



# 网络与系统安全

## 第一章 计算机网络安全基础

黄 玮

中国传媒大学



---

关于课程你需要了解...

---

中国传媒大学



## 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 A407 / 实验：48教 A202

- 上课时间

- 讲授：1-12 周五 第5、6节                      四十八教A407

- 实验：3-8,10,12周 周二 第5、6节 四十八教A202

- 答疑地点/时间

- 教室 / 课后

- 新浪微博 @中传黄玮 / 随时



## 课程概况

---

- 先修课程
  - 计算机网络A
  - 信息安全概论
- 推荐教材
  - 无
- 硬件和软件环境
  - PC
  - Linux (Backtrack 5)



## 在线资源

---

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



## 小调查

- 你的电脑中过病毒吗?
- 你被盗过“号”吗?
- 你知道黑客入侵系统的方法吗?
- 你用过网络嗅探工具吗?
- 你知道防火墙的用途吗?
- 你能说出几种网络安全设备?



## 课程目的

---

- 通过本课程的讲授和实验操作
  - 你能了解到
    - 网络攻防基本原理
    - 网络攻防基本手段
  - 你不能了解到
    - 如何编写恶意代码





# 课程体系

实验上机：2学时  
讲授：6学时

计算机网  
络安全基  
础

实验上机：4学时  
讲授：4学时

网络监听  
与扫描

实验上机：4学时  
讲授：4学时

网络与系  
统渗透

实验上机：6学时  
讲授：10学时

网络与系  
统防御

由易到难  
由基础到综合



## 考核方式

- 平时成绩
  - 占总评成绩的百分比为**40%**
  - 主要包括以下形式：
    - 上课考勤，作业、测验，实验上机
- 期末考试
  - 开卷
  - 占学期总成绩**60%**，着重进行能力考察



---

# 第一章 计算机网络安全基础



## 本章内容提要

---

- 一. 专业术语定义
- 二. 威胁模型
- 三. 安全策略和安全机制
- 四. 计算机网络安全模型
- 五. 等级安全保护
- 六. 计算机安全法规



# 一、专业术语定义



## 术语定义

---

- 资产 Asset
- 安全 Security
- 威胁 Threat
- 风险 Risk
- 漏洞 Vulnerability
- 影响 Impact
- 攻击 Attack

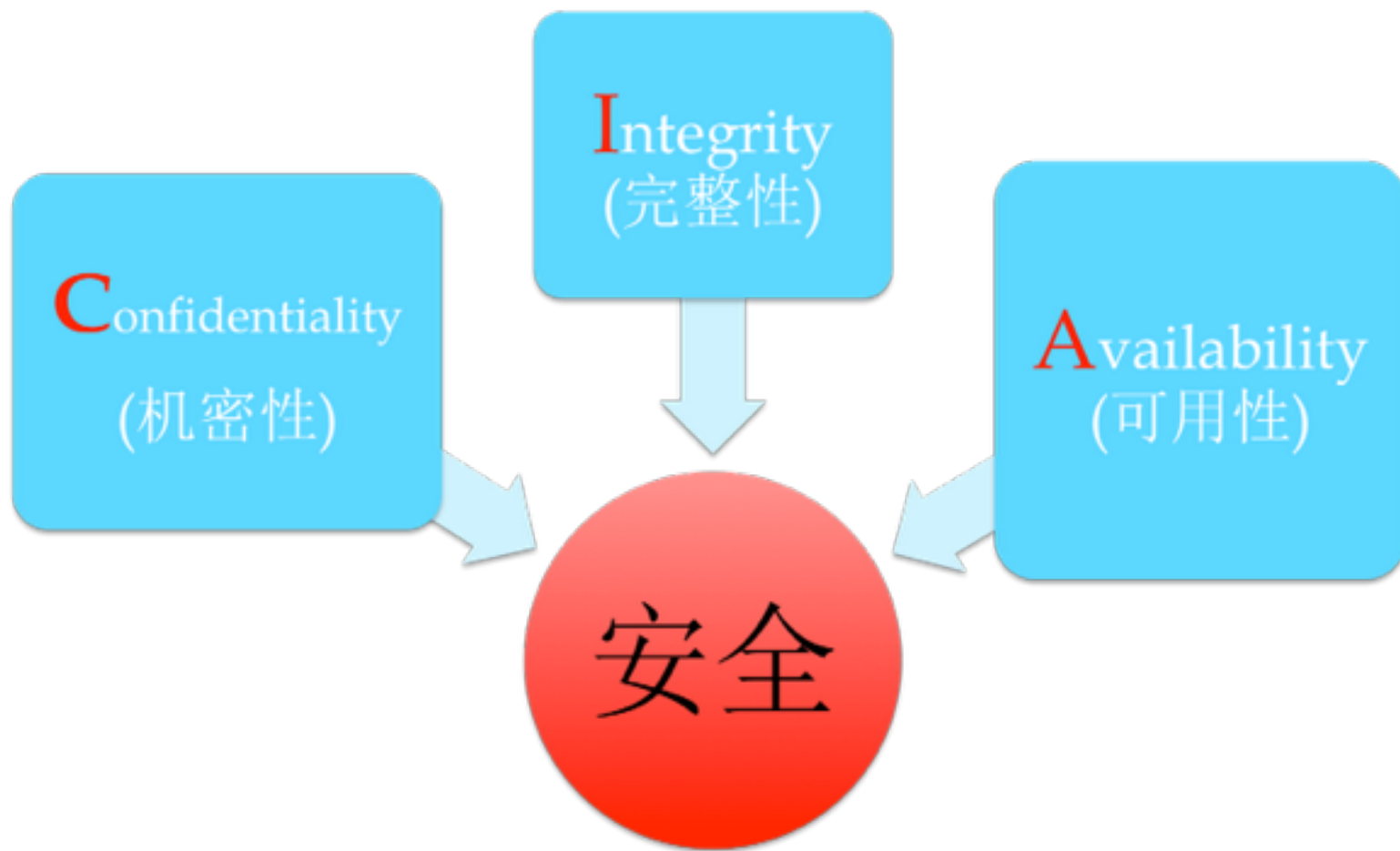


## 资产是什么

- 任何对组织业务具有**价值**的信息资产，包括
  - 计算机硬件
  - 通信设施
  - IT环境
  - 数据库
  - 软件
  - 文档资料
  - 信息服务和人员
  - ...



# 安全是什么







## 威胁是什么

- 威胁就是一种可能破坏安全基本要素的**来源**或**原因**
  - 对于数据库中的数据来说，**SQL注入攻击**就是一种威胁。一旦攻击得手，可能会被窃取机密数据，导致数据的**机密性**被破坏
  - 对于网站来说，**拒绝服务攻击**一旦得手，会破坏网站的**可用性**
- 特定威胁有可能通过利用某一**漏洞**对资产带来**可能的影响**——**风险**



## 漏洞是什么

- 又称脆弱性 / 弱点
- 漏洞存在于
  - IT基础设施(计算机软硬件、通信设施)
  - 人(管理制度、操作规范和流程)
- 漏洞一旦被利用，会对资产造成影响



## 风险是什么

- 风险是威胁事件发生的可能性与影响综合作用的结果
- 风险成为事实后，就会造成具体的影响
  - 机密数据被窃
  - 网页被篡改
  - 网站被拒绝服务攻击所瘫痪



## 攻击是什么

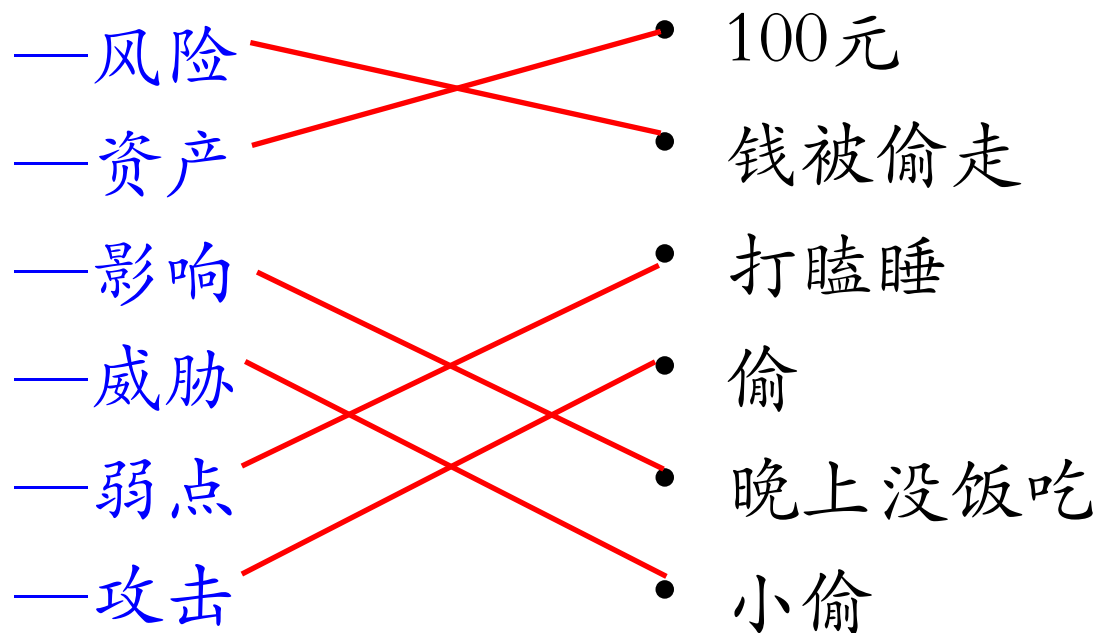
---

- 漏洞利用的过程
- 实现威胁
- 攻击得手会造成影响



## 类比案例分析

- 小明口袋里有100元，因为打瞌睡，被小偷偷走了，导致小明晚上没饭吃

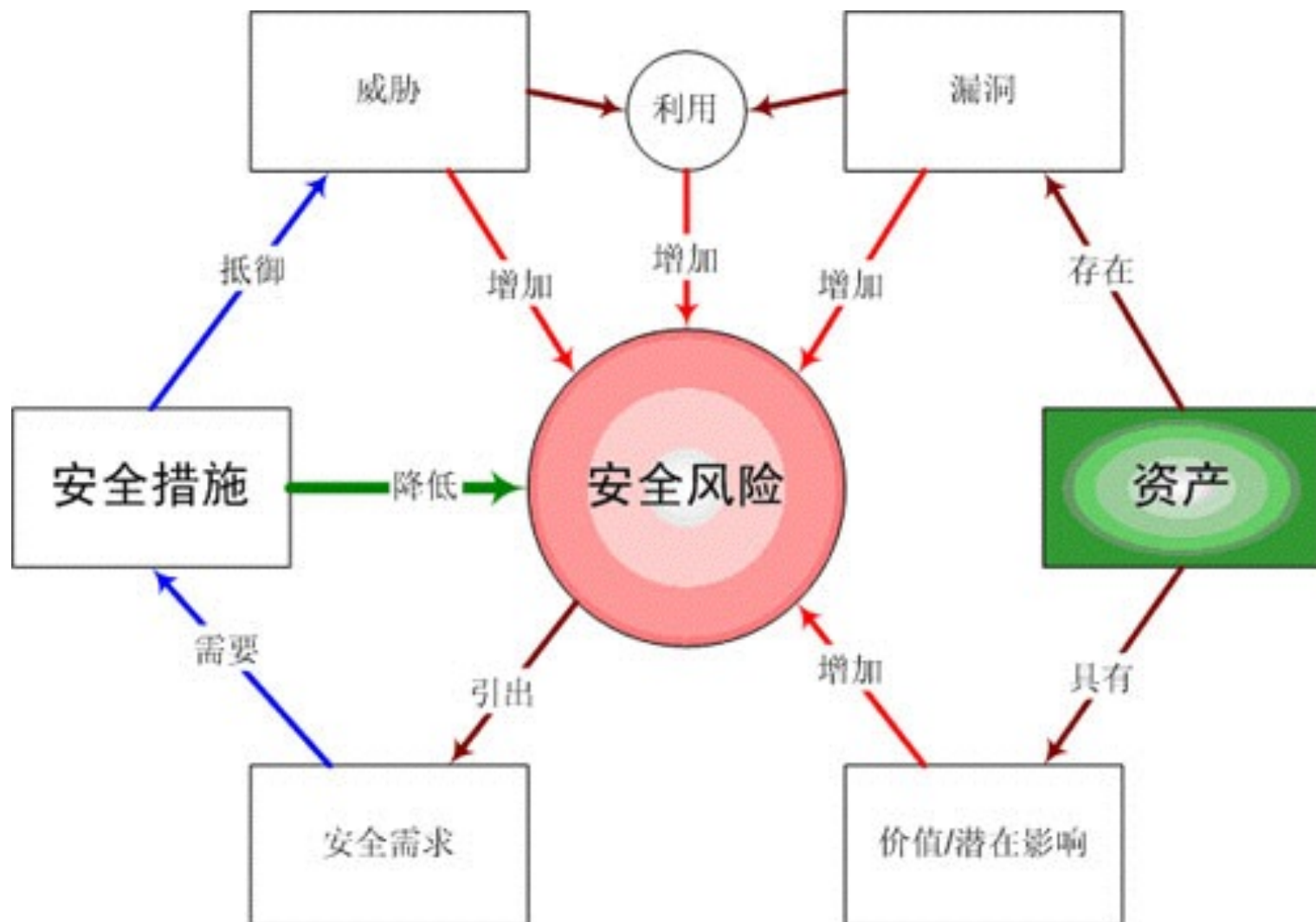


重要启示：

- 如果没有漏洞（弱点），攻击无法得手
- 如果没有价值（资产），不会招来威胁



## 小结





---

## 二、威胁模型



## 微软STRIDE模型

威胁	安全性属性
假冒 (S <sub>poof</sub> )	认证 (Authentication)
篡改 (T <sub>amper</sub> )	完整性
否认 (R <sub>epudiation</sub> )	不可抵赖性
信息泄露 (I <sub>nformation Disclosure</sub> )	机密性
拒绝服务 (D <sub>enial of Service</sub> )	可用性
提升权限 (E <sub>levation of Privilege</sub> )	授权 (Authorization)





## 安全性属性的扩充

- 认证 / 授权 / 不可抵赖性
- 不可抵赖性可通过审计来保证
- 认证(Authentication): 身份验证
- 授权(Authorization): 行为验证
- 审计(Audit): 结果验证+责任认定  
— 责任认定(能力): Accountability



# 概念对比

---

- 真实性
  - 完整性+（身份）认证
  - 复合概念
- 完整性
  - 原子概念



## 其他威胁模型

---

- 见参考文献[4]
  - CVSS
  - DREAD
  - Trike
  - OCTAVE



## 通用弱点评价体系 (CVSS) (1/3)

- Common Vulnerability Scoring System
- 美国国土安全部主导的NIAC开发
  - Cisco, Symantec, ISS, Qualys, Microsoft, CERT/CC, eBay
- 目前由FIRST在维护
  - Forum of Incident Response and Security Teams
- 试图量化评估漏洞的影响大小（危害程度）



# 通用弱点评价体系 (CVSS) (2/3)

## • 评价体系构成

—基本评价(组) / 生命周期评价(组) / 环境评价(组)

### 基本评价 (Base Metrics)

metric	要素	可选值	评分标准
AccessVector	攻击途径	远程/本地	0.7/1.0
AccessComplexity	攻击复杂度	高/中/低	0.6/0.8/1.0
Authentication	认证	需要/不需要	0.6/1.0
confidentiality	机密性	不受影响/部份地/完全地	0/0.7/1.0
integrity	完整性	不受影响/部份地/完全地	0/0.7/1.0
availability	可用性	不受影响/部份地/完全地	0/0.7/1.0
bias	权值倾向	平均/机密性/完整性/可用性	各0.333/权值倾向要素0.5另两个0.25

### 生命周期评价 (Temporal Metrics)

metric	要素	可选值	评分标准
Exploitability	利用代码	未提供/验证方法/功能性代码/完整代码(无需代码)	0.85/0.90/0.95/1.00
Remediation Level	修正措施	官方补丁/临时补丁/临时解决方案/无	0.87/0.90/0.95/1.00
Report Confidence	确认程度	传言/未经确认/已确认	0.90/0.95/1.00

### 环境评价 (Environmental Metrics)

metric	要素	可选值	评分标准
Collateral Damage Potential	影响	无/低/中/高	0/0.1/0.3/0.5
Target Distribution	目标分布	无/低/中/高(0/1-15%/16-49%/50-100%)	0/0.25/0.75/1.00



## 通用弱点评价体系 (CVSS) (3/3)

- 相关标准与体系
  - CVE：公共漏洞曝光
    - Common Vulnerabilities & Exposures
  - CWE：常见缺陷列表
    - Common Weakness Enumeration
- 目标
  - 创建可度量的安全（标准）



---

### 三、安全策略和安全机制



## 安全策略和安全机制

- 安全策略 (Security Policy)
  - 声明
  - 哪些能做，哪些不能做
  - 哪些行为允许，哪些行为禁止
- 安全机制 (Security Mechanism)
  - 方法/工具/手段
  - 实现安全策略





- 打开一扇门需要一把钥匙

- 安全假设

- 门锁不会被开锁匠用工具打开

- 安全需求

- 只有通过匹配的钥匙才能打开这扇门

- 实际环境

- 技术高超的开锁匠可以在没有钥匙的情况下用自制工具打开门锁

- 信任

- 如果开锁匠是可信的，上述安全假设可以成立



- 信任的内涵

- 开锁匠是可信的：在没有获得门锁主人的授权的前提下，开锁匠不会去“开锁”

- 门锁的“后门”是可信的：“后门”不会被不可信的人发现，更不会被恶意利用

- 一旦信任不再，基于该信任的安全机制将失去效果

- 开锁匠非授权利用门锁的“后门”，在没有得到门锁主人授权的前提下，不使用钥匙也打开了该门  
实现了“漏洞利用”



## 安全策略中存在的安全假设

- 系统的状态能被正确、无歧义的分分为“安全”和“不安全”两种状态
  - 安全策略能正确的定义系统的“安全”状态
  - 某银行规定：银行经理进行转账操作是被授权的
- 安全机制能够强制保证系统不会进入“不安全”状态
- 如果以上2个安全假设中的任意一个为假，则系统的安全性无法得到保证



## 安全机制中存在的安全假设

- 每一个安全机制都是被设计用来实现安全策略中的一个或多个具体策略
- 安全策略的集合能够实现所有的安全策略
- 安全机制的实现是正确的
- 安全机制的部署和管理是正确的

如果安全假设为假，  
谈何“网络与系统安全”？



## 四、计算机网络安全模型



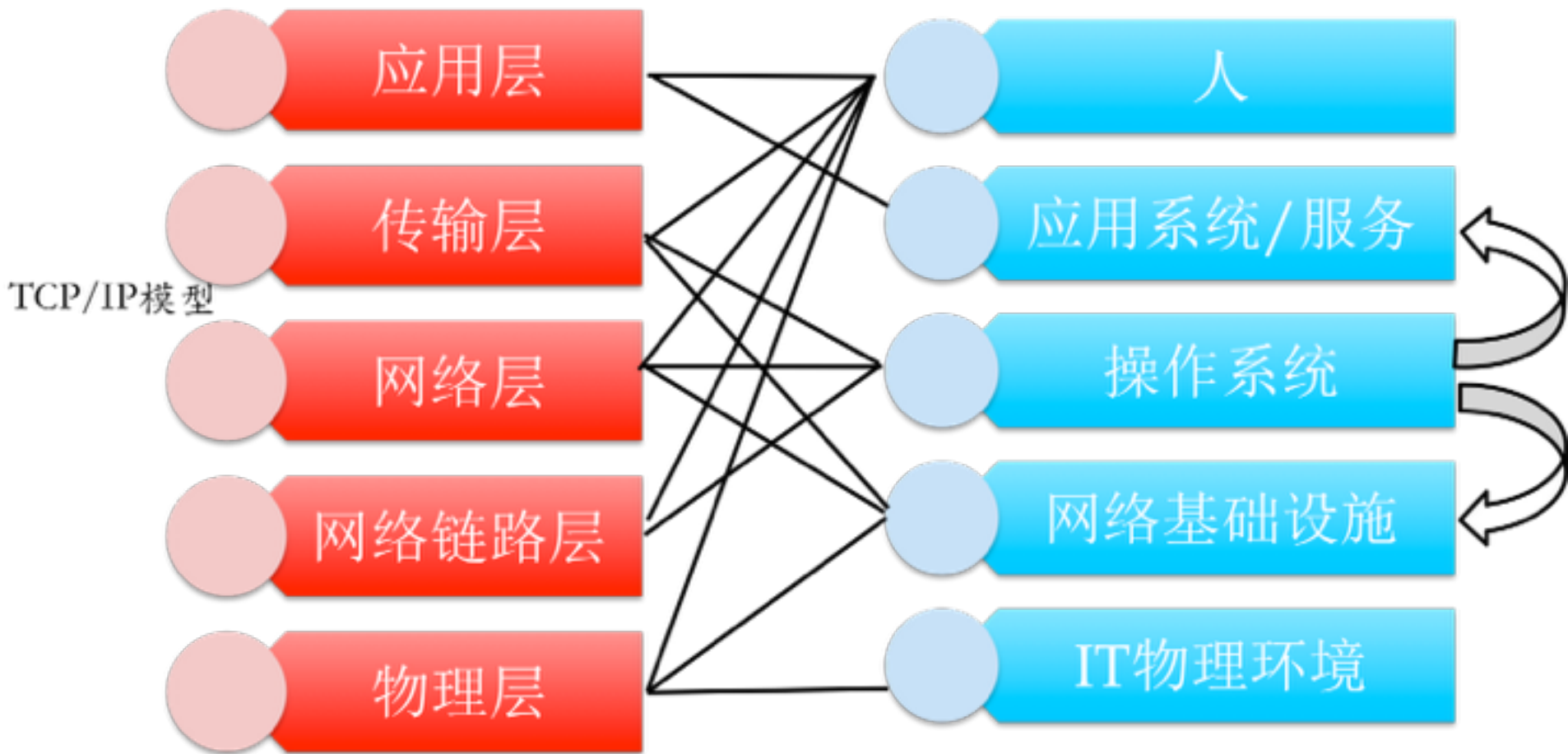
## 2种模型

---

- 静态模型
  - 安全威胁的分层模型
- 动态模型
  - P2DR模型



## 安全威胁的分层模型





## 用分层的方法来看Web威胁模型







## 分层模型小结

- 和计算机网络的分层模型类似
  - 每一层的安全威胁是既相互独立，又相互联系、相互影响的
  - 每一层的安全威胁必须依靠当前层的安全策略和安全机制解决
  - 下一层的安全机制是上一层安全机制的基础
  - 上一层的安全机制等级不会高于下一层的安全机制等级
    - 下层不安全，上层安全无法保障
    - 下层安全，并不代表上层安全



## P2DR模型

- 安全是
  - 持续循环过程
  - 动态变化
- 策略 (Policy)
- 防护 (Protection)
- 检测 (Detection)
- 响应 (Response)





- 安全策略的体系化

- 制订

- 执行

- 评估





- 主动防护
  - 数据加密
  - 身份认证
  - 访问控制
  - 虚拟专用网(VPN)
- 被动防护
  - 防火墙
  - 安全扫描
  - 入侵检测



## 安全检测

---

- 安全测试
- 蜜罐
- 入侵检测
- 安全审计



- 一旦检测到安全防护措施正在遭受攻击、或已失效(安全机制被突破), 响应机制(系统)开始发挥作用, 例如
  - 产生告警
  - 限制访问
  - 灾难恢复
  - 启用备用系统
- 世界上首个计算机应急响应小组CERT
  - Computer Emergency Response Team
  - 中国计算机应急响应小组: CNCERT



## 用P2DR模型审视：STRIDE/CVSS/CVE/CWE

- 策略
  - 基于STRIDE进行系统设计
- 防护
  - 基于CWE在系统开发过程中规避已知弱点
- 检测
  - 检测到新漏洞后添加到CVE
- 响应
  - 基于CVSS对CVE条目的评分确定响应策略
    - 轻重缓急



## 计算机网络安全模型小结

- 从静态的视角看计算机网络安全模型
  - 安全威胁是可以分层的
- 从动态的视角看计算机网络安全模型
  - 安全威胁是持续变化的
- 计算机网络安全模型的核心特点
  - 对抗
    - 威胁 VS. 安全策略/机制
  - 变化
    - 威胁 / 安全策略/机制 / 环境





---

## 五、等级安全保护



## 等级安全保护的发展历史

---

- 橘皮书：TCSEC
- 红皮书：TNI
- ITSEC
- CC



- TCSEC, 1983, 美国国防部发表
  - 《可信计算机系统评估准则》
  - 计算机安全等级定义：4类7级
    - 无保护级：D
    - 自主保护级：C1、C2
    - 强制保护级：B1、B2、B3
    - 验证保护级：A1
  - TCSEC的评估目标只涉及了保密性，而没有涉及完整性和可用性的评估
  - 于2000年被废止



- TNI, 1987, 美国国防部, 基于TCSEC
  - 评估电信和网络系统
  - 加入了完整性评估
- ITSEC, 1995, 欧洲标准
  - 《信息技术安全评估准则》
  - 与TCSEC相比, 加入了完整性和可用性评估标准
  - 对目标的评估基于两个标准
    - 有效性和准确性
  - 分为功能等级 (F) 和保证性等级 (E)



## CC 准则

---

- 1993年6月，六国七方  
—加拿大、法国、德国、荷兰、英国、美国 NIST 及  
美国 NSA
- ISO 15408  
—CC 2.1版，1999年发布
- GB18336  
—《信息技术安全性评估准则》，2001年发布  
—中国版CC



## 我国等级保护现状

---

- 《信息安全等级保护管理办法》  
—公通字[2007]43号
- 《关于开展全国重要信息系统安全等级保护定级工作的通知》  
—公信安[2007]861号



## 等级保护的意义

- 明确安全需求
  - 资产在哪儿？价值多大？
- 安全防护是需要成本投入的
  - 信息安全与信息化建设要协调
- 安全建设和管理需要兼顾系统性、针对性、可行性
- 明确重点、突出重点、保护重点



---

## 六、计算机安全法规





# 我国信息安全相关法律法规总览

刑法修正案(七)在刑法第285条中增加两款(第二款、第三款):

违反国家规定,侵入前款规定以外的计算机信息系统或者采用其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,或者对该计算机信息系统实施非法控制,情节严重的,处三年以下有期徒刑或者拘役,并处或者单处罚金;情节特别严重的,处三年以上七年以下有期徒刑,并处罚金。

六. 2004年.....	9.3 境外组织和个人在华使用密码产品管理办法.....	102
6.1 中华人民共和国.....	十. 2009年.....	103
七. 2005年.....	10.1 刑法修正案(七)关于信息安全的修订与解读.....	111
7.1 互联网安全保护.....	10.2 深圳经济特区企业技术秘密保护条例.....	113
	十一. 2010年.....	113

提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,依照前款的规定处罚。



- 《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
  - 2011年6月20日最高人民法院审判委员会第1524次会议、2011年7月11日最高人民检察院第十一届检察委员会第63次会议通过
  - 自2011年9月1日起施行



- 网络与系统安全**攻防**实验必须严格限制在局域网范围内
- 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



## 本章内容小结

---

- 一. 专业术语定义
- 二. 威胁模型
- 三. 安全策略和安全机制
- 四. 计算机网络安全模型
- 五. 等级安全保护
- 六. 计算机安全法规



## 专业术语定义

---

- 资产 Asset
- 安全 Security
- 威胁 Threat
- 风险 Risk
- 漏洞 Vulnerability
- 影响 Impact
- 攻击 Attack



## 威胁模型

---

- STRIDE
- CVSS / CVE / CWE



## 安全策略和安全机制

---

- 术语定义
- 关系
  - 安全策略和安全机制
  - 安全假设和信任
- 安全假设的重要性



# 计算机网络安全模型

---

- 2种角度
  - 静态
  - 动态
- 安全模型的特点





## 等级安全保护

---

- 等级保护的必要性
- 等级保护的意義
- 等级保护的现状



- 知法守法



## 参考文献

- ① R. Shirey, Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards, Internet Draft: draft-irtf-psrg-secarch-sect1-00.txt (Nov. 1994).
- ② The STRIDE Threat Model. [http://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx) (2002)
- ③ 使用STRIDE发现安全设计缺陷. <http://msdn.microsoft.com/zh-cn/magazine/cc163519.aspx> (2006.11)
- ④ Threat Risk Modeling, OWASP. [https://www.owasp.org/index.php/Threat\\_Risk\\_Modeling](https://www.owasp.org/index.php/Threat_Risk_Modeling)
- ⑤ 电子银行安全评估方案, 启明星辰. <http://www.venustech.com.cn/NewsInfo/423/9199.Html> (2011.1)
- ⑥ 大成天下: 《中国信息安全相关法律法规汇编》 (2011.6.26)
- ⑦ 通用弱点评价体系 (CVSS) 简介 <http://www.xfocus.net/articles/200602/850.html>



## 课后思考题

- 以下行为分别破坏了CIA和AAA中哪一个属性或多个属性?
  - 小明抄小强的作业
  - 小明把小强的系统折腾死机了
  - 小明修改了小强的淘宝订单
  - 小明冒充小强的信用卡账单签名
  - 小明把自己电脑的IP修改为小强电脑的IP，导致小强的电脑无法上网



## 课后思考题

- 有一次，小明口袋里有100元，因为打瞌睡，被小偷偷走了，搞得晚上没饭吃。又一天，小明口袋里有200元，这次小明为了防范小偷，不打瞌睡了，但却被强盗持刀威胁抢走了，搞得一天没饭吃，小明当天就报警了。
  - 试分析两次失窃事件中的：风险、资产、威胁、弱点、攻击、影响
  - 试用P2DR模型分析以上案例中的“现金被抢”事件中的安全策略、安全防护、安全检测和安全响应
  - “被抢”事件中，小明的安全策略存在何问题？



## 课后思考题

- 针对下述论点，分别设计一场景案例（必须和课程相关），使得该论点在该场景中成立
  - 预防比检测和恢复更重要
  - 检测比预防和恢复更重要
  - 恢复比预防和检测更重要



## 课后思考题

- 试分析“CAPTCHA图片验证码技术可以阻止恶意批量注册行为”这句话中的安全策略、安全机制和安全假设分别是什么？CAPTCHA图片举例

邮件地址，以便我们可以及时和你联系。

计算  
E码：

设  $a, b \in \mathbf{R}$  集合  $\{1, a+b, a\} = \left\{0, \frac{b}{a}, b\right\}$ ，则  $b-a =$

在这里输入  [想知道答案](#)

以上所有信息都必须先正确填写后才能继续下一步注册操作。



## 课后思考题

- 某大型软件开发公司的总裁担心公司的专利软件设计方法被内部员工泄露给其他公司，他打算防止泄密事件的发生。于是他设计了这样一个安全机制：所有员工必须每天向他汇报自己和其他竞争对手公司员工的所有联系(包括IM、电子邮件、电话等等)。你认为该安全机制能达到总裁的预期安全效果吗？为什么？