## 第三讲 对称密码

1. 密码学发展大致阶段及各阶段的特点：
2. **古典密码时期**：

起始时间：从古代到19世纪末，长达几千年。 

技术工具：手工。 

通信手段：信使。 

密码体制：纸、笔或者简单器械实现的代换及置换，是一种艺术（富有创造性的方

式、方法）。

 典型密码：凯撒密码、维吉尼亚密码等。

1. **近代密码时期**：

起始时间：从20世纪初到20世纪50年代，即一战及二战时期。

技术工具：机械设备。 

通信手段：电报。 

密码体制：手工或电动机械实现复杂的代换及置换，仍是一门艺术。

典型密码：Vernam密码、转轮密码等。

1. **现代密码时期**：

起始时间：从1949年至今。 

技术工具：计算机。(针对二进制的比特位，而不是字符) 

通信手段：无线通信、有线通信、计算网络等。 

密码体制：对称密码(分组密码、序列密码)和非对称密码(公钥密码)，有坚实的数学理

论基础，成为一门科学。

典型密码：DES、AES、RC4、RSA、SHA等。

1. 现代密码的两次飞跃和两个里程碑事件
2. 1949年Shannon发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成了一门科学。（第一次飞跃）
3. 1976年后，美国数据加密标准（DES）的公布使密码学的研究公开，密码学得到了迅速发展。（里程碑的事件） 
4. 1976年，Diffe和Hellman发表《密码学的新方向》，提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元。（第二次飞跃） 
5. 1978年由Rivest、Shamire和Adleman首先提出第一个实用的公钥密码体RSA，使公钥密码的研究进入了快速发展阶段。 （里程碑的事件）
6. 密码算法公开的意义
7. 有利于增强密码算法的安全性；
8. 有利于密码技术的推广应用；
9. 有利于增加用户使用的信心；
10. 有利于密码技术的发展。

* DES事件成为现代密码史上里程碑的事件，其主要 贡献在于密码算法公开，密码进入了更广泛领域。

1. DES（分组密码）加密算法的要素以及安全性

见纸；

1. 子密钥的生成算法是迭代分组算法的一个重要组成部分，目的是从初始(种子)密钥产生各轮迭代使用的子密钥。也就是说，轮函数F的功能是在子密钥的参与和控制下实现的，子密钥的生成很重要，其评价指标： 

实现简单、速度快，满足轮函数F的要求；

种子密钥的所有比特对每个子密钥比特的影响应大致相同;

1. 轮函数F是分组密码的核心，是分组密码中单轮加解密函数，其基本准则：

非线性：体现算法复杂度

可逆性：能够实现解密

雪崩效应：输入(明文或密钥)即使只有很小的变化，也会导致输出(密文)产生巨大的

变化现象

其主要性能指标是安全性、速度、灵活性(成本)。

1. DES解密算法和加密算法是相同的，只是子密钥在迭代过程中输入次序相反，这是DES算法的优点。
2. DES的设计思想及其含义
3. 扩散：所谓扩散，是指要将算法设计成明文每一比特的变化尽 可能多地影响到输出密文序列的变化，以便隐蔽明文的统计 特性。形象地称为雪崩效应。
4. 混乱：所谓混乱，指在加解密变换过程中明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用解析法(即通过建立并求解一些方程)进行破译攻击

混乱可以用“搅拌机”来形象地解释，将一组明文和一组密钥输入到算法中，经过充分混合，最后变成密文。同时要求，执行这种“混乱”作业的每一步都必须是可逆的，即明文和密钥混乱以后能得到密文，反之，密文和密钥经过逆向的混乱操作后能恢复出明文。（按照混乱原则，分组密码算法应有复杂的非线性因素）

1. 密钥序列产生器的基本要求
2. 种子密钥K的长度足够长，一般应在128位以上；
3. 极大周期：至少大于所 需使用密钥序列的长度， 否则出现使用相同密钥；
4. 随机性；
5. 不可逆性；
6. 雪崩效应；
7. 密钥序列{ki}不可预测的。
8. 现代密码体制的分类以及对称密码的分类
9. 对称密码体制：加密密钥和解密密钥相同，或者虽然不相同，但由其中一个可以很容易地推出另一个，又称传统密码体制、秘密密钥体制或单密钥体制。

* 从密钥使用方式上分为分组密码和序列密码。

1. 非对称密码体制：加密密钥和解密密钥不相同，并且从一个很难推出另一个，又称公钥密码体制。公钥密码体制用一个密钥进行加密(验证)，而用另一个进行解密(签名)。其中一个密钥可以公开，成为公开密钥，简称公钥；另一个密钥需要秘密保存，称为私有密钥，简称私钥。

## 第四讲 公钥密码

1. Diffie-Hellman密钥交换方案

前提条件：Bob和Alice公开协商p和g，所有用户均可获取。

详情见纸；

1. 公钥密码的基本思想
2. 1976年底，W．Diffie和Hellman发表了著名的文章《密码学 的新方向》，首次提出了公钥密码算法的思想。
3. 具体内容：加密密钥和解密密钥不同，其中加密密钥公开，解密密钥秘密保存，这样可以解决密钥安全传递问题。
4. 公钥密码体制是现代密码学的一个标志，到目前为止，是密码学史上最大且唯一真正的革命。
5. 利用公钥密码的密钥分发过程

第一步：A向B发出会话密钥请求，请求内容包括A的身份、一次性随机数N1以及利用B

的公钥加密一次性会话密钥Ks。

第二步：B使用会话密钥Ks 加密一次性随机数N1 ,并将加密结果发送给A。

第三步：A使用会话密钥Ks 加密f(N1),并将加密结果发送给B。

1. RSA公钥密码的简评

* 第一个实用的公开密钥算法。 
* 目前使用最多的一种公钥密码算法。 
* RSA的理论基础是数论的欧拉定理。 
* RSA的安全性依赖于大数的素因子分解的困难性。 
* 密码分析者既不能证明也不能否定RSA的安全性。 
* 既能用于加密也能用于数字签名。 
* 目前密钥长度1024位是安全的。

1. 公钥密码的优缺点：
2. 优点：
3. 密钥分发简单；
4. 需秘密保存的密钥量减少；
5. 可以实现数字签名和认证的功能。
6. 缺点：
7. 公钥密码算法比对称密码算法慢；
8. 密钥相对比较长；
9. 有数据扩展；
10. 对称密码的优缺点：
11. 优点：
12. 对称密码算法比公钥密码算法快；
13. 密钥相对比较短；
14. 没有数据扩展；
15. 缺点：
16. 密钥分配问题：需要安全信道进行保密通信，但很难实现
17. 密钥管理问题：密钥量大，易存在安全隐患；
18. 数字签名问题：对称密码体制中通信双方拥有同样的密钥，所以接收方可以伪造签名，发送方也可以否认发送过某消息，难于解决陌生人之间的身份认证和交易不可否认的问题。

## 第五讲 Hash函数及应用

1. Hash函数的性质
2. 输入：消息，“任意”长度。
3. 输出：哈希值，固定长度。
4. 容易计算：对干任意给定的消息，容易计算其哈希值。
5. 单向性：对于给定的哈希值h，要找到M使得H(M)＝h在计算上是不可行的。
6. 抗弱碰撞性：对于给定的消息M1，要发现另一个消息M2，满足H(M1)＝H(M2)在计算上 是不可行的。
7. 抗强碰撞性：找任意一对不同的消息M1，M2 ，使H(M1)＝H(M2 )在计算上是不可行的。
8. 雪崩效应：当输入消息有一点变化时，输出的哈希值有很大变化。
9. Hash函数实现的基本过程

见纸；

* MD5算法输出哈希值长度是128位，主要用于确保信息完整性，是计算机广泛使用的哈希算法之一。
* 以目前的计算能力，安全的哈希值长度为160位。

1. 消息认证实现的基本过程

见纸；

* 用于消息认证的最常见的密码技术是基于哈希函数的消息认证码

1. 数字签名实现的的基本过程

见纸；

* 数字签名的复制是有效的；而手写签名的复制品是无效的。

1. 数字证书包含内容及安全性
2. 内容：
3. 版本号：用来区分X.509 的不同版本。
4. 序列号：由发证机构给予每一个证书的分配唯一的数字型编号。
5. 认证机构标识：发证机构的名称。
6. 主体标识：证书持有者的名称。
7. 主体公钥：与该主体私钥相对应的公钥。
8. 证书有效期：证书有效时间包括两个日期：证书开始有效期和证书失效期。
9. 证书用途：描述该主体的公/私密钥对的合法用途。
10. 扩展内容：说明该证书的附加信息。

最后，发证机构签名：用发证机构的私钥生成的数字签名。

1. 安全性：

* 证书是以文件形式存在，是公开的，可复制的。
* 任何具有CA公钥（根证书/CA证书，自签名证书）的用户都可以验证证书的有效性
* 除了CA以外，任何人都无法伪造、修改证书。
* 证书的安全性依赖于CA的私钥。

1. 消息认证码和数字签名的对比

|  |  |  |
| --- | --- | --- |
|  | **消息认证码** | **数字签名** |
| **发送者** | 用对称密钥计算MAC | 用私钥生成签名 |
| **接受者** | 用对称密钥计算MAC | 用公钥验证签名 |
| **密钥分发问题** | 存在 | 不存在，但公钥需要另外认证 |
| **效率** | 高 | 低 |
| **完整性** | 支持 | 支持 |
| **认证性** | 支持(仅限通信双方) | 支持(可适用于任何第三方) |
| **不可否认性** | 不支持 | 支持 |

## 第六讲 恶意代码（计算机病毒）

1. 恶意代码的含义和特征
2. 含义：指在未经授权的情况下，在信息系统中安装、执行并达到不正当目的的程序。
3. 特征：
4. 可执行代码：嵌入一个正常程序中，通过运行正常程序而运行，或是一个独立的程

序。

1. 恶意目的：多数出于经济利益，部分源于“成就感”。
2. 强制安装：通常通过漏洞或“误”操作，未经用户许可安装软件的行为。
3. 难以卸载：未提供通用的卸载方式，卸载后可能还会复活。
4. 破坏性：不同的恶意代码对用户的电脑破坏程度差别很大。
5. 计算机病毒的含义和特点

* 计算机病毒产生的根本原因：计算机软、硬件所固有的脆弱性

1. 含义：计算机病毒是一段附着（寄生）在其他程序上的、可以自我繁殖（传染）的程序

代码。

法律性、权威性定义：指编制者在计算机程序中插入的破坏计算机功能或者数

据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码

1. 特点：
2. 可执行性：病毒是一段可执行程序，但一般不是一个完整的程序。
3. 传染性：具有把自身复制到其它程序的能力，病毒的基本特征，必备的特征。
4. 非授权性：强调病毒程序的执行对用户是未知的。
5. 寄生性：嵌入到宿主程序中，依赖于宿主程序而生存。
6. 隐蔽性：自身具有隐蔽能力，其传染过程也具有隐蔽能力。
7. 衍生性：为了逃避查杀，可以衍生出与原版本不同的变种。
8. 破坏性

* 病毒一般不以文件的形式独立存在，一般没有文件名，它隐藏在正常程序和文件中，是一种非完整的程序。

1. 计算机病毒的生命周期
2. 创造期：病毒的编写调试期。
3. 感染期：病毒的发布期，通过一定途径传播病毒。
4. 传播期：病毒不断地繁殖与传染。
5. 发病期：病毒的表现形式或破坏能力。
6. 发现期：病毒被检测、发现、隔离并被通报研究。
7. 根除期：使用检测及控制这种病毒的杀毒软件，消除病毒。
8. 灭绝：由于用户的防护，病毒难以生存和传播。
9. 计算机病毒的主要组成

见纸；

1. 计算机病毒的关键点
2. 存在方式：静态，动态

* 消除计算机病毒的关键还是清除静态病毒，这样就不会出现动态病毒。

1. 基本原理：传播方式，寄生方式，激活方式。
2. 举例：引导型病毒，文件型病毒，宏病毒，脚本病毒，蠕虫病毒，U盘病毒。
3. 计算机病毒的趋势
4. 计算机网络（互联网、局域网）成为计算机病毒的主要传播途径。
5. 计算机病毒变形的速度快并向混合型、多样化发展
6. 传播方式和运行方式的隐蔽性
7. 计算机病毒技术与黑客技术将日益融合
8. 物质利益或特殊目的将成为推动计算机病毒发展的最大动力
9. 哪些“好习惯”能避免计算机病毒入侵
10. 不要随意开放共享并且设置最大权限以及弱口令 
11. 及时打补丁，尤其常用系统补丁 
12. 不要安装使用盗版软件或来历不明的软件 
13. 谨慎下载并执行（或打开）软件或文件 
14. 不要浏览一些不良的恶意网站 
15. 杀毒软件要及时升级，并启动监控或定期查杀 
16. 增强网络安全意识

## 第七讲 网络防御（防火墙）

1. 防火墙、包过滤、NAT技术、VPN技术的含义
2. 防火墙：一种高级访问控制设备，置于不同网络安全域之间，它通过相关的安全策略来控制(允许、拒绝、记录)进出网络的访问行为。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和Internet之间的任何活动，保证了 内部网络的安全。
3. 包过滤：包过滤技术是基于IP地址来监视并过滤网络上流入和流出的IP包，它只允许与指定的IP地址通信。它的作用是在可信任网络和不可信任网络之间有选择地安排数据包的去向。

信息过滤规则是以其所收到的数据包头信息为基础，包头信息中包括IP源地址，IP目的地址、封装协议类型等

1. NAT技术：网络地址转换，可保护及隐藏内部网络资源并减少由于架设网络防火墙所引起的IP地址变动，方便网络管理，并可以解决IP地址不足的问题。
2. VPN技术：指通过一个公共网络建立一个临时的、安全的连接，是一条穿混乱的公用网络的安全和稳定的隧道，能提供与专用网络 一样的安全和功能保障。
3. 防火墙能实现的哪些功能

见纸；

1. 防火墙的不足(包括不能实现的具体功能)
2. 防火墙给人虚假的安全感。
3. 可能带来传输延迟、瓶颈及单点失效。
4. 防火墙不能实现的安全功能。

–不能防范来自内部的攻击;

–不能防范不通过它的连接;

–不能防范利用标准协议缺陷进行的攻击;

–不能防范数据驱动式的攻击；

–不能防范策略配置不当或错误配置引起的安全威胁;

–不能防范本身安全漏洞的威胁;

1. 防火墙发展的趋势：多功能化，性能方面，分布式防火墙，强大审计和自动分析，与其他网络安全技术的结合
2. 入侵检测、漏洞扫描、漏洞、补丁的含义
3. 入侵检测：形象的说，它就是一台网络摄象机，能捕获并记录网络上的所有数据；同时它也是智能摄象机，能够分析网络数据并提炼出可疑的、异常的网络数据；它还是X光摄象机，能穿透一些巧妙的伪装，抓住实际的内容。

* 为什么需要入侵检测系统：

-内部的非法行为难于控制；

-外部的入侵行为难于杜绝；

-需要对网络内部进行实时检测，主动发现入侵行为或非法行为，以提高网络的安全性。

1. 漏洞扫描：对重要计算机信息系统进行检查，发现其中可被黑客利用的漏洞。漏洞扫描的结果实际上就是系统安全性的一个评估。是网络安全防御中的一项重要技术。
2. 漏洞：指硬件、软件或策略上存在的的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

* 漏洞与bug不等同。大部分的Bug并不涉及安全性，也就不构成漏洞；大部分的漏洞来源于Bug，但并不是全部，它们之间只是有一个很大的交集。

1. 补丁：为了加强软件的功能而推出。安全补丁是软件开发厂商为堵塞安全漏洞，提高软件的安全性和稳定性，开发的与原软件结合或对原软件升级的程序。当前打补丁是“堵”漏洞最有效的方法。

## 第八讲 网络攻击

1. 网络攻击与病毒对比有哪些不同
2. 攻击一般有明确的对象，如服务器、特定的主机等，而病毒传染不区分对象；
3. 针对的对象不同，攻击的目标有区分，如攻击对象不能正常工作、窃取信息、控制等等，而病毒程序的破坏是无区的；
4. 针对的对象不同，攻击的手段有差异的，如DOS、植入木马、欺骗等等，而同种病毒的传染手段基本一致。
5. 从安全属性看，攻击类型可分为哪些，以及各自的特点
6. 截取攻击: 可使非授权者得到信息系统的敏感信息，这是一种针对机密性的攻击；
7. 篡改攻击：是非授权者不仅获得信息，而且能修改信息，这是一种针对完整性的攻击
8. 伪造攻击：非授权者在系统中冒充合法的实体，这是一种针对真实性(认证性)的攻击
9. 阻断攻击：使系统的服务被停止，用户无法正常使用，这是一种针对可用性的攻击。
10. 木马的含义以及木马攻击的过程
11. 含义：指附着在应用程序中或者单独存在的一些恶意程序，可以利用网络远程响应网络另一端的控制程序的控制命令，实现对感染木马程序计算机的控制，窃取感染木马程序计算机上的机密资料。由客户端和服务端组成。

* 传染性是病毒最本质的性质之一。
* 与计算机病毒相比，木马主要以偷盗为主，偷取机密文件，记录各种密码，为黑客提供控制受害者机器的后门等。木马不具有自我复制性。
* 木马主要实现的技术：自动启动技术，隐蔽技术，远程监控技术。

1. 攻击过程：

见纸；

* 木马攻击核心技术在于植入

1. DoS的含义以及DDoS的攻击过程
2. 含义：拒绝服务攻击简称。是阻止或拒绝合法使用者存取网络服务的一种破坏性攻击方式。攻击广义上，Dos可以指任何导致服务器不能正常提供服务的攻击。
3. DDOS（分布式拒绝服务）攻击过程：
4. 探测：攻击者使用扫描工具探测扫描大量主机以寻找潜在入侵目标。
5. 植入：黑客设法入侵有安全漏洞的主机并获取控制权。这些主机将被用于放置木马。
6. 管理：黑客在得到入侵计算机清单后，从中选出满足建立网络所需要的MasterServer，放置已编译好的守护程序，并对被控制的计算机发送命令。
7. 命令：黑客发送控制命令给MasterServer ，准备启动对目标系统的攻击。
8. 实施：MasterServer发送攻击信号给被控制计算机开始对目标系统发起攻击。
9. 结果：目标系统被无数的伪造的请求所淹没，从而无法对合法用户进行响应，DDoS攻击成功。
10. TCP三次握手为例描述DoS攻击基本原理，为什么DoS难根除？
11. 客户端向服务器发送具有虚假IP源地址的SYN，服务器响应虚假IP源地址并保持连接等待ACK，但服务器无法收到客户端的ACK报文（第三次握手无法完成），处于半连接状态，如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源：数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的CPU时间和内存。服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正 常请求（毕竟客户端的正常请求比率非常之小），最后的结果往往是系统崩溃，不能正常工作。
12. 由于可以通过使用一些公开的软件进行攻击，它的发动较为简单，能够迅速产生效果，同时要防止这种攻击又非常困难。从某种程度上可以说，拒绝服务攻击永远不会消失，而且从技术上目前还没有根本的解决办法。

## 第九讲 信息系统安全

1. 信息系统自身安全的基本要素：身份认证，访问控制，安全审计，数据安全（详情见纸）
2. 身份认证的作用和意义

* 身份信息的认证是对我们现实世界的数字模拟。
* 保密用来确保信息的机密性，防止窃听攻击；
* 认证用于确保信息或身份的真实性，防止篡改或假冒攻击。

1. 计算机网络信息系统中，各种计算资源（如：文件、数据库、应用系统）需要认证机制的保护，确保这些资源被授权的人使用。
2. 身份认证是对网络中的实体进行验证的过程，必须提供实体真实性的证明。在大多数情况下，身份认证机制与访问控制和审计等应用紧密结合在一起，否则，这些应用无法实现。
3. 身份认证往往是许多应用系统中安全保护的第一道设防，它的失败可能导致整个系统失败。
4. 零知识证明：

零知识证明实际上一种安全协议，该协议的一方称为证明者(Prover)，通常用P表示，协议的另一方是验证者(Verifier)，一般用V表示。零知识证明是指P试图使V相信某个论断是正确的，但却不向V提供任何有用的信息，或者说在P论证的过程中V得不到任何有用的信息。也就是说，零知识证明除了证明证明者论断的正确性外不泄露任何其它信息或知识，或者说零知识证明是那种除了论证论题的有效性外不产生任何知识的证明。

*例如：若Alice要向Bob证明自己拥有某房间的钥匙，假设该房间只能用钥匙打开锁，而其它任何方法都打不开。这时有两个办法可 以完成上述任务：*

*1. Alice把钥匙出示给Bob ， Bob用这把钥匙打开该房间的锁；*

*2. Bob确定该房间内有某一物体，Alice用自己拥有的钥匙打开该房间的门(进入这个房间只能通过这个门)，然后把物体拿出来出示给Bob ，从而证明自己的确拥有该房间的钥匙。*

*第二个方法属于零知识证明，其好处在于在整个证明过程中 ， Bob 始终不能看到钥匙的样子，从而避免了钥匙的泄露。*

1. 基于Hash函数实现口令认证的好处

* 口令易实现、成本低、使用方便
* 口令信息实现安全传输
* 管理员不知道用户的口令

1. 基于Hash函数口令验证的过程：见纸；
2. 基于数字证书的单向身份认证协议

A向B发送（加密）EyB(Ks)||（签名）SxA(rA,IDA,IDB)、rA 、IDA、A的数字证书，其中A,B的公私钥对分别为(xA,yA)和(xB,yB)，Ks为会话密钥。 

B收到A发来的信息后，首先验证A的数字证书的有效性，然后验证签名S的有效性，最后使用自己的私钥解密得会话密钥。 

用户B选取随机数rB，使用会话密钥加密后发送给用户A。 

A收到后使用会话密钥解密后，计算后加密后发送给B。

1. 指纹身份认证的重要安全指标和主要方式

* 指纹具有终身不变性、唯一性和方便性，已几乎成为生物特征识别的代名词。
* 生物认证的关键技术在于生物特征值的提取和匹配。

1. 重要安全指标：
2. 错误接受率：衡量用户本应该遭到拒绝却被系统接受的可能性。
3. 错误拒绝率：衡量用户本应该被系统接受却遭到拒绝的可能性。
4. 主要方式：辨别（一对多匹配，他是谁？），验证（一对一，他是他自称的这个人吗？）
5. 访问控制和安全审计的含义
6. 访问控制：访问控制是实现既定安全策略(譬如权限)的系统安全技术，它通过某种方法管理着对所有资源的访问请求。

根据安全策略的要求，访问控制对每个资源请求做出许可或限制访问的判断，可以有效地防止非法用户使用资源和合法用户越权使用资源。访问控制是实现数据保密性和完整性的主要手段，美国国防部的可信计算机系统评估标准（TESEC）把访问控制作为评价系统安全的主要指标之一。

1. 安全审计：安全审计主要指对信息系统中与安全有关的活动及其相关信息进行识别、记录、存储和分析，贯穿计算机安全机制实现的整个过程，通常是实现系统安全的最后一道防线。通俗来讲，信息安全审计就是信息系统的“监控摄像头”。

## 第十讲 数据安全（数据备份）

1. 数据安全的原因有哪些；(数据为什么要备份？)

* 网络安全的核心也就是数据的安全

1. “硬”性灾难：系统设备、存储设备等硬件故障（44%），自然灾害（3%）；
2. “软”性灾难：计算机病毒等恶意程序（9%），误操作、恶意行为等人为错误（32%），系统软件、应用软件等软件故障（12%）。

* 数据备份除了拷贝外，还包括更重要的内容，如备份管理和数据恢复等。

1. 数据备份和数据恢复的含义；
2. 数据备份：数据备份是指为防止系统出现操作失误或系统故障等原因而导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。

* 目前数据备份通常采用网络备份
* 数据备份是存储领域的一个重要组成部分，也是信息系统不可缺少的部分。

1. 数据恢复是指当存储设备故障或系统崩溃等造成数据损坏时，通过转储或载入的数据备份重新安装数据的过程。

* 恢复技术依赖于备份技术

1. 数据备份的简评；

* 数据备份是信息系统不可缺少的部分； 
* 数据备份是需要代价的，有时影响系统正常运行； 
* 数据备份贵在坚持，尤其系统一直稳定运行时； 
* 数据备份是为数据恢复做准备的； 
* 数据备份要有专人负责； 
* 数据备份的内容依赖系统的功能，或数据的重要程度。 
* 一般来说，数据备份技术并不保证系统的实时可用性；

1. 应用恢复的主要指标是什么，其含义是什么？
2. 恢复点目标RPO：

* 恢复点：宕机后数据开始恢复的时间点。
* 恢复点指标RPO：指当灾难发生后，系统和数据能够恢复到的时间点要求。
* RPO对应着灾难造成的数据丢失: 如果RPO=0，相当于没有任何数据丢失，否则，就需要进行业务回复处理，修复数据丢失

1. 恢复时间目标RTO：该指标是应用恢复的时间指标

广义上来说，是从灾难发生造成业务中断，直到使业务能够得以继续所需要的时间。通常RTO越短意味着应用恢复能力越高。

1. 集中存储的好处；

* 空间利用率高
* 扩展能力强
* 数据安全性高
* 便于管理
* 可靠性高

1. RAID的关键目标及RAID5的特点；
2. 关键目标：

* 数据可靠性：通过把相同数据同时写入到多块磁盘（典型地如镜像），或者将计算的校验数据写入阵列中来获得冗余能力。在这样的冗余机制下，当磁盘出现故障时可以用新磁盘替换故障磁盘，并重建丢失的数据，保证数据一致性。
* 性能：数据分散保存在 RAID 中的多个不同磁盘上，并发数据读写要大大优于单个磁盘，因此可以获得更高的 I/O 带宽。

1. RAID 5（三分之一冗余）： 是一种存储性能、数据安全和存储成本兼顾的存储解决方案。
2. 容灾的含义、分类及灾难的后果有哪些；
3. 含义： 容灾是指为了保证关键业务和应用在经历各种灾难后，仍然能够最大限度的提供正常服务的所进行的一系列系统计划及建设行为。

目的：确保业务连续性

容灾技术是系统的高可用性技术的一个组成部分

1. 分类：

* 按生产中心和容灾中心的距离分类：本地容灾，近距离容灾，跨地域远距离容灾；
* 按容灾系统的应用分类：数据级容灾，系统级容灾，应用级容灾。

1. 后果：

* 有形资产灾难：硬件系统的损毁，软件系统的崩溃，企业生产的中断。
* 无形资产灾难：数据信息的丢失，系统服务的中止，企业信誉的受损。

1. 了解Share78 容灾国际标准分级原则及各级主要特点。
2. 分级原则：

* 备份/恢复的范围
* 灾难恢复计划的状态
* 应用地点与备份地点之间的距离
* 应用地点与备份地点如何相互连接
* 数据是怎样在两个地点之间传送的
* 允许有多少数据丢失
* 怎样保证备份地点数据的更新
* 备份地点可以开始备份工作的能力

1. 第一级：卡车异地备份

第二级：卡车＋热备站点

第三级：在线数据恢复

第四级：活动状态的备份中心

第五级：双活数据中心

第六级：零数据丢失

## 第十一讲数字内容安全

1. 数字内容的含义以及面临的威胁
2. 含义：以数字形式存在的文本、图像、视频、音频等信息，它可以存储在如光盘、硬盘等数字载体上，并通过网络等手段传播。

* 数字内容是信息的一种表现形式。 
* 数字内容的记录载体是数字化设备。 
* 数字内容的传播手段是网络。

1. 威胁：数字内容的非法复制，数字内容的篡改，数字内容的伪造，数字内容的失控。
2. 信息隐藏技术模型以及其主要特征
3. 模型：见纸；
4. 主要特征：不可感知性，鲁棒性（保持信息的完整性），隐藏容量。
5. 数字水印的含义及主要特点
6. 含义：数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并且不影响宿主数据的可用性。
7. 特点：隐蔽性，鲁棒性，安全性
8. 数字水印的主要应用：版权保护，盗版跟踪，拷贝保护，防伪。
9. 信息隐藏与数字水印的主要区别

|  |  |  |
| --- | --- | --- |
|  | 信息隐藏 | 数字水印 |
| 用途 | 用于保密通信 | 用于版权标识 |
| 前提 | 一般不知有信息隐藏(如果已怀 疑有隐藏信息，则已经不安全) | 可以公布有水印 存在 |
| 主要攻击 | 隐写分析(分析是否正常载体) | 水印擦除 |
| 主要考核 | 不可感知性 | 鲁棒性 |

1. 了解数字版权管理的基本原理：见纸；
2. 了解描述内容监管的主要过程：见纸；

## 第十二讲其它安全(区块链 大数据安全)

1. 区块链的含义、主要技术以及主要特点
2. 含义：狭义来讲，区块链是一种由多方共同维护并按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式 。

简单地说，区块链是分布式数据存储、点对点传输、共识机制、密码算法等计算机技术的新型应用模式

1. 主要技术：密码技术，共识机制，智能合约。
2. 特点：

* 去中心，去信任：按照系统制定的规则进行，共同监督，节点之间无法欺骗。
* 开放，共识
* 交易透明，双方匿名：公开透明
* 不可篡改，可追溯

1. 区块链的简评

* 区块链不是数据革命，是信任革命(解决中介信任问题)； 
* 区块链技术是一种新型的底层 IT技术，不是一种产品； 
* 比特币是区块链的应用； 
* 区块链是“全民”记账，具有更高可靠性、容错性； 
* 区块链去中心，没有特权； 
* 区块链能更好地实现高效、低成本； 
* 区块链更容易溯源，找问题的源头；
* 区块链更好地实现制度化、规则化，体现公平性。

1. 大数据下为何个人隐私问题突出

* 大数据特点：大量，高速（数据增长速度），多样，低价值密度。

1. 个人隐私数据不断“公开化”
2. 掌控个人隐私数据的企业约束了差
3. 个人的隐私数据保护的意识淡薄
4. 技术上的进步，体现在计算机软硬件上
5. 简述应从几个方面实现隐私防护：技术，国家，企业，个人。

## 第十三讲 信息安全管理

1. 信息安全管理的主要原则

* 策略明确原则
* 系统工程原则
* 综合保障原则
* 以人为本原则
* 首长负责原则
* 预防为主原则
* 风险评估原则
* 动态持续原则
* 成本效益原则
* 均衡防护原则

1. PDCA模型： P(plan)：计划；D(do)：实施；C(check)：检查；A(action)：改进
2. 网络态势感知（CSA）的含义：指在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，而最终的目的是要进行决策与行动。
3. 了解《网络安全法 》《密码法》

亮点：明确了网络空间主权的原则；

 明确了网络产品和服务提供者的安全义务；

 明确了网络运营者的安全义务；

 进一步完善了个人信息保护规则；

 建立了关键信息基础设施安全保护制度；

 确立了关键信息基础设施重要数据跨境传输的规则

1. 标准、测评、认证之间的关系
2. 标准：国际标准，区域标准，国家标准，行业标准，企业标准。
3. 测评与认证：
4. 信息安全测评：

* 依据标准对信息技术产品、系统、服务提供商和人员进行测试与评估，检验其是否符合测评的标准。
* 信息安全测评是检验/测试活动。

1. 信息安全认证：

* 对信息技术领域内产品、系统、服务提供商和人员的资质、能力符合规范及安全标准要求的一种确认活动，即检验评估过程是否正确，并保证评估结果的正确性和权威性。
* 信息安全认证是质量认证活动，更确切地说是产品认证活动

1. 两者关系：信息安全测评为信息安全认证提供必要的技术依据。