第 1 讲 概述

➢网络空间安全的含义（本身、环境、层次）（重点，必考）

信息安全保密性、完整性、真实(认证)性、不可否认性和所寄生信息系统的安全性。
网络安全是指网络系统的硬件、系统软件及其应用中的数据受到保护，不因偶然的或者恶意的原因而遭受到泄露、破坏、更改、假冒、抵赖等，系统连续可靠正常地运行，网络服务不中断。
网络空间安全涉及安全问题，分别对应这个四个层面：设备、运行、数据、内容。（必考）

➢网络空间安全的主要威胁都有哪些（重点，必考）

1.窃取 2.篡改 3.假冒 4.抵赖 5.破坏 6.中止服务 7.非授权访问
其它，譬如重放、流量分析、盗版、恐吓等。

➢网络空间安全的主要目标及相关术语解释（重点，必考）

“进不来”——身份认证机制 (认证) “拿不走”——授权机制(角色)
“看不懂”——加密机制 “改不了”——完整性机制
“逃不掉”——监控和审计机制 “打不跨”——备份和可用机制
机密性、完整性、认证性、不可否认性、可用性、可控性、可追踪性

➢了解网络空间安全发展历程(重点：信息保障（保护、检测、反应、恢复）)（重点，必考）

信息保障 IA(Information Assurance)的模型(PD2R)中，除了要进行信息安全保护，还应该重视提高安全预警能力、系统的入侵检测能力，系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。

第 2 讲 密码基础与对称密码

➢密码系统的组成（重点）

明文（有意义的文字）、密文（无意义的乱文字）
加密算法（由接线板、轮子、反射器三部分构成）和解密算法
密钥（接线板连线、轮子排序、轮子位置）

➢现代密码体制的分类以及对称密码的分类（重点）

对称密码体制(Symmetric Syetem)、非对称密码体制(Asymmetric System)
从密钥使用方式上分为分组密码和序列密码。

➢Enigma 的组成及其各部分的作用（重点）

键盘：操作方便，易掌握，速度快。 接线板：增加密钥量(单表代换)
轮子：增加加解算法复杂度(多表代换) 反射器：使得加解密算法相同。

➢实用密码设备应必备的要素（重点）（必考）

安全、性能、成本、易用(适用性)

➢现代密码的两次飞跃和两个里程碑事件（重点）

1.1949 年 Shannon 发表题为《保密系统的通信理论》，（第一次飞跃）
2.1976 年后美国数据加密标准（DES）的公布（里程碑的事件）

3.1976 年，Diffe 和 Hellman 发表了**《密码学的新方向》**（第二次飞跃）
4.1978 年由 Rivest、Shamire 和 Adleman 首先提出**第一个实用的公钥密码体制 RSA**（里程碑的事件）

➢分组的设计思想及其实现过程（重点）

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。**
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。

➢序列密码的特点、应用模型

运算速度快、密钥相对比较短、没有数据扩展

➢对称密码的优缺点（重点）（必考）

密钥分发难以实现；需秘密保存的密钥量大，难以维护；难以实现数字签名和认证的功能。

作业：
Q：为什么需要每日密钥、通信密钥，而不是双方协商同一密钥后就一直使用？给我们的启示是什么？
答：每日密钥，就是每天使用的密钥，来自于机要部门下发的“密码本”，是用来加密通信密钥的；通信密钥，也称会话密钥，针对一个会话（譬如任务）而生成的密钥，用来加密通信信息，一旦会话结束，会话密钥就可舍弃。
密钥分为每日密钥、通信(会话)密钥，这大大提高 Enigma 密码机应用的安全性，**因为长时间使用同一密钥，由此产生大量密文，有利于敌手破译，还有可能增加泄露密钥风险(譬如内奸等)。**
启示：密码系统的安全性来自**密钥的安全性**；（如密码设备被敌手得到(可能性大)，加解密算法就被敌手掌握了）**密钥需要定期更新；**（密钥按需要动态变化的，如新任务开始就要使用新的密钥）**密钥分发在实际应用中是件重要和困难的事**。（如密码本的管理）

Q:在实际应用中，为什么密码本是核心？得到敌手的密码本就能够破译其密文了？给我们的启示是什么？
答：**因为密码算法很难不能被敌手得到**，譬如通过战争的缴获、内奸、密码专家 分析等等，**而密码本易于控制，且不同使用对象密码本不同，所以，密码本是核心，**敌手得到密码本就能破译密码。
启示：密码系统的安全性并不取决对密码算法的保密，而是由密钥的保密性决定的。

Q:如果需要增加 Enigma 密码机的安全强度，通常需要怎么做？为什么？
答：**增加轮子。**因为**轮子决定了 Enigma 密码机加解密算法的复杂程度，轮子越多，算法复杂度就越高**.

Q:假设你使用的计算机具有如下能力: 1.每台计算机每秒可尝试 1 百万(10^6)个密钥。2.共有 100 万(10^6)台计算机参与并行使用。那么，遍历 64 比特、112 比特、128 比特的密钥分别大约需要多少年？(要求简 要过程) 注： $2^{10}\approx10^3$，
解：1 年=356*24*3600≈$3*10^7$ 秒，1 年遍历密钥个数≈$3*10^{19}$
$2^{64}\approx10^{19.2}$ $2^{112}\approx10^{33.6}$ $2^{128}\approx10^{38.4}$
年数≈1 年数≈10^{13} 年数≈10^{18}
答：大约分别为 1 年，10^{13} 年，10^{18} 年

第 3 讲 公钥密码

➢Diffie-Hellman 密钥交换方案

发送方 A 查找接受方 B 的公钥；
A 采用公钥加密算法以 B 的公钥作为加密密钥对明文加密；
A 通过不安全信道将密文发送给 B；
B 收到密文后使用自己的私钥对密文解密还原出明文

➢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
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 2048 位是安全的

➢公钥密码的优缺点（重点）（必考）

密钥分发简单、需秘密保存的密钥量少、可以实现数字签名和认证的功能。
算法运算慢、密钥位数相对比较长、有数据扩展。

第 4 讲 哈希函数与应用

➢Hash 函数的性质及其安全性（重点）

固定长度、正向计算容易、逆向计算不行
抗弱碰撞性、抗强碰撞性、雪崩效应

➢消息认证码的含义及实现的基本过程（重点）

消息认证码（MAC）是与密钥相关的的单向哈希函数
信息的来源是真实的，验证消息的完整性（必考）

➢数字签名的含义及实现的的基本过程（重点）

所谓数字签名（Digital Signature），也称电子签名，是指附加在数据单元上的一些数据，这些数据是利用签名算法首先对该数据单元进行关键信息提取，然后使用签名者的独有信息进行签名而形成的，用于标识签名者的身份以及签名者对该数据单元的认可，并能被接收者利用签名者的公有信息来验证该数据单元是否被篡改或伪造或抵赖。

（以下实现过程必考）
系统初始化过程：生成数字签名方案用到的所有参数(主要包括签名者的公私钥对)。
签名生成过程：签名者使用自己的私钥利用给定的签名算法对消息产生签名 s=Signsk(m)。
签名验证过程：验证者使用签名者的公钥利用公开的验证算法对给定消息的签名进行验证，得出签名的有效性。Verpk(s,m)=0 或 1

➢数字证书包含内容及安全性

内容：版本号、序列号、认证机构标识、主体标识、主体公钥、证书有效期、证书用途、扩展内容、发证机构签名
安全性：1.证书是以文件形式存在，是公开的，可复制的。
2.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
3.除了 CA 以外，任何人都无法伪造、修改证书。

4.证书的安全性依赖于 CA 的私钥

作业：从生成、验证、效率、安全特性等多方面，请简要对比消息认证码和数字签名的异同。

	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，但公钥需要额外认证(譬如数字证书)
效率	高	低
完整性	支持	支持
认证性	支持(仅限通信双方)	支持(需要可信第三方支持)
不可否认性	不支持	支持

第 5 讲 恶意软件

➢恶意软件的含义和特征（重点）

含义：恶意软件是指在**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**软件**。

特征：**可执行代码、恶意目的、强制安装、隐蔽性、破坏性**

➢计算机病毒的含义和特点（重点）

目前最流行的定义：计算机病毒是一段附着在其他程序上的、可以自我繁殖的程序代码。

特点：**可执行性、传染性、非授权性、寄生性、隐蔽性、衍生性、破坏性（必考）**

➢计算机病毒的生命周期和主要组成（重点）

创造期、传播期、传染期、发病期、发现期、根除期、灭绝

引导模块、传染模块、表现模块

➢计算机病毒的关键点（重点）及简评

关键点：传染方式(核心)、寄生方式、激活方式

简评：1.计算机网络（互联网、物联网、通信网）成为计算机病毒的主要传播途径。

2.计算机病毒变形的速度快并向混合型、多样化发展并常针对最新计算机技术。

3.传播(染)方式和运行方式的隐蔽性

4.计算机病毒技术与黑客技术将日益融合

5.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

➢好习惯能避免计算机病毒入侵（重点）

✓ 不要**随意开放**共享并且设置最大权限以及**弱口令**；

✓ 取消文件夹隐藏共享，**显示文件的扩展名**；

✓ 不要**随意**安装使用盗版软件或来历不明的软件；

✓ **谨慎**下载并**执行（或打开）**软件或文件，尤其电子邮件的附件；

✓ 不要浏览一些**诱惑**的恶意网站；

✓ **及时打补丁，尤其常用系统补丁；**

✓ **杀毒软件要及时升级，并启动监控或定期查杀；**

✓ **养成做备份的好习惯，重要数据或文件一定要做备份；**

✓ **时刻有网络安全意识。**

第 6 讲 网络安全技术

➢防火墙（重点）、包过滤、DMZ、VPN（重点）的含义

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。（必考）

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，包头信息中包括端口号、IP 源地址和目的地址、封装协议类型等。当一个数据包满足过滤规则，则允许此数据包通过，否则拒绝此包通过，起到了保护内部网络的作用。

DMZ：DMZ 是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”

VPN：指通过一个公共网络建立一个临时的、安全的连接，是一条穿过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。

➢防火墙能实现的那些功能（重点）

包过滤：基于源 IP 地址、基于目的 IP 地址、基于源端口、基于目的端口
IP 与 MAC 的绑定、基于时间、基于流量(带宽)、MAP(地址/端口映射)、VPN 功能、日志审计

➢MAP 的好处以及 VPN 实现的功能（重点）

好处：公开服务器可以使用私有地址，隐藏内部网络的结构

功能：数据保密性、数据完整性、身份认证

➢防火墙的主要性能参数（记记记）

✓吞吐量：指防火墙在不丢包的情况下转发数据包的最大速率。
✓时延：指防火墙对数据包的存储转发时延，体现它处理数据的速度。
✓丢包率： 指防火墙在连续负载的情况下，由于资源不足应转发而未转发的包百分比。该指标与吞吐量有一定的关联性，吞吐量比较高的防火墙包丢失率一般比较低。
✓并发连接数：指穿越防火墙的主机之间或主机与防火墙之间能同时建立的最大连接数目，主要用来测试被测防火墙建立和维持 TCP 连接的性能，同时也体现防火墙接受客户端 TCP 连接请求的响应能力。
✓平均无故障时间（MTBF）
✓最大允许加载规则数：允许最多加载访问控制规则的条数

➢防火墙发展的简评

1.多功能化 2.性能方面：非常高的速率处理数据。
3.分布式防火墙 4.强大审计和自动分析
5.与其它网络安全技术的结合

➢入侵检测、漏洞扫描系统、漏洞、安全补丁的含义（提了一嘴）

入侵检测：是指对企图入侵、正在进行的入侵或已经发生的入侵进行**识别**的过程。

漏洞扫描系统：对网络和主机的安全性进行**风险分析和评估**的软件，是一种能自动检测远程或本地主机系统在安全性方面存在**弱点和隐患**的程序包。

漏洞：是指硬件或**软件**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。

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。

第 7 讲 网络攻击简介

➢网络攻击含义以及它与病毒对比有哪些不同。

“网络攻击”的含义：**任何非授权的攻击者通过计算机网络入侵目标系统的行为，包括查看、偷取、控制、修改、破坏、影响系统正常运行或服务等行为。**

对比：1.攻击一般有明确的**对象**，而病毒传染不区分对象；

2.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分的；

3.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。

➢从安全属性看，攻击类型有那些，各自的特点是什么。（重点）

攻击可分为物理攻击和非物理攻击，网络攻击分为被动攻击和主动攻击。

被动攻击（主要是收集信息而不是进行访问，合法用户对这种行为一般也不会觉察到。）：截取攻击

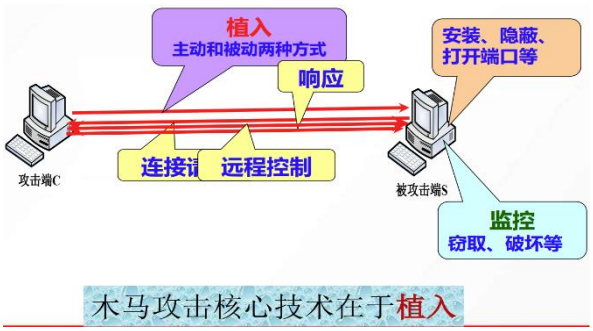
主动攻击（主要包含攻击者访问他所需信息的故意行为，合法用户对这种行为一般能够“觉察到”）：阻断攻击、伪造攻击、篡改攻击、重放攻击

从安全属性看，网络攻击类型可分为 5 类：

1.截取攻击（机密性）2.篡改攻击（完整性）

3.伪造攻击（认证性）4.阻断攻击（可用性）5.重放攻击

➢简要描述木马攻击的过程。（重点）



➢木马攻击的主要实现技术有哪些，其核心技术是什么，采用方式有哪些。（重点）

1.植入技术 2.自动启动技术 3.隐蔽技术 4.远程监控技术

主动(漏洞)、被动(欺骗或不经意)

➢DoS 的含义及以 TCP 三次握手为例描述 DoS 攻击基本思想。（重点）

“拒绝服务攻击（Denial of Service）”，简称 DoS，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。它的恶毒之处是通过向服务器发送大量的虚假请求，服务器由于不断应付这些无用信息而最终筋疲力尽，而合法的用户却由此无法享受到相应服务，实际上就是遭到服务器的拒绝服务

➢简要描述分布式拒绝服务(DDoS)的攻击过程。（重点）

探测——植入——管理——命令——实施——结果

➢简要描述 APT 攻击的过程

1.情报收集 2.社工攻击，网络攻击，渗透扩大 3.交互控制 4.目标实施

第 8 讲 信息系统安全

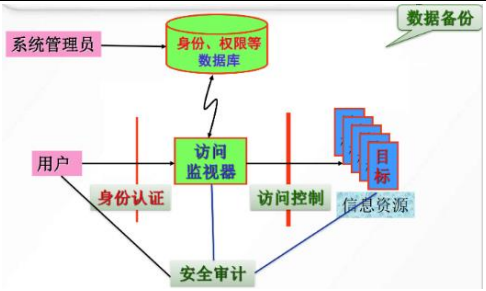
➢信息系统自身安全的基本要素包括那些（重点）

（身份认证、访问控制、安全审计、数据备份）

身份认证作用和意义：（重点重点）

1.身份认证就是确保身份的真实性，能够抵御假冒攻击。

2.身份认证是权限管理和审计等应用的基础，否则，这些应用无法实现。
3.身份认证往往是信息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的失败。



➢零知识证明含义（重点）

证明者试图使验证者相信某个论断是正确的，但却不向验证者提供任何有用的信息

➢基于 Hash 函数实现口令认证的好处

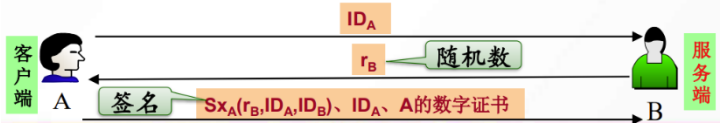
总：易实现、成本低、使用方便
1.明文口令不存储在任何地方；
2.口令是以其散列值传输和存储，保证口令的安全性；
3.系统管理员不知道终端用户口令。（三点表明：考考考）
安全目标：✓口令信息实现安全传输✓管理员不知道用户的口令

➢基于 Hash 函数口令更改和验证的过程

更改：
新口令——缺（旧）口令作密钥加密新口令——密文——公开信道——解密——哈希值——认证系统
验证：
输新明文口令——请求——返回随机数（提问）——与哈希值作运算——应答——对比哈希函数——是否匹配

➢基于 Ukey 的单向身份认证协议

1.客户端 A 向服务端 B 发送自己的标识 ID_A，表明自己是用户 A。
2.服务端 B 选取随机数 r_B，作为回应发送 r_B 给客户端 A。
3.客户端 A 收到 r_B 后向服务端 B 发送 $S_{xA}(r_B,ID_A,ID_B)$、ID_A、A 的数字证书，其中 x_A 为用户 A 的私钥。
4.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，从而确定用户 A 的身份。



➢指纹身份认证的重要安全指标和主要方式（重点）

安全指标：
1.错误接受率（False Accept Ratio，FAR）
衡量用户本应该遭到拒绝却被系统接受的可能性。通俗的理解为“把不应该匹配的指纹当成匹配的指纹”的概率。
2.错误拒绝率（False Reject Ratio，FRR）
衡量用户本应该被系统接受却遭到拒绝的可能性。通俗的理解为“把应该匹配成功的指纹当成不能匹配的指纹”的概率
主要方式：
1.辨识：这也叫"一对多匹配"。辨识其实是回答了这样一个问题：“他是谁？”
2.验证：一对一的比对来确定身份的过程。验证其实回答了这样一个问题："他是他自称的这个人吗？"

➢访问控制(权限)含义和功能

含义：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。
功能：**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。

➢安全审计的含义和好处

含义：安全审计是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**，是系统安全机制的一个**不可或缺**的部分。
好处：✓对潜在的攻击者起到**震摄或警告。**
✓对于**已经发生**的攻击行为提供**溯源和追纠证据。**
✓有助于系统管理员完善**安全策略**和实施有效**安全机制。**
✓有助于准确全面**评估**系统的安全状况。
✓有助于**数据恢复。**

第 9 讲 数据存储安全 数据备份

➢数据安全的原因有那些(数据为什么要备份？) （重点）

自然灾害、硬件故障、软件故障、恶意代码、人为错误

➢数据备份和数据恢复的含义

数据备份：是指为防止软硬系统出现损坏、故障、操作失误等原因而导致数据丢失，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存储介质的过程。
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。

➢数据备份的简评

数据备份是信息系统不可缺少的部分；是有代价的，需要投入及影响系统正常运行；贵在坚持，尤其系统一直稳定运行时；是为数据恢复做准备的；要有专人负责；策略与数据的重要程度密切相关；并不保证系统的实时可用性；考虑备份数据本身的安全问题，防止泄密。

➢应用恢复的主要指标是什么，其含义是什么（数据恢复是应用恢复的基础。）（重点）

1.恢复点目标 RPO(Recovery Point Object)
指当灾难发生后，系统和数据能够恢复到的时间点要求。
2.恢复时间目标 RTO(Recovery Time Object)
✓是指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。

➢集中存储的好处(相比早期附属存储形式相比)

1.资源集中管理 2.容量可扩展性 3.性能优化 4.数据共享
5.备份和恢复简化 6.安全性提升 7.成本效益 8.易于维护

➢RAID 的关键目标及 RAID5 的特点

关键目标：1.数据可靠性 2.性能
RAID 5 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。

➢容灾的含义、分类及灾难的后果有哪些

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。
分类：

按生产中心和容灾中心的距离分类

➢本地容灾

✓生产中心与容灾中心在同一建筑物内 ✓可抵御软件故障、硬件故障等本地灾难

➢近距离容灾

✓相距 10~200km 内 ✓可抵御火灾、停电、建筑物倒塌等局部性灾难

➢跨地域远距离容灾

✓相距 200km 以外 ✓可抵御地震、洪水、海啸等大范围灾难

按生产中心和容灾中心的备份内容分类

➢数据级容灾

✓数据同步或异步复制到容灾中心 ✓投资少，业务恢复时间长

➢系统级容灾

✓保证业务数据、系统数据、网络通信系统 ✓业务恢复时间短

➢应用级容灾

✓保护整个业务流程 ✓实现技术要求高，难度大，投资多

灾难后果：（重点）

➢有形资产灾难(直接损失)

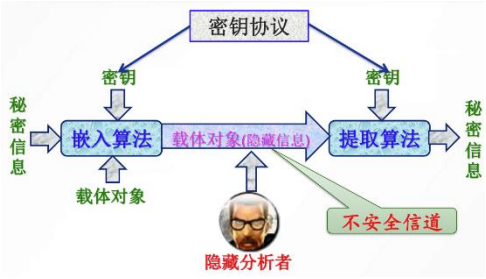
✓硬件系统的损毁✓软件系统的崩溃✓企业生产的中断

➢无形资产灾难(间接损失)

✓数据信息的丢失✓业务服务的中止✓企业信誉的受损

第 10 讲 数字隐藏和数字水印

➢信息隐藏技术模型以及其主要特征（重点）



不可感知性、鲁棒性、隐藏容量

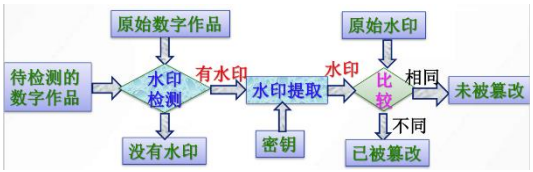
➢数字水印的含义及主要特点（重点）

含义：数字水印是永久镶嵌在其它数据（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

特点：

1.透明性 2.鲁棒性 3.安全性

➢基于非盲水印的检测过程（重点）



➢数字水印的主要应用

✓用于版权保护的数字水印✓用于盗版跟踪的数字指纹
✓用于拷贝保护的数字水印✓用于防伪的数字水印

➢信息隐藏与数字水印的主要区别（重点）

	信息隐藏	数字水印
载体内容	无关，一般一对一	有关，一对多
主要用途	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	安全性

第 11 讲 个人信息安全、社会工程学攻击（不讲）

➢简述应从几个方面实现个人信息防护

1.技术层面：尽力而为 2.国家层面：底线，法律法规
3.企业层面：重要性，关乎生存。4.个人层面：意识

➢社工攻击的特点

1.（社工攻击对象是人）（社工攻击武器是信息）
2.（社工攻击是反复迭代的）（社工攻击的普遍性）
3.（社工攻击利益受害者无防备的心理）
作业: 在我们日常生活学习中，如何尽可能避免或减少个人信息泄露
谨慎地给个人信息，慎入网站慎用“记住密码”，不用免费 Wifi，不泄露个人信息，不要公布他人的个人信息。

第 12 讲 信息安全管理 网络安全态势感知系统（不考）

➢信息安全管理的主要遵循原则

✓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

➢PDCA 模型

1.概要
P(plan)：规划 D(do)：实施 C(check)：检查 A(action)：处置
2.特征
PDCA 特点一：按顺序进行，不断循环。
PDCA 特点二：一层一层地解决问题。
PDCA 特点三：总结，再进行第二次 PDCA 循环。

➢安全态势感知的含义及三个层次

1.含义：态势感知就是在一定的时间和空间条件下，对环境因素的感知、理解以及对其未来发展趋势的预测。
2.层次（1）感知（感觉）（2）理解（3）预测

➢习主席的重要讲话（感知，深入）

原文：网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

含义：网络安全态势感知是在大规模网络环境中，对能够引起网络态势发生变化的所有安全要素进行获取、理解、评估以及预测未来的发展趋势，从而进行决策和行动。态势感知体系包括四个部分：态势察觉、态势理解和评估、态势预测和安全决策。

➢了解安全态势感知的实现过程

态势察觉、态势理解、态势评估、态势预测

英文缩写的中文解释（重点）一定考几题

DES (Data Encryption Standard) 数据加密标准
AES (Advanced Encryption Srandard)高级加密标准
RSA (Rivest, Shamir, Adleman) 公钥密码算法
MAC (Messages Authenticarion Code)消息认证码
DMZ (DeMilitarized Zone)隔离区或非军事化区
VPN (Virtual Private Network） 虚拟专用网
IDS (Intrusion Derection Sistem）入侵检测奈统
IPS (Instrusion Prevention Sustem）入侵防御系统
DDoS (Distibuted Denial of Service) 分布式拒绝服务
APT (Adranced Persistent Threat) 高级持续性威胁
RAID (Redundant Array of Independent Disks) 磁盘阵列

北京邮电大学 2023—2024 学年第一学期《网络空间安全导论》期中考试试卷
（总分：50 分）

1.是非判断题（5 分，每题 1 分，“v”表示正确，“x”表示错误）
(1)网络空间安全的目标就是保证网络空间的绝对安全。( )
(2)现代密码系统的安全性不应取决于不易改变的算法，而应取决于可改变的密钥。( )
(3)RSA 算法的安全性是依赖于基于分解大整数的困难问题，如果这个难题被攻破，那么 RSA 算法就不安全了。（ ）
(4)防火墙是网络安全的重要一环，通过合理地配置防火墙才能发挥出防火墙所具备的 功能。（ ）
(5)目前，网络攻击基本都来自于个人行为，其目的就是获取经济利益。（ ）
2．选择题（5 分，每题 1 分，每题只有一个选项最符合题目要求）
(1)按现在的计算能力，对称密码的密钥长度至少为( )才是安全的。
A.64 位 B. 128 位 C. 256 位 D.1024 位
(2)公钥密码体制的出现，解决了对称密码体制的密钥分发问题，在公钥密码算法中，加密对称密钥所使用的密钥是( )。
A.发送方的公钥 B.发送方的私钥 C.接受方的公钥 D.接受方的私钥
(3)设 hash 函数的输出长度为 n 比特，则安全的 hash 函数寻找碰撞的复杂度应该为（ ）。A.O(n) B.O(2n) C.O(2n-1) D.O(2n/2)
(4)防火墙哪项技术能够实现不公开内部服务器真实 IP 地址及隐藏内部网络结构。（ ）
A.包过滤技术 B. IP 与 MAC 的绑定 C. MAP (地址/端口映射) D. 带宽管理
(5)下面哪项安全技术能够对网络和主机的安全性进行风险分析和评估。（ ）
A.防火墙 B.入侵检测系统 C.漏洞扫描系统 D.防病毒软件
3.填空题（10 分，每空 1 分）
(1)信息安全保障包括保护、____、_____和恢复四个子过程，是一个完整的动态、不断循环上升的过程。
(2) Enigma 密码机出现是近代密码发展史中里程碑的事件，从这个事件得到启示，实用密码设备应必备四要素，即 ___、_____、成本、易用。

(3)消息认证的目的是指_____ 、____。
(4)计算机病毒的生命周期包括创造期、传播期、_____、发病期、发现期、_____和灭绝。 (5) 从安全属性看，攻击类型可分为 5 类：截取攻击、篡改攻击、_____、 阻断攻击和_____。 4.术语解释（共 6 分）
(1)完整性（2 分）

(2)Hash 函数（2 分）

(3)防火墙（2 分）

5.简答题（共 18 分）
(1)请指出公钥密码体制的优点与不足。(6 分)

(2)请描述数字签名实现的的基本过程。(4 分)

(3)请指出恶意软件的特征有哪些。(说出 4 点即可) 。(4 分)

(4) 简要描述分布式拒绝服务(DDoS)的攻击过程。(4 分)

6.灵活题（6 分）
(1)通过这门课的学习，谈谈你的收获和期望。(3 分)

(2)请评价这门课的教学（包括助教的工作）。(3 分)