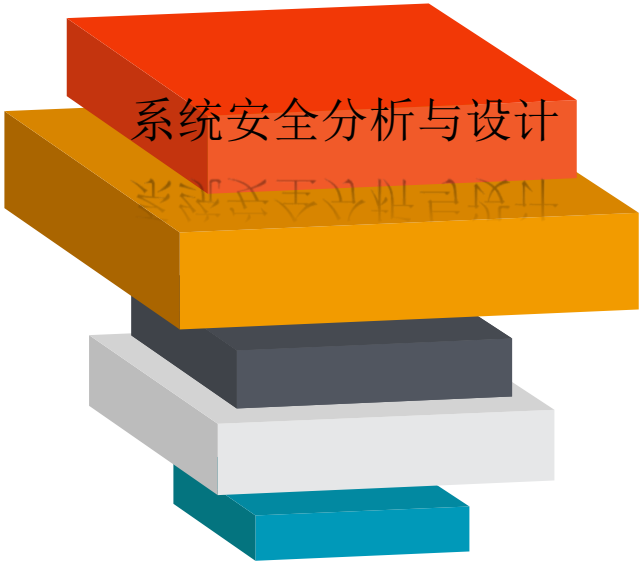
系统架构设计师

DESIGNER:王川林

系统安全分析与设计



安全基础技术

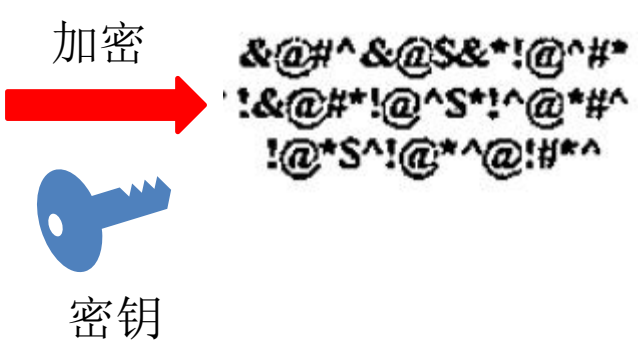
网络安全

计算机病毒与木马 ★

对称非对称加密 ★★★★
数字签名 ★★★★
信息摘要 ★★★★

安全协议 ★★★★
防火墙 ★★★
入侵检测 ★★★

软考教育：帮助客户成功，创造社会价值



软考教育：帮助客户成功，创造社会价值

缺陷： 1.加密强度不高，但效率高。
2.密钥分发困难

常见对称密钥加密算法：

DES：替换+位移、56位密钥、64位数据块、速度快、密钥易产生

3DES（三重DES）：两个56位的密钥K1、K2

加密：K1加密→K2解密→K1加密

解密：K1解密→K2加密→K1解密

RC-5：RSA数据安全公司的很多产品都使用了RC-5

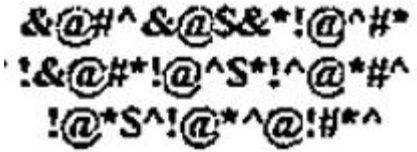
IDE算法：128位密钥、64位数据块、比DES的加密性好、对计算机功能要求相对低，PGP。

非对称加密技术

软考教育：帮助客户成功，创造社会价值

加密

公钥



解密

私钥

软考教育：帮助客户成功，创造社会价值

常见非对称密钥加密算法：RSA：512位（或1024位）密钥、计算量极大、难破解

ECC：椭圆曲线算法

缺陷：加密速度慢

单向散列函数、固定长度的散列值。

信息摘要

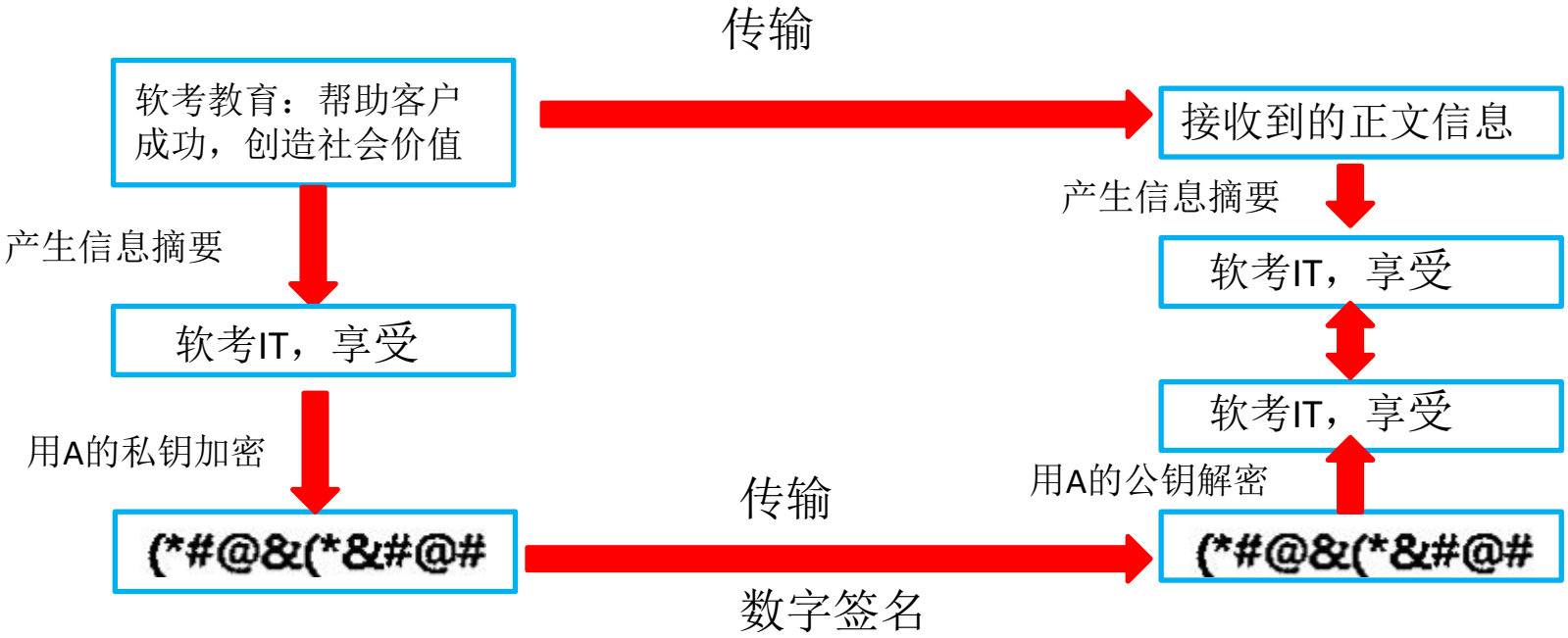
软考教育:IT在线教育平台，
让每个人随时随地享受IT教育

产生信息摘要

%%&^#@(*&(@

常用的消息摘要算法有MD5，SHA等，市场上广泛使用的MD5，SHA算法的散列值分别为128和160位，由于SHA通常采用的密钥长度较长，因此安全性高于MD5。

软考教育


传输
软考教育：帮助客户成功，创造社会价值
产生信息摘要
软考IT，享受
用A的私钥加密
(*#@&(*&#@#
传输
数字签名
接收到的正文信息
产生信息摘要
软考IT，享受
软考IT，享受
用A的公钥解密
(*#@&(*&#@#

请依据依已学习的加密技术，以及信息摘要，数字签名解决以下问题：

请设计一个安全邮件传输系统，要求：

该邮件以加密方式传输，邮件最大附件内容可达到500MB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

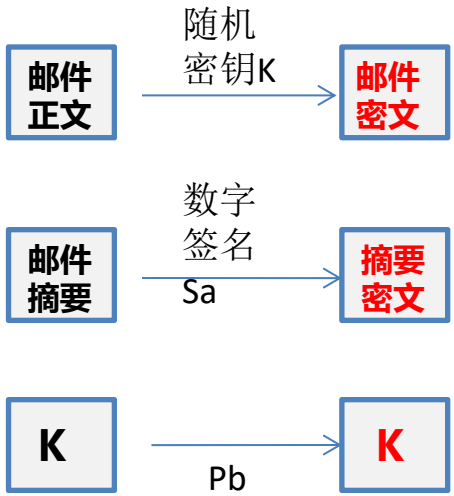
DESIGNER:
练习题

加密解密技术　　对称加密　　数字签名

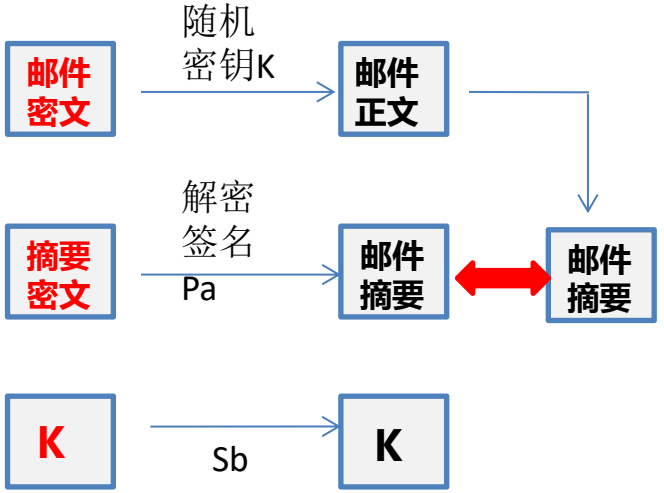
该邮件以加密方式传输，邮件最大附件内容可达500MB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

信息摘要技术

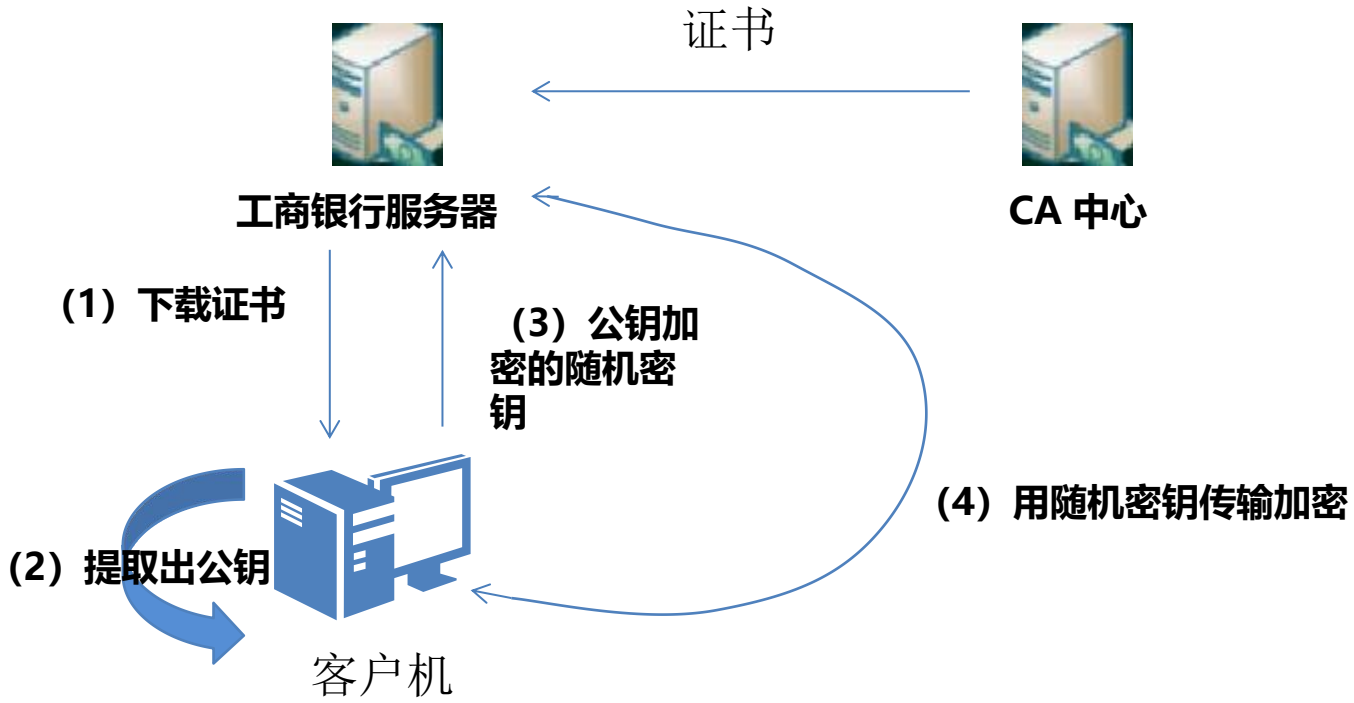
发送方A（公钥：Pa，私钥：Sa）：



接收方B（公钥：Pb，私钥：Sb）：



钓鱼网址何意?



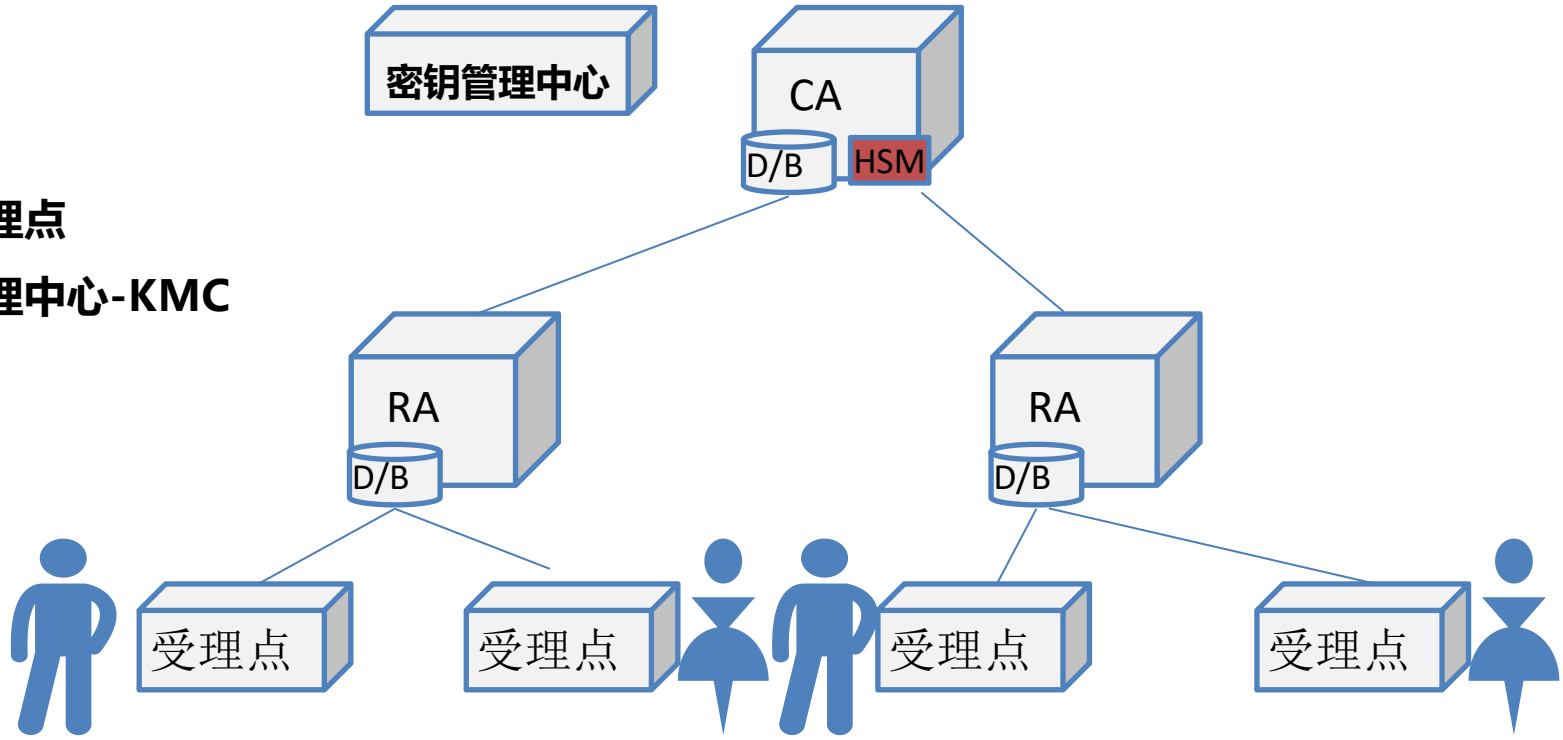
Digital Certificate

CA

RA

证书受理点

密钥管理中心-KMC



X.509数字证书内容

证书的版本信息；

证书的序列号，每个证书都有一个唯一的证书序列号；

证书所使用的签名算法；

证书的发行机构名称，命名规则一般采用X.500格式；

证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950-2049；

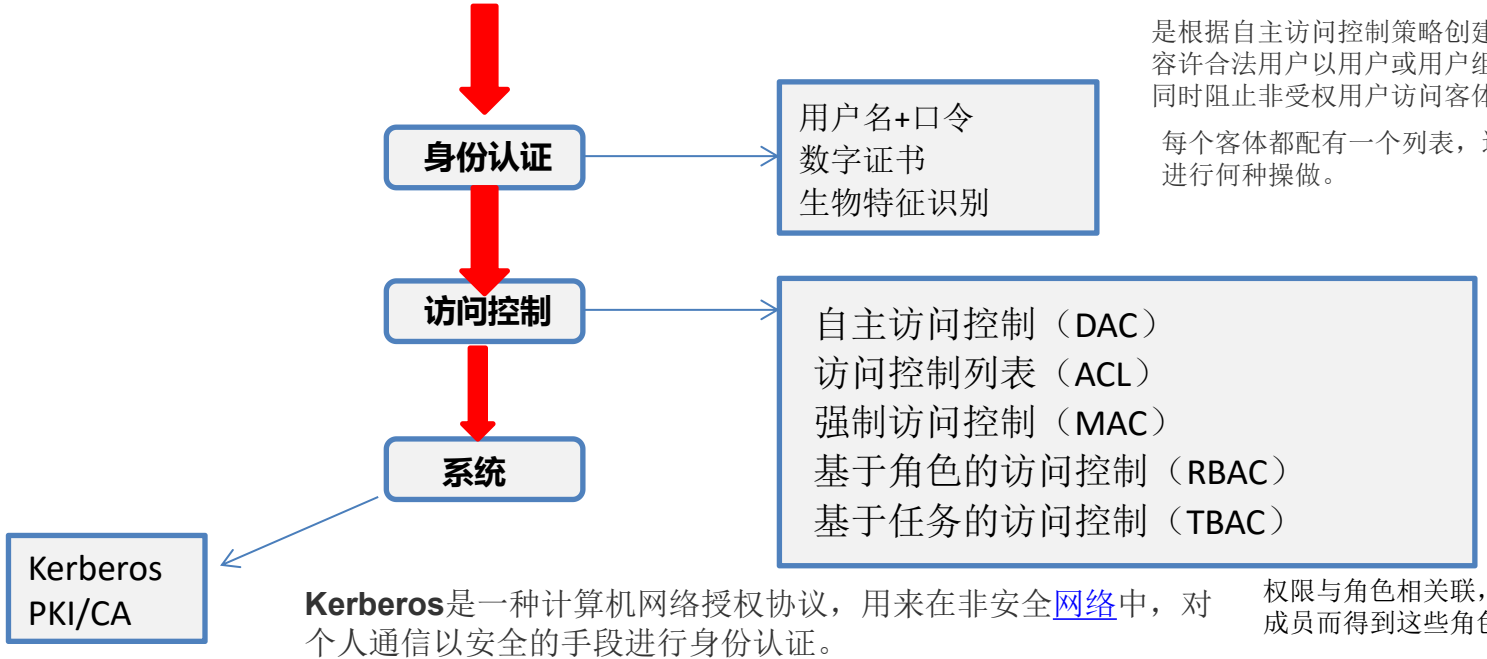
证书所有人的名称，命名规则一般采用X.500格式；

证书所有人的公开密钥

证书发行者对证书的签名

DESIGNER:

信息系统安全-保障层次



是根据自主访问控制策略创建的一种模型，
容许合法用户以用户或用户组的身份访问策略规定的客体
同时阻止非受权用户访问客体。

每个客体都配有一个列表，这个列表记录了主体对客体进行何种操做。

Kerberos是一种计算机网络授权协议，用来在非安全网络中，对个人通信以安全的手段进行身份认证。

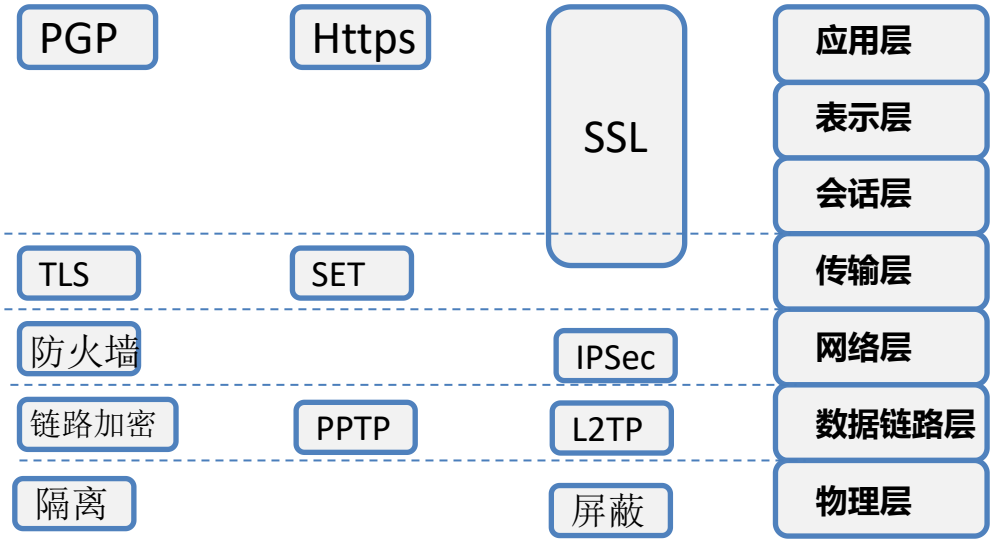
PKI/CA的解决方案的完整性和优越性是普遍的一个共识，非对称算法解决了密钥传递的问题，对称算法提高加密运算效率，哈希算法解决了完整性验证的问题的同时提高了数字效率，*CA*作为第三方为公钥的所有者背书，解决公钥的持有者证明问题，形成一个解决信息安全信息机密性、完整性、抗抵赖的完整解决方案。

权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。

是一种以任务为中心，动态授权的主动安全模型，授权时要考虑当前执行的任务。

DESIGNER:

网络安全-各个网络层次的安全保障



L2TP是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如PPTP要求网络为IP网络，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道.

电子邮件安全协议--PGP

HTTPS协议 = HTTP协议 + SSL/TLS协议，
在HTTPS数据传输的过程中，需要用SSL/TLS对数据进行加密和解密，需要用HTTP对加密后的数据进行传输。

TLS（传输层安全）是更为安全的升级版 SSL。

SET协议是基于信用卡支付模式而设计的。它保证了开放网络上使用信用卡进行在线购物的安全，是一个专门针对于信用卡电子支付的安全协议。

IPsec协议工作在OSI模型的第三层，以用来构建虚拟专用网（VPN），而这也是Ipsec最主要的用途之一。

PPTP点对点隧道协议。该协议是在PPP协议的基础发的一种新的增强型安全协议,支持多协议虚拟专用网(VPN).

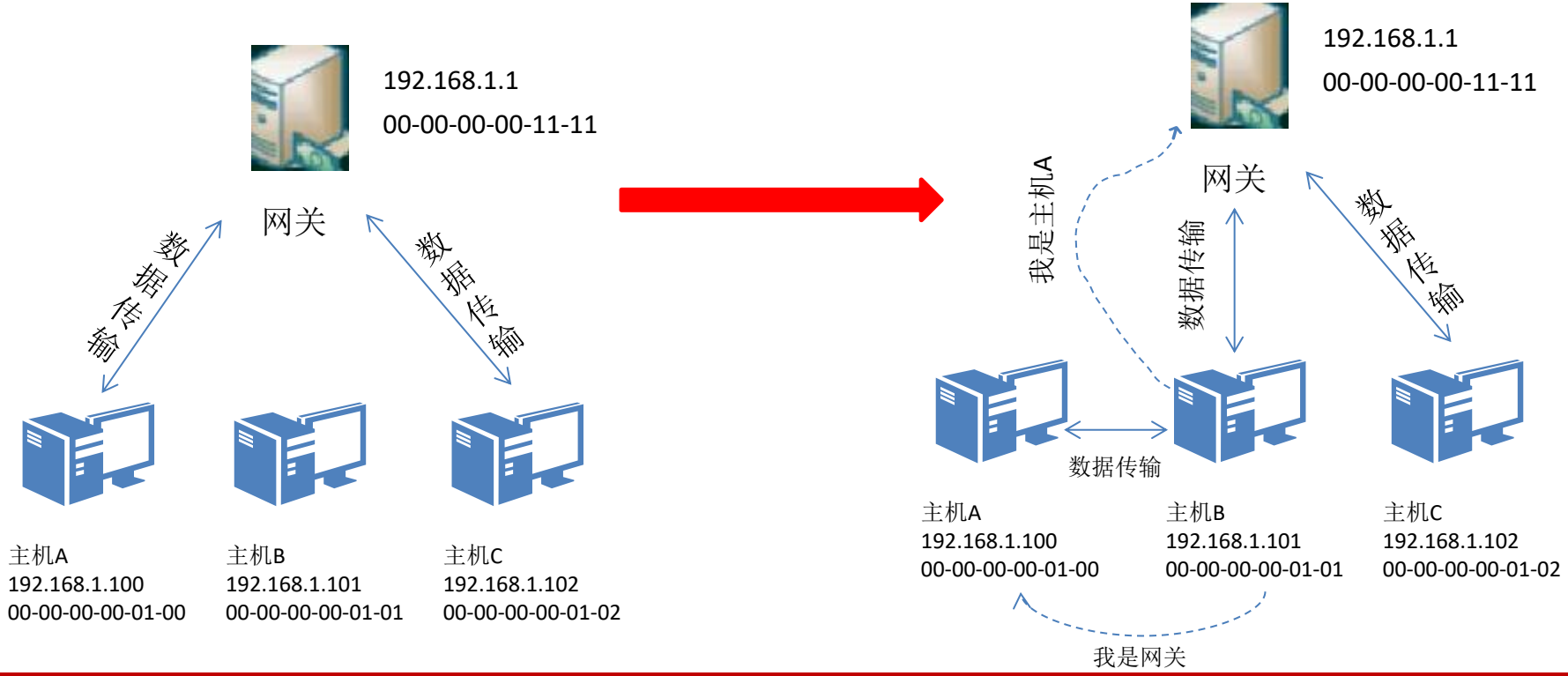
DESIGNER:

网络安全-网络攻击的类型

- ✓ ARP欺骗攻击
- ✓ DoS（拒绝服务）与DDoS
- ✓ 重放攻击

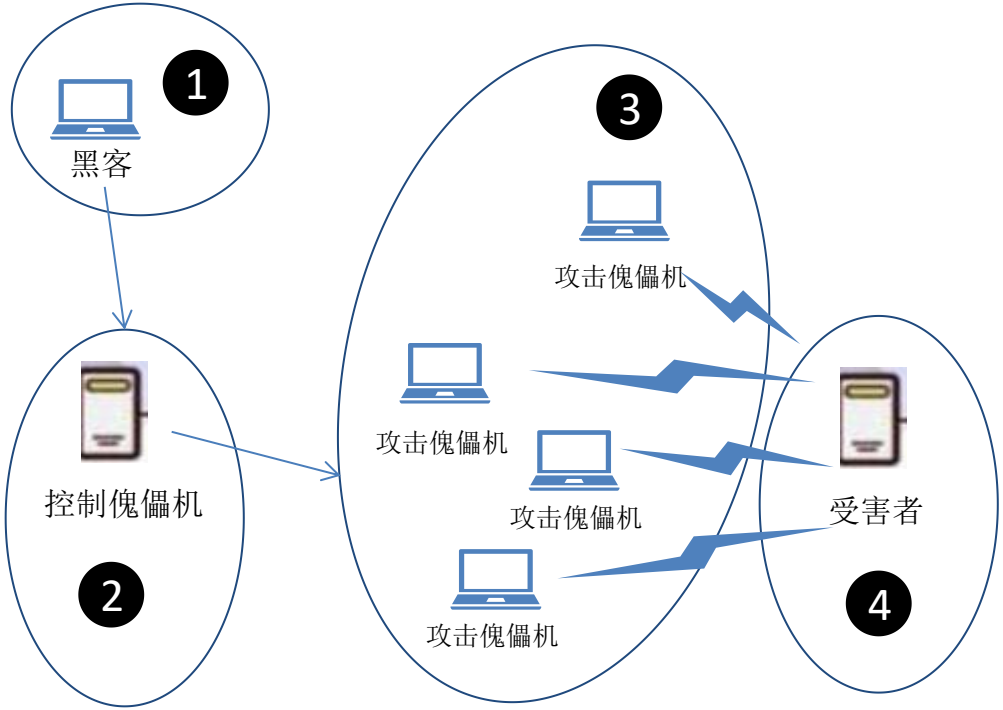
DESIGNER:

网络安全-ARP欺骗攻击



DESIGNER:

网络安全-DoS（拒绝服务）与DDoS



DOS攻击：一台或多台计算机对受攻击服务器的某一个端口发送大量无关的UDP报文，导致整个通道内的正常服务无法进行。

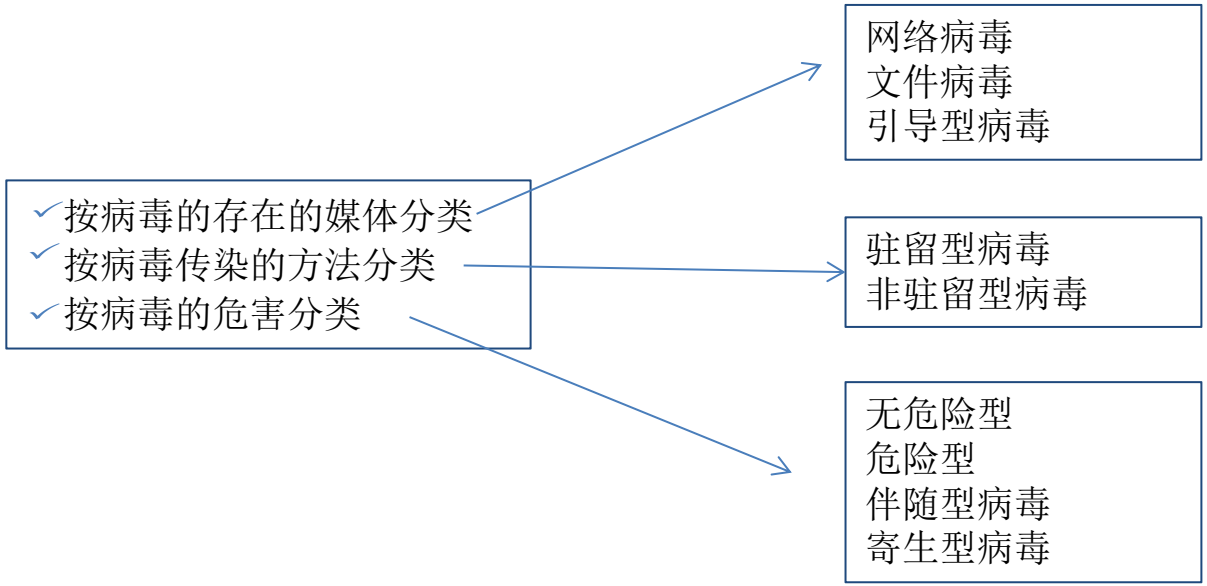
DDOS攻击：大量的肉鸡对服务器的不同端口发送巨型流量的UDP报文，无法通关关闭端口的方式来进行隔离，破坏力极强，严重会造成服务器当宕机。

计算机信息系统安全保护等级划分准则（GB17859-1999）

用户自主保护级：适用于普通内联网用户
系统审计保护级：适用于通过内联网或国际网进行商务活动，需要保密的非重要单位
安全标记保护级：适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位
结构化保护级：适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研机构和国防建设等部门
访问验证保护级：适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

计算机病毒与木马

病毒：编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机适用并且能够自我复制的一组计算机指令或者程序代码。
木马：计算机木马是一种后门程序，常被黑客用作控制远程计算机的工具。



计算机病毒与木马

系统病毒（前缀：Win32、PE、W32，如：KCOM——Win32.KCOM)
蠕虫病毒（如：恶鹰——Worm.BBeagle)
木马病毒、黑客病毒（如：QQ消息尾巴木马——Trojan.QQ3344)
脚本病毒（如：红色代码——Script.Redlof)
宏病毒（如：美丽莎——Macro.Me l isaa)
后门病毒（如：灰鸽子——Backdoor.Win32.Huigezi)
病毒种植程序病毒（冰河播种者——Dropper.BingHe2.2C)
破坏性程序病毒（杀手命令——Harm.Command.Killer)
玩笑病毒（如：女鬼——Joke.Girl ghost)
捆绑机病毒（如：捆绑QQ——Binder . QQPass.QQBin)

DES 加密算法的密钥长度为 56 位，三重 DES 的密钥长度为（64）位。(64)A. 168 B. 128 C. 112 D. 56

【答案】C

【解析】

DES 加密算法的密钥长度为 56 位，三重 DES 要用到 2 个 DES 的密钥，所以长度为 112 位。

下列攻击方式中，流量分析属于（65）方式。

(65)A. 被动攻击 B. 主动攻击 C. 物理攻击 D. 分发攻击

【答案】A

【解析】

在被动攻击(passive attack)中，攻击者的目的只是获取信息，这就意味着攻击者不会篡改信息或危害系统。系统可以不中断其正常运行。常见的被动攻击包括：窃听和流量分析。

主动攻击(active attack)可能改变信息或危害系统。威胁信息完整性和有效性的攻击就是主动攻击。主动攻击通常易于探测但却难于防范，因为攻击者可以通过多种方法发起攻击。常见的主动攻击包括：篡改、伪装、重放、拒绝服务攻击。