计算机安全:保护信息免受未授权的访问\中断\修改,为系统预期用户保持可用性**网络安全:**采用各种技术和管理措施,使网络正常运行,确保经过网络传输和交换的数据不会增加\修改\丢失\泄露**信息安全:**为防止意外事故和恶意攻击而对信息基础设施\应用服务和信息内容的保密性\完整性\可用性\可控性\不可否认性进行的安全保护**黑客:**试图突破信息系统安全\侵入信息系统的非授权用户**恶意软件:**在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上安装运行,侵犯用户合法权益**威胁:**破坏安全的潜在可能**被动攻击:**利用系统的信息但不影响系统资源,对传输进行窃听和监测(预防而不是检测,加密解决,搭线监听\无线截获\病毒截获\流量分析)**主动攻击:**改变系统资源或影响系统运作,对数据流进行修改或伪造数据流(伪装\重放\消息篡改\拒绝服务)**5 性:**保密用加密,完整用 hash,可控用身份认证,不可否认用数字签名**安全:**攻击成本大于攻击收益**资产:**物理\知识\时间\名誉**评估:**漏洞\威胁\风险(规避\最小化\承担\转移)**柯克霍夫:**密码系统安全是基于密钥的而不是算法的保密**对称:**分组\序列(周期长,接近随机数流,输出取决于输入)**密码分析:**唯密文\已知明文\选择明文\选择密文**代换:**替换字母(频率分析攻击)**置换:**改变顺序**凯撒:**简单相加取模**维吉尼亚:**分组凯撒**one-time pad:**一次一密最安全 **DES:**56 位有效密钥,S 盒 b1b6 做行,其余做列,EDE 三重 DES**AES:**MC 变换左乘(02 03 01 01,01 02 03 01,01 01 02 03,03 01 01 02),加法用异或,对 0x1b 取余,SB 高四位行,第四位列**对称工作模式:**分组链接,随机计数器**对称问题:**密钥管理,通信要求,密钥泄露,数据完整性和不可否认性不能保证**公钥特点:**加解密分开\多人加密一人解读\一人签名多人验证\无需事先分配密钥\密钥持有量少\提供安全伪随机数和零知识证明**要求:**密钥易产生\加解密容易\密文和公钥不能恢复明文或私钥\加解密次序可换 **proof of zero knowledge:**不泄露消息的情况下证明我知道消息 **one-way function:**易计算难求逆 **trapdoor:**具有限门知识能求逆 **RSA:**大整数分解困难,n=pq,gcd(e,pn)=1,de=1 % pn,d 私 e 公,c=m^e % n(速度慢,中间人攻击)**ELGamal:**签名(r,s),k 和 p-1 互质,r=g^k % p,s=k^-1(m-x*r) % p-1,验证 y^r*r^s=g^m % p(基于 Discrete Logarithm Problem)**Diffie-Hellman Problem:**给 g^x % p,g^y % p,求 g^xy % p(前提是解决 DLP)**Elliptic Curve Cryptography:**椭圆曲线,可以用少得多的密钥大小取得和 RSA 相等的安全性,加解密速度快**公钥与对称:**双方互信\双方不互信,两两分享密钥\每人公私钥,暴力破解\解决数学难题,速度快\速度慢,DES 和 AES\RSA 和 ELGamal 和 ECC **哈希:**定长输出,易于求解不能求逆,给定 m1 找不到 h(m1)=h(m2),找不到任意 h(m1)=h(m2)**以上三条:**单向性\弱无碰撞\强无碰撞**性质:**算法公开\改变消息一位引起多位改变\1 和 0 个数相近 **MD5:**迭代 hash,上轮输出是本轮输入,用 10...0 和 64 位消息长度填充为 512 的倍数,4 轮 64 步迭代(基本逻辑函数,异或 Ti,循环移位),生日攻击需 2^64 次,输出 128bit**SHA-1:**wi=CLS1(wi-16^wi-14^wi-8^wi-3),kt 加法常量,输出 160bit,生日攻击需 2^80 次,比 MD5 慢**哈希攻击:**预映射(preimage)\次预映射(second primage)\碰撞(collision),分别对应性质二三四 **Pre-Birthday Problem:**多少人与我相同生日概率大于 1/2,1/2 = 1-(364/365)^k,k=253**Birthday Problem:**多少人至少有相同生日概率大于 1/2,1-(365*...*365-k+1)/365,k=23**Y 集合至少有一个与 X 相等的概率:**1-(1-1/n)^k2,由于 1-1/n<e^-1/n,大于 0.5 时 k=sqrt(nln2)**认证:**对称加密 h **认证和机密:**消息和 h 同时加密**认证和签名:**私钥加密 h **摘要不一致:**传输错误\消息被篡改\消息伪造\密码软件不正确使用 **Authentication:**证实某事是否名副其实或是否有效的过程(加密用以确保数据的保密性,阻止对手的被动攻击\认证用以确保报文发送者和接受者的真实性以及保文的完整性,阻止对手的主动攻击,适用于用户\进程\系统\信息,只有符合和不符合)**身份认证:**Prover\Verifier\Trusted third party **身份认证基础:**用户知道\用户拥有\用户特征(密码\身份证\指纹)**身份认证方式:**one-way\two-way\trusted third-party authentication**Challenge-Response:**发送挑战值,返回挑战值和私钥的 hash**Kerberos:**认证服务器\票据授权服务器\Server(一次会话一次密钥)**八种攻击:**泄密\传输分析\伪装\内容修改\顺序修改\计时修改\发送方或接收方否认(12 加密,3456 消息认证,7 数字签名)**消息认证:**验证所受到的消息确定是来自真正的发送方且未被修改过**认证符:**一个用来认证消息的值。由消息的发送方产生认证符,并传递给接收方**认证函数:**产生认证符的函数,认证函数实际上代表了一种产生认证符的方法 **FCS:**错误检测码,校验和**内部错误控制:**先 FCS 再加密(外部是先加密在 FCS)**Message Authenticaion Code:**消息和密钥的公开函数,它产生定长的值,以该值作为认证符\数据附加在消息之后\通信双方共享密钥 K **两个要求:**MAC 可以不可逆\可以多对一(破译难度更大,无法确定密钥是否正确)**穷举 MAC**:k 位密钥,k=x*n,则需 x 次循环才能找到正确的密钥(但可以改变 M 使 MAC 正确:Y=x1^...^xm)**性质:**不能构造明文等于已知 MAC\对于随机两个消息其 MAC 相等概率为 2^-k **基于 DES 的 MAC:**分成 64 位的组(最后一位不足则补 0)**MAC 好处:**保密与真实性不同,信息加密提供保密\加密代价大\分离后功能更灵活\有些消息只要真实而不保密**签名:**可信\不可伪造\不可重用\签名后文件不可变\不可抵赖(私钥加密公钥解密)**要求:**验证作者和时间\验证内容\可以由第三方验证(依赖\唯一\可验\抗伪造\可用)**直接 DS:**方案的有效性取决于发方密钥的安全性**仲裁 DS:**发方签名给仲裁,仲裁对消息和签名验证完后,再连同一个表示已通过验证的指令一起发给接收方(无共享消息\仲裁不泄露则不能重放\消息一直保密)**DSS:**Digital Signature Standard(320bit)**DSA:**r=(g^k % p) % q,s=k^-1(h(M)+xr) % q,x 是私钥,p 是素数(2^L-1<p<2^L,512<L<1024),q 是 p-1 素因子,g=h^p-1 % p 且 h^(p-1)/q % p>1,1<h<p-1 **验证:**w=s^-1 % q,u1=h(M)w % q,u2=rw % q,v=g^u1y^u2 %p %q,v==r?**两种签名:**不可否认\盲(授权才可验证\签名但不知消息)**防止伪造签名:**先签名后加密**攻击签名方式:**唯密钥\已知消息\选择消息**攻击签名目的:**完全破译\有概率产生有效签名(选择性伪造)\至少有一个消息可以有效签名(存在性伪造)**数字证书:**CA 颁布的数据结构,可进行身份验证(时间\A 公钥\A 身份\CA 签名)**过程:**用户确定私钥发送公钥\RA 验证用户身份向 CA 发请求\CA 发包含用户和自己公钥的证(CA 也为自己发证)**条件:**任何人可确定拥有者公钥\任何人可验证 CA 签名\只有 CA 产生证书\任何人可验证证书过期否**证书撤销:**RA 维护 CRL,所有人可下载证书撤销列表**对称密钥管理:**主(真随机,物理噪声源,明文存储)\二级(主密钥加密或随机数)\初级(随机数解密)密钥**对称密钥性质:**随机性\长周期\非线性\统计等概率\不可预测**密钥备份:**异地存储\仔细保护\高级保护低级\不能密文备份,可多个分量备份\方便恢复\记录日志**密钥更新:**主密钥重新安装\二级密钥重新产生\会话密钥一次一密,文件密钥把密文解密再加密**密钥销毁:**保留一段时间\清除所有痕迹,重现不可能 **PKI:**公钥基础设施**五种模型:**严格层次\分布式信任(中心辐射\网状)\Web\用户中心\交叉认证**数字证书分类:**电子邮件\服务器(SSL)\客户端个人证书 **access control:**限制访问主体(或称为发起者,是一个主动的实体,如用户\进程\服务等)对访问客体(需要保护的资源)的访问权限,从而使计算机系统在合法范围内使用,决定用户及代表一定用户利益的程序能做什么,以及做到什么程度**过程:**认证验证身份\Authorization(授权)限制用户对资源的访问级别 **Access:**使信息在主体和客体之间流动的一种交互方式 **Access Permissions:**决定了谁能够访问系统,能访问系统的何种资源,如何使用这些资源**控制策略:**主体对客体的访问规则集,定义了主体对客体的作用行为\客体对主体的约束 **discretionary(自主) AC:**具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体(灵活性高,但访问权限会被改变)**AC matrix**:二维矩阵,行主体列客体,每一格表示访问授权 **AC lists:**能访问某个客体的主体列表和权限 **AC capabilities lists:**某个主体能访问的客体列表和权限 **mandatory(强制) AC:**管理员决定用户等级(TSCRU,递减),低级不能访问高级 **role-based AC:**将访问权限分配给一定的角色,用户通过饰演不同的角色获得角色所拥有的访问权限 **task-based AC:**对象的访问权限随着执行任务的上下文环境发生变化(工作流\授权结构体\受托人集\许可集,适合分布式计算和多点访问控制的信息处理控制和决策制定)**object-based AC:**将访问控制列表与受控对象或受控对象的属性相关联,允许对策略和规则进行重用\继承和派生操作 **MAC 地**

址过滤:过滤物理地址 **VLAN 隔离:**同 VLAN 可通信,跨 VLAN 需三层交换机或路由器 **ACL:**基于包过滤,把源地址\目的地址\端口号作为数据包检查依据(可两台设备间或网段管理)**防火墙访问控制:**划分为内外网,对内外网间通信协议的业务流进行控制**攻击\入侵:**破坏系统\获取信息**五步:**侦察(踩点,网络域名\内部和外部网络\OS 信息)\扫描及漏洞分析(端口\漏洞扫描,全 TCP\SYN\FIN\第三方)\获取访问权限(缓冲区溢出,sql 注入)\保持访问权限(开新号,后门隐蔽和非授权,rootkit 替换文件)\消除痕迹(应用程序\安全性\系统日志)**OS 侦察:**主动(发送数据)\被动(嗅探网络数据)**端口:**FTP(21,文件传输)\telnet(23,远程登陆)\http(80,超文本)\pop3(110,邮件)\smtp(25,简单邮件)\socks(1080,代理)\rpc(111,远程调用)\snmp(161,网络管理)\tftp(69,简单文件)**zero day:**未公开的漏洞(只能扫描公开的漏洞)**denial of service:**拒绝服务(消耗带宽\磁盘空间\CPU 资源\系统缺陷(大于 65535 的包\多段数据))**DDoS:**分布式 DoS **解决:**打补丁\检查子网\删除多余服务\TCP 封装\安全通信协议\firewall 外不共享\firewall 上端口映射\检查日志**恶意代码:**目的恶意\是程序\执行发挥作用**病毒:**感染宿主,auto 复制,人为传播(感染可执行文件\磁盘引导区\文档文件(macro)\脚本,传播移动存储\电邮附件\共享目录)**反病毒:**最小特权和最小化服务数量\杀毒\良好习惯\阻断输出连接 **worm:**网络传播,auto 复制,无须人为传播(探测装置\传播引擎\目标选择\扫描引擎\有效载荷)**恶意代码:**从 server 传播到 client,利用漏洞入侵(浏览器脚本,DoS\browser hijacking\窃取 cookie\跨网站脚本攻击)**后门:**远程访问目标计算机的通路(权限提升\命令远程执行\命令行访问\控制 GUI)**trojan horse:**伪装成正常程序(独立恶意操作\修改应用\完全覆盖应用)**rootkit:**替换系统文件,控制 OS 内核(不直接获取权限,用户\内核模式,是保护权限的措施,检查文件完整性解决)**firewall:**所有 data 过墙\安全才过墙\自身抗攻击(服务\方向\用户\服务控制)**形式分类:**软件\硬件\芯片级**结构分类:**单一主机\路由器集成\分布式**部署分类:**网络\基于主机**实现技术分类:**包过滤\状态\应用网关**包过滤:**基于数据包(性能好\规则简单\不专门配置,管理员要求高\不阻止应用层\只对某些 TCP 攻击敏感\不支持用户连接认证\日志有限)**包过滤依据:**网络层(源和目的 IP\TCP 和 UDP 等协议\IP 优先级域),传输层(TCP 和 UDP 端口号\TCP 控制标记)**状态:**解决包过滤的问题用开端口\检查 TCP 控制位,对数据流建立连接(知道连接状态\不打开大范围端口\日志更丰富\预防 DoS)**应用网关:**根据传输\网络\应用层过滤(连接网关\直通代理,实现用户认证\检测应用层,内存和磁盘消耗大)**体系结构:**双重宿主(内外网之间一台,用户登录\服务代理)\屏蔽主机(包过滤\堡垒主机)\屏蔽子网(DMZ 区(供外网访问的专用区域)\两台包过滤\堡垒)**参数:**吞吐量(不丢包时过墙的数据包)\并发数(最大会话数,需考虑 CPU)\用户数**局限:**不能防内网\限制不能绕过通信\不能防外网病毒\关闭了一些服务\传输延迟\对用户不透明\更新快 **P2DR 模型:**策略=响应+防护+检测**审计:**确定责任\复盘事件\评估损失\检测系统问题区\灾难恢复\阻止不正当使用 **intrusion detection system:**信息收集(大范围收集日志),分析(模式匹配\统计分析\完整性分析),结果处理(主动切断连接\被动报警)**完整性:**防止删除记录\防止修改 IDS\减轻 OS 负担**功能:**识别入侵手段\监控异常通信\鉴别系统漏洞\完善安全管理**分类:**(host(主机)\network-based(嗅探器 sniffer)\distributed)**入侵检测:**滥用 Misuse(基于特征,入侵行为模式匹配)\异常检测 Anomaly Detection(规定正常行为)**Snort:**数据包嗅探器\预处理器\检测引擎和规则集\日志模块(NIDS 滥用检测)**矛盾:**误报\漏报,隐私\安全,被动分析\主动发现,海量信息\分析代价,功能性\可管理性,单一产品\复杂网络(工业优化算法,学术引入 AI)**Intrusion Prevention System:**IDS 的深层分析和防火墙的在线部署结合(嵌入式运行\深入分析\入侵特征库\高效处理,与 firewall 串联,单点故障代价大\性能瓶颈\误报漏报多)**Unified Threat Management:**统一威胁管理(复杂性低\维护量小,性能和检测能力平衡\可用性低\不适合高性能大流量)**IPsec:**Authentication Header(验证报头,数据源认证和完整性保证)\Encapsulating Security Payload(封装有效安全负载,定义加密方法提供可靠性)\Internet Key Exchange(密钥交换标准)**模式:**传输(IP 首部增加 AH\ESP)\隧道(传输基础上再加上新首部)**Virtual Private Network:**穿过公网的安全\稳定隧道,网络封包的加密传输 **SSL:**传输层安全协议,基于传输层可靠流传输协议(TCP),用户合法性认证\加密并隐藏数据\保护数据完整性**过程:**接通,密码交换,产生会话密码,客户检验服务器,服务器认证客户,结束**两层:**记录 Record 协议(机密性\完整性)\握手 Handshake 协议(消息结构:Type1 字节\Length3 字节\Content 大于 0 字节)**Session:**一组 C\S 就是一个会话,可能含有多个 connection **缺点:**客户端假冒\无 UDP\不能抵抗流量分析\主密钥泄露\临时文件脆弱\针对公钥加密标准 PKCS 的选择密文攻击**不规范问题:**攻击证书\中间人攻击\安全盲点\IE 的 SSL 身份鉴别缺陷 **Secure Electronic Transaction:**安全电子交易,公钥加密\数字签名\数字信封\数字证书,应用层提供安全通信管道,购买请求(初始请求,采购订单信息和购买证书\初始回应\购买请求\购买回应)\支付认定\收款(认证安全\完整性\机密性\抗否认\保护隐私)**双重签名:**连接两个不同接收者消息,订单信息 order information 和支付命令 payment instruction**Trusted Computer System Evaluation Criteria:**可信计算机系统评价标准(安全策略 Security Policy\标识 Identification\标记 Marking\可记账性 Accountability\保障机制 Assurance\连续性保护 Continuous Protection)**四类七级:**A1 验证设计\B3 安全域\B2 结构化保护\B1 标记安全保护\C2 受控的存取保护\C1 自主安全保护\D 最小保护 **Common Criteria for Information Technology Security Evaluation:**通用评估准则(消费者\开发者\评估者,简介和一般模型\安全功能和保障要求,结构开放\表达通用\内在完备性\实用性)**EAL:**评估保证级别(CC 中有 7 个 EAL,功能测试\结构测试\方法测试校验\系统设计测试评审\半形式化设计测试\半形式化和形式化验证设计测试)**信息隐藏:**利用载体信息冗余性,将秘密信息隐藏于普通信息中,对非授权者不可见,实现信息的保密传播 **Digital Watermarking:**解决数字作品侵权行为(数字作品具有易修改\易复制\无失真传播特点),将一些标识信息嵌入数字载体当中,用于传送隐秘信息或验证是否被修改,不影响原载体使用价值,不易探知和修改**特点:**安全\隐蔽\鲁棒(经历多种信号处理后保持完整性)\容量大**方法:**时空间域(难以抵抗噪声\压缩\剪切)\变换域(离散余弦转换\小波)**隐写:**将秘密信息隐藏到看上去普通的信息(如数字图像)中进行传送**联系:**都是把文件隐藏到另一个文件中**区别:**隐写侧重隐藏,水印侧重保护著作权\隐写识破后秘密文件易泄露,水印更在乎鲁棒**方法:**替换系统\变换域\扩展频谱\统计方法\失真技术 **PGP:**基于 RSA 邮件加密软件**功能:**邮件加密\身份认证\私钥加密\硬盘密码保护\共享资料加密\PGP 自解压文档创建\资料安全擦除 **Computer Information System:**由计算机及配套设备构成,按照一定的应用目标和规则对信息进行采集\加工\存储\传输\检索等的人机系统 **Trusted Computing Base of Computer Information System:**计算机系统内保护装置的总体,硬件\固件\软件\执行安全策略组合体,建立基本的保护并提供可信计算系统所要求的附加用户服务 **Object:**信息的载体 **Subject:**引起信息在客体之间流动的人\进程\设备 **Sensitivity Label:**表示客体安全级别并描述客体数据敏感性的一组信息 **Security Policy:**管理\保护\发布敏感信息的规定 **Channel:**系统内的信息传输路径 **Covert(隐蔽) Channel:**允许进程以危害系统安全策略的方式传输信息的通信信道 **Reference Monitor:**监控主客体之间授权访问关系的部件 **Trusted Channel:**为执行关键的安全操作,在主体\客体\可信 IT 产品之间建立和维护的保护通信数据免遭修改和泄露的通信路径**客体重用:**在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始制定\分配或再分配一个主体之前,撤销该客体所含信息的所有授权(当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息)**第一级:**自主 AC\身份鉴别\数据完整**第二级:**客体重用\审计**第三级:**强制 AC\标记**第四级:**隐蔽信道分析\可信路径**第五级:**可信恢复名称:用户自主\系统审计\安全标记(增加了强制 AC,三级以上强制 AC 为主)\结构化\访问验证(接近 TCSEC 中的 A1)