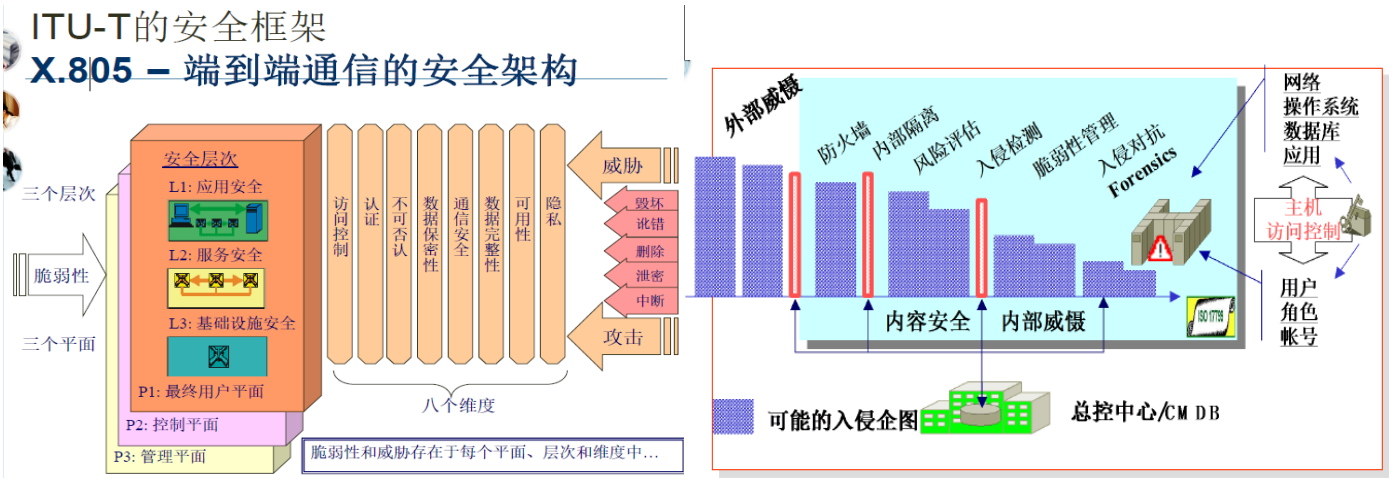
一、第一章：概述

1、**信息安全范畴？网络安全**：访问控制,入侵检测,网络连通性；**系统安全**：灾难恢复,系统冗余,线程管理；**数据安全**：数据加密,数据备份,病毒防护；**应用安全**：权限管理,身份认证,密钥管理,内存管理；**管理安全**：安全政策,安全组织,风险评估,安全流程,安全审计/绩效；2、**信息安全管理**？1）保护信息保密性,完整性,有效性；2）确保业务的永续性；3）确保信息安全前提下，建立有效的信息共享机制；3、**安全属性**（通俗说法--打不垮）：进不来、拿不走、改不了、看不懂、跑步了；4、**信息安全属性**：1）三大安全属性(CIA)：机密性(confidentially)、完整性(integrity)、可用性(availability)；2）其它属性：不可否认性(不可抵赖性, non-repudiation)、真实性；5、**分析方法**：1）保护什么；2）存在哪些安全威胁；3）达到什么安全目标。



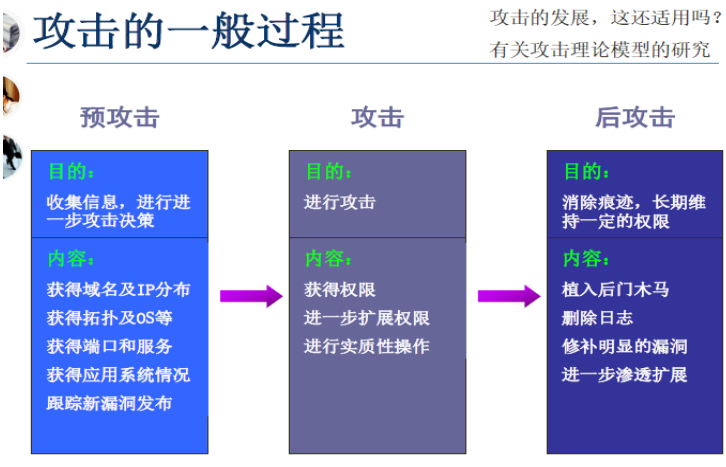
6、**安全模型**：1）风险评估模型；2）纵深防御模型：a.纵深：功能,路由,位置,协议层次等; b.**方法论**（方法**核心思想**）：等级划分、边界防护；3）TBS(基于时间的安全体系)模型：a. P>D+R：P(protection)即防护手段所能支持的时间、D(detection)即检测手段发现入侵所需时间、R(response)即事件响应机制采取有效措施所需时间，即安全体系具有充足的时间在攻击成功之前进行有效响应，阻止网络攻击；**指导思想**：快速检测、有限影响、快速溯源，快速恢复相应的安全机制；b. 其它：PDRR(保护、检测、响应、恢复)、P2DR(策略 policy、保护、检测、响应，**动态安全模型**)、wPDRpc--PPT(人 people、流程/管理 process、技术 technology)

7、**网络模型有问题吗**(网络及威胁的发展) ？1）网络：a. 分布式网络,扁平化网络,内、外不分,层次减少：纵深防御的问题; b.动态的网络,如 SDN 软件可定义. 2）攻击：APT

8、基础模型的研究与创新：方法论的改变，基本思路的改变，新的安全产品，安全市场

9、**可信计算**：1）可信的定义：一个设备的行为是按照其预期目标和指定方式执行的，且一个可信平台应当至少提供三个基本特性：保护能力、完整性测量和完整性报告；TPM(可信平台模型)

10、**可生存性**：1）当前主要的安全技术：a. 检测、保护、响应、恢复,攻击与防护的矛盾,防护总处于被动；b.风险总是存在的：网络不可能没有病毒,网络上不会没有黑客,网络系统肯定存在漏洞/BUG,管理员不能全部永远地忠诚,人总会有疏忽,安全产品也可能有漏洞；c.当前比较认同的可生存性的**定义**：当攻击，失效和事故发生的时候，系统在规定的时间内完成任务的能力；2）主要研究内容：可生存性模型、可生存性评估方法、可生存性技术（a. 基于冗余资源的网络生存性机理: 入侵容忍技术、多方安全计算、门槛密码技术、Byzantine 协议技术、容错备份技术、灾难恢复方法、分布式存储; b. 基于紧急事件响应网关的网络生存性机理：紧急响应技术等）



11、**安全的一些特性**：1)安全的相对性：没有绝对的安全; 2)安全的时效性/时代性; 3)安全的动态性：技术跟进和维护支持的重要性; 4)安全的对抗性; 5)安全的多样性/复杂性(环境,网络,系统,信息,人员等；技术复杂、管理难度大); 6)安全的层次性; 7)安全的分布性

12、计算机系统安全等级保护（1~5 级）：自主保护级(用户自主),指导保护级(系统审计),监督保护级(安全标记),强制保护级(结构化),专控保护级(访问验证)

第二章、网络攻防

1、攻击者来源：内部人员(70%)，准内部人员，特殊身份人员，外部个人和小组(黑客)，竞争对手和恐怖组织，敌对国家和军事组织。

2、**攻击分类**：1）主动攻击：包括网络扫描、拒绝服务攻击、缓冲区溢出、欺骗和网络钓鱼、信息篡改、会话劫持、隐密通道等攻击方法；2）被动攻击：包括嗅探、流量分析、信息收集等攻击方法。多数情况下这两种类型被联合应用；3）其它分类方法：a.攻击目的：拒绝服务攻击(Dos)、获取系统权限的攻击、获取敏感信息的攻击; b.攻击切入点：缓冲区溢出攻击、系统设置漏洞的攻击等; c. 攻击的纵向实施过程：获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等; d.攻击目标：包括对各种应用系统的攻击(系统攻防)、对网络设备的攻击(网络攻防)。

3、**攻击手段**：1）**预攻击阶段**(收集信息)：a.扫描：主机扫描,端口扫描,漏洞扫描,无线; 操作系统类型鉴别，网络拓扑分析; b.窃听，嗅探; c.利用一些信息服务：搜索引擎,网站,出版物; d.社会工程（SNS)；2）**攻击阶段**：缓冲区溢出攻击;操作系统漏洞;应用服务缺陷;口令攻击;错误及弱配置攻击;欺骗,伪造;信息窃取、窜改\插入,删除,重发;劫持 ;-In-The-Middle(MITM); DOS/DDOS; SPAM; WEB 攻击; BOTNET：P2P, SNS; Zero-day; Phishing; APT(Advance-Persistent-Threat);Covert-channel；3）**后攻击阶段**：后门木马、痕迹擦除；

4、**安全建模**：攻击树、攻击图、博弈论、Petri 网；**5、攻击图**：状态攻击图和属性攻击图。1）状态攻击图中的节点表示网络的当前状态，网络状态信息包括主机相关信息、用户权限、主机提供的服务等信息。有向边表示引起状态改变的攻击行为；2）属性攻击图有两类节点，一类代表原子攻击，另一类是属性节点，代表原子攻击的前提或结果。连接属性节点与原子攻击节点之间的边称为前提边或者后果边。只有当所有通过前提边与原子攻击节点相连的属性都被满足时，该原子节点所代表的原子攻击才会被执行。

密码学在信息网络安全中的作用

违反安全性的例子：

（1）用户**A**传输一个文件到用户**B**，该文件包含了敏感的数据，这样数据必须加以保护以防泄密。没有被授权读取该文件的用户**C**可能监视该传输过程，并在传输过程中截取了该副本。（机密性）

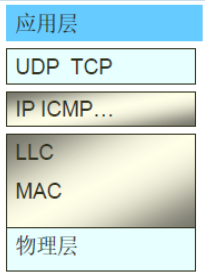
（2）某网络管理员**D**在其管理下向一台计算机**E**传输一条消息，该消息指示计算机**E**更新一个授权文件，该文件包含了能够访问该计算机的一些新用户标识符。用户**F**中途截取了该消息，并且增加和删除一些项从而改变了该消息，然后将该消息转发给**E**。计算机**E**以为该消息是从管理者**D**接收的，因而更新了这个授权文件。（完整性）

（3）用户**F**并没有中途阻止某消息，用户**F**构造了具有它自己希望内容的消息，并将该消息传输给**E**，好象该消息来自于管理员**D**。计算机**E**接收了以为来自于管理者**D**的消息并更新了它的授权文件。（鉴别性）

（4）一个客户向一个股票代理商发出带有多个交易指示的消息。随后，该投资跌值，而该客户不承认发送了该消息。（抗抵赖性）

IP网络面临的安全威胁

- **恶意攻击**
  - 网络扫描
  - DDoS
  - 窃取机密数据（窃听，中间人），流量分析
  - 欺骗和网络钓鱼（Phishing）
  - 会话劫持
  - 消息窜改，插入，删除，重发
  - 物理破坏
- **误用和滥用（内部和外部）**
  - 配置错误、缺省配置
  - 内部窃取：客户资料、充值卡等
  - 内部越权
  - 操作行为抵赖
  - 垃圾流量、邮件、电话和短信
- **恶意代码：**
  - 病毒和蠕虫,木马
  - 逻辑炸弹,时间炸弹



IP网络各层的主要威胁

查询CERT/CC – CNCERT/CC – SANS官方网站可以了解当前最新的漏洞和安全事件统计报告

6、**描述一种攻击方式的攻击原理**：1）DDOS：**a.定义**：分布式拒绝服务攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力；**b.攻击原理**：一个完善的 DDoS 攻击体系分成几大部分，控制和实际发起攻击者，对被攻击者(服务器，路由器，防火墙)来说，DDoS 的攻击包是从攻击傀儡机(僵尸电脑)上发出的，控制者只发布命令而不参与实际的攻击。有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自控制者的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了；**c.攻击方式**：通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。这种攻击方式可分为以下几种：通过使网络过载来干扰甚至阻断正常的网络通讯；通过向服务器提交大量请求，使服务器超负荷；阻断某一用户访问服务器；阻断某服务与特定系统或个人的通讯。

7、漏洞：1）漏洞预防：安全意识，安全审记；2）漏洞检测：渗透测试，风险评估；3）漏洞修复：补丁(patch)管理。

第三章、密码学

1、**密码学基本概念**：密码学包括两个方面：密码编码学和密码分析学；1)**密码编码学**就是研究对数据进行变换的原理、手段和方法的技术和科学;2)**密码分析学**是为了取得秘密的信息，而对密码系统及其流动的数据进行分析，是对密码原理、手段和方法进行分析、攻击的技术和科学。

2、**基本概念**：1)**明文**：需要秘密传送的消息；2)**密文**：明文经过密码变换后的消息；3)**加密**：由明文到密文的变换；3)**解密**：从密文恢复出明文的过程；4)**破译**：非法接收者试图从密文分析出明文的过程；5)**加密算法**：对明文进行加密时采用的一组规则；6)**解密算法**：对密文进行解密时采用的一组规则；7)**密钥**：加密和解密时使用的一组秘密信息；8)**密码系统**：用以下数学符号描述 S={P, C, K, D, E}(注：P 明文空间, C 密文空间, K 密钥空间, E 加密算法, D 解密

算法)；9)当给定密钥 $k \in K$ 时，加解密算法分别记作 E_k、D_k，密码系统表示为

$$S_k = \{P, C, k, E_k, D_k\}; C = E_k(P); P = D_k(C) = D_k(E_k(P))$$

3、加密安全性体现在：破译成本超过加密信息的价值,破译时间超过该信息有用的生命周期

4、**密码算法分类**：1)受限制的算法：算法的保密性基于保持算法的秘密；2)基于密钥的算法：算法的保密性基于对密钥的保密。

5、**加密体制的分类**：1) **基于密钥的算法，按照密钥的特点**分类:a. **对称密钥算法**：又称传统密码算法，就是加密密钥和解密密钥相同，或实质上等同，即从一个易于推出另一个。又称秘密密钥算法或单密钥算；b. **非对称密钥算法**：加密密钥和解密密钥不相同，从一个很难推出另一个。又称公开密钥算法。**公开密钥算法**用一个密钥进行加密,而用另一个进行解密.其中的加密密钥可以公开,又称公开密钥,简称公钥。解密密钥必须保密,又称私人密钥.简称私钥；c. 混合密钥体制；2)**按照明文的处理方法**：a.**分组密码**：将明文分成固定长度的组,用同一密钥和算法对每一块加密,输出也是固定长度的密文,计算机软件处理时代的主流；b. **流密码**：又称序列密码.序列密码每次加密一位的明文,序列密码是手工/机械密码时代的主流。

流密码（stream cipher):又称序列密码.序列密码每次加密一位的明文。序列密码是手工和机械密码时代的主流。

- 明文$m=m_1,m_2,\ldots\ldots m_k$
- 随机序列$k=k_1,k_2,\ldots\ldots k_k$
- 密文$c_i=m_i \oplus k_i$,i=1,2,……k
- 解密过程与加密过程一致, $m_i=c_i \oplus k_i= m_i \oplus k_i \oplus k_i$
- 序列密码的安全性完全依赖于随机序列的强度.
- 移位寄存器是产生序列密码的有效方法
- Key的作用， 密钥序列发生器的输出为key和函数

6、**密码模式**：某个分组密码算法为基础,对任意长度的明文加密的方法：**电码本 ECB、密码分组链接 CBC、密码反馈 CFB、输出反馈 OFB、计数器模式、分组链接 BC、扩散密码分组链接 PCBC。**

7、**应用(CBC)**：如何防止电脑彩票的伪造问题。**方法**：(1)选择一个分组密码算法和一个认证密钥，将他们存于售票机内；(2)将电脑彩票上的重要信息，如彩票期号、彩票号码、彩票股量、售票单位代号等重要信息按某个约定的规则作为彩票资料明文；(3)对彩票资料明文扩展一个校验码分组后，利用认证密钥和分组密码算法对之加密，并将得到的最后一个分组密文作为认证码打印于彩票上面。**认证过程**：执行(3),并将计算出的认证码与彩票上的认证码比较，二者一致时判定该彩票是真彩票，否则判定该彩票是假彩票。

8、**短块处理方法(直接扩充法)**：在电码本 ECB 模式和密码分组链接 CBC 模式中,都要求明文长度是明文分组规模的整数倍.否则就会出现最后一个明文分组是短块的情形.这时应如何处理呢?**方法 1**：对明文扩充,使最后一个分组不是短块,但需在文件头或最后一个明文分组中指明文件所含的字节数.(A) 添充全 0 比特或其它固定比特,或计算机内存中自然存放的数据。(B) 添充随机数. 相对而言,方法(A)简单,易实现,但安全性没有第二种方法好.

- 古典密码
  - 置换密码
    - 用加密置换去对消息进行加密
    - 举例：
      - 加密算法E =（2，1，4，3）
      - 解密算法D =（2，1，4，3）
      - 明文M =“置换密码”
      - 密文C = E(M) = “换置码密”
  - 代换密码
    - 明文中的字母用相应的密文字母进行替换
    - 单表代换密码
    - 多表代换密码

- 单表代换密码举例

明文: a b c d e f g h i j k l m n o p q r s t u v w x y z
密文: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- m = “Caser cipher is a shift substitution”
- c = “FDVHDU FLSHU LV D VKLIW VXEVWLWXWLRO”

9、**总结**：1)ECB 模式简单高速,但最弱,易受重发和替换攻击。商业软件中仍应用,可用于无结构小数据；2)低丢包率,低误码率,对明文的格式没有特殊要求的环境可选用 CBC 模式,需要完整性认证功能时也可选用该模式；3)高丢包率,或低误码率,对明文格式有特殊要求的环境(如字符处理),可选用 CFB 模式；4)低丢包率,但高误码率,或明文冗余多,可选用 OFB 模式。(但加密前先将明文压缩是一种安全的方法)

10、**对称加密算法**：1)优点：加密速度快；缺点:网络规模扩大后,密钥管理很困难；无法解决消息确认问题；缺乏自动检测密钥泄露的能力。2)典型算法：a.**DES**(数据加密标准，分组加密算法，以 64 位为分组对数据加密，密钥长度 56 位)，**分组密码设计准则(混淆、扩散、迭代结构)**；b.**IDEA**(国际数据解密算法，对称、分组密码算法,输入的明文为 64 位，密钥为 128 位,生成的密文为 64 位)；c.**AES**(高级加密标准, Rijndael 是迭代分组密码,其分组长度和密钥长度都是可变的;为了满足 AES 的要求,分组长度为 128bit,密码长度为 128/192/256bit,相应的轮数 r 为 10/12/14)；d.**RC 4/5/6** 系列。

11、**非对称密码技术**又称公钥密码技术,或双钥密码技术,即加密和解密数据使用不同的密钥

分组密码设计准则

混淆（confusion）：用于掩盖明文和密文间的关系。在加密变换过程中使明文、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统计分析法，通过研究密文以获取冗余度和统计模式。

扩散（diffusion）：通过将明文冗余度分散到密文中使之分散开来。密码分析者寻求这些冗余度将会更难。（扩散函数，通过换位，亦称置换）

迭代结构：选择某个较为简单的密码变换，在密钥控制下以迭代方式多次利用它进行加密变换，就可以实现预期的扩散和混乱效果。（轮函数）

公钥密码算法重要特性

- 加密与解密由不同的密钥完成
  加密X得到Y：$Y = E_{KU}(X)$
  解密Y得到X：$X = D_{KR}(Y) = D_{KR}(E_{KU}(X))$
- 知道加密算法，从加密密钥得到解密密钥在计算上是不可行的。
  $X = D_{KR}(E_{KU}(X)) = E_{KU}(D_{KR}(X))$
- 应用中一对密钥为：
  - 秘密密钥（私钥），由使用者自己掌握使用
  - 公共密钥（公钥），可以公开发布；
- 由公共密钥加密的信息必须用秘密密钥解密（必须是同一对密钥），由秘密密钥加密的信息必须用公共密钥解密。

12、**非对称加密算法**：公钥 pub、私钥 pri、A/B 通信终端（注:私钥具有唯一性,定要保存好）

加密	解密	功能
A + Bpub	B + Bpri	可以，可保证通信的机密性(具有唯一性)
A + Bpri		不可以，假冒攻击(身份假冒)
A + Apub	A + Apri	可以，但毫无意义(类似对称加密算法)
A + Apri	任何人 + Apub	可以，“认证功能”

由于公开密钥加密在计算上的巨大开销，当前主要用于：**密钥交换，数字签名**

典型算法	加密	密钥交换	数字签名
RSA(分组密码)	Y	Y	Y
EIGamal(盖莫尔算法)	Y	Y	Y
ECC(椭圆曲线密码算法)	Y	Y	Y
DH	N	Y	N
DSA	N	N	Y

Elgamal 算法步骤及其事例

Elgamal (cont.)

- 选择一个素数p，两个随机数g和x， g和x都小于p，计算$y=g^x \bmod p$，
  - 公钥为y，g，p
  - 私钥为x
  - g，p可由一组用户共享。
- Elgemal加密：
  - M-待加密消息，0<k-(随机数,秘密）< p-1，计算密文(a,b)：
    - $a = g^k \bmod p$
    - $b = y^k M \bmod p = (g^x)^k \bmod p$
  - 解密时，计算$M = b/a^x \bmod p = M(g^x)^k g\text{-}x^k \bmod p = M$
- Elgemal签名：
  - 计算$a = g^k \bmod p$
  - b满足$M = (xa+kb) \bmod (p-1)$， a,b为签名值, $b=(M-xa)k^{-1} \bmod (p-1)$
  - 验证：$y^a a^b \bmod p = g^M \bmod p$

- 生成密钥：使用者Alice选取素数p=2357及Z_{2357}*的生成元g=2,Alice选取私钥x=1751并计算
  $g^x \bmod p = 2^{1751} \bmod 2357 = 1185$
  A的公钥是p=2357，g=2, $g^x=1185$
- 加密：为加密信息m=2035，Bob选取一个随机整数k=1520并计算
  $a = 2^{1520} \bmod 2357 = 1430$,
  $b = 2035 \times 1185^{1520} \bmod 2357 = 697$
  Bob发送a,b给Alice
- 解密：Alice计算
  $a^{-x} \equiv 1430^{p-1-x} \equiv 1430^{605} \equiv 872 \pmod{2357}$
  $M \equiv b/a^x \equiv ba^{-x} \equiv 697 \times 872 \equiv 2035 \pmod{2357}$

13、非对称密钥算法的优缺点：1)优点:可以适用网络的开放性要求,密钥管理相对简单;可以实现数字签名,认证鉴权和密钥交换等功能; 2)缺点：算法一般比较复杂，加解密速度慢。

14、数字信封的定义：利用接收方公开密钥对加密信息原文的密钥 P 进行加密后再定点传送，这就好比用一个安全的“信封”把密钥 P 封装起来，所以称做数字信封。采用**公开密钥加密法的数字信封，实质上是一个能分发、传播称数字密钥的安全通道（概念）**。

15、**Hash 函数(哈希)**：1)函数 y=H(x),将任意长度的 x 变换成固定长度的 y;2) 单向 Hash 函数特性：a.单向性,任给 y,计算 x,使得 y=H(x)困难; b.快速性,计算 y=H(x)容易; c.无碰撞,寻找 x1 不等于 x2 时,满足 H(x1)=H(x2)是困难的。**HASH(散列算法)**:a.算法特点:不定长度输入,固定长度输出; b.输入很小的变动可引起输出较大变动;c.完成单向(已知输出无法

推算出输入,即无法让消息摘要不变而修改原文;已知两个输出的差别无法推算出输入的差别);d.常用 MD5,SHA; e.抗碰撞性的能力体现出单向散列函数对抗生日攻击和伪造的能力(强与弱抗碰撞性)

下图：左图表示公开密钥算法的基础、右图展示的是 RSA 计算事例

Whitfield Diffie提出绝大多数公开密钥算法都基于以下三种难题之一：

1.背包问题：给定一个互不相同的数组成的集合，找出一个子集其和为N

2.离散对数：如果p是素数，g和M是整数，找出x满足 $g^x \equiv M \pmod p$

3. 因子分解：设N是两个素数的积，则

(a) 分解N

(b) 给定整数M和C，寻找d满足 $M^d \equiv C \pmod N$

(c) 给定整数e和C，寻找M满足 $M^e \equiv C \pmod N$

(d) 给定整数x，判定是否存在整数满足 $x \equiv y^2 \pmod N$

例：如果p=47 q=71,那么n=pq=3337

加密密钥e与（p-1）(q-1)=46X70=3220没有公因子

随机选取e，如79，那么： $d=79^{-1} \bmod 3220=1019$

公开e和n，将d保密

加密消息 m=6882326879666683

首先将其分成小的组，在此例中，按三位数字一分组就可进行加密，这个消息将分成六个分组mi进行加密：

m1=688 m2=232 m3=687 m4=966 m5=668 m6=003

第一组分组加密为：$688^{79} \bmod 3337=1570= c1$

对随后的分组进行加密得密文：

c=1570 2756 2091 2276 2423 158

解密消息时用解密密钥d=1019进行相同的指数运算。因而：

$1570^{1019} \pmod{3337}=688= m1$

消息的其余部分可用同样的方法恢复出来。

16、**消息认证 MAC**：1)a.**消息摘要**(保证数据的完整性);b.**消息摘要算法**采用单向散列函数从明文产生摘要密文,**摘要密文**又称为**数字指纹**、**数据认证码 DAC**、**篡改检验码 MDC**; 2) 消息的散列值由只有通信双方知道的秘密密钥 K 来控制，此时散列值称作**消息认证码 MAC**;

17、**数字签名**：1)其作用相当于手写签名,功能:a.保证数据完整性;b.具有不可否认性; c.用于发送方的身份认证; 2)**数字签名常见算法**：a.**普通数字签名算法**(RSA--数字签名事实上的标准, ElGamal,DSS,DSA, ECDSA); b.**盲签名算法**(消息拥有者先将消息盲化,签名者对盲化的消息进行签名,消息拥有者对签字除去盲因子,得到签名者关于原消息的签名); c.群签名算法(正确性、匿名性、可追踪性、不可陷害性); d.环签名; e.门限签名; 3)**数字签名** $E\left[H(m)\right]_{pri}$，$E\left[H(m)\right]_{k}$ 为消息认证码，其中 H(m)表示消息摘要(用于保证文件的完整性)，E[]表示加密，key 表示密钥，pri 表示文件发送方的私钥，其功能是对完整性的检查，且可验证消息认证者的身份；4)发送的消息：m+ $E\left[H(m)\right]_{Apri}$ +Bpub；5)**解密过程**：用 pub 解密得到 H(m),再计算 m 的哈希值 H'(m),再判断 H(m)是否等于 H'(m),从而验证消息是否被篡改。

18、数字水印(指永久镶嵌在其它数据(主要指宿主数据)中具有可鉴别性的数字信号或数字模式)：1)主要特征:不可感知性/鲁棒性/可证明性/自恢复性/安全保密性

19、密钥管理技术:包括密钥产生、**生成**、**分发**、**验证**、**存储**、备份、保护、**吊销**、**更新**等

20、密钥组织结构(多层密钥系统):1)基本思想:用密钥保护密钥一个系统中常有多个密钥; 2) **会话密钥或数据加密密钥**：最底层的密钥，直接对数据进行加密和解密；**密钥加密密钥**：最底层上所有的密钥，对下一层密钥进行加密；**主密钥**：最高层的密钥，是密钥系统的核心

21、**公钥、私钥进行身份验证时，需第三方可信权威机构的验证其功能的有效性**

22、**密钥分发中威胁**：1)**消息重放**:a.攻击者简单复制一条消息，以后重新发送它(可能导致向敌人暴露会话密钥,或成功地冒充其他人); b.**抵抗消息重放的方法**(添加随机因素)：时间戳、挑战/应答方式(分发随机数); 2)**中间人攻击**:a.过程:截获信息、伪造身份并加密、发送; b.**对策**(针对伪造身份进行验证)：使用数字签名的密钥交换(到第三方权威机构进行身份验证)、联锁协议。 23、典型的**自动密钥分配途径**：集中式和分布式（无中心的）分配方案。

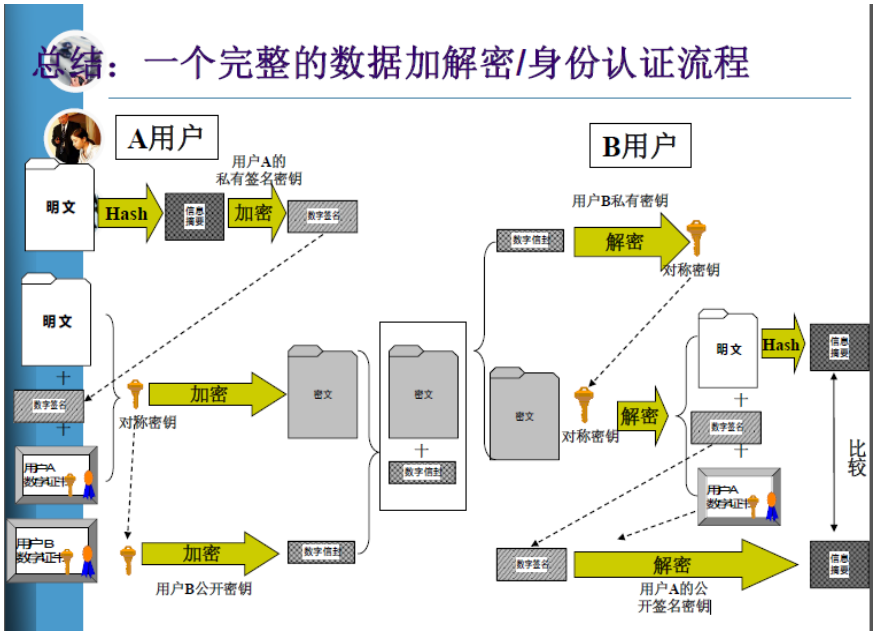
24、**数字证书**：提供一种在 Internet 上验证身份的方式，是用来标志和证明网络通信双方身份的数字信息文件(**功能**：使公钥系统得以提供**认证、数据完整性、机密性和不可否认**等安全服务)

25、**证书机构(CA)**: 是可以签发数字证书的信任机构(线上签发); **注册机构 RA**：进行用户身份信息的审查，确保真实性(线下审核); **证书管理协议 CMP**：PKCS/CMP/CMC/SCEP/IETF OCSP; **CA 在证书失效前进行吊销，需要两种方法来吊销证书并通知吊销的终端实体(CRL/OCSP)**; **使用数字证书的用户之间通过 CA(一个可信的第三方)来建立信任关系**。

26、**PKCS**：公钥密码标准 **CMC**:证书管理消息 **SCEP**：简单证书登记协议 **OCSP**：在线证书状态协议

27、第二种身份验证机构：PMI，区别于 PKI，即增加了属性特级机构，其它：SPKI/SDSI

28、应用题：A,B 用户分别有公钥 P(A),P(B),私钥 S(A),S(b),A 与 B 之间需对大量电子公文进行交互,为保证机密性/完整性,并完成身份认证,请简述 A 向 B 发送公文下的工作步骤,并指出这一过程中的消息摘要/消息验证码(验证码)/数字签名/数字信封分别是什么?**步骤如下页左图所示，具体概念请参考以上内容**



第四章 安全防御体系

1、网络和业务的发展 vs 安全的挑战：1)网络结构：a.虚拟化（设备、拓扑、网络功能）;b.软件定义，动态按需部署; 2)挑战：安全域的边界：模糊、跨边界交互增加; 3)对策：软件定义？对网络、计算、存储资源的感知. 注：**IDS 入侵检测系统 IPS 入侵防御系统**

2、**防火墙技术种类**：1)包(IP 分组)过滤技术：a.基本包过滤(静态包过滤); b.基于状态检测的包过滤(动态包过滤); c.常见包过滤设备/软件(路由器访问控制表 ACL/硬件包过滤设备); 2) 代理服务技术：应用层网关级防火墙.

3、**入侵检测分类**：1)**误用检测模型**(特征分析或基于知识的检测)：a.**概念**：收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵; b.**性能**：检测准确率高，但检测范围受已知知识的局限;对目标系统依赖性高，移植性差; 2)**异常检测模型**：a.**概念**：首先总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵(度量及门限); b.**性能**：通用性较强，甚至有可能检测出以前未出现过的攻击方法;异常与入侵并不一定总是相关;可能被恶意训练欺骗。

4、**按数据来源(文件内容分析/信誉)分类**：1)**基于主机**:系统获取数据的依据是系统运行所在的主机(系统日志、应用程序日志),保护的目标也是系统运行所在的主机; 2)**基于网络**：系统获取的数据是网络传输的数据包,保护的是网络的运行,往往将一台机器的网卡设于混杂模式,监听所有本网段内的数据包并进行判断; 3)混合型：基于主机又基于网络，一般是分布式的。5、**按系统各模块的运行方式分类**：集中式与分布式。

6、**入侵检测关键技术**：1)**主要功能部件**:信息收集、信息分析、结果处理; 2)**检测算法**：a.误用检测：首先定义违背安全策略的事件的特征，检测主要判别这类特征是否在所收集到的数据中出现; b.**异常检测**：建立系统“正常”情况的模型，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。

第五章 访问控制 访问控制是最基本的安全服务

1、**访问控制构成**：1)**授权**：规定可对该资源执行的操作/权限(与系统相关); 2)**策略**; 3) **客体**：又称作目标,规定需要保护的资源(所有可供访问的软、硬件资源、数据、信息等); 4) **主体**：又称发起者,是一个主动的、可以访问资源的实体. **访问控制(策略、审计及身份认证)。其中，策略：允许问题(是否允许) 审计：记录系统**

2、**访问控制模型**：1)**自主访问控制(任意访问控制/选择性访问控制)**,它允许用户可以自主地在系统中规定谁可以存取它的资源实体; 2)**强制访问控制**,指用户的权限和文件(客体)的安全属性都是固定的,由系统决定一个用户对某个文件能否实行访问; 3)**区别**：决定访问控制权限的归属权；

3、**访问控制技术**：1)**DAC**：a.实现结构(访问控制矩阵); b.特点：由个体决定权限;授权基于主体和客体的标识/身份;其自主性为用户提供了极大的灵活性,适合于小规模的系统和应用; **无法防止特洛伊木马攻击**; 2)**MAC**：a.**最典型的MAC**: BLP 模型(禁止向下写、禁止向上读)；b.**问题**：限制了高安全级别用户向非敏感客体写数据的合理要求;高安全级别的主体拥有的数据永远不能被低安全级别的主体访问,降低了系统的可用性;不能同时实现系统对机密性和完整性(不可篡改)的要求;过于偏重保密性,对其它方面如系统连续工作能力、授权的可管理性等考虑不足,造成管理不便,灵活性差; e.**特点**：比较适合与等级划分严格的行业;当存在隐密信道时，这种访问准则会被破坏; 3)**RBAC**：**基于角色的访问控制模型**，a.**目的**：解决访问控制管理的复杂性; b.**原理**：将访问权限分配给角色,用户担任一定的角色,从而具有角色对应的权限; c.**假设**：用户变化频繁，角色相对稳定; d.**优势**：便于授权管理，便于权限划分;策略与访问控制模型分离;操作系统、数据库中广泛的支持; e.**问题**：角色限定了权限,难以实现细粒度的访问权限管理;必须预先知道用户信息,配置用户到角色的分配;4)**ABAC**：**基于属性的访问控制**; 5)UWA：用户管理访问

第六章 身份管理(IDM/IAM/AIM)与认证

1、**AAA**：**认证**(Authentication),**授权**(authorization),**行政审计**(accounting),业务系统中最基本的安全服务;**身份管理和认证是基础**:证实客户的真实身份与其所声称的身份是否相符的过程.

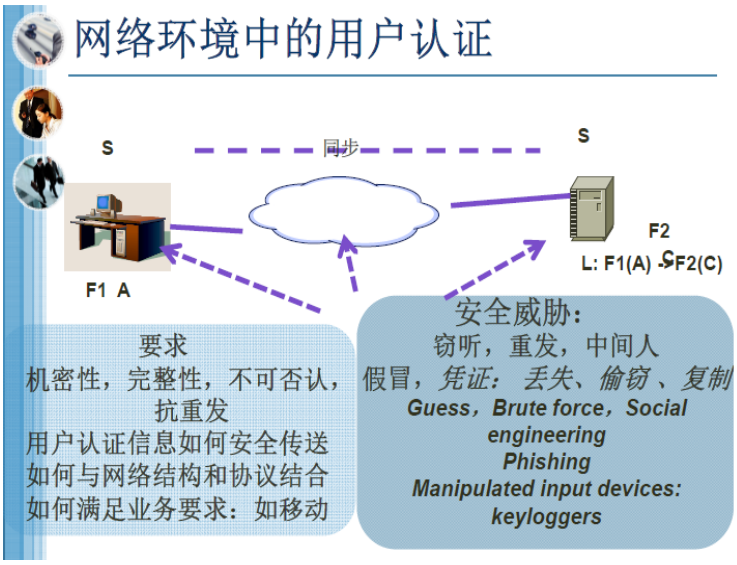
例如：辅导员证明(认证) → 院里审核(授权) → 盖章+登记(行政审计)

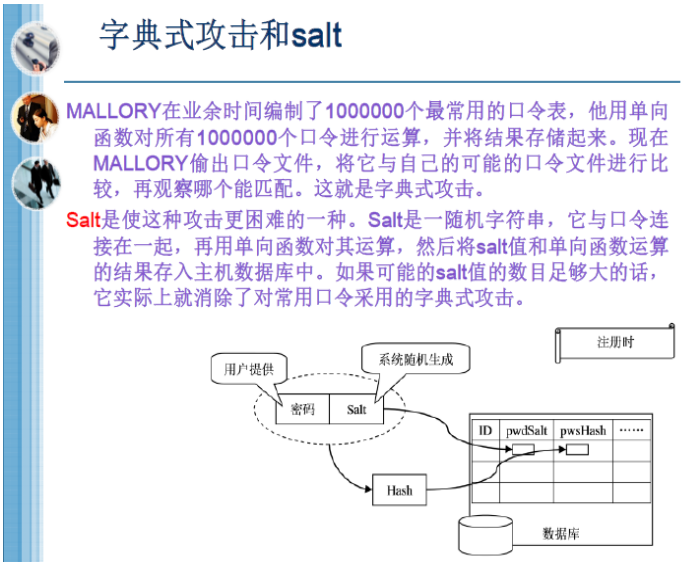
2、大题：网络环境中的身份管理和认证，即举几个你**熟悉的业务系统身份管理和认证实例**；当前的使用现状你还满意吗？觉得有什么需改进的地方；总结（需完成的功能；可能面对哪些安全威胁） 解答：**北邮统一身份认证平台（北邮信息服务门户网站）**

3、**实体认证的作用**：1)认证分为实体认证和消息认证; 2)**实体认证**是对通信主体的认证，目的是识别通信方的真实身份，防止假冒，常用**数字签名**的方法；3)**消息认证**是对通信数据的认证，目的是验证消息在传送或存储过程中是否被篡改，一般用消息摘要的方法；4)其它：1)**Passfaces**: 一个身份验证系统,让用户识别认识的人脸; 2)**CAPTCHA**：计算机区分人和计算机

4、**IDM 参考模型**：1)三方身份管理模型对应的实体：用户/终端实体(人/法人)、**依赖方 SP**(业务或资源提供商)、**身份提供者 IDP**(政府或可信第三方); 2)**SSO：单点登录**; 3)SAML：基于 XML 的框架

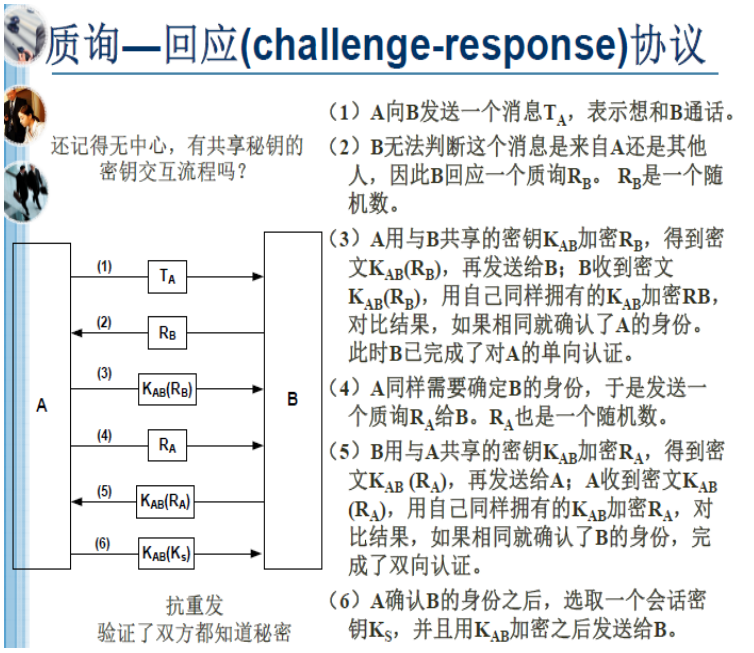
5、**身份认证基本原理**：1）**凭证**：(1)知道什么：口令，PIN 码，秘密或私钥等；(2)拥有什么：磁卡、令牌、密码智能卡、ID 卡、门钥匙，数字证书，手机；生物识别特征：指纹、声音、虹膜、DNA 及签名等；(3)**双因子认证机制**：你有什么+ 你知道什么。如：用户必须同时提供卡片与卡片相应的 PIN 码，具体事例：移动手机卡寻回过程（须有身份证，并知道 3 个常用联系人的电话号码）

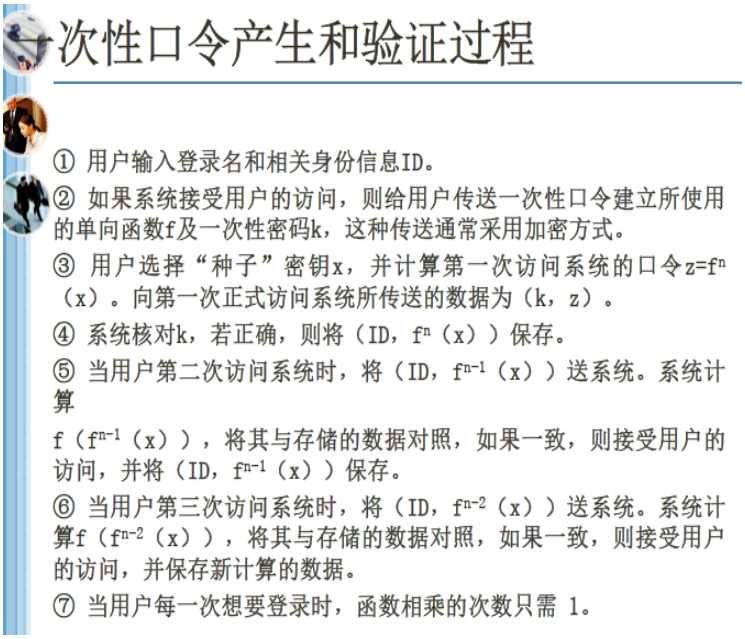




6、**一次性口令**：1）每次登录过程中传送的口令都不相同，以提高登录过程安全性，并可对付重放攻击；2）**特点**：a.概念简单，易于使用（基于一个被记忆的密码，不需要任何附加的硬件）；b.算法安全（不需要存储诸如密钥、口令等敏感信息）；c.**需要**：种子、迭代及同步。

7、**基于共享密钥的认证**：1）常见认证协议：(1)无可信第三方的质询--回应协议（使用 HASH，如 CHAP）；(2)有可信第三方，使用密钥分发中心的认证协议；(3)Needham-Schroeder 认证协议(多路质询--回应协议) (如 kerberos)；(4)Otway-Rees 认证协议。





Needham-Schroeder认证协议

（1）产生一个大的随机数R_A作为临时值，向KDC发送消息M(R_A, A, B)；

（2）KDC产生一个会话密钥KS，再用B的密钥K_B加密(A, K_S)，作为下轮A发给B的Ticket K_B (A, K_S)，然后再用A的密钥K_A加密(R_A, B, K_S, K_B (A, K_S))，发送给A；

（3）A用自己的密钥K_A解密密文，获取K_S和K_B (A, K_S)；然后产生一个新的随机数R_{A2}，用KDC发过来的K_S加密R_{A2}，将票据K_B (A, K_S)和K_S (R_{A2})发给B；

（4）B接收到消息用自己的密钥K_B解密密文K_B (A, KS)得到K_S，再用K_S解密密文K_S（R_{A2})得到R_{A2}；然后用K_S加密(R_{A2}-1)并产生随机数R_B，再发回给A。

（5）A收到消息后确认了B的身份，再向B发送K_S (R_B-1)。B收到消息后也可以确认A的身份，也确认了双方都有K_S。

共享秘密：K_A 和 K_B

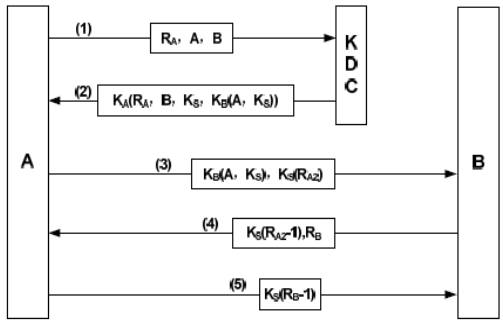
（1） A → KDC ： A || B|| Ra

（2） KDC → A ： EKa [Ra || B || Ks || EKb [Ks ||A]]

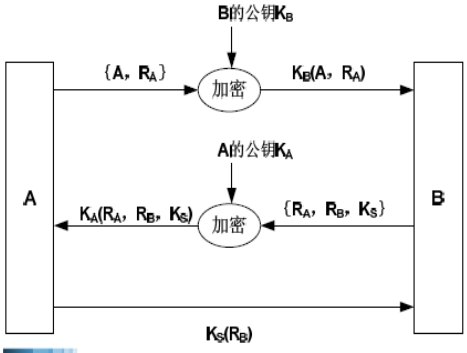
（3） A → B： EKb [Ks || A]

（4） B → A： EKs [Rb]

（5） A → B： EKs [Rb-1]



基于公钥的认证（无可信第三方的）



（1）A首先生成质询信息R_A，R_A是一个随机数；接着A用B的公钥K_B加密会话信息｛A, R_A｝，然后发给B。

（2）B用自己的私钥解出｛A, R_A｝，再生成质询信息R_B和会话密钥K_S，接着B用A的公钥K_A加密会话信息｛R_A, R_B, K_S｝，然后发给A。

（3）A用自己的私钥解出｛R_A, R_B, K_S｝，核对R_A无误后，用K_S加密R_B，然后发给B。B收到后用K_S解出R_B，核对无误后完成双向认证。

公钥私钥对的可信问题

Otway-Rees认证协议

（1）A产生一消息，包括用和KDC共享的密钥Ka加密的一个索引号R、A的名字、B的名字和一随机数Ra。

（2）B用A消息中的加密部分构造一条新消息。包括用和KDC共享的密钥Kb加密的一个索引号R、A的名字、B的名字和一新随机数Rb。

（3）、KDC检查明文R和两个加密部分中的索引号R是否相同，如果相同，就认为从B来的消息是有效的（认证了A,B)。KDC产生一个会话密钥Ks用Kb和Ka分别加密后传送给B，每条消息都包含KDC接收到的随机数。

（4）B把用A的密钥加密的消息连同索引号R一起传给A。

KDC对A, B认证

（1） A → B： A || B || R || EKa [A || B || R ||Ra]

（2） B → KDC： R || A || B || EK a [A || B || R ||Ra] || EK b [A || B || R ||Rb]

（3） KDC → B： R || EKb [Rb || Ks] || EKa [Ra || Ks]

（4） B → A： R || EKa [Ra || Ks]

8、**Needham-Schroeder 认证协议**：1）问题：记住 KS，重发 KB (A, KS)和 KS (RA2)，可假冒 A；2）解决：加时间戳；3）A 如何对 B 进行认证；4）KA 泄密后？

9、**数字时间戳**：1）数字时间戳服务 DTS 是网上安全服务项目，由专门的机构提供；2）时间戳是一个经过加密后形成的凭证文档，包括：需加时间戳的文件的摘要、DTS 收到文件的日期和时间、DTS 的数字签名；3）时间戳**产生过程**：用户将需加时间戳的文件用 HASH 编码加密形成摘要，并将其发送到 DTS；DTS 在加入了收到日期和时间信息后再对该文件加密和数字签名，然后返回用户。

10、**数字证书 X.509**：1）原理说明：B 使用证书，通过验证 A 对 M 的签名，从而验证 A 的身份；2）三向认证，常同时传送证书 CERT，并由 PKI 系统验证证书的有效性；3）利用随机数而不是时间戳实现抗重发。

11、**实际系统**：1）宽带接入中 PAP， CHAP，EAP，端口认证；2）电信网中的 RADIUS，DIAMETER；3）Kerberos；4）Web 2.0 中的 Oauth；5）Skype；6）更多：IPSEC, TLS 等协议中的认证及密钥交互。

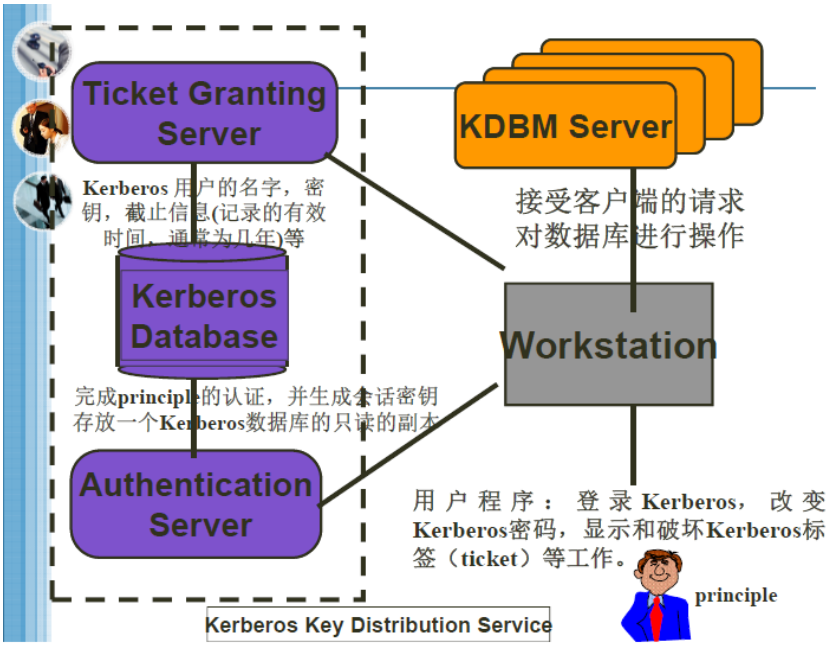
12、**实例：拨号接入用户的认证 PPP**：1）建立在 PPP 上的**口令验证协议**（PAP、SPAP、CHAP、MPPE 和 EAP)；2）口令验证协议（PAP）、挑战-握手验证协议（CHAP)、微软挑战-握手验证协议（MS-CHAP)；3）**PAP 身份认证的方式**：PAP 不是一个强壮的认证协议，它利用双向握手确认呼叫方的合法性，但是口令以明文的形式在链路转送，并且它不能防止重放或重复尝试攻击；PAP 允许在远端节点控制身份认证的频率和时间；PAP 协议的身份认证是两次握手验证过程。4）即客户端向服务器端请求信息（用户名，密码），服务器端向客户端返回验证结果（Ack/Nak)。

13、**CHAP（防止重发攻击)**：1）对 PAP 进行了改进，不再直接通过链路发送明文口令；2）CHAP 采用是三次握手验证，服务器端存有客户的明文口令，所以服务器可以重复客户端进行的运算，将结果与用户返回的口令进行对照；3）CHAP 为每一次验证任意生成一个挑战字符串来防止受到重发攻击。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第 3 方冒充远程客户进行攻击。

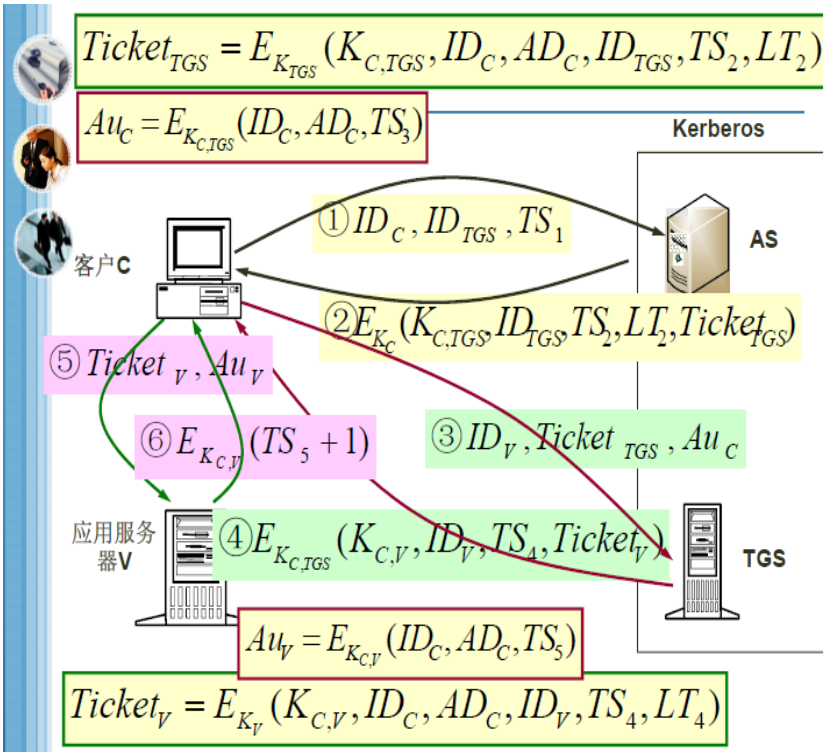
14、**以太网接入：基于端口的认证（点对点业务)**：1）**RADIUS**：管理远程用户验证和授权的常用方法，是一种基于 UDP 协议的轻量级协议；允许用户信息集中管理；适用于以 PPP 为基础的接入；功能弱:

授权功能几乎没有，计费功能很差，计费开始_结束(只计时间,不能计流量)。2）RADIUS 服务器可以被放置在 Internet 网络的任何地方为客户 NAS 提供验证；可以提供代理服务将验证请求转发到远端的 RADIUS 服务器。3）**其它协议：Diameter**（可靠传送: TCP SCTP）

15、**Kerberos**：1）为网络通信提供可信第三方服务的面向开放系统的认证机制；2）问题：口令次数问题，每次访问服务器均需输入口令；3）解决方法：票据重用、引入票据许可服务器 TGS；4）完整的 Kerberos 验证协议（如图）；



5）Kerberos 两种证书：票据 ticket 和认证符 authenticator，这两种证书都要加密，但加密的密钥不同。**(1) Ticket** 用来安全地在 AS 和 TGS 之间传递用户的身份，同时保证使用 ticket 的用户必须是 ticket 中指定的用户。**Ticket 的组成**：C/S 的标识，client 的地址，时间戳，生存时间，会话密钥五部分组成。Ticket 一旦生成，在 life 指定的时间内可以被 client 多次使用来申请同一个 server 的服务。**(2) Authenticator**：提供信息与 ticket 中的信息进行比较，一起保证发出 ticket 的用户就是 ticket 中指定的用户。**认证符组成**：client 的名字，client 的地址，记录当前时间的时间戳。authenticator 只能在一次服务请求中使用，每当 client 向 server 申请服务时，必须重新生



成 Authenticator。6）**Kerberos 验证标准**：(1)**术语**：IDc、IDv、IDtgs 分别为 C、V、TGS 的身份；ADc：用户的网络地址；TSi：第 i 个时戳；Lifetime：第 I 个有效期限；Pc：C 上的用户口令；Kc：C 和 AS 的共享密钥；Kv：V 和 TGS 的共享密钥；Ktgs： TGS 和 AS 的共享密钥；Kc,tgs：C 与 TGS 的共享密钥；Kc,v：C 与 V 的共享密钥（会话密钥）；C：客户机；V：服务器；TGS: ticket-granting server；AS：认证服务器。**(2)工作过程说明**：用户口令 PC 由用户和 AS 共享，AS 将 PC 保存在数据库中；不输入 C 的口令，就不能解开来自 AS 的信息；TS1 时戳用来防止重放攻击；Kc 由用户口令导出（用户机器收到 AS 回应后，要求用户输入密码，将密码转化为 DES 密钥 Kc）；Kc，tgs 是 C 和 TGS 间的会话密钥；TGS 拥有 Ktgs，可以解密 Tickettgs，然后使用从 Tickettgs 得到的 Kc,tgs 来解密 Authenticatorc；将认证符中的数据与票据中的数据比较，以验证票据发送者就是票据持有者。**7）Kerberos 安全性**：(1)时间同步:整个 Kerberos 的协议都依赖于时钟；(2)口令安全性；(3)重放攻击（Ticket 的生存时间）；(4)密钥的管理（认证中心保存大量的共享私钥）；(5)对系统程序的破坏（如恶意篡改登录程序）。

16、Oauth：1）应用实例：用户在两家服务提供商的网站上各自注册了两个用户，假设这两个用户名各不相同，密码也各不相同。当用户要使用服务 B 打印存储在服务 A 上的图片时，用户该如何处理？**方法一**：用户可能先将待打印的图片从服务 A 上下载下来并上传到服务 B 上打印；**方法二**：用户将在服务 A 上注册的用户名与密码提供给服务 B，服务 B 使用用户的帐号再去服务 A 处下载待打印的图片；**方法三**：OAuth 为用户提供了一种方法，可以使服务 A 在用户的许可下产生一令牌发送给服务 B，服务 B 使用此令牌便可以访问用户在服务 A 上存储的的资源。此方法避免了用户直接将服务 A 的用户名和密码告诉服务 B 而造成用户信息泄露的问题。**2）概念定义**：OAuth 协议为用户资源的授权提供了一个安全的、开放而又简易的标准。**3）基于令牌模式的授权**：允许用户提供一个令牌，而不是用户名和密码来访问他们存放在特定服务提供者的数据。每一个令牌授权一个特定的网站在特定的时段（例如，接下来的 2 小时

内）内访问特定的资源（例如仅仅是某一相册中的视频）。**4）OAuth 中的三种角色**：服务提供方（拥有需要授权才能使用的 API 的一方）、应用程序方（希望使用 API 的一方）、最终用户（资源的拥有者）。

第七章 安全协议

1、主要安全协议：1）**网络接口层**：PAP(密码认证协议)、CHAP(挑战握手认证协议)、PPTP(点对点隧道协议)、L2F(第二层转发协议)、L2TP(第二层隧道协议)、WEP(有线等效保密)、WPA(Wi-Fi 网络保护访问)；2）**网际层**：IPSec(IP 层安全协议)；3）**传输层**：SSL(安全套接字层)/ TLS(安全传输层)；4）**应用层**：SSH(安全外壳协议)、Kerberos、PGP(Pretty Good Privacy)、S/MIME(安全的多功能 Internet 电子邮件扩充)、S-HTTP(安全超文本传输协议)、SET(安全电子交易)。**2、隧道技术**：1）被封装的数据包在外层网络（如：公共互联网络）上传递时所经过的逻辑路径称为隧道；1）三要素：入口，出口，隧道封装协议。**3、虚拟专网 VPN**：1）VPN 使用户通过公用网络（如 Internet)安全地访问企业网络(如 Intranet，Extranet)；2）名字含义上理解 VPN：(1) 虚拟：不是企业自己用专线连接的；(2)专网：统一的地址策略/统一的管理策略/安全性，具有企业网络的安全性，只有合法用户才可访问，网络上传送的数据只有专网中的用户才可见；3）种类：(1)从用户类型的角度：a.拔号用户: access VPN (VPDN); b.企业用户：site-to-site VPN (Intranet , Extranet VPN); (2)采用的技术角度: a.二层 VPN:利用 ATM, FR, MPLS 等二层虚连接技术; b.三层 VPN：IP 安全隧道技术, MPLS; c.应用层 VPN：SSL VPN。**4、网络层安全协议**：1）**IP 包的不安全性**：a.能很容易伪造 IP 包的地址、修改内容、重播以前的包及在传输中途拦截并查看包的内容; b.不能保证 IP 包(来自原先要求的发送方(源地址)/包含的是发送方当初放在其中的原始数据/原始数据在传输途中未被其他人看过)；**2）IPSEC**：**(1)**IPSec 为 IP 及上层(UDP 和 TCP)提供的**保护形式**：数据源验证/无连接数据的完整性验证/数据内容的机密性(是否被人看过)/抗重发保护；**(2)IPSEC 的体系结构**：**a.**包括以下几个基本部分：**AH**(认证头：认证、完整性检查，可选的重发保护)、**ESP**(封装安全载荷：机密性、认证、可选的重发保护、完整性检查)、**IKE**(密钥交换协议)、**SA**(安全关联)、**DOI**(解释域)、认证和加密算法；**b. SA** 是 IPSec 的基础,决定通信中采用的 IPSec 安全协议、散列方式、加密算法和密钥等安全参数,通常用一个三元组（安全参数索引、目的 IP 地址、安全协议）唯一表示。**SA** 总是成对出现的,对等存在于两端的通信实体,是通信双方协商的结果；**c. AH 或 ESP** 提供的安全保障完全依赖于它们采用的加密算法,因此需要一系列强制实行的加密算法；**d.**IPSec 提供的安全服务需要用到共享密钥,因此定义了一种标准的方法,用以动态地验证 IPSec 参与各方的身份、协商安全服务以及产生共享密钥等---**IKE(Internet 密钥交换)**。(3) **IPSec 的实施**：**a.** IPSec 可以在终端主机、网关/路由器或两者中同时进行实施和配置；**b.**在主机实施(保障端到端的安全/能够实现所有 IPSec 安全模式/能够逐数据流提供安全保障/在建立 IPSec 的过程中,能维持用户身份的验证)；**c.**在路由器实施(能对通过公共网在两各子网之间流动的数据提供安全保护/能进行身份验证,并授权用户进入私有网络 VPN)。(4) **IPSec 的模式**：IPSec 可以用来保护一个完整的 IP 载荷，也可以用来保护某个 IP 载荷的上层协议,是通过两种不同模式来完成的：**a.**传送模式(保护上层协议及 IP 头的部分字段，只用于基于主机的实现); **b.**通道模式(保护整个 IP 数据报)。**3)安全联盟(SA)**：是构成 IPSec 的基础，是两个通信实体经协商建立起来的一种协定。**(1)决定**：用来保护数据包安全的 IPSec 协议(AH,ESP)/算法/密钥/模式/密钥的有效存在期; **(2)特点**：SA 是单向的、与协议相关、SA 数据库(SADB)用来维持 SA 记录、安全策略数据库(SPD, 定义了安全通信特性;什么时间使用什么安全协议;如何对待 IP 包(对一个包提供的安全服务)); **(3)如何确定采用什么 SA?** 安全参数索引 SPI、IPSec 协议(AH, ESP)、方向。**4)安全参数索引 SPI**：**(1)**SPI 是一个 32 位长的数据实体,用于独一无二地标识接收端上的一个 SA; **(2)**由于 SA 是通信双方约定的密钥、加密算法等参数，需要告诉收方用哪个 SA 来保护这个数据; **(3)**SPI 被当成 AH 和 ESP 的一部分,随每个数据包发送; **(4)**由接收端/目标主机维护 SPI 与 SA 之间映射的唯一性。**5、Internet 密钥交换(IKE 协议)**：**(1)作用**：代表 IPSec 对 SA 进行协商、对 SADB 数据库进行填充。**(2)** ISAKMP、Oakelay 和 SKEME 这三个协议构成了 IKE 的基础。**(3)协商 SA**(IKE 利用 ISAKMP 语言来定义 SA 协商和密钥交换需要的信息)、**生成安全的密钥**(通过安全的交换过程实现)。**(4)密钥生成过程**：IKE 使用了两个阶段的交换。第一阶段建立 IKE 的 SA；第二阶段利用这个协商好的 IKE SA，为 IPSec 协商具体的 SA，对消息提供源验证、完整性以及机密性保护。**(5)** IKE 定义了 2 个阶段一交换，1 个阶段二交换。**阶段一的交换**：主模式（身份保护交换以及对 ISAKMP 协商能力的完全利用）；野蛮（积极）模式（野蛮交换）(当使用公共密钥加密来验证时，积极模式仍然提供身份保护); **阶段二的交换**：快速模式交换(用它为其他安全协议(IPSec)生成相应的 SA)。**(6) IKE 协议的安全保护**：**cookie**(为了抵御 DOS 攻击，密钥交换前先采用 cookie 交换，以确认对方能收到回应，然后才进行密钥交换和计算)、**nonce**(伪随机数 nonce 在 IKE 交换中随信息一起发送，在一定程度上防止重播攻击)、**完整性保护**(IKE 协议通过交换验证载荷(包含散列值或数字签名)保护交换消息的完整性,并进行身份认证)、身份验证(主模式或积极模式中都允许四种不同的验证方法：预共享密钥/公钥签名认证方式/公钥加密的认证方式/改进的公钥加密认证方式)。**6、传输层安全协议**：**(1)** 可在传输层上提供保密、认证和完整性检验功能；**(2) SSL(安全套接字层)**：**a.**采用 PKI(Public Key Infrastructure), 提供 CIAN(安全属性缩写); **b.**广泛用于 HTTP 连接; **c.** SSL 提供的安全服务：认证（客户对服务器的身份认证(SSL 服务器允许客户的浏览器使用标准的公钥技术和一些可靠的认证中心(CA)的证书，来确认服务器的合法性)、服务器对客户的身份认证(也可通过公钥技术和证书进行认证,也可通过用户名, password 来认证))、建立服务器与客户之间安全的数据通道（传输数据的机密性/传输数据的完整性）、密钥交互。**(4)TLS**：**a.** TLS 记录协议，位于可靠的传输协议（例如 TCP）上面; **使用 TLS 记录协议的上层为握手协议**（**握手协议**(建立客户与服务器之间的安全通道,包括双方的相互认证,交换密钥参数)、**告警协议**(向对端指示其安全错误：致命错误/警告消息)、**修改密码规格协议**(改变密码参数)；**b.记录协议两个基本安全特性**：机密性、完整性；**c.安全性分析**：中间人攻击、易受 DOS 攻击、流量数据分析攻击；**d.存在问题**：密钥管理问题、加密强度问题、不严谨的实现（man in the middle 攻击）、gotofail（苹果 SSL/TLS（对签名的认证不会失败））、Heartbleed 安全漏洞（获得服务器私钥）。**(5)WTLS**：Wireless Transport Layer Security