**问答和讨论：**

1. **对称算法DES/AES/RC4/3DES特点、安全特性与适用场合；**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 算法 | DES | AES | RC4 | 3DES |
| 分组长度 | 64 | 128 | 流密码 | 64 |
| 密钥长度 | 56 | 128/192/256 | 可变 | 112/168 |
| 相对速度 | 较快 | 慢 | 很快 | 较快 |
| 迭代轮数 | 16 | 10/12/14 | ---- | 48 |
| 安全强度 | 依赖密钥受穷搜索法攻击（2^57） | 安全级别高，高级加密标准 | 很难 | 相比DES，大大提高了安全性 |
| 是否feistel | 是 | 不是 | 不是 | 是 |

DES: 1.8 适用于加密大量数据，古典算法，老程序中，强度弱

3DES: 加密：C=Ek3(Dk2(Ek1(P)))  解密：P=Dk1((EK2(Dk3(C)))

相比DES，大大提高了安全性。

RC4: 1.17 轻量级，个人场合

AES: 1.10 新环境，关键场合

1. **RSA原理与计算，给p、q、e、c求d和m；**

试题二（3）

1. **公钥算法的用途，从加密(传递会话密钥)到签名；**
2. **Hash函数的特性与用途；**

单向函数，将任意长度的消息映射为固定长度的散列值（消息摘要），以该散列值作为认证码。对于消息认证码，安全散列函数必须以某种方式和密钥捆版起来。

特性：1.输入可变长度的分组，输出固定长的分组。

2.任意x,计算H(x)容易，软硬件都可以实现。

3.单向性。已知H(x)=h，求x在计算上不可行。

4.抗弱碰撞性。任意x，找y，是H（x）=H（y）计算上不可行。

5.抗强碰撞性。找到满足H（x）=H（y）的x，y计算上不可行。

用途：（和其他算法配合实现）

1.认证。（数据完整性的认证，数据源的认证） 2.保证数据完整性。

1. 数字签名。（双方事先协商好都支持的Hash函数和签名算法） 4.给明文增加结构特征以保护明文。 5.产生MAC码 6.产生伪随机数 7.PKCS#5中从口令衍生密钥
2. 挑战应答 9.用作预防重放攻击的一次性值 10.系统文件防护和P2P共享方面。常用来唯一标识一个文件。 11.时间戳 12.证书

王晓云教授用她的方法找到相同hash值的效率很高，说明hash并不想人们想象的安全。

1. **随机数的特性与用途；**

**特性：** 随机数应有随机性和不可预测性。应达到以下质量要求：1.均与分布。在任何尺度上看其统计规是律均匀的。 2.独立性。没有周期，无法预测和推导。

**用途：**1.会话密钥 [需保密] 2.用来产生公钥 [需保密] 3.对称算法产生密钥 4.S盒的构造 5.很多挑战-应答协议里的挑战值 [不需保密] 6.D-H协议中的临时交互号

7.传输填充 8.鉴别方案中用来避免重放攻击 nonce [不需保密]

9.salt in /etc/passwd etc [不需保密]

安全不仅依赖于密钥的保密，也依赖于随机数的质量

产生：1.随机数做种子产生随机数 2.真随机数发生器，伪随机数发生器 3.线性拟合发生器 4.基于加密算法产生随机数

1. **以PKCS#5为代表的，从口令衍生密钥加密文件的方法；**

盐和迭代次数构成了PKCS#5中基于口令加密的基础。基于口令的密钥导出是口令、盐和迭代次数的一个函数，其中后两个量不需要保密。

口令作为输入加密程序的密钥，加密算法需用“盐”值修改（通常，盐值与用户口令产生的时间有关），输出结果作为二次加密的输入，经过迭代，最后可以得到密文进行文件的加密。

口令是实现认证的最简单的方式，具有正确的口令才有权访问某些资源或进行某些操作。密钥是加密算法函数中一个参数。用口令得到密钥的方式可以用hash算法实现，输入任意的口令，经过hash得到固定长度的密钥。

1. **以PGP为代表的邮件/文件的加密交换/存储方案；**
2. 发送方生成消息，产生作为会话密钥的128位随机数（MD5）
3. 发送方用自己的私钥对数据的HASH值进行数字签名
4. 用会话密钥加密消息和签名
5. 用对方的公钥按RAS加密产生的会话密钥，将这些消息组传给对方。
6. 接收方用自己的私钥按RAS解密回复会话密钥。
7. 用会话密钥解密消息，用对方公钥验证签名
8. **破解，7475方法等，对抗破解的方法的讨论**

软件经过破解之后就会变成破解版。原软件需要注册收费的，不注册的话只能试用一段时间，而且有的软件试用版会限制某些功能，有些还要在启动时等上一会，而破解版的就是不会出现这些情况。  
 学习一下破解，你就会知道没有软件是不可以破的

在讨论对抗破解时，首先要清楚一个问题——你的软件值不值得保护

1. 不要用有意义的过程名字。可以把程序中需要的一部分代码置入其内，如果破解者禁止了这个函数，你的程序将产生错误的结果。   
   3.用好的加密算法进行加密  
   4.加上长时间延迟，当发现被自身被损坏时，不要发出警告，随后开始等待。   
   5.加入短暂延迟，当输入口令或做其它检测时，停一到两秒钟，使穷举无法继续。

6.使用相互检查，在DLL和EXE中互相检查，这可以使破解变得更困难。   
7.在软件中使用自我修复。如果破解者使用反编译工具，它会见到一串无用的列表。   
8.修补你的软件！把代码变为每次调用不同的确认程序段。   
9.把序列号放在不寻常的地方    
11.使用“保留字”，当使用硬密钥或口令时，使它们看来像程序代码或者函数调用，可以迷惑一些反编译工具。   
12.避免不必要的提示信息，多余提示信息会引导对你代码的反向工程而且经常直接引导至你的程序保护代码。   
13.经常更新，经常更换代码，典型（简单）的破解只修改你的硬字节代码位置，这可能当它还未面市已经过期了。并且保证上载到公共服务器，使你可以更好的控制程序，人们无法找到破解所针对的旧版本。

14.毁坏结果，毁坏结果有时是保护程序的有效措施。   
15.不要依赖EXE压缩程序，几乎任何EXE压缩程序都有反压缩程序。

16.到处贴条件转移   
17.贴上连续的NOP。混乱的注释代码。把代码分成小块，把它们遍布在可执行代码中，在它们中间使用跳转。   
18.提早发现SoftIce.。   
19.不要用由双击按钮或有属性监视器生成默认的方法，在程序的其它部分写代码，最好是在另外的模板中，然后用代码与按钮关联。  
20.注册码输入区必须无限制的接受任何长度的信息。  
21.从用户名到注册码不应该只有简单的运算，它必须是有既精通数学又精通汇编语言的人用汇编语言实现。   
22.要有创新意识，不要用任何看起来简单、迅速、有效的东西。

1. 在服务器上认证
2. 对软件中重要的数据进行加密变换
3. delphi 软件的保护，基于 delphi 为核心的软件将被反编绎，但以 mck 为核心编 绎的软件则在 dede 中至今还是很安全的
4. 锁住键盘，鼠标，防止被调试
5. 读完注册码后不要立刻检查注册码
6. 在检查前分散隐藏注册码，或者可以在读到注册码后，多次将注册码在内 存的各个位置做大量拷贝，这最多浪费一些内存
7. 程序多处做 CRC 校验文件大小检查，发现不对就退出。
8. 用 inline 函数将注册部分分成许多小块， 分散到程序各处运行
9. **序列号+在线激活，经常检查重复序列号。**
10. **反调试器**
11. **代码虚拟化**
12. **垃圾指令**
13. **代码有暗桩（改动就会蓝屏，死机，硬盘格式化等）**
14. **把核心代码放在云上**
15. **混淆代码，对发布出去的程序进行重新组织和处理，使得处理后的代码与处理前代码完成相同的功能，即使反编译成功也很难得出程序的真正语义。**
16. **将核心代码使用NDK进行编程**
17. **花指令，借助于反编译工具的bug，在自身代码中添加特定代码，让反编译工具无法正常运行**
18. **底层验证签名**

**最好的办法，会让大家都富起来啊·····**

1. **逆向，比如针对apk的，以及对抗逆向的方法的讨论；**

逆向：根据已有的东西和结果，通过分析来推导出具体的实现方法

1.混淆代码，对发布出去的程序进行重新组织和处理，使得处理后的代码与处理前代码完成相同的功能，即使反编译成功也很难得出程序的真正语义。

2.将核心代码使用NDK进行编程

3.花指令，借助反编译工具的bug，在代码中添加特定代码，让反编译工具无法正常运行

4.底层验证签名

5.通过java代码对APK(压缩文件)进行伪加密，解压是提示需要输入密码

6.标志尾添加其他数据对，使解压工具认为其已经损坏

7.Art虚拟机

8.将核心代码使用C/C++编写然后编译成为.so文件

9.DEX文件隐藏（加壳技术）

1. **缓冲区溢出；**

[缓冲区](http://baike.baidu.com/view/266782.htm" \t "http://baike.baidu.com/_blank)溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。

[缓冲区](http://baike.baidu.com/view/266782.htm" \t "http://baike.baidu.com/_blank)溢出可以作为一种系统攻击的手段，通过向程序的缓冲区写入超出其长度的内容，造成[缓冲区](http://baike.baidu.com/view/266782.htm" \t "http://baike.baidu.com/_blank)溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。简单的说就是程序对程序对接受的输入数据没有进行有效的检测而导致错误，后果可能造成程序崩溃或者执行攻击者的命令。在C语言中，常见的造成[缓冲区](http://baike.baidu.com/view/266782.htm" \t "http://baike.baidu.com/_blank)溢出的函数有：

sprintf（），vsprintf（），gets（），scanf（）等。

1. **计算器病毒的机制与防范讨论；不光关心windows，也要考虑linux，更要关心手机，包括安卓和苹果。**

电脑病毒是一种具有自我复制能力的计算机程序。它在传播期间一般会隐蔽自己，由特定的出发条件触发开始产生破坏。病毒的特性是传染，潜伏，触发，破坏。传染使得病毒以传播，潜伏使得病毒不易被发现，破坏体现了病毒的杀伤能力，而可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒感染和破坏的频度，兼顾杀伤力和潜伏性。

**计算机病毒的运作机制**

(1)引入：病毒的引入依赖于病毒的来源，一般病毒的引入者是非授权的。

(2)存储：病毒的存储方式有BIoS驻留方式、内存驻留方式、注册表驻留方式和文件驻留方式等。

(3)控制：计算机病毒的存在和控制要受操作系统的制约。任何病毒，都需要适当的时机来夺取系统的控制权，并利用控制权来执行传染和破坏。

(4)触发：所有的触发条件，必须在病毒程序获得系统控制权限后才能够作用。

**计算机病毒的触发机制**

(1)日期触发：许多病毒使用此种触发方式，例如：CIH病毒就是在4月26日发作。日期触发还包括：特定日期触发、月份触发、前半年或后半年触发等。

(2)时间触发：是指在特定时间触发、染毒后累计工作时间触发等。

(3)键盘触发：是指病毒监视用户的击键动作，当发现病毒预定的键入时，病毒被激活，进行某些特定操作。

(4)感染触发：许多病毒的感染需要某些条件触发，而且相当数量的病毒又以与感染有关的信息反过来作为破坏行为的触发条件。

**计算机病毒的破坏机制**

通过修改某一中断向量入口地址(例：时钟中断INT 8H)，使该中断向量指向病毒程序的破坏模块。这时，当系统或被加载的程序访问该中断向量时，病毒破坏模块被激活，在满足条件的基础上，对系统或磁盘上的文件进行破坏活动。

**Windows**

(1)坚持从不带毒的硬盘引导系统。

(2)安装能够实时监控引导扇区的杀毒软件，或经常用能够查杀引导型病毒的杀毒软件对系统进行检查。

(3)经常备份系统引导扇区。

(4)某些底板上提供引导扇区计算机病毒保护功能，启用它对系统引导扇区也有保护作用。

(5)安装最新版本的、有实时监控文件系统功能的查杀毒软件，并经常对系统进行查杀。

(6)及时更新查杀毒引擎，一般每月至少更新一次，并在计算机病毒突发事件时及时更新。

(7)对关键文件，如系统文件、保密的数据等，要在没有计算机病毒的环境下经常备份。

(8)在不影响用户正常工作的情况下对系统文件设置最低的访问权限,防止文件型病毒。

**Linux**

Linux 防毒比 Windows 容易的多

1. 做好系统加固工作。  
   (2)留心安全公告，及时修正漏洞。  
   (3)日常操作不要使用root权限进行。  
   (4)不要随便安装来历不明的各种设备驱动程序。  
   (5)不要在重要的服务器上运行一些来历不明的可执行程序或脚本。  
   (6)尽量安装防毒软件，并定期升级病毒代码库。  
   (7)对于连接到Internet的Linux服务器，要定期检测Linux病毒，有专人负责管理。  
   (8)对于提供文件服务的Linux服务器，最好部署一款可以同时查杀Windows和Linux病毒的软件。  
   (9)对于提供邮件服务的Linux服务器，最好配合使用一个E-mail病毒扫描器。
2. 充分发挥防火墙作用

**安卓**

1.不要打开手机接收到的陌生号码发送的信息或链接。

2.不要下载并安装任何来历不明的软件。

3.使用SD卡、T-FLASH等内存卡交换数据时注意防止病毒感染。

4.隐藏或关闭手机的蓝牙功能，以防手机自动接收病毒，更不要安装通过蓝牙发送过来的可疑文件。

5.平时对手机内的电话本及重要信息要经常性备份，以防感染病毒后丢失。

6.建议给手机安装适用的杀毒软件，并关注最新手机恶意软件及病毒的信息及防范措施。

7.不要随意蹭网，注意公共WiFi网络的安全问题。

**苹果**

ios系统是封闭的，因此安全性比安卓要高，但并不代表绝对安全，尤其对于某些越狱机。

1.及时更新操作系统和软件，安装最新的安全补丁。

2.运行一款反病毒产品或安全套装。Avast、Avira等

3.不要下载并安装任何来历不明的软件。

1. **讨论比特币中的密码技术是如何起关键作用的；**
2. **文件加密存储，360密盘、truecrypt、ntfs的文件夹绿色加密、bitlock等机制与原理；**
3. **考虑这3个应用：电商及网银、无纸化办公、QQ。有哪些安全问题和需求、目前是怎么做得，该怎么注意安全，该怎么改进或解决。另，网银u盾和动态口令牌，原理或机制上有啥区别？**

**电商及网银**

网络购物时需要提供真实姓名，手机号，身份证号，银行卡号等详细信息，而这些信息与消费者的个人隐私和财务安全息息相关，一旦网站或哪个环节出了问题，消费者的个人隐私和财务安全就会收到威胁。银行卡盗刷；仅需手机验证，快捷支付存在风险；

信息真实有效；信息机密性（保证客户或商户的信息不被泄露和篡改）；信息可靠性（合法用户对信息资源的使用不会被拒绝），不可抵赖性（有效的责任机制，防止实体否认行为），可鉴别性；信息完整性；电商系统和网银系统的可靠性（防止计算机失效，程序错误等）；资金在网上划拨，交易的安全性；登录密码或支付密码应该加密；防备恶意攻击；

系统层--采用安全web服务器模式；采用安全认证系统；建立安全监控工作站；采用安全的管理措施 应用层--数据加密技术（数字签名，数字时间戳，数字证书）；身份认证技术（PKI体系结构，公钥密码和对称密码结合起来，实现公钥自动管理）；SSL和SET协议；交易密码；登录密码与支付密码分离；登录验证码，预留信息提示，手机绑定，操作短信提示；账户变动短信提示；检测证书，核对登录密码，通报系统访问次数；动态口令，短信（一次一密）；密码的软键盘技术；RSA加密；完善的身份认证和CA认证系统；判断假冒网站（注册时只有我和服务器知道的特殊字符）；口令账号保护；针对互联网访问进行限制，正确识别网上客户和商户的身份；控件对抗口令监控软件；登录口令加密；

完善相应法律法规；

**无纸化办公**

电子文档的安全性备受瞩目。在无纸化办公中，别有用心者仅用一个U盘，几条命令或者一封邮件就可以将机密文档泄露出去，还有可能导致重要资料的流失，篡改等等。

办公系统的可靠性，防止被入侵者入侵；信息载体（U盘，手机等的安全，防泄漏）；网络交换设备和网络路由设备的安全可靠性；各级网络应具有网络监督和管理能力；拒绝未经授权的访问；上传电子签署文件时不会被截取，篡改；信息真实有效；信息机密性（保证客户或商户的信息不被泄露和篡改）；信息可靠性（合法用户对信息资源的使用不会被拒绝），不可抵赖性（有效的责任机制，防止实体否认行为），可鉴别性；信息完整性；

**使用VPN技术；传输信息用加密算法加密；安全web服务器模式；采用SSL协议；数据库的安全（备份，数据库用户身份鉴别，对使用数据库的时间地点加以限制）；使用数据库管理系统提供的审计功能，跟踪每个用户对数据库的操作；防病毒软件，防火墙，web,email的安全监测系统；漏洞扫描系统；利用网络监听维护子网系统安全；关键设备和线路的冗余，能够在线修复；优秀的网管系统对网络进行监控；**数据加密技术（数字签名，数字时间戳，数字证书）；身份认证技术（PKI体系结构，公钥密码和对称密码结合起来，实现公钥自动管理）；及时补丁安装和修补漏洞

通盘考虑文件信息在政府部门中可能的多种存在状态，以及可能的访问途径，对涉及到文件的所有操作包括访问、打印、网络传输、移动存储等进行全面控制，严格限制非法计算机接入，防止重要信息外泄，帮助做好保密工作！

对网内终端运行的应用程序的全面审计，杜绝危险程序，合理限制无关程序使用；通过对网页浏览与流量的全面审计，规范网络应用，保证正常政务运行效率，同时杜绝网络滥用带来的安全隐患；

对于用户个人：

增强安全意识，在网络账户的使用上多花心思：个人电脑和智能手机安装杀毒软件，防患于未然；手机开启骚扰拦截功能可一定程度屏蔽恶意来电和短信；不浏览，不注册不良网站；不轻易在公开场合暴露个人信息；网银，支付账户尽量设置复杂密码，并不要与其他网络账号相同；尽量使用动态口令；定期更换网络账户密码

以上方法只是尽可能降低网络账户被盗取的可能性，并非绝对安全，因为账户信息最终还是放在企业的服务器中，一旦企业网站受到攻击，我们的利益仍可能受到损害。同时我们也呼吁电商能够以正确的态度面对信息安全事件，不但可以有效的帮助消费者解决问题，也有助于企业获得消费者的理解和宽恕。

**网银u盾和动态口令牌，原理或机制上的区别**

**U盾**是用于网上银行电子签名和[数字认证](http://baike.baidu.com/view/2120092.htm" \t "http://baike.baidu.com/_blank)的工具，它内置微型[智能卡](http://baike.baidu.com/view/30512.htm" \t "http://baike.baidu.com/_blank)[处理器](http://baike.baidu.com/view/50152.htm" \t "http://baike.baidu.com/_blank)，采用1024位非对称[密钥](http://baike.baidu.com/view/934.htm" \t "http://baike.baidu.com/_blank)算法对网上数据进行加密、解密和数字签名，确保网上交易的[保密性](http://baike.baidu.com/view/992854.htm" \t "http://baike.baidu.com/_blank)、真实性、完整性和[不可否认性](http://baike.baidu.com/view/3871580.htm" \t "http://baike.baidu.com/_blank)。U盾又作[移动数字证书](http://baike.baidu.com/view/394486.htm" \t "http://baike.baidu.com/_blank)，它存放着你个人的数字证书，并不可读取。

当你尝试进行网上交易时，银行会向你发送由时间字串，地址字串，交易信息字串，防重放攻击字串组合在一起进行加密后得到的字串A，你的U盾将根据你的个人证书对字串A进行不可逆运算得到字串B，并将字串B发送给银行，银行端也同时进行该不可逆运算，如果银行运算结果和你的运算结果一致便认为你合法，交易便可以完成，如果不一致便认为你不合法，交易便会失败。

**动态口令牌**是一种内置电源、密码生成芯片和显示屏，根据专门的算法，每隔一定时间自动更新动态口令的专用硬件。基于该动态密码技术的系统又称一次一密（OTP）系统，即用户的身份验证密码是变化的，密码在使用过一次后就失效，下次使用时的密码是完全不同的新密码，使得不法分子难以仿冒合法用户的身份。作为一种重要的双因素认证工具，动态口令牌被广泛地运用于安全认证领域。动态口令牌可以提升网上银行的登录和交易安全。

不需要安装驱动，不用连接电脑，不用记忆密码，只需输入液晶屏显示的6位数字就可以验证用户的身份。

1. U盾安全性高，只需办理一次，就能永久使用，但是必须插入电脑上才可以使用。
2. 动态口令卡有使用次数的限制，口令使用完之后，还要到银行重新办理新的动态口令卡，动态口令卡使用携带比较方便。
3. **那些泄漏案例引发的思考。素材：用户名、口令、邮箱、qq库、开房记录、云中照片、12306、CSDN、tianya、Ashley-Madison，以及传说但是后来未经证实的163的5亿邮箱，等。对于这些泄漏案例，你可以猜测、分析其泄漏的途径和机制，给出你的看法、建议，尤其是针对当前使用的登录、存储、备份、管理、立法等方面的某些缺陷，从技术、管理、立法方面，你有什么建议、改进方案等，深入思考、讨论一下。**

防泄密的最终效果完全取决于整个防护环节中最薄弱的地方。

途径：多种多样，在企业内部，有可能有以下途径

1.通过USB口拷到U盘，移动硬盘等移动存储介质带离公司

2.通过3G上网卡等连接网络，把信息通过网络带走

3.将文件通过邮件发送给外部人员

4.打印，把电子文档转换成纸质文档带走

5.通过共享目录将文件拷贝到笔记本电脑带离公司

6.电脑或硬盘丢失则难以防范；

7.补丁安装和修补漏洞不及时

8.管理及操作人员缺乏安全知识-----对操作管理人员的培训显得尤为重要

9.打印机和传真机输出的信息过度暴露。部门之间的机密文件就可以从设备室开始，在其他部门传播

10.企业员工跳槽，但是电脑易手问题没有妥善解决

11.向企业的客户提供资料时没有考虑到企业敏感信息泄露的可能性。在发布的信息中应该出现“此为本公司机密信息，请保密。”字样，并在事前签订保密协议，但是目前企业根本没有考虑到这个问题，也没有规定信息安全对应到每个员工的责任。

12.没有实现集中化的安全管理

外部：

1. 攻击者可以采用如Sniffer等网络协议分析工具，在网络安全的薄弱处进入网络，并非常容易地在信息传输过程中获取信息内容。
2. 系统内部攻击者伪装成系统内部的其他正确用户

3.通过通信电缆进行传输，极易受到雷击，造成连锁反应，使整个网络瘫痪，设备损坏-----防雷

**技术**

1.通过完整的文档操作审计发现网内安全的威胁，及时进行防御

2.根据企业内部的部门和职位划分立体化的保密体系，对数据的使用权限控制要细化，同时对网络和外部设备等可能的泄密渠道加以控制，防止文档外流。外发的文档，和内部使用一样，受到加密保护和泄密控制，不会造成文档内容泄露

3.高强度的透明加密保证文档在任何地方都能得到有效保护

除了加密外还应该包括密钥管理、身份认证、访问控制、安全审计等一系列的安全防护手段。

4.PCI-DSS compliance 以及信用卡3D验证，其中PCI 是预防信息泄漏， 3D是防止盗取信息者牟利

5.防火墙，入侵检测（IDS），漏洞扫描，防病毒

6.运用协议分析和模式匹配方法 可以动态地调整防火墙的防护策略，使得防火墙成为一个动态的智能的的防护体系

7.有效的用户口令和访问控制，确保只有合法用户才能访问合法资源。

8.数据备份，对于重要的服务器，利用RAID5等数据存储技术加强数据备份和恢复措施；对敏感的设备和数据要建立必要的物理或逻辑隔离措施。

9.选用安全设备

10.重要信息点防电磁泄漏

11.VPN

12.用户统一使用USB-KEY进行身份认证

**管理**

1. “白帽子”们提交的漏洞经常得不到网站管理员的重视
2. 要有系统管理的思想。主动防御，做好前期的预防，采用建立在风险评估基础上的动态的持续改进的管理方法。
3. 安全技术和安全管理（管理的技术和流程，以及员工的管理）同样重要。
4. 在管理上采取逐级纵向管理的方式
5. 制定相应的安全管理制度和内部的法规政策
6. 在主管部门直接领导下，自上而下地构建层次清楚、职责明确的安全组织体系。
7. 成立安全工作小组，对内部人员进行安全教育和管理，指导、监督和考核安全制度的执行
8. 设置三个层次的安全管理机构：决策层、管理层和执行层。决策层是决定系统安全重大事宜的领导机构，由主管信息工作的负责人为首。管理层是决策层的日常管理机关，根据决策机构的决定全面规划并协调各方面力量实施信息系统的安全方案，制定、修改安全策略，处理安全事故，设置安全相关的岗位。执行层是在管理层协调下具体负责某一个或某几个特定安全事务的一个逻辑群体，这个群体分布在信息系统的各个操作层或岗位上。

**立法**

1.在现行法律下，执法机构抓不到黑客的话，也很难追究到网站的责任，这个苦水就只有自己吞了。而在国外， 身份窃取或者是信用卡诈骗都是联邦重罪， 为了预防和打击可能的犯罪，信用卡公司和金融机构每年投入大量的经费，联合治理网络支付安全。

2.中国网民的安全意识需要普及。

3.规范信息安全管理措施，配合信息[安全服务](http://www.chinabyte.com/keyword/%E5%AE%89%E5%85%A8%E6%9C%8D%E5%8A%A1/" \t "http://sec.chinabyte.com/412/_blank)[企业的技术](http://www.chinabyte.com/keyword/%E4%BC%81%E4%B8%9A%E6%8A%80%E6%9C%AF/" \t "http://sec.chinabyte.com/412/_blank)手段为数据资产建立安全屏障