信息安全导论

课程串讲复习

黄 玮

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

信息安全的目标理论

- 基本目标
  - ——机密性、完整性、可用性
- 扩展目标
  - ——鉴别、授权、不可抵赖性
    - 鉴别：认证
    - 不可抵赖性：审计
- 访问控制的基本面
  - ——认证、授权、审计

信息安全的目标理论相关主线问题

- 如何实现信息安全的不同维度目标?
- 密码学算法的分类有哪些?

  —密码学算法的基本原理框图

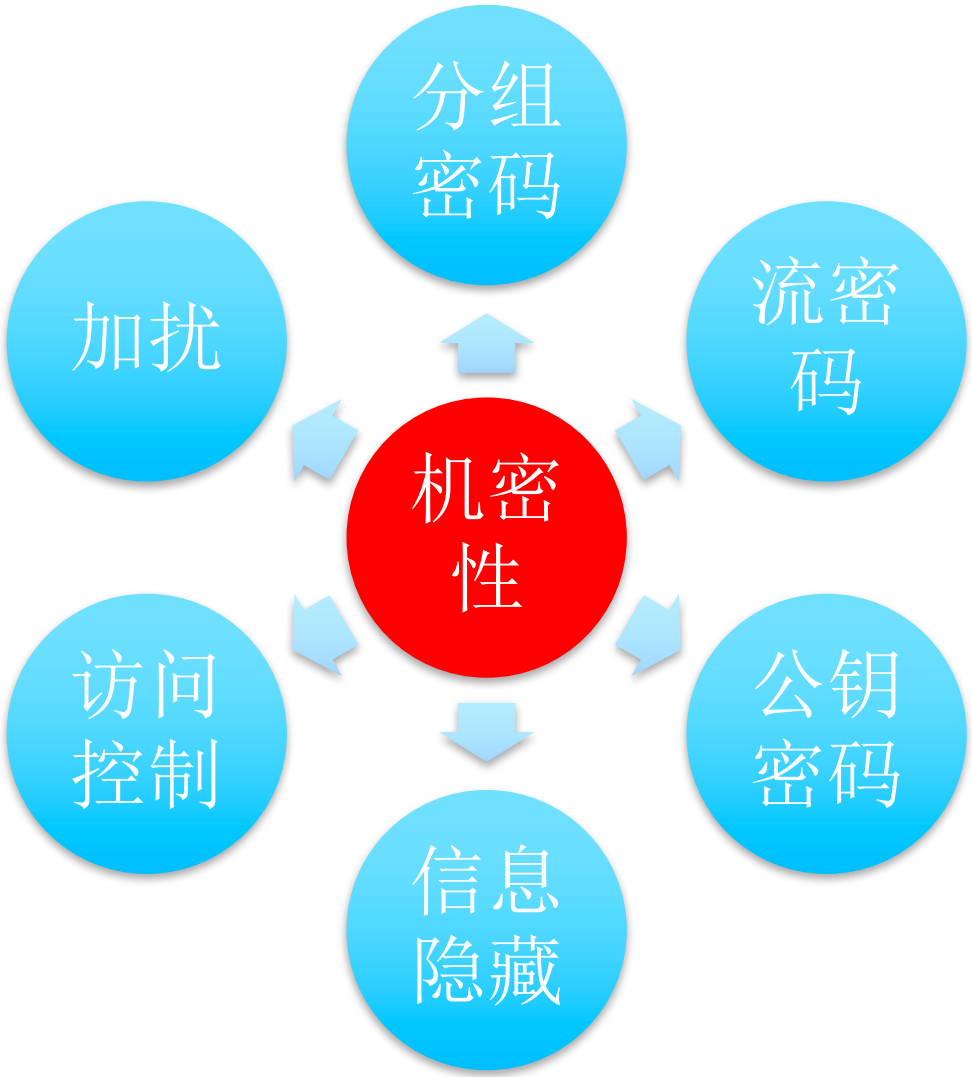
  – 基于以上原理框图的保密通信系统威胁建模

- 现代密码与传统密码的核心区别

  —算法的安全基于密钥而不是算法的保密

信息安全目标——机密性

- 加密
  - —密钥数量
    - 对称加密
    - 非对称加密
  - —明文处理方式
    - 分组密码、流密码
- 信息隐藏
- 访问控制
- 加扰
  - —条件接收



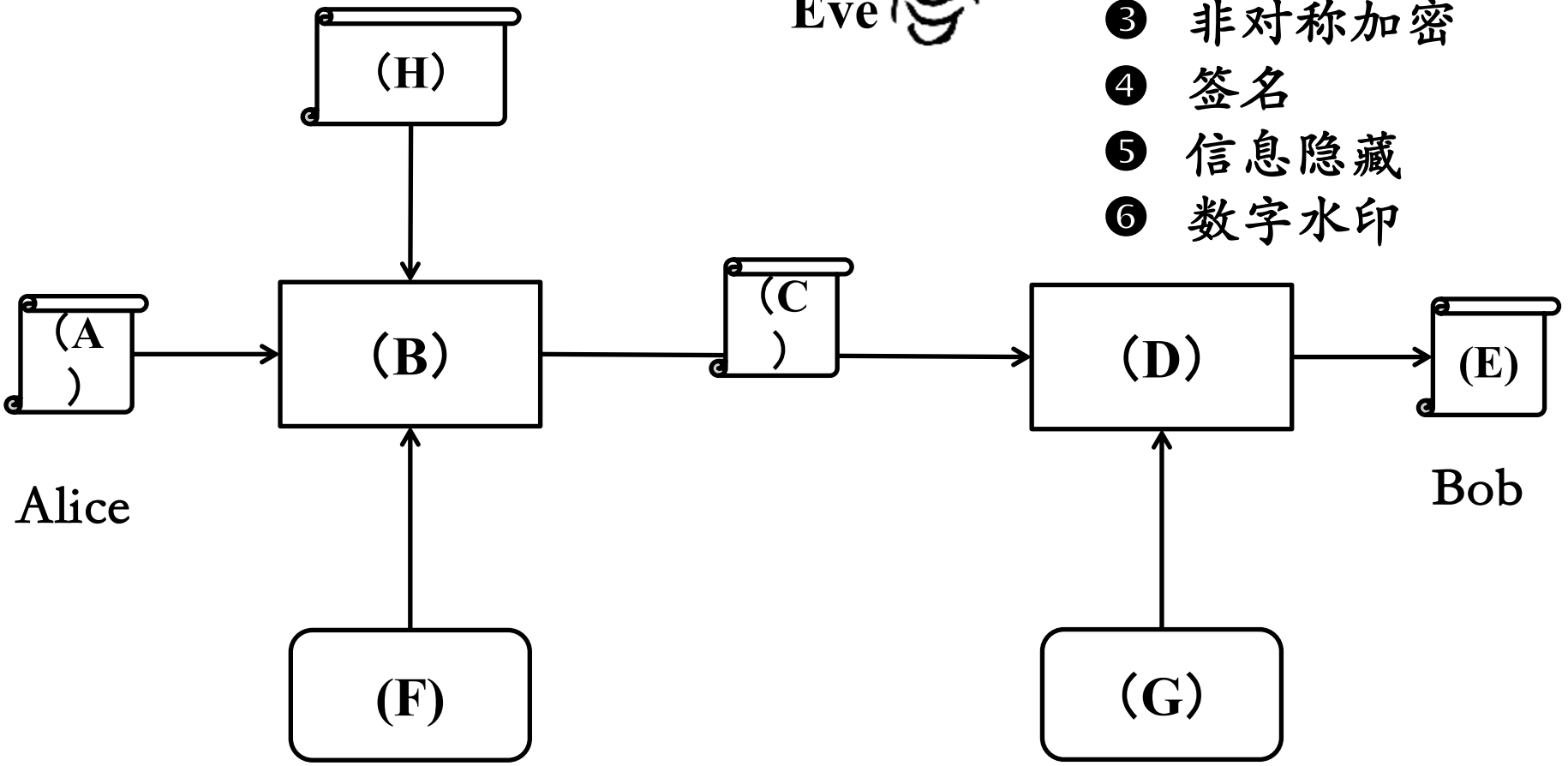
信息安全目标——机密性

- 对称加密与非对称加密的区别与联系
- 加密算法与Hash算法的区别与联系
- 加密与签名的区别与联系
- 加密算法的安全性评价
  - —密码分析的条件与工具
  - —实用安全性评价准则

一图胜千言

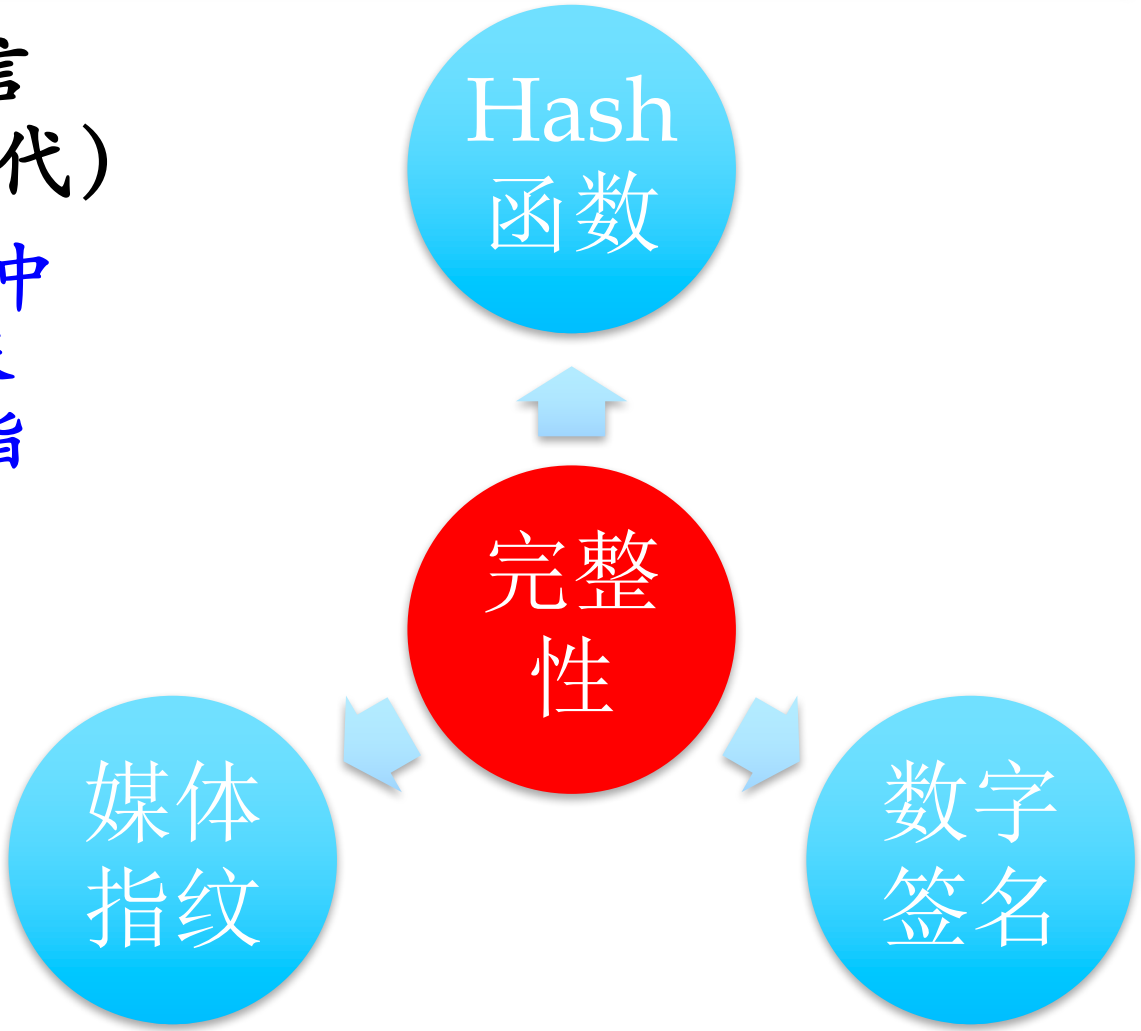
能对以下信息保密系统带来哪些风险?

1. 对称加密
2. 序列密码
3. 非对称加密
4. 签名
5. 信息隐藏
6. 数字水印



信息安全目标——完整性

- 数据安全（通信安全/前数字时代）
  - ——访问控制体系中的“可信”定义采用的是完整性指标
- 内容安全
  - ——媒体指纹



信息安全目标——可用性

- 课程中并未详细介绍
- 不仅是信息安全目标，也是系统工程目标
  - —代码优化
  - —架构优化
  - —运维优化

信息安全目标——认证

- 双因素认证
  - —有哪些因素可以用于认证
  - —生物特征身份认证方式的优缺点分析

身份认证

- 将身份标识（数字标识）唯一的绑定到主体
- 外部实体能够向系统证明其身份标识唯一性的因素
  - —知道的（例如：口令或秘密信息）knows
  - —拥有的（例如：令牌或磁卡）has
  - —生物特征（例如：指纹、虹膜）is
  - —实体位置（例如：在特定终端上）where
- 以上因素可以单一使用，也可以多个同时使用

双因素认证

- 混合2种可认证因素
  - —know / has / is /where
- 现实中的例子
  - —网银强制安全手段
    - – 证书
      - PC证书 / USB-Key证书
    - – 动态口令
      - 手机短信 / SecureID / 口令刮刮卡
  - —高等级物理门禁
    - – 口令 + 虹膜/指纹/IC卡

双因素认证设计与应用的要点

- 设计要点
  - —至少2个完全独立的认证信息传输信道
  - —至少2个完全独立的验证者
  - —以上2点至少满足其中一点
- 应用要点
  - —可用性保证：避免单点验证失效
  - —完整性保证：数字标识信息的生命周期完整性保护措施
  - —机密性保证：数字标识信息的生命周期机密性保护措施

信息安全目标——授权

- 访问控制模型
  - ——访问控制的基本面
  - ——访问控制的基本模型
    - 强制访问控制、自主访问控制

      BLP和Biba模型的区别与联系

信息安全目标——不可抵赖性

- 审计是重要的不可抵赖性目标实现手段
- 以下应用场景中特别强调不可抵赖性目标的实现
  - —数字签名
  - —密钥管理
    - – PKI机制
  - —访问控制
    - – 必不可少的环节

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

系统安全的主线问题

- 访问控制
  - —现代操作系统的访问控制策略设计和机制实现
- 可信计算
  - —访问控制策略设计与机制实现
  - —可信计算基（TCB）：硬件信任根
    - 可信平台控制模块（TPCM）
  - —安全操作系统：软件信任根
    - 信任的度量：完整性等级
- 恶意代码
  - —定义、概念、分类

网络安全的主线问题

- 网络攻击的过程可以看作是一个恶意数据输入的过程
  - ——关键是堵住漏洞的入口点
    - 核心是软件或硬件存在安全漏洞
    - 病从口入原理
- 网站被黑的可能原因

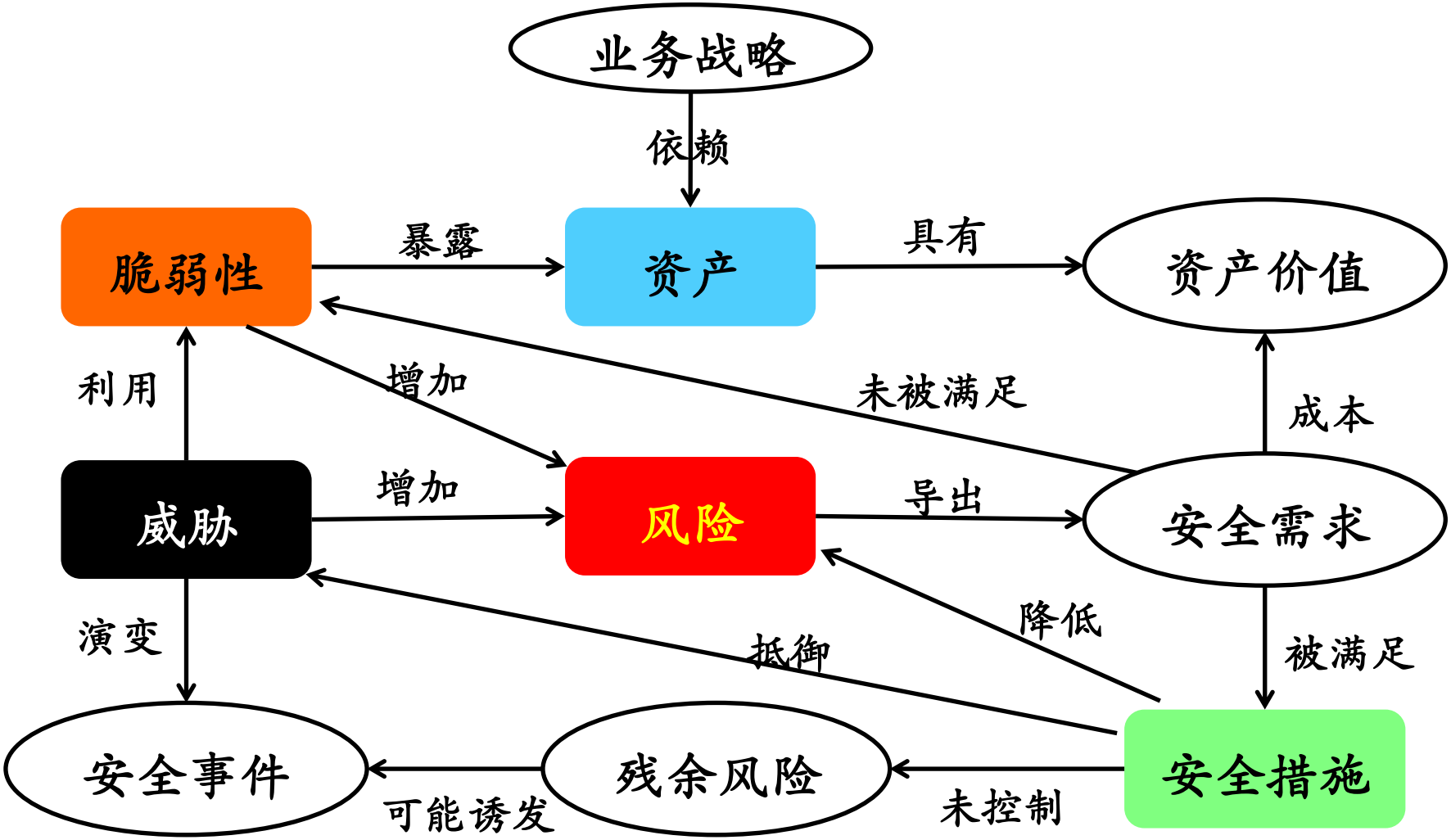
内容安全的主线问题

- 数据安全和内容安全的区别与联系
- 版权管理的主要方法
  - —非技术方法 VS. 技术方法
  - —为什么不能唯密码学方法
- 信息隐藏与数字水印的区别与联系
  - —区别
    - 信息隐藏：保护秘密消息，牺牲载体；
    - 数字水印：保护【载体】，【秘密】消息可见（可见水印）
  - —联系
    - 过程相同、要素相似

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

信息系统安全要素之间的关系



信息安全意识

- 信息安全的本质是持续对抗
  - —如何持续?
  - —如何对抗?
- 正确的安全观
  - —Built-in Security: 内置安全
  - —Security by Default: 默认安全
  - —Security in Depth: 纵深防御
  - —Proactive Security: 主动安全

- 信息系统安全保护等级应用指南
  - —三十二字方针
    - 明确责任，共同保护
    - 依照标准，自行保护
    - 同步建设，动态调整
    - 指导监督，重点保护
  - —分级矩阵
  - —等级安全基本安全保护能力描述

信息系统安全工程

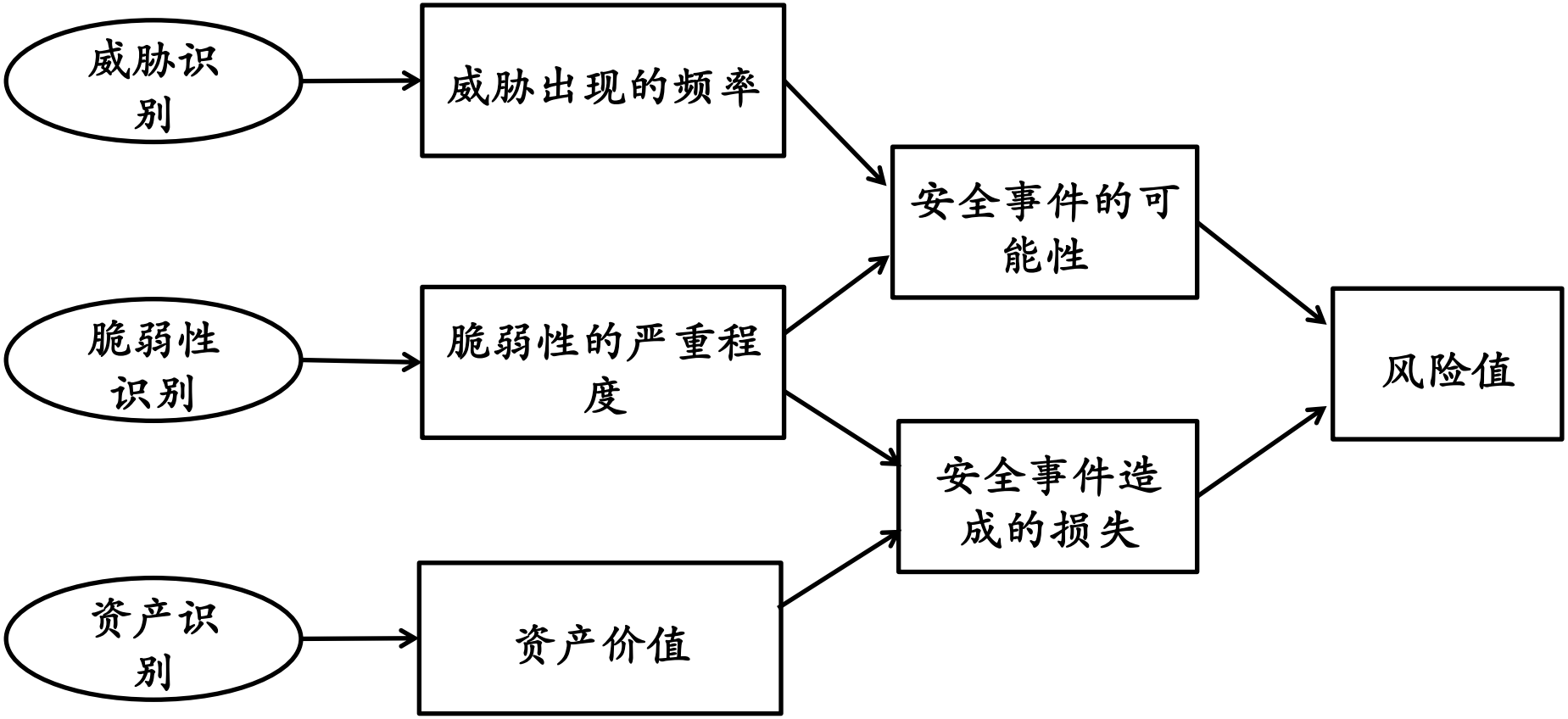
- 信息系统安全工程的一般过程
  - —发掘需求、定义系统功能、设计系统、评估系统、有效性评估
- 系统安全成熟度能力模型
  - —满足信息安全工程过程能力的改进与评估
    - 信息安全的持续对抗本质
    - 衡量和不断改进

信息安全管理

- 什么是信息安全管理
- BS 7799标准
  - —ISO/IEC 17799标准
  - —ISO/IEC 2700X系列标准
- PDCA模型
  - —Plan、Do、Check、Action
    - 和P2DR模型的联系？
  - —PDCA循环

- 风险分析原理与CVSS

—威胁识别、脆弱性识别、资产识别



我国信息安全法律法规

- 了解保密相关法律法规
  - —泄密坐牢，卖密杀头
  - —涉密不联网，联网不涉密
- 我国主要信息安全法律
- 我国主要信息安全行政法规
- 我国主要信息安全部门规章
- 我国地方性法规和地方政府规章

网络安全相关标准

- 可信计算机系统评估准则（TCSEC）
- 可信网络解释（TNI)
- 通用准则CC
- 《计算机信息系统安全保护等级划分准则》
- 信息安全保证技术框架
- 《信息系统安全保护等级应用指南》