网安期末复习总纲

第一章

网络空间安全的重要性

- 网络空间安全事关政治安全
- 网络空间安全事关经济安全
- 网络安全事关文化安全
- 网络安全事关社会安全
- 网络安全事关国防安全

网络强国的目标:

- 近期目标: 技术强,基础强,内容强,人才强,国际话语权强
- 中期目标: 建设网络强国的战略部署与"两个一百年"奋斗目标同步推进,向着网络基础设施基本普及,自主创新能力强,信息经济全面发展,网络安全保障有力的目标不断前进
- 远期目标: 战略清晰,技术先进,产业领先,制网权尽在掌握,网络安全坚不可摧

网络安全观

- 网络安全是整体的而不是割裂的
- 网络安全是动态的而不是静态的
- 网络安全是开放的而不是封闭的
- 网络安全是相对的而不是绝对的
- 网络安全是共同的而不是孤立的

战略原则

- 尊重维护网络空间主权
- 和平利用网络空间
- 依法治理网络空间
- 统筹网络安全与发展

第二章

网络安全的基本属性

- 保密性
- 完整性
- 可用性

安全服务

- 鉴别
- 访问控制
- 数据完整性
- 数据保密性
- 抗抵赖

安全产品

- 防火墙:

> 功能:
>
> - 访问控制功能
> - 内容控制功能
> - 安全日志功能
> - 集中管理功能
> - 附加流量控制功能,网络地址转换功能,虚拟专用网功能

> 局限性:
>
> - 不能当但被保护网络内部人员发起的攻击
> - 不能防范不经过防火墙的攻击
> - 不能防范数据驱动型攻击
> - 不能完全防止传动易感染病毒的软件或文件
> - 不能防范不断更新的攻击方式

- 入侵检测系统
- 恶意代码防护

> 恶意代码: 恶意代码就是一个计算机程序或一段程序代码,执行后完成特定的功能
>
> 恶意代码分类: 病毒,蠕虫,木马和逻辑炸弹

第三章

RSA算法

1. 任意选取两个不同的素数p和q计算乘积

   n = p*q

   z = (p - 1)*(q - 1)

2. 任意选取一个大整数e，e与z互质
3. 确定的解密钥d，满足

   e*d mod z =1

4. 将明文m（m<n是一个整数）加密成密文c，加密算法为

   $c = m^e \bmod n$

5. 将密文c解密为明文m，解密算法为

   $m = c^d \bmod n$

密码学发展的三个阶段

- 第一阶段 到1949年 密码技术是一种艺术,密码专家凭自己的直觉和信念来进行密码设计
- 第二阶段 1949到1975 香农发表的<保密系统的信息理论>标志着开始,产生了信息论,为私钥密码系统建立了理论基础.
- 第三阶段 1976至今 Diffe和Hellman发表了<密码学新方向>开创了公钥密码学的新纪元

分组密码的工作模式:

- 电子密码本模式
- 密码分组链接模式
- 密文反馈模式
- 输出反馈模式

分组密码的差错传播

- 电子密码本模式 1
- 密码分组链接模式 2
- 密文反馈模式 2
- 输出反馈模式 1

第四章

信息系统安全模型

- BLP安全策略模型
- Biba安全策略模型
- Clark-Wilson模型
- 中国墙模型
- RBAC模型

安全策略模型面临的挑战

- 信息流安全理论和现有体系结构的融合问题
- 信息流模型需要避免绝对的无干扰限制
- 信息流模型需要能够解释和管理复杂的安全策略

安全威胁

- 可用带宽损耗
- 网络管理通信的破坏
- 网络基础设施失去管理

指标(安全要求)

- 访问控制
- 鉴别
- 可用性
- 保密性
- 完整性
- 不可否认性

安全措施

- 网络管理通信的保护
- 网络管理数据的分离
- NMC的保护
- 配置管理

第五章

中国可信计算体系创新的体现

- 全新的可信计算体系构架
- 跨越了国际可信计算组织(TCG)可信计算的局限性
- 创新可信密码体系
- 创新主动免疫体系结构
- 开创可信计算3.0新时代

可信计算平台技术规范实现的基本功能

- 可信计算平台密码方案
- 可新平台控制模块
- 可信计算平台主板
- 可信软件基
- 可信网络连接

密码与可信计算平台功能的关系

- 平台完整性度量与报告
- 平台身份可信
- 平台数据安全保护

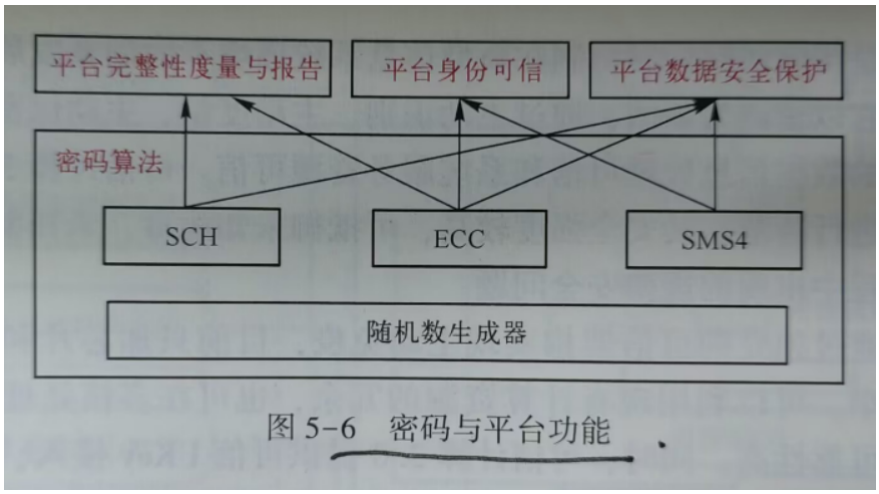

图 5-6 密码与平台功能

第六章

等级保护的对象:

- 网络基础设施
- 信息系统
- 大数据
- 云计算平台
- 物联网
- 工控系统

等级保护的工作流程

- 定级
- 备案
- 建设整改
- 等级测评
- 监督检查

等级保护的定级对象

- 基础信息网络
- 信息系统
- 大数据

等级保护对象的信息系统的基本特征

- 业务流程的完整性
- 软硬件设备的先对独立性
- 安全管理责任权的统一性
- 多级互联隔离性

对客体的侵害程度

- 一般侵害
- 严重侵害
- 特别严重侵害

判别标准

- 如果受侵害客体是公民,法人或其他组织的合法权益,则以本人或者本单位的总体利益作为判断侵害程度的基准
- 如果受侵害客体是社会秩序,公共利益或国家安全,则应以整个行业或国家的总体利益作为判断侵害的基准

第七章

风险分析的三要素

- 资产
- 威胁
- 脆弱性

风险分析的主要内容

- 对资产进行识别,并对资产的价值进行赋值
- 对威胁进行识别,描述威胁的属性,并对威胁出现的频率赋值
- 对脆弱性进行识别,并对具体资产的脆弱性的严重程度赋值
- 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性
- 根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失
- 跟据安全事件发生的可能性及安全事件出现后的损失,计算安全事件一旦发生对组织的影响,即风险值

风险计算原理

- 风险值 = R (A,T,V) = R(L(T , V),F(I_a , V_a))
- R : 安全风险计算函数
- A : 资产
- T : 威胁
- V : 脆弱性
- I_a : 安全事件所作用的资产价值
- V_a : 脆弱性严重程度
- L : 威胁利用资产的脆弱性导致安全的可能性
- F : 安全事件发生后造成的损失

影响风险值的因素

- 安全风险计算函数
- 资产
- 威胁
- 脆弱性
- 安全事件所作用的资产价值
- 脆弱性严重程度
- 威胁利用资产的脆弱性导致安全的可能性
- 安全事件发生后造成的损失

第八章

攻击过程

- 确定目标
- 获取控制权
- 权限提升与保持
- 实施攻击
- 消除痕迹

网络攻击分类

1. 根据攻击的效果: 主动攻击,被动攻击
2. 根据攻击的技术特点: 基于网络协议的攻击,基于系统安全漏洞的攻击
3. 根据攻击的位置: 远程攻击,本地攻击,伪远程攻击

网络攻击的方法

- 口令猜解
- 木马
- 拒绝服务
- 漏洞攻击
- 网络钓鱼
- 社会工程
- 后门攻击
- 高级持续攻击

有害程序事件

- 计算机病毒事件
- 蠕虫事件
- 特洛伊木马事件
- 僵尸网络事件
- 混合攻击程序事件
- 网页内嵌恶意代码事件
- 其他有害程序事件

第九章

云计算服务模式

- 基础设施即服务
- 平台即服务
- 软件即服务

云计算部署模式

- 私有云
- 公有云
- 社会云
- 混合云

云计算安全风险

- 客户对数据和业务系统的控制能力减弱
- 客户与云计算服务提供商之间的网络安全责任难以界定
- 可能产生司法管辖权错位问题
- 客户对数据所有权难以保障
- 客户数据的安全保护更加困难
- 客户数据残留风险
- 容易产生对云服务商的过度依赖

物联网分类

- 私有物联网
- 共有物联网
- 社区物联网
- 混合物联网

物联网关键技术

- 传感网技术
- 射频识别技术
- M2M技术
- 云计算和大数据技术

物联网面临的主要安全风险

- 身份欺诈
- 数据篡改
- 抵赖
- 信息泄露
- 拒绝服务
- 权限升级

第十章

网络安全法律

- 中华人民共和国网络安全法
- 中华人民共和国电子签名法
- 中华人民共和国宪法
- 中华人民共和国刑法

我国网络安全立法存在的问题

- 结构不合理
- 法规的协调性和相通性不够.
- 针对性和操作性不够强
- 有些法规制度明显滞后
- 公民个人权益缺乏法律保护

标准的五个层次

- 国家标准 GB国标
- 行业标准　T为强制标准
- 地方标准
- 团体标准
- 企业标准

国家网络安全标准制定流程

- 工作组征求意见
- 评审通过形成送审稿
- 秘书处网上征求意见
- 评审通过形成报批稿
- 主任办公会审查
- 国标委批准发布
- 定期复审提出修订
- 立项申请提出草案