM/OA
- 信息联网
  - —网购
    - 机票、火车票、电影票（二维码）
    - 电话卡、游戏币充值
- 电子出版
  - —电纸书、电子阅读器代替纸质书籍

信息化与互联网、移动互联网

- 2012年
  - —网民数量：5.38亿
    - 连续四年保持全球第一
    - 其中手机网民：3.88亿
  - —超过40家上市公司
  - —市值总额：1460亿美元
- 2002年
  - —网民数量：<5千万
  - —4家上市公司
  - —市值总额：4.2亿美元

2002年~2012年，中国互联网经济的平均增速在60%以上，是国家GDP增速的5倍还多，2011年，我国互联网产业的总体规模超过2600亿元人民币

信息化与TMT



中国社会化媒体格局


论坛/论坛聚合
社交游戏
视频分享
社交网络
博客/博客聚合
商务社交网络
音乐/图片分享
社会化电子商务
社会化书签
签到/位置服务
问答
微博
百科
即时通讯
消费点评
RSS订阅
中国社会化媒体格局概览
本图由CIC整理制作并定期更新，转载请注明出处；由于篇幅限制，该图仅选取部分代表性平台，特此说明。
Big Boards
zynga
facebook
YouTube
Linked in
Blogger
flickr
delicious
Answers
twitter
yelp
Google reader
Hudong
MBAlib
FeedSky
抓虾
renren
开心网
豆瓣 douban
白社会
Weolink
Ushi.cn
高朋
糯米
拉手网
美团
聚划算
街旁 Jiepang
新浪微博
腾讯微博
网易微博
搜狐微博
Baidu 贴吧
Baidu 知道
Baidu 百科
SOSO百科
知乎
TASK爱问
Yahoo! 知识堂
QQ书签
新浪博客
Bolaa
blogbus
和讯
Ku6.com
56网
帖易
天涯社区
虾米 xiami
YUPOO
一听音乐
淘米网
五岸钟
腾讯游戏
腾讯朋友
天际网
芒果网
信任+分享
切客
微领地
.ai 开开

中国主流网络媒体地图


中国主流网络媒体地图2012
【地方门户网站】
新疆网
亚心网
天山网
乌鲁木齐
新疆维吾尔自治区
塔里木河
中国甘肃网
每日甘肃网
内蒙古新闻网 正北方网
呼和浩特
千龙网
北京
北青网
东北网
黑龙江新闻网 哈尔滨新闻网
黑龙江网络广播电视台
中国吉林网 新文化网
长春新闻网 东亚网
沈阳
北国网 沈阳网 华商辽一网
东北新闻网
天健网 大连新闻网
长城网
河北新闻网
燕赵新闻网
北京网
天津网 今晚网
银川
宁夏新闻网
银川新闻网
大秦网
太原
山西新闻网
黄河新闻网
中原网
大众网 齐鲁网 鲁网 舜网 水母网
胶东在线 中国山东网 半岛网
西宁
青海新闻网
中国西藏新闻网
中国兰州网
华商网
大河网
青岛新闻网
龙虎网 中国江苏网
新华报业网 扬子晚报网
中安在线
合肥在线
安徽网络电视台
EAST3AY.COM
解放牛网 上海热线
文新传媒 东方早报网
西安新闻网
西安网
商都网
SCOL.COM.CN 四川在线
成都全搜索网
四川日报网 大成网
华龙网
大渝网
武汉
长江网 汉网 大楚网
杭州
浙江在线
杭州网 温州网
中国宁波网
中国江西网
南昌新闻网
湖南在线
星辰在线
长沙
今视网
东南网 福建之窗 福州新闻网
厦门网 泉州网 台海网 大闽网
金黔在线
贵阳新闻网
昆明
云南网
昆明信息港
广西新闻网
南宁新闻网
南宁
大洋网
奥一网 广州视窗 金羊网 21CN
深圳新闻网 南方报业网 大粤网
东莞时间网
广州
澳门
Southcn.com 南方网
海口
南海网 海口网
南海诸岛
【综合性门户网站】
sina 新浪网
搜狐 SOHU.com
網易 NETEASE www.163.com
腾讯网 QQ.com
凤凰網 ifeng.com
china.com 中华网 www.china.com
【视频网站】
YOUKU 优酷
土豆网 tudou.com
56.我乐.com
酷6网 Ku6.com
QIYI 爱奇艺
激动网 WWW.JOY.CN
LeTV 乐视网
V1.CN 第1视频 www.v1.cn
【中央级网站与中央媒体网站】
人民网 people www.people.com.cn
新华网 WWW.NEWS.CN
中国网
CNTV 中国网络电视台
CHINADAILY
CRI online 国际在线
中国青年网 youth.cn
中国传媒网 www.ce.cn
中国台湾网
中国广播网
中国新闻网 WWW.CHINANEWS.COM
光明网 GMW.CN
中青在线
中工网
Tibet.CN
说明：收录范围为具备媒体属性的综合网站，不含港澳台地区网站，排名不分先后。
截止日期：2012年4月23日零点
制作：
@北大新媒体
Weibo.com/pkuNBOOOKer

如果媒体被黑？

央视官网昨晚“被黑”两小时 主页成裸女照片

2010年02月16日00:40　新华网　喻晓　我要评论(27)　字号：T | T

昨晚不少网友反映中央电视台官方网站间歇性无法登录，WWW.CCTV.COM主页变成了一欧美女子照片，并持续至20时20分钟才被完全修复。记者此后致电多名央视工作人员，但没有得到正面回应。

昨天20时5分，记者欲登录央视官网查看今日温哥华冬奥会直播预告，却惊讶地发现WWW.CCTV.COM主页变成了一幅衣着裸露的欧美女子的照片，照片右下角还贴有“新快网”的水印。此后记者在一些论坛上看到有许多网友反映“央视官网被黑”，其中最早的一个帖子是18时14分发布的，帖子所附的截屏与记者看到的相同。虽然被篡改的央视官网与春晚没有任何关系，但仍有许多网友将这一事件与前天播出的春晚联系在一起，认为这是黑客对央视在晚会中过多地植入广告的行为发泄不满。记者随后致电多名央视工作人员，他们均表示“正在度假，不了解此事”。

今年以来，央视官网被黑已经不是第一次。据《潇湘晨报》报道，1月30日12时左右，央视视频互动平台的“星播客”频道突然贴出了一些内容不健康的视频，直到14时才被删除。当时央视网站客服中心给《潇湘晨报》记者的回应是：“我们这边的技术部门周末不上班，而且也没有人举报此事，可能是恶作剧。”（来源：北京晨报 记者 喻晓））

信息化发展对信息安全的需求——国家层面

- 党的十六届四中全会明确提出
  - —增强国家安全意识，完善国家安全战略
  - —确保国家的政治安全、经济安全、文化安全和信息安全
- 国务院关于大力推进信息化发展和切实保障信息安全的若干意见 国发〔2012〕23号[1]
  - —国家信息安全保障体系基本形成。重要信息系统和基础信息网络安全防护能力明显增强，信息化装备的安全可控水平明显提高，信息安全等级保护等基础性工作明显加强。
- 现代安全观：信息安全+国土安全
  - —信息疆域

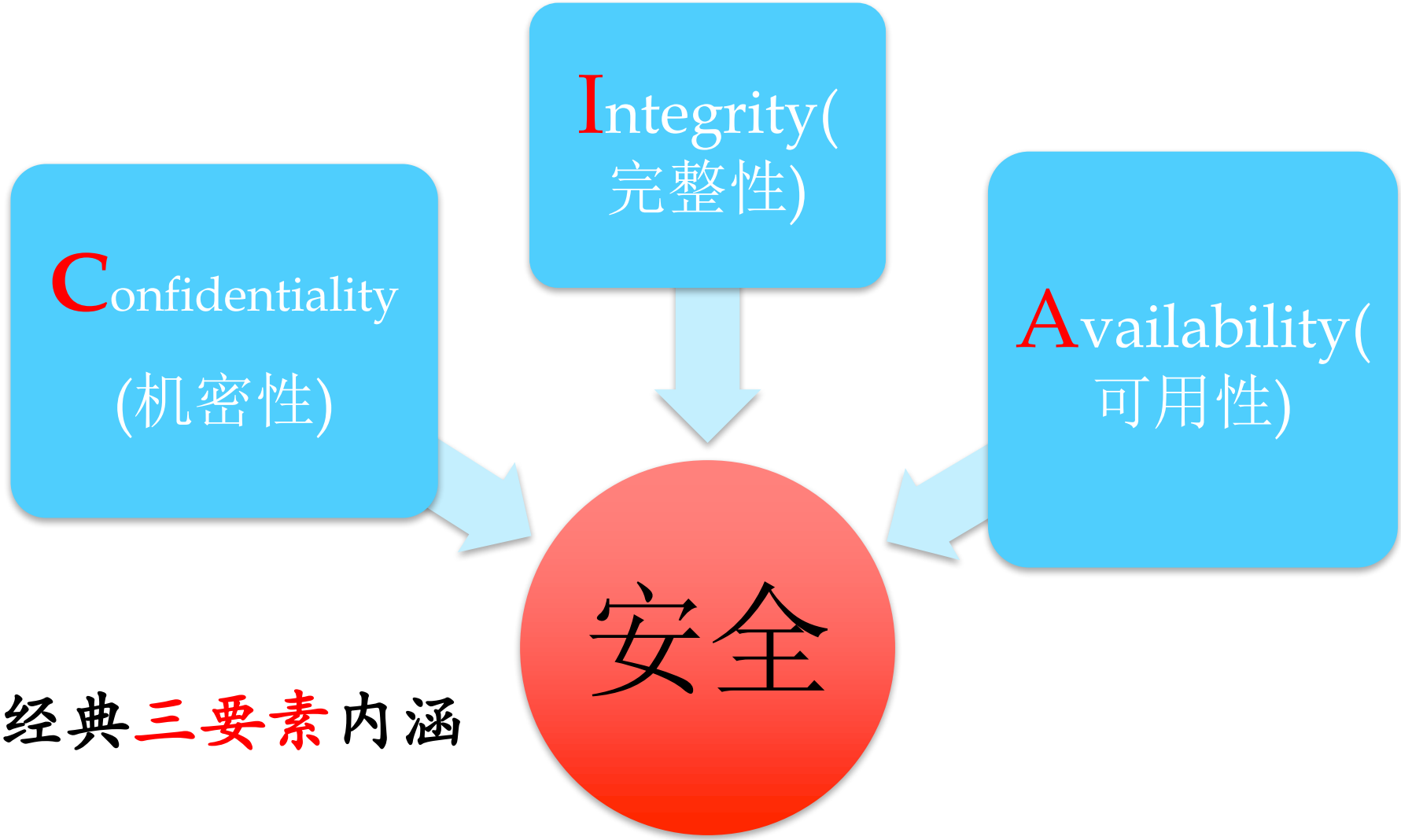
信息化发展对信息安全的需求——公民层面

- 传统网络犯罪借助信息技术新手段扩大危害
  - —网络诈骗、网络赌博、网络传销等
  - —网络攻击与病毒传播
  - —垃圾邮件、垃圾短信、垃圾电话
  - —网络造谣诽谤、攻击谩骂
- 2009年5月19日的全国大规模断网事件
- 地下黑色产业链
  - —制造木马、传播木马、盗窃账户、网络销赃、网络攻击勒索

本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

安全是什么



经典三要素内涵

机密性

- “不可见”是机密性的基本要求
  - —信件要装入密封完好不透光的信封
  - —保密性要求高的单位禁止使用无线网络，仅允许使用有线网络
- “不可感知”是机密性的更高要求
  - —基于流量异常的军情分析
- 除了通信过程，信息存储与处理过程中同样存在机密性要求
- 信息不可见，状态不可知

完整性

- 信息未经授权不能进行更改
  - —信息在存储或传输过程中保持不被偶然或蓄意的删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性
- 完整性强调“不可被修改”
  - —机密性强调“不可见”和“不可感知”
- 提问：你知道有哪些完整性保护方法？

可用性

- 信息可被授权实体访问并按需使用的特性
- 影响信息可用性的因素

  —硬件、软件、人、环境

本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

通信保密

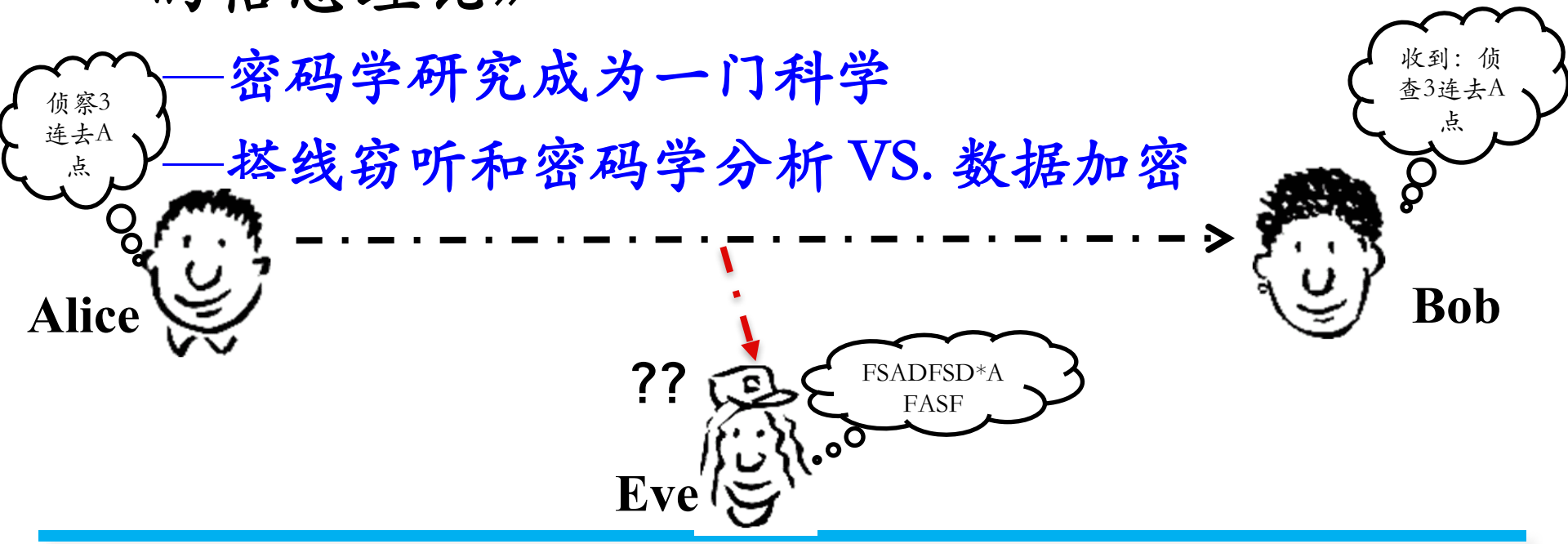
- 军事领域自古以来的需求

  ——古典密码学的诞生和发展过程

- 香农（Shannon）于1949年发表的《保密系统的信息理论》

  ——密码学研究成为一门科学

  ——搭线窃听和密码学分析 VS. 数据加密



计算机安全和信息系统安全

- 计算机安全
  —20世纪70年代以来
- 数据加密标准（DES）
  —美国国家标准局（NBS）1977年公布
- 可信计算机系统评估标准（TCSEC）
  —美国国防部（DoD）1985年公布
- 典型计算机安全威胁
  —黑客、恶意代码、外部访问、恶意用户、口令窃取、私人通信

信息保障

- Information Assurance

  —保护和防御信息及信息系统，确保其可用性、完整性、保密性、鉴别、不可否认等特性。这包括在信息系统中融入保护、检测、响应功能，并提供信息系统的恢复功能

- 纵深防御

  —美国军方的信息保障技术框架

新的信息安全观

- 从以往关注技术后果延伸到
  - —国家政治、经济、文化、军事等全方位的影响
  - —社会化网络传播
    - 意识形态危机
    - 文化扩张和文化霸权
- 中国特色的信息安全观
  - —保障信息化健康发展
  - —关注信息内容安全

本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

威胁的多元性

- 恐怖分子、毒品贩子和国际罪犯
- 黑客组织

  —炫技、宗教信仰、个人情感
- 为了利益

  —政治、经济、文化

攻防的非对称性

- 攻防技术非对称
  - —千里之堤溃于蚁穴
    - – 攻破马奇诺防线只需在一点上突围成功
- 攻防成本非对称
  - —时间成本：你晚上休息，TA晚上攻击
  - —技术成本：PC VS. 复杂的网络防御系统
- 攻防主体非对称
  - —个人 VS. 国家防御
    - – FBI、五角大楼内部网络多次被个人渗透

影响的广泛性

- 影响人群十分广泛
  - —自然灾害导致的地区范围大规模断网
- 扩散性极强
  - —1988年的莫里斯蠕虫
    - – 90行代码、2小时、10%的世界联网计算机瘫痪
  - —2001年的Nimda蠕虫
    - – 24小时、220万台计算机
- 连锁反应突出
  - —Stuxnet病毒攻击导致伊朗导弹发射过程中爆炸

后果的严重性

- 推翻国家政权
- 瘫痪国家基础设施
- 造成巨大经济损失
- 引发公共安全灾难

事件的突发性

- 我在明，敌在暗

  ——你永远无法预计到对手下一秒将做什么

- 全方位、全天候预警机制

本章内容提要

- 信息化发展
- 信息安全的基本属性
- 信息安全概念的演变
- 信息安全的非传统安全特点
- 我国信息安全保障工作

总体要求

- 国家信息化领导小组关于加强信息安全保障工作的意见（中办发[2003]27号）

  —2003年，中共中央办公厅、国务院办公厅转发

- 积极防御
- 综合防范

主要原则

- 立足国情，以我为主
  —自主知识产权
- 坚持管理与技术并重
  —3分技术，7分管理
- 正确处理安全与发展的关系，以安全保发展，在发展中求安全
  —安全建设有成本
- 统筹规划，突出重点，强化基础工作
- 充分发挥各方面的积极性，共同构筑国家信息安全保障体系

主要基础工作

- 实行信息安全等级保护
- 开展信息安全风险评估
- 加强密码技术应用，建设网络信任体系
- 高度重视应急处理工作
- 加强技术研发，推进产业发展
- 加强法制建设和标准化建设
- 加快人才培养，增强全民意识

本章小结

- 信息化发展
- 信息安全概念
- 信息安全的非传统安全特点
- 我国信息安全保障工作

参考资料

[1] 国务院关于大力推进信息化发展和切实保障信息安全的若干意见，国发〔2012〕23号，2012-06-28