# 网络空间安全复习归纳

### ****第一章：网络空间安全概述****

1.生活中的网络空间安全问题：

1）QQ账号被盗

2）支付宝账号被盗

3）银行卡被盗刷

（钓鱼网站 ，个人隐私泄露，网络诈骗，摄像头等遭到入侵）

2.工作中的网络空间安全问题

1）网络设备面临的威胁

2）操作系统面临的威胁

3）应用程序面临的威胁

3. 概述：从广义来说，凡是涉及网络信息的保密性、完整性、可用性、真实性、可控性、可审查性的相关技术和理论，都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等的综合性学科。

4. 网络安全包括网络硬件资源和信息资源的安全性，而硬件资源包括通信线路、通信设备（路由机、交换机等）、主机等，要实现信息快速安全的交换，必须有一个可靠的物理网络。信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中储存和传输的用户信息数据等。信息资源的安全也是网络安全的重要组成部分。

### 第二章：物理安全

1.物理安全一般分为环境安全，设备和介质安全。

2.要解决的两个方面的问题：

1）对信息系统实体的保护

2）对可能造成信息泄露的物理问题进行防护防范

3.意义：是信息安全的必要前提。

### 第三章：网络安全

1.OSI安全体系中的五类相关安全服务：

1）认证（鉴别）服务：提供通信中对等实体和数据来源的认证（鉴别）。

2）访问控制服务：用于防止未授权用户非法使用系统资源，包括用户身份认证和用户权限确认

3）数据保密性服务:为防止网络各系统之间交换的数据被截获或被非法存取而泄密，提供机密保护。同时，对有可能通过观察信息流就能推导出信息的情况进行防范。

4）数据完整性服务：用于防止非法实体对交换的数据的修改、插入、删除以及在数交换过程中的数据丢失。

5）抗否认性服务（也叫不可否认性服务）：用于防止发送方在发送数据后否认发送和接收方在接收到数据后否认收到或伪造数据的行为。

2．TCP/IP协议：由OSI七层模型中的网络层IP协议和传输层TCP协议组成，定义了电子设备如何连入因特网，以及数据如何在他们之间传输的标准。

3.网络层协议：IP协议——IP欺骗攻击、ARP协议（地址解析协议）——ARP欺骗或ARP攻击；

4.传输层协议：

TCP协议：使用三次握手，四次分手的机制来建立和断开一条连接（类似打电话和接电话的过程）。

UDP协议：一种无连接的协议（类似发QQ消息，微信消息的过程）。

TCP协议和UDP协议的区别、比较：

1）TCP面向连接（如打电话要先拨号建立连接）;UDP是无连接的，即发送数据之前不需要建立连接

2）TCP提供可靠的服务。也就是说，通过TCP连接传送的数据，无差错，不丢失，不重复，且按序到达;UDP尽最大努力交付，即不保证可靠交付.

3)TCP较UDP更为可靠，因为UDP没有可靠性保证、顺序保证和流量控制字段。

5.安全封装协议：

1）IPSec（Internet Protocol Security）：是为IPv4和IPv6协议提供基于加密安全协议，它使用AH（认证头）和ESP（封装安全载荷）协议来实现其安全，使用ISAKMP/Oakley及SKIP进行密钥交换、管理及安全协商，使用DH交换算法进行加密。

2）SSL协议（安装套接层协议，Security Socket Layer）：工作在传输层之上，应用层之下。

3）S-HTTP：位于应用层。

6.信息安全风险评估相关要素：

1）资产：对组织具有价值的信息资源

2）威胁：可能对组织或资产造成危害的潜在原因

3）脆弱点：一个或一组资产所具有的、可能被威胁利用、对资产造成损害的薄弱环节

4）风险：威胁利用资产的脆弱点导致组织受损的潜在可能性

5）影响：威胁利用资产的脆弱点导致不期望发生事件的后果

6）安全措施：为保护资产、抵御威胁、减少脆弱点、限制影响而才去的各种实践、规程和机制的总称

7）安全需求：为保证组织业务战略的正常运作而在安全措施方面提出的要求

7.应对网络安全风险

从国家层面应对：

1. 出台网络安全战略，完善顶层设计
2. 建立网络身份体系，创建可信网络空间
3. 提升核心技术自主开发能力，形成自主可控的网络安全产业生态体系
4. 加强网络攻防能力，构建攻防兼备的安全防御体系
5. 深化国际合作，逐步提升网络空间国际话语权

从安全技术层面应对：

1. 身份认证技术：在计算机网络中为确认操作操作者身份而采取的有效解决方法。如生物认证技术、口令技术、令牌技术等等……
2. 访问控制技术：为防止对任何资源进行未授权的访问，使计算机系统在合法的范围内使用的技术。意指用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。
3. 访问控制技术三要素：

·主体：发起者，是一个主动的实体，可以操作被动实体的相关信息或数据。如：用户、程序、进程等

·客体：一种被动实体，被操作的对象，规定需要保护的资源

如：文件、存储介质、程序、进程等

·控制策略

··主体和客体之间的关系：

主体：接收客体相关信息和数据，也可能改变客体相关信息。一个主体为了完成任务，可以创建另外的主体，这些子主体可以在网络上不同的计算机上运行，并由父主体控制它们

客体：始终是提供、驻留信息或数据的实体

主体和客体的关系是相对的，角色可以互换

1. 访问控制的内容包括：

·认证：包括主体对客体的识别和客体对主体的检验确认

·控制策略：通过合理地设定控制规则集合，确保用户对信息资源在授权范围内的合法使用

·安全审计：系统可以自动根据用户的访问权限，对计算机网络环境下的有关活动或行为进行系统的、独立的的检查验证，并做出相应评价与审计

8.入侵检测技术：

1）异常检测：它的基本假设是：入侵者的活动异于正常主题的活动。根据这一理念建立主体正常活动的档案，将当前主体的活动状况与活动档案相比较，当其违反统计规律时，认为该活动可能是入侵行为。

2）特征检测（误用检测）：它的基本假设是：具有能够精确地按某种方式编码的攻击，并可以通过捕获攻击及重新整理，确认入侵活动是基于同一弱点进行攻击的入侵方法的变种。

异常检测和误用检测的区别：

1. 异常检测：入侵和滥用行为通常和正常的行为存在严重的差异，检查出这些差异就可以检测出入侵。异常检测的局限在于并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。
2. 误用检测：是通过某种方式预先定义行为，然后见识系统的运行，从中找出符合预先定义规则的入侵行为。误用检测只能发现已知的攻击，对未知的攻击无能为力。
3. 异常检测是指通过攻击行为的特征库,采用特征匹配的方法确定攻击事件.误用检测的优点是检测的误报率低,检测快,但误用检测通常不能发现攻击特征库中没有事先指定的攻击行为,所以无法检测层出不穷的新攻击。
4. 异常检测一般用于系统的检测，而误用检测与杀毒软件类似。

9.蜜罐技术：

1）定义：蜜罐技术本质上是一种对攻击方进行欺骗的技术。

2）方式：通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击。

3） 作用：可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

10. DOS（Denial of Service）拒绝服务攻击

DDOS(Distributed Denial of Service) 分布式拒绝服务攻击

### 第四章：系统安全

1.操作系统的本质：工作在计算机硬件之上的第一层软件。

2.计算机操作系统的主要功能包括：

1. 进程管理
2. 内存管理
3. 设备管理
4. 文件管理
5. 用户管理

3.操作系统中常见的安全保护机制：

1） 进程隔离和内存保护：

为每个进程提供互相独立的运行空间，该机制通过禁止进程读写其他进程以及系统进程的内存空间来实现隔离，并通过一系列复杂的机制实现环境隔离下的进程间通信机制与进程间资源共享机制。

2） 运行模式：

现代CUP的运行模式通常分为内核模式和用户模式两种运行模式。

CUP的运行模式的区分起到了保护操作系统的运行不受其他应用程序干扰和破坏的作用。

3） 用户权限控制：

在多任务与多用户的环境下，为提升系统安全性以及减少误操作，操作系统对用户权限进行了区分。

4） 文件系统访问：

操作系统通过对文件的操作权限进行限制来实现文件的访问控制机制。

4.虚拟机逃逸：指利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的。

### 第五章：应用安全

1.C/S架构与B/S架构

C/S(Client/Server)架构: 即客户端/服务器架构,一般针对特定的用户群体，如军队，企业等等。

B/S（Browser/Server）架构：一般面向普通用户群体。

2.SQL注入：所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。通过递交参数构造巧妙的SQL语句，从而成功获取想要的数据。

3.CSRF

定义：指跨站请求伪造。

原理：（1）登录受信任网站A，并在本地生成Cookie； （2）在不登出A的情况下，访问危险网站B。（只有两者同时满足才会受到CSRF攻击）

4.恶意代码

定义：恶意代码又称恶意软件，其本质是一种程序。

特点：1）具有恶意破坏的目的。

2）其本身为序。

3）通过执行发生作用。

分类：1）逻辑炸弹、Rootkit

2）木马：客户端（开门），服务器端（操控）

3）病毒：具有自我复制能力

4）蠕虫：独立的恶意代码，能够自我复制，传播迅速

5）Zombie：具有自我复制能力的独立的恶意代码

6）WebShell

### 第六章：数据安全

1.数据安全的三要素：Confidentiality（保密性）、Integrity（完整性）和Availability（可用性），简称CIA。

2.数据安全的组成：

1）数据安全的本身：主要是采取现代密码算法对数据进行主动保护。

2）数据防护的安全：采用现代信息储存手段对数据进行主动防护。

3）数据处理的安全：是指如何有效的防止数据在录入、处理、统计或打印中由于硬件故障、断电、死机、人为的操作失误、程序缺陷、病毒或黑客等造成的数据库损坏或数据丢失现象。

4）数据存储的安全：数据库在系统外的可读性。

3.数据的存储方案：

1）直连式存储（DAS）：外部存储设备直接挂接在服务器内部的总线上，数据存储设备是整个服务器结构的一部分（DAS相当于U盘）。

2）网络接入存储（NAS）结点

3）存储区域网络（SAN）连接结点与 的高速网络

4.数据备份：

1）本地备份：也叫手工备份，是每台服务器有自己的本地备份设备

2）不仅增加了硬件投资，还增加了管理的费用。

网络备份：也叫做LAN备份，带有备份设备的备份服务器被放置在网络中。备份服务器负责整个系统的备份，它管理整个网络的备份策略、备份媒体和备份目标。

（1）实现了大容量自动化、集中式备份

（2）备份过程有策略管理，无需管理员介入

（3）网络内所有需要备份的服务器可共享一台备份设备

### 第七章：大数据背景下的先进计算机安全问题

1.大数据的思维方式：一是采集数据的方式和路径越来越多，内容和类型日益丰富多元。二是数据分析不仅仅靠围观采样，更可以全面获得宏观整体的数据。

2.大数据为高级持续性威胁（APT）提供了便利（SCAN）

APT（Advanced Persistent Threat）高级持续性威胁，是利用先进的攻击手段对特定目标进行长期持续性网络攻击的一种攻击形式。APT攻击相对于其他攻击形式而言更为高级和先进，这主要体现在攻击者在发动攻击之前会对攻击对象进行精确的信息收集，在收集的过程中攻击者还会主动挖掘被攻击目标系统的漏洞，从而利用这些漏洞发起有效的攻击，例如利用0day漏洞进行攻击。而大数据及其分析技术的发展也为APT攻击者提供了极大地便利

3.云服务提供的三种不同层次的模式：

1）基础架构即服务（IaaS）；

2）平台即服务（PaaS）；

3）软件及服务（SaaS）；

4．物联网体系的三层结构：

1）感知层：感知层解决的是人类世界和动物世界的数据获取问题，该层被认为是物联网的核心层，主要具备“物”的标识和信息的采集功能。

2）网络层

3）应用层

5.工控系统（ICS）与传统IT信息系统的对比

6．工控系统的关键组件包括：

1）控制器

2）数据采集监视控制组件

3）人机界面

4）分布式过程控制系统

7.工控系统一般要比传统的IT系统脆弱，其自身脆弱性主要表现在以下几个方面：

1）系统漏洞难以及时处理。工控设备使用周期长，当前主流的工控系统存在普遍安全漏洞，同时又存在工控系统软件难以升级、补丁兼容性差、补丁管理困难等弱点

2）工控系统通信协议在设计之初缺乏足够的安全性考虑。

3）没有足够的安全教育及管理政策，人员安全意识缺乏，缺乏对违规操作，越权访问行为的审计能力

4）工控系统直接暴露在互联网上，面对新型的APT攻击，缺乏有效的应对措施，安全风险不断增加

8.工控系统的安全防护中基于主控系统安全基线的防护方法：

1）基线建立：基线建立是防护的先决条件。从环境中提取工控系统的主要文件的特征值作为安全基线。

2）运行监控

3）实施防御

### 第八章：舆情分析

1．网络舆情的特点：详见P166-167（理解即可）

2．网络舆情分析系统通常具有以下功能；

1）热点话题、敏感话题识别：根据新闻出处的权威度、评论数量、发言时间密集程度等参数，识别出给定时间段内的热门话题。利用关键字布控和语义分析，识别敏感话题。

2）倾向性分析：对于每个话题了解发标人的观点，对倾向性进行分析与统计。

3）主题跟踪：分析网络上新发表的文章和论坛帖子，关注话题是否与已有主题相同或类似。

4）趋势分析：分析在不同的时间段内，人们对某个主题的关注程度。

5）突发事件分析：对突发事件进行跨时间跨空间综合分析，获知事件发生的全貌并预测事件发展的方向。

6）报警系统：及时发现突发事件、涉及内容安全的敏感话题并报警。

7） 统计报告：根据舆情分析引擎处理后的结果库生成报告用户可通过浏览器浏览，提供信息检索功能，根据指定条件对热点话题、倾向性进行查询，并浏览信息的具体内容，提供决策支持。

### 第九章：隐私保护（略）

### 第十章：密码学及应用

1．Kerckhoffs准则（要求能简述出来）：攻击方知道所用的密码系统。更具体的说，除密钥之外，攻击方和用户知道的信息一样多。 Kerckhoffs准则认为，一个安全保护系统的安全性不是建立在它的算法对于对手来说是保密的，而应该建立在他选择的密钥对于对手来说是保密的

2.加密置换矩阵和解密置换矩阵

3.矩阵加密置换的方法（做几道题）

4.分组密码设计过程中，混乱和扩散的解释：

1）混乱：所设计的密码应使得密钥、明文以及密文之间的依赖关系相当复杂，以至于这种依赖性对密码分析者来说是无法利用的。

2）扩散：所设计的密码应使得密钥的每一位数字影响密文的许多位数字，以防止对密钥进行逐段破译，而且明文的每一位数字也应影响密文的许多位数字，以便隐蔽明文数字统计特性

5.DES是安全的么？DES加密过程中S盒的使用

很明显不是。

缺陷：密钥长度短（只有56比特），不能抵抗最基本的攻击方法-穷搜索攻击

存在弱密钥

难以对抗偏差分析攻击

有人提出专用芯片可快速搜索使用的密钥

·DES的核心是S盒，除此之外的计算是线性的

·S盒作为该密码体制的非线性组件对安全性至关重要

·S盒的设计准则：

·S盒不是它输入变量的线性函数

·改变S盒的一个输入位至少要引起两位的输出改变

·对任何一个S盒，如果固定一个输入比特，其它输入变化时，输出数字中0和1的总数近于相等

DES的两个主要弱点：

密钥容量：56位不太可能提供足够的安全性

S盒：可能隐含有陷井（Hidden trapdoors）

6.单向陷门函数：

单向陷门函数是满足下列条件的函数f：

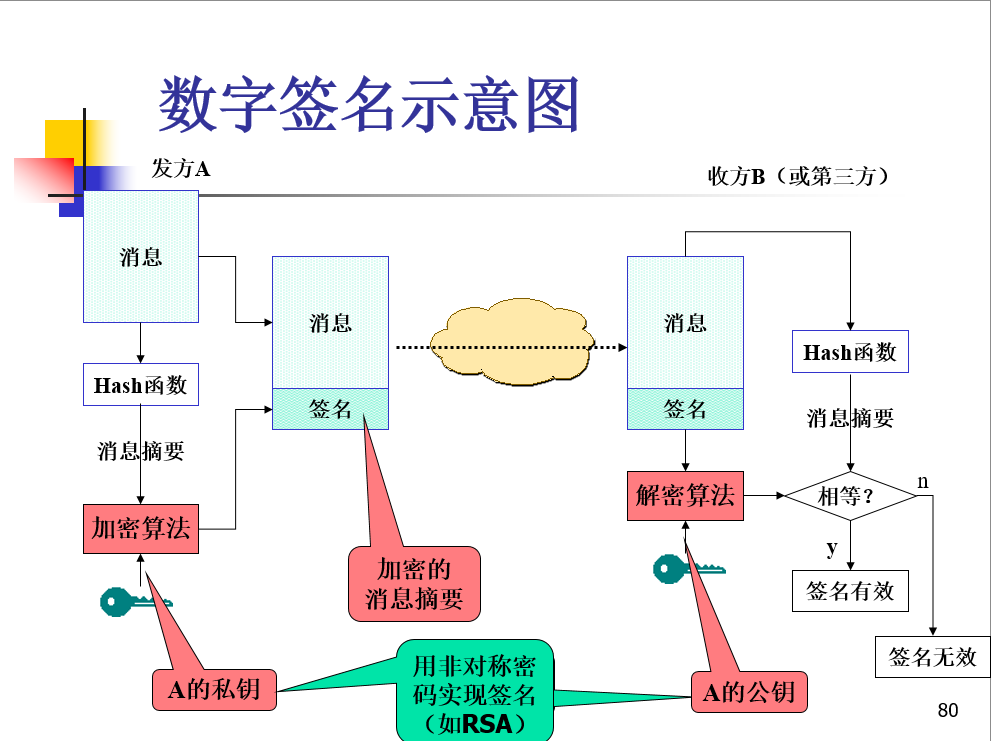
(1)给定x，计算y=fk(x)是容易的；

(2)给定y, 计算x使x=fk-1(y)是不可行的。

(3)存在k，已知k 时,对给定的任何y，若相应的x存在，则计算x使fk-1(y)是容易的，k即为函数陷门。

7.对称密钥和非对称密钥的区别：对称密钥加解密使用的同一个密钥，或者能从加密密钥很容易推出解密密钥；而非对称密钥算法加解密使用的不同密钥，其中一个很难推出另一个密钥

8.数字签名的过程（可以结合图示）



9. 数字签名的特性：

1）签名是可信的：任何人都可以方便地验证签名的有效性

2）签名是不可伪造的：除了合法的签名者之外，任何其他人伪造其签名都是困难的（计算上不可行）

3）签名是不可复制的：对一个消息的签名不可通过复制变成对另一个消息的签名。如果一个消息的签名是从别处复制的，任何人都可以发现消息与签名之间的不一致性

4）签名的消息是不可改变的：经签名的消息不能被篡改。一旦签名的消息被篡改，则任何人都可以发现消息与签名之间的不一致性

5）签名的不可抵赖性：签名者不能否认自己的签名

10.PKI的中英文解释和用途：

也称公开密钥基础设施（Public Key Infrastructure）。是一种遵循标准、利用公钥加密技术提供安全基础平台的技术规范。

11．VPN（虚拟专用网络）

通常指在公用网络中，利用隧道技术，建立一个临时的、安全的网络。

1. 成本低（2）安全保障（3）服务质量保障（4）可管理性（5）可拓展性

### 第十二章网络空间安全治理：

1.信息安全的主要特征：

保密性：确保信息只被授权人访问。防被动攻击。保证信息不被泄漏给未经授权的人。

完整性：防主动攻击。防止信息被未经授权的篡改。

可用性：保证信息及信息系统在任何需要时可为授权者所用。

可控性：对信息及信息系统实施安全监控

不可否认性：防抵赖

（前三点为信息安全三要素）

2.主动攻击与被动攻击的解释与举例：

主动攻击：主动攻击包含攻击者访问他所需信息的故意行为。包括拒绝服务攻击（DOS）、分布式拒绝服务（DDOS）、信息篡改、资源使用、欺骗、伪装、重放等攻击方法。

被动攻击：亦称“反应性攻击”，被动攻击主要是收集信息而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。

3.网络空间安全的目标：

1）“进不来”：访问控制机制

2）“拿不走”：授权机制

3）“看不懂”：加密机制

4）“改不了”：数据完整性机制

5）“逃不掉”：审计/监控/签名机制

6）“打不垮”：数据备份与灾难恢复机制

4.APPDRR动态安全模型的六个关键环节，每个环节的作用和地位

1）风险分析（Assessment）

2）安全策略（Policy）

3）系统防护（Protection）

4）实时监测（Detection）

5）实时响应（Reaction）

6）灾难恢复（Restoration）

·APPDRR模型：隐含了网络安全的相对性和动态螺旋上升的过程

·不存在百分之百的静态的网络安全，网络安全表现为一个不断改进的过程。

·通过风险评估、安全策略、系统防护、动态检测、实时响应和灾难恢复六环节的循环流动，网络安全逐渐地得以完善和提高，从而实现保护网络资源的网络安全目标。

5.网络安全保障的三大支柱：

1）网络及信息安全技术

2）信息安全法律法规

3）信息（网络空间）安全标准

6．计算机犯罪（刑法）

·计算机犯罪的定义：指行为人通过计算机操作所实施的危害计算机信息系统（包括内存数据及程序），以及其他严重危害社会的，并应当处以刑罚的行为

·计算机犯罪的常用方法：

1. 以合法的手段为掩护，查询信息系统中不允许访问的文件，或者侵入重要领域的计算机信息系统
2. 利用技术手段（如破解帐号密码、使用病毒木马、利用系统漏洞和程序及网络缺陷），非法侵入重要的计算机信息系统，破坏或窃取信息系统中重要数据或程序文件，甚至删除数据文件或者破坏系统功能，直至使系统瘫痪
3. 在数据传输或者输入过程中，对数据的内容进行修改，干扰计算机信息系统
4. 未经计算机软件著作权人授权，复制、发行他人的软件作品，或制作、传播计算机病毒，或制作传播有害信息等

7.信息系统安全保护法律法规

·构成：命令性规范、禁止性规范。

·我国信息系统安全保护法律规范的体系

问：我国对信息系统安全的保护主要通过三大体系予以保障，这三大体系是什么？

我国对信息系统安全的保护主要通过三大体系予以保障

1）基本法律体系

2）政策法规体系

3）强制性技术标准体系：

代表性标准（容易出选择题）：《计算机信息系统安全保护等级划分准则》、《计算机信息系统安全专用产品分类原则》、《计算机场地安全要求》等

8. 信息系统安全保护法律规范的基本原则：

1）谁主管谁负责的原则

2）突出重点的原则

3）预防为主的原则

4）安全审计的原则

5）风险管理的原则