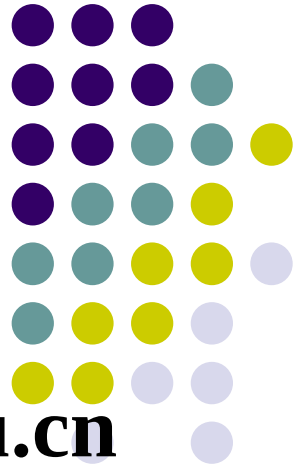
网络安全

罗　敏

武汉大学计算机学院

QQ: 5118924　Email：mluo@whu.edu.cn

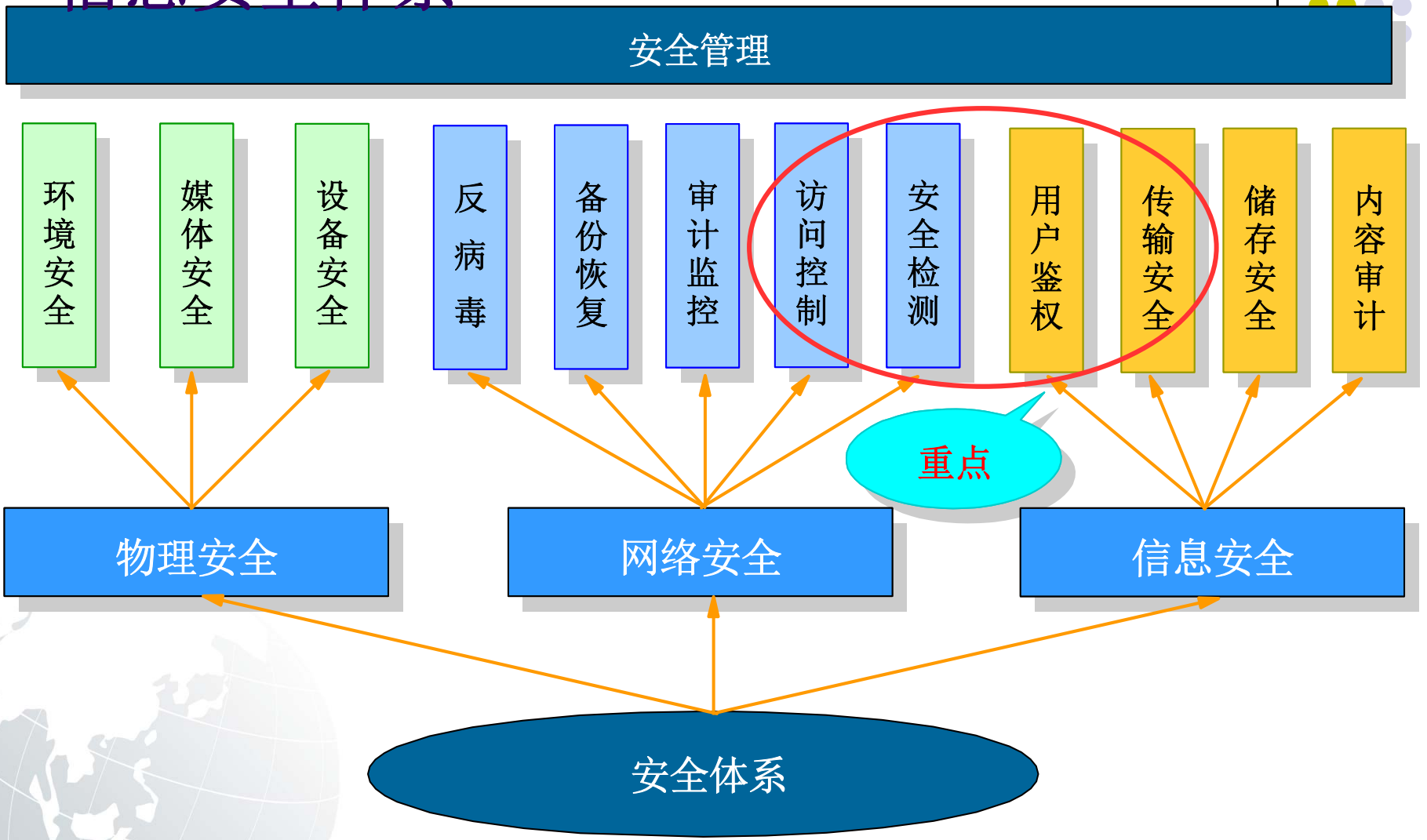
13907125177



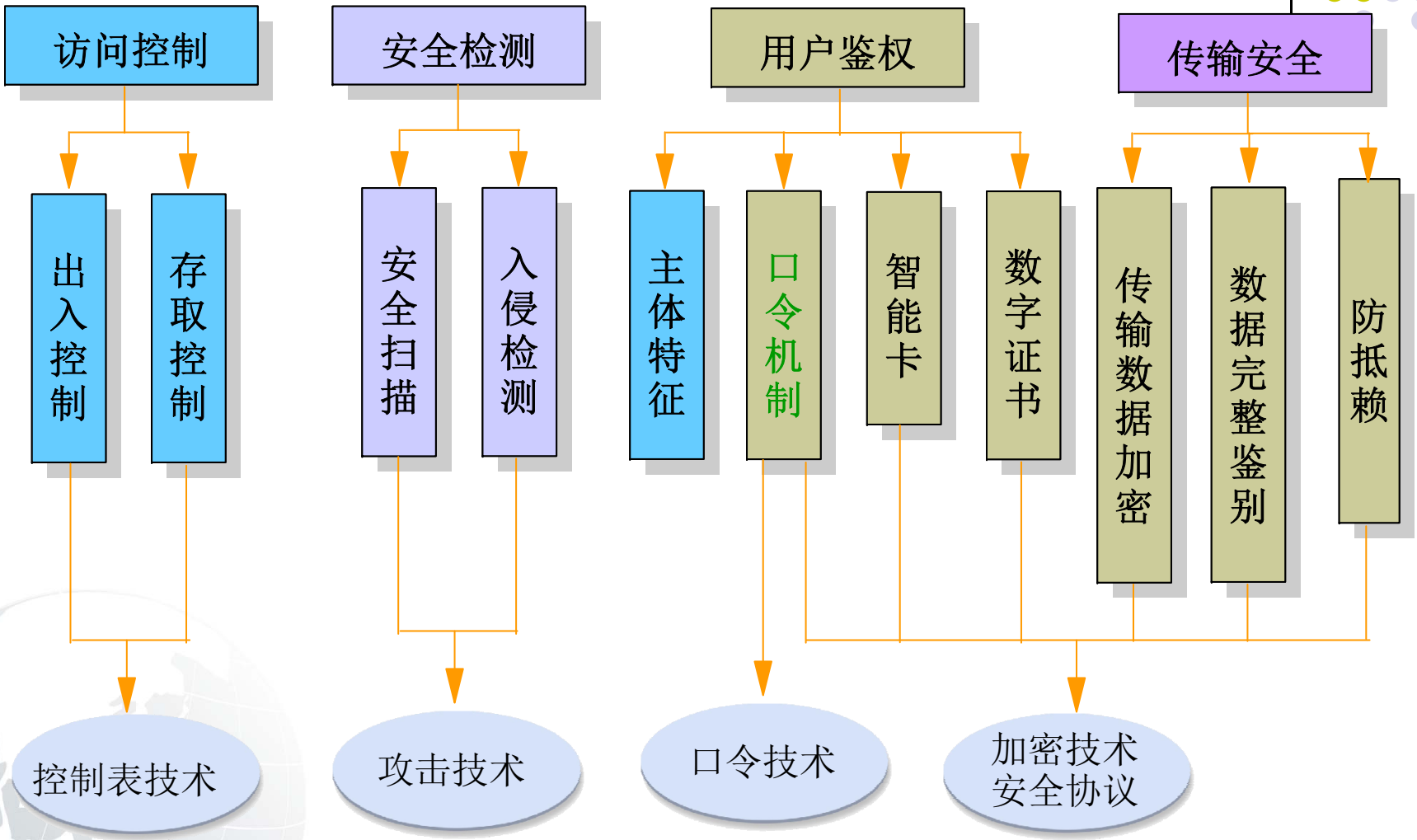
第一章回顾

- 什么是安全
- 信息安全的级别
- 安全的几个要素
- 安全威胁的来源
- 安全的目标
- 信息安全体系
- P2DR模型
- PDRR

信息安全体系


安全管理
环境安全
媒体安全
设备安全
反病毒
备份恢复
审计监控
访问控制
安全检测
用户鉴权
传输安全
储存安全
内容审计
重点
物理安全
网络安全
信息安全
安全体系

信息安全体系


访问控制
安全检测
用户鉴权
传输安全
出入控制
存取控制
安全扫描
入侵检测
主体特征
口令机制
智能卡
数字证书
传输数据加密
数据完整鉴别
防抵赖
控制表技术
攻击技术
口令技术
加密技术
安全协议

第2章 网络攻击行径分析

- 本章对攻击事件、攻击的目的、攻击的步骤及攻击的诀窍作一些简要的介绍，为随后深入学习攻击技术打下基础。

黑客和黑客技术

- 如何理解hacker
  - Hacker的定义？
    - Hacker代表了数字时代的一种文化
    - 强盗和侠客如何界定？
    - 警察和匪徒如何界定？
  - 从道德和技术两方面来看
    - 道德：服从人民大众的利益
    - 技术：过硬
  - 还需要强烈的热忱和坚持不懈的毅力
- 黑客技术
  - 防护技术的一部分
    - 发展黑客技术，也是为了更加有效地实施系统防护
  - 技术繁多，没有明显的理论指导

黑客技术

- 从一个攻击过程来看待黑客技术
  - 攻击过程中涉及到的技术都可以看成黑客技术
  - 有时候，一种技术既是黑客技术，也是网络管理技术，或者网络防护技术
- 粗分类
  - 信息收集技术：入侵之前的准备
  - 入侵技术：拒绝服务、欺骗、溢出、病毒邮件，…
  - 信息获取：入侵之后的增值服务，如木马、解口令等
  - 藏匿：希望自己被发现吗？
  - 其他，比如针对cookie或者一些协议、机制的攻击

第2章 网络攻击行径分析

- 2.1攻击事件
- 2.2攻击的目的
- 2.3攻击的步骤
- 2.4攻击诀窍

攻击事件

- 安全威胁
  - 外部攻击、内部攻击和行为滥用
- 攻击事件分类
  - 破坏型攻击
  - 利用型攻击
  - 信息收集型攻击
  - 网络欺骗攻击
  - 垃圾信息攻击

攻击目的

- 攻击的动机
  - 恶作剧
  - 恶意破坏
  - 商业目的
  - 政治军事

攻击目的

- 攻击性质
  - 破坏
  - 入侵
- 攻击目的
  - 破坏目标工作
  - 窃取目标信息
  - 控制目标机器
  - 利用假消息欺骗对方

攻击的步骤

- 一般的攻击都分为三个阶段：
  - 攻击的准备阶段
  - 攻击的实施阶段
  - 攻击的善后阶段

攻击的步骤

- 攻击的准备阶段
  - 确定攻击目的
  - 准备攻击工具
  - 收集目标信息

攻击的步骤

- 攻击实施阶段的一般步骤
  - 隐藏自己的位置
  - 利用收集到的信息获取账号和密码，登录主机
  - 利用漏洞或者其它方法获得控制权并窃取网络资源和特权

攻击的步骤

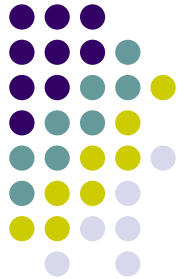
- 攻击的善后阶段
  - 日志
  - Windows
    - 禁止日志审计，清除事件日志，清除IIS服务日志
  - Unix
    - messages、lastlog、loginlog、sulog、utmp、utmpx、wtmp、wtmpx、pacct
  - 为了下次攻击的方便，攻击者都会留下一个后门，充当后门的工具种类非常多，最典型的是木马程序

攻击诀窍

- 常用攻击工具
  - 网络侦查工具
    - superscan，Nmap
  - 拒绝服务攻击工具
    - DDoS攻击者,sqldos,Trinoo
  - 木马
    - BO2000，冰河，NetSpy，

网络攻击行径分析

- 攻击目的
- 攻击步骤
  - 攻击的准备阶段
  - 攻击的实施阶段
  - 攻击的善后阶段



网络攻击行径分析

- 课后习题
  - 利用向目标主机发送非正常消息的而导致目标主机崩溃的攻击方法有哪些？
  - 简述破坏型攻击的原理及其常用手段。
  - 叙述扫描的作用于并阐述常用的扫描方法。
  - 简要叙述攻击的一般过程及注意事项。