网络安全

第一章 网络安全基础

黄 玮

关于课程你需要了解…

课程概况

- 上课地点/时间
  - —讲授&实验：48教 B907
  - —周五 3-4节、5-6节
- 答疑地点/时间
  - —A101E 周一到周五白天
  - —邮箱：i@huangwei.me

课程概况

- 先修课程
  - — 计算机安全与维护
  - —计算机网络A
  - —密码学应用实践（推荐）
- 推荐教材
  - — https://sec.cuc.edu.cn/huangwei/textbook/ns (alpha)
- 硬件和软件环境
  - —PC
  - —Linux (Kali)

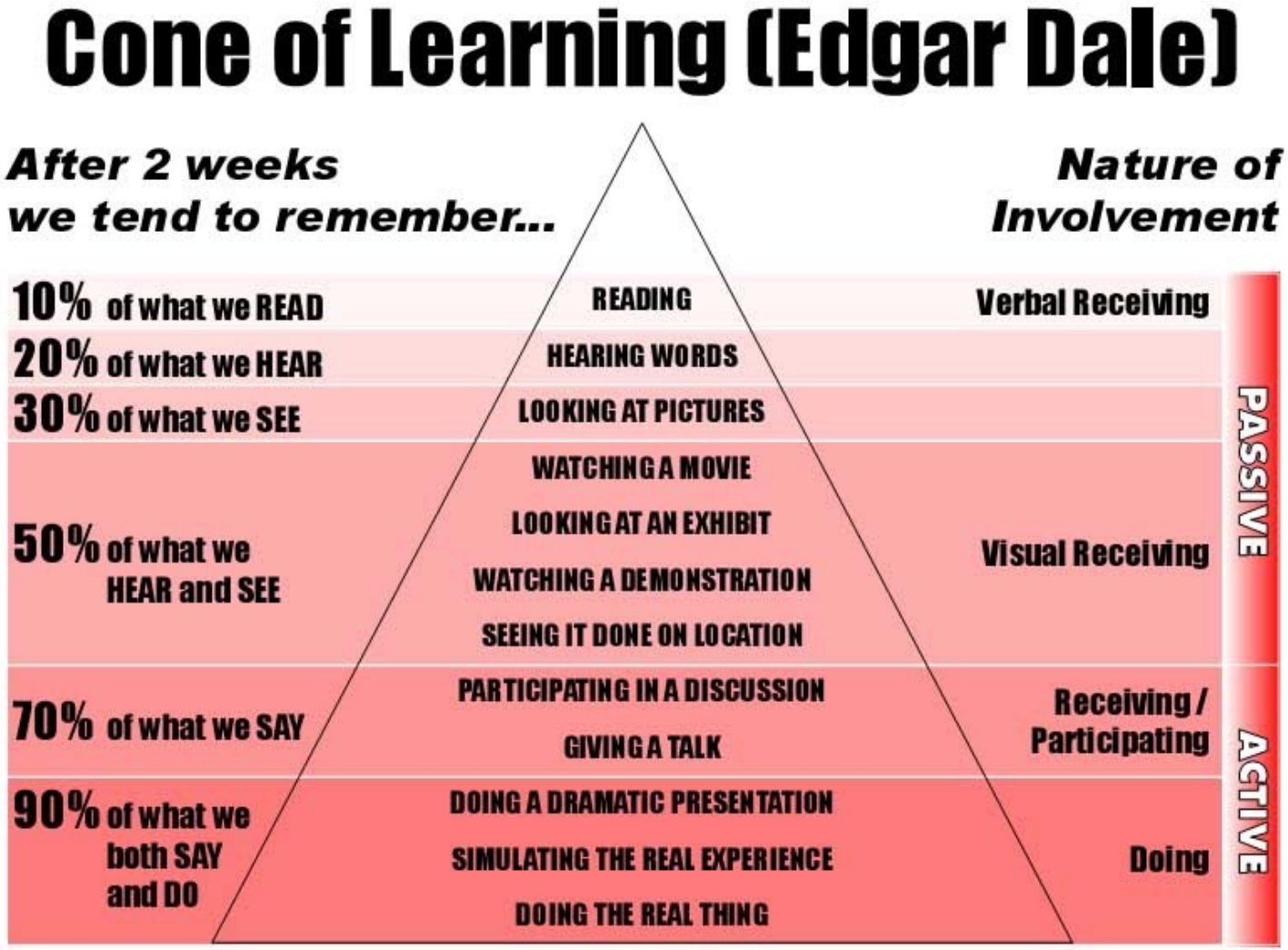
在线资源

- https://sec.cuc.edu.cn/huangwei/wiki

关于课程的教、学方法和原则

- 教
  - 授人以渔
    - 重思路、方向讲解，轻傻瓜式重复
- 学
  - 兴趣第一
  - 尽信师，不如无师：质疑、思考、实践
  - 会用、用好互联网，特别是“搜索”
  - 一定要亲自动手实践

学习金字塔



教授给他人
模拟实践
实践

引用美国教育学家艾德格·戴尔（Engar Dale）于1969年设计的“学习金字塔”

遗忘金字塔

两周后我们大概记得什么		涉及本质
我们说过和做过的事记得 90%	实际做事 模拟实际经验 做一场引人注目的演讲	主　动
我们说过的事记得 70%	做正式的演讲 参与讨论 当场看到事情完成	被　动
我们听过和看过的事记得 50%	观看示范说明 看展览示范 看电影	
我们看过的事记得 30%	看图片	
我们听过的事记得 20%	听讲	
我们读过的事记得 10%	阅读	

重要的事情说三遍

- 主动学
- 主动学
- 主动学
- 主动做
- 主动做
- 主动做
- 主动讲
- 主动讲
- 主动讲

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

计算机网络安全基础	网络监听与扫描	网络与系统渗透	网络与系统防御
实验上机：2学时 讲授：6学时	实验上机：4学时 讲授：6学时	实验上机：4学时 讲授：8学时	实验上机：6学时 讲授：12学时

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 网络安全基础

本章内容提要

一.专业术语定义（回顾）

二.威胁模型

三.安全策略和安全机制（回顾）

四.融合网

五.计算机网络安全模型

六.等级安全保护

七.计算机安全法规

一、专业术语定义

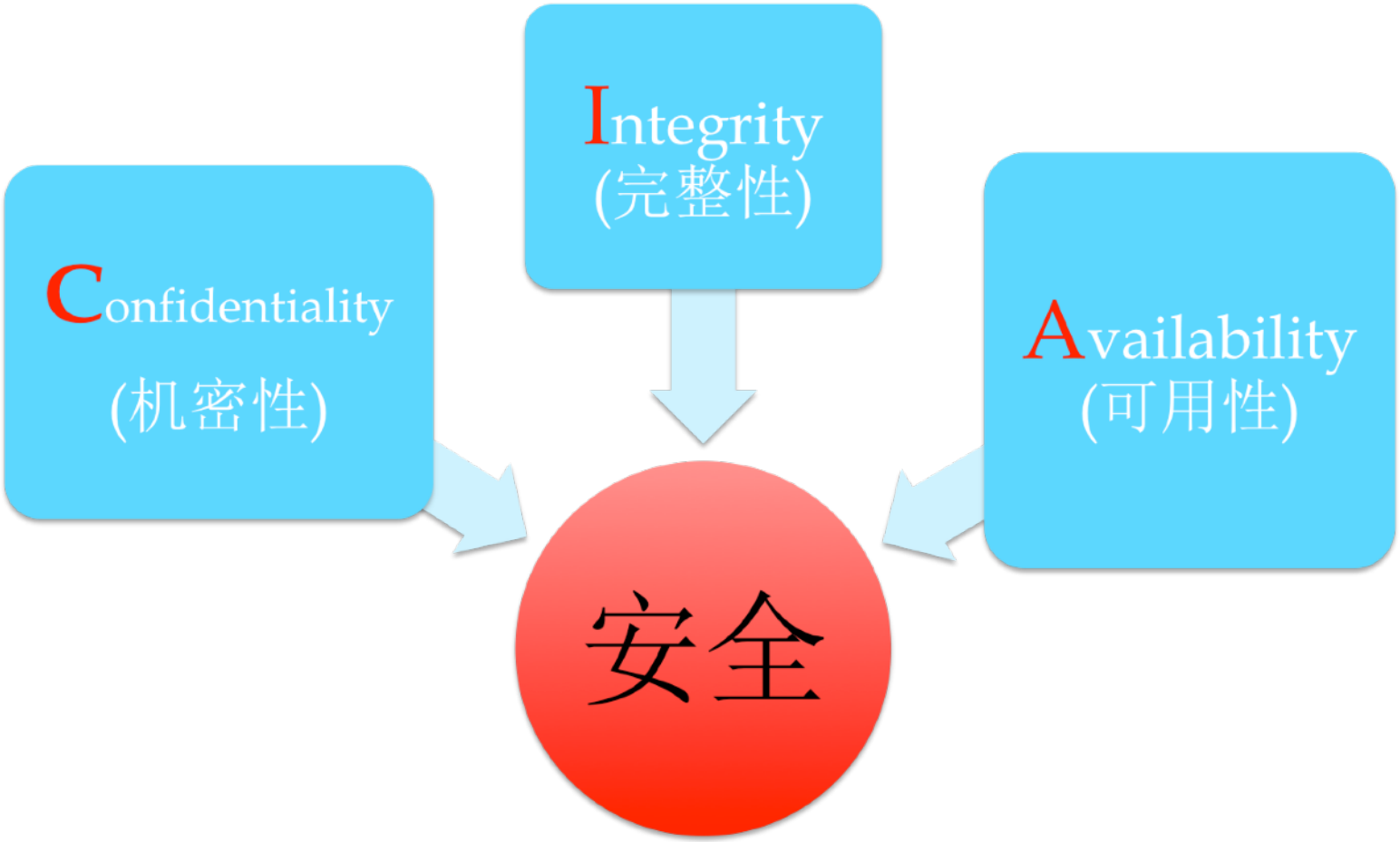
术语定义

- 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
- 漏洞研究是信息安全所有研究的内核

风险是什么

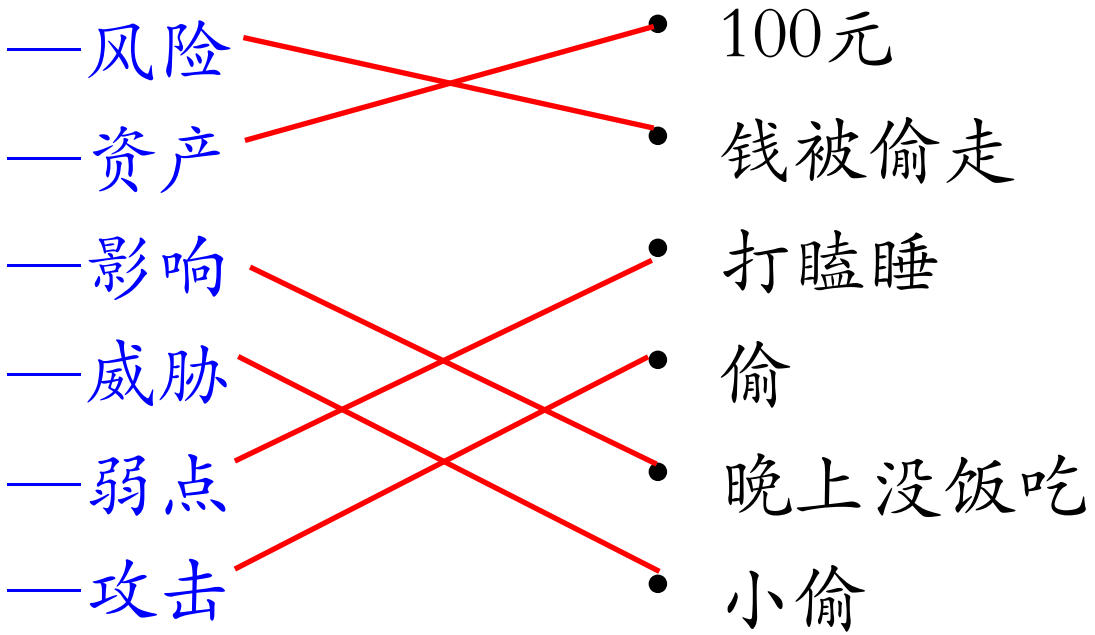
- 风险是威胁事件发生的可能性与影响综合作用的结果
- 风险成为事实后，就会造成具体的影响
  - —机密数据被窃
  - —网页被篡改
  - —网站被拒绝服务攻击所瘫痪

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

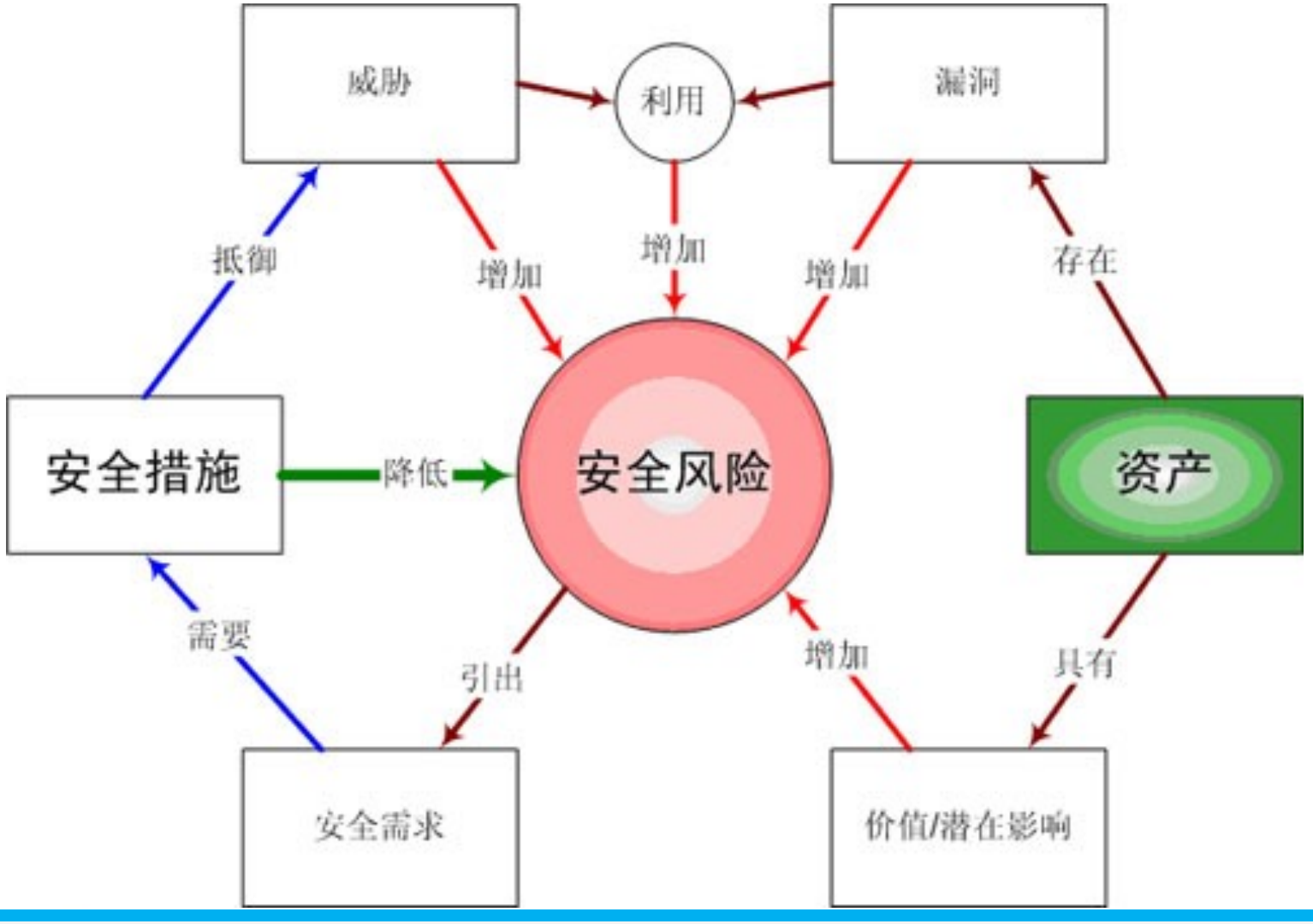
- 小明口袋里有100元，因为打瞌睡，被小偷偷走了，导致小明晚上没饭吃



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 (Spoof)	认证 (Authentication)
篡改 (Tamper)	完整性
否认 (Repudiation)	不可抵赖性
信息泄露 (Information Disclosure)	机密性
拒绝服务 (Denial of Service)	可用性
提升权限 (Elevation 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

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 (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条件下，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条件下，不使用钥匙也打开了该门

实现了“漏洞利用”

信息世界中的“信任”

- 下载软件并安装
- 编译代码并运行
- 打开Office文档
- 打开网页
- 查看邮件
- 查看视频
- 加入局域网

- 信任软件作者和分发渠道
- 信任代码作者
- 信任文档作者和来源
- 信任网站主
- 信任发信人
- 信任视频来源
- 信任网络中的其他使用者

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

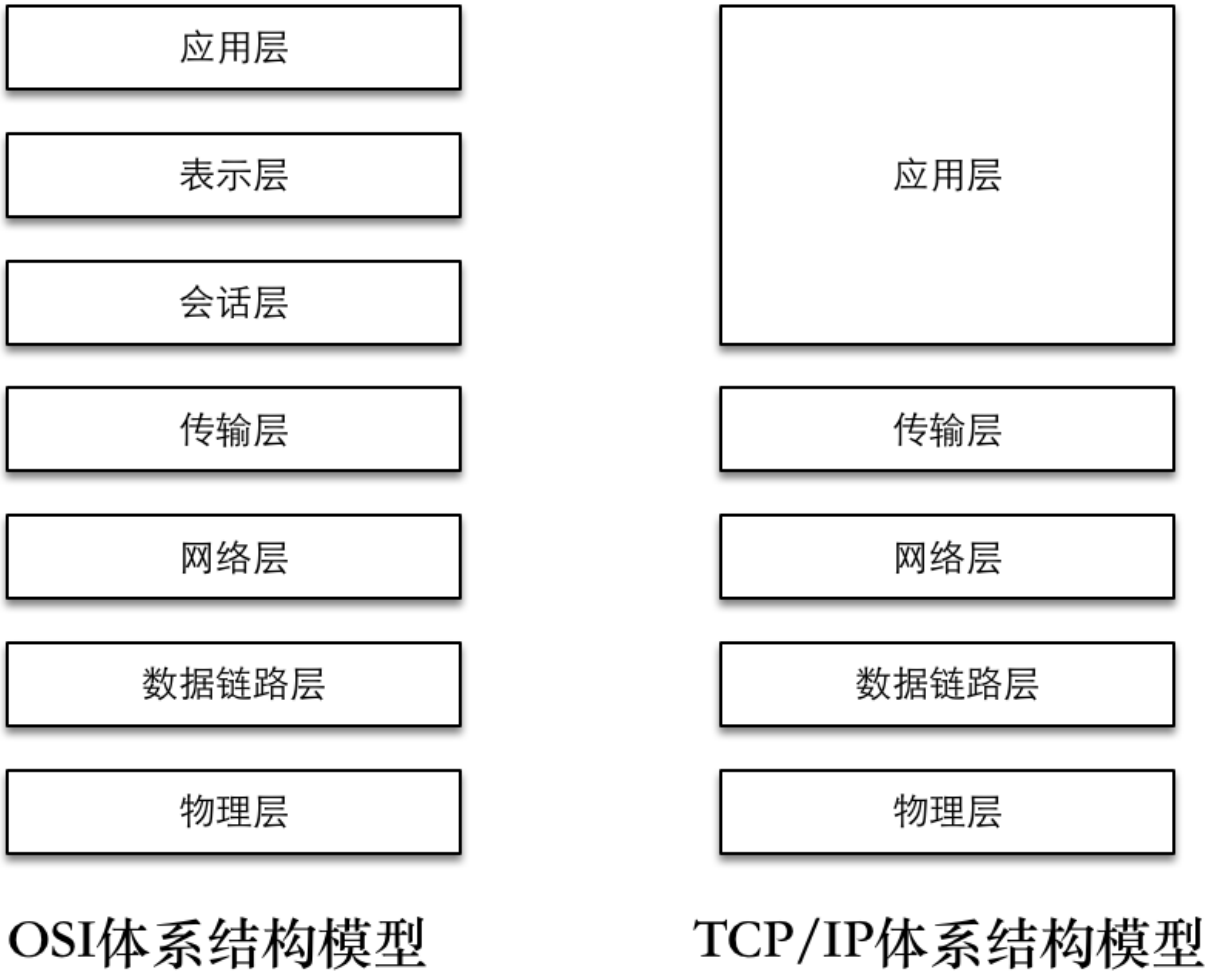
- 每一个安全机制都是被设计用来实现安全策略中的一个或多个具体策略
- 安全策略的集合能够实现所有的安全策略
- 安全机制的实现是正确的
- 安全机制的部署和管理是正确的

如果安全假设为假，
谈何“网络安全”？

四、融合网

术语

- 融合网的概念来源于网络融合（Network Convergence），国际上有据可查的针对网络融合的法案始于美国的《1996年电信法》（Telecommunication Act of 1996）
- 三网
  - 电信网、广播电视网（以下简称广电网）和计算机网（事实代表是：互联网）


应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
OSI体系结构模型
应用层
传输层
网络层
数据链路层
物理层
TCP/IP体系结构模型

电信网络 VS. 计算机网络

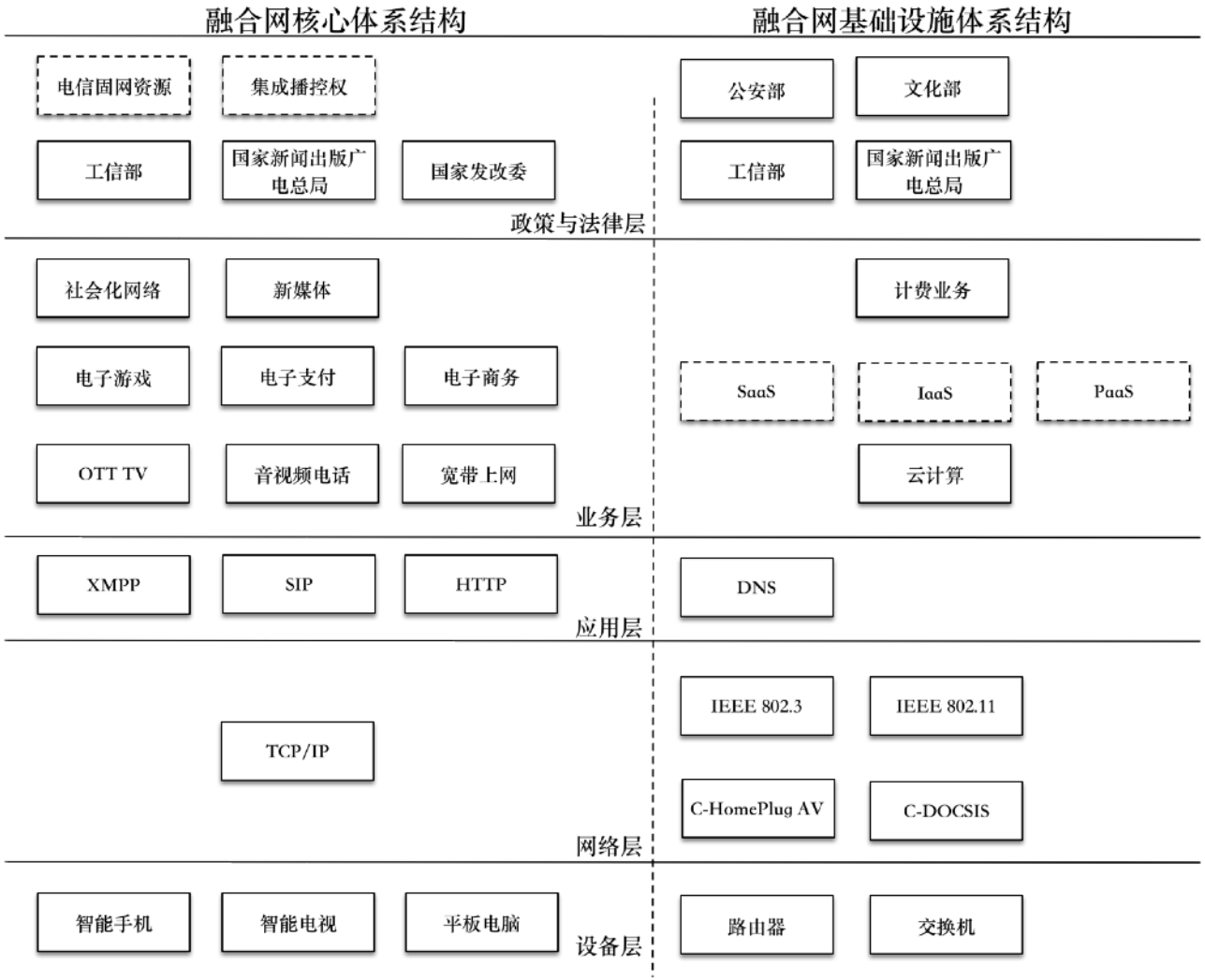
	电信网	计算机网
终端	傻瓜化	智能化
管理方式	集中管理	自治管理
通信模式	物理链路交换	分组交换
服务质量	有保障的传输质量和业务连续性	尽力而为传输

通信4.0：通过“软件化”实现通信网络的降本增效，通过“开放化”实现通信网络的价值提升，全面数字化服务

广电网 VS.（电信网 && 计算机网）

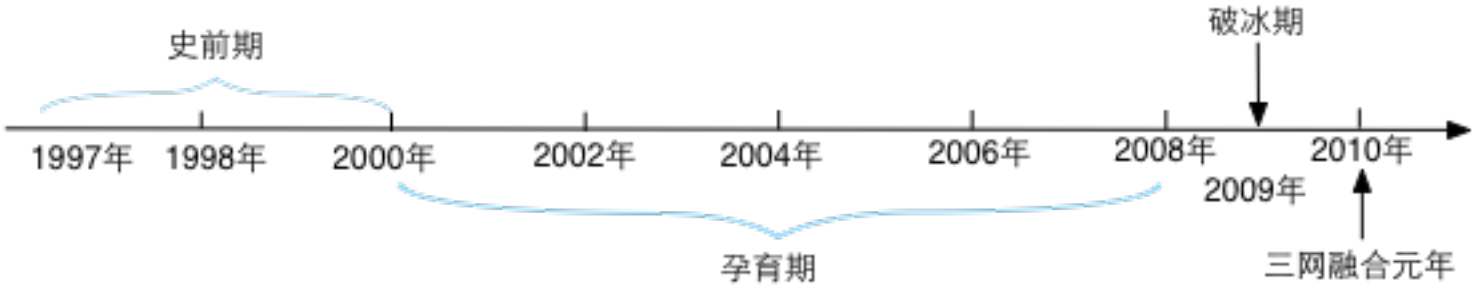
- 单向广播
  - 经过三网融合改造升级之后，目前大部分地区的广电网络实现了双向通信
    - 模拟化 —》数字化
    - 单向化 —》双向化

融合网体系结构模型


融合网核心体系结构
融合网基础设施体系结构
电信固网资源
集成播控权
公安部
文化部
工信部
国家新闻出版广电总局
国家发改委
工信部
国家新闻出版广电总局
政策与法律层
社会化网络
新媒体
计费业务
电子游戏
电子支付
电子商务
SaaS
IaaS
PaaS
OTT TV
音视频电话
宽带上网
云计算
业务层
XMPP
SIP
HTTP
DNS
应用层
IEEE 802.3
IEEE 802.11
TCP/IP
C-HomePlug AV
C-DOCSIS
网络层
智能手机
智能电视
平板电脑
路由器
交换机
设备层

三网融合

- 网络融合的目标是给消费者带来体验上的改进，让不同物理网络的终端用户可以享受到相同无差别的服务



中国广播电视网络有限公司

中国广播电视网络有限公司

全国首页 总局首页

工商公示信息 企业公示信息

登记信息 | 备案信息 | 行政处罚信息

基本信息			
注册号	100000000044948	名称	中国广播电视网络有限公司
类型	有限责任公司(国有独资)	法定代表人	赵景春
注册资本	450000 万元人民币	成立日期	2014年04月17日
住所	北京市西城区灵境胡同42号		
营业期限自	2014年04月17日	营业期限至	长期
经营范围	有线电视网络规划、建设、运营和维护；为开展上述业务所进行的技术研究、技术开发、信息咨询。（依法须经批准的项目，经相关部门批准后方可开展经营活动）		
登记机关	国家工商行政管理总局	发照日期	2014年04月17日
经营状态	登记成立		

投资人信息				
投资人类型	投资人	证照类型	证照号码	详情

多网融合

- 电力线（PLC, Power Line Communication）宽带
  - 数据链路层协议，符合标准的802.3以太网规范
- 物联网
  - 麻省理工学院Auto-ID中心Ashton教授1999年在研究射频识别（RFID, Radio-frequency identification）时最早提出来的
- IP化
  - 目前应用最广泛、前景最明朗的网络层面融合方向，特别是IPv6技术的成熟和普及为各种异构网络统一到IP网络奠定了重要的通信协议基础

融合网安全新问题

- 设备安全
  - 智能设备的爆炸式发展
- 内容安全
  - 信息来源多样化
  - 信息传播渠道的界限模糊
  - 信息传播范围的扩大化
- 边界安全
  - 异构网络边界接口标准的不统一

我们的课程关注

- 计算机网络安全问题
  - IP网络是所有异构网络的终极演化方向
  - 计算机网络是IP网络的成熟应用代表
  - 软件定义一切的时代：网络安全与软件安全越来越密不可分，息息相关
- 融合网安全问题其实是旧瓶（IP网络）装新酒（新业务、新应用、新内容）

五、计算机网络安全模型

2种模型

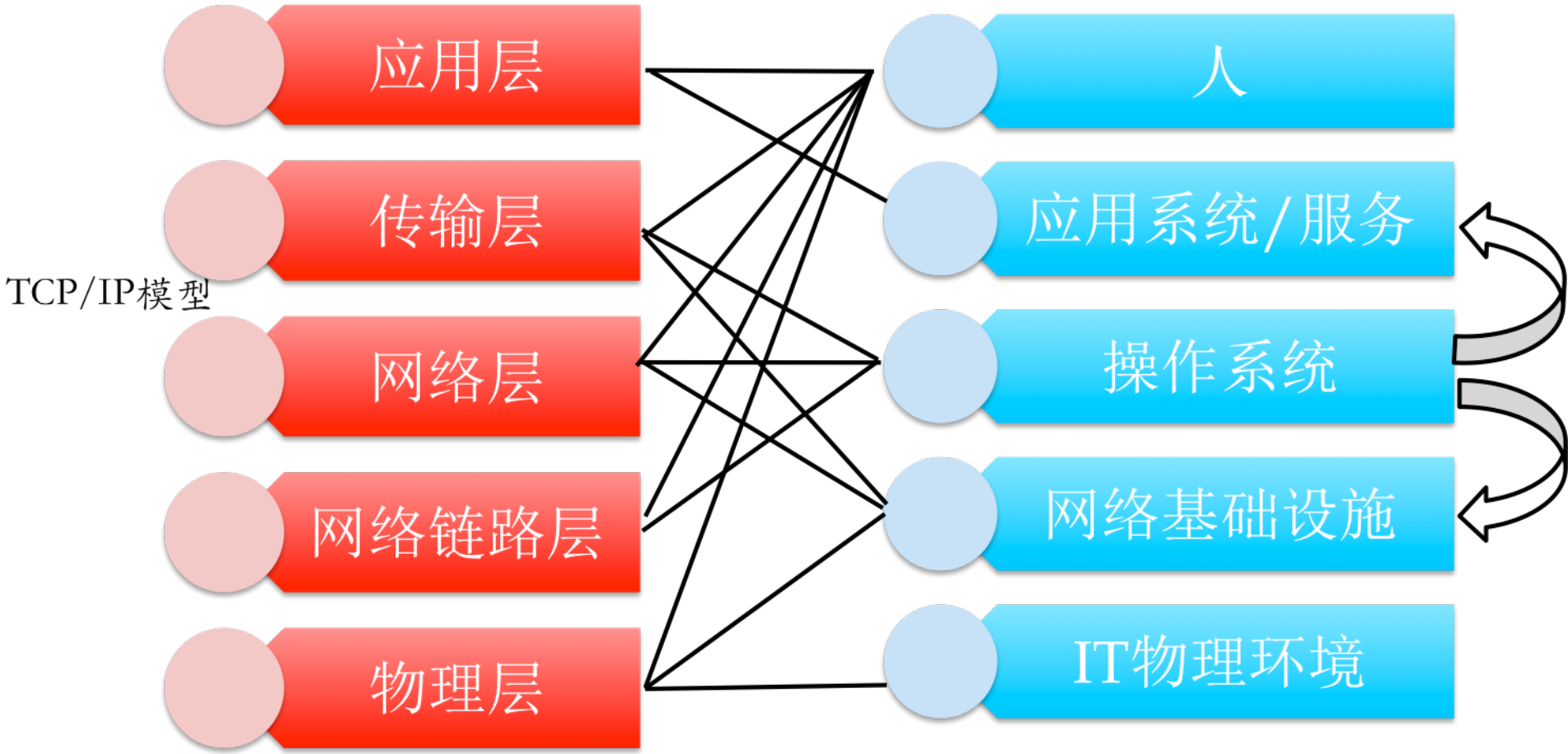
- 静态模型

  —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)

再论安全策略

- 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

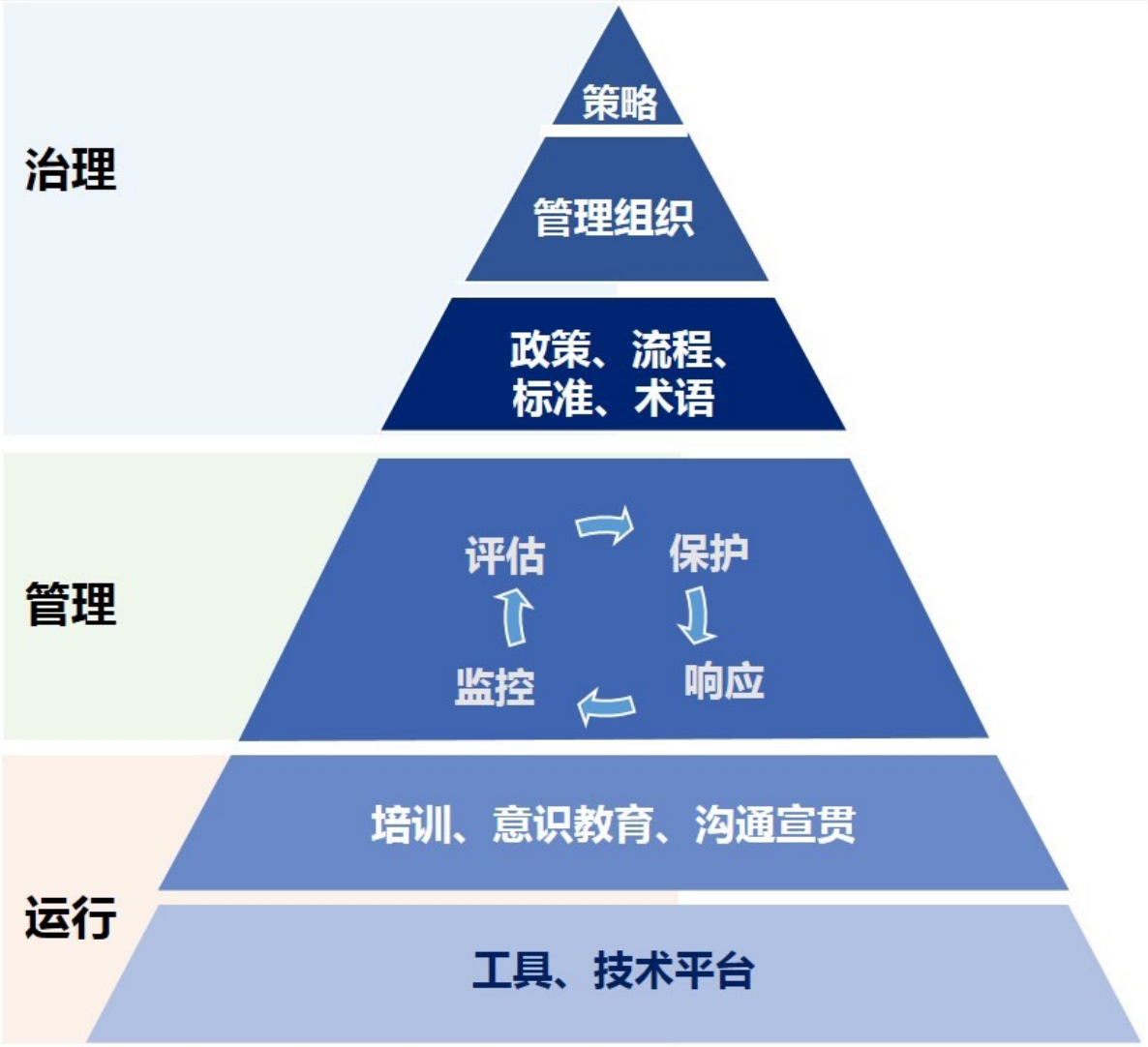
安全响应

- 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

顶层设计、底层实现和持续改进



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

六、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

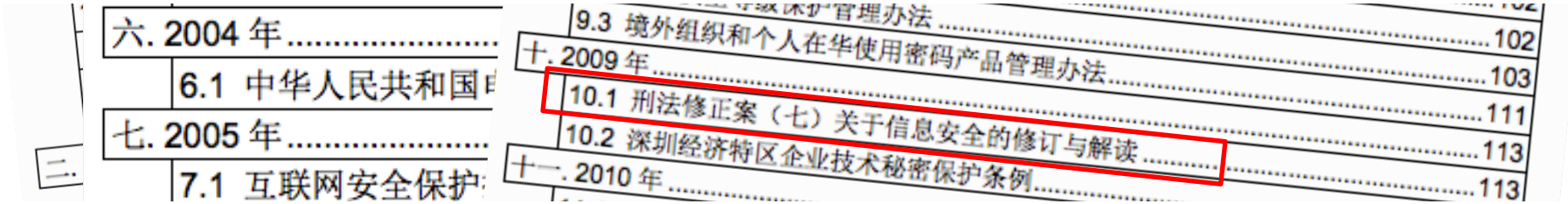
- 明确重点、突出重点、保护重点

七、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。



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

- 中国信息安全测评中心 - 标准法规 -相关法规

中华人民共和国网络安全法

- 2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过
  - 第七章，第七十六条（二）
  - 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

知法守法

- 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

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

- 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

融合网

- 不仅是技术问题
- IP化趋势
- 异构网络现状
- 新业务
  - 新媒体、三网融合、O2O、智能家居、物联网。。。

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
- 等级保护的意义
- 等级保护的现状

- 知法守法

黑客守则

黑客守则（精简版）

- 不恶意破坏
- 不恶意篡改
- 不与不可信的人分享隐私与秘密

推荐阅读

- 如何成为一名黑客
  - https://translations.readthedocs.org/en/latest/hacker_howto.html （中文翻译版）
  - http://catb.org/~esr/faqs/hacker-howto.html （英文原版）

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 (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

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

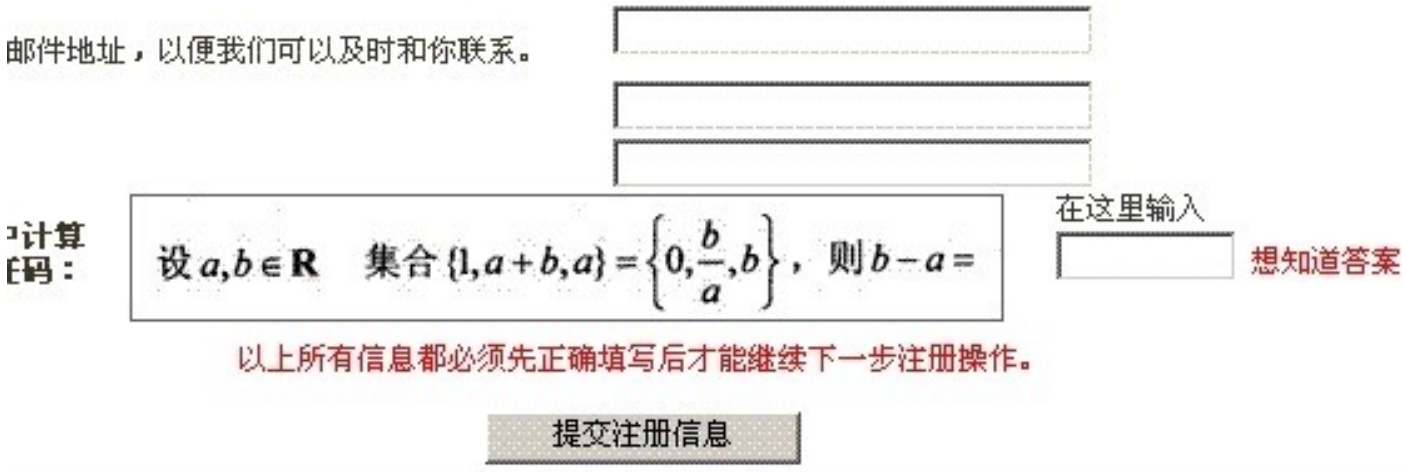
  —“被抢”事件中，小明的安全策略存在何问题？

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



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

- 在过去的一年中，有哪些重要的网络安全事件发生？这其中有哪些安全事件可以被归类为融合网安全事件？试简要阐述归类依据。
- 请列举你经常使用的互联网服务有哪些，通过公开渠道检索这些服务提供商在历史上是否经历过安全事件？据此，撰写一篇主题为：《某某互联网服务安全问题概要》的调研报告。