



信息安全导论

第二章 信息安全基础

黄 玮

中国传媒大学



温故

- 信息安全专业课程体系概述
- 信息与信息技术基础
- 信息化发展与现状
- 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
- 我国信息安全保障现状



知新

- 信息系统安全要素
- 网络安全基础
- 信息安全保障体系
- 信息安全技术框架



提纲

- 信息系统安全要素
- 网络安全基础
- 信息安全保障体系
- 信息安全技术框架



基础概念

- 使命

- 企业的信息化“需求”

- 一个组织通过信息技术手段实现的工作任务
 - 信息化程度越高，信息资产价值越高，信息系统安全就越重要

- 资产

- 有形资产 && 无形资产

- 通过信息化建设积累起来的信息系统、信息、生产或服务能力、人员能力和赢得的信誉等



基础概念

• 威胁

—可能破坏安全基本要素的**来源**或原因

- 一个组织的信息资产的安全可能受到的侵害
- 多种属性，包括威胁的主体（来源）、能力、资源、动机、途径、可能性和后果

—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**

—内部威胁VS.外部威胁 / 自然威胁VS.人为威胁



微软STRIDE模型

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



其他威胁模型

- 见参考文献
 - 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）



基础概念

- 脆弱性

- 又称漏洞或弱点

- 信息资产及其安全措施在安全方面的不足和弱点

- 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



基础概念

- 事件

- 漏洞被利用，产生安全事件

- 如果威胁主体能够产生威胁，利用资产及其安全措施的脆弱性，那么实际产生危害的情况称为事件



基础概念

• 风险

- 风险是威胁事件发生的**可能性**与影响综合作用的结果
 - 由于系统存在的脆弱性，人为或自然威胁导致安全事件发生的可能性及其造成的影响
- 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



基础概念

- 残余风险
 - 安全机制实施之后仍然遗留的风险
- 安全需求
 - 信息系统安全建设需求
- 安全措施
 - 安全策略和安全机制的统称
 - 对抗威胁，减小脆弱性，保护资产，降低意外事件的影响，检测、响应意外事件，促进灾难恢复和打击信息犯罪而实施的各种实践、规程和机制的总称



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



安全假设和信任

- 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



安全假设和信任

- 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



安全机制的内涵

- 符号定义

- P: 实施安全机制前系统所有的可能状态

- Q: 系统所有的安全状态（由安全策略定义）

- R: 实施安全机制后系统所有的可能状态

- 安全机制的三种等级

- 安全: $R \subseteq Q$

理想 —精确: $R = Q$

现实 —宽泛: $r \in R \wedge r \notin Q$



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”？



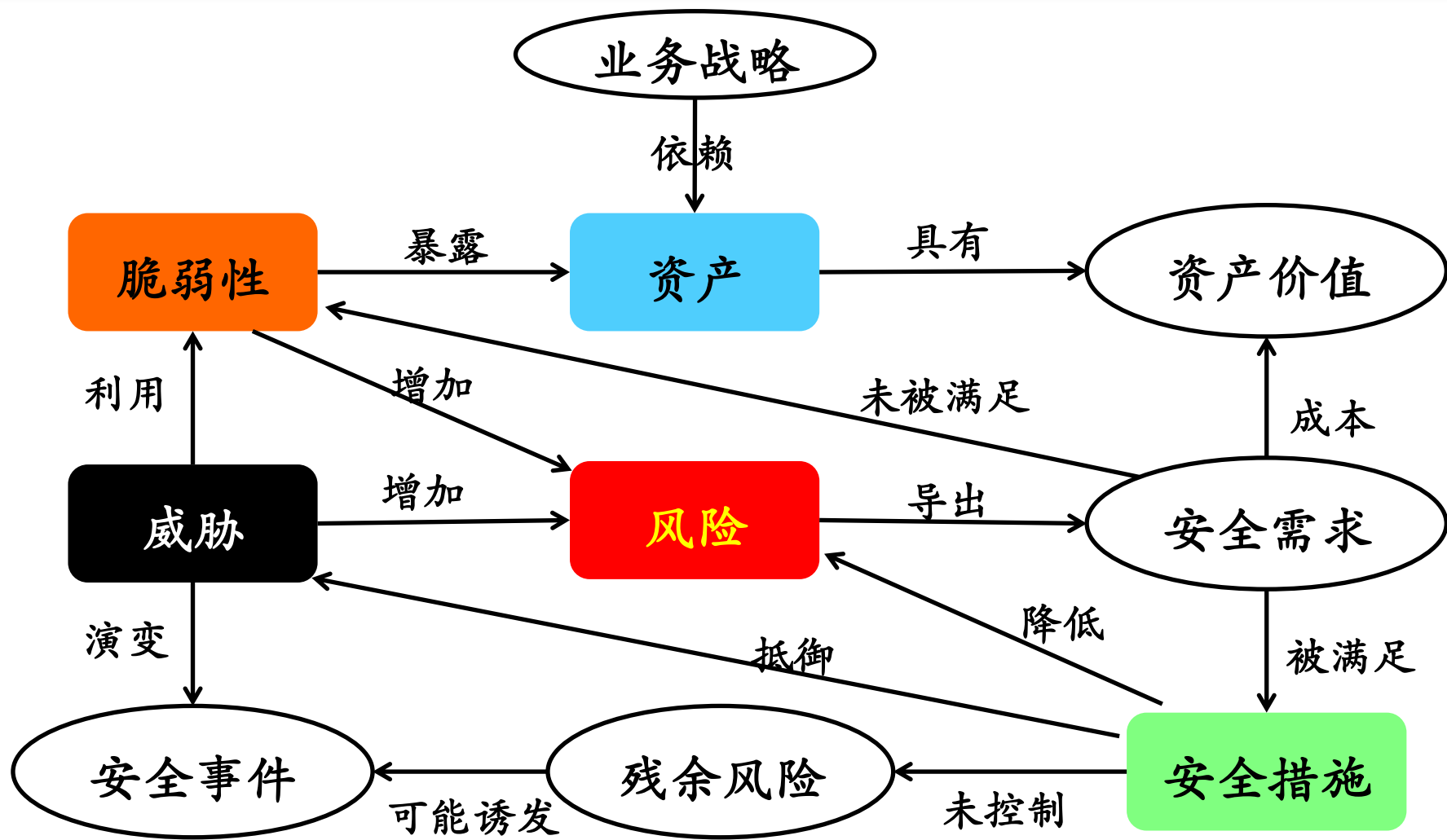
基础概念

- 攻击

- 由威胁源所实施的、导致安全事件发生的行为
- 漏洞利用的过程
- 实现威胁
- 攻击得手会造成影响



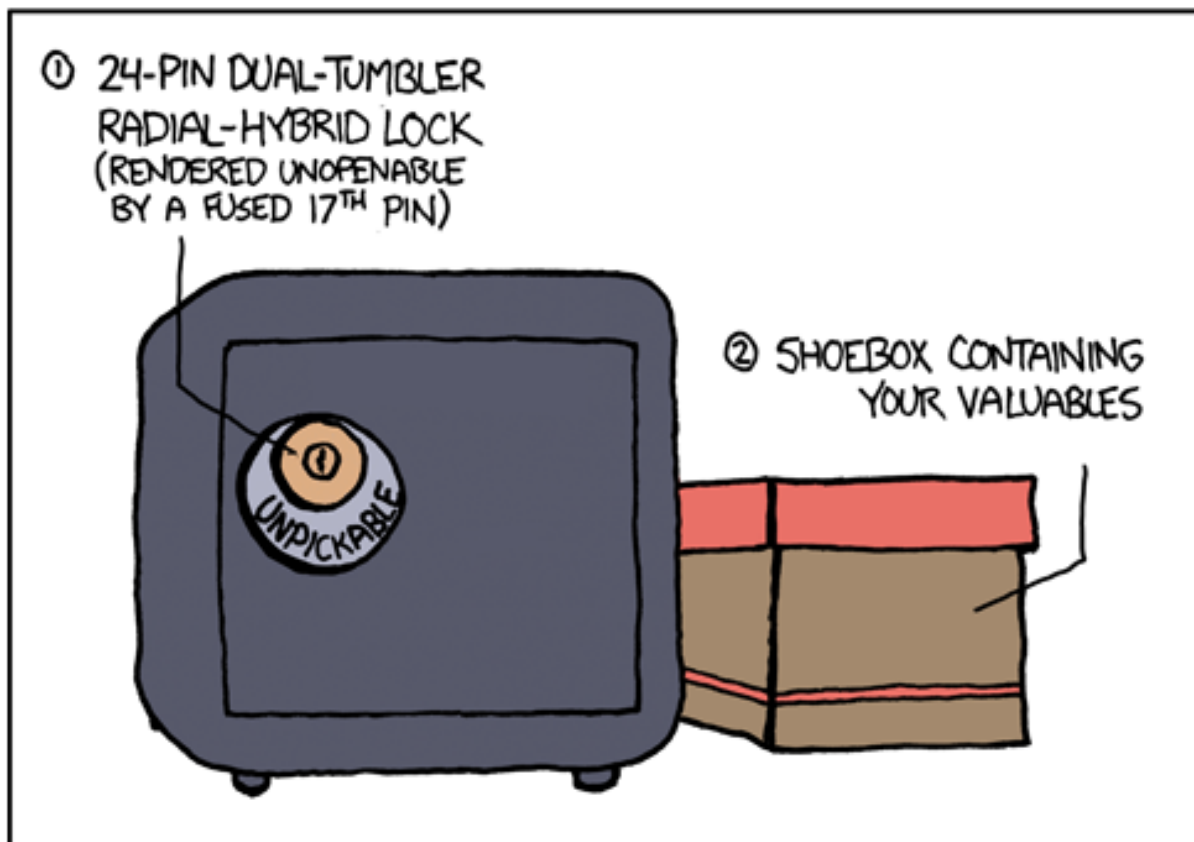
我国国家标准给出的信息系统各要素间关系





信息安全建设中正确评估资产价值的重要性

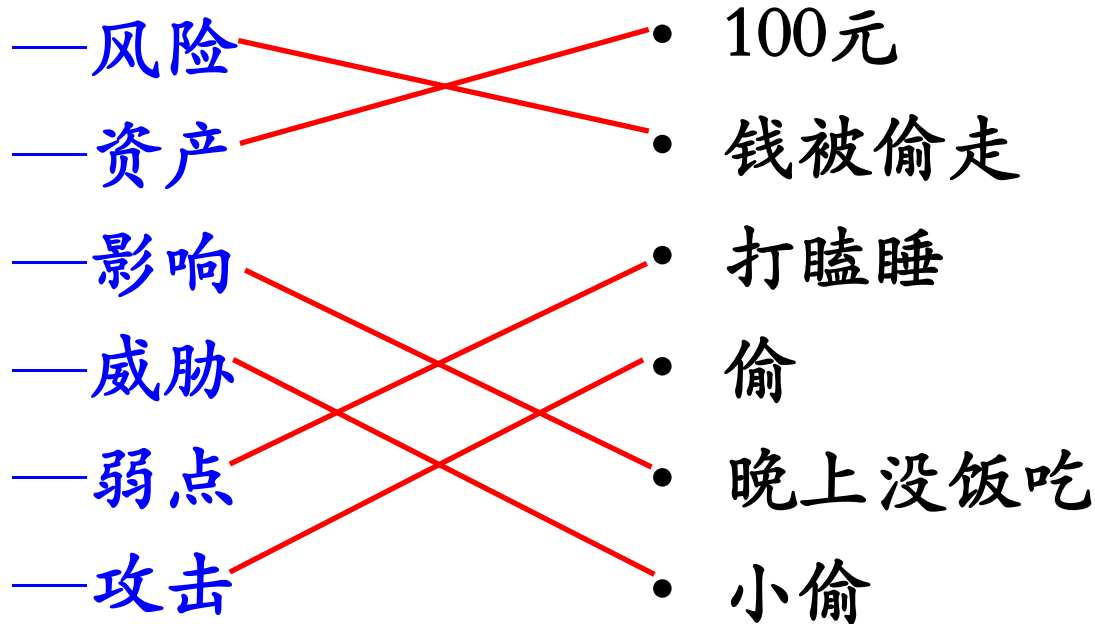
HACKER SHIELD GEEK-PROOF SAFE SYSTEM:





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

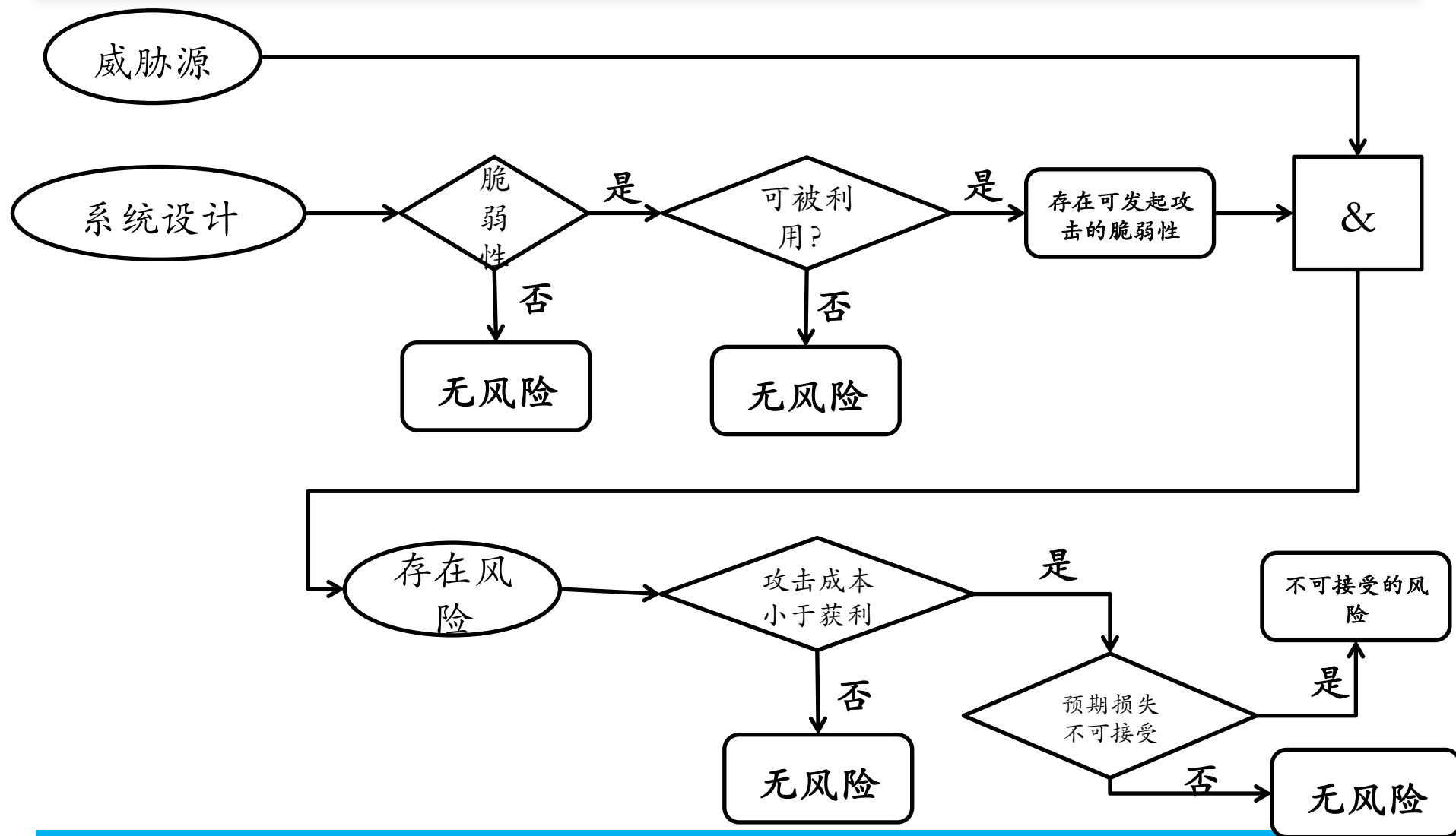


信息安全风险控制

- 风险降低
 - 实施安全措施，把风险降低到一个可接受的级别
- 风险承受
 - 接受潜在的风险并继续运行信息系统
- 风险规避
 - 通过消除风险的原因和/或后果（如在发现风险后放弃系统某项功能或关闭系统）来规避风险，即不介入风险
- 风险转移
 - 通过使用其他措施来补偿损失，从而转移风险，如购买保险
- 分散风险
 - 异构化信息系统
 - 重要信息资产分散在多个异构系统



风险控制的实施点





提纲

- 信息系统安全要素
- 网络安全基础
- 信息安全保障体系
- 信息安全技术框架



网络安全基础

- 先修知识：ISO/OSI参考模型
— 计算机网络

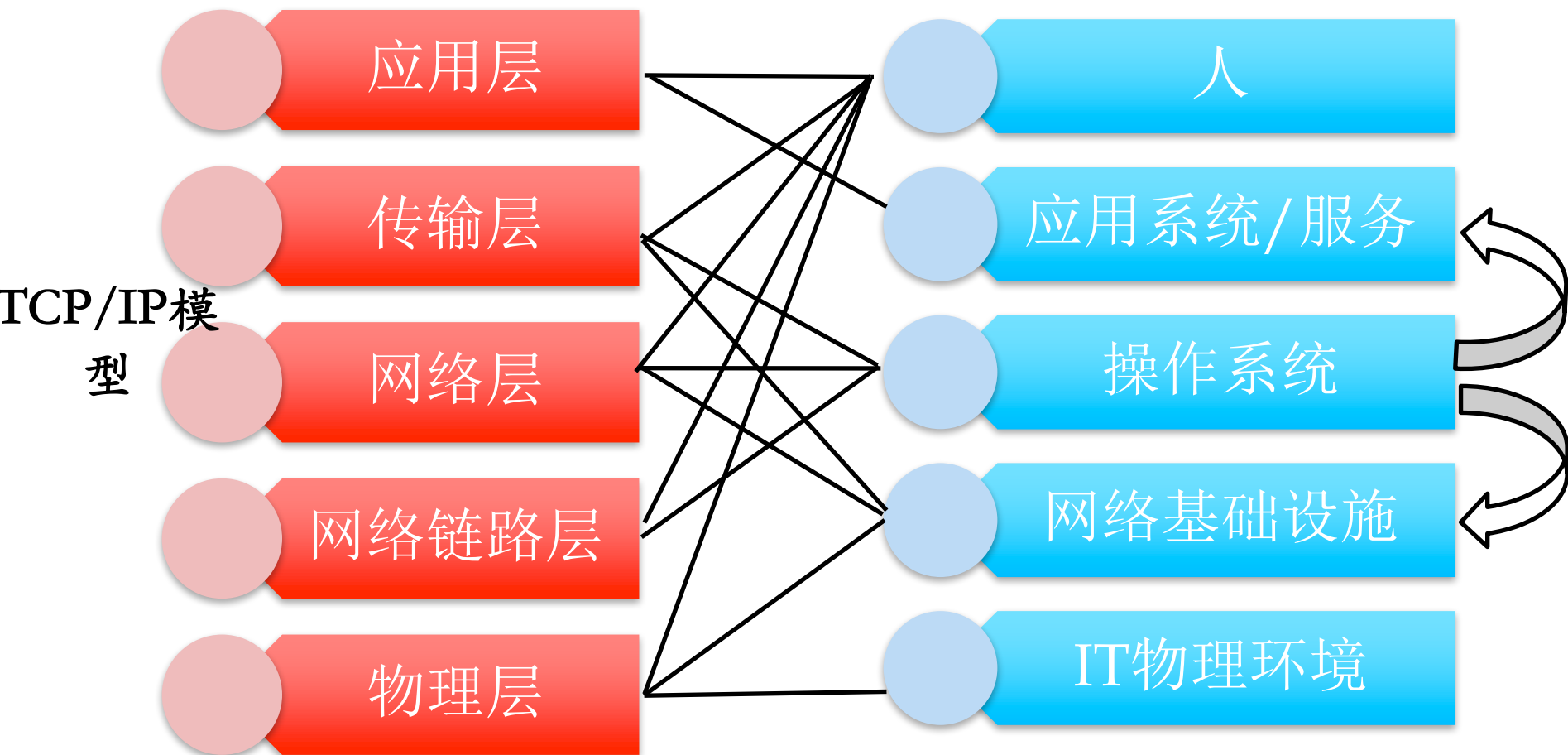


2种模型

- 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)





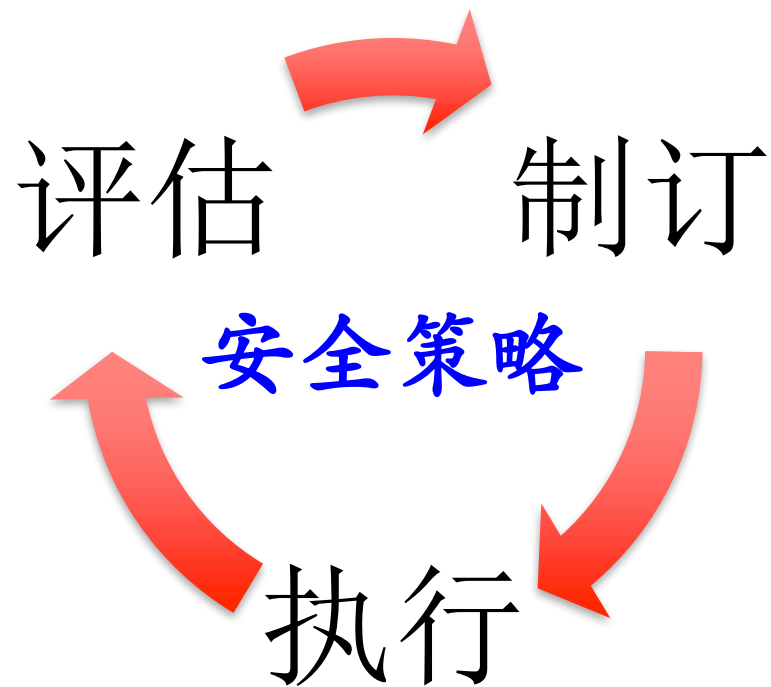
再论安全策略

- 安全策略的体系化

—制订

—执行

—评估





安全防护

- 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



安全响应

- 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



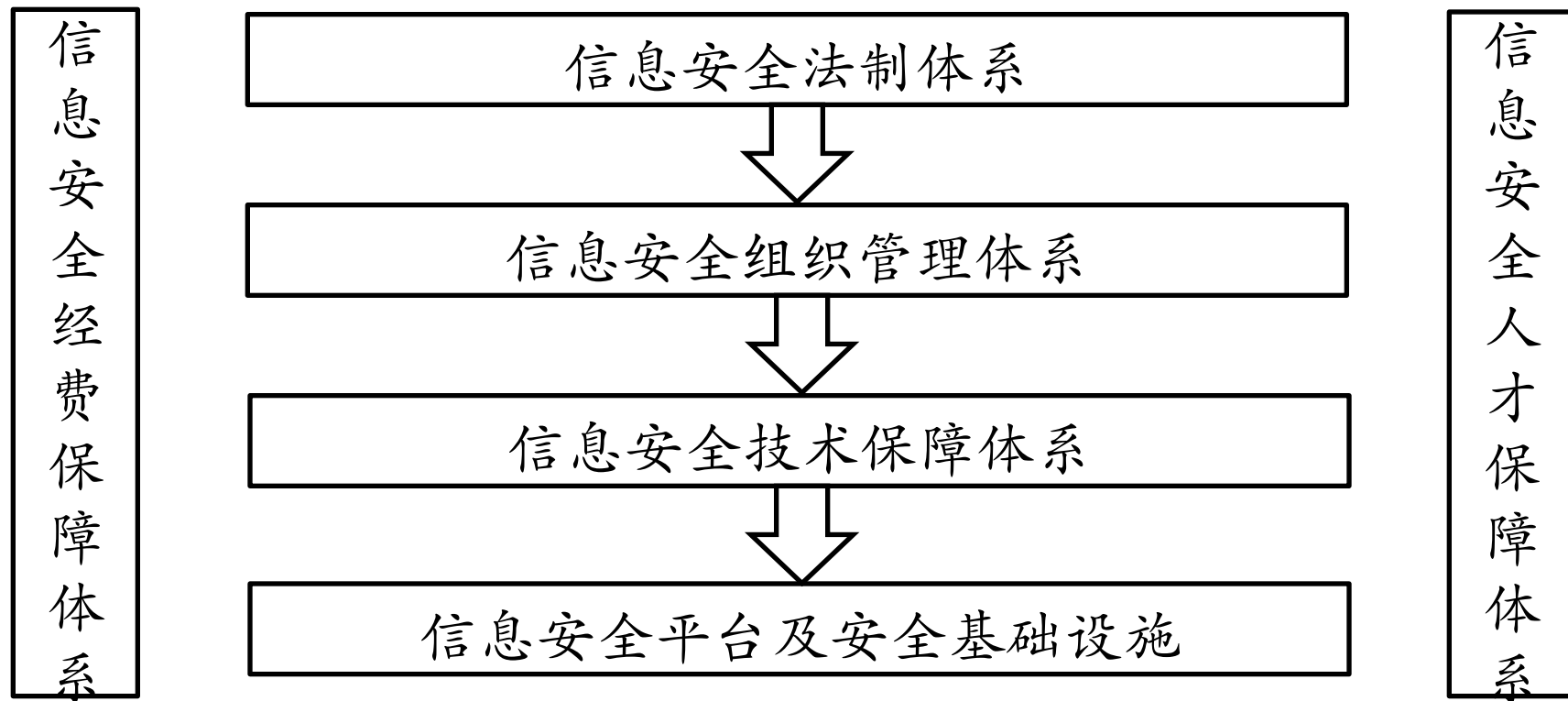
提纲

- 信息系统安全要素
- 网络安全基础
- 信息安全保障体系
- 信息安全技术框架



信息安全保障体系

一个重点确保，四个层面，两个支撑



基础信息网络和重要信息系统

中国传媒大学



提纲

- 信息系统安全要素
- 网络安全基础
- 信息安全保障体系
- 信息安全技术框架



对当前信息安全保护思路的反思



防外为主，边界防御



防内为主，内外兼防

——纵深防御

——等级安全保护

——安全是信息系统的基本属性



“两个中心”支持下的三重信息安全技术保护框架

- 一般信息系统的基本组成

- 操作应用

- 面向客户端（用户）

- 共享服务

- 面向服务端

- 网络通信



“两个中心”支持下的三重信息安全技术保护框架

• 复杂互联系统的信息安全防护框架

—三纵

- 涉密区域、专用区域、公共区域
- 采用安全隔离与信息交换设备进行连接

—三横

- 应用环境、应用区域边界、网络通信

—两个中心

- 安全管理中心、密码管理中心



信息安全科普之意识和行动

中国传媒大学



提纲

- 安全常识
- 社交媒体使用守则
- 常用软件
- 不可忽视的细节



图标说明



• 危险意识/行为



• 科普意识/行为



• 提倡意识/行为



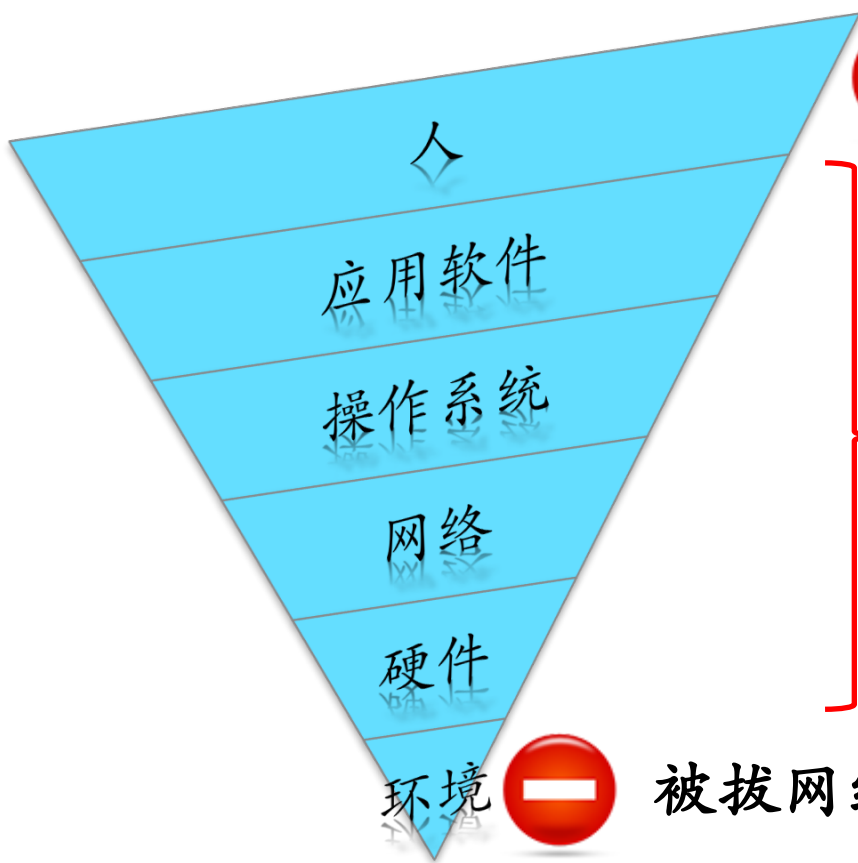
安全常识

- 安全的本质是持续对抗
 - 自动更新
 - 使用最新版软件
- 安全防御的倒金字塔现象和木桶原理
- 天上不会掉馅饼
 - 无事献殷勤：非奸即盗
- 保密原则
- 千里之堤毁于弱口令



安全防御的倒金字塔现象

• 底层安全程度决定上层安全的稳固性



弱口令/记住口令功能/无视安全警告
用Excel、Word、记事本管理密码
用QQ、电子邮件发送口令



自动更新



使用最新版软件

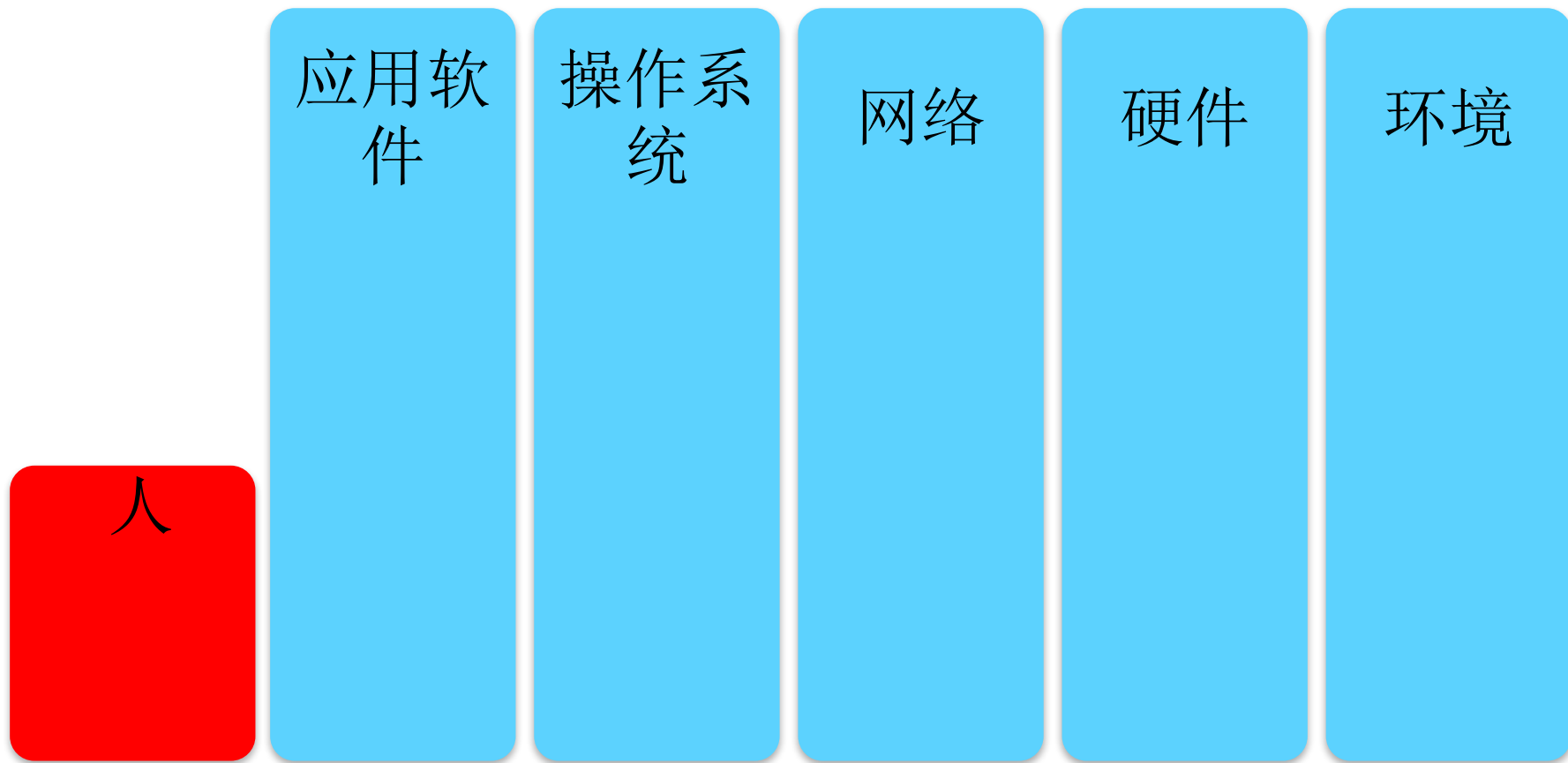


被拔网线/外来人员的偷拍











安全防御的木桶原理

- 整体安全防御的能力高低取决于最短板的**长度**





天上不会掉馅饼

-  • 恭喜您，中奖了！
 -  —“把你公司的员工通讯录发给我吧”
 -  —“这是礼品目录，下载查看吧”
-  • 恭喜您获得了我们公司的试用体验机会
 -  —“我们将派工作人员上门登记你们公司的员工信息，以便准备足够数量的试用套装”
-  • XXX大优惠
 -  —话费冲300返600
 -  —10MB带宽XXX元



保密原则

- 我借用一下你们公司的
 - 电脑 / 无线网络 / 有线网络
- 公司内任何形式的资料未经允许
 - 不得对外传播
 - 不得私自携带外出
 - 不得私自存储和备份
 - 纸质文件
 - 源代码/电子文档/会议纪要/电子邮件/产品概念图/研发计划/薪酬待遇…



千里之堤毁于弱口令 (1/4)

- 你在用这些弱口令吗?



—手机号



—公司/住宅电话号码



—生日



—123456 / 888888 / 1qaz2wsx / asdf

- 你的口令都是怎么记忆的?



—使用软件自带的“记住密码”功能



—新建一个文本文件



—记在一个本子上



千里之堤毁于~~弱口令~~ (2/4)

- 强口令就真的很强吗?
 - ba1f2511f
 - 手机号+手机号
 - 手机号+生日
- 如果你的人人网账号被盗，你的QQ账号还保得住吗?
 - 单一口令也是弱口令



千里之堤毁于弱口令 (3/4)

- 口令是信息安全的安全底座
 - 口令被盗即意味着安全大厦的根基被毁
- 口令的强度和记忆难度的平衡
 - 无规则随机产生的口令是无法记忆的
 - 记忆友好强口令产生规则
 - 使用短语/长句（拼音首字母/全拼）
 - 一系列人名/古诗词等等
 - 使用独立口令
 - 使用更“安全”的密码管理软件
 - 自定义一套不同站点/应用的口令派生规则



千里之堤毁于~~弱口令~~ (4/4)

- 口令被盗的原因

- 主机中病毒/木马

- 键盘输入截获
- 软件“已保存/已记住”的口令被解密/提取

- 被“钓鱼”

- 口令的网络传输使用明文

- 第三方站点/应用被黑客攻陷

- “加密”口令被黑客解密
- 黑客使用A站点解密出的用户名+口令组合去尝试登录B/C/D…站点/应用



强口令很了不起吗？

• 找回口令功能

— 密码提示问题



— 你爸爸/妈妈的名字？



— 你高中时的学校名字？



— 你的第一任班主任姓名？



— 你是如实回答以上问题的吗？

— 发送口令重置链接到你的邮箱

— 你的邮箱口令也是强口令吗？

你的邮箱的找回口令功能足够安全吗？

...



社交媒体使用守则

- 禁言

- 不要发布不为公众所知的和公司相关的业务数据
- 团队的内部规划，正在进行的项目及相关实施细节，未经相关负责人允许也尽量不要披露

- 慎言

- 不要匿名攻击公司(包括自己的雇主和竞争对手)
- 微博上的信息具有不可修改性，被转发后会引来不同的解读

- 公关

- 必要的时候尽可能转发对用户的警示信息
- 抓住每一个营销和推广产品的机会进行正面宣传和引导



常用软件

- 浏览器
- 办公软件
- 即时通讯
- 电子邮件
- 下载和安装软件
- 安全软件



浏览器



- 记住口令功能



- URL



- 地址栏



- 页面内的链接

——短网址



- 使用现代浏览器





浏览器——记住口令功能

- 黑客可以从浏览器中提取出保存的口令
- 禁用浏览器的口令保存功能
- 删除已经保存的口令
- 定期清空所有浏览历史记录数据



办公软件 (1/2)

- 微软Office系列
 - 禁用宏
- PDF
 - 使用第三方PDF阅读器
 - Foxit
- 不打开来历不明的文档
- 不要被“图标”迷惑
 - 应用程序图标是可以被伪造的
 - 一个具有Word图标的文件可以是.exe伪装的



办公软件 (2/2)

- 不要被“扩展名”迷惑
 - 使用大量空格填充可以轻松“伪造”任意扩展名
 - 如果再使用自定义的文件“图标”呢?

内部资料.doc

... 2011/12/12 10:57 TXT 文件

0 KB

- 通过异常的文件大小来识别一些恶意文档
 - 3MB的简历文档（正常简历大小在50KB左右）
- 使用Web版邮箱中的在线查看文档功能
 - 尽量不要下载简历后在本地打开查看



即时通讯——QQ

- 视频欺诈
- 恶意文件
- 恶意链接
- 不和陌生人说话
- 熟人之间不谈“不熟”之事
——借钱/询问口令/询问帐号



电子邮件

- 钓鱼邮件
 - 伪造发信人
 - 伪造内容
 - 邮件发信人昵称/邮件标题/邮件正文
- 邮件附件中的病毒和木马
- 重要资料不通过邮件发送和讨论
 - 内网传输和讨论
- 重要行动前，电话/当面再确认行动内容
 - 收到陌生邮件通知：“XXX，我更换了邮箱地址，请惠存”



下载和安装软件



- 国内下载站



- 内部下载站



- 使用XX卫士的软件管家
——一站式安装



- 卸载不再使用的软件



安全软件



- 多多益善



- 病毒库越大越好



- 核心功能必须有

- 卫士功能

- 系统和常用软件的安全补丁自动安装功能

- 系统体检（了解你的电脑的风险等级）

- 杀毒和卫士功能分离



不可忽视的细节(1/3)

- 随手关门
- 门禁卡请保证仅限本人使用
 - 不得借予外人
 - 不得随意借予同事
- 不要在U盘上长期存放公司资料
 - 定期清理和格式化U盘
- 公司保密资料存放
 - 入柜加锁
 - 涉密资料不随身



不可忽视的细节(2/3)

- 公开WIFI慎连
——WIFI钓鱼
- 文件共享
——少用移动存储介质
——优先选择内网
 - FTP
 - 飞鸽传书
- 口令共享
——口传言授不留凭据

LAN口状态

MAC 地址:	40-16-9F-65-A4-D6
IP地址:	192.168.1.1
子网掩码:	255.255.255.0

无线状态

无线功能:	启用
SSID号:	CMCC
信道:	自动 (当前信道 1)
模式:	11bgn mixed
频段带宽:	自动
MAC 地址:	40-16-9F-65-A4-D6
WDS状态:	未开启

WAN口状态



不可忽视的细节(3/3)

- 电脑前无人时及时锁屏
- 禁用Windows的文件夹共享功能
 - 关闭Windows的默认共享服务
- 避免在公司电脑上使用外来U盘和移动存储介质
 - 必须使用时务必先杀毒，后打开
- 不在陌生人电脑上输入口令
 - 不确定对方电脑环境的安全程度
- U盘使用完后及时从电脑上拔除



参考文献

- ① 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)
- ② 使用STRIDE发现安全设计缺陷. <http://msdn.microsoft.com/zh-cn/magazine/cc163519.aspx> (2006.11)
- ③ Threat Risk Modeling, OWASP.
https://www.owasp.org/index.php/Threat_Risk_Modeling
- ④ 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
- 举一例说明破坏机密性可以导致完整性也被破坏



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？该安全机制是精确的？安全的？还是宽泛的？简述理由。

—CAPTCHA图片举例

邮件地址，以便我们可以及时和你联系。

计算
[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。

提交注册信息



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？



课后思考题

