**整理人：PB20 wkt mzy**

**由于是辅修，及格万岁，遗漏不少，仅供参考（狗头保命）**

**习近平:没有网络安全就没有国家安全,没有信息化就没有现代化.将网络空间安全提到国家战略高度.“网络空间的国际竞争方兴未艾”是我国网络空间安全面临重大挑战之一,个别国家强化网络威慑战略,加剧网络空间军备竞赛,世界和平受到新的挑战。**

1. **信息安全三要素:机密性;完整性;可用性**

**消息层次:机密性**:确保数据在存储和传输过程中不被非授权实体浏览,甚至不暴露保密通信的事实.*通过访问控制、加密变换实现.***完整性**:保障被传输、接收、存储的数据是完整和未被非法修改的.在被非法修改的情况下发现被修改的事实和位置.*通过访问控制、消息摘要算法来实现.信息的完整性有数据和系统的完整性.***网络层次:可用性:**指保障信息资源随时可提供服务的能力特性,即授权用户根据需要可以随时访问所需信息.当突发事件(故障、攻击等)发生时,用户依然得到或使用信息系统的数据,信息系统的服务亦能维持运行.*是信息资源服务功能和性能可靠性的度量,是对信息网络总体可靠性的要求.*

**信息安全模型**也称威胁模型或敌手模型。含：保密通信系统模型, 无仲裁认证模型,Dolev-Yao威胁模型(不低估攻击者) **IATF的信安原则**纵深层防御战略(核心是人|技术|操作)+ 保护多个位置+分层防御+安全强健性

1. **信息安全威胁分类:安全是相对的**

**信息泄露**:破坏了机密性；**非授权的篡改**:破坏了完整性**拒绝服务**:破坏了可用性；**非法使用(非授权访问)**:破坏了机密性；**假冒**:破坏了真实性,而没有破坏机密性(没有打开盒子)**抵赖**:破坏了不可否认性;**网络与系统攻击**:破坏了机密性、可用性、完整性等.如,缓冲区溢出攻击；**恶意代码**:破坏机密性、可用性、完整性等

1. **以智能手机为例,2个访问控制的例子数字安全证书**(CA**证书**)由可信任的第三方机构(CA中心)颁发给个人或者企业用户,来验证身份、数据签名、数据加密等操作；**智能手机可用于移动访问控制**.如智能门禁,公交卡等
2. **密码学=密码编码学+密码分析学；计算上安全**(1)破译密码的代价>密文信息的价值。(2)破译密码的时间>密文信息的有效生命期。
3. **一个密码系统有哪些要素？(P,C,K,E,D)密码体制**:加解密并解决网络安全中的机密性、完整性、可用性、可控性和真实性等问题；P称为**明文**空间,是所有可能的明文构成的集合；C称为**密文**空间K称为**密钥**空间；E和D分别表示**加密算法和解密算法**的集合,；它们满足；**对每一个k∈K,必然存在一个加密算法ek∈E和一个解密算法dk∈D,使得对任意m∈P,恒有dk(ek(m))=m**
4. **攻击密码体制(1)密码分析攻击(①唯密文攻击②已知明文攻击③选择明文攻击 ④选择密文攻击)(2)穷举攻击:对所有可能的密钥组合进行测试**
5. **现代密码思想置换和代换(单表多表)对称密码(分组密码+流(序列)密码,前者广泛)**
6. **对称密钥(传统)和非对称密钥(公钥)**

公钥安全性基于**数学上难解的问题**(单向陷门函数=大整数因子分解+离散对数),计算上**no由1密钥推知另1密钥**,秘密通信双方无需预先商定密钥,克服对称密码必须事先使用安全通道约定密钥的缺点.**陷门信息为私钥**

1. **RSA算法(公钥)的理论基础+流程**RSA是一种分组密码体制,理论基础是“**大整数的素因子分解是困难问题**”。**密钥计算方法:**①选择两个大素数p和q(典型值为1024位)②计算n=p×q和z=(p-1)×(q-1)③选择一个与z互质的数,令其为d④找到一个e使满足e×d=1(modz)⑤公开密钥为(e,n),私有密钥为(d,n)；**加密方法**:①将明文看成比特串,将明文划分成k位的块P即可,这里k是满足2k<n的最大整数.②对每个数据块P,计算C＝Pe(modn),C即为P的密文；**解密方法:**对每个密文块C,计算P＝Cd(modn),P即为明文.
2. **散列(哈希)函数**单向性、强抗碰撞性和弱抗碰撞性.使用最多MD5和SHA
3. **数字签名和消息鉴别**

消息认证码MAC和数字签名都属于**哈希函数应用(消息完整性)**的范畴,数字签名其实也是一种消息认证技术.**数字签名属于非对称密码体制,而消息认证码属于对称密码体制.消息认证码无法实现不可否认性.**认证分为实体认证和消息认证:**消息认证码只能实现消息认证**,数字签名则同时可以实现**实体认证和消息认证.数字签名比**前者**处理更慢**。MAC算法比加密算法**不要求可逆性,更不容易被攻破。**

1. 工作|会话|密钥加密|主机主**密钥管理**

密码系统安全性全取决于密钥的保密程度,**核心问题**确保密钥从产生-使用全过程安全可靠

1. **三重DES目前在计算上是安全的.**

被称为计算机第一定律的摩尔定律指IC上可容纳的晶体管数目,约**每隔18个月便会增加一倍,性能也将提升一倍.**双密钥三重DES算法的安全性:；破译它的穷举密钥搜索量为2^112≈5\*10^35量级；差分分析破译也要超过10^52量级；仍有足够的安全性

1. **计算机如何对人进行认证(用户认证)**A.所知道的信息,如身份证号码、账号密码、口令等.B.所拥有的物品,如IC卡、USBKey等.C.所具有的独一无二的身体特征,如指纹、虹膜、声音等.
2. **Kerbeross**v5的改进：1)加密系统依赖性2)Internet协议依赖性3)消息字节顺序4)门票的生命期5)向前认证6)域间认证7)冗余加密8)PCBC加密9)会话密钥
3. **数字证书&基本功能**数字证书由权威公正第三方机构(**CA中心)签发**,由用户的**身份**与其所持有的**公钥相结合**的计算机文件；以数字证书为核心的加密技术,可对网络上传输的信息加密、解密、数字签名和签名验证**；**确保网上传递信息的**机密性、完整性,及交易实体身份的真实性,签名信息的不可否认性**,而保障网络应用的安全性.
4. **X.509证书包含的信息(1)版本号(2)序列号(3)签名算法标识(4)签发者(5)有效期**.**(6)证书主体(7)证书主体的公钥信息(8)签发者惟一标识(9)证书主体惟一标识(10)扩展(11)签名**
5. **CA的主要职能**①**制定并发布本地CA策略**.但本地策略只是对上级CA策略的补充,而不能违背；②**对下属各成员进行身份认证和鉴别**；③**发布本CA的证书**,或者代替上级CA发布证书；④**产生和管理下属成员的证书；**⑤**证实RA的证书申请**,返回证书制作的确认信息,或返回已制作的证书；⑥**接收和认证对所签发证书的撤销申请**；⑦**产生和发布所签发证书和CRL**；⑧**保存证书、CRL信息、审计信息和所制定的策略**.

主要的PKI信任模型如何**确保银行根证书可信**：信任根的可信性由**物理安全、技术安全与管理安全**共同确保。**1层次模型**：最常见.根CA出all信息,中间CA是下一个,仅信任根的信息.根CA还信任层次结构中其级别的中间CA.允许在分层树all level进行高级别的控制,允许严格控制基于证书的活动.2**交叉模型如左图3信任链模型如右图。**

****

**4混合模型**:混合环境之外的中间CA只信任混合环境中的根CA和中间CA,信任连接到混合环境中任何中间CA所有的根CA。**桥CA模型**:根CA之间有许多P2P关系,可以相互通信、允许交叉证书.允许在组织(或部门)之间建立认证过程.每个中间CA仅信任其上方和下方的CA,但可以扩展CA结构,no创建其他CA层.组织之间的额外灵活性和互操作性好**.**

**操作系统安全机制**硬件机制(内存保护|运行域保护|I/O保护)/软件(标识与鉴别(认证)机制|访问控制|审计机制)机制

1. **访问控制**是实施授权的基础,它控制资源只能按照所授予的权限被访问
2. **自主(基于主人的)访问控制策略**是基于主体的**身份和先行规定的访问规则**来对访问进行控制.灵活性高**自主访问控制的授权管理**集中式管理; 分级式管理; 所属权管理; 协作式管理; 分散式管理**控制实现技术**保护位/能力表/访问控制表/授权关系表机制**缺点**信息移动时访问权限关系改变,引起隐患.不利于实现统一的全局访问控制.DAC有用户滥用职权的问题**按访问许可机制不同**分为自由型、等级型(最广泛)和宿主型
3. **MAC强制(基于系统权威,如安全管理员,制定的访问规则/基于安全性标识的)访问控制集中控制..**用户和客体资源都**被赋安全级别**,用户不能改变自身/客体的安全级别；用户(或其他主体)与资源(或其他客体)都**被标记了固定的安全属性**(如安全级、访问权限等),在每次访问发生时,**系统检测安全属性**以便确定一个用户是否有权访问；当且仅当**用户许可证级别大于或等于数据的密级**时,该用户才能对该数据进行**读**操作,当且仅当小于或等于,该用户才能**写(阻止高级更新低级,敏感数据泄露)**;访问控制完全**根据主体和客体的安全级别决定**,只有安全管理员才能改变主体和客体的安全级.**多级访问控制**,向上/下读/写→信息单向流通**缺点**完整性不够;应用窄不适合复杂现实
4. **RBAC(以角色为中心的访问控制)**模型**基本思想**对系统操作的各种权限**不是直接授予具体的用户**,而是**在用户集合与权限集合之间建立一个角色集合**,**每一种角色对应一组相应的权限。关键概念**主体|客体|用户|权限|用户角色分配|角色权限分配|会话|活跃角色集|保护域**核心思想**将权限与角色联系通过角色沟通主体和客体**好处**简化权限管理|灵活表达和实现组织的安全策略|安全性高|(有效实现最小权限管理)|实用性强**备注**属于策略中立型存取控制模型,既可实现自主存取控制策略,又可实现强制存取控制策略
5. **ABAC(基于属性的访问控制) 将主体和客体属性作为决策基本依据**,有效解决了具有**大规模、强动态性和强隐私性**特点的新型计算环境下**细粒度**访问控制. S/O/P/E:主体/客体/权限/环境属性.**阶段**：准备和执行阶段**ABE基于属性的加密机制**：非对称密码机制；属性为加解密关键要素同密文和用户密钥相结合
6. **授权：**给已通过认证的用户授予相应的权限,授权在用户中的应用程序级别强制执行策略。**授权策略基本内容：**委托/SOA信任源/角色指派/动作/用户/目标访问/角色集成 策略。**特权**在内核中强制执行安全策略。
7. **PMI和PKI**PMI即权限/授权管理基础设施,是属性证书、属性权威、属性证书库等部件的集合体,用来实现权限和证书的产生、管理、存储、分发和撤销等；**PMI以资源管理为核心,对资源的访问控制权交由授权机构统一处**理,即由资源的所有者来进行访问控制.公钥基础设施**PKI是以公开密钥技术为基础,以数据的机密性、完整性和无可抵赖性为安全目的而构建的认证、授权、加密**等硬件、软件的综合设施；PKI证明用户是谁,而PMI证明这个**用户**有什么权限,能干什么,而且PMI需要PKI为其提供身份认证.类似**签证和护照**
8. **访问者为主体,实体统一指代客体和主体**
9. **PMI**含实体:对象/权限声称者/权限验证者
10. **AA属性权威**AC签发/受理/管理/数据库服务器(非必须)/目录服务器**AC属性证书**将1标识和1角色/权限/属性绑定**公钥证书**将一个身份标识和公钥绑定。和公钥证书一样**属性证书**能被分发和存储或缓存在非安全的分布式环境中,不可伪造,防篡改。
11. 信息加密密文通过公开信道传输,没隐藏秘密信息存在的事实.信息隐藏把秘密信息隐藏于可以公开的信息中,掩盖通信过程中存在秘密信息的事实.主要目的不是限制信息的访问,而是确保宿主信息中隐藏秘密信息不被改变或消除,而在必要时提供有效的证明信息
12. **数字水印** 将标记嵌入媒体.向数字产品中嵌入版权拥有者的一些信息.**鲁棒性水印**用于版权标识**脆弱性水印**能察觉载体信息变化,根据破坏情况记录产品受到的攻击。**信息隐藏分类**按载体类型/密钥/嵌入域/检测是否需要原始载体信息参与/保护对象/
13. **数字隐写:**将隐秘信息嵌入掩护载体中,嵌入密钥,将形成的含密载体放入公开信道再用密钥作提取处理,从而得到私密信息。**要求：透明性/不可感知性**指载体在隐藏信息前后没明显差别,除使用特殊手段,否则(主要指人的感官)无法感知机密信息存在.个别场合也需要可见水印.**鲁棒性**抗拒常规信号处理带来的隐藏信息丢失**安全性**抗恶意攻击能力**不可(通过技术)检测性;自恢复性;嵌入强度**
14. **LSB空域/像素域算法将隐秘信息嵌入到随机选择的取样点的值的最低几位上的最低有效位.**相当于叠加一个能量微弱的信号,因而在视觉和听觉上很难察觉.算法对信道干扰及数据操作的鲁棒性差**DCT变换域算法** (比空域鲁棒性更强) 先计算原始图像的离散余弦变换(DCT),然后将隐秘信息**叠加到变换域的系数上**(不含直流分量),这些系数通常为图像的低频分量**NEC算法**有鲁棒性、安全性、透明性
15. **数字指纹**在产品中嵌入用户有关信息.跟踪非法用户.分发和跟踪体制.算法和协议.**要求:保真性/鲁棒性/嵌入量/合谋容忍性/效率.**

**合谋安全、合谋容忍编码(含编码+跟踪方案)确定性|概率性(now)跟踪；连续/离散指纹；随机指纹**

1. 结合鲁棒性水印+脆弱性水印+数字指纹技术所形成的**综合版权管理系统**可以对数字化产品同时实现版权认证、完整性认证和非法复制跟踪的保护功能.
2. **最小特权原则在完成某操作时系统只授予每个主体(用户或进程)必不可少的特权,用户所得到的特权仅能完成当前任务.**它**限定每个主体所必需的最小特权**,确保可能的事故、错误、网络部件的篡改等原因造成的**损失最小；**给予主体“必不可少”的特权,这就保证了所有的主体都能在所赋予的特权之下**完成所需要完成的任务**或操作**；**它只给予主体“必不可少”的特权,这就**限制了每个主体所能进行的操作.**
3. **LKM机制：可加载内核模块**, 有利于Linux的并发开发模式。但由于加载以后的LKM不受控制地使用内核的所有功能和内存,所以**很容易引起恶意程序作为模块加入内核空间后破坏系统**.
4. **CSA云安全模型中,云存储安全机制**

(1)**云存储平台安全机制保护整个云存储平台系统自身的安全**,有两个技术:一个是**密码技术**,保证完整性,提供基于PKI的强身份鉴别以及存储节点的透明加密.另一个是**加固技术**,**主动防御技术；操作系统内核加固；主机虚拟化技术。**(2)**云存储管控安全机制主要解决安全管理的问题**,有对云节点服务器密钥的统一管理、密钥生命周期的可控性、云数据接口／云客户端密钥的自主性等.从管理安全的角度来说,云存储的管理需要满足“相互约束、相互独立”的三员管理.(3)**云存储应用安全机制主要从以下几方面来实现**:存储加密、备份加密、交换加密、身份认证与访问控制、接口安全、手机安全以及云端数据库.

1. **TCB可信计算基**在TCSEC中的定义:**一个计算机系统中的保护机制的全体。**一个TCB由在一个产品或系统上共同实施一个统一的安全策略的一个或多个组件构成。**功能**提供敏感性数据的保密性和完整性。**构成**(1)**固件和硬件**:CPU、内存、寄存器和I/O设备等,为保证系统的安全性,这些部分必须可信地完成它们的设计任务.(2)**与安全策略相关的文件**:如安全策略库,标识与鉴别的数据库.(3)**负责安全管理的人员**:他们一般具有较大权限,很容易引起系统的安全问题.(4)**安全核**:实现引用监视器思想的硬件、固件和软件(5)**具有特权的进程或命令**.**数据库安全技术安全性:**机密性、完整性、可用性。**需求：**防止不适当访问,分级保护,防止推断性攻击,数据库的完整性+操作完整性+语义完整性+审计功能**方法：**)用户身份认证2)存取控制3)数据加密4)审计追踪与攻击检测**外包数据库安全机制**1数据库加密技术2密文数据查询策略3数据库隐私保护4数据完整性验证5外包数据库版权保护**云数据库／云存储安全风险/问题**身份认证和访问控制问题,数据存储和传输的保密性问题,数据隔离问题。应用安全问题。**机制**(1)云存储平台安全(2)云存储管控安全(3)云存储应用安全机制
2. **可信计算**宗旨是以可信计算安全芯片为核心改进现有平台体系结构,增强通用计算平台和网络的可信性.**基本思想**A.首先在计算机系统中**建立一个信任根**,信任根的可信性由物理安全、技术安全与管理安全共同确保B再**建立一条信任链,**从信任根开始到硬件平台,到操作系统,到应用.一级测量认证一级,一级信任一级,**把这种信任扩展到整个计算机系统,从而确保整个计算机系统的可信.信任是一种二元关系**,它可以是一对一、一对多(个体对群体)、多对一(群体对个体)或多对多(群体对群体)的.
3. **网络与系统攻击技术网络与系统调查**攻击者对网络信息和弱点的搜索与判断;**口令攻击**指攻击者试图获得其他人的口令而采取的攻击；**拒绝服务攻击DoS**指攻击者通过发送大量的服务或操作请求使服务程序出现难以正常运行的情况；破坏了**可用性、可靠性**；**缓冲区溢出攻击**属于针对主机的攻击,破坏了**可用性、机密性、完整性、可靠性、可控性等**
4. **网络攻击的一般流程系统调查:**通过网络收集目标主机相关信息的过程；**系统安全缺陷探测**:寻找攻击目标系统内部的安全漏洞**；步骤(1)和(2)也称为网络探测/侦查**；**实施攻击:**当获取到足够的信息后,攻击者就可以结合自身的水平及经验总结制定出相应的攻击方法,实施真正的网络攻击；**巩固攻击成果:**重点是长期隐蔽潜伏,并完成攻击任务；**痕迹清理:**消除攻击过程的痕迹**网络探测**分为踩点、扫描和查点**网络扫描**主动/被动式扫描基于网络/主机,TCP连接/TCP SYN/TCP FIN/TCP ACK/TCP Null/TCP RPC/UDP/ICMP扫描
5. **缓冲区溢出攻击**基本原理是攻击者利用了系统堆栈结构,通过向目标程序的缓冲区写超出其长度的内容,造成缓冲区的溢出,从而破坏程序的堆栈, 使程序的返回地址发生变化,程序执行其他指令,达到攻击的目的;原因:**程序没有仔细检查用户输入的参数.防范缓冲区溢出攻击通过操作系统控制使接收转入数据的缓冲区不可执行；要求程序员编写正确的代码；利用C编译器的边界检查(代价较大)**
6. 常见的拒绝服务攻击方法**SYN泛洪(目前流行):**利用TCP缺陷,发送大量伪造的TCP连接请求,TCP连接无法完成第三步握手,使被攻击主机的资源耗尽(CPU满负荷或内存不足)而停止服务。**；UDP泛洪:**利用简单的TCP/IP服务,如字符发生器协议(chargen)和Echo,来传送占满带宽的垃圾数据,通过伪造与某一主机的Chargen服务之间的一次UDP连接,回复地址指向开着Echo服务的一台主机。这样就在两台主机之间存在很多的无用数据流,这些无用数据流会导致针对带宽服务的攻击。**；Ping泛洪**早期路由器对包的最大尺寸都有限制,许多操作系统对TCP/IP堆栈的实现在ICMP包上都是规定64kB,并且在对包的标题头进行读取之后,要根据该标题头里包含的信息来为有效载荷生成缓冲区。当产生畸形时,声称自己的尺寸超过ICMP上限的包,也就是加载的尺寸超过64kB上限时,就会出现内存分配错误,导致TCP/IP堆栈崩溃,致使接收方主机宕机**；泪滴攻击**利用在TCP/IP堆栈中,实现信任IP碎片中的包的标题头所包含的信息来实现自己的攻击。IP分段含有指明该分段所包含的是原包的哪一段的信息,某些TCP/IP(包括ServicePack4以前的WinNT)在收到含有重叠偏移的伪造分段时将崩溃。**；Land攻击**原理是设计一个特殊的SYN包,它的源地址和目标地址都被设置成某一个服务器地址。此举将导致接收服务器向它自己的地址发送SYN-ACK消息,结果这个地址又发回ACK消息并创建一个空连接。被攻击的服务器每接收一个这样的连接都将保留,直到超时。不同的操作系统对Land攻击的反应不同,大多数UNIX系统将崩溃,Win NT系统则变得极其缓慢(大约持续5分钟)；**Smurf攻击(反弹攻击)**通过向一个局域网的广播地址发出ICMP回应请求,并将请求的返回地址设为被攻击的目标主机,导致目标主机被大量的应答包淹没,最终导致目标主机崩溃。攻击者不直接向目标主机发送任何数据包,而是引导大量的数据包发往目的主机
7. 分布式拒绝服务攻击(DDoS)借助于客户／服务器技术,将多台主机(包括傀儡主机)联合起来作为攻击平台,对一个或多个目标发动DoS攻击,从而成倍地提高拒绝服务攻击的威力。**防范：**①关闭不必要的服务。②限制同时打开的SYN半连接数目。③缩短SYN半连接的超时等待(timeout)时间。④除此之外,及时更新系统补丁也非常重要。
8. **僵尸网络攻击阶段？各阶段的任务？**

**(1)感染目标主机,构建僵尸网络**逐渐以更为隐蔽的网页或邮件木马为主要传播方式**(2)发布命令,**控制僵尸程序**(3)展开攻击。**分为**本地攻击和远程攻击。本地攻击**指发起对僵尸网络内部被控主机的攻击,**远程攻击**指攻击非僵尸网络内部的主机,分为两类：一类是**扩展僵尸网络规模**,这类攻击目的是让外部主机感染同样的僵尸程序,最终成为僵尸网络的一部分。另一类攻击是**打击、渗透方式**,比如分布式拒绝服务、垃圾邮件等。**(4)攻击善后。**主要目的是隐藏攻击痕迹,防止被追踪溯源

防火墙**特性/目标**：(1)针对所有的通信2)被授权的通信才能通过3)本身对渗透攻击免疫

**采用技术(1)服务控制**决定哪些Internet服务可以被访问**(2)方向控制**决定在哪些特定的方向上服务请求可以被发起并通过防火墙。**(3)用户控制**根据用户正在试图访问的服务器,来控制其访问。**(4)行为控制**控制一个具体的服务怎样被实现。**典型功能**访问控制功能；内容控制功能；日志功能；集中管理功能；自身安全和可用性；可能还具有流量控制、网络地址转换(NAT)、虚拟专用网(VPN)等功能。**防火墙局限性**不能防御(1)不经由防火墙的攻击。(2)来自内部的威胁。(3)病毒感染的程序和文件进出内部网。(4)数据驱动式的攻击。**分类(1)从工作原理：**网络层防火墙技术和应用层防火墙**(2)防火墙的硬件环境：**基于路由器的防火墙和基于主机系统的防火墙**(3)防火墙的功能**FTP防火墙、Telnet防火墙、E-mail防火墙、病毒防火墙、个人防火墙**通常也将几种防火墙技术结合**

1. 包过滤防火墙工作原理基本原则**“最小特权原则”,**即明确允许管理员希望通过的那些数据包,禁止其他的数据包。**具体实现**建立安全策略,将其转化包过滤规则表,由规则表和数据头内容的匹配情况来执行过滤操作.默认值：丢弃/转发.**工作在网络层；**将IP数据报的各种包头信息与防火墙内的规则进行比较,然后根据过滤规则有选择地阻止或允许数据包通过防火墙。常用的包头信息包括**源地址、目的地址、源端口、目的端口、协议类型。优点**安全性好一个过滤器能协助保护整个网络；对用户透明；速度快效率高；通用、廉价、有效**缺点**安全性较差；日志功能十分有限；无法执行某些安全策略；容易受到利用TCP/IP规定和协议栈漏洞的攻击；做出安全控制决定时,起作用的只是少数几个因素

代理服务技术代理服务器防火墙又称应用层网关、应用层防火墙,完全阻隔了网络通信流**实现：**应用代理服务器；回路级代理服务器；智能代理服务器；邮件转发服务器**优点**安全性好；能过滤数据内容；方便地与其他安全技术合成**缺点**速度较慢；对用户不透明

**选用**考虑用户的安全策略中的特殊需求如(1) IP地址转换(2)双重DNS(3)VPN(4)病毒扫描功能(5)特殊控制需求**发展**1)智能化2)高速度3)分布式并行结构4)多功能5)专业化

1. NSTAC定义**入侵检测**是监测计算机网络和系统、发现违反安全策略事件的过程。**入侵检测过程**信息收集、信息(数据)预处理、数据的检测分析、根据安全策略做出响应**入侵检测系统**是完成入侵检测功能的软件、硬件的组合。IETF定义**通用入侵检测模型(1)事件生成器：**是采集和过滤事件数据的程序或模块。负责收集原始数据,对数据流、日志文件等进行追踪,然后将搜集到的原始数据转换成事件,并向系统的其他部分提供此事件**(2)事件分析器：**事件分析器是分析事件数据和任何CIDF组件传送给它的各种数据。**(3)事件数据库：**负责存放各种原始数据或已加工过的数据。**(4)响应单元：**是针对分析组件所产生的分析结果,根据响应策略采取相应的行为,发出命令响应攻击。**(5)目录服务器**：目录服务器用于各组件定位其他组件,以及控制其他组件传递的数据并认证其他组件的使用,以防止入侵检测系统本身受到攻击。
2. **IDS入侵检测系统分类:基于检测对象的分类:基于主机HIDS**对象是主机系统和本地用户；**基于网络NIDS**监听网络中的分组数据包；**混合式IDS**综合了网络和主机两种结构特点。**基于检测技术的分类1)异常检测:基于行为的检测2)误用检测(特征检测)**。**基于工作方式的分类1)离线检测系统**非实时工作,在事后分析审计事件**2)在线检测系实时联机**1)&2)都是一旦发现入侵迹象,立即断开入侵者与主机的连接,并搜集证据和实施数据恢复}**分布式入侵检测DIDS**各个模块分布在网络中不同的计算机设备上,分布性主要体现:数据收集模块上,细分:层次式~和协作式DIDS
3. **异常检测入**侵和滥用行为通常和正常的行为有严重差异,查出这些差异就可检测出入侵. **局限**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**误用检测**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.**局限**只能发现已知的攻击,对未知的攻击无能为力
4. **入侵检测的研究重点**:分布式入侵检测&智能入侵检测&高效的模式匹配算法&基于协议分析的入侵检测&与操作系统的结合&入侵检测系统之间以及入侵检测系统和其他安全组件之间的互动性研究&入侵检测系统自身安全性的研究&入侵检测的标准化**Snort的组成**解码器；预处理器；检测引擎；输出插件；日志/警报子系统系统
5. **蜜罐(诱捕网络)对攻击方进行欺骗**.布置作为诱饵的主机、网络服务或者信息(蜜罐),诱使攻击方攻击,从而**对攻击行为捕获和分析**,了解其工具与方法,推测意图和动机,让防御方清楚安全威胁,通过技术和管理增强系统安全防护能力**分类**按系统功能/系统交互活动级别/服务实现方式/服务提供方式分类**关键机制**欺骗环境构建/威胁数据捕获/威胁数据分析机制**辅助机制**安全风险控制机制,配置与管理机制,反蜜罐技术对抗机制**部署结构**蜜网/蜜场
6. **CSIRT应急响应**对国内外发生有关计算机安全的事件实时响应与分析,提出解决方案/应急对策,**功能:**保证计算机信息系统和网络免遭破坏.**策略**全局策略,服务特定策略,基础策略**阶段**准备/检测/抑制/根除/恢复/报告和追踪**技术和工具？**
7. **审计**记录和分析用户使用信息系统过程中的相关事件。**安全审计对系统安全的审核、稽查与计算,监控**来自信息系统内部和外部的用户活动,对与安全有关的活动的相关信息进行**识别、记录、存储和分析**,对突发事件进行**报警和响应**,还能通过对系统事件的**记录**,为事后处理提供**重要依据**,为网络犯罪行为及泄密行为提供**取证基础**.同时,通过对安全事件的**不断积累并且加以分析**,能有选择性和针对性地对其中的对象进行**审计跟踪,即事后分析及追查取证,**以保证系统的安全**过程** 1)安全审计自动响应2)安全审计数据生成3)安全审计分析4)安全审计浏览5)安全审计事件存储6)安全审计事件选择**审计系统的结构**1. 集中式结构2分布式结构(优点：扩展/容错/能力+兼容/适应性强)**审计数据来源**①基于主机的数据源1)首选操作系统日志2)系统日志3)应用日志4)基于目标的信息②基于网络的数据源(通过正常/混杂模式获取)③其他途径数据源：带外数据源,通过人为、非系统方式
8. **数字取证主要步骤1收集2检查3分析4报告(**不同的解释不同的听众**)作用:获得证据打击违法**(1)发现和归档证据和线索.(2)固定其他途径发现的证据.(3)帮助揭示事件模型.(4)关联攻击和受害的计算机.(5)展现端到端侵害事件的路径,不管是否已遂.(6)提取隐藏、删除或者其他不能直接得到的数据.(7)排除故障:(8)日志监控:(9)数据恢复:(10)数据提取:(11)完善策略**分类：**主机取证和网络取证,事后取证和实时取证,司法取证和非司法取证**数据媒介：**标准的计算机系统,网络设备,外部设备,存储设备,消费电子产品**遵循原则：**及时性/取证过程合法性/多备份/环境安全/严格管理过程原则**证据信息类别和取证技术分类：**来自文件的,来自操作系统的,来自网络的,来自应用软件的。**电子证据根本属性**可接受性和完整性**特点**(1)数字性(2)技术性(3)脆弱性(4)多态性(5)人机交互性(6)复合性**安全攻击被动(**(1)信息收集(2) 流量分析**)主动(**(1)伪装(2)重放(3)消息修改(4)拒绝服务**)安全服务**加强数据处理系统和信息传输的安全性的一种处理过程或通信服务.其目的在于利用一种或多种安全机制进行反攻击. **数据保密性(**连接/无连接/选择字段/信息流~**)完整性(**带|不带恢复/的连接/选择字段/无连接/选择字段无连接~**)服务。安全机制**加密/数字签名/访问控制/数据完整性/鉴别交换/鉴别交换/通信业务填充/路由选择/公证机制.**IPSec的两种工作模式1)传输模式**主要为直接运行在IP层之上的协议,如TCP、UDP和ICMP,提供安全保护,一般用于在两台主机之间的端到端通信.**2)隧道模式**对整个IP包提供保护.为达到这个目的,当IP数据包附加了AH或ESP域之后,整个数据包加安全域被当做一个新IP包的载荷,并拥有一个新的外部IP头.一般用于两个网络之间的通信.**ESP协议和AH协议的不同IP认证头(AH)协议**为IP数据包提供数据完整性校验和身份认证,还有可选择的抗重放攻击保护,但不提供数据加密服务。**封装安全载荷(ESP)协议**为IP数据包提供数据完整性校验、身份认证和数据加密,还有可选择的抗重放攻击保护.
9. **SSL记录协议**发送时,SSL记录协议接收上层应用消息、将数据分段为可管理的块、可选择地压缩数据、应用MAC、加密、添加一个头部,并将结果传送给TCP.接收到的数据则被解密验证、解压缩、重组后交付给高层
10. **SSL握手协议**握手指客户端与服务器端间建立安全连接的过程.握手协议在传递应用数据之前使用.握手协议由客户端和服务器间交换的一系列消息组成,每个消息由三个域组成.
11. **WEP共享密钥认证的主要步骤**认证请求、挑战文本、加密的挑战文本、接入成功/失败
12. **802.11i定义的安全服务A.认证:**定义用户和网络的交互,以提供相互认证,并生成用于STA和AP之间无线通信的短期密钥.**B.访问控制:**对认证功能的增强,能与多种认证协议协同工作.**C.带消息完整性的机密性:**MAC层数据与消息完整性校验码一起加密以提供机密性和完整性.
13. **802.11i的认证过程的阶段？(1)发现阶段**.**(2)认证阶段: (3)密钥管理阶段 (4)安全通信阶段: (5)连接终止阶段**
14. **GSM安全功能**①用户身份认证②用户身份保密③用户数据保密以及信令数据保密
15. **3GPP安全总体结构**在应用层、归属/服务层和传输层,分别保障了：(1)网络接入安全(2)网络域安全(3)用户域安全(4)应用域安全(5)安全特性的可视性及可配置能力
16. **5G安全架构与4G安全架构的不同**一是加强了**网络接入安全**,增加了非3GPP接入,同时增强了AKA协议,堵上了拜访域欺骗归属域的漏洞；二是**面向垂直行业需求**,新增了二次认证,在满足垂直行业差异化需求的同时增强了安全性；**三是新增了SBA域的安全,**考虑了服务化网元的安全交互；**四是应用域安全**,新增了空口可选的完整性保护手段.
17. **恶意活动代码**最初指最传统意义上的病毒和蠕虫.目前木马、后门、恶意脚本、广告软件、间谍软件等都是**独立的恶意代码**独立传播和运行,是一个完整的程序,它不需要寄宿在另一个程序中.**非独立的恶意代码**只是一段代码,必须寄生在某个程序(或文档)中,作为该程序的一部分进行传播和运行**分类：**(1) 后门(2) 逻辑炸弹(3) 间谍软件(4) 特洛伊木马(5) 病毒(6) 蠕虫(7) 僵尸(8) P2P系统(9) RootKit病毒分类引导型,文件型,混合型,变形, 脚本,宏~**特性：**(1) 感染性(2) 非授权性(3) 潜伏性(4) 可触发性(5) 破坏性
18. 病毒和蠕虫的区别计算机病毒与蠕虫的一个重要区别是,病毒需要借助活动的宿主程序或已被感染的活动操作系统才能运行、造成破坏并感染其他可执行文件或文档；而蠕虫是独立的恶意程序,可以通过计算机网络进行自我复制和传播,不需要人工干预。
19. **广义病毒**网络蠕虫是一种**自治的、智能的恶意代码**(广义上的病毒).**传统意义上的病毒是狭义病毒**,指**既具有自我复制能力,又必须寄生在其他程序(或文件)中**的恶意代码.
20. **计算机病毒4模块引导模块**:毒的入口模块,它最先获得系统的控制权.**感染模块:**完成病毒感染功能,是病毒最核心、最关键的代码**触发模块**:对预先设定的条件进行判断,如果满足则返回真值,否则假值.**破坏模块**:完成具体破坏,其破坏形式和表象由编写者目的决定.
21. **蠕虫模块侦察模块:**确定哪些系统可以成为其攻击目标；判断目标是否能被攻击；搜集机器的重要配置情况**攻击模块:**可在非授权情形下侵入系统、获取系统信息**通信模块:**用于实现与蠕虫制作者及其它蠕虫之间的信息交互.**(可有)命令接口模块**:可以采用手工方式控制传播出去的某些蠕虫,进而可以控制受害主机,类似于木马功能.**(可有)数据库支持模块**:.蠕虫将自身的一些信息存入数据库中,以方便攻击者进行管理系统漏洞. **传播** 电子邮件系统. 局域网. 即时工具.多种方式
22. **内容安全需求**1.数字版权侵权及其控制2.不良内容传播~3.敏感内容泄露~ 4.内容伪造~
23. **不良文本过滤**的方法及工作原理：**关键字的过滤方法**：编制一个不良文本关键字词库中出现的字词是敏感词汇代表不良文本。文本到来对文本进行检索,简单的布尔逻辑运算匹配超过一定阈值认为不良文本过滤。**分级标签过滤方法：**不同的网页根据内容赋予不同的级别来过滤。地址库过滤方法：**IP过滤**指封锁指定网站的IP地址；URL过滤定位不良文本在互联网上的位置,对该网页进行屏蔽；**内容的动态过滤法**：文本的表示形式具体化~过滤算法对指定的文本划分类别属性~将对不良文本进行过滤。**话题发现步骤**：报道.事件.活动.话题**多媒体内容安全问题**:鉴别创建者.确定版权声明.公证作品签名与版权声明.控制访问作品权限
24. **主机系统安全：如何添加用户？**