信息安全导论

第一章 初识信息安全

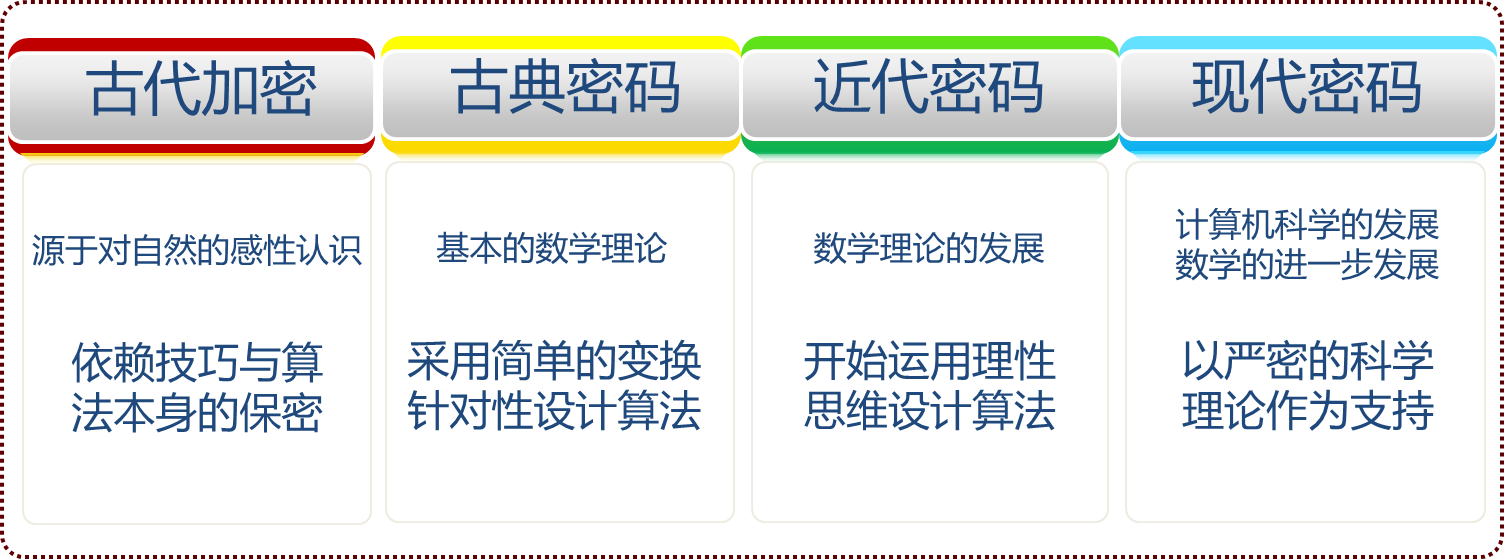
1. 信息的本质特征：“信息就是用来消除不确定的东西。”——香农

信息的基础资源：“信息是区别于物质与能量的第三种资源，是客观事物的基本存在形态之一。”——维纳

信息的产生来源：“信息是事物运动的状态与方式。”——钟义信

1. 信息处理周期：外部世界→信息获取→信息传递→信息认知→信息再生→信息传递→信息实效→……
2. 信息的特性：普遍性、载体依附性、共享性、传递性、价值性、时效性、真伪性、可处理性。
3. 为什么存在信息安全问题？①信息具有显著的价值特征；②存在众多威胁信息价值的风险。
4. 信息安全：“在技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”（ISO、保护信息资产的角度）、“对信息的保密性、完整性和可用性的保持，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他特征。”（GB标准、提供安全属性的角度）
5. 信息安全》网络空间安全》计算机安全
6. 信息安全属性CIA：保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。
7. 其他属性ANRC：真实性（Authenticity）、抗抵赖（Non-repudiation）、可靠性（Reliability）、可控性（Controllability）。
8. 安全威胁：人为威胁、非人为威胁。
9. 安全攻击：被动攻击、主动攻击。
10. 安全威胁的类型：信息泄露、信息伪造、完整性破坏、业务否决或拒绝服务、未授权访问。
11. 信息安全发展阶段：通信安全（香农《保密通信的信息理论》）→主机安全（美国国防部《橘皮书TCSEC》）→网络安全（《ISO7489标准》）→安全保障（1998年《信息保障技术框架》IATF）→网络空间安全（习近平）。
12. 认识：信息安全是相对的、动态的、“木桶原理”、人是最薄弱的部分、是国家安全不可分割的部分。
13. 信息系统基本要素：信息、系统、人员。
14. 安全层次：物理安全、运行安全、数据安全、内容安全、管理安全。
15. 信息安全保障体系结构：保护、检测、反应、恢复。
16. 安全服务：为系统提供安全措施；安全机制：用来实施安全服务的技术规范；关系：安全服务可以采用一种或多种安全机制来实现、同一种安全机制也可以用于实现不同安全服务。
17. 一级学科：网络空间安全。
18. 二级学科：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。
19. 学科意义：网络渗透危害政治安全、网络攻击危害经济安全、网络有害信息侵蚀文化安全、网络恐怖和违法犯罪破坏社会安全、网络空间的军事化和对抗加剧威胁军事安全。

第二章 信息安全技术概述

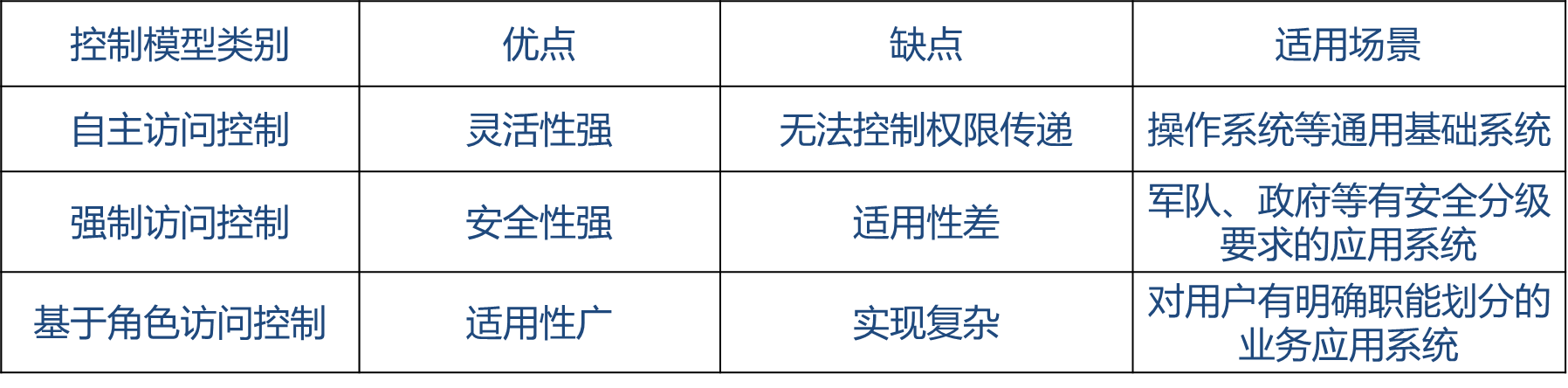
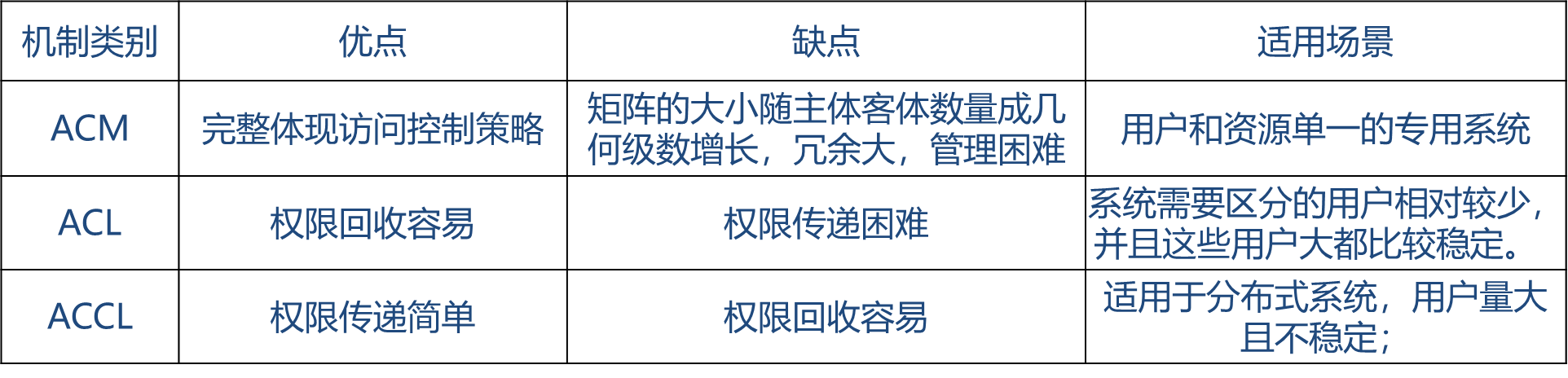
1. 密码学：研究编制、破译密码的技术科学。（编码学：研究密码变化规律应用于编制密码；破译学：破译密码）
2. 古代加密方法（隐形墨水）→古典密码（凯撒、Polybius校验表）→近代密码（加密机、Hill矩阵密码）→现代密码（加密标准）。
3. 古代加密方法：思想简单、技巧性强、依赖算法本身保密性、依赖于实体
4. 古典密码：基于变化的思想、安全性有所提高，安全性依赖密钥的保密
5. 近代密码：数学开始主导
6. 现代密码：基于计算机科学的发展，完全依赖于数学证明与数学理论、破解代价极高
7. 
8. 明文空间：未加密信息的集合M；

密文空间：加密后信息的集合C；

加密方法：隐藏内容的过程E；

解密方法：恢复内容的过程D；

密钥空间：加解密过程中提供的特殊输入集合K。

1. 对称密钥加密算法：加解密密钥相同、速度快、大量数据保密（DES、3DES、AES）
2. 公开密钥密码体制：加解密密钥不同、速度慢、用于认证（RSA、ECC、ElGamal）
3. Hash：映射为定长输出（SHA-1、MD5）
4. 物理安全需求：环境安全、设备安全；解决途径：提供防护措施、隔绝危险、提高可靠性
5. 设备安全防护：防盗防毁、防电磁泄露（抑制、屏蔽、干扰、直接加密）与干扰（频域、时域、屏蔽）
6. 设备安全防护、机房环境安全防护、提高可靠性、隔绝威胁
7. 身份认证：用户与主机、主机与主机
8. 数目：单因子、双因子、多因子（U盾：本身+U盾PIN码）认证；状态：静态（口令）、动态（动态口令卡）；
9. 生物特征（指纹）
10. 认证协议：公钥密码
11. 访问控制：主体（规定谁）、客体（被保护的）、授权
12. 自主访问控制模型（DAC：Discretionary Access Control）、强制访问控制（MAC：Mandatory、Access Control、分级）、基于角色（Role-based Access Control）
13. 
14. 实现机制：访问控制矩阵（ACM）、访问控制列表（ACL，以文件开始）、访问控制能力表（ACCL，以用户开始）
15. 
16. 访问控制安全标签列表（给用户和文件划等级）

第三章：信息安全的攻与防

1. 分类：攻击者角度：主动型（黑客攻击）、被动型（网络监听）；

攻击手段及破坏方式：计算机病毒、网络入侵、欺骗类。

1. 计算机病毒：影响计算机正常工作的代码。
2. 传统型病毒：宿主程序（必须执行），寄生性、传染性、潜伏性、触发性、破坏性。
3. 蠕虫病毒：自我复制，自传播性、隐蔽性、破坏性；
4. 特洛伊木马：隐蔽性、非授权性（远程控制另一主机，见于客户端、服务端）
5. 防范：加强安全防御、提高安全意识。
6. 安全攻击手段：网络入侵（前期准备、实施入侵、后期处理）：拒绝服务（利用漏洞产生大量流量使服务器崩溃）、口令攻击（获取、猜、探测、破解）、嗅探攻击（监听）、欺骗类、利用型、诈骗类
7. APT（Advanced Persistent Threat）攻击（针对性）
8. 防火墙：硬件+软件，控制内外网网络数据流量，主要作用：网络流量过滤、网络监控审计、其他安全服务（VPN）（静态防范措施）
9. 入侵检测系统（动态防范措施）：信息收集、信息分析、结果处理
10. 入侵诱骗系统（HoneyPot、HoneyNet）
11. 入侵响应系统
12. 新型防御：态势感知、云安全

第四章 信息管理概述

1. 信息安全管理体系（ISMS）：从PDCA（Plan规划、Do实施、Check检查、Act处置）演化而来。
2. 《网络安全法》的必须性：是维护网络安全的客观需要、是维护广大人民群众切身利益的必然要求、是参与互联网国际竞争和国际治理的必然选择。
3. 《网络安全法》地基本原则：网络空间主权、网络空间与信息化发展并重、共同治理。
4. 《网络安全法》：总则+6章=79条，9800余字。
5. 
6. 网络安全等级保护（“等保”）：

等保1.0：GB17895-1999《计算机信息系统安全保护等级划分准则》、《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》

等保2.0：GB/T 22239-2019 《网络安全等级保护基本要求》、《GA/T 1389—2017 网络安全等级保护定级指南》、《GA/T 1390.2—2017 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》

1. 扩展了对云计算、移动互联、物联网、工业控制系统的安全要求。
2. 保护对象：大数据、信息系统（云计算、物联网、移动互联、工业控制系统）、基础信息网络。
3. 信息系统应建立“可信、可控、可管”的安全防护体系。
4. 等保五步：定级、备案、安全建设、等级评测、监督检查